официальное сообщение Безоп

26 сентября, 2017

Безоп

Беком Блокчейн

Чтобы ознакомиться с научной работой нажмите ссылку Актуальные исследования

и новые версии этой статьи будут предоставлены по ссылке [https://bezop.io](https://bezop.io/). Для заявлений и комментариев обратитесь к нам по адресу researchHYPERLINK "mailto:research@bezop.io"@HYPERLINK "mailto:research@bezop.io"bezopHYPERLINK "mailto:research@bezop.io".HYPERLINK "mailto:research@bezop.io"io

**Содержание**

**1 Введение** ……………………………………………………… 3

1.1 Базовые компоненты …………………………………… 4

1.2 Сеть Эфириум и Токен ERC-20 ………………… 5

1.3 ​ Возможности рынка и бизнес-модель …………… 6

1.4 Облачный майнер Веб-сервисов Амазон в одно нажатие клавиши ……….. 9

**2 Минимальный жизнеспособный продукт**

2.1 Децентрализованное введение заказа в производство ……………………… 10

2.2 Технологии, требования и возможности …… 10

**3 Элементы программы краудсейла токенов**

3.1 Информация о программе токена ……………………………………….. 14

3.1.2 программа стимулирования ……………………………………………. 16

3.1.3 Бюджет………………………………………………………..……. 17

**4 План развития**

4.0.1 Выход шифра Рэйнбоу ………………………………….. 18

 4.1 Выпуск М.Ж.П……………………………………………………… 18

4.2 Запуск Краудсейла токена ………………………………………….. 18

4.3 Выпуск кошелька и интеграция Jvzoo …………………. 18

4.4 Выпуск децентрализованного управления заказами (Д У З)………….. 18

4.5 Выпуск кошелька…………………………………………………….. 18

4.6 Внедрение сети Безоп …………………………... 18

4.7 Усовершенствование Мессир (повышение уровня безопасности)....................... 18

4.8 Усовершенствование Андромеда (модернизация сети)............... 18

**5 Кто мы**

5.1 Наша миссия …………………………………………………………..19

5.2 команда Безоп …………………………………………………………. 20

**6 Ресурсы** ……………………………………………………………... 20

6.1 Общий обзор законодательной базы ……………………………………………………... 21

6.2 Важные даты ………………………………………………..….. 23

6.3 проверка …………………………………………………..………...… 23

6.4 ссылки ………………………………………………..…………… 23

**1 Краткое описание**

Безоп — это децентрализованная пиринговая электронная система управления и обработки заказов, автономная служба защиты покупателей-продавцов, и простая система сбора налога на добавленную стоимость (НДС) - все при поддержке смарт - контрактов и построены на децентрализованной сети блокчейн. Безоп направлена на предоставление полного открытого исходного кода для успешного ведения бизнеса электронной коммерции в Интернете. Торговые компании могут участвовать в продаже продуктов и услуг с собственным сервером в магазинах электронной коммерции (децентрализованное управление заказами Безоп или Безоп ДУЗ) и с заказами на вещательную рекламу в сети.

Площадка Безоп работает на блокчейне с прямым доступом к протоколу денежного знака ERC-20 (также называемым «Безоп»), который майнеры зарабатывают на блокчейне Эфириум посредством доказательства работы. Клиенты тратят валюту Безоп при покупке товаров и услуг в системе Безоп ДУЗ и на прочих интегрированных сайтах, которые предлагают услуги и принимают платежи в валюте системы Безоп. И наоборот, можно заработать валюту Безоп, продавая товары и услуги и / или просто получая деньги Безоп посредством перевода из кошелька в кошелек. В будущем появится сеть Безоп, где майнеры будут конкурировать по созданию бОльших блоков с бОльшими вознаграждениями. До этого мощность добычи системы Безоп будет пропорциональна активным заказам в сети, а это означает, что стоимость майнинга Безоп будет ограничиваться поддержанием договоренностей по блокчейну. Это создает мощный стимул для майнеров выполнять как можно больше заказов. Протокол ERC-20 сплетает эти накопленные ресурсы в сеть блокчейна целенаправленного самовосстановления, на которую может положиться любой человек в мире. Сильные методы защиты покупателей, встроенные в смарт-контракты, укрепляют надежность сети. Заказы шифруются сквозным через портал безопасного управления протоколом. У майнеров нет доступа к ключам дешифрования. Безоп работает в качестве стимулирующего слоя поверх блокчейна и вычисляет доказательство порядка для любой транзакции, что делает Безоп особенно эффективным для децентрализации платежей, создания и работы распределенных порталов электронной коммерции и реализации смарт-контрактов.

**1.1 Базовые компоненты**

Протокол Безоп основывается на шести компонентах из числа последних разработок:

**I.** **децентрализованное управление заказами ДУЗ**: портал управления заказами с открытым исходным кодом

**II. сеть Безоп:** Смарт-контракты дружественные к сети блокчейн

**III. Доказательство заказа:** Краткий обзор различных доказательств - подробности этих новейших

Доказательств заказа представлены в Разделе 3 (Подробная информация о программе токенов) в этой научной работе.

**A. Доказательств налога:** транзакция НДС содержит данные, указывающие на основную транзакцию - x должен быть рассчитан для правильности, посредством отбора бессмысленных данных на входе в γ.Φ.

Налоговые данные: {α|obj: val, γ|str: val, δ|float: val, ε:bool:val, x|str:val}

**B. Доказательство транзакции:** служат квитанции и показывает всю информацию о приобретенном продукте или услуге.

Данные транзакции: {α|obj: val β |str: val, γ₁|str: val, δ₁|float: val, ε:bool: val, tid|str: val}

**IV. Доказательство доставки:** Доказательства того, что товар или услуга доставлены

**V. Смарт-контракты и обещания Безоп:** Смарт - контракты обеспечивают полностью безопасные и надежные решения для электронной коммерции работающие безупречно вместе по протоколу доказательства заказа, и обеспечивая защиту покупателя через блокчейн.

**VI. Доказательство работы (ДР):** Безоп будет базироваться на той же системе ДР, что и Эфириум, которая будет доведена до полного «Доказательства Заказа», где майнерам не нужно тратить вычисления на блоки, а вместо этого подтверждать заказы в сети.

**1.2 Сеть Эфириум и токены ERC-20:**

Работающий на специально изготовленном блокчейне Эфириум, Безоп — это чрезвычайно мощная и прозрачная глобальная инфраструктура, которая может перемещать денежные средства, одновременно представляя принадлежность собственности. Это позволяет нам создавать площадки Безоп, хранить реестры сделок, поставки, статус заказа и налоги и переводить средства в соответствии с инструкциями, данными в прошлом (например, в завещаниях или фьючерсных контрактов). Такие возможности потенциально могут способствовать развитию многих будущих изобретений, без риска посредника или контрагента. Сила смарт - контракта, сеть Эфириум и децентрализованные платформы Эфириум гарантируют, что транзакции, которые обычно происходят в электронной торговле, могут быть выполнены в Безоп без какой-либо вероятности простоя, цензуры, мошенничества или вмешательства со стороны третьих лиц

**Корректность алгоритма**

Корректность алгоритма доказывает, когда говорят, что алгоритм является правильным в отношении спецификации. Функциональная правильность относится к поведению алгоритма на вводе-выводе (т. е. для каждого входа он производит ожидаемый результат).

Различают полную правильность, которая дополнительно требует завершения алгоритма и частичную корректность, которая просто принимают ответ как правильный, если он возвращается. Поскольку общее решение проблемы неалгоритмизированной задачи нет (проблема остановки), то общее утверждение о корректности может лежать гораздо глубже.

Проверка завершаемости программ — это тип математического доказательства, играющего важную роль в формальной проверке, поскольку полная правильность алгоритма зависит от завершения. Например, при последовательном поиске целых чисел 1, 2, 3, ... для определенного явления, скажем, для нечетного совершенного числа, легко написать частично правильную программу (используя длинное деление на два, чтобы проверить, является ли n совершенным или нет. Однако ни одна известная теория чисел не может поддерживать утверждение о том, что программа полностью правильная.

**1.3 Возможности рынка и бизнес-модель:**

По данным исследовательской компании «Бостон Консалтинг Групп», платежная индустрия переживает значительный сдвиг в сторону мобильных платежей:

● Объем мобильных платежей составил 8,6 млрд. долл. США в Соединенных Штатах. Ожидается, что к 2021 году он увеличится в 10 раз и достигнет 274 млрд. долларов США.

● Ожидается, что доля мобильных в электронной торговле возрастет до 48,5% к 2020 году. В 2015 году она составила 23,6%.

● Ожидается, что к 2020 году сеть приема платежей мобильных устройств вырастет в десять раз.

**1.3.1 Взрывной рост электронной торговли**

По данным портала «Статиста», электронные коммерческие продажи в мире в 2014 году составляли 1,33 трлн. долл. США и, согласно прогнозам, к 2020 году возрастут до 4,06 трлн. долл. Рост прекрасно иллюстрируется количеством магазинов, созданных на платформе «Shopify». На платформе было размещено 84 000 магазинов в 2013 году, 144 000 в 2014 году, 243 000 в 2015 году и почти 378 000 в 2016 году - рост на 450% за 3 года.

В глобальном масштабе электронная торговля также набирает обороты в общем объеме розничных продаж. Ожидается, что он увеличится с 7,4% в 2015 году до 14,6% в 2020 году.

доля электронной торговли в розничных продажах

статистика

<http://joxi.ru/J2bqvQLS4nq8km>

годовой рост

Кроме того, согласно сведениям портала Статиста, количество людей, покупающих товары или услуги в Интернете, увеличится с 1,46 млрд. В 2015 году до более 2 млрд. В 2020 году.

График – Количество людей, покупающих товары или услуги в интернет

<http://joxi.ru/V2VOqoVH0lGEEA>

Количество людей

**1.3.2 Объем транзакций и выручка от платежей по всему миру**

Индустрия платежей огромна. Общая стоимость глобальных розничных платежей оценивается в 16 трлн. долл. США в 2015 году. По прогнозам, к 2020 году этот показатель возрастет до 21 триллиона долларов.

Оценки включают транзакции между потребителями и продавцами через розничные вертикали, такие как продукты питания и бакалейные товары, одежда, потребительские товары длительного пользования и т. д. Цифровые платежи составили 1,26 трлн. долл. США, или 8% глобальных розничных платежей в 2015 году, и, согласно прогнозам, увеличится до 6,3 триллиона долларов США или 18-24%, к 2020 году.

Размер рынка глобальных платежей - примерно 2 триллиона долларов США и неуклонно растет. В большинстве случаев глобальные платежи — это доходы от платежей, которые включают прямые и косвенные доходы от безналичных платежных услуг (за исключением межбанковских переводов). Проще говоря, это общие доходы, собираемые компаниями финансовых услуг по всему миру.

Как показано на графике ниже, глобальные доходы от платежей должны достигнуть 2,2 триллионов долларов США за несколько лет.

График - выручка от платежей (в триллионах долларов)

<http://joxi.ru/xAeMPWaSY4VJbA>

Время

**1.3.3 Бизнес модель**

Безоп предоставляет систему программного обеспечения с открытым исходным кодом, в которой торговые компании могут продавать свои товары и услуги. Кроме того, Безоп предоставляет сеть, которая обрабатывает криптографические токены.

Эти токены являются принятой формой оплаты (монета Безоп).

Смарт-контракты Безоп будут автономно управлять состоянием заказа. В спорном случае, смарт-контракт может поручить субъекту права (человеку) принять окончательное решение.

«Безоп» взимает комиссионный сбор в размере 1,4% с торговых компаний. Из них 1% будет использоваться для поддержания службы, поддержки маркетинга и покрытия заработной платы.

**1.3.4 Облачная установка для майнеров в 1 клик от интернет сервиса Амазон**

Сеть Безоп позволит майнерам получать прибыль за счет работы в облаке, используя графический процессор Амазон (ГПА).

Майнер должен предоставить действующий ключ API Амазон и стандартный адрес Безоп с минимальным набором в 5000 денежных знаков системы Безоп.

Сложность конфигурации этого майнера останется скрытой, так как сеть будет полностью управлять через API.

- Сеть будет отвечать за создание новых экземпляров записи.

- Сеть прекратит выполнение малоактивных и не отвечающих экземпляров записи.

- Сеть может продолжать работу, даже когда устройства майнера отключены.

