# Haven Protocol
# Finanza Privata Decentralizzata

## *Core* Protocol v3.0

Questo documento ha come obiettivo la documentazione della funzionalità principale che offre Haven Protocol. Le funzioni di secondo livello non verranno esposte in questo documento, ma verranno approfondite separatamente caso per caso.

**Introduzione**

Bitcoin ha dato via alle valute elettroniche peer-to-peer. È stata la prima valuta digitale ad implementare con successo un libro mastro di transazioni basato sulle prove crittografiche in luogo della fiducia. Più di recente, con la consapevolezza che tutti i wallet e transazioni in molte criptovalute sono visibili a tutti coloro che sono interessati a consultarli, la domanda per transazioni private e valute di privacy è cresciuta. Haven ha alla base la tecnologia di Monero, che è ampiamente considerato essere il leader nelle tecnologie legate alla privacy. Haven, pertanto, eredita da Monero tutte le sue funzionalità di privacy, includendo "ring signatures" e "bulletproofs". Estende tale funzionalità a fornire versioni sintetiche, private, e anonime di valute e commodities (xAssets) che possono esistere unicamente mediante la "distruzione" della valuta base di Haven - XHV. Haven estende anche la prova di fungibilità di Monero, consentendo a multipli tipi di asset di essere equiparati sulla base del valore monetario piuttosto che del solo numero di coin scambiati, creando per la prima volta nel suo genere una collezione totalmente privata di valute sintetiche e di asset.

Benvenuti a Haven - Finanza privata decentralizzata.

## La Storia del Progetto

Il concetto di Haven nasce dall'idea di due sviluppatori all'inizio del 2018. Questo primo tentativo raggiunse la fase di testnet (rete pubblica di prova) prima che delle lacune nella soluzione, una pausa nello sviluppo, e una susseguente mancanza di progressi da parte degli sviluppatori originali mise il futuro del progetto in uno stato di incertezza. Alla fine di gennaio 2019, alcuni membri della prima community di Haven presero in mano il progetto con l'obiettivo di completarlo, fornendo un meccanismo di storage offshore e costruendo un'infrastruttura di supporto per ottenere un'adozione di massa di questa funzionalità molto richiesta nel mercato di criptovalute, il quale sta espandendo in maniera esponenziale. Il mainnet (rete principale) di Haven Protocol si è lanciato con successo il 20 di luglio del 2020, introducendo la sua prima valuta privata al mercato, xUSD.

## Haven Protocol

Il promesso: 1 xUSD sarà sempre scambiabile per l'equivalente di $1.00 in XHV.

### i. Il Concetto

Haven è una criptovaluta non tracciabile con un mix di prezzi del mercato standard e stabili valute vincolate ad asset del mondo reale. La stabilità degli xAsset si mantiene attraverso un processo di "conia e brucia" eseguito dentro un singolo blockchain. Nel caso più semplice, gli utilizzatori possono bruciare Haven (XHV) per l'equivalente ammontare in valore USD (dollari statunitensi) in dollari Haven (Haven Dollars xUSD). O, per restituire uno stato volatile, l'utilizzatore può in ugual modo bruciare xUSD per il valore di $1 USD in XHV.

Altre valute fiat importanti che includono GBP, EUR e CNY, così come argento, oro e altre commodity importanti come il petrolio, approderanno nel corso del tempo nell'ecosistema Haven al fine di consentire agli utilizzatori la scelta degli xAsset che più preferiscono e che soddisfi al meglio le proprie esigenze.

### ii. Il Processo Offshore - "Mint and Burn"

Haven utilizza un sistema chiamato "mint and burn" (coniatura e bruciatura, creazione e distruzione) per maniere il suo valore in di fronte ai suoi asset. In pratica, usando il sintetico US dollar (xUSD) come esempio, questo processo funziona come segue: Bob decide che vuole mettere offshore 200 dei suoi Haven (XHV). Quando gli utilizzatori mettono monete di XHV offshore, bruciano gli XHV e coniano il valore attuale degli XHV bruciati come nuove monete di xUSD. Il meccanismo offshore determina il valore di mercato attuale in xUSD degli XHV bruciati in base ad una media ponderata di volume tra gli exchange supportati. Ciò viene calcolato tramite un oracolo di prezzi (un meccanismo per scoprire dati del mondo reale e far sì che questi dati siano disponibili per un blockchain) per ottenere dati di prezzo per l'ecosistema completo di Haven e creare registri di prezzo.

Se il valore attuale di Haven è di $1, il processo di deposito offshore brucerà i 200 XHV di Bob mediante la creazione di una transazione speciale nella quale i 200 XHV che si inviano si bruceranno in xUSD e l'offerta di moneta totale di XHV diminuirà. Se il prezzo di mercato di XHV poi si alza a $2 e Bob decide di accedere al suo deposito offshore, gli verrano tornati 100 XHV (100 * $2 = 200 USD secondo il valore originale).

