Protokol Haven
Keuangan Swasta yang Terdesentralisasi

Protokol Core v3.0

Makalah ini dimaksudkan untuk mendokumentasikan fungsionalitas core yang ditawarkan oleh Protokol Haven. Fungsi layer kedua lainnya tidak tercakup dalam makalah ini, dan akan dibahas secara terpisah berdasarkan kasus per kasus.

Pendahuluan

Bitcoin membuka jalan bagi mata uang elektronik peer-to-peer. Bitcoin merupakan mata uang digital pertama yang berhasil mengimplementasikan buku besar transaksi terdistribusi berdasarkan bukti kriptografi atas kepercayaan. Baru-baru ini, dengan kesadaran bahwa semua dompet dan transaksi dalam banyak mata uang digital dapat dilihat oleh semua orang yang peduli untuk melihatnya, permintaan untuk transaksi pribadi dan koin privasi telah meningkat. Haven dibangun di atas Monero, yang secara luas dianggap sebagai pemimpin dalam teknologi privasi. Oleh karena itu, Haven mewarisi semua fitur privasi Monero, termasuk tanda tangan cincin dan Anti Peluru. Ini memperluas fungsionalitas tersebut dengan menyediakan mata uang dan komoditas sintetis pribadi, anonim, dan sintetis (xAssets) yang hanya dapat ada melalui "pembakaran" mata uang dasar Haven - XHV. Haven juga memperluas bukti kesepadanan Monero, untuk memungkinkan beberapa jenis aset disamakan berdasarkan nilai moneternya daripada hanya jumlah koin yang dipertukarkan, menciptakan set mata uang dan aset sintetis yang sepenuhnya privat dan pertama kali ada.

Selamat datang di Haven - Keuangan Swasta yang Terdesentralisasi.

Riwayat Proyek

Konsep Haven dimulai oleh dua pengembang pada awal tahun 2018. Upaya pertama ini mencapai tahap testnet publik sebelum kelemahan dalam solusi, jeda dalam pengembangan, dan kurangnya kemajuan dari pengembang asli membuat masa depan proyek diragukan. Pada akhir Januari 2019, kumpulan anggota komunitas Haven yang asli mengambil alih proyek ini dengan tujuan untuk menyelesaikan proyek, memberikan mekanisme penyimpanan lepas pantai, dan membangun infrastruktur pendukung untuk mendapatkan adopsi massal dari utilitas yang sangat dibutuhkan di pasar mata uang kripto yang berkembang pesat.
Mainnet dari Protokol Haven diluncurkan dengan sukses pada tanggal 20 Juli 2020 dengan memperkenalkan mata uang privat pertama xUSD ke pasar.

Protokol Haven

Janjinya: 1 xUSD akan selalu dapat ditukarkan dengan XHV senilai $1.00.

i. Konsep

Haven adalah mata uang kripto yang tidak dapat dilacak dengan perpaduan harga pasar standar dan dunia nyata
penyimpanan nilai yang dipatok dengan aset. Hal ini dicapai melalui proses 'mint and burn' dalam satu blockchain. Dalam kasus yang paling sederhana, pengguna dapat membakar Haven (XHV) dengan nilai USD yang setara dengan nilai Haven Dollars (xUSD). Atau, untuk mengembalikan ke kondisi yang tidak stabil, pengguna dapat membakar xUSD untuk XHV senilai $1 USD.

Mata uang fiat utama lainnya termasuk GBP, EUR dan CNY, serta Perak, Emas, dan komoditas terkenal lainnya seperti Minyak dimaksudkan untuk ditambahkan ke ekosistem Haven dari waktu ke waktu agar pengguna dapat memilih mekanisme pegging yang sesuai dengan kebutuhan mereka.

ii. Proses Offshore - "Mint dan Bakar"

Haven menggunakan sistem yang disebut "mint and burn" untuk mempertahankan hubungan nilainya terhadap patokan asetnya. Dalam praktiknya, dengan menggunakan Dolar AS sintetis (xUSD) sebagai contoh, cara kerjanya adalah sebagai berikut: Bob memutuskan bahwa ia ingin menempatkan 200 Haven (XHV) miliknya ke dalam Penyimpanan Offshor Ketika pengguna memasukkan XHV ke dalam Penyimpanan Offshore, mereka membakar koin XHV dan mencetak nilai saat ini dari XHV tersebut sebagai xUSD baru. Offshore Storage menentukan nilai pasar saat ini dari Haven tersebut (dalam xUSD) berdasarkan rata-rata tertimbang volume di seluruh bursa yang didukung. Hal ini dilakukan dengan menggunakan harga oracle (mekanisme untuk menemukan data dunia nyata dan membuat data ini tersedia untuk blockchain) untuk mengambil data harga untuk ekosistem Haven secara penuh dan membuat catatan harga.

Jika nilai Haven saat ini adalah $1 USD, penyimpanan luar negeri akan membakar 200 XHV milik Bob dengan membuat transaksi khusus di mana 200 XHV yang telah dikirim kemudian dibakar menjadi xUSD dan total pasokan XHV berkurang. Jika harga pasar XHV kemudian bergerak ke $2 USD dan Bob memutuskan untuk mengakses penyimpanan luar negerinya, dia akan mendapatkan kembali 100 XHV (100 * $2 = $200 USD sesuai dengan nilai aslinya).

Jika hal sebaliknya terjadi dan harga Haven turun menjadi $0,50, maka 400 XHV akan dicetak dan dikirim ke Bob (400 * $0,50 = $200 USD sesuai dengan nilai aslinya). Jelas, penggunaan mint dan burn mengubah sirkulasi pasokan aset dasar secara dinamis.