На приведенной ниже схеме показано, как работает Облачный Майнер. Он / она может подключить свой кошелек и ключ API интернет сервиса Амазон (ИСА). Кошельки, которые не могут сделать ставку на 5000 монет площадки Безоп, не будут получать выручку от работы.

|  |  |
| --- | --- |
| Miner | Майнер |
| Request | Запрос |
| Data Validation Failed | Не удалось выполнить проверку данных |
| Cloud Miner AppMiners Public Address Miners AWS API keyMaintain Minimum balance (5000 Bez) | Приложение для облачного майнераОбщедоступный адрес майнераКлюч API майнера от ИСА Обеспечение минимального баланса (5000 монет площадки Безоп)  |
| Condition No Yes  | Состояние Нет Да |
| Instance Manager  | Диспетчер экземпляров записи |
| Mine | Добыча (работы по майнингу) |
| Spawn Manager  | Диспетчер создания записи |
| Cleanup Manager  | Диспетчер удаления записи |

**2 Минимальный жизнеспособный продукт**

**2.1 Децентрализованное управление заказами**

**Исключительное положение «Безоп» завершилось. Сейчас его бета-минимальный жизнеспособный продукт (MVP) доступен для публичного использования.**

Первый в мире децентрализованным портал управления заказом (ДУЗ) будет связан с сетью. ДУЗ «Безоп» — это платформа полностью разработана для электронной коммерции, которую торговые компании могут поставить на свой веб-сервер и использовать для простой настройки магазина электронной торговли. Пользователи могут ввести запрос на получение ДУЗ «Безоп» от веб-сервиса github и начать продавать свои продукты и услуги и получать валюту Безоп онлайн за считанные минуты.

**2.2 Технологии, требования и возможности**

**Технологии**

ДУЗ «Безоп» построено с HTML5, React JS, Node Js, и MongoDb. Это все языки с открытым исходным кодом.

**Требования**

Для запуска ДУЗ «Безоп» требуется установка следующих средств поддержки:

- сервер LAMP / WAMP server

- программный софт Mean Stack

- платформа NodeJs

**Возможности**

ДУЗ «Безоп» предлагает ряд решений, предназначенных для удовлетворения потребностей клиентов, как описано ниже, с некоторыми реальными сценариями.

**(I) Создание магазина**

Клиент 1

Джейн является владельцем малого бизнеса, который продает спортивные наряды и комплекты с ценой в 10-150 долларов США. Она хочет построить свой собственный цифровой магазин, где она может легко совершать сделки со своими клиентами в Интернете, не разочаровываясь в необходимости оплачивать огромные сборы за пользование централизованным порталом для выполнения транзакций.

Решение «Безоп» для клиента 1

С ДУЗ «Безоп», Джейн может мгновенно запустить полностью децентрализованный портал электронной коммерции без необходимости доступа к «PrestaShop», «Shopify», «Amazon» или другим централизованным магазинам электронной торговли, которые взимают огромные транзакционные сборы и / или ежемесячные платежи.

Клиент 2

Джон является владельцем среднего бизнеса, который продает электронику с ценовым диапазоном в 99-1999 долларов США. Недавно он приобрел интернет-магазин, но стал часто ссориться со своими поставщиками услуг. Он ждет 21 день, чтобы получить средства, чтобы погасить свои счета, и предпочитает не ждать так долго, чтобы отправить деньги своим поставщикам.

Решение «Безоп» для клиента 2

С ДУЗ «Безоп» Джон не действует под влиянием какого-либо центрального органа и может обрабатывать свои транзакции, связав главный адрес «Безоп» и налоговый адрес «Безоп» в интернет-магазине ДУЗ «Безоп». Его средства будут автоматически отправлены сразу же после предоставления доказательств доставки, как правило, в течение нескольких минут.

**(II) Добавление продукта** - без ограничений по дизайну

Клиент 3

Джуд является владельцем большого супермаркета, где продает сотни предметов по цене от 99 долларов США до 1 999 долларов США. У него есть интернет-магазин, но он ограничен показом только 200 его продуктов за раз.

Решение «Безоп» для клиента 3

ДУЗ «Безоп» оптимизирована так, чтобы позволить столько продуктов, сколько пожелает Джуд, с оптимизацией под низкие объемы памяти и требованиями к хранению.

**(III) Классификация продуктов**

Клиент 4

Рэй является владельцем крупного бизнеса, который продает продукты по категориям. Ему нужно простое решение начать продажу в Интернете, и ему необходимо реализовать эту структуру, не затрагивая присущую ей сложность с разработкой дизайна или занятием программированием.

Решение «Безоп» для клиента 4

ДУЗ «Безоп» оптимизирован, чтобы позволить Рэю классифицировать и сегментировать свой магазин в нескольких отделах, доступ к которым его клиенты могут получить через автоматически созданное меню. С централизованной версией системы Рэй должен будет написать плагин управления контентом и другие коды и переконфигурировать различные базы данных, чтобы добиться такого же эффекта.

**(IV) Управление заказами**

ДУЗ «Безоп» обеспечивает идеальную систему управления заказами, которая отображает состояние статуса заказа и флаги, как описано ниже.

|  |  |
| --- | --- |
| Flags: - p proceed; -s success; -f failure; -c cancelled | Флажок состояния: - p proceed (продолжать); - s success (успех); - f failure (провал); - c cancelled (отмена); |
| Order Placement:Client A Finds Desired Product and clicks checkout | Размещение Заказа: Клиент A Находит желаемый продукт(ы) и нажимает проверить |
| Payment:Client A fills out there desired shipping information and scans the payment barcode | Оплата: Клиент A заполняет информацию желаемом месте доставки и сканирует штрих-код платежа |
| Order PendingClient A is Redirected to the Order Page Where they Have to wait for there order to get approved | Ожидаемый заказ: Клиент A перенаправляется на страницу заказа, где им нужно дождаться, когда будет утвержден заказ |
| Transaction Confirmed Order has received more than 2 successful confirmations | Подтверждена транзакция: У Клиента A заказ получил более 2 успешных подтверждений |
| Order Shipped:Client A’s Order order gets shipped by Seller, Seller can send shipment tracking information to order page | Заказ отправлен: Заказ Клиента A заказ отправляется продавцом, продавец может отправить информацию отслеживания отправки на страницу заказа |
|  |  |
| Transaction Rejected: Client A’s Order Order could not be confirmed on the network | Транзакция отклонена:Заказ Клиента A Заказ не может быть подтвержден в сети |
| Order cancelledOrder Status Changes  | Заказ отменен:Изменился статус заказа |

(s1-p): стадия 1 -продолжить. Это сообщение указывает на состояние первого этапа размещения заказа. На этом этапе покупатель готов предоставить свой адрес электронной почты и информацию по доставке для отправки.

(s2-p): стадия 2 -продолжить Это сообщение указывает на состояние второго этапа размещения заказа. На этом этапе покупатель успешно оплатил продукт / услугу и перенаправляется на страницу заказа, где он / она должен проверить информацию, чтобы его / ее заказы могли быть подтверждены в сети.

(s3-s): стадия 3 -успех

Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и первого успешного перевода. На этой странице, транзакция покупателя получила уже больше 2 успешных подтверждений.

(s3-f): стадия 4 -провал. Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и первого провального перехода. На этой стадии, заказ покупателя не получил успешного подтверждения и, в результате, оказался провален.

(s4-s): стадия 4 -успех. Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и второго успешного перевода. На этой стадии, заказ покупателя был отправлен продавцом.

(s4-c): стадия 4 -отменен. Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и первого провального перевода и отмены заказа. На этой стадии, транзакция была отменена потому, что случился провал с заказом покупателя. Покупателю будет предоставлены ссылка возвращающая его/ее обратно в его/ее корзине. Он/она может выбрать и снова сделать заказ.

Выполнение заказа

Это последняя стадия где можно достигнуть договоренностей между покупателем и продавцом, указывающая на то, что транзакция завершена.

**(V) Поддержка клиентов с помощью сообщений**

ДУЗ «Безоп» позволяет покупателям обмениваться сообщениями с продавцами после того как произойдет размещение заказа. Это позволяет объединять обе стороны.

**(VI) Получение доказательств налоговой цепи**

Новаторской особенностью Безоп является его способность собирать НДС и разбить средства на сегменты на два адреса - первичный (основной) адрес и вторичный (налоговый) адрес - когда оба адреса вовлечены. Доказательство налоговой цепи позволяет создать таблицу для всех действительных транзакций, при этом средства распределяются между основным адресом и налоговым адресом.

Запуск контракта (Trigger\_contract) (“PoTxM”,”PoTxV”) //Function returns Xm, Xv

XM; XV; I:INT=0; XM:ARRAY=[T1,T2,T3,..,TN] //holds transaction history XV:ARRAY=[T1,T2,T3,..,TN] //vat history

WHILE I<COUNT(XM){PRINT XM[I]}

WHILE I<COUNT(XV){PRINT XM[I]; PRINT <hr />}

**(VII) Интеграция кошелька Безоп**

ДУЗ Безоп позволит беспроблемной интеграции с нашими торговыми кошельками, легкими поступлениями и сверхбыстрой обработкой транзакций. С помощью блокчейна Эфириум (Ethereum Blockchain) Безоп очистит транзакции за один шаг за одну таксу, что приведет к принятию платежей в целом до 5 раз дешевле и быстрее для торговых компаний. Торговые компании смогут принимать платежи от кошельков на основе Эфириума.

**3 Элементы программы краудсейловых продаж токенов**

3.1 Элементы программы Токена

Краудсейл Безоп (\*досл. «народная продажа», crowd — толпа, sale — продажа, т.е. коллективное сотрудничество людей, которые объединяют свои ресурсы, как правило через интернет, чтобы приобрести цифровые токены) - и соответствующий процесс создания токенов будут выпущены компанией Bezop Blockchain Ltd (Безоп Блокчейн Лимитед), Общество с ограниченной ответственностью Соединенного Королевства (Великобритании и Северной Ирландии). События будут организованы по принципу смарт-контрактов, работающих на платформе Эфириум.

Участники, желающие поддержать развитие проекта «Безоп», могут поддержать проект, отправив Эфириум валюту (ETH) на адрес, обозначенный компанией Безоп. После того, как Безоп получит ETH («вклады»), участники будут немедленно вознаграждены Безоп токенами (BEZ) с курсом 1,929 BEZ за 1 ETH. Валюта BEZ будет отправлена на кошельки участников.

(изображение монеты Безоп смотреть по ссылке <http://joxi.ru/xAeMPWaSYO5wbA> )

Ключевые сведения о программе токенов:

● Приемлемой валютой при первичном предложении монет ППМ (от ICO - initial coin offering) является ETH (валюта платформы Эфириум).

● Создание (токенов) будет ограничено (Soft Cap \*«Мягкая крышка» - количество средств, которых будет достаточно для развития основных продуктов и сервисов стартапа) после получения взносов, эквивалентных 421 000 долл. США. Эта сумма может быть изменена до события создания токена.

● Период создания токена будет длиться шестнадцать (16) дней, если не будет достигнуто состояние «мягкая крышка» (Soft Cap).

● Если «мягкая крышка» (Soft Cap) будет достигнута до истечения 16-дневного периода, взносы будут принимаются в течение дополнительных 120 часов для размещения тех, кто желает принять участие, но пропустил короткий период создания валюты BEZ.

● Если Краудсейл (“Crowdsale”) кампания не достигает своей минимальной цели в размере 421 000 долларов США, все средства будут автоматически возвращены владельцам валюты BEZ через смарт-контракты Эфириум.

● У процесса создания токенов есть «жесткая крышка» (\*Hard Cap - максимальное количество средств, которые будут собраны) в 21 423 ETH. Достигнув этого предела, создание токена будет прекращено и дальнейшие взносы не будут приняты.

● Токены, которые не продадутся во время Краудсейла, будут автоматически уничтожены смарт контрактом.

● Из-за изменчивости цен значения валюты ETH не фиксированы и могут быть пересчитаны в любое время.

График РАСПРЕДЕЛЕНИЕ ТОКЕНОВ БЕЗОП

КОМАНДА БЕЗОП

Консультанты команды: 15%

Стратегический маркетинг: 5%

Бонусы от продажи токенов: 5%

Хранение: 15%

Доступно: 65%

График <http://joxi.ru/5mdqw6ZSvoKan2>

**3.1.1 Коэффициенты создания валюты Безоп BEZ**

● 1-й ценовой пакет до достижения «мягкой крышки»: 1 ETH = 1,929 BEZ

● 2-й ценовой пакет после достижения «мягкой крышки»: 1 ETH = 1,500 BEZ

Будет объявлен лимит взносов для каждой ценовой партии.

**3.1.2 Токены BEZ**

Токены Безоп станут знаками ценности, основанным на платформе Эфириум. Знак - это цифровой актив, имеющий ценность сам по себе на основе его базовых активов, свойств и / или связанными с ним правами.

Токены, основанные на платформах Эфириум, полагаются на хорошо развитую инфраструктуру Эфириум, пользующуюся несколькими преимуществами:

● Безопасность и предсказуемость (в отличие, например, от необходимости запуска независимой блокчейн-сети).

● Вовлечение надежных и обеспеченных клиентов (токены на основе платформы Эфириум могут управляться официальными клиентами Эфириум).

