Haven Protocol
Finanzas Descentralizadas Privadas

Core Protocol v3.0

Este documento tiene como objetivo documentar la funcionalidad principal que ofrece Haven Protocol. Otras capas de funcionalidad no se exponen en este documento y se abordarán por separado..

Introducción

Bitcoin allanó el camino para la moneda electrónica peer-to-peer. Fue la primera moneda digital en implementar con éxito un libro mayor distribuido de transacciones basado en pruebas criptográficas en lugar de la confianza. Más recientemente, la demanda de transacciones privadas y monedas de privacidad ha crecido debido al hecho que todas las billeteras y transacciones en muchas criptomonedas son visibles para todos los que quieran mirar. Haven está construido sobre Monero, que es ampliamente considerado el líder en tecnología de privacidad. Por lo tanto, Haven hereda todas las características de privacidad de Monero, incluidas las “ring signatures” y “Bulletproofs”. Además, extiende esa funcionalidad al proporcionar monedas y commodities privados, anónimos y sintéticos (llamados (xAssets) que solo pueden existir mediante la "destrucción" de la divisa base de Haven - XHV. Haven también amplía la fungibilidad de Monero, para permitir múltiples tipos de activos en función de su valor monetario en lugar de solo la cantidad de monedas intercambiadas, creando así la primera plataforma de su tipo, un conjunto completamente privado de monedas y activos sintéticos.

Bienvenido a Haven - Finanzas privadas descentralizadas.

Historia del proyecto

El concepto de Haven fue iniciado por dos desarrolladores a principios de 2018. Esta primera etapa llegó a la fase de testnet (red pública de prueba) antes de que las debilidades en la solución, una pausa en el desarrollo y una falta de progreso de los desarrolladores originales pusieran el futuro del proyecto en duda. A finales de enero de 2019, un grupo de miembros originales de la comunidad de Haven se hizo cargo del proyecto con el fin de completar el proyecto, entregar el mecanismo de almacenamiento offshore y desarrollar la infraestructura para lograr la adopción masiva de una herramienta muy necesaria en mercado de las criptomonedas, el cual está en una fase de crecimiento exponencial.

La red principal del Protocolo de Haven (Mainnet) se lanzó con éxito el 20 de Julio de 2020, presentando su primera moneda privada, xUSD, al mercado.

Haven Protocol

La promesa: 1 xUSD siempre se podrá canjear por $1.00 en XHV.

i. Concepto

Haven es una criptomoneda imposible de rastrear con una combinación de precios de mercado estándar y almacenamiento de valor vinculado a activos en el mundo real. Esto se logra a través de un proceso de “creación y destrucción” dentro de un solo blockchain. En el caso más simple, los usuarios pueden quemar o destruir Haven (XHV) por el valor equivalente en dólares de xUSD. Para regresar a un estado volátil, el usuario puede igualmente quemar o destruir xUSD por un valor de $1 USD en XHV.

Otras monedas importantes, incluidas GBP, EUR y CNY, así como la plata, el oro y otros commodities como el petróleo, están planeados agregarse al ecosistema de Haven con el tiempo para permitir a los usuarios elegir un activo adecuado para sus necesidades.

ii. El Proceso Offshore - "Mint and Burn"

Haven utiliza un sistema llamado "mint and burn" (creación y destrucción) para mantener su relación de valor frente a sus activos fijos. En la práctica, usando el dólar estadounidense sintético (xUSD) como ejemplo: Bob decide que quiere poner 200 de sus XHV offshore. Cuando los usuarios colocan XHV Offshore, en efecto están quemando monedas XHV y transfiriendo el valor actual de esos XHV como nuevos xUSD. El mecanismo Offshore determina el valor de mercado actual de ese XHV (en xUSD) en función de un promedio ponderado de volumen entre las casas de intercambio soportadas (exchanges). Esto se hace utilizando un oráculo de precios (un mecanismo para descubrir datos del mundo real y hacer que estos datos estén disponibles para el blockchain) para obtener datos de precios para el ecosistema completo de Haven y crear registros de precios.

Si el valor actual de Haven es $1 USD, el almacenamiento offshore quemará los 200 XHV de Bob mediante la creación de una transacción especial en la que los 200 XHV que se enviaron se quemarán en xUSD y el suministro total de XHV disminuirá. Si el precio de mercado de XHV luego se mueve a $ 2 USD y Bob decide acceder a su almacenamiento offshore, se le devolverá 100 XHV (100 * $2 = $200 USD según el valor original).

Si ocurre lo contrario y el precio de Haven se reduce a la mitad a $ 0.50, entonces se crearan 400 XHV y se enviarán a Bob (400 * $0.50 = $200 USD según el valor original). Claramente, el uso de creación y destrucción, por lo tanto, altera la oferta circulante de los activos subyacentes de manera dinámica.