Hal ini menciptakan skenario pasokan yang menarik - sangat berbeda dengan mata uang kripto lainnya - yang perlu ditinjau oleh pembaca secara menyeluruh untuk memahami sepenuhnya konsep Haven Protocol.

iii. Bagaimana Cara Kerja Offshoring Sebenarnya?

Protokol Haven memungkinkan transaksi luar negeri di dalam Haven Vault menggunakan model 'koin berwarna'. Ini adalah implementasi pertama dari koin berwarna pada protokol Cryptonote. Konsep koin berwarna sudah dikenal dan didefinisikan dalam jaringan Bitcoin, dan dijelaskan sejak tahun 2013 di sini:

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

Akan tetapi, koin berwarna pada Cryptonote tidak dapat bekerja dengan cara yang sama seperti Bitcoin, dan pada kenyataannya konsep koin berwarna dalam Cryptonote harus dikerjakan ulang dan ditata ulang. Terima kasih kepada Nate Eldredge untuk penjelasan yang jelas mengenai perbedaan antara implementasi menggunakan Bitcoin dan Monero:

"Dengan Bitcoin, ada korespondensi satu-ke-satu antara input dan output transaksi. Misalkan ada transaksi X dengan output X1 yang mengirimkan 1 satoshi ke alamat A milik Alice, dan semua orang setuju bahwa output X1 diwarnai sehingga memberikan hak kepemilikan atas mobil Chevy Nova tahun 1977 milik Alice. Jika Alice memutuskan untuk memberikan mobil tersebut kepada Bob, dia membuat transaksi baru Y, dengan input yang mengarah ke X1, dan satu-satunya output Y1 yang mengirimkan 1 satoshi ke alamat Bob di B. Sekarang Bob dapat membuktikan, dengan membuat tanda tangan yang sesuai dengan alamatnya di B, bahwa dia adalah pemilik sah mobil tersebut.

Jika Mallory mencoba untuk mengklaim mobil tersebut dengan membuat sebuah transaksi yang berbeda dengan input X1, ia akan ketahuan, karena ia tidak dapat menandatangani transaksi tersebut dengan kunci pribadi Alice, sehingga tidak akan terverifikasi. Jika Alice mencoba memberikan mobil tersebut kepada orang lain dengan membuat transaksi kedua yang ditandatangani dengan benar, yaitu Z dengan input X1, maka transaksi tersebut akan terdeteksi sebagai pengeluaran ganda karena ada transaksi lain yang menggunakan X1 yang mendahuluinya dalam blockchain.

Dengan tanda tangan dering, korespondensi ini rusak. Saat membuat transaksi, selain satu keluaran (dari transaksi sebelumnya) yang benar-benar ingin Anda keluarkan, Anda dapat mencantumkan banyak keluaran lainnya. Anda membuat tanda tangan yang membuktikan bahwa Anda memiliki wewenang untuk membelanjakan salah satu keluaran yang Anda daftarkan, tetapi tidak memberikan informasi apa pun tentang keluaran yang mana. Akan tetapi, algoritme penautan memastikan bahwa setiap upaya di masa depan untuk membelanjakan keluaran itu lagi akan diketahui dan ditolak.

Dalam skenario di atas, jika Alice menggunakan tanda tangan cincin pada transaksi Y-nya, termasuk tidak hanya X1 tetapi juga keluaran lain Z1, maka tanda tangannya tidak akan membuktikan bahwa ia berhak membelanjakan X1 (dan oleh karena itu adalah pemilik sah mobil dan dapat memberikannya); tanda tangan tersebut hanya akan membuktikan bahwa ia berhak atas X1 atau Z1.

Lebih jauh lagi, Mallory dapat membuat sebuah transaksi M yang mencakup X1 dan output lain K1 yang berhak ia belanjakan. Karena ia memiliki private key yang sesuai dengan K1, ia dapat menandatangani transaksi M dengan benar, tetapi tidak jelas apakah ia membelanjakan X1 (yang akan memberikan hak milik atas mobil tersebut) atau K1 (yang tidak)."

Penjelasan di atas menjelaskan bagaimana koin berwarna dilihat dan diimplementasikan di dalam jaringan Bitcoin, dan dengan tepat menunjukkan bahwa model ini gagal ketika X1 dan Z1 masih ada setelah transaksi awal. Akan tetapi, Haven bekerja dengan cara yang sedikit berbeda. Haven tidak memiliki Alice, dan kita juga tidak memiliki Mallory. Yang kita miliki hanyalah Bob.

Ketika Bob mengonversi dari XHV ke xUSD, ia mengirimkan sebuah transaksi dengan dua warna, X (XHV) dan Z (xUSD). Transaksi ini hanya menerima koin dengan warna pertama X, dan memiliki output X dan warna kedua Z. Setiap transaksi dalam jaringan Haven berisi dua nilai untuk setiap tujuan (#X,#Z), dan untuk semua transaksi, hanya satu dari nilai ini yang tidak boleh nol untuk setiap tujuan.

Jadi, ketika Bob mengonversi 200 XHV miliknya dengan harga $1,00 per XHV, ia mengirimkan transaksi dengan input (200,0) dan tujuan nilai (0,200) sehingga menghasilkan output 200 xUSD dan 0 XHV. Jika harga XHV kemudian bergerak ke $2 per XHV maka konversi kembali ke XHV akan mengirimkan transaksi dengan input (0,200) dan nilai tujuan (100,0) yang menghasilkan output 100 XHV dan 0 xUSD. Dengan cara ini, input ke transaksi dan UTXO secara permanen dan efektif dibakar secara atomik dan real time selama proses transaksi, dan output dicetak dengan cara yang sama.
Ini semua bagus, namun Haven adalah fork dari Monero dan mewarisi semua fitur keamanan dan anonimitasnya... dan Monero dibangun di atas premis, kondisi, dan jaminan mutlak bahwa untuk setiap

transaksi; selisih antara input dan output adalah nol. Setiap transaksi yang tidak memenuhi persyaratan ini akan selalu gagal.