● Высокая ликвидность (взаимозаменяемы с другими токенами Эфириум или эфирами), проще внести в список на обменных биржах с уже существующей инфраструктурой. Наш токены на основе платформы Эфириум соответствуют стандарту ERC-20. Более подробная информация о стандарте ERC-20 представлена по ссылке [httpsHYPERLINK "https://github.com/ethereum/EIPs/issues/20"://HYPERLINK "https://github.com/ethereum/EIPs/issues/20"githubHYPERLINK "https://github.com/ethereum/EIPs/issues/20".HYPERLINK "https://github.com/ethereum/EIPs/issues/20"comHYPERLINK "https://github.com/ethereum/EIPs/issues/20"/HYPERLINK "https://github.com/ethereum/EIPs/issues/20"ethereumHYPERLINK "https://github.com/ethereum/EIPs/issues/20"/HYPERLINK "https://github.com/ethereum/EIPs/issues/20"EIPsHYPERLINK "https://github.com/ethereum/EIPs/issues/20"/HYPERLINK "https://github.com/ethereum/EIPs/issues/20"issuesHYPERLINK "https://github.com/ethereum/EIPs/issues/20"/20](https://github.com/ethereum/EIPs/issues/20) .

**3.1.3 Мотивационная программа**

Любой может участвовать в мотивационной программе Безоп, подписавшись на нее по ссылке

[httpsHYPERLINK "https://bitcointalk.org/index.php?topic=2635554"://HYPERLINK "https://bitcointalk.org/index.php?topic=2635554"bitcointalkHYPERLINK "https://bitcointalk.org/index.php?topic=2635554".HYPERLINK "https://bitcointalk.org/index.php?topic=2635554"orgHYPERLINK "https://bitcointalk.org/index.php?topic=2635554"/HYPERLINK "https://bitcointalk.org/index.php?topic=2635554"indexHYPERLINK "https://bitcointalk.org/index.php?topic=2635554".HYPERLINK "https://bitcointalk.org/index.php?topic=2635554"phpHYPERLINK "https://bitcointalk.org/index.php?topic=2635554"?HYPERLINK "https://bitcointalk.org/index.php?topic=2635554"topicHYPERLINK "https://bitcointalk.org/index.php?topic=2635554"=2635554](https://bitcointalk.org/index.php?topic=2635554)

**3.1.4 Бюджет**

Все собранные средства пойдут прямо в развитие и обслуживание площадки Безоп

График <http://joxi.ru/Q2KQOoMT91W8Pr>

Обратная покупка: 10%

Технология: 5%

компьютерный банк данных: 10%

Размещение рекламы: 10%

Стратегический маркетинг: 10%

Развитие: 55%

● 55% привлеченных средств пойдут непосредственно на развитие и расширение команды Безоп.

● 10% средств пойдут на правовую работу, чтобы гарантировать, что Безоп совместим со всеми нормативными стандартами во всех странах, где работает Безоп.

● 5% войдут в технологические усовершенствования, такие как обновление серверов и инфраструктуры, безопасность (покупка SSL-сертификатов высокой надежности) и т. д.

● 10% пойдет на маркетинг площадки Безоп для повышения осведомленности о платформе и привлекать больше пользователей.

● 10% будут вложены в рекламу наряду с обучением пользователей, которые хотят начать

зарабатывать деньги онлайн как торговые представители Безоп.

● 10% будет использоваться для обратной покупки токенов Безоп (см. программу выкупа Безоп). Ни одного токена Безоп не выдается никому из команды Безоп.

План развития проекта Безоп

|  |  |
| --- | --- |
| MPV PUBLIC RELEASE 1 Bezop’s minimal viable product will be released first week of december 12th December 2017 | Выпуск минимального жизнеспособного продукта для публичного доступа 1 Минимальный жизнеспособный продукт Безоп будет выпущенВ первую неделю декабря12 декабря 2017 года |
| 20th December, 2017 2.1 Token launch Bezop token sale is scheduled for 3rd week of December and tokens will be released once the ico ends 20th January, 2017 2.2 Listing on exchanges Bezop tokens will engage Exchanges and tokens Will be tradable by 20th January | 20 декабря 2017 года2,1Запуск токенаПродажа токенов Безопзапланирована на третью неделюдекабря и токеныбудет выпущены послеокончания ППМ (первичного предложения монет)20 января 2017 года2,2Внесение в списки на биржахТокены Безоп будут задействоватьКурс обмена и токеныДействительны в сделках к 20-муянваря |
| Standard Wallet Release 3 The release of a standard wallet is Scheduled 60 days After the token saleFeb-March, 2018 | выпуск стандартного кошелька3 Выпуск стандартного кошельказапланировано через 60 днейпосле продажи токеновФевраль-март 2018 года |
| 4 Decentralize Order Management Release Stable Release of Bezop DOM marketing begins July June-July, 2018 | 4 Выпуск система децентрализованного управления заказами выпуск стабильного маркетингового Безопначинается в июлеИюнь-июль 2018 года |
| Major5 Merchant Wallet Release Bezop Merchant Wallets and Other Smart Contracts are FinalisedThousands of Merchants can start selling with BezopAugust 2018 | Главное5 выпуск кошелька для торговлиЗакончена работа над торговыми кошельками Безоп и другими смарт контрактами Тысячи торговых компаний смогут начать продавать с площадкой БезопАвгуст 2018 года |
| 20196 Bezop Network Bezop splits to its own network Q1 | 20196 Сеть Безоп отделяется на собственную сеть Безоп Q1 |
| 7 Messier Upgrade (Security Upgrade)Mandatory Security Review And Upgrade is performedQ3  | 7 Обновление Мессир (обновление безопасности)Выполняется обязательная проверка безопасности и обновление выполняетсяQ3 |
| 8 Andromeda Upgrade (Network Upgrade)General Network Review And Upgrade is Performed Q4  | 8 Обновление Андромеды (обновление сети)Выполняется общая проверка сети и происходит обновление сети Q4 |

**5 Кто мы**

**5.1 Наша миссия**

Основная задача Безоп - обеспечить жизнеспособное и масштабируемое решение для электронной торговли, которое будет стимулировать предприятия и отдельных трейдеров к продаже товаров и услуг с использованием технологии блокчейн.

Безоп — это комплексное решение для успешного ведения бизнеса средствами электронной коммерции в сети для новичов и опытных пользователей. Любой может продавать свои продукты и услуги и получать зарплату в валюте Безоп без необходимости программирования.

«Безоп» реализует новое «Доказательство заказа», который снижает уровень мошенничества как для торговых компаний, так и для потребителей, используя элегантно разработанные контракты, основанные на блокчейне Эфириум и защищенные криптографически. Торговые компании могут взимать НДС и точно управлять заказами.

**Пять ключевых компонентов проекта «Безоп»**:

i. Портал ДУЗ

ii. сеть Безоп

iii. Система доказательства заказа

iv. Система доказательства доставки

V. Смарт контракты и обещания площадки Безоп

Безоп также произведет революцию в части использования кошелька, приватного ключа и шифрования транзакций с использованием запатентованного шифра Рэйнбоу (от англ. Досл. Rainbow «Радуга»).

**5.2 Команда Безоп**

**Дэрик Джонес (Deryck Jones)** – Главный Директор по Технологиям

Г-н Джонес имеет 20-летний опыт работы в списке Fortune 1000, возглавляющий оба направления как инжиниринговых, так и маркетинговых позиций при наблюдении за ИТ-операциями. Он был вице-президентом по исследованиям и разработкам программного обеспечения в подразделении Массачусетского технологического института стоимостью 3,1 млрд. долл. США и

отделение производственного бизнеса в системный бизнес стоимостью 270 миллионов долларов. Он также запустил сервисы Data-Force, партнера по развитию и продажам Salesforce, который предоставлял услуги Sony, Canon, RFS и т. д., путем разработки корпоративных программных приложений и выполнения корпоративной системной интеграция с SAP, Oracle и Microsoft SQL Server.

**Саймон Дисней (Simon Disney)** – Главный Директор по Маркетингу

Саймон Дисней является одним из самых влиятельных маркетологов в Интернете и хозяином популярного «Маркетингового саммита». Он сильный инвестор, ему нравится криптовалюта, он контролирует 1,7 миллиона активов и список рассылки лояльных клиентов. Саймон успешно продал более 60 наименований программного обеспечения онлайн и пассивно создавал миллионы в год для поставщиков. У Саймона также есть огромное количество тысяч ведущих маркетологов, которые активно продвигают «Безоп».

**Кевин Бирн (Kevin Byrne)** - эксперт по электронной коммерции, по связям с общественностью и рекламе

Кевин имеет степень магистра в области электронной коммерции и степень отличия в бизнесе и маркетинге. Он является экспертом в рекламе на Facebook и обошел несколько платформ, таких как Shopify. Кевин может произвести тысячи продаж для нового магазина в течение нескольких недель и готов передать свои обширные знания, опыт и страсть к электронной коммерции новым торговым компаниям.

**Камелиус «Звезда» Уба (Camelius “Blaze” Ubah)** – Ведущий инженер

Камелиус не только аппаратный разработчик, но также филантроп и любит многое отдавать обществу. Он имеет степень бакалавра в области компьютерных наук и системного проектирования и участвует в нескольких революционных проектах в программном пространстве, таких как Флекси (Flexy), Проект AI встроен в Гугл ЭмэЛ (google ML). Работа с сильной командой смарт контрактов и разработчиками блокчейн, Камелиус также ведет разработку технологии шифрования Реинбоу (Rainbow), один из самых сильных методов шифрования кошельков, известных на сегодняшний день.

**6. Ресурсы**

**6.1 Правовые аспекты**

Денежная валюта Безоп не имеет юридической квалификации безопасности, поскольку она не дает никаких прав на дивиденды или проценты. Продажа токенов Безоп является окончательной и не подлежит возврату. Денежная валюта Безоп не являются акциями и не дают никаких прав на участие в общих встречах руководства Безоп Блокчейн Лимитед. Денежная валюта Безоп не может иметь производительность или конкретное ценности вне Безоп платформы. Таким образом, токены Безоп не должны использоваться или приобретаться для спекулятивных или инвестиционных целей. Покупатель токенов Безоп осознает, что национальные законы о ценных бумагах, которые гарантируют, что инвесторы продают инвестиции, которые включают все необходимые раскрытия информации и подлежат нормативному контролю для защиты инвесторов, неприменимы. Любой, кто покупает токены Безоп, прямо признает и представляет, что он / она внимательно рассмотрели этот экспертный документ и полностью понимают риски, издержки и выгоды, связанные с покупкой Безоп.

**6.1.1 Требуемые знания**

Покупатель токенов Безоп берет на себя обязательства, что он / она понимает и имеет значительный опыт в приобретении криптовалют, системе блокчейн и сервисов и что он / она полностью понимает риски, связанные с краудсейлом, а также с механизмами, связанными с использованием криптовалюты (включая хранение). Безоп не должен нести ответственность за любую потерю токенов Безоп или ситуаций, из-за которых невозможно получить доступ к Безоп, которые могут быть результатом любых действий или бездействия пользователя, или любого лица взявшего на себя обязательство по приобретению токенов Безоп, а также в случае хакерских атак.

**6.1.2 Риски**

Приобретение токенов Безоп и их хранение связано с различными рисками, в частности Безоп Блокчейн Лимитед возможно не может запустить свои операции и развить сеть блокчейн и предоставить обещанные услуги. Поэтому до приобретения токенов Безоп, любой пользователь обязан тщательно рассматривать риски, затраты и преимущества приобретения токенов Безоп методом краудсейла; и, при необходимости, получить любой независимый совет в этом деле. Любое заинтересованное лицо, которое не в состоянии принять или понять риски, связанные с деятельностью (включая риски, связанные с неразвитием платформы Безоп) или любых других рисков, указанных в Условиях и положениях краудсейла не должен приобретать токены Безоп.

**6.1.3 Важное предупреждение**

Этот технический документ не должен и не может рассматриваться в качестве приглашения для инвестиций. Он ни каким-либо образом не является, не должен рассматриваться как предложение ценных бумаг в какой- либо юрисдикции. В этом техническом документе не содержит или не включает в себя никакую информацию или указания, которые могли бы рассматриваться в качестве рекомендации или которые могли бы использоваться в качестве основы для любого инвестиционного решения. Токены Безоп - это только токены утилиты, которые могут использоваться только на платформе Безоп и не предназначены для использования в качестве инвестиций.

Предложение покупки токенов Безоп в рамках торговой платформы сделано для того, чтобы позволить платформе Безоп функционировать, а не для спекулятивных целей. Предложение токенов Безоп на торговой платформе не изменяет юридическую квалификацию токенов, которые остаются простым средством для использования платформы Безоп и не являются обеспечением защиты.

Безоп Блокчейн Лимитед не может рассматриваться в качестве консультанта по любым юридическим, налоговым или финансовым вопросам. Любая информация, содержащаяся в техническом документе, предоставляется только в общих информационных целях, и Безоп Блокчейн Лимитед не дает никаких гарантий относительно точности и полноты этой информации.

Безоп Блокчейн Лимитед не является финансовым посредником в соответствии с британским законодательством и не нуждается в получении разрешения на противодействия отмыванию денег. Приобретение токенов Безоп не дает никаких прав или влияния на организацию и / или управление Безоп Блокчейн Лимитед покупателям токенов.

