Протокол Хейвен
Частное децентрализованное управление финансами

Базовый протокол v3.0

Здесь будут рассмотрены основные функции протокола Хейвен (Haven).
Функции второго уровня будут разобраны отдельно на конкретных примерах.

Вступление

Биткойн положил начало электронной одноранговой валюты.
Это первая цифровая валюта, которая успешно ввела распределенный реестр транзакций, основанный на криптографическом доказательстве, а не на доверии.

С осознанием того, что электронные кошельки и транзакции многих крипто-валют недостаточно защищены, спрос на частные транзакции и анонимные криптовалюты возрос.
Haven построен на платформе Monero, которая широко известна как лидер в области защитных технологий.
Таким образом, Haven имеет все функции конфиденциальности Monero, включая кольцевые подписи и Bulletproofs (Булетпруфы).
Протокол Haven также предоставляет частные, анонимные, синтетические валюты и товары (xAsset), за счет «перевода» в базовую валюту Haven - XHV.
Haven также расширяет систему взаимозаменяемости Monero, позволяя обменивать несколько типов активов на основе их денежной стоимости, создавая первый в своем роде, полностью частный набор синтетических валют и активов.

Добро пожаловать в Haven - частное децентрализованное управление финансами.

История проекта

Концепция Haven появилась в ходе работы двух разработчиков в начале 2018 года. Первая попытка достигла стадии общедоступной тестовой сети с последующим выявлением слабых мест, неопределенным перерывом в разработке, и, как следствие, отсутствием прогресса, что поставило под сомнение будущее проекта.
В конце января 2019 года настоящий состав разработчиков протокола Haven взял проект в свои руки с целью его завершения, с предоставлением офшорного хранилища и сопутствующей системой поддержки.
А также создания вспомогательной инфраструктуры для массового использования этой системы на быстрорастущем рынке криптовалюты.

Протокол Haven был успешно запущен 20 июля 2020 года, представив на рынок свою первую частную валюту xUSD.

Протокол Хейвен

Обязательство: 1 xUSD всегда можно обменять на XHV на сумму 1 доллар.

i. Концепция

Haven - это неотслеживаемая криптовалюта, сочетающая стандартные рыночные цены с привязкой к реальной системе хранения активов.
Это возможно с помощью процесса "чеканки и перевода" в рамках единой цепочки блоков (блок-чейна).
Так, пользователи могут перевести Haven (XHV) в эквивалентную сумму долларов Haven (xUSD) в долларах США.
Или, для восстановления волатильности, пользователь может также перевести xUSD за 1 доллар США равный XHV.

Со временем, другие основные фиатные валюты, как GBP (фунт стерлингов), EUR (евро), CNY (китайский юань), серебро, золото и другие биржевые товары, такие как нефть, будут добавлены в экосистему Haven чтобы пользователи могли выбрать нужную привязку цены к определенному ценовому ориентиру.

ii. Оффшорный процесс - «чеканки и перевода»

Протокол Haven использует систему «чеканки и перевода» для поддержания соотношения стоимости и привязки активов.
Используя синтетический доллар США (xUSD) в качестве примера, давайте рассмотрим как это работает: Боб решает поместить 200 своих Haven (XHV) в оффшорное хранилище.

Когда пользователь помещает XHV в оффшорное хранилище, он "переводит'' монеты XHV и "чеканит" текущую стоимость этих XHV равную стоимости xUSD.

Оффшорное хранилище определяет текущую рыночную стоимость Haven (в xUSD) на основе средне-взвешенного объема по поддерживаемым биржам.
Это определяется с помощью системы ценообразования (механизма для получения текущих данных и передачи их в цепочку блоков). Таким образом получается ценовая информация для всей экосистемы Haven и создаются ценовые записи.

Если текущая стоимость Haven составляет 1 доллар США, оффшорное хранилище переведет 200 XHV Боба путем создания специальной транзакции, в которой 200 XHV переводятся в xUSD, а общее количество XHV уменьшается.

Если рыночная цена XHV вырастет до 2 долларов США, и Боб решит получить доступ к своему оффшорному хранилищу, ему вернут 100 XHV (100 * 2 доллара = 200 долларов США по исходной стоимости).

Если же цена Haven упадет до 0.50 доллара, то Боб получит 400 XHV (400 * 0.50 доллара = 200 долларов по исходной стоимости).
Таким образом, процесс "перевода и чеканки", корректирует базу активов динамически.

Это создает интересные перспективы отличающие Haven от другой криптовалюты.
Чтобы полностью понять концепцию протокола Haven важно рассмотреть все сценарии .

iii. Как же работает оффшоринг?

Протокол Haven позволяет осуществлять оффшорные транзакции в хранилище Haven с применением модели «цветной монеты».
Это первая рабочая реализация цветных монет по протоколу Cryptonote (Криптоноут).