Se accade l'opposto e il prezzo di Haven si dimezza a $0.50, allora 400 XHV saranno coniati e mandati a Bob (400 * $0.50 = $200 USD secondo il valore originale). Chiaramente, l'uso di conia e brucia risulta in alterazioni dinamiche dell'offerta circolante delle monete sottostanti.

Questo crea degli scenari interessanti di offerta circolante, molto differenti da altre criptovalute, che devono essere rivisti rigorosamente dai lettori per arrivare ad una comprensione completa del concetto di Haven Protocol.

### iii. Come funziona veramente il processo offshore?

L'Haven Protocol permette transazioni di offshore dentro L'Haven Vault (camera blindata di Haven) utilizzando un modello di "valuta colorata." È la prima implementazione funzionante di valute colorate sul CryptoNote Protocol. Il concetto di valuta colorata è ben saputo ed è definito dentro la rete Bitcoin. Una descrizione del concetto risalente al 2013 si trova qui:

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

Le valute colorate su CryptoNote non possono comunque funzionare nella stessa maniera che funzionano con Bitcoin, e infatti il concetto di valuta colorata su CryptoNote deve essere rilavorato e reinventato. Grazie a Nate Eldredge per questa descrizione chiara delle differenze di implementazione tra Bitcoin e Monero:

> *"Con Bitcoin, c'è una corrispondenza uno a uno tra entrate e uscite delle transazioni. Supponi che c'è una transazione X con un'uscita X1 che manda 1 satoshi all'indirizzo A di Alice, e tutti sono d'accordo che l'uscita X1 sia colorata in modo che conceda il titolo alla Chevy Nova 1977 di Alice. Se Alice decide di dare la macchina a Bob, crea una nuova transazione Y, con un'entrata che indica X1, e con una sola uscita Y1 che manda 1 satoshi all'indirizzo B di Bob. Ora Bob può provare, creando una firma digitale corrispondente al suo indirizzo B, che è lui il proprietario legittimo dell'automobile.*
>
> *Se Mallory tenta di reclamare la macchina creando una transazione diversa con entrata X1, verrà scoperta, perché non può firmare quella transazione con la chiave privata di Alice, e la transazione non si verificherà. Se Alice tenta di dare la macchina a qualcun altro, creando una seconda transazione Z debitamente firmata con entrata X1, si rileverà come doppio speso perché un'altra transazione che spende X1 la precede nel blockchain.*
>
> *Con le firme ad anello, questa corrispondenza viene interrotta. Nel momento di creazione di una transazione, in aggiunta alla singola uscita (di una transazione precedente) che si vuole spendere, se ne possono elencare molte altre. Puoi creare una firma che attesti l'autorizzazione a spendere una tra quelle elencate, ma non dà alcuna informazione su quella che è stata scelta. Ad ogni modo, un algoritmo di collegamento assicura che ogni tentativo futuro di spendere di nuovo quell'uscita verrà notata e rifiutata.*
>
> *Nello scenario precedente, se Alice utilizza una firma ad anello con la sua transazione Y, che include non solo X1, ma anche un'altra uscita Z1, allora la sua firma non attesterà che abbia il diritto di spendere X1 (e pertanto che sia la proprietaria legittima della macchina e può regalarla); attesta solo che abbia diritto a X1 o Z1.*
>
> *Inoltre, Mallory potrebbe creare una transazione M che include X1 e un'altra uscita K1 che ha il diritto di spendere. Dal momento che ha una chiave privata che corrisponde a K1, lei può correttamente firmare la transazione M, ma non sarà chiaro se sta spendendo X1 (che porta il titolo alla macchina) o K1 (che invece non lo fa)."*

La descrizione precedente descrive il modo in cui le valute colorate sono state viste ed implementate dentro la rete di Bitcoin, ed indica giustamente che questo modello fallisce quando entrambe X1 e Z1 sono ancora in esistenza dopo la transazione iniziale. Haven, comunque, funziona in un modo leggermente diverso. Haven non ha un' Alice né una Mallory. Esiste solo Bob.

Quando Bob converte da XHV a xUSD manda una transazione con due colori, X (XHV) e Z (xUSD). La transazione impiega come moneta di input di solo il primo colore X ed ha come uscita sia X che il secondo colore Z. Ogni transazione fatta mediante la rete Haven contiene due valori per ogni destinazione (#X, #Z), e per tutte le transazioni, solo uno di questi valori può non essere non-zero per ciascuna destinazione.