Регулирующие органы тщательно изучают предприятия и операции, связанные с криптовалютами по всему миру. В этом отношении меры регулирования, расследования или регламентационные действия могут повлиять на бизнес Безоп Блокчейн Лимитед и даже ограничить или предотвратить его развитие в будущем. Любое лицо, которое приобретает токены Безоп, обязано должно знать о бизнес-модели Безоп Блокчейн Лимитед. Технический документ или Положения и условия могут меняться или нуждаться в изменении из-за новых нормативных требований и / или норм соответствия, вытекающих из применимых законов в любых сферах его применения. В этом случае покупатели и любой, кто обязуется приобретать токены Безоп, признают и понимают, что ни Безоп Блокчейн Лимитед, ни какие-либо из ее аффилированных лиц не несут ответственности за любые прямые или косвенные убытки, или причиненный ущерб, вызванные такими изменениями.

Безоп Блокчейн Лимитед сделает все возможное, чтобы начать свою деятельность и разработать платформу Безоп. Любой, кто возьмется за приобретение токенов Безоп, признает и понимает, что Безоп Блокчейн Лимитед не дает никаких гарантий, что им это удастся. Они признают и понимают, что Безоп Блокчейн Лимитед (включая учреждения и сотрудников) не берет на себя никаких обязательств или ответственности за любые потери или ущерб, которые могут возникнуть в связи с неспособностью использовать токены Безоп, за исключением случаев умышленных неправомерных действий или грубой халатности.

**6.1.4 Представительство и гарантии**

Участвуя в Краудсейле, покупатель соглашается с вышеуказанным и, в частности, они представляют и гарантируют, что они:

● внимательно ознакомьтесь с положениями и условиями, прилагаемыми к «Техническому документу», согласились с полным содержанием и приняли обязательство быть юридически обязанными им следовать;

● уполномочены и имеют полное право на приобретение токенов Безоп в соответствии с законами, которые применяются в сфере их компетенции по месту жительства;

● не являются гражданами США или резидентами этой страны;

● жить в сфере компетенции, которая позволяет Безоп Блокчейн Лимитед продавать токены Безоп посредством крайдсейла, не требуя каких-либо локальных полномочий;

● знакомы со всеми соответствующими правилами в конкретной сфере компетенции, в которой они основаны, и что покупка криптографических токенов в этой сфере компетенции не запрещена, не ограничена или не подлежит дополнительным условиям любого рода;

● не использовать краудсейл для любой незаконной деятельности, включая, помимо прочего, отмывание денег и финансирование терроризма;

● имеют достаточные знания о характере криптографических токенов и обладают значительным опытом с ними и функциональным пониманием использования и сложностей в работе с криптографическими токенами и валютами и системами, и службами на основе блокчейна;

● купить токены Безоп, потому что они хотят иметь доступ к платформе Безоп;

● не покупают токены Безоп для целей спекулятивных инвестиций или использования.

**6.2 Важные даты**

Актуальные вопросы и ответы

 Дерик: будет указано дополнительно

 Саймон: не предусмотренный графиком

 Кевин: будет указано дополнительно

**Дата предварительных продаж**

 Начало предварительных продаж: будет указано дополнительно

 Ссылка предварительных продаж: будет указано дополнительно

 Объёмы предварительных продаж: будет указано дополнительно

**Дата массовых продаж**

 Начало краудсейловых продаж: будет указано дополнительно

 Ссылка на покупку: будет указано дополнительно

Завершение для «ранних пташек»: 12 вечера по североамериканскому восточному времени (полночь)

 **6.3 Проверки**

 Содержание этого документа подлежит будущим изменениям (послед. изменения: 01/01/2018, в 4:21 утра по североамериканскому восточному времени

● Добавлено (пункт 6.1.2 Риски) на PG. 19 на дату 11/10/2017, 4:21 в 4:21 утра по североамериканскому восточному времени

● Добавлена неустойчивость валюты Эфириум ETH – стр 15 25/12/2017

● установление размера «мягкой крышки» в долл США USD - p15 25/12/2017

● Завершенные косметические изменения всех страниц 2/1/2018

**6.4 Справочные материалы**

[1] Бернардмун, 2016. <https://www.slideshare.net/bernardmoon/fintech-industry-report-2016>

[2] Статистика, 2008. <https://www.statista.com/statistics/249863/us-mobile-retail-commerce-sales-as-percentage-of-ecommerce-sales/>

[3] Википедия, Доказательство доставки, Январь 2012. wikipedia.org

[4] Виталик Бутерин, Эфириум, Апрель 2014. <https://ethereum.org/>

[5] Сатоши Накамото, Биткоин: Децентрализованная электронная денежная система от пользователя к пользователю, 2008. [https://bicoin.org](https://bicoin.org/)

[6] Википедия, Доказательства корректности, Январь 2014. wikipedia.org

[7] Гугл, Доля мобильных платежей в электронной торговле, 2017.

<https://www.google.lt/#q=mobile+payment+share+of+ecommerce&start=10>

содержания документа может быть изменено (последние изменения: 2/1/2017)

Сеть Безоп

(Техническая документация Безоп)

Ссылки:

<https://bezop.io/app/mvp>

<https://github.com/bezopteam>

Безоп: Децентрализованная сеть электронной торговли с проверенным подтверждением доставки.

Технический анализ по 5 ключевым компонентам безопасной децентрализованной сети электронной торговли.

Безоп блокчейн лимитед

Проект с открытым исходным кодом, [httpsHYPERLINK "https://opensource.org/licenses/MIT"://HYPERLINK "https://opensource.org/licenses/MIT"opensourceHYPERLINK "https://opensource.org/licenses/MIT".HYPERLINK "https://opensource.org/licenses/MIT"orgHYPERLINK "https://opensource.org/licenses/MIT"/HYPERLINK "https://opensource.org/licenses/MIT"licensesHYPERLINK "https://opensource.org/licenses/MIT"/HYPERLINK "https://opensource.org/licenses/MIT"MIT](https://opensource.org/licenses/MIT)

26 сентября 2017

РЕЗЮМЕ

Всемирная паутина переживает изменения, не функциональные; дизайна и структуры. Неизбеж-ный конец централизованных частных услуг будет эффективно заменен децентрализованными и демократизированными вариантами; устранение ненадежного и основанного на доверии к чело-веку с неизменным и математическим доверием, поддающимся проверке путем вычислений; постоянный пересмотр адреса местоположения с жизнеспособными по содержанию адресами; неэффективные и негибкие примитивные (централизованные) услуги станут пользоваться мень-шим спросом, поскольку алгоритмические технологии продолжат процветать. Биткойн, Эфириум и другие сети блокчейна доказали полезность децентрализованных регистров транзакций. Эти публичные регистры обрабатываются сложными приложениями смарт контрактов и транслируют крипто-активы стоимостью в десятки миллиардов долларов. Эти системы являются первыми экземплярами открытых сервисов публичного доступа, в которых участники образуют децентра-лизованную сеть, предоставляющую полезные услуги для кредитования, без централизованного управления или доверенных лиц.

Децентрализованные приложения вынуждены быстро принимать вызов «законности цели», аргу-ментируя опасностью мошенничества и отмывания денег, иначе появятся строгие правила, если появится предположение, что сделка может оказаться «помощью или подстрекательством к нару-шению законов страны». В настоящий момент технология блокчейн может широко восприни-маются как легкий инструмент для уклонения от уплаты налогов, поскольку транзакции происхо-дят тайно и криптографически, что является основной и фундаментальной особенностью. Нет простого способа для бизнеса адаптировать блокчейн и доказать, что они не облагаются налогом; следовательно, не идеально подходит для некоторых бизнесов. Несмотря на то, что существует еще множество критических вопросов, таких как масштабирование, безопасность и стабильность, вышеупомянутые пункты представляют собой прямую угрозу выживанию блокчейна.

Безоп - это децентрализованная система управления и обработки заказов средствами электрон-ной коммерции, основанная на смарт контрактах, автономная служба защиты продавцов-поку-пателей и простая система сбора данных о налогах, построенная на децентрализованной сети блокчейн. Безоп стремится предоставить открытое и полное решение с открытым кодом для успешного ведения бизнеса средствами электронной коммерции в сети Интернет. Торговые компании могут участвовать, продавая продукты и услуги в своих собственных магазинах электронной торговли (Безоп ДУЗ) и передавая заказы в сеть. Торговая площадка Безоп работает на блокчейне с токенами протокола erc-20 (также называемым «Безоп»), который майнеры зарабатывают на блокчейне Эфириум с помощью доказательства работы. Клиенты тратят Безоп на покупку товаров и услуг на Безоп ДУЗ и других интегрированных сайтах, предлагающих услуги и принимающих оплату в валюте Безоп. И наоборот, можно заработать валюту Безоп, продавая товары и услуги и или просто получая Безоп через кошелек в качестве перевода на кошелек. В будущем появится сеть Безоп, где майнеры будут конкурировать чтобы создать блоки со значительными наградами; однако мощность добычи Безоп будет пропорциональна активным заказам в сети. Следовательно, полезность добычи Безоп не ограничивается поддержанием консенсуса в блокчейне. Это создает мощный стимул для майнеров выполнять как можно больше заказов. Протокол сплетает эти накопленные ресурсы в сеть целенаправленного самовосстанов-ления, на которую может положиться любой человек в мире. Сеть обеспечивает надежность, применяя очень мощные методы защиты покупателей посредством смарт контрактов. Протокол портала управления заказами обеспечивает адекватную безопасность, поскольку заказы шиф-руются на стороне клиента, в то время как у майнеров нет доступа к ключам дешифрования. Безоп работает как стимулирующий слой поверх блокчейна, который вычисляет доказательство заказа для любой транзакции. Это особенно полезно для децентрализации платежей, создания и работы распределенных порталов электронной торговли и реализации смарт контрактов.

**Этот документ:**

**(a) Представляет сеть Безоп, дает обзор протокола и подробно рассматривает несколько компонентов**

**(b) Децентрализованное управление заказами и его свойства**

**(c) Реализация на сетях Эфириум и токенов Erc-20**

**(d) Внедряет «доказательство заказа», которое позволяет доказать транзакцию с богатыми деталями покупки, а также поддающимся проверке доказательством доставки (что является достаточным доказательством), поставляемый продукт / услуга, сбор налогов и подтверждение правильности для цепочки транзакций**

**(e) Обсуждает варианты использования, подключения к другим системам и способы использования протокола. Безоп – это работа в процессе.**

**Активные исследования ведутся, и новые версии этой статьи будут по ссылке** [**httpsHYPERLINK "https://bezop.io/changes/changelog.pdf"://HYPERLINK "https://bezop.io/changes/changelog.pdf"bezopHYPERLINK "https://bezop.io/changes/changelog.pdf".HYPERLINK "https://bezop.io/changes/changelog.pdf"ioHYPERLINK "https://bezop.io/changes/changelog.pdf"/HYPERLINK "https://bezop.io/changes/changelog.pdf"changesHYPERLINK "https://bezop.io/changes/changelog.pdf"/HYPERLINK "https://bezop.io/changes/changelog.pdf"changelogHYPERLINK "https://bezop.io/changes/changelog.pdf".HYPERLINK "https://bezop.io/changes/changelog.pdf"pdf**](https://bezop.io/changes/changelog.pdf) **Для комментариев и предложений, пишите на электронную почту research@Bezop.io.**

**Содержание**

**1 Введение 3**

1.1 Элементарные компоненты 4

1.2 Сеть Эфириум, Токены ERC20 5

1.3 Обзор протокола 6

1.4 Организация документа 6

**2 Определение децентрализованного управления заказами 7**

2.1 Определение 7

2.2 Технологии и требования 7

2.3 Свойства 7

**2 Доказательство заказа 10**

2.1 Введение, мотивация, консенсус 10

2.2 Атаки 10

2.4 Доказательство выполнения работы, в защиту вычислительной системы от злоупотребления услугами, майнинг 12

2.3 Доказательство транзакции и доставки 14

2.4 Доказательство налога 16

**3 Смарт контракты 17**

3.1 Контракты в Безоп 17

**4 Будущая работа 23**

4.1 Продолжающаяся работа 24

4.2 Открытые вопросы 24

4.4 Рекомендации 25

**1. Введение**

Безоп - это токен протокола, чей блокчейн работает на доказательстве работы, где блоки создаются майнерами, которые подтверждают заказы (транзакции). Доказательством работы является часть данных, которая является трудной к созданию (дорогостоящей, отнимающей много времени), но легко проверяемой для других и которая удовлетворяет определенным требованиям. Создание доказательства работы может быть случайным процессом с малой вероятностью, так что в среднем потребуется много проб и ошибок, прежде чем будет создано действительное доказательство работы. Безоп использует систему доказательств работоспособности Хешкеш (Hashcash).

Одним из применений этой идеи является использование Хешкеш в качестве метода предотвращения спама электронной почты, требующего подтверждения работы по содержимому электронной почты (включая «Адрес») по каждому электронному письму. Легитимные электронные письма смогут выполнять работу по созданию доказательств легко (не требуется много работы для одного электронного письма), но массовые спам-почтовые клиенты будут испытывать трудности с получением необходимых доказательств (что потребует огромных вычислительных ресурсов).

