SafeHaven.io

… Решение проблемы наследования цифровых активов …

Брюссель, Ноябрь 2017
www.safehaven.io

Разработано Командой Safe Haven

Содержание

Список Рисунков

Отказ от Ответственности

Цель этого документа – облегчить понимание того, что из себя представляет SafeHaven. Настоящая статья представляет собой технический документ, в котором излагаются текущие и будущие изменения в рамках проекта SafeHaven. Этот документ предназначен исключительно для информационных целей и не гарантирует развития проекта в будущем. Если не указано иное, продукты и инновации, изложенные в настоящем документе, находятся на стадии разработки и не являются работающими в настоящее время. Мы не даем никаких гарантий или заверений в отношении успешной разработки или внедрения данных технологий и инноваций, а также осуществления любой другой деятельности, указанной в документе, и отказываемся от любых гарантий, подразумеваемых законами или любым иным образом. Никто не несет ответственности за содержание настоящего документа или за любые выводы, сделанные из него, включая (но не ограничиваясь) любые взаимодействия с Safe Haven или технологии, упомянутыми в этом документе. Safe Haven не несет никакой ответственности за любые убытки или ущерб любого рода, который может возникнуть у любого лица, действующего на основании информации, касающейся проекта Safe Haven, платформы Safe Haven или экосистемы Safe Haven, содержащейся в настоящем документе, или любой другой информации, которая может быть доступна о Safe Haven.

1 Введение

Мало кто знает, но криптовалюты стали побочным продуктом другого изобретения. У Сатоши Накамото, неизвестного изобретателя Биткоина (первой и самой важной криптовалюты), изначально не было намерения изобретать валюту.

В своем заявлении о Биткойне в конце 2008 года Сатоши сказал, что он разработал «Децентрализованную электронную систему по обмену денежными средствами.»

Его цель состояла в том, чтобы изобрести что-то, что многие люди не смогли создать раньше.

Единственной и самой важной частью изобретения Сатоши была децентрализованная цифровая денежная система. В девяностые годы было много подобных попыток создать цифровую валюту, но все они провалились.

Увидев, что все централизованные попытки терпят неудачи, Сатоши попытался построить цифровую денежную систему без единого центра управления. Подобную Peer-to-Peer сети для обмена файлами.

Это решение стало рождением криптовалют. Это был недостающий элемент, который нашел Сатоши, чтобы создать цифровые деньги. Идея сложна и может быть ее трудно понять, но если вы понимаете ее, вы будете знать больше о криптовалютах, чем большинство людей. Итак, давайте попробуем разобраться простыми словами:

Если сделать общий вывод, то цифровые деньги – это платежная сеть со счетами, балансами и транзакциями. Это легко понять. Одна из основных проблем, которую должна решить каждая платежная сеть, - это предотвращение "двойных расходов" (когда одна организация тратит одну и ту же сумму дважды, и только одна из этих транзакций приводит к изменению баланса счета). Обычно это делается центральным сервером, который ведет учет балансов. В децентрализованной сети не существует такого сервера. Таким образом, необходимо чтобы каждый объект сети осуществлял данную работу. Каждый узел в сети должен иметь список со всеми транзакциями, чтобы иметь возможность проверить, являются ли транзакции действительными или есть ли попытка удвоить расходы.

Но как эти субъекты могут сохранять консенсус в отношении этих записей?

Если пользователи сети не согласны только с одним единственным, незначительным балансом, все нарушается. Им нужно абсолютное согласие. Как правило, у вас есть центральный орган, чтобы объявить правильное состояние балансов. Но как можно достичь консенсуса без центрального органа?

Никто не знал, как это сделать, пока откуда не возьмись, не появился Сатоши. На самом деле, никто не считал это даже возможным.

Сатоши доказал, что это возможно. Его главным новшеством было достижение консенсуса без центрального органа. Криптовалюты – это часть этого решения. Часть, которая сделала это решение захватывающим, увлекательным и помогла изменить традиционный бизнес.

Поскольку вы читаете нашу белую книгу, значит Вы инвестировали или собираетесь инвестировать в этот перспективный рынок.

2 Проблема

Вы когда-нибудь задумывались о том, как в любую секунду с вами что-то может случиться? Задумывались ли вы когда-нибудь про тот день, когда ваша семья будет жить без вас? Как насчет ваших инвестиций в криптовалюту? Как насчет тех сложных рынков с сотнями приватных ключей, бирж и кошельков? Смогут ли они когда-нибудь вернуть ваши инвестиции без вас? Могут ли они доверять любому, кто помог бы им, не опасаясь, что что-то пойдет не так? Да, они могут! Safe Haven обеспечивает такое решение! Мы строим платформу на самых популярных и безопасных блокчейнах, чтобы вы могли перестать беспокоиться о своем наследии!

3 Решение

Мы в Safe Haven даем Вам возможность защитить ваши цифровые активы, не блокируя денежные средства. Благодаря нашему TFC ключу распределения долей, Escrow протколу (протокол депонирования) и Trust Alliance program (доверенные лица) приватные ключи/пароли могут быть распределены между участниками или членами семьи прозрачным и надежным образом.

Наш протокол распределяет доли таким образом, чтобы инвестор сохранял при любых условиях возможность управления своими активами. После смерти инвестора зарегистрированный член платформы Trust Alliance (нотариус) может получить оставшуюся долю на блокчейн, чтобы передать наследие инвестора его детям/заинтересованным сторонам.

Как это достигается? Ознакомьтесь с пошаговым руководством, которое включает несколько шагов и методы, описанные далее в этом документе.

3.1 Шаг за Шагом

Шаг 1: пользователь защищает свое наследство (крипто активы) и планирует распределить среди его троих детей свои приватные ключи или пароли, безопасно используя Safe Haven и прозрачное решение на блокчейн. Чтобы пройти необходимые шаги проверки, инициатор процесса обращается к зарегистрированному члену нашей сети Trust Alliance; это группа юридических лиц, которые имеют доверительные отношения с Safe Haven.