Quindi, quando Bob converte i suoi 200 XHV ad un prezzo di $1.00 ciascun XHV, manda una transazione con entrate (200, 0) e valori di destinazione di (0, 200), generando uscite di 200 xUSD e 0 XHV. Se il prezzo di XHV poi cambia a $2 per XHV, allora la riconversione in XHV manderebbe una transazione con entrate (0, 200) e valori di destinazione di (100, 0), generando uscite di 100 XHV e 0 xUSD. In questo modo, le entrate a transazioni e le UTXO vengono bruciate definitivamente, atomicamente ed in tempo reale durante il processo, e le uscite si creano in maniera parallela.

Tutto ciò è fantastico, però Haven è un fork di Monero ed eredita tutte le sue funzionalità di sicurezza e anonimato… e Monero è basato sulla premessa assoluta che per ogni data transazione, la differenza tra entrate e uscite equivale sempre a zero. Ogni transazione che non soddisfi questo requisito non andrà a buon fine.

Nel caso di XHV, questo aspetto fondamentale di Monero non può essere vero, e infatti per qualsiasi scambio tra XHV e xUSD laddove la il prezzo di XHV non è precisamente $1.00, questa regola si rompe completamente, non saranno uguali le entrate e uscite, e neanche le nostre somme di $C^a$ e $C^b$, e in conseguenza src/ringct/rctSigs.cpp verRctSemanticsSimple() fallirà la prova di Monero per:

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

Qui introduciamo il concetto della rete Haven nella "*prova di valore*".

Ringraziamenti vanno fatti alla Monero Research Lab per l'articolo Concise Linkable Ring Signatures and Forgery Against Adversarial Keys [Brandon Goodell, Sarang Noether and Arthur Blue] https://eprint.iacr.org/2019/654.pdf [d'ora in avanti "l'articolo"] che è stato utilizzato come parte dell'implementazione Haven della Prova di Valore.

In una prima bozza dell'articolo, gli autori hanno proposto un "toy" model dove hanno creato una valuta colorata con un gancio fisso tra due colori: dollari e centesimi con tasso di cambio 100 : 1 tra loro e mostrano come questo possa essere fatto utilizzando CLSAG. Qui di seguito il processo:

1. Definire un tasso di cambio determinando una costante ξ e alcune costanti γC , γD on 1, 2, . . ., 2 ξ−1, (nel nostro esempio, γC = 100 e γD = 1).
2. Modificare la struttura degli impegni in modo che ogni impegno sia ora una coppia di impegni C e D per i colori corrispondenti.
3. Creare una prova di intervallo che copra i valori di C e D. Qui, C e D giocano il ruolo dei punti Zj, e P sono dati aggiuntivi richiesti per il protocollo di transazione.
4. Diciamo che una chiave di transazione semplice è valida se quanto segue è soddisfatto:
    a. ogni membro dell'anello di input (Xi, Ci, Di, Pi) ∈ Q ha una prova di intervallo valida Pi quindi Ver (Pi) =1; e
    b. ogni prova di intervallo P o k è valida se Ver (P o k)=1; e
    c. per l'anello modifica pk = X1 X2 ⋯ Xn Z1 Z2 ⋯ Zn la firma σ passa la verifica 2-CLSAG, Verifica (m, pk, σ) = 1.

Il risultato è che la transazione non si firma con un impegno a zero, ma con un impegno ad una differenza - che si definisce come differenza del numero di monete che la transazione crea in uscita in relazione al numero di monete in entrata. Se un utente dovesse scambiare 1 USD per 100 centesimi, la differenza sarebbe uguale a 99 - il numero di nuove monete coniate. Questo modello funziona perché l'utente può firmare la transazione con la differenza solamente nel caso in cui lui sa sia il numero di monete usate come entrata (che solo il portatore della chiave private per quelle entrate può sapere) che il tasso di cambio corretto di 100:1, con tutti i bulletproofs contenenti i valori di entrambi i colori possibili. Facendo così, l'utente potrà firmare correttamente usando la differenza tra entrate e uscite, e la transazione andrà a buon fine.

Il modello sopraindicato ha un importante difetto quando si considera il sistema Haven di coniatura e bruciatura. Esso richiedere un tasso di cambio fisso. Fisso e conosciuto da entrambi i lati della transazione e anche fissato e conosciuto da tutti i validatori della transazione. Questo per noi crea dei problemi, e questo modello non funziona perché per definizione per agganciare un asset volatile a uno stabile, la cosa che deve cambiare è il tasso di cambio.