Концепция цветных монет хорошо известна и работает в сети Биткойн.

Здесь дается её подробное описание от 2013 года:
https://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin

Однако цветные монеты на крипто-банкноте не могут работать так же, как Биткойн, и вся концепция должна быть переработана и переосмыслена.

Спасибо Нейту Элдриджу за это четкое описание различий между реализацией с использованием Биткойна и Monero:

«Биткойн осуществляет взаимно однозначное соответствие между входами и выходами транзакций. Предположим, существует транзакция X с выходом X1, которая отправляет 1 сатоши на адрес Алисы A, и все согласны с тем, что выход X1 окрашен так, что он дает право собственности на Chevy Nova 1977 года Алисы. Если Алиса решает передать машину Бобу, она создает новую транзакцию Y, вход которой указывает на X1, а единственный выход Y1 отправляет 1 сатоши на адрес Боба B. Теперь Боб может доказать, поставив подпись, соответствующую его адресу B, что он является законным владельцем автомобиля.

Если Мэллори попытается потребовать автомобиль, создав другую транзакцию с вводом X1, ничего не выйдет, потому что она не может подписать эту транзакцию секретным ключом Алисы. Если Алиса попытается передать машину кому-то другому, создав вторую правильно подписанную транзакцию Z с входом X1 - попытка будет не эффективной, поскольку в цепи блоков ему уже предшествует другая транзакция X1.

При кольцевых подписях это соответствие нарушено.
При создании транзакции, помимо одного выхода (предыдущей транзакции), вы можете указать множество других.

Вы создаете подпись, которая доказывает, что вы имеете право использовать один из перечисленных вами выходов, но не дает никакой информации о том, какой именно.
Однако привязанный алгоритм гарантирует, что любая будущая попытка снова использовать этот вывод будет замечена и отклонена.

В приведенном выше сценарии, если Алиса использует кольцевую подпись для своей транзакции Y, включая не только X1, но и другой выход Z1, то её подпись не будет доказывать, что она имеет право на X1 (и, следовательно, является законным владельцем автомобиля и может отдать это); это только доказывает, что она имеет право на X1 или Z1.

Кроме того, Мэллори может создать транзакцию M, которая будет включать X1 и другой выход K1, который она имеет право использовать .
Поскольку у нее есть секретный ключ, соответствующий K1, она может подписать транзакцию M, но не будет ясно, относится ли она к X1 (которая передает право собственности автомобилем) или K1 (которая не дает).

Выше описаный способ реализации цветных монет в сети Биткойн указывает на то, что эта модель не работает, когда и X1, и Z1 все еще существуют в цепи блоков после начальной транзакции.

Однако Haven работает несколько иначе.
Здесь нет Алисы, нет Мэллори. Есть только Боб.

Когда Боб конвертирует из XHV в xUSD, он отправляет транзакцию с двумя цветами: X (XHV) и Z (xUSD). Транзакция принимает за вход монеты только первого цвета X, а за выход, как X, так и второй цвет - Z.

Каждая транзакция в сети Haven (Хейвен) имеет два значения для каждого пункта назначения (#X,#Z), и для всех транзакций только одно из этих значений может быть ненулевым для каждого пункта назначения.

Поэтому, когда Боб конвертирует свои 200 XHV по цене 1.00$ за XHV, он отправляет транзакцию с входными данными (200,0) и конечной ценностью (0,200), что дает на выходе 200 xUSD и 0 XHV.

Если цена XHV вырастет до 2 долларов за XHV, то при обратном преобразовании в XHV будет отправлена транзакция с входными данными (0,200), и конечной ценностью (100,0), что даст на выходе 100 XHV и 0 xUSD.

Таким образом, входные данные для транзакций и UTXO (Неизрасходованный входящий остаток транзакций) постоянно и эффективно корректируются атомарно, в реальном времени во время процесса транзакции, и выходы создаются аналогично.

Все это замечательно, однако Haven является производным Monero и имеет все его функции безопасности и анонимности... и Monero построен на условии, что для любой данной транзакции разница между входами и выходами равна нулю.
Любая транзакция, которая не удовлетворяет этому требованию, всегда будет неудачной.

В случае с Haven, это фундаментальное условие Monero не может быть верным.
Более того, для любого и каждого обмена между XHV и xUSD, где цена XHV не равна точно $ 1.00 это правило полностью нарушается.
Входы и выходы не будут равны, также как и суммы обязательств по Ca и Cb; и, следовательно, src/ringct/rctSigs.cppverRctSemanticsSimple() не пройдут проверку Monero для:

$$\sum_j C_j'^a - \sum_t C_t^b = 0$$

Далее будет представлена концепция «анализа эффективности» в системе Haven.