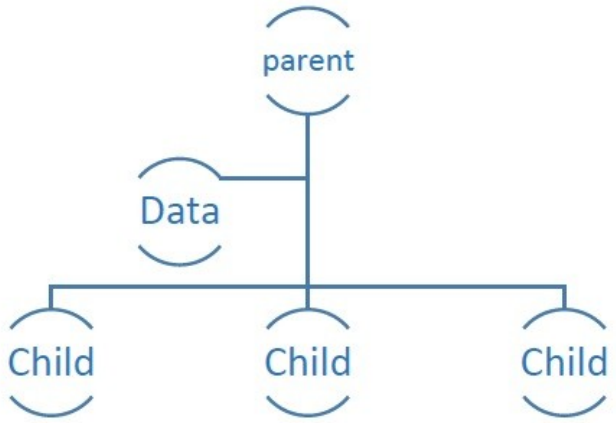


Рис.1 : Семейный Круг

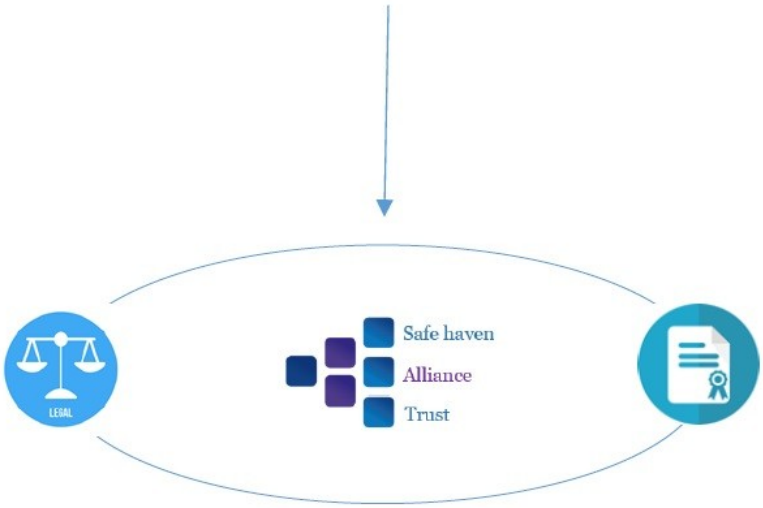


Рис.2 : Доверенные Лица

Шаг 2: юридическое лицо, которое является (в протоколе Safe Haven) валидатором, делит между детьми данные для защиты и распределения (см. TFC Протокол Распределения Долей) полученных долей с помощью протокола Safe Haven, специально разработанного для такого использования. Программное обеспечение, используемое для этого, не будет хранить данные в памяти или в централизованных базах данных. В блокчейн будут отправляться только общие ресурсы валидаторов (см. Процесс Проверки Долей). Алгоритм безопасности для шифрования и расшифровки общего ресурса перед развертыванием по смарт-контракту не будет доступен по очевидным причинам безопасности. У Safe Haven будут только первичные данные для идентификации валидатора и смарт контракта, общие данные будут находиться в децентрализованном регистре на блокчейн. Также для валидаторов будет существовать возможность резервного копирования (см. Система Многоуровневой Проверки и TFC Безошибочная Доля).

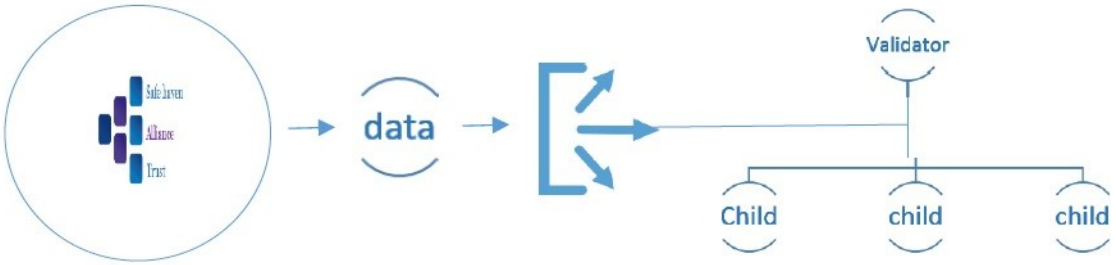


Рис.3 : Этап Распределения Долей

Шаг 3: доли, раздаваемые детям, управляются нотариусом в форме юридического свидетельства. Защищаемая доля, исходящая от родителя/инициатора, будет зашифрована приложением Safe Haven (доступна только членам Trust Alliance) и отправлена на блокчейн в виде смарт контракта.

Рис.4 : Сертификаты на Детей

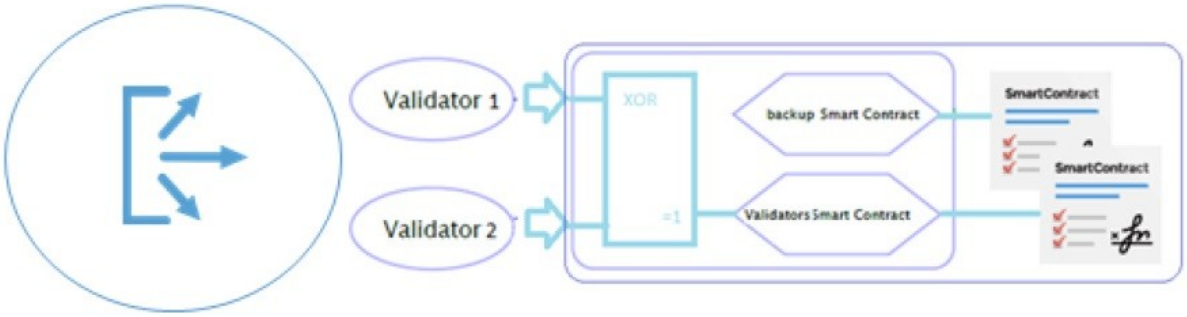


Рис.5 : Процесс Проверки

Доли детей могут быть разделены путем создания сертификата и/или интеграции аппаратного кошелька в наш протокол. В настоящее время мы ведем разработки в этом направлении, в том числе в области создания собственного холодного кошелька. Детали разработок пока не опубликованы, поскольку мы еще находимся на этапе ICO нашего проекта.

Шаг 4: В случае внезапной смерти или в случае, если инвестор не в состоянии самостоятельно управлять своими активами, дети или заинтересованные стороны могут получить свою долю, представив необходимые юридические документы своему нотариусу. После чего он, как только пройдет проверку Safe Haven, сможет извлечь из блокчейна положенную долю.

Наш протокол исключает возможность ошибки при распределении долей и при проверке создает резервную копию; дополнительная информация содержится в разделах TFC Fail-Safe Share(s) и Multiple Validators Possibility данного документа.

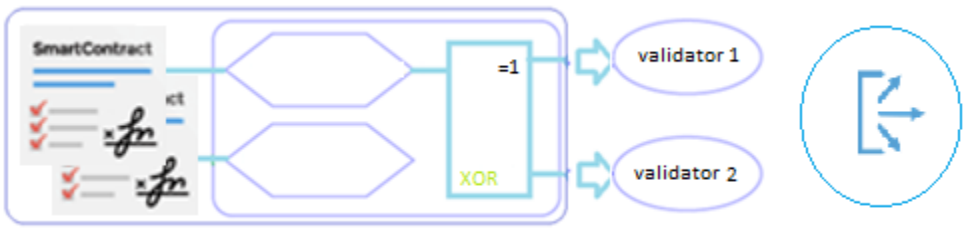


Рис. 6 : Процесс Извлечения Долей

4 Базовые Принципы

4.1 Блокчейн

Блокчейн – это инновационное программное обеспечение, создающее цифровое доверие между пользователями, облегчающее транзакции в сети. Блокчейн позволяет распределять доверие по всей сети, отпадает необходимость в центральном посреднике для отслеживания, проверки и утверждения обмена цифровыми активами. В настоящее время гарантом доверия, центральным посредником выступают как частные, так и правительственные институциональных структуры, однако их услуги стоят дорого, их работа медленная, они уязвимы для хакерских атак. Блокчейн решает эти проблемы, так как представляет собой децентрализованную распределенную базу данных, содержащую постоянно растущий список записей, называемых блоками.

4.2 Смарт Контракт

Компьютерный код на Блокчейн или «Умные контракты» – это компьютерные протоколы, которые облегчают, проверяют и обеспечивают выполнение контракта, делая необязательным заключение традиционного договора. Смарт контракты часто имитируют логику договорных условий. Смарт контракты могут обменивать деньги, имущество, акции или что-либо ценное прозрачным, бесконфликтным способом, избегая при этом услуг посредника. Обычно процесс требует оплаты посреднику, государственному органу, банку, адвокату или нотариусу, а затем время для обработки перед получением товаров или услуг. Однако с технологией смар контрактов все это может быть автоматизировано. Технологию смарт контракта можно сравнить с автоматизированным торговым автоматом. Вы вставляете деньги в торговый аппарат и выбираете нужный предмет, оплачиваете необходимую сумму и получаете заказ. При использовании смарт контракта деньги отправляются на блокчейн, а взамен вы получаете актив (например, цифровой сертификат права собственности на дом), который после выполнения условий мгновенно передается под контроль контрагента. Смарт контракты не только определяют условия соглашения, как традиционный контракт, но и обеспечивают исполнение этих обязательств.