### iv. Prova di valore

Per far funzionare il modello di monete colorate di cui sopra con un tasso di cambio variabile è necessario:

1. Un modo per raccogliere informazioni sui prezzi concordate e immutabili, in modo che in qualsiasi momento una transazione di scambio possa utilizzare un prezzo che possa essere validato
2. Un modo per convertire gli input in output basati su quel prezzo
3. Un modo per verificare che il mittente di una transazione soddisfi gli stessi requisiti di qualsiasi altra transazione CryptoNote - vale a dire che conoscano la chiave segreta per gli input utilizzati e che possano quindi convertire utilizzando un tasso di cambio e una firma di transazione con una differenza corretta
4. Un modo per validare che il prezzo concordato sia stato effettivamente applicato allo scambio, senza divulgare eventuali importi ai validatori.

I dettagli sui prezzi sono ottenuti da un fornitore di prezzi del mondo reale (cioè un oracolo dei prezzi) e viene creato un record di prezzi in preparazione della risoluzione di un nuovo blocco. I record dei prezzi contengono i tassi di cambio (rispetto a XHV) per ciascuno dei pegging xAsset al momento dell'estrazione del blocco. Le informazioni sui prezzi vengono aggiornate a intervalli di 30 secondi e presentate al daemon Haven su richiesta. I record dei prezzi sono incorporati nella blockchain in ogni intestazione di blocco dal minatore che risolve quel particolare blocco.

Includendo queste informazioni in ogni blocco, il protocollo garantisce che il valore della transazione non possa essere manomesso o alterato in alcun modo: la blockchain garantisce che le informazioni sui prezzi siano immutabili. Se più blocchi vengono estratti con successo entro la durata di 30 secondi del record di prezzi attuale, lo stesso record verrà incluso in più blocchi.

Un record di prezzo contiene i seguenti tassi di conversione (tutti rispetto a XHV), nonché uno spazio riservato per future aggiunte e la firma dell'oracolo che fornisce i dati. Un esempio di record di prezzi è:


```
{
   "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
   }
}
```


*Pricing Record Example: Carbon*

2 / Haven esegue questa operazione nell'esempio che abbiamo utilizzato precedentemente [Bob], utilizzando coppie di impegni anziché singoli valori di impegno. Questo è anche il metodo utilizzato nell'esempio di giocattoli dei laboratori di ricerca Monero.

3/ Le transazioni Haven vengono firmate utilizzando CLSAG e bulletproof accoppiati come descritto sopra. Tuttavia, non firmiamo utilizzando la differenza come nell'esempio di giocattoli. Firmiamo utilizzando l'impegno originale a valori zero. Il nostro impegno è per una differenza di **valore** pari a zero.

4/ Qui è dove le cose si complicano. Per capire come Haven convalida o rifiuta le transazioni utilizzando una prova di valore si richiede un po' di lavoro preliminare e una certa comprensione degli algoritmi a chiave pubblica e di come CryptoNote utilizza le operazioni e i punti della curva ellittica per convalidare gli importi di input e output.

Ogni transazione passa attraverso la funzione verRctSemanticsSimple() che somma tutti gli input e gli output di una transazione per verificare che i risultati siano uguali. Sebbene i valori siano in questa fase completamente crittografati e rappresentati come punti della curva ellittica ["EC"] anziché come numeri reali, queste somme funzionano ancora a causa delle proprietà dell'aritmetica modulare e del modo specifico in cui i punti EC di Monero vengono scelti/generati.

In breve, sebbene i numeri siano crittografati, mantengono comunque determinate proprietà: le differenze tra loro (all'interno dello spazio EC) sono ancora valide, quindi una differenza zero sarà ancora una differenza zero perché gli impegni sono additivi.

In altre parole, se avessimo una transazione con input contenenti importi a1, ..., aj e output con importi b1, ..., bk, allora un osservatore si aspetterebbe giustificatamente che:

$$\sum_{j} a_j - \sum_{k} b_k = 0$$

Per Haven questo funzionerebbe ancora per i trasferimenti XHV e xUSD, ma per gli scambi questo è completamente errato.

Quindi, riutilizzando alcune notazioni dall'alto, definiamo le costanti γC, γD come il tasso di cambio per una singola transazione, tasso di cambio fornito dal nostro oracolo dei prezzi. E ora con impegni accoppiati nella nostra gamma di prove che sono rispettivamente (C, D). Per dimostrare l'uguaglianza di valore, richiediamo che la somma del valore degli input sia uguale alla somma del valore degli output.

La nostra convalida ora appare così:

$$\lambda C \left( \sum_{i} C_i - f_c G - \sum_{k} C'_k \right) = {}_{1/\lambda D} \left( \sum_{i} D_i - f_D G' - \sum_{k} D'_k \right)$$

Dove λC, λD indicano che i valori tra parentesi sono sommati in base ai rispettivi tassi di cambio. (C, D) indicano impegni di input, (C ', D') indicano impegni di output e *fxG* indica le commissioni pagate.