Выражаем благодарность исследовательской лаборатории Monero за их статью о связующих кольцевых подписях, и о борьбе с подделками ключей [Брэндон Гуделл, Саранг Нётер и Артур Блю] https://eprint.iacr.org/2019/654.pdf
Эта статья была использована при проведении «анализа эффективности» системы Haven.

В черновике «статьи» авторы предложили использовать «игровую» модель, в которой они создают цветную валюту с фиксированной привязкой между двумя цветами: долларами и пенни с обменным курсом 100: 1, и показывают, как это можно сделать с помощью CLSAG.

Процесс выглядит следующим образом:

1. Определить обменный курс, определив константу ξ и некоторые константы γC, γD на 1, 2,. . . , 2 ξ-1, (в этом примере γC = 100 и γD = 1).
2. Изменить структуру обязательств так, чтобы каждое обязательство стало парой обязательств C и D с соответствующими цветами.
3. Создать доказательство охватывающее значения как C, так и D. Здесь C и D играют роль точек Zj, а P - дополнительные данные, необходимые для протокола транзакции.
4. Мы знаем, что простой ключ транзакции действителен, если выполняются следующие условия:

а. каждый вводный компонент (Xi, Ci, Di, Pi) ∈ Q имеет допустимое доказательство диапазона Pi, поэтому Ver (Pi) = 1; а также

б. каждое доказательство выходного диапазона P 0 k действительно, поэтому Ver (P 0 k) = 1; а также

с. для модифицированного биржевого круга pk = X_1 X_2 ... Xn Z_1 Z_2 ... Zn подпись σ проходит проверку 2-CLSAG, Verify (m, pk, σ) = 1

Таким образом, транзакция подписывается не с обязательством равенства к нулю, а с обязательством к разнице, которая определяется количеством «монет/токенов», создаваемых этой транзакцией на входе и выходе. Если бы

пользователь обменивал 1 доллар США на 100 пенни, разница составила бы 99 - количество отчеканенных новых монет.

Эта модель работает, потому что для того, чтобы отправитель смог подписать транзакцию, используя эту разницу, он ДОЛЖЕН знать как количество монет, используемых на вводе (которое может знать только владелец секретного ключа этой транзакции), как и использовать правильный обменный курс 100:1, с содержанием всех булетпруфов со значениями двух возможных цветов.

Только так можно правильно подписать транзакцию, используя разницу между входами и выходами чтобы она была подтверждена.

Вышеупомянутая модель имеет один серьезный недостаток при применении "чеканки и перевода" системы Haven. Это - обязательный фиксированный обменный курс. Курс должен быть фиксированным и известным обеим сторонам транзакции, а также всем без исключения проверяющим эту транзакции.

Эта модель не будет работать, потому что по определению, чтобы привязать волатильный актив к стабильному, необходимо изменить обменный курс.

iv. Анализ эффективности

Чтобы указанная выше модель цветных монет работала с переменным курсом обмена, необходимо выполнение следующих условий:

1. Способ сбора согласованной и неизменной ценовой информации, чтобы в любой момент времени в обменной транзакции использовалась цена, которая может быть подтверждена.

2. Способ преобразования входов в выходы на основе этой цены.

3. Способ подтверждения, что отправитель транзакции удовлетворяет тем же требованиям, что и любая другая транзакция с криптовалютой, а именно, что он знает секретный ключ к используемым входам и, следовательно, может конвертировать, используя обменный курс, и подписывать транзакцию с правильная разницей.

4. Способ подтверждения того, что цена действительно согласована с биржей, без раскрытия каких-либо сумм проверяющим.

Подробная информация о ценах получается из системы ценообразования в реальном времени (т.е. Оракула ценообразования), а ценовая запись создается при подготовке к новому блоку.

Записи о ценах содержат обменные курсы (по отношению к XHV) для каждой привязки xAsset на момент создания блока.

Информация о ценах обновляется с интервалом в 30 секунд и предоставляется управляющей программе Haven по запросу.
Записи о ценах внедряются в блок-чейн в каждый заголовок блока майнером, решающим этот конкретный блок.

Включая эту информацию в каждый блок, протокол гарантирует, что стоимость транзакции не может быть изменена или изменена каким-либо другим образом - цепочка блоков гарантирует, что информация о ценах неизменна.

Если несколько блоков успешно созданы в течение 30 секунд текущей ценовой записи, одна и та же запись будет включена в несколько блоков.