5 Методы и Концептуальная Математика

5.1 Полиномиальная Интерполяция

Полиномиалы (многочлены) могут быть использованы для округления сложных кривых, например, форм букв в типографском деле. Соответствующим приложением является оценка естественных логарифмических и тригонометрических функций: выбор нескольких известных точек данных, создание таблицы поиска и интерполяция между указанными точками данных. Это приводит к значительно более быстрым вычислениям.

Уравнение:

Дается набор из *n +1* точек *(Xi, Yi)* в котором нет двух *Xi* таких же как многочлен *p* в степени не более чем *n*

$$p(x_i) = y_i, \qquad i = 0, \ldots, n.$$

Теорема «unisolvence» утверждает, что такой многочлен p существует и является уникальным и может быть доказан матрицей Вандермонда, как описано ниже

Теорема утверждает, что для N + 1 нод интерполяции (xi) полиномиальная интерполяция определяет линейное деление

$$L_n : \mathbb{K}^{n+1} \to \Pi_n$$

Где Пn-векторное пространство многочленов (определенных на любом интервале, содержащем ноды) в степени не более n.

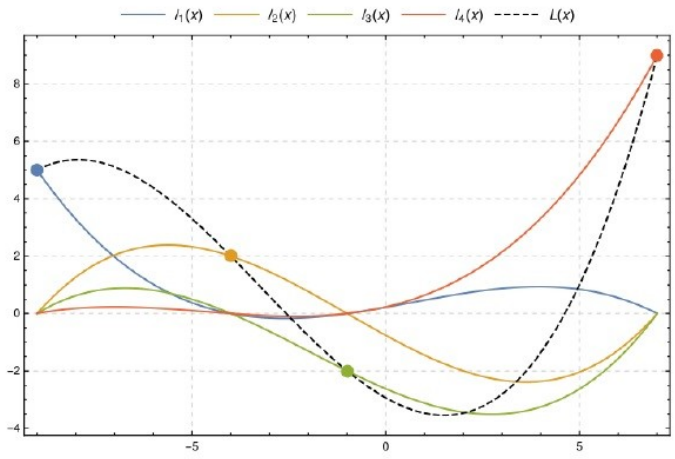


Рис.7: Полиномиалы

Полиномиальная интерполяция также составляет основу для алгоритмов в числительной квадратуре, числительных обыкновенных дифференциальных уравнениях и безопасных многоуровневых вычислениях в схемах секретного обмена. Схемы секретного обмена мы используем для достижения нашей цели.

5.2 Ключевой Депозит

Мы не бессмертны, и было бы обидно, если бы наши активы исчезли вместе с нами.

Внезапная потеря владельца активов может стать проблемой для получения парольной фразы, в этом документе мы будем продолжать использовать пример семейного круга и близких родственников, чтобы обозначить различные варианты развития событий.

Одним из ответов на эту проблему является то, что называется ключевым депонированием, которое позволяет третьей стороне «при определенных условиях» получить доступ к активам. Но что это за третья сторона? При каких условиях? И как мы можем обеспечить не только психологическую, но и техническую уверенность? Инструмент депонирования должен иметь возможность надежно гарантировать конфиденциальность приватных ключей.

Во-первых, мы можем зашифровать данные, это может быть закрытый ключ с алгоритмом безопасного шифрования (например, SHA256-512) и с помощью парольной фразы. Эта парольная фраза может быть разделена на доли и распределена нашим протоколом TFC SD.

5.3 Секретные Доли

В криптографии схемы разделения секрета – это метод распределения секрета среди группы участников, каждому из которых выделяется доля секрета. Секрет может быть восстановлен только тогда, когда доли будут объединены, отдельные доли сами по себе бесполезны.

Другими словами, в секретной схеме разделения долей есть один дилер и несколько игроков. Дилер раздает игрокам секрет, но только при выполнении определенных условий. Дилер дает каждому игроку долю таким образом, что любая группа t (для порога) или несколько игроков могли вместе восстановить секрет, но ни одна группа из менее чем t игроков не могла это сделать. Такая система называется (t, n)-пороговой схемой.

В схеме (t, n) можно доказать, что нет никакой разницы, имеет ли или не имеет злоумышленник действительные доли t-1 в своем распоряжении; до тех пор, пока у него меньше долей t, он может только догадаться о секретных долях, другого варианта быть не может.

Некоторые случаи использования совместного секретного использования: (см. Планы Безопасности)

- Хорошие пароли трудно запомнить. Умный пользователь может использовать секретную схему обмена для создания пароля и хранить одну часть в своей адресной книге, другую в своем банковском депозитном сейфе, третью часть у друга и т. д. Если однажды он забудет свой пароль, то сможет легко восстановить его. Конечно запись пароля непосредственно в адресную книгу будет представлять угрозу безопасности, поскольку он может быть украден злоумышленником. Если используется секретная схема обмена, злоумышленник должен украсть много частей ключа из разных мест.

Типичным применением этого сценария является безопасная реализация зашифрованной системы резервного копирования. Предполагая, что восстановление данных требуется редко, резервные копии данных могут быть зашифрованы открытым ключом, это может быть сделано автоматически и без взаимодействия с пользователем, в то время как закрытый ключ восстановления защищен с помощью секретного общего доступа.

- Дилер может отправить t частей, все из которых необходимы для восстановления первоначального секрета одним получателем, используя t различных каналов. Злоумышленник должен будет перехватить все t части, чтобы восстановить секрет, задача, которая может быть более трудной, чем перехват одного сообщения.

- Директор банка мог бы генерировать части кода для разблокировки хранилища банка и раздать их своим сотрудникам. Даже если директор в данный момент недоступен, хранилище может быть открыто, но только тогда, когда определенное количество сотрудников делают это вместе. В таком случае секретные схемы обмена позволяют трудоустраивать не полностью доверенных людей.

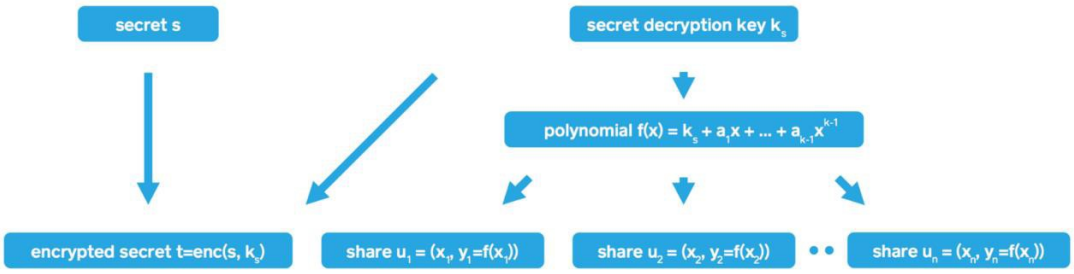


Рис. 8 : Принципы Секретных Долей

5.4 Правило Двух Человек

Это правило (правило двух человек) используется в особо чувствительных областях, таких как ядерные испытания ракет для предотвращения случайного или злоумышленного использования. В криптографии американцы используют фразу «целостность двух человек» (TPI), когда дело доходит до предотвращения доступа одного человека к криптографическим ключам (COMSEC).

Эта интересная концепция могла бы решить вопросы доверия и безопасности в области управления условного депонирования. Только при взаимодействии двух человек могут быть раскрыты данные о депозите, таким образом, мы можем защитить себя от мошенников.

Давайте разделим парольную фразу ключа escrow и дадим ее части группе доверенных людей, которых мы называем Семейный Круг (TFC)

Как разбить эту парольную фразу? Просто нужно раздать N частей между членами TFC, заставить их собраться вместе, чтобы использовать приватный ключ, а если один из них недоступен или отсутствует, то потребуются лишь части тех, чьи доли мы должны распределить в данный момент.