Доказательства работы Хешкеш используются в Безоп для создания блоков. Для того, чтобы блок принимался участниками сети, майнеры должны заполнить доказательство работы, которое охватывает все данные в блоке. Трудность этой работы настраивается таким образом, чтобы ограничить скорость, с которой новые блоки могут быть созданы сетью по одному каждые 10 минут. Из-за очень низкой вероятности успешной генерации это делает непредсказуемым тот факт, какой рабочий компьютер в сети сможет генерировать следующий блок.

Для того, чтобы блок был действительным, он должен хешировать до значения, меньшего, чем текущая цель; это означает, что каждый блок указывает, что была выполнена работа по его созданию. Каждый блок содержит хэш предыдущего блока, поэтому каждый блок имеет цепочку блоков, которые вместе составляют большой объем работы. Изменение блока (которое может быть выполнено только путем создания нового блока, содержащего тот же предшествующий элемент) требует восстановления всех последующих элементов и проведения повторной работы, которую они содержат. Это защищает блокчейн от несанкционированного доступа.

Наиболее широко используемая схема доказательства работы основана на SHA-256 и была представлена в составе Биткоин. Некоторые другие алгоритмы хэширования, которые используются для проверки работоспособности, включают Scrypt, Blake-256, CryptoNight, HEFTY1, Quark, SHA-3, scrypt-jane, scrypt-n и их комбинации.

Существует два класса протоколов проверки работы.

● **Протоколы ответа на вызовы** предполагают прямую интерактивную связь между запрашивающим (клиентом) и провайдером (сервером). Провайдер делает выбор, скажем, элемент в наборе с свойством, а запрашивающий находит соответствующий ответ в наборе, который отправляется обратно и проверяется провайдером. Поскольку вызов выбирается на месте провайдером, его трудность может быть адаптирована к его текущей нагрузке. Работа на стороне запрашивающего может быть ограничена, если протокол запроса-ответа имеет известное решение (выбранное провайдером) или, как известно, существует в ограниченном пространстве поиска.

|  |  |
| --- | --- |
| 1 request service  | Запрос услуги |
| 2 choose  | Выбор  |
| 3 challenge  | затруднение |
| 4 solve  | решение |
| 5 response  | Ответная реакция  |
| 6 verify | Подтверждение  |
| 7 grant service  | Оказание услуги |
| Client Server  | Клиент Сервер |

<http://joxi.ru/Y2L5noGfnlznDA>

● **Протоколы проверки решений** не предполагают такую ссылку: в результате проблема должна быть установлена самостоятельно, прежде чем решение поищет клиент, и провайдер должен проверить как выбор проблемы, так и найденное решение. Большинство таких схем - неограниченные вероятностные повторяющиеся процедуры, такие как Хешкаш.

<http://joxi.ru/p27Pzydc0XkooA>

|  |  |
| --- | --- |
| 1 Compute  | Произвести расчет |
| 2 solve  | решение |
| 3 send  | отправка |
| 4 verify | подтверждение |
| Sender Receiver  | Отправитель Получатель |

Протоколы известных решений имеют тенденцию иметь несколько более низких величин отклонения, чем неограниченные вероятностные протоколы, поскольку величина отклонения прямоугольного распределения ниже, чем величину отклонения распределения Пуассона (с тем же средним значением). Общий метод сокращения величин отклонения и заключается в использовании нескольких независимых подзадач, так как среднее значение для нескольких выборок будет иметь более низкую величину отклонения.

**1.1 Элементарные компоненты**

Протокол Безоп основывается на четырех новых компонентах.

**i. Децентрализованное управление заказами (ДУЗ): портал управления заказами с открытым исходным кодом**

**ii. сеть Безоп:** Смарт контракт дружественная сеть блокчейн

**iii. Доказательство заказа:** Краткий обзор различных доказательств,

Мы подробно представляем эти инновационные доказательства заказа (раздел 3).

**a. Доказательство налога:** - НДС транзакция хранит данные

(i) указывая на основную транзакцию.

- x должен быть вычислен для правильности, взяв хэш из γ.Φ

Налоговые данные : { α|obj : val , γ|str: val, δ|float : val, ε:bool:val, x|str:val}

α - данные, γ – временная отметка ,γ₁ - временная метка родительской транзакции

 δ - Объем, δ₁ - объем материнской сделки

ε – направляющийся в (входящий: 1, исходящий: 0)

Φ – val (γ₁.δ₁)

i – проверка первоначальной транзакции

x - байт правильности [**хеш** (γ.Φ) ]

**b. Доказательством транзакции:** служит квитанция и показывает всю информацию о приобретенном продукте или услуге.

Данные транзакции: { α|obj : val , β|str : val, γ₁|str: val, δ₁|float : val, ε:bool:val, tid|str : val }

α - данные (смотри страницу XX)

β – адрес отправителя, γ₁ - временная отметка, δ₁ - объем (количество)

ε - направляющийся в (входящий: 1, исходящий: 0), проверка – номер транзакции

**iv) Доказательство доставки:** Доказательства того, что товар или услуга доставлены.

**v) Безоп смарт контракты и обещания:** Смарт контракты позволят полностью обеспечить безопасные и надежные решения электронной коммерции для безупречной работы вместе над доказательством протокола заказа, а защита покупателя обеспечивается через блокчейн.

**Прочее:**

i **Правильность: правильность** алгоритма утверждается, когда говорят, что алгоритм является правильным в отношении спецификации. Функциональная правильность относится к поведению ввода-вывода алгоритма (т. Е. Для каждого входа он производит ожидаемый выход).

Различают **полную корректность**, которая дополнительно требует завершения алгоритма и **частичную корректность**, которая просто требует, чтобы, если ответ возвратится, то он будет правильным. Поскольку общее решение проблемы остановки отсутствует, общее утверждение о корректности может быть гораздо глубже. Доказательство о прекращении — это тип математического доказательства, играющего важную роль в формальной подтверждении, поскольку полная правильность алгоритма зависит от прекращения.

Например, последовательно просматривая целые числа 1, 2, 3, ..., можно увидеть, сможем ли мы найти пример некоторым явлениям - скажем, дополнительное совершенное число - довольно легко написать частично правильную программу (используя длинное деление на два, чтобы проверить n как идеальное или нет). Но сказать, что эта программа абсолютно правильна, - это утверждать, что в настоящий момент не все известно в теории чисел.

**Доказательство выполнения работы:**

Безоп будет базироваться на той же системе доказательства работы, что и Эфириум, которая будет обновлена до полного «доказательства заказа», когда майнерам не нужно тратить время вычисления на майнинг блоков, а вместо этого подтверждать заказы в сети.

**1.2 Сеть Эфириум, токены ERC20:**

Эфириум - это децентрализованная платформа, которая управляет площадкой Безоп, используя силу смарт контрактов, обеспечиваемых сетью продаж товаров и услуг Эфириум, общие транзакции происходят без какой-либо угрозы простоя, цензуры, мошенничества или вмешательства третьих сторон.

Безоп работает на специально построенном блокчейне (Эфириум), которая является чрезвычайно мощной, прозрачной и глобальной инфраструктурой, которая может перемещать стоимость и представлять права на собственность. Это позволит нам создавать площадки Безоп, хранить реестры транзакций, поставки, статус заказов, налоги, а также перемещать средства в соответствии с инструкциями, данными в прошлом (например, волей или фьючерсным контрактом) и многими другими вещами, которые не были изобретены, все операции без риска услуг посредников или контрагентов.

**1.3 Обзор протокола:**

• Протокол Безоп — это децентрализованная сеть электронной торговли, построенная на блокчейне и с собственным токеном. Клиенты тратят токены в обмен на товары, услуги, запуск контрактов и получение налоговых доказательств.

• Майнеры зарабатывают путем подтверждения заказов (сделок) и разрешения споров.

• Безоп ДУЗ обрабатывает заказы на интерфейсе. Владельцы магазина устанавливают цену за свой продукт / услугу и ставку НДС и добавляют их на свою собственную платформу Безоп, клиенты отправляют токены, которые служат кредитом для товаров и услуг.

• Рынки управляются сетью Безоп, которая использует доказательство работы и доказательство заказа, чтобы гарантировать, что майнеры правильно выполнили работу для подтверждения заказа.

• Наконец, майнеры могут участвовать в создании новых блоков для базового блокчейна. Влияние майнера на следующий блок пропорционально количеству активных заказов в сети.

**Обзор протокола**

[**http://joxi.ru/Q2KQOoMT91Q4Br**](http://joxi.ru/Q2KQOoMT91Q4Br)

|  |  |
| --- | --- |
| Client | клиент |
| Bezop DOM or Integration | ДУЗ Безоп или Интеграция  |
| Order Placement Smart Contract  | Размещение заказа смарт контракт |
| Mine | Процесс майнинга |
| Store Promises  | Обещания магазина |
| Cold Storage  | "замораживание" |
| Proof of Delivery Reject Accept | Подтверждение доставки отказ прием |
| Agreement Txn complete  | Договор завершен |
| Credit Merchant | Кредит торговой компании |
| Close Promises  | Закрытие обещаний |
| Claim denied txn complete | Требование отклонено завершен |
| Dispute on Network | Рассмотрение споров в сети |
| Cancellation | Отмена |
| Close Promises  | Закрытие обещаний |

**1.3 Организация документа**

Остальная часть этой статьи организована следующим образом. Мы представляем наше определение и требования к ДУЗ в **разделе 2.**

В **разделе 3** мы мотивируем, определяем и представляем наше доказательство заказа (Доказательство транзакции и доказательство налога), используемое в пределах Безоп

В **Разделе 4** мы приводим краткое описание смарт контрактов Безоп.

В заключение мы обсудим будущую работу в **разделе 5**.

**2.1 Определение системы децентрализованного управления заказами**

Децентрализованное управление заказами (ДУЗ) полностью разработанная электронная платформа, которую заинтересованный пользователь может скачать, установить, и управлять ею без централизованного управления или внешнего контроля. Пользователи могут ввести запрос на получение ДУЗ «Безоп» от веб-сервиса github на адрес их самоуправляемого сервера. Они могут начать продавать свои продукты и услуги и получать валюту Безоп онлайн за считанные минуты.

**2.2 Технологии**

Платформа Безоп ДУЗ построена с использованием HTML5, ReactJS, NodeJs, MongoDB

Эти языки программирования с открытым кодом доступа.

**2.2 Требования**

Запуск ДУЗ Безоп DOM требует установки следующих компонентов

- Linux

- Nginx

- NodeJs

- Npm (Node Package Manager)

- MongoDB

**2.3 Особенности (Described by Real-Life Case Analysis)**

**(i) Создание магазина:**

 **Анализ проблемы A - Клиент 0:**

Джейн является владельцем малого бизнеса, который продает спортивные наряды и комплекты с ценой в 10-150 долларов США. Она хочет построить свой собственный цифровой магазин, где она может легко совершать сделки со своими клиентами в Интернете, не разочаровываясь в необходимости оплачивать огромные сборы за пользование централизованным порталом для выполнения транзакций.

**Решение «Безоп» A:** С ДУЗ «Безоп», Джейн может мгновенно запустить полностью децентрализованный портал электронной коммерции без необходимости доступа к «PrestaShop», «Shopify», «Amazon» или другим централизованным магазинам электронной торговли, которые взимают огромные транзакционные сборы и / или ежемесячные платежи.

**Анализ проблемы B - Клиент 1:** Джон является владельцем среднего бизнеса, который продает электронику с ценовым диапазоном в 99-1999 долларов США. Недавно он приобрел интернет-магазин, но стал часто ссориться со своими поставщиками услуг. Он ждет 21 день, чтобы получить средства, чтобы погасить свои счета, и предпочитает не ждать так долго, чтобы отправить деньги своим поставщикам.

**Решение «Безоп»** **B:** С ДУЗ «Безоп» Джон не действует под влиянием какого-либо центрального органа и может обрабатывать свои транзакции, связав главный адрес «Безоп» и налоговый адрес «Безоп» в интернет-магазине ДУЗ «Безоп». Его средства будут автоматически отправлены сразу же после предоставления доказательств доставки, как правило, в течение нескольких дней.

**Добавление продукта (без ограничений по дизайну)**

**Анализ проблемы A - Клиент 2:** Джуд является владельцем большого супермаркета, где продает сотни предметов по цене от 99 долларов США до 1 999 долларов США. У него есть интернет-магазин, но он ограничен показом только 200 его продуктов за раз.

**Решение «Безоп»** **A:** ДУЗ «Безоп» оптимизирована так, чтобы позволить столько продуктов, сколько пожелает Джуд, с оптимизацией под низкие объемы памяти и требованиями к хранению.

**(ii) Классификация продуктов**

**Анализ проблемы A - Клиент 3:** Рэй является владельцем крупного бизнеса, который продает продукты по категориям. Ему нужно простое решениеначать продажу в Интернете, и ему необходимо реализовать эту структуру, не затрагивая присущую ей сложность с разработкой дизайна или занятием программированием.