Ценовая запись содержит следующие коэффициенты конверсии (все по XHV), а также место для будущих добавлений и подписи оракула, предоставляющего данные.
Примерная ценовая запись выглядит так:


```
{
   "pr":{
      "PricingRecordPK":923646,
      "xAG":52311967606,
      "xAU":736146731,
      "xAUD":1970789081906,
      "xBTC":125577435,
      "xCAD":0,
      "xCHF":1298984107110,
      "xCNY":0,
      "xEUR":1209035163606,
      "xGBP":1082483149674,
      "xJPY":151562100074207,
      "xNOK":0,
      "xNZD":0,
      "xUSD":1429685290000,
      "unused1":1424100000000,
      "unused2":1424000000000,
      "unused3":1398100000000,

 "signature":"9dcc4cd4f862dd5731f9142614fd4fd6c7f795d3c1b07923092abfb25e70a9941498134022ea1958ce07b704930c6891204fc7
ce0366742529c559b6c15c72b2",
      "timestamp":1598523249
   }
}
```


Пример ценовой записи: копия

2/ В приведенном выше примере с [Бобом], система Haven использует пары обязательств, а не значения отдельных обязательств.

Этот же метод используется в примере модели исследовательских лабораторий Monero.

3/ Транзакции в протоколе Haven подписываются с использованием CLSAG и парных булетпруфов, как описано выше.
Однако, при подписи не используется разница, а первоначальное обязательство о значении нулю.
Наша цель - нулевая разница в **значении**.

4/ Здесь всё немного сложнее.
Чтобы понять, как Haven подтверждает или отклоняет транзакции с использованием доказательства ценности, требуется некоторое понимание алгоритмов открытого ключа, а также того, как Cryptonote использует операции и точки эллиптической кривой для проверки входных и выходных сумм.

Каждая транзакция проходит через функцию *verRctSemanticsSimple()*, которая суммирует все входы и выходы транзакции, чтобы проверить равенство результатов.
Хотя значения на этом этапе полностью зашифрованы и представлены точками эллиптической кривой ['EC'], а не действительными числами, эти суммы по-прежнему работают из-за свойств модульной арифметики и особого способа выбора/создания точек EC Monero.

Вкратце, хотя числа зашифрованы, они по-прежнему обладают определенными свойствами - различия между ними (в пространстве EC) по-прежнему действительны, поэтому нулевая разница по-прежнему будет нулевой разницей, поскольку обязательства являются аддитивными.

Другими словами, если бы у нас была транзакция с входами, содержащими суммы a_1, ..., a^j, и выходами с суммами b_1, ..., b, то наблюдатель с полным основанием ожидал бы, что:

$$\sum_j a_j - \sum_k b_k = 0$$

Для протокола Haven (Хейвен) это будет работать при переводе XHV и xUSD, но для бирж - нет.

Итак, повторно используя некоторые обозначения из вышеприведенного, давайте определим константы γC, γD как обменный курс для одной транзакции.
Этот обменный курс предоставляется нашим оракулом ценообразования.
А теперь, с обязательствами в паре в нашем диапазоне доказательств существования (C, D) соответственно.
Чтобы доказать равенство стоимости, требуется, чтобы сумма стоимости входов была равна сумме стоимости выходов.

Наша проверка теперь выглядит так:

$$\lambda C \left(\sum_i C_i - f_c G - \sum_k C_k^{'} \right) = 1/\lambda D \left(\sum_i D_i - f_D G' - \sum_k D_k^{'} \right)$$

Где λC, λD означают, что значения в скобках суммируются на основе их соответствующих обменных курсов.
(C, D) обозначают обязательства при входе, (C', D') обозначают обязательства по выводу.

A, ƒxG - уплаченная комиссия.

v. Система ценообразования

Для получения реальных данных в блок-чейнах используется конструкция, называемая «оракул».

«Оракул цепочки блоков - это сторонний источник информации, единственная функция которого - предоставление данных в цепочки блоков».

Источник:
https://www.mycryptopedia.com/blockchain-oracles-explained/

В первой версии Haven (Хейвен), и нескольких последующих разработках создание безопасного, точного и высокопроизводительного оракула считалось ключом к успеху протокола.
Однако с момента создания, и успешного примениения таких сервисов, как Chainlink, предназначенных исключительно для выполнения функций оракула в качестве независимого источника данных, стало ясно, что встроенный оракул для системы Haven (Хейвен) не только не требуется, но и не желателен.
Так как это повысит централизацию самой важной части уравнения конверсии - ценообразования.

В связи с этим, протокол Haven (Хейвен) сотрудничает с Chainlink,
и использует их системы ценообразования для обработки и предоставления данных о ценах.
Оракулы Chainlink для XHV / USD можно увидеть ниже.

Источник: *https://feeds.chain.link/xhv-usd*

Цель создателей протокола Хейвен, это обеспечить гибкость в получении данных о ценообразовании.
Поэтому мы не будем полагаться исключительно на одну систему оракулов, но планируем добавлять, менять и удалять оракулы с течением времени, чтобы гарантировать, что Хейвен будет использовать самые надежные и проверенные системы получения данных сейчас и в будущем.