Dalam kasus Haven, aspek fundamental Monero ini tidak mungkin benar, dan pada kenyataannya untuk setiap pertukaran antara XHV dan xUSD di mana harga XHV tidak tepat $ 1,00, aturan ini benar-benar rusak, input dan output tidak akan sama, begitu juga dengan jumlah komitmen C^a dan C^b dan akibatnya *src/ringct/rctSigs.cpp verRctSemanticsSimple()* akan gagal dalam pengujian Monero:

$$\sum_{j}^{a} C_j \quad - \sum_{t} C^b{}_t = 0$$

Di sini kami memperkenalkan konsep dalam jaringan Haven tentang 'Bukti Nilai'.

Terima kasih diberikan kepada Monero Research Lab untuk makalah mereka tentang Tanda Tangan Cincin yang Dapat Ditautkan Ringkas dan Pemalsuan Terhadap Kunci Musuh [Brandon Goodell, Sarang Noether, dan Arthur Blue] https://eprint.iacr.org/2019/654.pdf ['makalah'] yang telah digunakan sebagai bagian dari implementasi Haven dari Bukti Nilai.

Dalam draf awal 'makalah', para penulis mengusulkan model 'mainan' di mana mereka membuat mata uang berwarna dengan pasak tetap di antara dua warna: dolar dan sen dengan nilai tukar 100: 1 di antara keduanya, dan menunjukkan bagaimana hal ini dapat dilakukan dengan menggunakan CLSAG. Prosesnya adalah sebagai berikut:

1. Tentukan nilai tukar dengan menentukan konstanta ξ dan beberapa konstanta γC , γD pada 1, 2, . . 2 ξ-1, (dalam contoh ini, γC = 100 dan γD = 1).
2. Mengubah struktur komitmen sehingga setiap komitmen sekarang menjadi sepasang komitmen C dan D dengan warna yang sesuai
3. Buat sebuah bukti rentang dari Prove yang mencakup nilai C dan D. Di sini, C dan D berperan sebagai titik Zj, dan P adalah data tambahan yang diperlukan untuk protokol transaksi.
4. Kunci transaksi sederhana dikatakan valid jika hal-hal berikut ini terpenuhi:
    a. setiap anggota ring input (Xi , Ci , Di , Pi) ∈ Q memiliki bukti rentang yang valid Pi sehingga Ver(Pi) = 1; dan
    b. setiap bukti rentang keluaran P 0 k valid sehingga Ver(P 0 k) = 1; dan
    c. untuk cincin yang dimodifikasi pk = X1 X2 - - - Xn Z1 Z2 - - - Zn tanda tangan σ lolos verifikasi 2-CLSAG, Verifikasi (m, pk, σ) = 1.

Efek dari hal ini adalah bahwa transaksi ditandatangani bukan dengan komitmen untuk nol, tetapi komitmen untuk selisih - selisih tersebut adalah perbedaan jumlah 'koin/token' yang dihasilkan oleh transaksi ini berdasarkan input dan output. Jika pengguna menukarkan 1 USD dengan 100 sen, selisihnya adalah 99 - jumlah koin baru yang dicetak. Model ini bekerja karena agar pengirim dapat menandatangani menggunakan selisih tersebut, pengguna HARUS mengetahui jumlah koin yang digunakan sebagai input (yang hanya dapat diketahui oleh pemegang private key dari input tersebut) dan mereka harus menggunakan nilai tukar yang tepat yaitu 100:1, dengan semua bulletproof yang memiliki nilai kedua warna tersebut. Dengan melakukan hal tersebut, mereka dapat menandatangani dengan benar menggunakan selisih antara input dan output, dan transaksi akan tervalidasi.

Model di atas memiliki satu kelemahan utama ketika mempertimbangkan sistem mint dan burn Haven. Sistem ini membutuhkan nilai tukar yang tetap. Tetap dan diketahui oleh kedua belah pihak yang bertransaksi, dan juga tetap dan diketahui oleh semua validator transaksi. Hal ini menciptakan masalah bagi kita, dan model ini tidak akan bekerja karena menurut definisi untuk mematok aset yang tidak stabil ke aset yang stabil, hal yang harus berubah adalah nilai tukar.

iv. Proof of Value.

Untuk membuat model koin berwarna di atas berfungsi dengan nilai tukar variabel, diperlukan nilai tukar yang bervariasi:

1. Cara untuk mengumpulkan informasi harga yang disepakati dan tidak dapat diubah, sehingga pada waktu tertentu, transaksi pertukaran dapat menggunakan harga yang dapat divalidasi
2. Cara untuk mengubah input menjadi output berdasarkan harga tersebut
3. Sebuah cara untuk memvalidasi bahwa pengirim transaksi memenuhi persyaratan yang sama dengan transaksi kriptonote lainnya - yaitu bahwa mereka mengetahui kunci rahasia dari input yang digunakan, dan oleh karena itu dapat mengkonversi menggunakan nilai tukar dan menandatangani transaksi dengan selisih yang benar
4. Sebuah cara untuk memvalidasi bahwa harga yang telah disepakati memang telah diterapkan pada bursa, tanpa mengungkapkan jumlah apa pun kepada validator.