**Решение «Безоп»** A: ДУЗ «Безоп» оптимизирован, чтобы позволить Рэю классифицировать и сегментировать свой магазин в нескольких отделах, доступ к которым его клиенты могут получить через автоматически созданное меню. С централизованной версией системы Рэй должен будет написать плагин управления контентом и другие коды и переконфигурировать различные базы данных, чтобы добиться такого же эффекта.

**(iii)** Управление заказами

Портал децентрализованного управления заказами Безоп (ДУЗ) предлагает идеальную систему управления заказами с кодами статусов указывающими на текущее состояние заказа и флаги обозначающие изменение состояния.

Смотри Рис 2 (Рисунок показывающий статус заказа)

<http://joxi.ru/Dr8Mb7LSk09Mlm>

**(s1-p): стадия 1 -продолжить**

Это сообщение указывает на состояние первого этапа размещения заказа. На этом этапе покупатель готов предоставить свой адрес электронной почты и информацию по доставке для отправки продукта. Таким же образом осуществляется выход

**(s2-p): стадия 2 -продолжить**

Это сообщение указывает на состояние второго этапа размещения заказа. На этом этапе покупатель успешно оплатил продукт / услугу и перенаправляется на страницу заказа, где он / она должен проверить информацию, чтобы его / ее заказы могли быть подтверждены в сети.

**(s3-s): стадия 3 -успех**

Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и первого успешного перевода. На этой странице, транзакция покупателя получила уже больше 2 успешных подтверждений.

**(s3-f): стадия 4 -провал.** Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и первого провального перехода. На этой стадии, заказ покупателя не получил успешного подтверждения и, в результате, оказался провален.

**(s4-s): стадия 4 -успех.** Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и второго успешного перевода. На этой стадии, заказ покупателя был отправлен продавцом.

**(s4-c): стадия 4 -отменен.** Это сообщение указывает на состояние второго этапа обработки заказа от размещения заказа и первого провального перевода и отмены заказа. На этой стадии, транзакция была отменена потому, что случился провал с заказом покупателя. Покупателю будет предоставлены ссылка возвращающая его/ее обратно в его/ее корзине. Он/она может выбрать и снова сделать заказ.

**Выполнение заказа**

Это последний этап и является положительным соглашением между покупателем и продавцом, что сделка завершена.

**(iv) Support Messages**

ДУЗ Безоп позволит клиентам обмениваться сообщениями с продавцом после их размещения,

Это позволит обеим сторонам оставаться на связи.

**(v) Генерация доказательств налоговой цепочки**

Особенностью Pioneer среди прочих является способность взимать НДС с Безоп и распределять фонды на два адреса; вторичный адрес (Налоговый адрес) и первичный (Основной адрес) - оба адреса смешаны. Доказательство налоговой цепочки позволяет создать таблицу сравнения всех действительных разрывов транзакций между Налоговым адресом и Главным адресом.

Trigger contract(“PoTxM”,”PoTxV”) //Function returns Xm,Xv

XM ; XV ; I:INT=0 ; XM:ARRAY=[T1,T2,T3,..,TN] //holds transaction history

XV:ARRAY=[T1,T2,T3,..,TN] //vat history

WHILE I<COUNT(XM){PRINT XM[I]}

WHILE I<COUNT(XV){PRINT XM[I] ; PRINT <hr />}

**Интеграция кошелька Безоп**

Основанный на смарт контракте, ДУЗ Безоп позволит торговым партнерам Безоп кошелек эффективное слияние, легкий прием и сверхбыструю обработку транзакций. С помощью блока Эфириум мы можем очистить транзакции в кошельке Безоп с 1-го шага и за 1 таксу, что приведет к принятию платежей в целом в 5 раз дешевле и быстрее для торговых компаний. Торговые компании смогут принимать платежи с кошельков на базе Эфириума.

**3) Доказательство заказа**

Позволяет проверить транзакцию. В случае покупки он должен предоставить (убедительное доказательство) предоставление услуги, действительное доказательство налога (НДС) и подтверждение правильности для одной или нескольких транзакций.

Доказательство порядка добавляет «легитимности» и «законность цели» к каждой транзакции в сети Безоп, пока она остается децентрализованной, анонимной и не требующей доверия. Консенсус для полного «Подтверждения заказа»

- Продавцы должны убедить сеть, что они доставили оплаченные продукты, услуги или программное обеспечение в хорошем состоянии; Продавцы будут генерировать доказательство доставки, которые могут отслеживаться сетью блокчейн

- Сеть блокчейн должна хранить подтверждение транзакции

- Сеть блокчейн может генерировать доказательство налога

В этом разделе мы мотивируем, представляем и намечаем реализации для схем Доказательства доставки (ДД) и Доказательства транзакции (ДT) и доказательства налога (ДН), используемые в Безоп.

**Мотивация**

Схемы орфографических ордеров, такие как схемы Proof-of-Delivery (POD) и Proof-of-Transaction (PoT), позволяют сети (N) отслеживать текущее состояние и хранить данные транзакции с помощью смарт-контракта с пользователем.

Схема Доказательства транзакции (ДT) гарантирует доставку заказа.

**Атаки**

В Безоп нам нужны более сильные гарантии для предотвращения трех типов атак, которые злоумышленники могут использовать для оплаты продуктов и услуг, которые они не предоставляют:

Атака Рогови («Rogovy attack»),

Атака постоянное затмение («Permanent Eclipse Attack»)

**Атака «Rogovy Attack»:**

Это своего рода атака, когда несколько торговцев становятся мошенниками и отмечают большое количество заказов доставленными, хотя фактическая доставка не соответствует описанию. В этом случае покупатель оплачивает то, что он не смогут использовать.

**Компоненты для атаки «Rogovy Attack» в Безоп**

Злоумышленник (и) должны владеть несколькими адресами торговых точек и быстро запускать протокол смарт контракт с помощью бота.

Доверие этой атаки зависит от способности клиента реагировать своевременно.

**Атака постоянное затмение:**

Это критически важная уязвимость в равноправном (пиринговом) протоколе Эфириум. Если уязвимостью воспользуются, то атака может привести к отказу в обслуживании и она также может быть использована злоумышленником в качестве атаки двойной траты.

Из-за низких требований к ресурсам атаки, злоумышленник с ограниченными возможностями может легко поддерживать атаку на всю сеть Эфириум (в конечном счете, сеть Безоп).

**Компоненты для атаки «Eclipse Attack» в сетях Безоп- Эфириум**

Атака является уязвимостью в равноправном (пиринговом) протоколе. Однако она была протестирован только с клиентом geth.

**- Распространение блоков**

Блоки распространяются тремя способами в сети Эфириум. Во-первых, узел B, который получает новый блок, будет напрямую подталкивать блок к √n своих подключенных равноправных (пиринговых) узлов, где n - общее количество подключенных узлов. Во-вторых, B отправит сообщение Хеши Нового Блока (NewBlockHashes) всем своим узлам, объявляя о новом блоке.

Когда узел A получает объявление о новом блоке, он будет запрашивать блок ровно через 0,5 секунды от случайного узла, из которого он получил соответствующее объявление (если только A не получил блок от другого узла в это же время), а затем забывает обо всех других объявлениях для этого блока. Это означает, что если A запрашивает блок из узла B, а B не смог ответить, то он не будет запрашивать блок у других узлов. Если A теряет блок, то используется третий метод распространения блоков, который является синхронизацией блоков, описанного ниже в разделе 1.3.2.

**- Синхронизация блоков**

Узел будет синхронизироваться только с одним другим узлом за один раз. Узел «A» запускает синхронизацию блоков в следующих случаях:

 «A» начинает соединение с новым узлом с более высокой общей сложностью объявления (например, после присоединения или воссоединившись с сетью).

Узел «А», с более высокой общей сложностью объявления, чем «А», подключается к «А».

 «A» получает блок с более высокой суммарной сложностью объявления, чем глава его текущего блокчейна, и отсутствует некоторые из предыдущих блоков.

**- Подробности атаки**

Ниже приведен критический недостаток консенсуса в равноправном (пиринговом) протоколе. Используя эту уязвимость, злоумышленник B может заставить жертву A получить блок в размере n + 1 почти бессрочно. В то время как A может получать более поздние блоки от других узлов, он будет оставаться на уровне 'n', поскольку он пропускает ссылку в блокчейне. Злоумышленник B может работать следующим образом:

1. B создает длинный блокчейн, начиная с первичного блока. Это можно осуществить, уменьшив сложность для каждого блока, тем самым сократив время, необходимое для создания действительного доказательства работы.

Создание альтернативного блокчейна занимает относительно большое количество предварительных вычислений. Однако, как только образуется альтернативный блокчейн, его не нужно будет снова вычислять и его можно будет использовать для нескольких атак.

2. Если цепочка B короче, чем действующая цепочка, B подделывает блок с высоким номером блока и действительным доказательством работы, т. е. создает блок без родителя, который использует произвольное значение в качестве родительского хеша.

3. Если блокчейн злоумышленника короче, чем действующий блокчейн, B также необходимо подделать блок с номером блока Получитьмаксимальныйзаголовок (MaxHeaderFetch) с длиной меньшей блокчейна A и блокировать в размерах, которые будут запрашиваться в двоичном поиске, но не будут содержатся в блокчейне B.

4. B соединяется с узлом A, объявляя общую высокую сложность.

5. отправляет заголовок блока с наивысшим размером блока из его цепи (или блока, созданного на шаге 2), на адрес узла A в ответ на первый запрос ПОЛУЧИТЬЗАГОЛОВОКБЛОКА (GetBlockHeaders) от узла A.

6. В ответ на второй запрос ПОЛУЧИТЬЗАГОЛОВОКБЛОКА (GetBlockHeaders) от узла A, B отправляет блок из своего отдельного блокчейна, соответствующей размеру блока, указанному в сообщении A (или блоке, подделанном на шаге 3).

7. В ответ на запросы двоичного поиска узла A узел B снова отвечает сообщением о заголовках блока из своего блокчейна, пока не будет достигнут первичный блок.

8. B отвечает блоками из своего собственного блокчейна, отправляя только один блок в ответ на каждый запрос. Для каждого запроса B может ввести задержку до 3 секунд.

9. Пока атака продолжается, узел A не сможет синхронизироваться с другими узлами.

Доказательство работы:

Механизм доказательства работы был прорывом, потому что он одновременно решал две проблемы. Во-первых, он обеспечил простой и умеренно эффективный алгоритм достижения консенсуса, позволяющий узлам в сети коллективно согласовывать набор обновлений до состояния журнала биткойнов. Во-вторых, он предоставил механизм для свободного входа в консенсусный процесс, разрешая политическую проблему поиска решения, кто может влиять на консенсус, одновременно предотвращая атаки Сибиллы. Он делает это, заменяя формальный барьер на участие, такой как требование быть зарегистрированным как уникальный объект в конкретном списке, с экономическим барьером - вес одного узла в процессе консенсусного голосования прямо пропорционален вычислительной мощности, которую узел приносит. С тех пор был предложен альтернативный подход, называемый доказательством доли, вычисляющий как вес узла пропорционален своим валютным резервам, а не его вычислительным ресурсам. Обсуждение относительных достоинств двух подходов выходит за рамки настоящего документа, но следует отметить, что оба подхода могут использоваться в качестве основы криптовалюты.

**Процесс майнинга в сети Безоп**

[**http://joxi.ru/L21oMOYC6Q1wer**](http://joxi.ru/L21oMOYC6Q1wer)

Если бы мы имели доступ к надежной централизованной службе, эта система была бы тривиальной для реализации; она может быть закодирована точно так, как описано, используя жесткий диск централизованного сервера для отслеживания состояния. Однако с биткоином мы пытаемся создать децентрализованную валютную систему, поэтому нам необходимо будет объединить систему государственного перехода с системой консенсуса, чтобы гарантировать, что все согласятся на порядок транзакций. Децентрализованный консенсусный процесс Биткоина требует, чтобы узлы в сети постоянно пытались создавать пакеты транзакций, называемые «блоками». Сеть предназначена для создания одного блока примерно каждые десять минут, причем каждый блок содержит метку времени, одноразовый номер, ссылку на (т.е. хэш) предыдущий блок и список всех транзакций, которые произошли со времени предыдущего блок. Со временем это создает стабильный, постоянно растущий «блокчейн», который постоянно обновляется, чтобы представить последнее состояние журнала биткойнов.

Алгоритм проверки правильности блока, выраженный в этой парадигме, выглядит следующим образом:

● Проверьте, существует ли предыдущий блок, на который идет ссылка, и действителен ли он.

● Убедитесь, что временная метка блока больше, чем у предыдущего блока и создана не менее 2 часов назад.

● Убедитесь, что доказательство работы блоком является действительным

● Позвольте S[0] быть состоянию в конце предыдущего блока

● Предположите TX это список транзакций блока с количеством транзакциями «n». Для всех, i в случае 0...n-1, установите S[i+1] = ПРИМЕНИТЬ APPLY(S[i],TX[i]) Если какое-либо приложение возвращается ошибкой, выходите и пишите «ошибку»

● Пишите «Верно», и регистрируете S[n] как состояние в конце этого блока.