Сценарии предложения

XHV - это чистая монета Proof-of-Work (PoW) с той же кривой эмиссии, что и Monero, у нее есть начальная добыча в 18,4 миллиона монет и небольшая хвостовая эмиссия после того, как эти 18,4 миллиона монет будут добыты.

Это стандартный сценарий предложения на рынке криптовалюты.

Теперь, когда функция офшорного хранилища Haven работает в основной сети, приведенные выше цифры продолжают применяться к вознаграждениям за майнинг, но больше не определяют фактическое оборотное предложение XHV, поскольку "чеканка и перевод" будут изменять эти значение динамически, как указано ранее.

Кроме того, как только в сети появятся дополнительные активы xAsset (помимо xUSD), оборот XHV больше не будет определять общую рыночную капитализацию экосистемы Haven.

Для этого необходимо учитывать совокупную стоимость имеющихся активов xAsset, а также саму стоимость XHV.

Это может быть выражено как HNV или стоимость сети Haven (Хейвен) и рассчитывается следующим образом: HNV = (цена XHV * оборотное предложение) + оборотное предложение + xUSD.

Дополнительные xAsset можно легко добавить в расчет по мере их добавления в цепь.

Чтобы понять потенциальный будущий оборот XHV и влияние этого предложения на экосистему Haven, ниже представлены следующие ознакомительные макро сценарии.

В этих сценариях рассматриваются следующие переменные:

1. Увеличение общей рыночной капитализации в рыночном цикле на повышение (inc_Bull)

2. Снижение общей рыночной капитализации в рыночном цикле на понижение (dec_Bear)

3. Процент монет XHV, отправленных и хранимых в офшорах в конце цикла на повышения рынка (perc_offBull)

4. Процент монет xAsset (на примере xUSD), возвращенных в XHV в конце цикла на понижение рынка (perc_onBear)

5. Процент местного значения ATH XHV в рамках цикла на повышение, который представляет собой среднее значение всех значений офшорных транзакций (например, если местный ATH для XHV составляет 2 доллара США, то 80% этого ATH составляет 1,60 доллара США, и это будет использоваться значение. в этих сценариях для оффшоринга, если для этой переменной используется 80%) (perc_LATH)

6. Процент местного значения ATL XHV в рамках медвежьего цикла, который является средним значением всех неоффшорных транзакций. (perc_LATL) §

a.*Примечание: значения для 5 и 6 можно применить для определения точности трейдеров при прогнозировании верхов и низов рынков.

7. Индекс волатильности XHV используется для моделирования того, насколько волатильность XHV может коррелировать по сравнению с волатильностью Биткойнов.

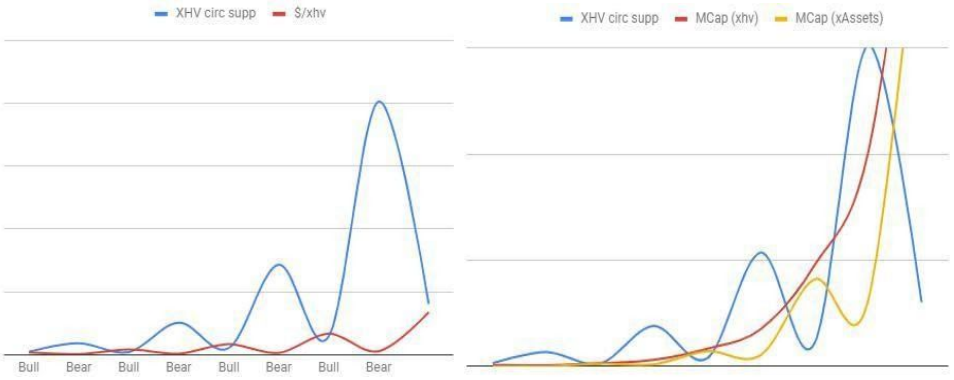
Значение 1 соответствует волатильности BTC, 0.5 -'вдвое менее волатильный', 2 - в два раза более волатильный и т. д.