Esto crea escenarios de suministro interesantes, muy diferentes de otras criptomonedas, que los lectores deben revisar a fondo para comprender completamente el concepto del Protocolo Haven.

iii. ¿Cómo funciona realmente el proceso de Offshore?

El Protocolo Haven permite transacciones totalmente confidenciales dentro de la boveda de Haven (Haven Vault) utilizando un modelo de "moneda de color". Es la primera implementación de este tipo en el protocolo Cryptonote. El concepto de monedas de colores es bien conocido y definido dentro de la red Bitcoin, data desde 2013 y se puede encontrar aquí:

https://www.coindesk.com/colored-coins-paint-sopheded-future-for-bitcoin

Sin embargo, las monedas de color en cryptonote no pueden funcionar de la misma manera que en Bitcoin. Esto significa que el concepto dentro de Cryptonote debe ser reelaborado y reinventado. Gracias a Nate Eldredge tenemos esta clara descripción de las diferencias en la implementación para Bitcoin y Monero:

> *"Con Bitcoin, existe una correspondencia uno a uno entre las entradas y salidas de las transacciones. Suponga que hay una transacción X con una salida X1 que envía 1 satoshi a la dirección A de Alice, y todos están de acuerdo en que la salida X1 está coloreada para que otorgue el título al Chevy Nova 1977 de Alice. Si Alice decide darle el auto a Bob, crea una nueva transacción Y, con una entrada apuntando a X1, y cuya única salida Y1 envía 1 satoshi a la dirección B de Bob. Ahora Bob puede probar, creando una firma correspondiente a su dirección. B, que es el legítimo propietario del automóvil.*
>
> *Si Mallory intenta reclamar el automóvil creando una transacción diferente con la entrada X1, será descubierta, porque no puede firmar esa transacción con la clave privada de Alice, por lo que no se verificará. Si Alice intenta darle el automóvil a otra persona creando una segunda transacción Z debidamente firmada con la entrada X1, se detectará como un gasto doble porque otra transacción que gasta X1 lo precede en la cadena de bloques.*
>
> *Con firmas de anillo, esta correspondencia se rompe. Al crear una transacción, además de la única salida (de una transacción anterior) que realmente desea gastar, puede enumerar muchas otras. Puedes crear una firma que prueba que estás autorizado a gastar una de las salidas que enumeraste, pero no proporciona ninguna información sobre cuál era. Sin embargo, un algoritmo de vinculación asegura que cualquier intento futuro de gastar esa salida nuevamente será notado y rechazado.*
>
> *En el escenario anterior, si Alice usa una firma de anillo en su transacción Y, incluyendo no solo X1 sino otra salida Z1, entonces su firma no demostrará que tiene derecho a gastar X1 (y por lo tanto es la dueña legítima del automóvil y puede regalarlo); solo prueba que tiene derecho a X1 o Z1.*
>
> *Además, Mallory podría crear una transacción M que incluye X1 y otra salida K1 que tiene derecho a gastar. Dado que tiene la clave privada correspondiente a K1, puede firmar correctamente la transacción M, pero no estará claro si gastará X1 (lo que le daría título al automóvil) o K1 (que no lo hará) ".*

La descripción anterior describe la forma en que se han visto e implementado las monedas de colores dentro de la red Bitcoin, y señala con razón que este modelo falla cuando tanto X1 como Z1 todavía existen después de la transacción inicial. Sin embargo, Haven funciona de manera ligeramente diferente. Haven no tiene a Alice ni Mallory. Todo lo que tenemos es Bob.

Cuando Bob convierte de XHV a xUSD, envía una transacción con dos colores, X (XHV) y Z (xUSD). La transacción contiene como entradas monedas de sólo el primer color X, y tiene salidas de ambos X y el segundo color Z. Cada transacción dentro de la red Haven contiene dos valores para cada destino (#X, #Z), y para todas las transacciones, sólo uno de estos valores puede ser distinto de cero para cada destino.

Entonces, cuando Bob convierte sus 200 XHV a un precio de $1.00 por XHV, envía una transacción con entradas de (200,0) y valores de destino de (0,200) dando una salida de 200 xUSD y cero XHV. Si el precio de XHV luego se mueve a $2 por XHV, entonces la conversión a XHV enviaría una transacción con entradas de (0,200) y valores de destino de (100,0) dando una salida de 100 XHV y cero xUSD. De esta manera, las entradas a las transacciones y las UTXO se queman definitivamente, atómicamente y en tiempo real durante el proceso, y las salidas se crean de manera similar.

Todo esto es genial, sin embargo Haven es un fork de Monero y hereda todas sus características de seguridad y anonimato ... y Monero se basa en la premisa, condición y garantía absoluta de que para cualquier transacción dada; la diferencia entre entradas y salidas es cero. Cualquier transacción que no cumpla con este requisito siempre fallará.