По сути, каждая транзакция в блоке должна обеспечивать действительный переход состояния из того, что было каноническим состоянием, прежде чем транзакция была выполнена в какое-то новое состояние. Обратите внимание, что состояние не закодировано в блоке каким-либо образом; это абстрактное чисто, которое следует запомнить проверяющему узлу и может быть (надежно) вычислено для любого блока, начиная с первичного состояния и последовательно применяя каждую транзакцию в каждом блоке. Кроме того, обратите внимание, что имеет значение порядок, в котором майнер включает транзакции в блок, если в блоке есть две транзакции A и B, так что B проводит UTXO, созданный A, тогда блок будет действителен, если A будет перед B, но не иначе.

Имеется одно условие действительности, указанное в приведенном выше списке, которое не встречается в других системах, это требование «доказательства работы». Точное условие состоит в том, что хеш двойного SHA256 каждого блока, рассматриваемый как 256-битное число, должен быть меньше, чем динамически скорректированная цель, которая на момент написания этой статьи составляет приблизительно 2187. Целью этого является создание блока «жестким» в вычислительном отношении, тем самым предотвращая злоумышленников атаки Сибиллы от возможности переделать целый блокчейн в свою пользу. Поскольку хеш SHA256 спроектирован как абсолютно непредсказуемая псевдослучайная функция, единственный способ создать действующий блок - просто метод проб и ошибок, неоднократно увеличивая значение одноразового номера и проверяя, соответствует ли новый хеш на этот раз.

Например, цель ~ 2187, сеть должна сделать в среднем ~ 269 попыток до того, как будет найден действительный блок; в общем, цель перенастраивается сетью каждые 2016 блоков, так что в среднем каждый блок в сети каждые десять минут генерирует новый блок. Чтобы компенсировать майнерам эту вычислительную работу, майнер каждого блока имеет право внести себе транзакцию, дающую ему 12,5 BTC из ниоткуда. Кроме того, если какая-либо транзакция имеет более высокую общую стоимость на своих входах, чем в ее результатах, разница также переходит к майнеру в качестве «платы за транзакцию». Кстати, это также единственный механизм, с помощью которого выпускается BTC; в первичном состоянии вообще не было монет.

Для того чтобы лучше понять цель добычи криптовалюты (процесса майнинга), давайте рассмотрим, что произойдет в случае злонамеренной атаки. Так как базовая криптография Биткоина известна как безопасная, злоумышленник будет нацелен на ту часть системы Биткоина, которая не защищена криптографией напрямую: на порядок транзакций. Стратегия злоумышленника проста:

1. Отправьте 100 BTC торговцу в обмен на какой-либо продукт (желательно быстродоставляемый цифровой товар).

2. Дождитесь доставки продукта.

3. Произведите еще одну транзакцию, отправляющую те же 100 BTC самому себе.

4. Попытаться убедить сеть в том, что его сделка была самой первой.

Как только шаг (1) произошел, через несколько минут какой-то майнер будет включать транзакцию в блок, например, номер блока 270 000. Примерно через час через цепочку будет добавлено еще пять блоков, причем каждый из этих блоков будет косвенно указывает на транзакцию и, таким образом, «подтверждать» ее. На этом этапе продавец примет оплату в соответствии с окончательной доработкой и поставкой продукта; так как мы предполагаем, что это цифровой товар, доставка мгновенная. Теперь злоумышленник создает другую транзакцию, отправляющую 100 BTC себе. Если злоумышленник просто отпускает ее на волю, транзакция не будет обработана; майнеры будут пытаться запустить APPLY (S, TX) и заметят, что TX потребляет UTXO, который больше не находится в состоянии. Поэтому вместо этого злоумышленник создает «вилку» блокчейна биткойн, начиная с разработки другой версии блока 270 000, указывающей на тот же блок 269,999 в качестве родителя, но с новой транзакцией вместо старой. Поскольку данные блока различаются, для этого требуется повторить доказательство работы для соответствующего блока. Кроме того, новая версия блока злоумышленника с условным номером 270 000 имеет другой хеш, поэтому исходные блоки начиная с 270,001 по 270,005 не «указывают» на него; таким образом, оригинальная цепочка и новая цепочка атакующего полностью разделены. Правило заключается в том, что в случае с «вилкой» самый длинный блокчейн воспринимается как истинный, и поэтому легальные майнеры будут работать над цепочкой, начиная с 270005, в то время, когда атакующий работает над цепью, начиная с 270 000. Для того, чтобы атакующий сделал его блокчейн самым длинным, ему понадобилось бы больше вычислительной мощности, чем остальная сеть, объединенная для того, чтобы догнать (следовательно, «51% -ая атака»). Блоки биткойнов зависят от хэша всех предыдущих блоков. Злоумышленник с огромной вычислительной мощностью может переделать доказательство работы (ДР) для значительного количества блоков и в конечном итоге может получить много биткойнов, но, как описано в документе Сатоши, вознаграждение за процесс майнинга действующего блока является намного большим, чем за разрыв сети. Но в вопросе невозможности получения награды за майнинг то же самое действие не будет оправдано.

**Доказательство транзакции и доставки**

Доказательство доставки: цифровое «Доказательство Транзакции» генерируется сетью Безоп для любой продажи товаров и услуг, она является общедоступной, неизменной и сохраняет анонимность для обеих сторон.

данные транзакции: { α|obj: val , β|str : val, γ₁|str: val, δ₁|float : val, ε:bool:val, tid|str : val }

α - данные, β – адрес отправителя, γ₁ - временная отметка, δ₁ - объем (количество)

ε – направляемый к (входящий :1 , исходящий: 0) , tid – идентификационный номер транзакции id

α - данные - это объект, содержащий

Наименование товара

Описание продукта

Product\_SKU

Статус заказа

Состояние доставки

Ставка НДС

Рис. Доказательство транзакции (структура данных)

 <http://joxi.ru/Q2KQOoMT91ldQr>

ДД: Доказательство доставки (ДД) - это способ установления факта, что получатель получил содержимое, отправленное отправителем. Когда отправитель отправляет несколько физических товаров или цифровой контент, есть вероятность того, что что-то не достигнет предполагаемого получателя.

Подтверждение доставки становится очень важным, когда юридические и финансовые документы должны быть предметом обмена между двумя сторонами. В Соединенных Штатах DHL, UPS и FedEx, а также почтовая служба США (USPS) предоставляют подтверждение доставки. Операторы коммерческих флотов также должны иметь возможность предоставить подтверждение доставки товаров своим клиентам.

В электронной коммерции предприятия обмениваются миллионами электронных документов для отслеживания информации о доставке с использованием компьютерных технологий, таких как электронная почта, FTP и EDI. Эти документы содержат различные данные о транзакциях, включая информацию о заказах на покупку, счета-фактуры, данные о доставке, спецификации продукта и ценовые котировки. Электронные документы могут обмениваться новыми данными, а также исправлениями ранее переданных сообщений.

Юридические осложнения могут возникнуть, если компания получателя опровергает получение исправленной спецификации продукта или сообщение о задержке отправки. Обе компании могут быть в ссоре, каждый из которых доказывает / не доказывает существование этого конкретного сообщения.

Decentralized proof of delivery is similar in function however works in reverse, the shipper/store owner Is liable to provide a ‘proof of delivery’ within 30days of marking the order as shipped on the network, this can be done through the DOM which is linked to the receiving wallet ; the options are Децентрализованное доказательство доставки аналогично по функциям, однако работает наоборот, грузоотправителя / владелец склада несет ответственность за предоставление «подтверждение доставки» в течение 30 дней с маркировкой заказа как «отправленного» в сети, это может быть сделано через ДУЗ, который связан с кошельком получающего отправление; варианты

a) Предоставление ссылки на отсканированный документ доставки

b) Предоставление ссылки на снимок экрана (скриншот) доказательства доставки

c) номер отслеживания пакета

Для подтверждения доставки требуется перечислить «плата за газ» (\*gas fee – это отчисление майнерам) , которую майнеры будут использовать для подтверждения доставки. После того, как доставка одобрена майнером, состояние заказа изменяется на «было предоставлено», заказ считается выполненным, а статус заказа обновляется.

**Доказательство налога**

Цифровое «Доказательство налога» создается и хранится в сети «Безоп» для операций, связанных с продажей товаров и услуг. ДУЗ Безоп предоставляет мощную функцию, которая позволяет пользователям собирать НДС для своих продуктов на их вторичный кошелек, который сеть автоматически выдает всем владельцам счетов Безоп. Доказательство налога является общедоступным, неизменным и сохраняет анонимность для обеих сторон.

Налоговый кошелек работает точно так же, как стандартный кошелек, за исключением того, что он соединен / связан с основным адресом с помощью легко вычисляемого хеша, известного как производное обязательсво. Цели, которые обслуживает налоговый кошелек, перечислены ниже:

1) Сбор налога на добавленную стоимость (НДС)

2) Автоматический расчет и формирование налогового отчета

**Налоговый отчет, хранящийся в блокчейне, неизменен и устойчив к потере**

Случаи на практике

**Ваш бухгалтер переезжает или фирма закрывается**

Ситуация: вчера я оказался в довольно затруднительном положении, когда не смог связаться со своим давним бухгалтером. Оказывается, его фирма закрылась, когда мне было нужно, чтобы он дал мне копию налогового отчета для рефинансирования по моему дому. Я был непредусмотрителен и не сохранил копию, и никогда не беспокоился о том, что у меня ее не было, потому что я всегда думал, что мой дипломированный бухгалтер-ревизор-аудитор подстрахует меня в вопросе хранения копий моего прошлого налогового отчета и моя уверенность в этом ... плохо, что это было не так. Итак, что вы будете делать, если окажетесь в подобной ситуации, и ваш бухгалтер по налогам сошел с дистанции?

**ВЫ переместили и выбросили все свои документы или просто уничтожили свою последнюю копию налогового отчета**

Ситуация: недавно я переехал, чтобы быть ближе к моей семье и моим близким, но понял, что я выбросил свою копию налогового отчета за прошлый год. Я подумал, почему-то мне он не понадобится, и так как мой налоговый составитель сейчас находится далеко и не берет трубку. Мой сын подал заявку на учебу в колледже и ходатайствует о финансовой помощи - мне нужен отчет, ведь это поможет ему освоиться здесь, и поэтому я теперь не перестаю отчитывать себя. Как быстро и надежно получить копию старого налогового отчета?

**Вы потеряли свою копию налогового отчета в результате пожара или наводнения**

Ситуация: моя семья и я пережили мучительное испытание, потеряв наш дом в результате пожара. Все целы и невредимы, но теперь мне нужно строить всю жизнь с нуля, и я даже не знаю, с чего начать. Я знаю, что мне нужно собрать свои финансы воедино, и чтобы сделать это, мне нужна копия моего налогового отчета. Я знаю, что есть какой-то способ получить копию, не дожидаясь, пока Служба по внутреннему налогообложению отправит их - я бездомный и я боюсь, но хочу, чтобы кто-то помог мне прямо сейчас! Есть ли способ получить копию моего прошлого налогового отчета и помощь, которая мне нужна?

**Ваш компьютер вышел из строя со всеми вашими загруженными в электронном варианте копиями налоговых отчетов**

Ситуация: Я аспирант, который считается обстоятельным, старательным и организованным. Но вчера мой компьютер неожиданно вышел из строя из-за вируса, и теперь у меня нет доступа к моим копиям налогового отчета, которые я подал и сохранил в электронном виде! Мне нужны мои финансовые документы для квалификационного экзамена, для моих собственных нужд и для моего заявления на новую аренду, которое я должен подать завтра! Помогите! Куда я могу обратиться за помощью, чтобы получить копию моего старого налогового отчета в 3 часа ночи?

**3) Смарт контракты**

**3.1 Контракты в Безоп:**

Смарт контракты обеспечивают полностью безопасное и надежное решение для электронной коммерции на основании протокола подтверждения заказа, а защита покупателя будет доступна через блокчейн Эфириум.

Ряд смарт контрактов, подробная структура и функциональность будут определены в этом разделе и завершены с большим количеством исследований. Чтобы проиллюстрировать предполагаемые функциональные возможности, мы предоставляем примерные рабочие процессы, иллюстрирующие процесс покупки, отмены, претензии и обработку споров на блокчейне.

**Торговый кошелек (на технологиях смарт контракта):**

Защита покупателя является важной проблемой в электронной торговле. Система ДУЗ Безоп (децентрализованное управление заказами) предназначена для работы только со специализированными кошельками. Стандартный кошелек Безоп состоит из «основного

кошелька» и «налогового кошелька», связанного с использованием легко вычисляемого хеша, известного как «производное обязательство».

The Merchant wallet is a simple smart contract on the blockchain that does the work of a middle-man (escrow system) and keeps both the client and merchant safe. The contract transfers a client’s funds into cold storage. Which is unlockable only after (X) days when proof-of-delivery is provided by the merchant. If a merchant fails to provide PoD, the buyer will have the option to cancel. Торговый кошелек — это простой смарт-контракт на блокчейне, который выполняет работу среднего человека (система условного депонирования) и обеспечивает безопасность как клиента, так и продавца. Контракт переносит средства клиента на холодное хранение. Это разблокируется только после (X) дней, когда продавцом предоставляется доказательство доставки. Если продавец не может предоставить PoD, у покупателя будет возможность отменить.