Сценарий 1

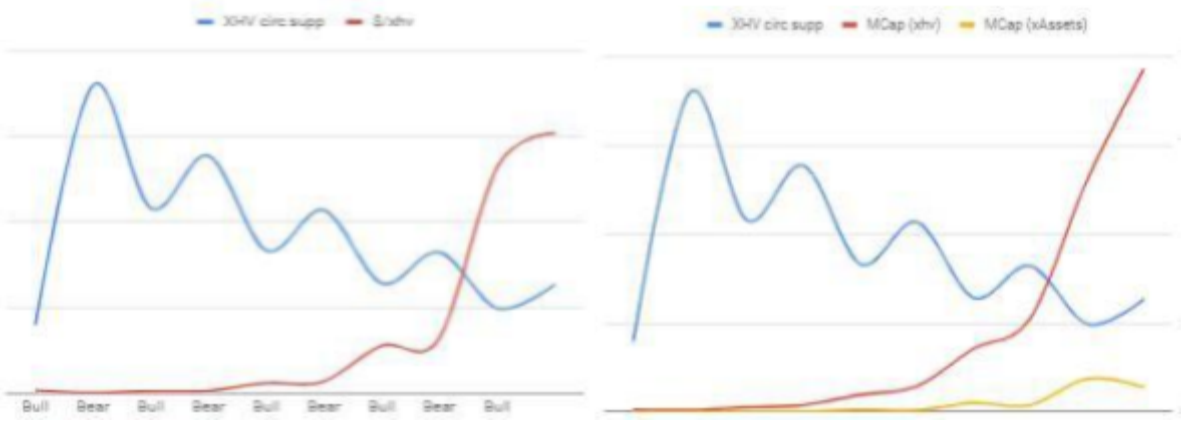
Расширение предложения XHV

В этом сценарии используются значения, которые со временем увеличат предложение XHV на рынке.

inc_Bull = 2500%
dec_Bear = 85%
perc_offBull = 80%
perc_onBear = 75%
perc_LATH = 90%
perc_LATL = 10%
iVol = 1.0



Из этой модели видно, что чрезвычайно интенсивное использование оффшоров и высокой точности торговли, использование оффшорных функций в сценарии расширения позволяет удерживать цену XHV на низком уровне, но со временем увеличивает рыночную капитализацию как XHV, так и экосистемы Haven в целом.
Этот сценарий приемлем для экосистемы, поскольку он снижает волатильность цены XHV, что, в свою очередь, изменяет показанные модели и переводит сценарий из расширения в состояние равновесия (или даже сокращения), что можно увидеть на графиках ниже, где единственное изменение к значениям, использованным выше, относится к iVol (0.5).

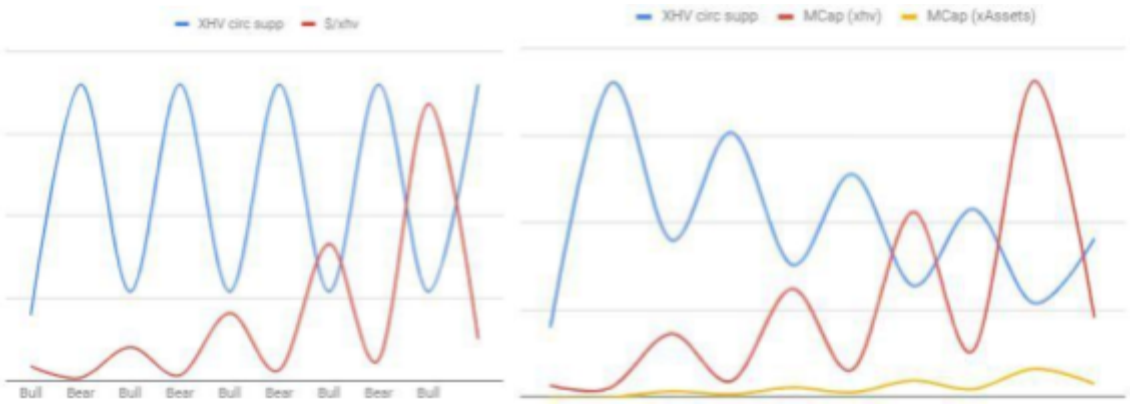


Сценарий 2

Сокращение предложения XHV

В этом сценарии используются значения, которые намеренно создают дефляцию в оборотном предложении XHV.

inc_Bull = 2500%
dec_Bear = 85%
perc_offBull = 50%
perc_onBear = 48%
perc_LATH = 60%
perc_LATL = 40%
iVol = 1.0



В этом сценарии сокращения, цена XHV увеличивается в волатильности, создавая со временем эффект, противоположный сценарию расширения, и будет перемещать модель от сжатия к равновесию или расширению.