Rincian harga diperoleh dari penyedia harga dunia nyata (yaitu harga oracle) dan catatan harga dibuat sebagai persiapan untuk blok baru yang sedang diselesaikan. Catatan harga berisi nilai tukar (terhadap XHV) untuk setiap pasak xAsset pada saat blok ditambang. Informasi harga diperbarui pada interval 30 detik, dan disajikan ke daemon Haven berdasarkan permintaan. Catatan harga disematkan ke dalam blockchain di setiap header blok oleh penambang yang menyelesaikan blok tersebut.

Dengan menyertakan informasi ini di setiap blok, protokol menjamin bahwa nilai transaksi tidak dapat dirusak atau diubah dengan cara apa pun - blockchain menjamin bahwa informasi harga tidak dapat diubah. Jika beberapa blok berhasil ditambang dalam waktu 30 detik dari catatan harga saat ini, catatan yang sama akan dimasukkan ke dalam beberapa blok.

Catatan harga berisi tingkat konversi berikut (semua terhadap XHV), serta beberapa ruang yang dicadangkan untuk penambahan di masa mendatang dan tanda tangan oracle yang menyediakan data. Contoh catatan harga adalah:


```
{
   "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
   }
}
```


Contoh Pencatatan Harga: Karbon

2/ Haven melakukan hal ini dalam contoh di atas [Bob] menggunakan pasangan komitmen daripada nilai komitmen tunggal. Ini juga merupakan metode yang digunakan dalam contoh mainan dari laboratorium penelitian Monero.

3/ Transaksi Haven ditandatangani menggunakan CLSAG dan bulletproof yang dipasangkan seperti yang dijelaskan di atas. Namun, kita tidak menandatangani menggunakan selisih seperti pada contoh mainan. Kami menandatangani menggunakan komitmen awal dengan nilai nol. Komitmen kami adalah pada selisih **nilai** nol.

4/ Di sinilah letak kerumitannya. Untuk memahami bagaimana Haven memvalidasi atau menolak transaksi menggunakan bukti nilai membutuhkan sedikit pekerjaan awal dan pemahaman tentang algoritma Public Key, dan bagaimana Cryptonote menggunakan operasi Elliptic Curve dan poin untuk memvalidasi jumlah input dan output.

Setiap transaksi melewati fungsi *verRctSemanticsSimple()* yang menjumlahkan semua input dan output dari sebuah transaksi untuk memeriksa apakah hasilnya sama. Meskipun nilai pada tahap ini sepenuhnya dienkripsi dan direpresentasikan sebagai titik-titik Elliptic Curve ['EC'] dan bukan bilangan real, jumlah ini masih berfungsi karena sifat aritmatika modular dan cara spesifik titik-titik EC Monero dipilih/dihasilkan.

Singkatnya, meskipun angka-angka tersebut dienkripsi, mereka masih memiliki sifat tertentu - perbedaan di antara mereka (dalam ruang EC) masih valid, sehingga perbedaan nol akan tetap menjadi perbedaan nol karena komitmen bersifat aditif.

Dengan kata lain, jika kita memiliki transaksi dengan input yang berisi jumlah a_1 , ..., a_j dan output dengan jumlah b_1 , ..., b_k , maka pengamat dapat mengharapkan hal tersebut:

$$\sum_j aj - \sum_k bk = 0$$

Untuk Haven, ini masih bisa digunakan untuk transfer XHV, dan transfer xUSD, tetapi untuk pertukaran, ini sama sekali tidak benar.

Jadi, dengan menggunakan kembali beberapa notasi di atas, mari kita definisikan konstanta γC, γD sebagai nilai tukar untuk *satu* transaksi, nilai tukar tersebut disediakan oleh pricing oracle kita. Dan sekarang dengan komitmen yang dipasangkan dalam pembuktian rentang kita masing-masing adalah (C, D). Untuk membuktikan kesetaraan nilai, kita membutuhkan jumlah nilai input sama dengan jumlah nilai output.

Validasi kami sekarang terlihat seperti ini:

$$\lambda C \left(\sum_i Ci - f_c \, \mathrm{G} - \sum_k C'_k \right) = 1/\lambda D \left(\sum_i Di - f \, \mathrm{DG}' - \sum_k D'_k \right)$$

Di mana *λC*, *λD* menandakan bahwa nilai dalam tanda kurung dijumlahkan berdasarkan nilai tukar masing-masing. (C,D) menunjukkan komitmen input, (C',D') menunjukkan komitmen output, dan *fxG* menunjukkan biaya yang dibayarkan.

v. Harga Oracle

Untuk mengambil data dari dunia nyata, blockchain menggunakan sebuah konstruksi yang disebut dengan "oracle". "Oracle blockchain adalah sebuah sumber informasi pihak ketiga yang memiliki fungsi tunggal untuk memasok data ke dalam blockchain"

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

Pada iterasi pertama Haven dan beberapa desain berikutnya sejak saat itu, penciptaan oracle yang aman, akurat, dan berkinerja tinggi dianggap sebagai kunci keberhasilan protokol. Akan tetapi, sejak penciptaan dan keberhasilan layanan seperti Chainlink, yang dirancang murni untuk menyediakan fungsi oracle sebagai sumber data independen, sekarang jelas bahwa tidak hanya oracle yang terpisah tidak perlu dibangun ke dalam sistem Haven, tetapi juga tidak diinginkan untuk melakukannya. Melakukan hal tersebut akan meningkatkan sentralisasi bagian terpenting dari persamaan konversi - penetapan harga.