### v. Oracoli di prezzo

Per recuperare i dati dal mondo reale, le blockchain utilizzano un costrutto chiamato "oracolo". "Un oracolo blockchain è una fonte di informazioni di terze parti che ha la sola funzione di fornire dati alle blockchain"

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

Nella prima iterazione di Haven e in diversi progetti successivi da quel momento, la creazione di un oracolo sicuro, accurato e ad alte prestazioni era considerata la chiave del successo del protocollo. Tuttavia, dopo la creazione e il successo di servizi come Chainlink, progettati esclusivamente per fornire funzioni di oracolo e come fonte di dati indipendente, è ora chiaro che non solo non è necessario integrare un oracolo separato nel sistema Haven, ma non è neanche desiderabile farlo. Facendo così aumenterebbe la centralizzazione della parte più importante dell'equazione di conversione: i tassi di cambio.

Con questo in mente, Haven Protocol ha collaborato con Chainlink per utilizzare la loro rete di oracoli per l'elaborazione e la fornitura di dati sui prezzi. Gli oracoli Chainlink per XHV / USD possono essere visti di seguito

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

Haven ritiene che sia vitale costruire flessibilità nella determinazione dei prezzi sin dall'inizio, e come tale non si baserà esclusivamente su un singolo sistema di oracoli, ma sarà in grado di aggiungere, scambiare e rimuovere oracoli nel tempo per garantire che Haven utilizzi i migliori dati della classe ora e in futuro.

## Scenari di offerta

XHV è una moneta Proof-of-Work (PoW) pura con la stessa curva di emissione di Monero, ha una fornitura minabile iniziale di 18,4 milioni e una piccola emissione di coda una volta estratti quei 18,4 milioni di monete.

Questo è uno scenario di fornitura standard e ben compreso nel mercato delle criptovalute. Ora che la funzione di archiviazione offshore di Haven è attiva sulla rete principale, le cifre sopra continuano ad applicarsi ai premi minerari, ma non definiscono più l'effettiva fornitura circolante di XHV poiché la coniatura e bruciatura lo altereranno dinamicamente come discusso in precedenza.

Inoltre, una volta che ulteriori xAssets (oltre xUSD) sono attivi sulla rete, l'offerta circolante di XHV non definisce più la capitalizzazione di mercato totale dell'ecosistema Haven. Per questo, è necessario considerare il valore cumulativo degli xAssets tenuti e dello stesso XHV.

Questo può essere espresso come HNV o Haven Network Value e sarà calcolato come segue:

*HNV = (prezzo XHV * offerta circolante) + offerta circolante xUSD*

xAsset aggiuntivi possono essere facilmente aggiunti al calcolo man mano che vengono aggiunti alla rete.

Per comprendere la potenziale offerta futura di XHV e l'effetto di tale offerta sull'ecosistema Haven, vengono presentati i seguenti macro scenari di alto livello.

Le variabili considerate in questi scenari includono:

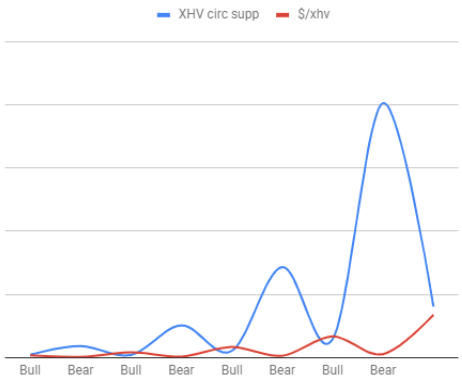
1. L'aumento della capitalizzazione di mercato totale in un ciclo rialzista (inc_Bull)
2. La diminuzione della capitalizzazione di mercato totale in un ciclo di mercato ribassista (dec_Bear)
3. La % di monete XHV inviate e conservate in offshore alla fine di un ciclo di mercato rialzista (perc_offBull)
4. La % di xAsset (utilizzando xUSD come esempio) monete restituite a XHV alla fine di ciclo di mercato ribassista (perc_onBear)
5. La % del valore ATH locale di XHV all'interno di un ciclo rialzista che è la media di valore di tutte le transazioni offshore (ad esempio, se l'ATH locale per XHV è $ 2,00, l'80% di tale ATH è $ 1,60 e questo sarebbe il valore utilizzato in questi scenari per l'offshoring se l'80% viene utilizzato per questa variabile) (perc_LATH)
6. La % del valore ATL locale di XHV all'interno di un ciclo ribassista che è la media di tutti i valori delle transazioni onshore. (perc_LATL) §
    a. * Nota: questi valori per 5 e 6 possono essere visti come l'accuratezza dei trader nel prevedere i massimi e i minimi dei mercati.
7. Indice di volatilità XHV: questo valore viene utilizzato per simulare quanto potrebbe essere correlata la volatilità di XHV rispetto alla volatilità di Bitcoin. Un valore di 1 è uguale alla volatilità di BTC, 0,5 è "metà volatile", 2 è due volte più volatile ecc.