Двух точек достаточно для определения линии, трех для определения параболы, четырех для кубической фигуры и так далее. Если теперь мы хотим поделиться секретом, то скажем, значение 1234, между шестью лицами и тремя из них необходимы, чтобы найти секрет, мы будем случайным образом выбирать параболу среди тех, кто проходит через точку (0, 1234), и мы дадим координаты шести его точек этим шести лицам (см. рис.9).

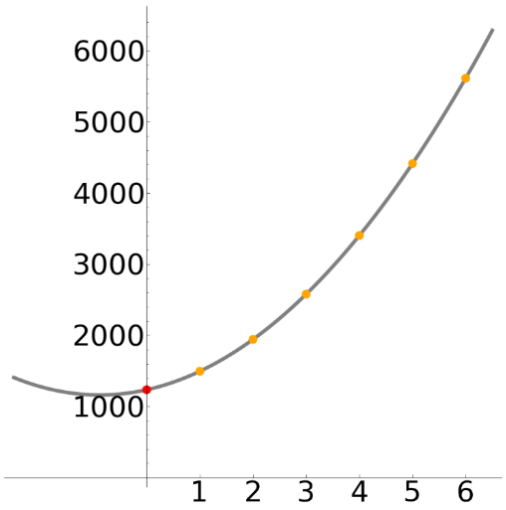


Рис.9 : Параболические Скрытые Пары (0, 1234)

Если бы только два из них, числа 2 и 4, пришли поделиться своими данными, они не смогли найти оригинальную параболу и, следовательно, значение секретной точки, когда x = 0 (см. рис.10).

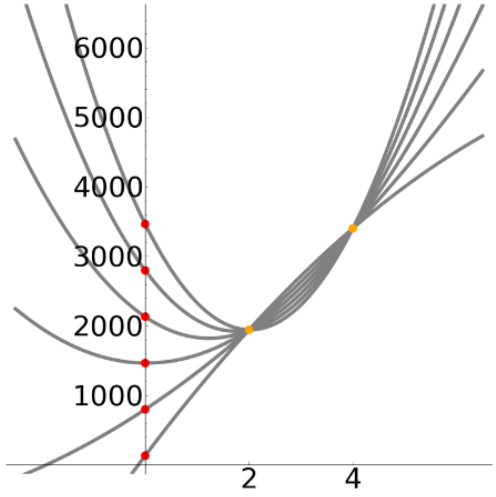


Рис.10 : Параболы проходящие через точки ° 2 и 4

Поэтому необходимо, чтобы третий человек согласился поделиться своими координатами, чтобы определить одну, только одну параболу и раскрыть секрет 1234 (см. рисунок 11).

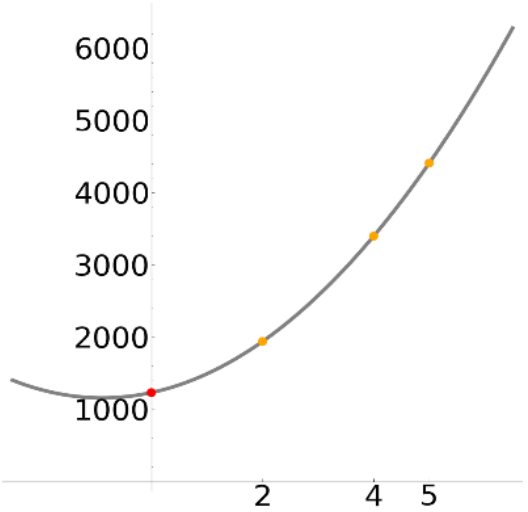


Рис.11 : Единственная парабола, проходящая через точки 2, 4 и 5

5.5 TFC Протокол Распределения Долей

Семейный круг в соответствии с принципами Safe Haven – это сообщество людей, принадлежащих к определенной группе, эта группа может включать в себя членов семьи, группу компаний, заинтересованных сторон или просто круг друзей. TFC SDP – это протокол, разработанный Safe Haven для того, чтобы создать круг доверия в нашей экосистеме.

Если рассмотреть методы, описанные выше, то можно заметить, что в системе есть наследодатель (человек, который хочет защитить свое наследство) и определенное количество наследников (его дети и валидатор). Наследодатель передает наследникам секрет, но только при выполнении определенных условий. Наследодатель передает каждому наследнику долю таким образом, что группа, состоящая только из определенного числа наследников, может вместе восстановить секрет; секрет не может быть восстановлен при меньшем количестве наследников. Такая система называется (t, n)-пороговой схемой.

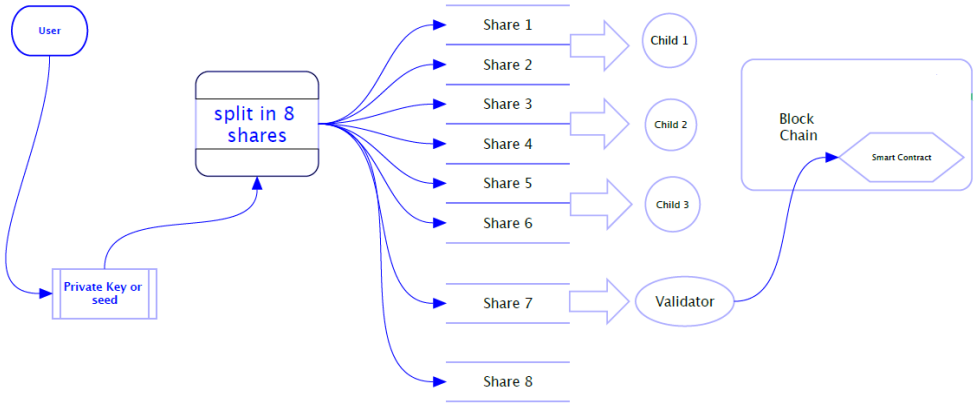


Рис.12 : TFC Протокол Распределения Долей

TFC Протокол основан на следующих правилах:

- Секрет разделен на доли (может быть максимум 1024 bit).
- Если вы хотите защитить секрет больше, чем на 1024 бит, должен быть применен гибридный метод, секрет должен быть зашифрован блочным шифром, а затем применяется только общий доступ к секретному ключу (допустимыми инструментами являются openssl и gpg).
- Уровень безопасности секрета обозначает верхнюю границу, а короткие секреты/ключи будут дополняться на определенное количество бит.
- Мы можем использовать 16-тизначные числа вместо символов ASCII для ввода-вывода, поэтому двоичные данные также будут защищены/разделены на доли.
- При разделении или объединении общего секрета протокол блокирует его виртуальный адрес в ОЗУ или из-за соображений конфиденциальности.
- С технической точки зрения, количество распределенных долей ограничено числом 99, мы ограничиваем их еще больше, до 15, в то же время у любого члена TFC может быть диапазон от 15 до 99.

- Валидатор (y) всегда имеет долю меньше чем n (другие участники / дети).
- Для создания доверия в экосистеме Safe Haven необходим как минимум 1 участник (n) и 1 валидатор (y).
- Имеется возможность добавить несколько валидаторов.

5.5.1 Распределение долей 1-й вариант: 1 ребенок и 1 валидатор

Формула разделения секрета на доли:

$$T=(y.n-1)+(X.n)$$

T = минимальное количество долей, необходимых для восстановления секрета.

Y = валидатор процесса, в данном случае это зарегистрированный член Альянса Safe Haven

X = держатели долей

$T = (y.n - 1) + (X.n)$

$T = (y.1 - 1) + (X.1)$

$T = (2.1 - 1) + (2.1)$

$T = (2 - 1) + (2)$

$T = 1 + 2$

$T = 3$ Минимум долей, необходимых для получения полного общего ключа.