En el caso de Haven, este aspecto fundamental de Monero no puede ser el caso, y de hecho para todas y cada una de las conversiones entre XHV y xUSD donde el precio de XHV no es precisamente $ 1.00 esta regla es completamente inválida, pues las entradas y salidas no serán iguales, tampoco nuestras sumas de C^a y C^b y, en consecuencia, *src / ringct / rctSigs.cpp verRctSemanticsSimple ()* fallará la prueba de Monero para:

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

Aquí presentamos el concepto dentro de la red Haven denominado 'Prueba de Valor'.

El artículo del Monero Research Lab sobre firmas de anillo enlazables concisas y falsificación contra claves adversas [Brandon Goodell, Sarang Noether y Arthur Blue] https://eprint.iacr.org/2019/654.pdf ['el artículo'] se ha utilizado como parte de la implementación de la Prueba de Valor de Haven.

En un borrador inicial del anterior documento, los escritores propusieron un modelo de 'juguete' en el cual crean una moneda de color con un enganche entre dos colores: dólares y centavos con una tasa de conversión de 100: 1 entre ellos, y muestran cómo esto puede hacerse usando CLSAG. El proceso es el siguiente:

1. Defina una tasa de conversión determinando una constante ξ y algunas constantes γC, γD en 1, 2,. . . , 2 ξ – 1, (en este ejemplo, γC = 100 y γD = 1).
2. Modifique la estructura de compromiso para que cada compromiso sea ahora un par de compromisos C y D para sus colores correspondientes
3. Cree una prueba de rango que cubra los valores de C y D. Aquí, C y D juegan el papel de los puntos Zj, y P son datos adicionales necesarios para el protocolo de transacciones.
4. Decimos que una llave de transacción simple es válida si se cumple lo siguiente:
    a. cada miembro del anillo de entrada (Xi, Ci, Di, Pi) ∈ Q tiene una prueba de rango válida Pi, por lo que Ver (Pi) = 1; y
    b. cada prueba de rango de salida P o k es válida entonces Ver (P o k) = 1; y
    c. para el anillo modificado pk = X1 X2 · · · Xn Z1 Z2 · · · Zn la firma σ pasa la verificación 2-CLSAG, Verificar (m, pk, σ) = 1.

El resultado es que la transacción no se firma con un compromiso a cero, sino con un compromiso con una diferencia; esa diferencia es la diferencia en el número de 'monedas / tokens' que crea esta transacción en función de las entradas y salidas. Si un usuario cambia 1 USD por 100 centavos, la diferencia sería de 99, la cantidad de monedas nuevas creadas. Este modelo funciona porque para que

un remitente firme usando la diferencia, ese usuario DEBE saber tanto el número de monedas utilizadas como entradas (que solo el titular de la clave privada de esas entradas puede conocer) y debe utilizar la tasa de conversión correcta de 100: 1, con todas las bulletproofs conteniendo los valores de los dos colores posibles. Al hacerlo, pueden firmar correctamente utilizando la diferencia entre entradas y salidas, y la transacción se validará.

El modelo anterior tiene un defecto importante cuando se considera el sistema de creación y destrucción utilizado en Haven. Requiere una tasa de conversión fija y conocida por ambos lados de la transacción, así como por todos y cada uno de los validadores de la transacción. Esto nos crea un problema y este modelo no funcionará porque, por definición, para vincular un activo volátil a uno estable, lo que debe cambiar es la tasa de conversión.

iv. Prueba de Valor.

Para que el modelo anterior de monedas de colores funcione con una tasa de conversión variable, se requiere:

1. Una forma de recopilar información de precios acordada e inmutable, de modo que en un momento dado, una transacción de conversión pueda usar un precio que pueda ser validado
2. Una forma de convertir entradas en salidas basadas en ese precio
3. Una forma de validar que el remitente de una transacción satisface los mismos requisitos que cualquier otra transacción de Cryptonote, es decir, que conoce la llave secreta de las entradas utilizadas y, por lo tanto, puede convertir utilizando una tasa de conversión y firmar una transacción con una diferencia correcta
4. Una forma de validar que el precio acordado se ha aplicado efectivamente a la conversión, sin revelar ningún monto a los validadores.

Los detalles de precios se obtienen de un proveedor de precios del mundo real (es decir, un oráculo de precios) y se crea un registro de precios en preparación para la resolución de un nuevo bloque. Los registros de precios contienen las tasas de conversión (contra XHV) para cada uno de los xAsset en el momento en que se mina el bloque. La información de precios se actualiza a intervalos de 30 segundos y se presenta al demonio Haven a pedido. Los registros de precios están incrustados en la cadena de bloques en cada encabezado de bloque por el minero que resuelve ese bloque en particular.