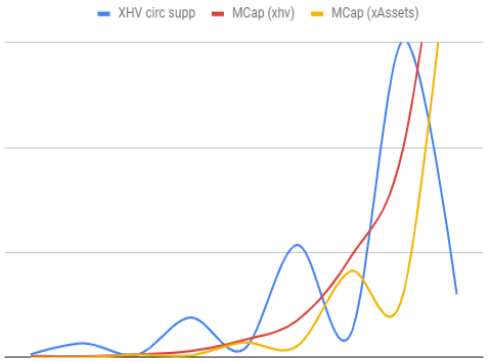
**Scenario 1**

## Espansione nella fornitura XHV

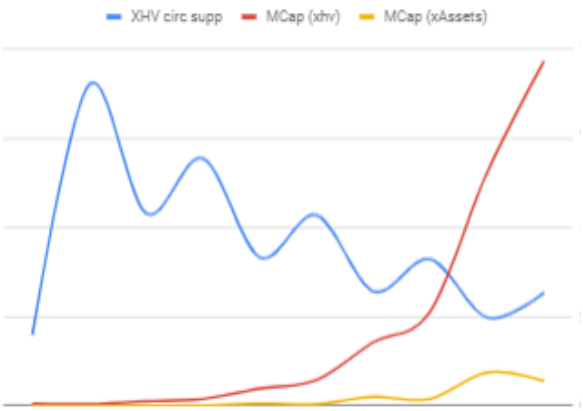
In questo scenario utilizziamo valori che aumenteranno l'offerta di XHV nel mercato nel tempo.

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




Come si può vedere in questo modello di utilizzo offshore estremamente pesante e con alta precisione di trading, l'uso della funzionalità offshore in uno scenario di espansione mantiene il prezzo di XHV contenuto, ma nel tempo aumenta la capitalizzazione di mercato sia di XHV che dell'ecosistema Haven nel suo complesso. Questo scenario è accettabile per l'ecosistema poiché abbassa la volatilità del prezzo XHV, che a sua volta altera i modelli mostrati e sposta lo scenario fuori dall'espansione e verso l'equilibrio (o addirittura contrazione) come si può vedere nei grafici sottostanti dove l'unico cambiamento ai valori usati sopra è iVol (0,5).

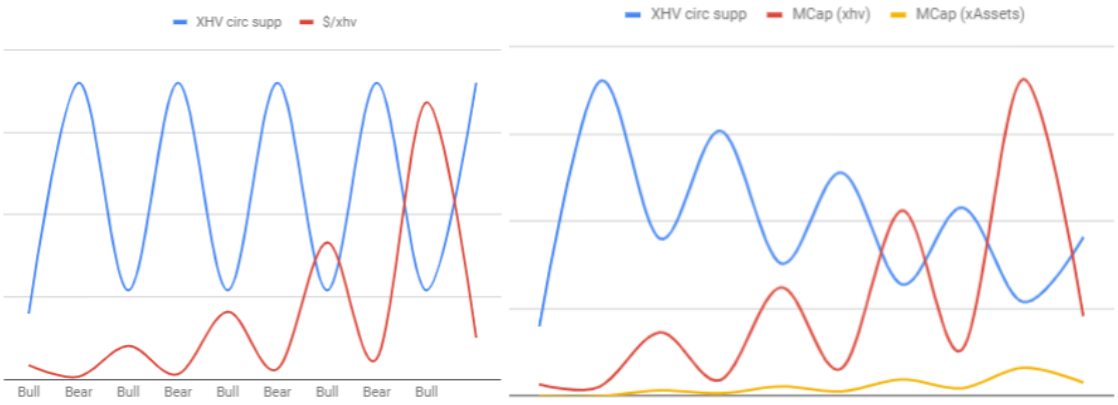



**Scenario 2**

Contrazione nella fornitura XHV

In questo scenario, vengono utilizzati valori che creano deliberatamente deflazione nella fornitura circolante di XHV.

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




Come si può vedere in uno scenario di contrazione, il prezzo di XHV aumenta in volatilità, creando nel tempo l'effetto opposto rispetto allo scenario di espansione e sposterà il pattern dalla contrazione all'equilibrio o all'espansione.

## Scenario 3

Equilibrio nell'offerta XHV

In questo scenario le variabili di previsione sono impostate con un uso medio dell'offshore e una precisione di trading media. Come punto centrale tra gli altri due scenari, ci si può aspettare che questo scenario si riproduca ripetutamente nel tempo, con scenari di espansione e contrazione entrambi tendenti all'equilibrio.