Dengan pemikiran ini, Haven Protocol telah berkolaborasi dengan Chainlink untuk memanfaatkan jaringan oracle mereka untuk pemrosesan dan penyediaan data harga. Oracle Chainlink untuk XHV/USD dapat dilihat di bawah ini

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

Haven percaya bahwa sangat penting untuk membangun fleksibilitas dalam penentuan harga sejak awal, dan dengan demikian tidak hanya bergantung pada satu sistem oracle, tetapi akan dapat menambah, menukar, dan menghapus oracle dari waktu ke waktu untuk memastikan Haven menggunakan data terbaik di kelasnya saat ini, dan di masa depan.

Skenario Pasokan

XHV adalah koin Proof-of-Work (PoW) murni dengan kurva emisi yang sama dengan Monero, XHV memiliki pasokan awal yang dapat ditambang sebanyak 18,4 juta dan emisi ekor kecil setelah 18,4 juta koin tersebut ditambang.

Ini adalah skenario pasokan standar yang sudah dipahami dengan baik di pasar mata uang kripto. Sekarang setelah fitur penyimpanan luar negeri Haven aktif di mainnet, angka-angka di atas terus berlaku untuk reward penambangan, tetapi tidak lagi menentukan pasokan XHV yang beredar secara aktual karena mint dan burn akan mengubahnya secara dinamis seperti yang telah dibahas sebelumnya.

Selain itu, setelah xAssets lebih lanjut (di luar xUSD) ditayangkan di jaringan, pasokan XHV yang beredar tidak lagi menentukan kapitalisasi pasar total ekosistem Haven. Untuk itu, perlu mempertimbangkan nilai kumulatif xAssets yang dimiliki serta XHV itu sendiri.

Ini dapat dinyatakan sebagai HNV atau Nilai Jaringan Haven dan akan dihitung sebagai

berikut: HNV = (harga XHV * pasokan yang beredar) + pasokan yang beredar xUSD

xAssets tambahan dapat dengan mudah ditambahkan ke dalam perhitungan saat ditambahkan ke jaringan.

Untuk memahami potensi pasokan XHV di masa depan dan pengaruh pasokan tersebut terhadap ekosistem Haven, skenario makro tingkat tinggi berikut ini disajikan.

Variabel yang dipertimbangkan dalam skenario ini meliputi:

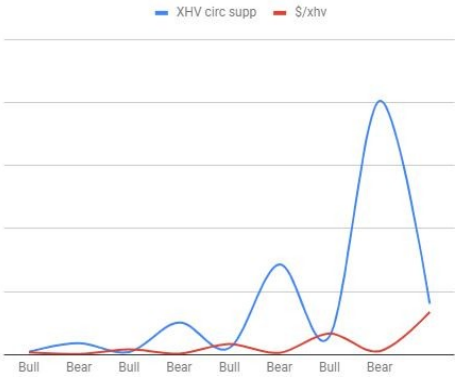
1. Peningkatan total kapitalisasi pasar dalam siklus kenaikan pasar (inc_Bull)
2. Penurunan total kapitalisasi pasar dalam siklus bearish pasar (dec_Bear)
3. Persentase koin XHV yang dikirim ke dan disimpan di luar negeri pada akhir siklus pasar naik (perc_offBull)
4. Persentase koin xAsset (menggunakan xUSD sebagai contoh) yang di-shipback ke XHV pada akhir siklus pasar turun (perc_onBear)
5. Persentase nilai ATH lokal XHV dalam siklus bullish yang merupakan rata-rata dari semua nilai transaksi luar negeri (Misalnya, jika ATH lokal untuk XHV adalah $2,00 maka 80% dari ATH tersebut adalah $1,60 dan ini akan menjadi nilai yang digunakan dalam skenario ini untuk offshoring jika 80% digunakan untuk variabel ini) (perc_LATH)
6. Persentase nilai ATL lokal XHV dalam siklus bearish yang merupakan rata-rata dari semua nilai transaksi darat. (perc_LATL) §
    a. **Catatan: Nilai-nilai untuk 5 & 6 ini dapat dilihat sebagai seberapa akurat trader saat memprediksi puncak dan dasar pasar.*
7. Indeks volatilitas XHV - nilai ini digunakan untuk mensimulasikan seberapa besar korelasi volatilitas XHV dibandingkan dengan volatilitas Bitcoin. Nilai 1 sama dengan volatilitas BTC, 0,5 berarti 'setengah lebih volatil', 2 berarti dua kali lebih volatil, dan seterusnya.

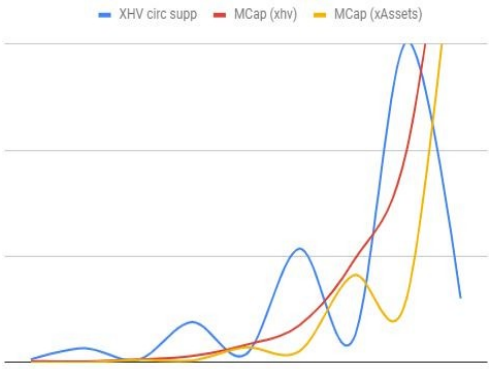
Skenario 1

Ekspansi dalam Pasokan XHV

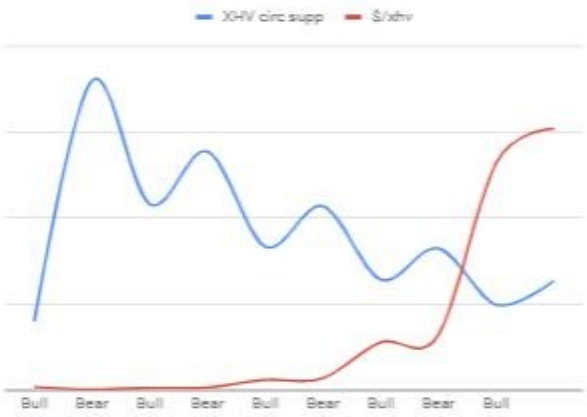
Dalam skenario ini kami menggunakan nilai yang akan meningkatkan pasokan XHV di pasar dari waktu ke waktu.