Al incluir esta información en cada bloque, el protocolo garantiza que el valor de la transacción no puede ser manipulado o alterado de ninguna manera: la cadena de bloques garantiza que la información de precios es inmutable. Si se extraen con éxito varios bloques dentro de los 30 segundos de vida útil del registro de precios actual, el mismo registro se incluirá en varios bloques.

1/ Un registro de precios contiene las siguientes tasas de conversión (todas contra XHV), así como un espacio reservado para futuras adiciones y la firma del oráculo que proporciona los datos. Un registro de precios de ejemplo es:

```
{
   "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
   }
}
```


Ejemplo de registro de precios: Carbon

2 / Haven hace esto en el ejemplo anterior [Bob] utilizando pares de compromiso en lugar de valores de compromiso únicos. Este también es el método utilizado en el ejemplo del juguete de los laboratorios de investigación de Monero.

3 / Las transacciones de Haven se firman utilizando CLSAG y emparejados con bulletproofs como ya se describio anteriormente. Sin embargo, no firmamos usando la diferencia como en el ejemplo del juguete. Firmamos usando el compromiso original de valores cero. Nuestro compromiso es cero diferencia en el **valor.**

4 / Aquí es donde se complica. Para comprender cómo Haven valida o rechaza transacciones utilizando una prueba de valor, se requiere un poco de trabajo previo y cierta comprensión de los algoritmos de llave pública, y de cómo Cryptonote usa operaciones y puntos de curva elíptica para validar cantidades de entrada y salida.

Cada transacción pasa por la función *verRctSemanticsSimple ()* que suma todas las entradas y salidas de una transacción para verificar que los resultados sean iguales. Aunque los valores en esta etapa están completamente encriptados y representados como puntos de curva elíptica ['EC'] en lugar de números reales, estas sumas aún funcionan debido a las propiedades de la aritmética modular y la forma específica en que se eligen / generan los puntos EC de Monero.

En resumen, aunque los números están encriptados, todavía tienen ciertas propiedades: las diferencias entre ellos (dentro del espacio de la CE) siguen siendo válidas, por lo que una diferencia cero seguirá siendo una diferencia cero porque los compromisos son aditivos.

En otras palabras, si tuviéramos una transacción con entradas que contengan cantidades a_1, ..., a_j y salidas con cantidades b_1, ..., b_k, entonces un observador esperaría justificadamente que:

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

Para Haven, esto aún funciona para transferencias XHV y transferencias xUSD, pero para conversiones esto es completamente incorrecto.

Entonces, reutilizando alguna notación de arriba, definamos las constantes γC, γD como la tasa de conversión para una ***sola*** transacción, esa tasa de conversión la proporciona nuestro oráculo de precios. Y ahora con compromisos emparejados en nuestras pruebas de rango, las pruebas son (C, D) respectivamente. Para demostrar la igualdad de valor, necesitamos que la suma del valor de las entradas sea igual a la suma del valor de las salidas.

Nuestra validación ahora se ve así:

$$\lambda C \left(\sum_{yo} C_{yo} - f_c G - \sum_{k} C_k^{'} \right) = {}_{1\ /\lambda D} \left(\sum_{i} D_i - f_D G' - \sum_{k} D_k^{'} \right)$$

Donde $\lambda C,\ \lambda D$ significan que los valores entre paréntesis se suman en función de sus respectivas tasas de conversión. (C, D) significa compromisos de entrada, (C ', D') significa compromisos de producción y fxG significa las tarifas pagadas.

v. Oráculos de fijación de precios

Para recuperar datos del mundo real, las cadenas de bloques usan un mecanismo llamado "oráculo". "Un oráculo de blockchain es una fuente de información de terceros que tiene la única función de suministrar datos a blockchains"

Fuente: *https://www.mycryptopedia.com/blockchain-oracles-explained/*

En la primera iteración de Haven y varios diseños posteriores, la creación de un oráculo seguro, preciso y de alto rendimiento se consideró clave para el éxito del protocolo. Sin embargo, desde la creación y el éxito de servicios como Chainlink, que están diseñados exclusivamente para proporcionar funciones de Oracle como una fuente de datos independiente, ahora está claro que no solo no se requiere que se integre un oráculo separado en el sistema de Haven, sino que no es deseable hacerlo. Si lo hace, se incrementa la centralización de la parte más importante de la ecuación de conversión - la fijación de precios.

Con esto en mente, el Protocolo Haver ha colaborado con Chainlink con el fin de utilizar su oráculo para el procesamiento y suministro de precios de datos. Los oráculos de Chainlink para XHV / USD se pueden ver a continuación

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

Haven cree que es vital crear flexibilidad en el descubrimiento de precios desde el principio y, como tal, no dependerá únicamente de un sistema Oracle, sino que podrá agregar, intercambiar y eliminar oráculos con el tiempo para garantizar que Haven use los mejores datos de su clase ahora y en el futuro.