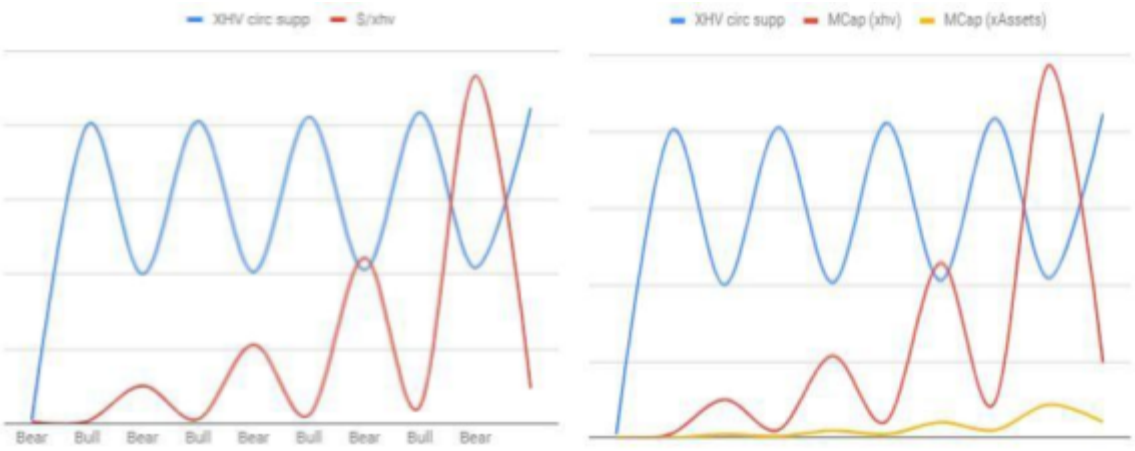
Сценарий 3

Равновесие в предложении XHV

В этом сценарии переменные устанавливаются со средним использованием оффшора и средней точностью торговли.
Этот сценарий будет работать с течением времени, так как оба сценария расширения и сжатия стремятся к равновесию.

inc_Bull = 2500%
dec_Bear = 85%
perc_offBull = 70%

perc_onBear = 50%
perc_LATH = 60%
perc_LATL = 40%
iVol = 1



В заключение, хотя невозможно предсказать, какой сценарий будет работать в определенный момент времени, протокол предназначен для адаптации к изменяющимся уровням использования путем расширения и сокращения поставок XHV непосредственно через действия пользователя, создавая новую и уникальную кривую предложения в ходе естественного и органического использования.

Сценарий 4

Стабильность и экономика

Для реализации процесса 'чеканки и перевода' в базовой форме требуется немного; должна быть известна цена, по которой необходимо выполнить перевод, и возможность конвертировать один тип активов в другой в той же цепочке с этим коэффициентом конверсии.

Это очень простая концепция. При этом простейшие концепции иногда труднее всего понять, и для того, чтобы экосистема Haven использовала надежную экономическую модель, необходимы определенные условия.

1. Прозрачность ресурсов
2. Оперирование биржевыми данными
3. Подтверждение и поддержание ценности синтетических активов в алгоритмической экосистеме PoW.
4. Возможность «массовых изъятий депозитов из банка» в периоды более широкой волатильности рынка.

Прозрачность ресурсов

Первоначальная концепция Haven была основана на наличии неизвестных оборотных ресурсов XHV и xAsset. Причина этого заключалась в том, чтобы предотвратить манипулирование сетью крупными держателями XHV или xAsset.

После тщательного обсуждения и консультаций с экспертами-консультантами было решено, что наличие прозрачного оборотного капитала будет полезно следующим образом:

· Это позволяет более эффективно контролировать сеть Haven, что означает, что попытки атак и крупномасштабные манипуляции могут быть обнаружены и устранены намного быстрее.

• Пользователи чувствуют себя более уверенно при использовании протокола Haven, имея возможность видеть количество XHV и xAsset в обращении в любой момент времени.

• Это обеспечивает большую доступность и, следовательно, лучший анализ на веб-сайтах с метриками монет. В результате, чтобы обеспечить точность и доступность, каждая транзакция 'чеканки и перевода' будет создана таким образом, чтобы суммы можно было найти с помощью анализа блок-чейна, и отобразить в обозревательных блоках протокола Haven. Это позволит пользователям использовать стандартные уровни анонимности системы Monero, и конфиденциальности адресов электронных кошельков, имея при этом четкое представление о приблизительном количестве токенов в обороте.

Приблизительное количество каждого типа активов можно увидеть здесь: https://explorer.havenprotocol.org/supply

Сценарий 5
Оперирование биржевыми ценами

Процесс 'чеканки и перевода', предполагает обязательство протокола Haven, что «1 xUSD всегда можно обменять на 1 доллар XHV».
Для динамики корректировки цен скользящих средних в рамках системы ценообразования Haven (Хейвен), необходимы определенные меры для устранения несоответствий между курсом биржи и оффшорными/ неоффшорными конверсиями.

Эта минимизация выполняется путем предоставления пользователю возможности выбора приоритета транзакции. За высоко приоритетные транзакции с минимальным временем разблокировки будет взиматься более высокая комиссия, чем за менее приоритетные транзакции с более длительным временем разблокировки (где комиссия будет близка к нулю).

С момента первого запуска разработчики протокола Haven отслеживали и анализировали данные, полученные в результате активности в течение первого месяца использования.

С момента первого запуска первоначальная структура комиссионных была заменена гораздо более простой и жесткой схемой для обеспечения работоспособности сети в краткосрочной перспективе, в то время как распределение токенов осуществляется ранними держателями. Со временем Хейвен предполагает, что сборы и их структура потребуют пересмотра и изменения. Полная структура платы будет опубликована вместе с этим документом и храниться для справки на веб-сайте Haven Protocol. https://havenprotocol.org/fees

Одна из проблем со многими существующими продуктами DeFi заключается в том, что у вас должен быть определенный токен в вашем кошельке, чтобы совершать транзакции в другом. Это может вызвать ненужное трение и затраты на его использование.