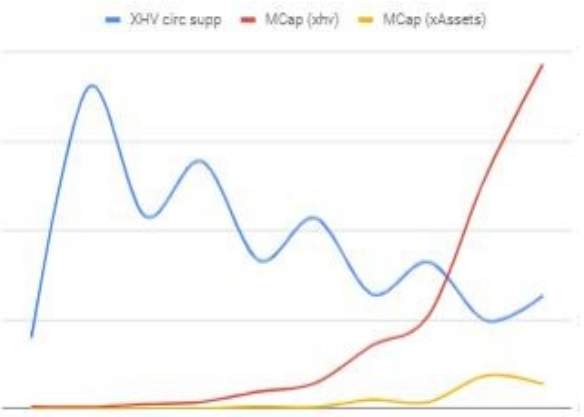
inc_Bull = 2500%
dec_Bear = 85%
perc_offBull = 80
perc_onBear = 75
perc_LATH = 90
perc_LATL = 10
iVol = 1.0





Seperti yang dapat dilihat dalam model penggunaan offshore yang sangat besar dan akurasi perdagangan yang tinggi ini, penggunaan fungsi offshore dalam skenario ekspansi membuat harga XHV tetap rendah, tetapi seiring waktu meningkatkan kapitalisasi pasar XHV dan ekosistem Haven secara keseluruhan. Skenario ini dapat diterima oleh ekosistem karena menurunkan volatilitas harga XHV, yang pada gilirannya mengubah pola yang ditunjukkan dan memindahkan skenario keluar dari ekspansi, dan menuju keseimbangan (atau bahkan kontraksi) seperti yang dapat dilihat pada grafik di bawah ini di mana satu-satunya perubahan pada nilai yang digunakan di atas adalah pada iVol (0,5).



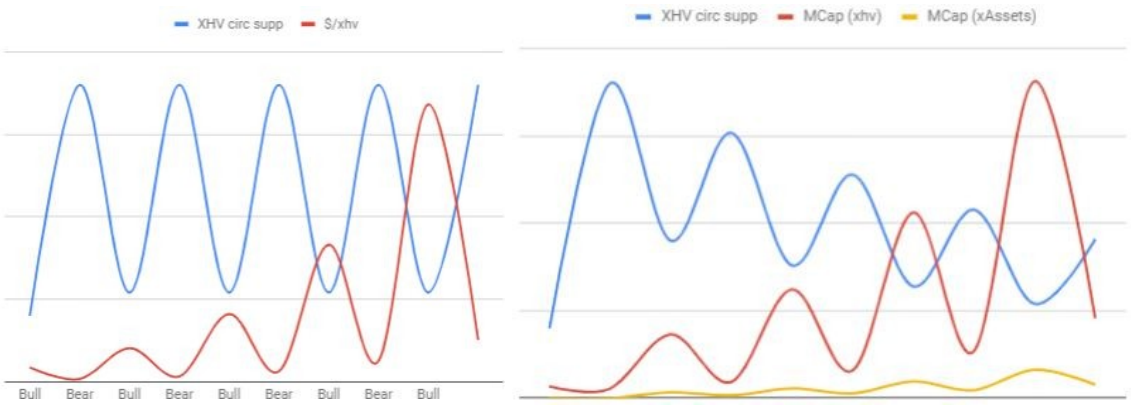


Skenario 2

Kontraksi dalam Pasokan XHV

Dalam skenario ini, nilai yang digunakan adalah nilai yang secara sengaja menciptakan deflasi dalam sirkulasi pasokan XHV.

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



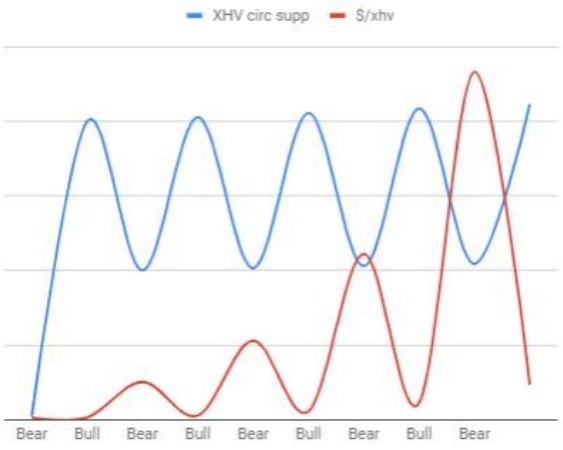
Seperti yang dapat dilihat dalam skenario kontraksi, harga XHV meningkat dalam volatilitas, menciptakan efek yang berlawanan dari skenario ekspansi dari waktu ke waktu dan akan memindahkan pola dari kontraksi menuju keseimbangan atau ekspansi.

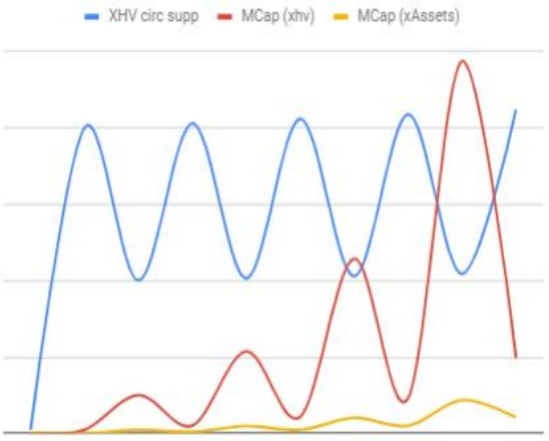
Skenario 3

Keseimbangan dalam Pasokan XHV

Dalam skenario ini, variabel prediksi ditetapkan dengan penggunaan offshore sedang, dan akurasi trading sedang. Sebagai titik tengah di antara dua skenario lainnya, kita dapat mengharapkan skenario ini untuk dimainkan berulang kali dari waktu ke waktu, dengan skenario ekspansi dan kontraksi yang cenderung menuju keseimbangan.