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


In conclusione, sebbene non sia possibile prevedere quale scenario si verificherà in un dato momento, il protocollo è progettato per adattarsi ai cambiamenti dei livelli di utilizzo espandendo e contraendo l'offerta di XHV direttamente attraverso le azioni dell'utente, creando una nuova e unica curva di offerta che deriva puramente da utilizzo naturale del protocollo.

## Stabilità ed economia

La coniatura e bruciatura richiedono poco per essere implementate in una forma basilare; solo un prezzo noto a cui eseguire la conversione e la possibilità di convertire un tipo di asset in un altro sulla stessa blockchain a quel tasso di conversione.

Per affermare l'ovvio, è un concetto molto semplice. Detto questo, i concetti più semplici a volte sono i più difficili da comprendere appieno e per garantire che l'ecosistema Haven utilizzi un modello economico robusto, è necessario affrontare alcune sfide.

1. Trasparenza dell'offerta.
2. Manipolazione dei prezzi sui siti di scambio
3. Dimostrazione e manutenzione del valore degli asset sintetici in un ecosistema algoritmico PoW.
4. Il potenziale per un "panico bancario" durante i periodi di più ampia volatilità del mercato

Queste sfide verranno affrontate una alla volta:

### Trasparenza dell'offerta

Il concetto originale di Haven era basato sull'avere una fornitura circolante sconosciuta di XHV e xAssets. Il motivo è stato quello di impedire la manipolazione della rete da parte di grandi possessori di XHV o xAssets.

Dopo molte considerazioni, discussioni nella comunità e consultazioni con consulenti esperti, è stato deciso che disporre di una fornitura circolare trasparente sarebbe effettivamente vantaggiosa per la rete nei seguenti modi:

- Consente a un monitoraggio più efficiente della rete Haven, il che significa che i tentativi di attacco e la manipolazione su larga scala possono essere rilevati e mitigati molto più velocemente.
- Offre agli utenti una maggiore sicurezza nel partecipare alla rete Haven con la possibilità di visualizzare il numero di XHV e xAssets in circolazione in un dato momento.
- Consente una maggiore visibilità e quindi una maggiore analisi sui siti web di metriche delle monete. Di conseguenza, per garantire precisione e visibilità, ogni transazione di coniatura e bruciatura verrà creata in modo tale che gli importi saranno rilevabili attraverso l'analisi della blockchain e visualizzati nei block explorer di Haven. Ciò consentirà agli utenti di mantenere la privacy e anonimato standard di Monero nei propri indirizzi di portafoglio, e allo stesso momento consentirà una visione chiara dell'offerta in circolazione.

L'offerta di ciascun tipo di asset è ora visibile e può essere visualizzata qui:

https://explorer.havenprotocol.org/supply

## Manipolazione dei prezzi sui siti di scambio

A causa della natura della coniatura e bruciatura, della promessa di lunga data di Haven che "1 xUSD sarà sempre rimborsabile per $ 1 di XHV" e dell'azione di livellamento dei prezzi delle medie mobili all'interno del sistema di prezzi di Haven, sono necessarie alcune misure per garantire che eventuali discrepanze tra i prezzi sui siti di scambio e le conversioni off/onshore siano ridotte al minimo.

Questa minimizzazione viene eseguita consentendo una scelta della priorità della transazione da parte dell'utente. Alle transazioni ad alta priorità, con tempi di sblocco minimi, verranno addebitate commissioni più elevate rispetto alle transazioni a bassa priorità con tempi di sblocco più lunghi (dove la commissione tenderà a quasi zero).

Dal primo lancio, i collaboratori di Haven hanno monitorato e analizzato i dati ottenuti dall'attività nel primo mese di utilizzo nel mondo reale. Dal primo lancio, la struttura tariffaria originale è stata sostituita da uno schema molto più semplice e rigoroso per garantire la salute della rete a breve termine mentre la distribuzione dei token è con i primi titolari. Nel tempo, Haven prevede che le tariffe e le loro strutture richiederanno una revisione e una modifica per lavorare insieme alla maturità della rete Haven. La struttura tariffaria completa per la rete Haven sarà pubblicata insieme a questo documento e mantenuta per riferimento in ogni momento sul sito Web del protocollo Haven. https://havenprotocol.org/fees

Uno dei problemi con molti prodotti DeFi esistenti è che uno deve avere un particolare token nel proprio portafoglio per poter effettuare transazioni in un altro. Ciò può causare attriti inutili e costi solo per l'utilizzo.