На простом рисунке показан дизайн торгового / контрактного кошелька, как основной кошелек и налоговый кошелек связаны с вторичными обязательствами).

<http://joxi.ru/823o0XQC6d1JL2>

|  |  |
| --- | --- |
| Main Wallet | Основной кошелек |
| Bond Derivative  | вторичные обязательства |
| Entangled | связан |
| Tax Wallet  | Налоговый кошелек |
| Cold Storage | Хранение на время приостановки операций |
| Smart contract  | Смарт контракт |
| Record Merchant wallet  | Запись о транзакции в торговом кошельке |

**Создание торгового кошелька (смарт контракт)** <http://joxi.ru/vAWngowHke8qW2>

|  |  |
| --- | --- |
| Regular User Provides  | Постоянный пользователь предоставляет |
| Provide Requirements Main Wallet addressAvg time to ship Tax wallet addressBond key | Предоставить ТребованияАдрес главного кошелькаСреднее время доставки Адрес налогового кошелькасвязанный ключ |
| Submit (Requires Gas) Smart Contract Field Merchant Wallet Method: Create New | Отправить (Требуется газовый взнос)Смарт контрактПоле действия торгового кошелька Метод: создать новый |
| Implementation Stores Immutable Record  | Реализация магазинов Неизменяемая запись |
| Merchant wallet & RecordsMain WalletTax wallet TransactionsCompletedReputationcancellations | Торговый кошелек и записиОсновной кошелекНалоговый кошелектранзакцииЗавершенныйрепутацияАннулирование |
| Dispatch  | Отправка  |
| return | возврат |
| Merchant wallet address | Адрес торгового кошелька |

Торговый кошелек имитирует поведение обычного кошелька, однако он основан на контрактном адресе и работает автономно.

X означает количество дней до отгрузки. Это определяется продавцом при создании своего торгового кошелька.

**Размещение заказа (смарт контракты)**

Во время размещения заказа, токены отправляются на адрес кошелька продавца (контракт в сети Эфириум), это запускает смарт-контракт, который автоматически переносит средства в защищенный кошелек для отложенного хранения и на месте, хранит цифровой отложенный платеж в реестре, известным как " обещанная запись". Это обещание кредитовать основной кошелек и налоговый кошелек выполняется только после того, как все условия будут выполнены для продажи. Некоторые общие условия:

i) X дней прошло

ii) предоставляется доказательство доставки

iii ) транзакция не была отменена

iv) i,ii,iii условия соблюдены

<http://joxi.ru/l2Zk0oDc81qEbA>

|  |  |
| --- | --- |
| Client  | клиент |
| Picks a product on Bezop DOM or integrated site | Выбирает продукт на площадке ДУЗ Безоп или другом интегрированном сайте  |
| Client Accepts to pay with eth and clicks pay now | Клиент принимает условие оплаты с помощью Эфириум и нажимает «Оплатить сейчас» |
| Logged in Yes No | Авторизован Да Нет |
| Store checkout details redirect to registration/ login page  | Сведения о контроле за покупкой перенаправляются на страницу регистрации / входа в систему  |
| Completes registration Yes-return, no | Завершение регистрации Да-возврат, нет |
| Cancel purchase intent | Отменить намерение покупки |
| General payment button and barcode initiate checkout | Кнопка общей оплаты и запуск проверки штрих-кода |
| Validate merchant address Yes no  | Подтвердить адрес продавцаДа нет |
| Trigger order placement Smart contract & Store Deal Conditions Dispatch  | Запустить Размещение заказа Смарт контракт & отправить Условия сделки магазина |
| Store Funds in Cold Storage  | Хранить средства в отложенном режиме |
| Update Merchant Data Table with New Promises and Product data (return)  | Обновление таблицы данных продавца с новыми обещаниями и данными о продукте (возврат) |
| Data Table updated  | Таблица данных обновлена |
| Return User to Payment Successful url and set order status to s2-p | Возврат пользователя к Успешному URL-адресу платежа и установить статус заказа до s2-p |

**Принудительное аннулирование заказа (смарт контракт)**

В случае аннулирования заказа токены не отправляются клиенту до истечения безопасного периода, в книге записей транзакций продавца хранится обещание вернуть средства отправителю после периода гашения чеков, все предыдущие обещания аннулируются, клиенту сообщается, что он получит возмещение после того как произведут расчеты.

<http://joxi.ru/KAxLyqET4gxvLA>

|  |  |
| --- | --- |
| Client | клиент |
| Opens Purchases panel in there bezop wallet  | Открывается панель «Покупки» в кошельке Безоп |
| Select transaction they wish to dispute  | Выберите транзакцию, которую они хотят оспаривать |
| 2FA Failed Passed  | 2FA Отказ Успешное прохождение |
| Retry | Попытаться снова  |
| Open Dispute on Merchant’s Wallet for that product  | Открыть спор в кошельке продавца для этого продукта |
| Completes 2fa | Завершается 2fa |
| Check if transaction is older than X (no) | Проверьте, не превышает ли транзакция X (нет) |
| Is proof of delivery ready? (Return)  | Готово ли подтверждение доставки? (Вернуть) |
| Cancellation cannot be processed after shipment  | Аннулирование заказа не может быть обработано после отгрузки товара |
| Trigger cancellation smart contract (dispatch)  | Запустить отмену через смарт контракт (отправка) |
| Move funds clearance cold storage  | Перевод средств после расчетов после отложенного хранения |
| Update merchant data Table, update promises, update order status (return)  | Обновить данные о торговых таблицах, обновить обещания, обновить статус заказа (возврат) |
| Add new reserval promises  | Добавить новые резервные обещания |
| Data table updated | Обновлена таблица данных |
| Return User to cancellation successful url and set order status to s4-c | Вернуть пользователя к Успешному URL-адресу отмены заказа и установить статус заказа на s4-c |

Примечание: в течение X дней покупатель может отменить транзакцию и вернуть все сделанные платежи, если заказ не был отправлен или клиент не хочет продолжать.

Отмененные средства попадают на отложенное хранение на срок в 14 дней, прежде чем возвратиться к клиенту. Стимулирующая выплата (газовый сбор майнерам) необходим для запуска смарт контракта отмены транзакции.

**Доказательство налога (смарт контракт)**

Этот договор возвращает все налоговые данные, относящиеся к адресу продавца

|  |  |
| --- | --- |
| Client | Клиент |
| Proof of Tax smart contract Verify merchant idPopulate vat record Assign XMatchCorrect failed Merge  | Подтверждение налога смарт контрактаПодтвердить идентификационный номер продавцаЗаполнение записи НДСПрисвоить XСовпадениеПравильноеНеправильное слияние |
| Return  | Возврат |
| Proof of Tax | Доказательство налога |
| - x must be computed for correctness by taking the hash of γ.ΦTax Data: { α|obj : val , γ|str: val, δ|float : val, ε:bool:val, x|str:val}α - data, γ – timestamp ,γ₁ - timestamp of parent transaction δ – volume, δ₁ - volume of parent transactionε – bound (inbound:1 , outbound: 0)Φ – val (γ₁.δ₁)i – tid of original transactionx – correctness byte [hash (γ.Φ) ] | - x должен быть вычислен для правильности, взяв хэш из γ.ΦНалоговые данные : { α|obj : val , γ|str: val, δ|float : val, ε:bool:val, x|str:val}α - данные, γ – временная отметка ,γ₁ - временная метка родительской транзакции δ - Объем,δ₁ - объем материнской сделкиε – направляющийся в (входящий:1 , исходящий: 0)Φ – val (γ₁.δ₁)i – проверка первоначальной транзакцииx - байт правильности [хеш (γ.Φ) ] |

**Доказательство доставки (смарт контракт)**

Этот контракт представляет подтверждение доставки для заказа в сети.

|  |  |
| --- | --- |
| Merchant | Продавец |
| Opens order on Merchant software | Открывает заказ на программное обеспечение продавца |
| Proof of delivery Max (60 characters) Proof verification instruction Max (120 characters) | Доказательство доставкиМаксимально (60 символов)Инструкция проверки подтвержденияМаксимально (120 символов) |
| Proof of delivery Smart contract  | Доказательство доставки (смарт контракт) |
| Update order status | Обновить статус заказа |
| Waiting for customers response (3 days max) Accept No responseDispute received  | Ожидание ответа клиентов (максимум 3 дня)Принять Нет ответаРазногласия (споры) |
| Agreement Txn complete  | Соглашение Txn завершено |
| Credit merchant’s Main and tax wallet  | Основной и налоговый кошелек кредитных средств продавца |
| Close promises update order status  | Закрыть обещание обновить статус заказа |
| Waiting for applications from dispute settlers | Ожидание заявок от участников спора |
| Randomly assigned to a decentralized agent after 5 applications | Случайно назначается децентрализованному агенту после 5 заявок |
| Resolved in favor of client | Решено в пользу клиента |
| Credit client  | Кредит в пользу клиента |
| Close promises update order status | Закрыть обещание обновить статус заказа |
| Resolved in favor of merchant  | Решено в пользу продавца |
| Claim denied txn complete  | Требование отклонено txn завершено |

После подачи подтверждения доставки, заказ помечен доставленным, а дополнительно дополнительный уровень безопасности дает клиенту 3 дня чтобы оспорить транзакцию, если у него возникнет проблема.

Спорный смарт контракт отличается от контракта аннулирования, который является автоматическим, тогда клиент может зарегистрировать проблему в заказе, но после того, как прошло X дней, продавец предоставит подтверждение доставки. Сеть подключает сторонних майнеров, которые могут заработать 0,5% от транзакции, разрешив этот спор.

Для открытия спора нужно (оплатить майнерам) газовый сбор.

**Децентрализованный агент по спорам**

агенты по спорам могут проверить подтверждение доставки, предоставленное продавцом, с использованием инструкций и принять решение в пользу клиента или продавца. Покупателю или клиенту не требуется в дальнейшем входной ключ.

**Доказательство транзакции (смарт контракт)**

Этот смарт контракт возвращает компонент данных транзакции, на входного адрес продавца.

|  |  |
| --- | --- |
| Client  | Клиент |
| Proof of Transaction smart contract Verify merchant idOpen transactionsSearch based for main addressMatches | Подтверждение транзакции смарт контрактомПодтвердить идентификационный номер продавцаОткрыть транзакцииПоиск основного адресаСовпадения |
| Correct  | Верное |
| Merge | Слияние |
| Return | Возврат |
| 1 Proof of Transactions | 1 Доказательство сделок |

**4 Будущая работа**

Эта работа представляет собой четкий и сплоченный путь к построению сети Безоп; однако мы также считаем эту работу отправной точкой для будущих исследований децентрализованных систем электронной торговли. В этом разделе мы определяем и заполняем три категории будущей работы. Это включает уже выполненную работу и просто ждет описания и публикации, также открытых вопросов для улучшения существующих протоколов и формализации протокола.

**4.1 Текущая работа**

Интеграция обращения

Кошелек Рейнбоу (Rainbow)

ДУЗ Безоп

Смарт контракты

Интеграция кошелька ДУЗ Безоп

Добавление продукта в сеть

**4.2 Открытые вопросы**

**Безоп представит рейтинг продукта?**

Да, будущие смарт контракты позволят пользователям добавлять продукты в сеть, и все покупки должны быть связаны с продуктами в сети.

После покупки, клиент получит дополнительную возможность опубликовать рейтинг после получения подтверждения доставки.

**Будет ли Безоп отделяться от своей сети?**

«Безоп» - такая масштабная концепция, что раскол сети эфириум неизбежен

Как только у нас будет стабильный продукт.

См. план действия технической документации - <http://bezop.org/whitepaper.pdf>

**Имеются ли в магазинах Безоп магазины для продавцов?**

На данный момент нет.

В будущем мы можем подумать над этим, поскольку блокчейн становится более масштабируемым.

Продавцам придется найти дешевые и надежные решения для размещения магазинов.

**Как насчет интеграции с другими системами?**

На данный момент мы изучаем эту тему, в нашей следующей статье будут представлены подробности об этой работе.

**4.3 Доказательства и формальная проверка**

Из-за явной ценности доказательств и формальной проверки мы планируем доказать многие особенности сети Безоп и разработать формально проверенные спецификации протокола в ближайшие месяцы и годы. Несколько доказательств находятся в процессе разработки и еще больше на стадии продумывания. Но будет тяжелая, многолетняя работа, чтобы доказать многие особенности площадки Безоп (например, масштабирование, автономная работа без подключения к сети Интернет).

**Ссылки**

[1] Виталик Бутерин. Эфириум, Апрель 2014. URL <https://ethereum.org/>.

[2] Сатоши Накамото. Биткоин: Электронная наличная система с равнозначным (пиринговым) доступом, 2008. [https://bicoin.org](https://bicoin.org/)

[3] Википедия: Доказательство доставки, Январь 2012: <https://en.bitcoin.it/>