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





Sebagai kesimpulan, meskipun seseorang tidak dapat memprediksi skenario mana yang akan terjadi pada waktu tertentu, protokol ini dirancang untuk beradaptasi dengan perubahan tingkat penggunaan dengan memperluas dan mengontrak pasokan XHV secara langsung melalui tindakan pengguna, menciptakan kurva pasokan baru dan unik yang murni berasal dari penggunaan alami dan organik.

Stabilitas dan Ekonomi

Mint and burn hanya membutuhkan sedikit hal untuk diimplementasikan dalam bentuk dasar; hanya harga yang diketahui untuk melakukan konversi, dan kemampuan untuk mengkonversi satu jenis aset ke aset lainnya pada rantai yang sama pada tingkat konversi tersebut.

Secara sederhana, ini adalah konsep yang sangat sederhana. Meskipun demikian, konsep yang paling sederhana terkadang merupakan konsep yang paling sulit untuk dipahami sepenuhnya, dan untuk memastikan bahwa ekosistem Haven menggunakan model ekonomi yang kuat, beberapa tantangan harus diatasi.

1. Transparansi pasokan
2. Manipulasi harga berbasis bursa
3. Membuktikan dan mempertahankan nilai aset sintetis dalam ekosistem algoritmik PoW.
4. Potensi 'Run on the Bank' selama periode volatilitas pasar yang lebih luas

Tantangan-tantangan ini akan dibahas satu per satu:

Transparansi Pasokan

Konsep awal untuk Haven didasarkan pada pasokan XHV dan xAssets yang tidak diketahui. Alasannya adalah untuk mencegah manipulasi jaringan oleh pemegang XHV atau xAssets dalam jumlah besar.

Setelah melalui banyak pertimbangan, diskusi komunitas, dan konsultasi dengan penasihat ahli, diputuskan bahwa memiliki sirkulasi pasokan yang transparan akan bermanfaat bagi jaringan dengan beberapa cara berikut ini:

- Hal ini memungkinkan pemantauan jaringan Haven yang lebih efisien, yang berarti upaya serangan dan manipulasi skala besar dapat dideteksi dan dimitigasi dengan lebih cepat.
- Ini memberi pengguna kepercayaan diri yang lebih besar untuk memasuki jaringan Haven dengan kemampuan untuk melihat jumlah XHV dan xAssets yang beredar pada saat tertentu.
- Hal ini memungkinkan visibilitas yang lebih besar dan oleh karena itu analisis yang lebih besar pada situs web metrik koin. Sebagai hasilnya, untuk memastikan keakuratan dan visibilitas, setiap transaksi mint dan burn akan dibuat sedemikian rupa sehingga jumlahnya dapat ditemukan melalui analisis blockchain, dan ditampilkan di penjelajah blok Haven. Hal ini akan memungkinkan pengguna untuk mempertahankan tingkat anonimitas standar Monero dan privasi alamat dompet sambil memungkinkan pandangan yang jelas tentang pasokan yang beredar.

Pasokan setiap jenis aset sekarang dapat dilihat di sini: https://explorer.havenprotocol.org/supply

Manipulasi Harga Berbasis Bursa

Karena sifat mint and burn, janji lama Haven bahwa "1 xUSD akan selalu dapat ditukarkan dengan XHV senilai $1," dan tindakan penghalusan harga rata-rata bergerak dalam sistem harga Haven, langkah-langkah tertentu diperlukan untuk memastikan bahwa perbedaan antara harga pertukaran dan konversi off/onshore dapat diminimalkan.

Minimalisasi ini dilakukan dengan memberikan pilihan prioritas transaksi kepada pengguna. Transaksi dengan prioritas tinggi, dengan waktu buka kunci yang minimal, akan dikenakan biaya yang lebih tinggi daripada transaksi dengan prioritas rendah dengan waktu buka kunci yang lebih lama (di mana biayanya cenderung mendekati nol).

Sejak pertama kali diluncurkan, kontributor Haven telah memantau dan menganalisis data yang diperoleh dari aktivitas selama satu bulan pertama penggunaan di dunia nyata. Sejak pertama kali diluncurkan, struktur biaya asli telah digantikan oleh skema yang jauh lebih sederhana dan lebih ketat untuk memastikan kesehatan jaringan dalam jangka pendek sementara distribusi token dilakukan oleh pemegang awal. Seiring berjalannya waktu, Haven membayangkan bahwa biaya dan strukturnya akan memerlukan peninjauan kembali dan perubahan untuk bekerja seiring dengan kematangan jaringan Haven. Struktur biaya lengkap untuk jaringan Haven akan dipublikasikan bersamaan dengan makalah ini, dan dipertahankan untuk referensi setiap saat di situs web Protokol Haven. https://havenprotocol.org/fees

Salah satu masalah dengan banyak produk DeFi yang ada adalah Anda harus memiliki token tertentu di dompet Anda untuk bertransaksi dengan yang lain. Hal ini dapat menyebabkan gesekan dan biaya yang tidak perlu hanya untuk menggunakannya.