Escenarios de Oferta y Demanda

XHV es una moneda de prueba de trabajo (Proof of Work - PoW) pura con la misma curva de emisión que Monero, tiene un suministro inicial de 18,4 millones y una pequeña emisión de cola una vez que se han extraído esos 18,4 millones de monedas.

Este es un mecanismo bien entendido en el mercado de las criptomonedas. Ahora que la función offshore de Haven está activa en el Mainnet, las cifras anteriores continúan aplicándose a las recompensas mineras, pero ya no definen el suministro circulante real de XHV ya que la creacion y destruccion de las monedas alterarán esto dinámicamente.

Además, una vez que más xAssets (más allá de xUSD) estén activos en la red, el suministro circulante de XHV ya no define la capitalización de mercado total del ecosistema de Haven. Para ello, es necesario considerar el valor acumulado de los xAssets mantenidos así como el propio XHV.

Esto se puede expresar como HNV o Haven Network Value y se calculará de la siguiente manera:

HNV = (precio XHV * suministro circulante) + xUSD suministro circulante

Se pueden agregar fácilmente xAssets adicionales en el cálculo a medida que se agregan a la red.

Para comprender el suministro futuro potencial de XHV y el efecto de ese suministro en el ecosistema de Haven, se presentan los siguientes escenarios macro.

Las variables consideradas en estos escenarios incluyen:

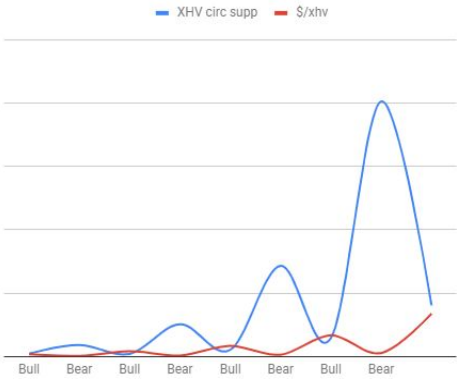
1. El aumento de la capitalización de mercado total en un ciclo de mercado alcista (inc_Bull)
2. La disminución de la capitalización de mercado total en un ciclo de mercado bajista (dec_Bear)
3. El % de monedas XHV enviadas y almacenadas offshore al final de un ciclo de mercado alcista (perc_offBull)
4. El % de xAssets (usando xUSD como ejemplo) convertidos de vuelta a XHV al final de un ciclo de mercado bajista (perc_onBear)
5. El % del valor ATH (All Time High - Valor más alto) de XHV dentro de un ciclo alcista que es el promedio de todos los valores de transacción offshore (Ej., si el ATH local para XHV es de $ 2.00, el 80% de este valor es de $ 1,60 y este sería el valor utilizado en estos escenarios para realizar el proceso offshore si el 80% se utiliza para esta variable) (perc_LATH)
6. El % del valor ATL (All time low - Valor más bajo) local de XHV dentro de un ciclo bajista que es el promedio de todos los valores de transacciónes onshore. (perc_LATL) §
    a. ** Nota: Estos valores para los puntos 5 y 6 pueden verse como la precisión con que los operadores predicen los máximos y mínimos de los mercados.*
7. Índice de volatilidad XHV: este valor se utiliza para simular qué tan correlacionada podría estar la volatilidad de XHV en comparación con la volatilidad del Bitcoin. Un valor de 1 es igual a la volatilidad de BTC, 0,5 es 'la mitad de volátil', 2 es el doble de volátil, etc.

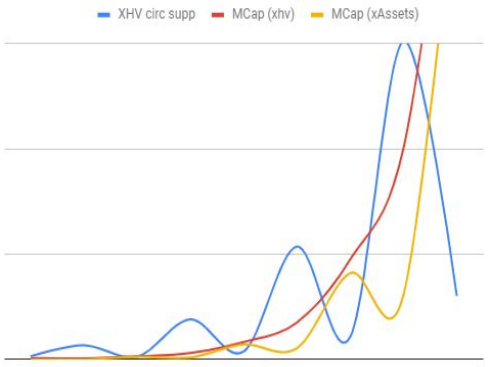
Escenario 1

Expansión en la oferta de XHV

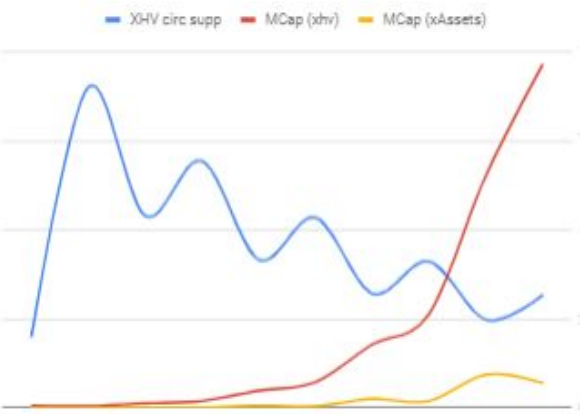
En este escenario usamos valores que aumentarán la oferta de XHV en el mercado con el tiempo.