С транзакцией в протоколе Haven, комиссия снимается в отправляемой валюте.
Как показано в таблице ниже:

Тип транзакции	Тип комиссии	Комиссия оплачивается в
XHV трансфер	стандартная	XHV

xUSD трансфер	стандартная	xUSD
XHV -> xUSD	за обмен + стандартная	XHV
xUSD -> XHV	за обмен + стандартная	xUSD

Доказательство и поддержание ценности синтетических активов в алгоритмической экосистеме PoW

«Как можно утверждать, что xUSD стоит 1 доллар, если он не имеет гарантии?" - был одним из наиболее часто задаваемых вопросов связана с концепцией «истинной ценности» или «источника ценности».
Это одна из самых серьезных проблем, связанных с алгоритмическими синтетическими активами.

После того как на этот вопрос ответили и обсудили, что xUSD «косвенно поддерживается» изменяющейся и соответствующей суммой XHV, пользователи сосредоточились на вопросах, касающихся предложения и ликвидности самого XHV.

Поскольку предложение XHV будет колебаться из-за оффшорных транзакций, как описано выше, случаи расширения и сокращения предложения потенциально изменяют динамику всей экосистемы.

Учитывая цикличность рынков криптовалюты, вероятность возникновения обоих случаев высока. Это и ожидаемо, и желательно.
Колебания циркулирующего предложения абсолютно необходимы, чтобы учесть расширение и сокращение предложения xUSD без создания еще большей волатильности цены XHV.

Сценарий 6

Возможность "массовых изъятий депозитов из банка" в периоды более высокой волатильности рынка

Во время возрастающих рыночных циклов («бычий рынок») по любому товару трейдеры часто оставляют стабильные опции в пользу волатильных активов и наоборот.
Для любой традиционно «обеспеченной» стабильной монеты, такой как USDT, размер поддержки является ключом к стабильности поддерживаемой криптовалюты.

Любое отклонение «обеспеченной» стоимости от «рыночной» стоимости создает реальную опасность для пользователей и создает ситуацию, в которой существует потенциал для необеспеченной стоимости и потери привязки к любому активу, который криптовалюта должна отслеживать.

В протоколе Haven нет этой проблемой благодаря использованию процесса "чеканки и перевода" и цветных монет.

В любое время и во всех ситуациях пользователь может обменять 1 xUSD на 1 доллар XHV.

Поскольку протокол Haven реализован с использованием модели разноцветных монет, он способен поддерживать не только xUSD, но и ряд других активов и товаров, которые называются «xAssets».
Это позволяет XHV самому стать залогом не только для одного, но и для набора частных синтетических активов, расширяя возможные механизмы привязки и превращая протокол в платформу с реальным пользовательским сценарием и ценностью для пользователей криптовалюты.

Сценарий 7

Из кого состоит команда Haven?

Команда Haven - это сообщество разработчиков и вкладчиков, которое приветствует любой вид вклада.

Основная команда разработчиков указана ниже.

Взяв на себя управление и разработку монеты от первоначальных разработчиков, сообщество получило поддержку и советы со стороны консультантов и профессионалов технологической отрасли, которые поставили перед собой задачу выполнить обещание Haven и стимулировать внедрение этой модели в мир криптовалютного ландшафта.
Мы очень ценим постоянную поддержку и вклад этих людей.

Основная команда разработчиков:

Дэвид Бандток (@dweab) https://www.linkedin.com/in/david-bandtock-9647101/

Дэвид - карьерный технолог, специализирующийся на поставке продуктов и стратегии. За последние 20 лет он занимал руководящие должности в крупных корпорациях Великобритании и в нескольких технологических старт-апах.
Имея опыт работы в области математики, технологий шифрования и разработки программного обеспечения, Дэвид привнес в Haven значительный опыт как в технической доставке, так и в управлении.

Нил Коггинс (@neac) https://www.linkedin.com/in/neil-coggins-7972352/

Нил - специализированный архитектор и разработчик программного обеспечения полного стека. Обладает 20-летним опытом разработки на ассемблере X86, C ++, Java, PHP и Javascript, Нил последние 18 лет проектировал и создавал криптографическое программное обеспечение.

@Marty (аноним)
Марти - разработчик пользовательского интерфейса, с опытом работы с множеством фреймворков. Его основная функция - это работа с кошельками и веб-сайтами Haven.

@Pierre Lafitte (аноним)
Пьер - специалист по дизайну продуктов Пьер - опытный разработчик пользовательского интерфейса криптографии. Он будет руководить разработкой UX/UI и воплощать в реальность видение команды.