Максимум долей – 3 (2 для детей и 2 (-1) для валидатора.

Например, мы берем секрет: "Моя общая парольная фраза" и получаем следующие 3 разные доли.

```
1-4894b94c42b425aea3dc379edb9fbf47acac1eff
2-ec6f4decf4f21704a1db1263971f4b05d5966e5f
3-5fb79bc83b2cf7e7a04fd38e6dff8e06e538afec
```

Поскольку доля представительства равна 100%, то есть возможен только один сценарий.

- 1 ребенок = (1 x 2) и (2 – 1) валидатор = 3 = T таким образом все правильно

5.5.2 Распределение долей 2-й вариант: 3 ребенка и 1 валидатор

Формула разделения секрета на доли:

$$T=(y.n-1)+(X.n)$$

T = порог минимального количества долей, необходимых для восстановления секрета.

Y = валидатор процесса, в данном случае это зарегистрированный член Альянса Safe Haven

X = держатели долей

$T = (y.n - 1) + (X.n)$

$T = (y.1 - 1) + (X.3)$

$T = (2.1 - 1) + (2.3)$

$T = (2 - 1) + (6)$

$T = 1 + 6$

$T = 7$ Минимум долей, необходимых для получения полного общего ключа.

Максимум долей – 8 (6 для детей и 2 (-1) валидатора).

Предположим, мы берем секрет: "Моя общая парольная фраза" и получаем 8 следующих долей.

```
1-4894b94c42b425aea3dc379edb9fbf47acac1eff
2-ec6f4decf4f21704a1db1263971f4b05d5966e5f
3-5fb79bc83b2cf7e7a04fd38e6dff8e06e538afec
4-71475064933c8d89f205f1ba5130482f4ad074ed
5-fe82d14bc9a2c2af21b9cb2b27f7baa4e819fc72
6-bf6c7907cde9d5aa66a366ef133b5c9260dde965
7-4f4e94991acbcead67cc871f04a4bfd1b8e98598
8-03d8b8a9d0e1d3b112c0ed60de3a9295639a7759
```

И нам понадобится 7 из 8, чтобы восстановить секрет. Так что, если мы возьмем доли:

- 3 ребенка = 3 x 2 = 6 < 7 ошибка
- 2 ребенка + 1 валидатор = 2 x 2 + 2 - 1 = 5 < T ошибка
- 3 ребенка + 1 валидатор = 3 x 2 + 2 - 1 = 7 = T ответ верный

5.5.3 Распределение долей 2-й вариант: 3 ребенка + страховка от ошибки и 1 валидатор

К формуле разделения секрета на доли добавляем (b=x-):

$$T = (y.n - 1) + (X.n) + (b = x)$$

T = порог минимального количества долей, необходимых для восстановления секрета.

Y = валидатор процесса, в данном случае это зарегистрированный член Альянса Safe Haven

X = держатели долей

$T = (y.n - 1) + (X.n)$ *+ (b=x)*

$T = (y.1 - 1) + (X.3)$ *+ (b=x)*

$T = (2.1 - 1) + (2.3)$ *+ (b = 2)*

$T = (2 - 1) + (6)$ *+ 2*

$T = 1 + 6$ *+ 2*

T = 7 Минимум долей, необходимых для получения полного общего ключа.

Максимум долей – 9 (6 для детей и 2 (-1) для валидатора + 2 (страховка от ошибки)

Допустим, мы берем секрет: "Моя общая парольная фраза" и получаем 9 следующих долей.

```
1-c6bde31ffc0b7474dcc576b0ab66cc3b09d7696a
2-aaae1588d6b7ddd80a14fac4fb68b7b7b19237f4
3-72061a3daf8af2585d139e37a095cddc35804e54
4-b158248b9dcf57d9c925287741532aa3ea5cc719
5-75516fa7eb1601e44863553254b0c99637392129
6-399bce6c6b29b04cfcf96e5292575f1670ff5b98
7-672c6a3398102ce986e62c46370861ffc6a0964c
8-1270dd67873bae0e21fba54a45e25622cbe7c7e1
9-084c327b0c9b727cd5d68210fe0000ce5da376af
```

Нам понадобится 7 из 9, чтобы восстановить секрет. Таким образом, если мы берем доли:

- 3 ребенка (или 2 + страховка от ошибки) = 3 x 2 = 6 < 7 ошибка
- 2 ребенка + 1 валидатор = 2 x 2 + 2-1 = 5 < T ошибка
- 3 ребенка (или 2 + страховка от ошибки) + 1 валидатор = 3 x2 + 2-1 = 7 = T ответ верный

5.5.4 Распределение долей 3-й вариант: 3 ребенка и 2 валидатора

Формула разделения секрета на доли:

$$T = (y.n - 1) + (X.n)$$

T = порог минимального количества долей, необходимых для восстановления секрета.

Y = валидатор процесса, в данном случае это зарегистрированный член Альянса Safe Haven

-1 = доля страховки

X = держатели долей

$T = (y.n - 1) + (X.n)$

$T = ((y.2) - 1) + (X.3)$

$T = ((2.2) - 1) + (3.3)$

$T = (4 - 1) + (9)$

$T = 12$

$T = 12$ Минимум долей, необходимых для получения полного общего ключа.

Максимум долей – 13 (9 для детей и 4 (-1) для валидатора).

Допустим, мы берем секрет: "Моя общая парольная фраза" и получаем 13 следующих долей.

```
01-b8d792946afa60b35d53609c03ae96320b78a0f6
02-92769c90836c393d06675d4e25201c3cc2ac0a85
03-9968d3d6e953590dc15363fc92acea7464eb2053
04-92a5e10da6dae5a4353ec755a5febaa76023c0fb
05-c0afccce07c511436f83db4c3a7aeaf5f69aa44f
06-a47453a4cd7b887f82df30ccdf864cc91467e738
07-3a95ee802152c02045cb1dc9aa2843291497a19c
08-82e043652371d0e9972520dade32660c6bc6d504
09-d0db492e80b8ebf2a5498867ebf91413864aa73f
10-a334c5ae2f2d00e6cb04dc97be9c1cf08c0e47e9
11-058f661fbe6bb9f94401c4b143888dbb9d58ed92
12-56f805b3d9a83ed57dcfed5014eb92a3c7ad287f
13-6803214791f5621cdb01a6291cc189e7a1b173b1
```

Нам понадобится 7 из 9, чтобы восстановить секрет. Таким образом, если мы берем доли:

- 3 ребенка = 3 x 3 = 9 < 12 ошибка
- 3 ребенка + 1 валидатор = 3 x 3 + 2 - 1 = 10 < T ошибка
- 3 ребенка + 2 валидатора = 3 x 3 + 4 - 1 = 12 = T ответ верный

5.6 TFC Безошибочная Доля

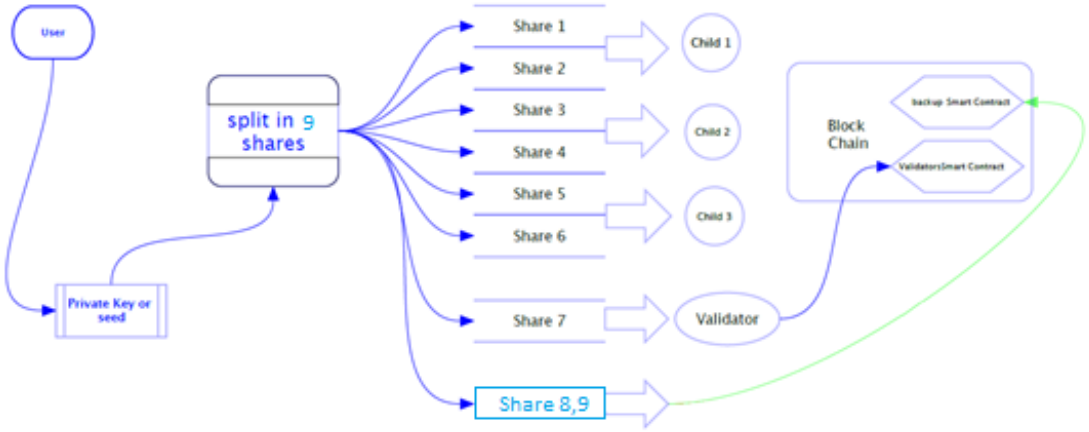


Рис. 13 : TFC Безошибочная Доля

TFC SD Безошибочный Протокол:

- Остальные доли будут использоваться как своего рода «безошибочные» доли.
- Это может быть полезно в том случае, если один из n (дольщиков/детей) потерял свою долю, начинает действовать не законно или умирает.
- Наш протокол предоставляет отдельный «возобновляемый» смарт-контракт на блокчейне с прописанными в нем различными условиями.
- Безошибочные доли не могут быть переданы ни при каких обстоятельствах ни кому из n (участников/детей), так как это поставит под угрозу условие наследодателя (родителя), а в случае 2 (3 детей + 1 валидатор) дети не могут восстановить секретную долю без долей валидаторов (через смарт контракт на блокчейн), это можно осуществить только, если им были переданы копии долей.
- Единственный вариант, когда безошибочная доля не нужна, – это когда есть 100% согласие заинтересованных сторон, например, 1-й вариант использования (1 ребенок + 1 валидатор).

5.7 Процесс Проверки Долей Валидаторами

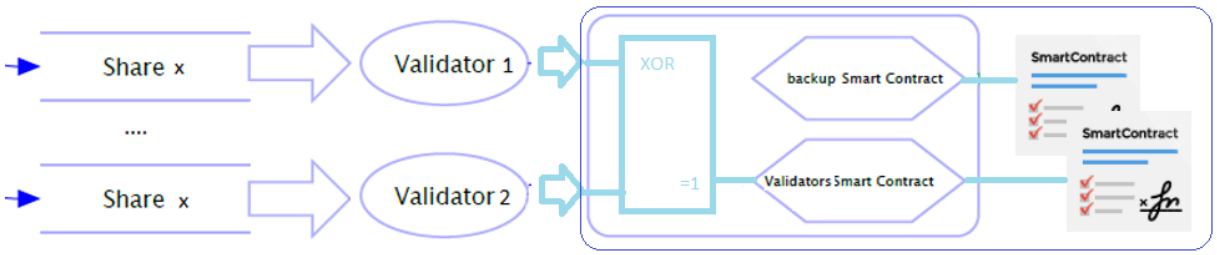


Рис. 14 : Процесс Проверки Долей

- В процесс совместного использования валидаторов включается пул валидаторов из юридических лиц, которые являются членами нашей сети Trust Alliance.
- Валидатор не хранит, не владеет или не видит долей, предназначенных для отправки в блокчейн, их действия абсолютно прозрачны.
- Они распределяют доли в пользу n (участников/детей/владельцев) в официальном порядке путем передачи n правовых сертификатов и проверки транзакций на блокчейн.
- Доля валидатора на самом деле является долей человека, который инициировал процесс наследства; валидатор защищает его в блокчейне, охраняет его права на целую секретную долю таким образом, что активы принадлежали только наследодателю до конца жизни.
- Валидатор(валидаторы) является/являются единственным(единственными), кто может получить долю, ранее отправленную на блокчейн. При соблюдении следующих условий:
    - Необходимо наличие общего количества долей n (участников/детей/заинтересованных сторон), в другом случае и если это необходимо, безопасная доля может быть извлечена валидатором, когда выполнены условия возобновляемого смарт-контракта.
    - В случае, если инициатор (родитель) умирает, валидатор должен проверить медицинское заключение для того, чтобы начать процесс извлечения доли, хранящейся в блокчейне.
- При необходимости доля инициатора/родителя также может быть передана другому законному лицу.

5.8 Возможность Многоуровневой Проверки

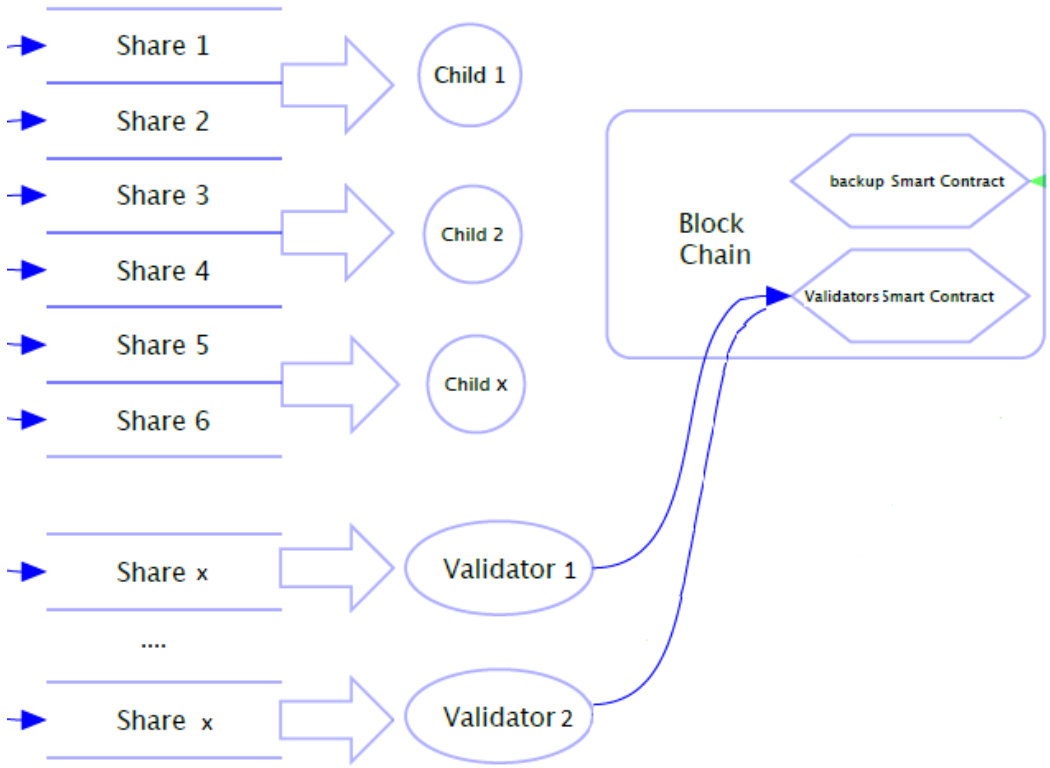


Рис. 15 : Система Многоуровневой Проверки

TFC SD Возможность Многоуровневой Проверки:

- Никто не бессмертен, как и юридические лица, участвующие в нашей программе Альянса. Поэтому мы предоставляем возможность создать сеть доверия, содержащую более одного валидатора.
- Когда вы выбираете несколько валидаторов для участия, мы запускаем резервный смарт-контракт в блокчейне, который содержит необходимые доли n (участников/детей) -1, которые могут быть использованы вторым валидатором.
- Делая это, мы создаем систему безопасности, которая полностью вытекает из распределения и проверки.

6 Сеть Trust Alliance Safe Haven

Сеть Trust Alliance Safe Haven - это группа юридических лиц, которые были проверены Safe Haven для того, чтобы выполнить все необходимые шаги для достижения нашей цели, они защищают ваши активы, доли родственников, заинтересованных сторон и ваше наследство.