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





Como se puede ver en este modelo de uso offshore extremadamente activo, el uso de la funcionalidad offshore en un escenario de expansión mantiene bajo el precio de XHV, pero con el tiempo aumenta la capitalización de mercado tanto de XHV como del ecosistema de Haven en conjunto. Este escenario es aceptable para el ecosistema, ya que reduce la volatilidad del precio de XHV, lo que a su vez altera los patrones mostrados y mueve el escenario fuera de la expansión y hacia el equilibrio (o incluso la contracción) como se puede ver en los gráficos a continuación donde el único cambio a los valores usados arriba es iVol (0.5).

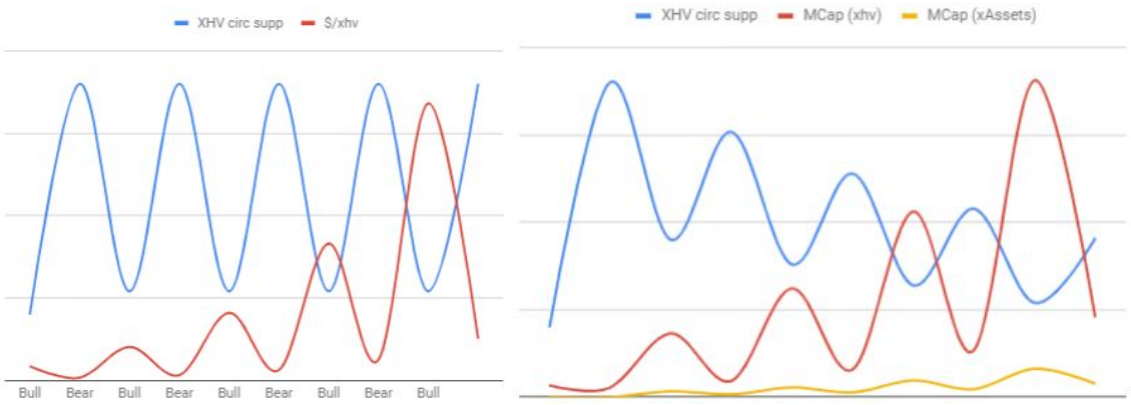


Escenario 2

Contracción en el suministro de XHV

En este escenario, se utilizan valores que deliberadamente crean deflación en el suministro circulante de XHV.

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



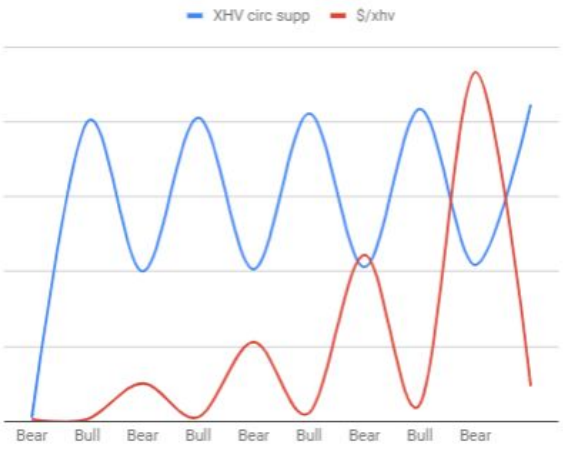
Como se puede ver en un escenario de contracción, el precio de XHV aumenta en volatilidad, creando el efecto contrario al escenario de expansión en el tiempo y moverá el patrón desde la contracción hacia el equilibrio o la expansión.

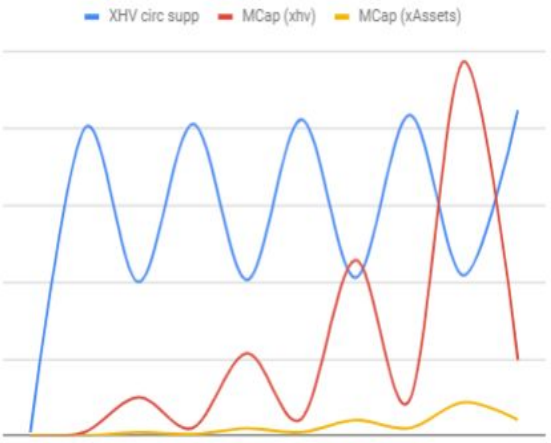
Escenario 3

Equilibrio en la oferta de XHV

En este escenario, las variables de predicción se establecen con un uso medio de offshore y un trading medio. Como punto central entre los otros dos escenarios, se puede esperar que este escenario se desarrolle repetidamente a lo largo del tiempo, con escenarios de expansión y contracción tendiendo hacia el equilibrio.