Transaksi Haven mengatasi hal ini dengan membebankan biaya dalam mata uang yang dikirim. Hal ini ditunjukkan pada tabel di bawah ini:

Jenis Transaksi	Jenis Biaya	Biaya yang harus dibayarkan:
Transfer XHV	biaya tx standar	XHV
Transfer xUSD	biaya tx standar	xUSD
XHV -> pertukaran xUSD	biaya penukaran + biaya tx standar	XHV
xUSD -> pertukaran XHV	biaya penukaran + biaya tx standar	xUSD

Membuktikan dan Mempertahankan Nilai Aset Sintetis dalam Ekosistem Algoritmik PoW

Salah satu tantangan terbesar aset sintetis algoritmik, serta salah satu pertanyaan yang paling sering ditanyakan, berpusat pada konsep "nilai sebenarnya" atau "sumber nilai". Pertanyaan seperti "bagaimana Anda bisa mengklaim xUSD bernilai $1 ketika tidak memiliki jaminan?" sering ditanyakan oleh pengguna.

Setelah pertanyaan tersebut dijawab dan dipahami (xUSD "secara tidak langsung didukung" oleh jumlah XHV yang bervariasi dan sesuai), pengguna kemudian fokus pada pertanyaan seputar pasokan dan likuiditas XHV itu sendiri. Karena pasokan XHV akan berfluktuasi karena transaksi luar negeri seperti yang dijelaskan di atas, maka ekspansi dan kontraksi pasokan berpotensi mengubah dinamika seluruh ekosistem.

Kemungkinan besar, dengan mempertimbangkan sifat siklus pasar mata uang kripto, potensi munculnya kedua kasus tersebut cukup tinggi. Hal ini diharapkan dan diinginkan. Fluktuasi dalam pasokan yang beredar adalah

mutlak diperlukan untuk memungkinkan ekspansi dan kontraksi dalam pasokan xUSD tanpa menciptakan volatilitas yang lebih besar dalam harga XHV.

Potensi 'Run on the Bank' Selama Periode Volatilitas Pasar yang Lebih Luas

Selama siklus pasar yang meningkat ('Bull market') pada komoditas apa pun, para pedagang sering kali meninggalkan opsi yang stabil dan memilih aset yang tidak stabil, dan sebaliknya. Dengan stablecoin yang secara tradisional 'didukung' seperti USDT, jumlah dukungan adalah kunci stabilitas mata uang kripto yang didukung. Setiap penyimpangan nilai 'yang didukung' dari nilai 'pasar' menciptakan bahaya nyata bagi pengguna, dan menciptakan situasi di mana ada potensi nilai yang tidak didukung, dan hilangnya patokan untuk aset apa pun yang seharusnya dilacak oleh mata uang kripto.

Haven tidak mengalami masalah ini karena penggunaan mint & burn dan koin berwarna.

Setiap saat, dan dalam segala situasi, pengguna dapat menukarkan 1 xUSD dengan XHV senilai $1. Pasak ini tidak akan pernah putus.

Karena Haven Protocol diimplementasikan menggunakan model koin berwarna, maka protokol ini tidak hanya mendukung xUSD, tetapi juga berbagai aset dan komoditas lain yang kami sebut 'xAssets'. Hal ini memungkinkan XHV sendiri untuk menjadi jaminan tidak hanya untuk satu, tetapi serangkaian aset sintetis pribadi, memperluas mekanisme pegging yang memungkinkan dan mengubah protokol menjadi platform dengan kasus penggunaan dan nilai yang sebenarnya bagi pengguna mata uang kripto.

Siapa tim Haven?

Tim Haven adalah sebuah komunitas yang terdiri dari para pengembang dan kontributor, dan dengan demikian menyambut baik semua masukan dan kontribusi dari pihak manapun.

Tim pengembangan inti tercantum di bawah ini.

Sejak mengambil alih manajemen dan pengembangan koin dari pengembang aslinya, komunitas telah mendapat manfaat dari dukungan dan bimbingan berkelanjutan dari beberapa penasihat, konsultan, dan profesional industri teknologi yang telah membuat misi mereka untuk memenuhi janji Haven, dan mendorong adopsi bagian penting dari lanskap mata uang kripto ini. Dukungan dan masukan yang berkelanjutan dari orang-orang ini sangat kami hargai.

Tim pengembangan core:

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

David adalah seorang ahli teknologi karir dengan fokus pada pengiriman produk dan strategi, ia telah memegang posisi senior di Perusahaan-perusahaan besar di Inggris dan beberapa perusahaan rintisan teknologi selama 20 tahun terakhir. Dengan latar belakang di bidang Matematika, teknologi enkripsi, dan pengembangan Perangkat Lunak, David membawa pengalaman yang cukup besar baik dalam penyampaian teknis dan tata kelola skala besar ke Haven.

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

Neil adalah seorang arsitek dan pengembang perangkat lunak full stack yang berdedikasi. Dengan lebih dari 20 tahun pengalaman pengembangan dalam X86 Assembler, C++, Java, PHP, dan Javascript, Neil telah menghabiskan 18 tahun terakhir untuk mendesain dan membangun perangkat lunak kriptografi.

@Marty (anonim)

Marty adalah seorang pengembang front end dengan pengalaman dalam banyak kerangka kerja, dan membawa ini ke permukaan dengan karyanya di dompet dan situs web Haven.

@Pierre Lafitte (anonim)

Pierre adalah spesialis desain produk, dan menciptakan semua perjalanan pengguna dan UI dalam portofolio produk Haven. Pierre adalah pengembang kripto Front End yang berpengalaman, merupakan kontributor lama di Haven dan akan memimpin sisi pengembangan UX/UI dan mewujudkan visi tim UX .