Если вы являетесь юридическим лицом, желающим присоединиться к нашему альянсу, отправьте запрос info@safehaven.io и мы свяжемся с вами, как только разработаем нашу юридическую платформу. Очень скоро мы запустим специализированный портал Trust Alliance, чтобы ответить на все юридические вопросы. Как только наш портал будет запущен, юридические лица смогут подписаться, у них будут запрошены юридические сертификационные документы, которые помогут процессу проверки. Участникам будет предложено внести ежегодную плату за получение подписки на наши услуги. Токены будут использоваться в качестве топлива для развертывания смарт-контрактов на блокчейне.

Сейчас мы анализируем, какие именно юридические лица могут быть членами нашего Альянса. Нам нужны доверительные субъекты в нашем Круге доверия.

7 Планы Безопасности Safe Haven

1. TFC План Семейного Круга

   План семейного круга предназначен для тех, кто хочет чтобы их родственники после ухода из жизни наследодателя могли незамедлительно получить доступ к активам, которые приобрел родитель. Возможности почти бесконечны, доли можно разделить посредством разных способов, безопасно и надежно сохранив секретные доли. Тот факт, что мы добавляем валидаторы к нашем процессу распределения, делает этот процесс прозрачным законным и надежным со всех сторон. Мы добавляем удивительный мир "блокчейн" в наш процесс, который делает доли децентрализованными. Децентрализованный валидатор базы данных (интеллектуальное сопоставление контрактов) добавляет дополнительную функцию безопасности в сочетании с современным, но еще упрощенным, секретным протоколом обмена.

2. BCP Бизнес Комьюнити План

   План Бизнес Комьюнити (BCP) очень похож на план TFC, основное отличие состоит в том, что мы говорим о заинтересованных сторонах, а не о детях, и что процесс проверки отличается с точки зрения разблокировки долей. В BCP валидатор не нуждается в медицинском заключении для получения через наш протокол недостающей доли, а нуждается в проверочных актах, подготовленных им самим. Этот план в настоящее время разрабатывается внутри нашей компании и будет доступен для использования с момента выхода Trust Alliance 3ortal в онлайн. BCP план может быть удобен при использовании мульти-SIG кошельков, работе на биржах или просто для хранения импортируемых паролей / ключевых фраз.

3. Круг Инвесторов

Круг инвесторов предназначен для тех, кто хочет создать фонд среди друзей, членов семьи или деловых партнеров. Допустим, что 5 друзей хотят инвестировать в криптовалюты, и каждый покупает на $1000. Какие у них возможности? Создать мульти-SIG кошелек (со всеми их недостатками, которые были обнаружены в последнее время). Даже когда такой кошелек полностью безопасен, вам всегда понадобится доверие внутри группы... Хорошо, но как мы будем справляться с этим? Просто! С помощью протокола распределения долей Safe Haven. Вы шифруете закрытый ключ, и мы делим парольную фразу на равное количество долей, заинтересованные стороны получат одинаковое количество долей. Если мы рассмотрим формулу без страховочного механизма, то получается, что T = (y.n − 1) + (X. n) , T = (2 -1) + (2.5) = 1 + 10 = 11 долей распределены, где 1 доля будет заморожена на блокчейне с помощью валидатора (юридического лица). Условия, чтобы освободить эту долю, могут быть любыми, от ценовых порогов до контрольных точек со 100% консенсусом. Таким образом, возможности безграничны.

4. Хранение Safe Haven

Хорошие пароли трудно запомнить, их нельзя отправлять в сети кому бы то ни было, даже вашим родственникам. Эти пароли могут быть от чего угодно, от Facebook, Gmail и любых других важных аккаунтов. Если вы хотите быть уверены, что ваше цифровое наследство не умрет вместе с вами, что ваши родственники смогут получить доступ к этим счетам, даже когда вас больше не станет, вы можете хранить их с помощью Safe Haven на блокчейне, используя один из наших протоколов распределения долей.

8 Заключение

Инвестирование в криптовалюту и Биткоин сегодня занимает много времени и является очень сложной задачей, с другой стороны оно может принести огромную прибыль на протяжении многих лет. Обеспечение этих активов и возможность защитить их от любого чужого воздействия – это то, чем постоянно озабочены все трейдеры и долгосрочные инвесторы. Мы все хотим быть финансово независимыми и строить безопасное будущее для себя и наших родственников. Именно поэтому мы будем развивать нашу децентрализованную платформу и предоставлять наши решения по всему миру. Для компания Safe Haven нет разницы в обеспечении безопасности и обычном хранении ваших цифровых ключей. Наше решение обеспечит спокойствие для инвестора и их родственников. Мы надеемся, что вы уверены в нашей платформе, и что мы можем приветствовать вас в качестве одного из наших инвесторов!

9 Рынок

Криптовалюты – это цифровые активы, которые используют криптографию, методы шифрования для обеспечения безопасности. Криптовалюты в основном используются для покупки и продажи товаров и услуг, хотя некоторые новые криптовалюты также функционируют, чтобы предоставить новый набор прав или обязанностей для своих владельцев. Они не имеют никакой внутренней ценности; в том плане, что они не имеют обеспечения в форме другого товара, например, такого как золото. В отличие от традиционных валют они не выдаются центральным органом и не считаются законным платежным средством.

На данный момент использование криптовалют во многом ограничивается "ранними адептами". Во всем мире есть около 10 миллионов владелцев Биткойнов, примерно половина из которых владеет Биткойном исключительно в инвестиционных целях. Если объективно посмотреть на вещи, то криптовалюты не нужны, потому что валюты, поддерживаемые государствами, на сегодняшний день функционируют лучше. Для большинства владельцев преимущества криптовалют являются теоретическими. Поэтому основное внедрение произойдет только тогда, когда будет существовать значительная и ощутимая выгода от использования криптовалют. Итак, каковы преимущества их использования?

Криптовалютные Биржи

Криптовалютные биржи – это сайты, на которых физические лица могут покупать, продавать или обменивать криптовалюты на другую цифровую или традиционную валюту. Биржи могут конвертировать криптовалюты в основные государственные валюты, а также могут конвертировать криптовалюты в другие криптовалюты. На некоторых из крупнейших бирж, включая Poloniex, Kraken и GDAX, можно торговать более чем на 100 миллионов долларов (в эквиваленте) в день. Почти каждый обмен подпадает под действие правительственных правил по борьбе с отмыванием денег, и клиенты должны предоставить удостоверение личности при открытии счета.

Вместо бирж люди иногда используют peer-to-peer транзакции через сайты, такие как LocalBitcoins, которые позволяют трейдерам избегать раскрытия личной информации. Посредством peer-to-peer транзакций пользователи торгуют криптовалютами при помощи программного обеспечения и без участия какого-либо другого посредника.

Криптовалютные Кошельки

Криптовалютные кошельки необходимы пользователям для отправки и получения цифровой валюты и мониторинга их баланса. Кошельки могут быть как аппаратными, так и программными, хотя аппаратные кошельки считаются более безопасными. Например, аппаратный кошелек выглядит как USB-флешка и подключается к USB-порту компьютера. При операциях и остатке на счете Биткоин на блокчейн, приватный ключ, используемый для подписи транзакции, сохраняется в регистр кошелька. Когда вы пытаетесь создать новую транзакцию, ваш компьютер просит кошелек подписать ее, а затем передает ее на блокчейн. Поскольку закрытый ключ никогда не покидает аппаратный кошелек, Ваши Биткойны безопасны, даже если ваш компьютер взломан. Тем не менее, если не сделать резервное копирование, потеря Кошелька приведет к потере активов владельца. В отличие от этого программные кошельки, такие как кошелек Coinbase, являются виртуальными. При таком варианте хранения владелец кошелька передает свои активы поставщику кошелька и поэтому рискует, так как активы могут быть доступны в сети.