inc_Bull = 2500%
dec_Bear = 85%
perc_offBull = 70%
perc_onBear = 50%
perc_LATH = 60%
perc_LATL = 40%
iVol = 1





En conclusión, aunque no se puede predecir qué escenario se desarrollará en un momento dado, el protocolo está diseñado para adaptarse para cambiar los niveles de uso al expandir y contraer el suministro de XHV directamente a través de las acciones del usuario, creando una curva de suministro nueva y única puramente de uso natural y orgánico.

Estabilidad y economía

Mint and burn (mecanismo de creación y destrucción de criptomonedas de Haven) requiere poco para implementarse en una forma básica; solo un precio conocido al que realizar la conversión y la capacidad de convertir un tipo de activo en otro en la misma cadena a esa tasa de conversión.

Para decir lo obvio, es un concepto muy simple. Dicho esto, los conceptos más simples a veces son los más difíciles de comprender por completo, y para garantizar que el ecosistema de Haven utilice un modelo económico sólido, se deben abordar ciertos desafíos.

1. Transparencia de la oferta
2. Manipulación de precios basada en intercambio
3. Demostrar y mantener el valor de los activos sintéticos en un ecosistema algorítmico de PoW.
4. El potencial de un 'Pánico Bancario' durante períodos de mayor volatilidad del mercado

Estos desafíos se abordarán uno a la vez:

Transparencia de la oferta

El concepto original de Haven se basaba en tener una oferta circulante desconocida de XHV y xAssets. El motivo de esto fue evitar la manipulación de la red por parte de grandes propietarios de XHV o xAssets.

Después de una gran consideración, discusión comunitaria y consultas con asesores expertos, se decidió que tener un suministro circulante transparente sería realmente beneficioso para la red de las siguientes maneras:

- Permite un monitoreo más eficiente de la red Haven, lo que significa que los intentos de ataque y la manipulación a gran escala se pueden detectar y mitigar mucho más rápido.
- Brinda a los usuarios una mayor confianza para ingresar a la red Haven con la capacidad de ver la cantidad de XHV y xAssets en circulación en un momento dado.
- Permite una mayor visibilidad y un mayor análisis en los sitios web de métricas de monedas. Como resultado, para garantizar la precisión y la visibilidad, cada transacción de creación y destrucción se creará de tal manera que las cantidades se puedan descubrir a través del análisis de la cadena de bloques y se mostrarán en los exploradores de bloques de Haven. Esto permitirá a los usuarios mantener los niveles estándar de anonimato de Monero y la privacidad de la dirección de la billetera al tiempo que permite una visión clara del suministro en circulación.

El suministro de cada tipo de activo ahora es visible y se puede ver aquí:

https://explorer.havenprotocol.org/supply

Manipulación de precios basada en el intercambio

Debido a la naturaleza de mint and burn, la promesa de Haven en la cual "1 xUSD siempre será canjeable por $ 1 de XHV", y la acción de promediar los precios dentro del sistema de precios de Haven, se requieren ciertas medidas para garantizar que las discrepancias entre los tipos de cambio y conversiones off/onshore sean minimizadas.

Esta minimización se realiza al permitir que el usuario elija la prioridad de la transacción. Las transacciones de alta prioridad, con tiempos de desbloqueo mínimos, cobrarán tarifas más altas que las transacciones de baja prioridad con tiempos de desbloqueo más largos (donde la tarifa tenderá a casi cero).

Desde sus inicios, los colaboradores de Haven han estado monitoreando y analizando los datos obtenidos de la actividad durante el primer mes de uso en el mundo real. La estructura de tarifas original ha sido reemplazada por un esquema mucho más simple y estricto para garantizar la salud de la red a corto plazo, mientras que la distribución de tokens se mantiene bajo un número reducido de entidades. Con el tiempo, Haven prevé que las tarifas y sus estructuras requerirán una revisión y modificación para trabajar junto con la madurez de la red Haven. La estructura de tarifas completa para la red Haven se publicará junto con este documento y se mantendrá como referencia en todo momento en el sitio web del Protocolo Haven. https://havenprotocol.org/fees

Uno de los problemas con muchos productos DeFi existentes es que debe tener un token particular en su billetera para poder realizar transacciones en otro. Esto puede causar fricciones y costos innecesarios solo por usarlo.