Le transazioni Haven superano questo problema addebitando le commissioni nella valuta inviata. Questo è mostrato nella tabella seguente:

| Tipo di transazione | Tipo di commissione | Commissione pagata in: |
|---|---|---|
| Trasferimento XHV | Commissione standard | XHV |
| Trasferimento xUSD | Commissione standard | xUSD |
| Scambio XHV -> xUSD | Commissione scambio + Commissione standard | XHV |
| Scambio xUSD -> XHV | Commissione scambio + commissione standard | xUSD |

## Dimostrazione e mantenimento del valore delle risorse sintetiche in un ecosistema algoritmico PoW

Una delle maggiori sfide delle risorse sintetiche algoritmiche, nonché una delle domande più frequenti, è incentrata sul concetto di "valore reale" o "fonte di valore". Domande come "come puoi affermare che xUSD vale $ 1 se non ha garanzie collaterali?" vengono chieste spesso dagli utenti.

Una volta che la domanda è stata risolta e compresa (xUSD è "indirettamente sostenuto" da una quantità variabile e appropriata di XHV), gli utenti si concentrano sulle domande sull'offerta e sulla liquidità di XHV stesso. Poiché l'offerta di XHV fluttuerà a causa delle transazioni offshore come descritto sopra, sia i casi di espansione che di contrazione dell'offerta cambieranno potenzialmente le dinamiche dell'intero ecosistema.

Con ogni probabilità, tenendo conto della natura ciclica dei mercati delle criptovalute, il potenziale per entrambi i casi è alto. Questo è sia previsto che auspicabile. Le fluttuazioni nell'offerta circolante sono assolutamente necessarie per consentire l'espansione e la contrazione dell'offerta xUSD senza creare una volatilità sempre maggiore nel prezzo di XHV.

### Il potenziale per un “panico bancario" durante i periodi di più ampia volatilità del mercato

Durante i cicli di mercato in aumento ("mercati rialzisti") in qualsiasi merce, i trader spesso lasciano opzioni stabili a favore di asset volatili e viceversa. Con qualsiasi moneta stabile "supportata" in modo tradizionale come USDT, la quantità di sostegno è la chiave per la stabilità della criptovaluta supportata. Qualsiasi deviazione del valore "supportato" dal valore di mercato crea un pericolo reale per gli utenti e crea una situazione in cui esiste un potenziale per valore non supportato e perdita di ancoraggio con la valuta che la criptovaluta dovrebbe garantire.

Haven non soffre di questo problema a causa del suo uso di coniatura e bruciatura e di valute colorate.

**In ogni momento e in tutte le situazioni un utente può riscattare 1 xUSD per $ 1 di XHV. Questo gancio non si romperà mai.**

Poiché il protocollo Haven è implementato utilizzando un modello di moneta colorata, è in grado di supportare non solo xUSD, ma anche una serie di altri asset e materie prime che chiamiamo "xAssets". Ciò consente a XHV stesso di diventare il collaterale non solo di uno, ma di un insieme di risorse sintetiche private, estendendo i meccanismi di pegging possibili e trasformando il protocollo in una piattaforma con vero caso d'uso e valore per gli utenti di criptovalute.

## Chi è il team Haven?

Il team Haven è una comunità collettiva di sviluppatori e collaboratori e come tale accoglie tutti gli input e i contributi di qualsiasi parte.

Il team di sviluppo principale è elencato di seguito.

Da quando ha assunto la gestione e lo sviluppo della moneta dagli sviluppatori originali, la comunità ha beneficiato del supporto e della guida continua di diversi consulenti e professionisti del settore tecnologico che hanno fatto della loro missione mantenere la promessa di Haven e guidare l'adozione di questa parte critica del panorama delle criptovalute. Il continuo supporto e contributo di queste persone sono molto apprezzati.

**Team di svilippo principale:**

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

David è un tecnologo specializzato nella fornitura di prodotti e strategia, ha ricoperto posizioni senior nelle principali società del Regno Unito e in molteplici startup tecnologiche negli ultimi 20 anni. Con un background in matematica, tecnologia di crittografia e sviluppo di software, David porta in Haven una notevole esperienza sia nella fornitura tecnica che nella governance su larga scala.

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

Neil è uno sviluppatore di software full stack. Con oltre 20 anni di esperienza nello sviluppo in X86 Assembler, C ++, Java, PHP e Javascript, Neil ha trascorso gli ultimi 18 anni progettando e costruendo software crittografici.

@Marty (anoniem)

Marty è uno sviluppatore front-end con esperienza in una moltitudine di framework e lo mette in primo piano con il suo lavoro sui wallet e sui siti web di Haven.

@Pierre Lafitte (anoniem)

Pierre è specializzato nella progettazione di prodotti e crea tutti i percorsi degli utenti e le interfacce nella gamma di prodotti Haven. Pierre è un esperto sviluppatore di criptovalute Front End, contribuisce da molto tempo ad Haven e guiderà il lato UX / UI dello sviluppo e porterà le visioni UX del team alla realtà.