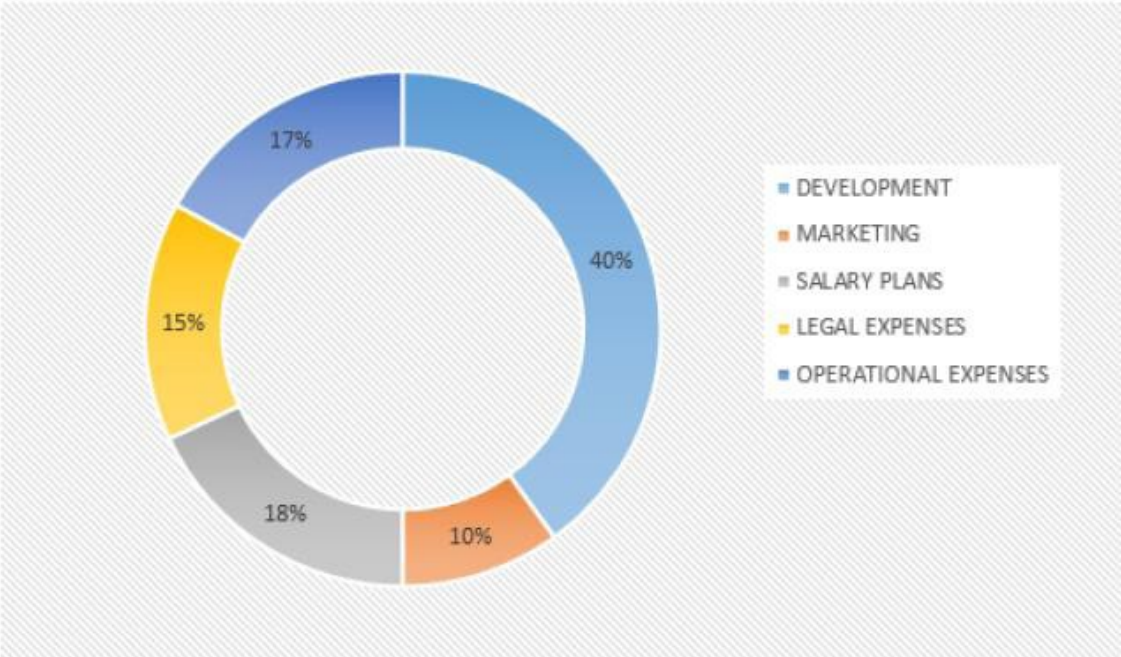
При все большем количестве людей и все большем количестве денег, поступающих на рынок криптовалют, все больше людей вынуждены открывать биржи или кошельки и получать приватные ключи. Safe Haven создает идеальное решение. В принципе, каждый человек, который открывает кошелек и покупает криптовалюту, может быть клиентом Safe Haven. Наш потенциал расти на этом рынке огромен! Мы уверены в том, что Safe Haven поможет изменить ситуацию.

10 Токен

Токен SHA – это токен ERC2, созданный на блокчейне Ethereum. Стандартный ERC20 токен был представлен на блокчейне Ethereum для того, чтобы позволить разработчикам создавать децентрализованные приложения (Dapps) для работы с токенами, без необходимости заново изобретать колесо каждый раз, когда внедряется новая система. Поэтому с помощью ERC20 любой человек со своей идеей может создать продукт на блокчейне, без необходимости проектирования и внедрения новой платформы. С помощью ERC20 мы можем определить общий набор правил, применимых для Ethereum, которым мы следуем при разработке токена SHA. Мы можем заранее знать, как токен будет вести себя на основе этого стандарта. Токен SHA разработан, чтобы реанимировать рынок, который мы описали в этом техническом документе. Первый этап разработки касается количества токенов, которые мы создадим. Токен SHA будет использоваться в качестве топлива в экосистеме.

11 Распределение Фондов

Разработка	40%
Маркетинг	10%
Зарплаты	18%
Юридические Издержки	15%
Операционные Издержки	17%



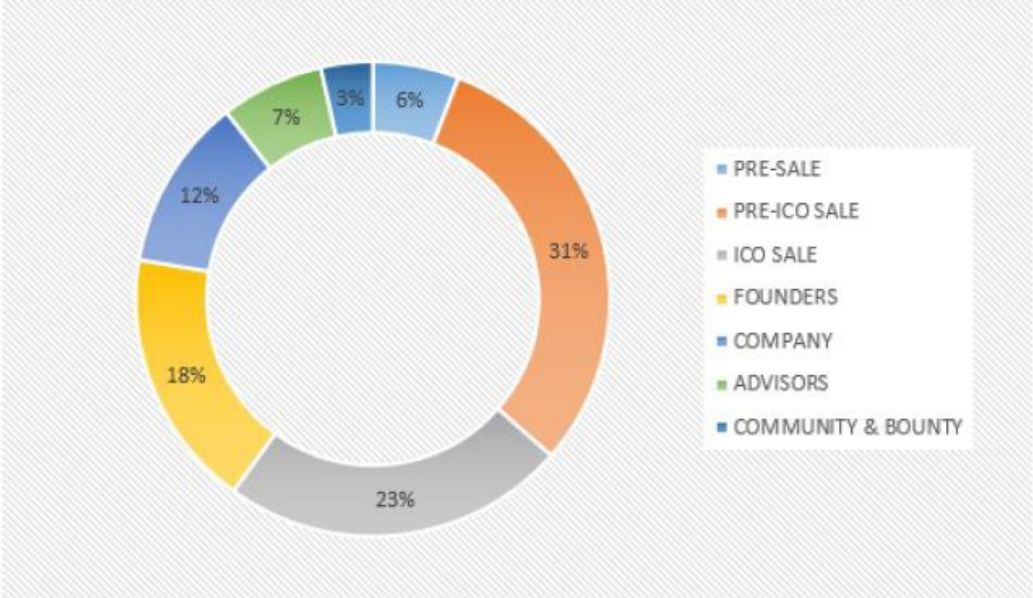
Мы намерены выделить большую часть собранных средств на дальнейшее развития платформы. Поэтому 40% средств пойдет на эту инициативу. 10% средств будет выделено для разработки различных маркетинговых мероприятий, включая баунти кампании и кампании с подписями. 15% будет выделено на юридические вопросы, например, такие как листинг на биржи. 17% - на операционные расходы, 18% - на зарплаты.

12 Параметры ICO + Распределение Токенов

Тикер: SHA
Общий объем: 85,000,000
Токен на блокчейне Ethereum (ERC20)
Дата начала ICO: см. https://ico.safehaven.io
Цена для ранних инвесторов: 2500 SHA = 1ETH
Цена на PRE-ICO: 2000 SHA = 1 ETH
Цена на ICO: 1500 SHA= 1 ETH
Минимальная капитализация: 3000 ETH
Максимальная капитализация: 25.000.000 $

Распределение Токенов

PRE-SALE:	2500 SHA/ETH TOTAL (5,000,000 SHA)	6%
PRE-ICO SALE:	2000 SHA/ETH TOTAL (26,000,000 SHA)	31%
ICO SALE:	1500 SHA/ETH TOTAL (20,000,000 SHA)	23%
УЧРЕДИТЕЛИ:	15,000,000 SHA	18%
КОМПАНИЯ:	10,000,000 SHA (Locked for 12 months)	12%
СОВЕТНИКИ:	6,000,000 SHA	7%
КОМЬЮНИТИ И БАУНТИ:	3,000,000 SHA	3%



13 Дорожная Карта