Las transacciones de Haven superan esto al cobrar las tarifas en la moneda que se envía. Esto se muestra en la siguiente tabla:

Tipo de Transacción	Tarifa	Se paga en
Transferencia de XHV	Cuota de tx standard	XHV
Transferencia de xUSD	Cuota de tx standard	xUSD
Conversión de XHV -> xUSD	De conversión + cuota de tx standard	XHV
Conversión de xUSD -> XHV	De conversión + cuota de tx standard	xUSD

Demostrar y mantener el valor de los activos sintéticos en un ecosistema algorítmico de PoW

Uno de los mayores desafíos de los activos sintéticos algorítmicos, así como una de las preguntas más frecuentes, se centra en el concepto de "valor real" o "fuente de valor." Preguntas como "¿cómo se puede afirmar que xUSD vale $ 1 cuando no tiene respaldo colateral?"

Una vez que se ha respondido y entendido esa pregunta (xUSD está "respaldado indirectamente" por una cantidad variable y apropiada de XHV), los usuarios se enfocan en preguntas sobre el suministro y la liquidez del XHV en sí. Dado que el suministro de XHV fluctúa debido a las transacciones offshore

como se describe anteriormente, tanto los casos de expansión como de contracción de la oferta cambian potencialmente la dinámica de todo el ecosistema.

Con toda probabilidad, teniendo en cuenta la naturaleza cíclica de los mercados de criptomonedas, la posibilidad de que surjan ambos casos es alta. Esto es esperado y deseable. Las fluctuaciones en la oferta circulante son absolutamente necesarias para permitir la expansión y contracción en la oferta de xUSD sin crear una volatilidad cada vez mayor en el precio de XHV.

El potencial de un "Pánico Bancario" durante períodos de mayor volatilidad del mercado

Durante los ciclos de mercado en alza ("mercados alcistas") en cualquier commodity, los operadores a menudo dejan opciones estables a favor de activos volátiles, y viceversa. Con cualquier stablecoin (criptomoneda estable) como USDT, la cantidad de respaldo es clave para la estabilidad de la criptomoneda respaldada. Cualquier desviación del valor 'respaldado' al valor de 'mercado' crea un peligro real para los usuarios y crea una situación en la que existe un potencial de valor sin respaldo y pérdida de vinculación con cualquier activo que se supone que la criptomoneda debe garantizar.

Haven no sufre este problema debido al uso de mint & burn y monedas de colores.

En todo momento y en todas las situaciones, un usuario puede canjear 1 xUSD por $1 en XHV. Esta garantía nunca se romperá.

Dado que el protocolo Haven se implementa utilizando un modelo de moneda de color, es capaz de admitir no solo xUSD, sino también una variedad de otros activos y productos básicos que llamamos 'xAssets'. Esto permite que el propio XHV se convierta en la garantía no solo de uno, sino de un conjunto de activos sintéticos privados, extendiendo los mecanismos de vinculación posibles y convirtiendo el protocolo en una plataforma con un verdadero caso de uso y valor para los usuarios de criptomonedas.

¿Quiénes son el equipo de Haven?

El equipo de Haven es un colectivo comunitario de desarrolladores y colaboradores y, como tal, agradece todas los aportes y contribuciones de cualquier individuo o empresa.

El equipo de desarrollo principal se enumera a continuación.

Desde que se hizo cargo de la gestión y el desarrollo de la moneda de los desarrolladores originales, la comunidad se ha beneficiado del apoyo y la orientación continuos de varios asesores, consultores y profesionales de la industria de la tecnología que han hecho su misión cumplir la promesa de Haven e impulsar la adopción de esta parte vital del panorama de las criptomonedas. Se agradece enormemente el continuo apoyo y aportes de estas personas.

Equipo de desarrollo principal:

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

David es un tecnólogo de carrera con un enfoque en la entrega del producto y la estrategia, ha ocupado puestos de responsabilidad en las principales corporaciones del Reino Unido y varias nuevas empresas de tecnología en los últimos 20 años. Con experiencia en matemáticas, tecnología de cifrado y desarrollo de software, David aporta a Haven una experiencia considerable tanto en la entrega técnica como en la gobernanza a gran escala.

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

Neil es un arquitecto y desarrollador de software. Con más de 20 años de experiencia en desarrollo en X86 Assembler, C ++, Java, PHP y Javascript, Neil ha pasado los últimos 18 años diseñando y construyendo software criptográfico.

@Marty (anónimo)

Marty es un desarrollador front-end con experiencia en una multitud de frameworks, y lo pone en práctica con su trabajo en los wallet y sitios web de Haven.

@Pierre Lafitte (anónimo)

Pierre es un especialista en diseño de productos y crea todas las experiencias de usuario y UI en la cartera de productos de Haven. Pierre es un experimentado desarrollador de criptografía de Front End, colabora desde hace mucho tiempo con Haven y liderará el lado del desarrollo de UX / UI y hará realidad las visiones de UX del equipo.