Haven Protocol
Anonieme Gedecentraliseerde Financiën

Core Protocol v3.0

Dit document is bedoeld om de kernfunctionaliteit van het Haven Protocol te documenteren. Andere *second layer functions* komen niet aan bod in dit document en zullen waar nodig per geval afzonderlijk worden behandeld.

Introductie

Bitcoin baande de weg voor elektronische peer-to-peer-valuta. Het was de eerste digitale valuta die met succes een gedistribueerd grootboek van transacties implementeerde op basis van cryptografisch bewijs in plaats van vertrouwen. Meer recent, door het besef dat alle balansen en transacties in veel cryptovaluta zichtbaar zijn voor iedereen die dat wil zien, is de vraag naar privétransacties en privacymunten toegenomen. Haven is gebouwd bovenop Monero, dat algemeen wordt beschouwd als de leider in privacytechnologie. Haven neemt daarom álle privacyfuncties van Monero over, inclusief ringhandtekeningen en *bulletproofs*. Het breidt die functionaliteit uit door anonieme synthetische valuta en activa (xAssets) aan te bieden die alleen kunnen bestaan door het "verbranden" van de basisvaluta van Haven - XHV. Haven breidt ook Monero's bewijs van vervangbaarheid uit, zodat meerdere soorten activa kunnen worden gelijkgesteld op basis van hun geldwaarde in plaats van alleen het aantal ingewisselde munten, waardoor een volledige privé-set van synthetische valuta's en activa ontstaat, de eerste in zijn soort!

Welkom bij Haven – Anonieme Gedecentraliseerde Financiën.

Geschiedenis van Haven

Het concept van Haven zag begin 2018 het levenslicht en werd door twee ontwikkelaars gestart. Deze eerste poging bereikte het stadium van een openbaar testnet. Doordat er sprake was van enkele kwestbaarheden in de oplossing, een onderbreking in de ontwikkeling en een daaropvolgend gebrek aan vooruitgang bij de oorspronkelijke ontwikkelaars, zag de toekomst van het project er niet erg rooskleurig uit. Echter, eind januari 2019 nam een gezelschap van oorspronkelijke leden van de Haven-gemeenschap het project over met het oog op de succesvolle voltooiing van het project; het leveren van het offshore-opslagmechanisme en het uitbouwen van de ondersteunende infrastructuur om massaal gebruik te maken van een broodnodig hulpprogramma in de snelgroeiende cryptocurrency markt. Het mainnet van Haven Protocol werd op 20 juli 2020 met succes gelanceerd en daarbij werd ook de eerste privévaluta, de xUSD, op de markt gelanceerd.

Haven Protocol

De belofte van Haven: 1 xUSD zal altijd inwisselbaar zijn voor $1.00 aan XHV.

i. Concept

Haven is een niet-traceerbare cryptovaluta met een mengeling van standaard marktprijzen en reële aan activa gekoppelde waardeopslag. Het bereikt dit via een *mint* en *burn*-proces op één enkele blockchain. In het meest eenvoudigste voorbeeld kunnen gebruikers Haven (XHV) 'verbranden' in ruil voor een gelijke USD-waarde aan Haven Dollars (xUSD). Of, om terug te keren naar een volatiele toestand kan de gebruiker ook xUSD verbranden in ruil voor XHV conform de op dat moment geldende dollarwaarde van XHV.

Op termijn zullen andere belangrijke valuta waaronder de EUR, GBP en CNY alsook grondstoffen zoals goud, zilver en olie worden toegevoegd aan het Haven-ecosysteem. Gebruikers hebben in dat geval de mogelijkheid om een geschikte waardekoppeling naar gelang hun eigen behoeften te kiezen.

ii. Het offshore-proces - "*Mint and Burn*"

Haven gebruikt een systeem genaamd *mint en burn* om zijn waardeverhouding ten opzichte van de gekoppelde activa te behouden. In de praktijk werkt dit, met de synthetische Amerikaanse dollar (xUSD) als voorbeeld als volgt:

Bob besluit dat hij 200 van zijn Haven (XHV) in Offshore-Opslag wil stoppen. Wanneer gebruikers XHV in offshore-opslag plaatsen, verbranden ze XHV-munten en creëren ze nieuwe xUSD ter waarde van de huidige waarde van de verbrande XHV. Offshore-opslag bepaalt de huidige marktwaarde van de verbrande XHV (in xUSD) op basis van een op volume gecorrigeerd gewogen gemiddelde afkomstig van verschillende beurzen. Dit wordt gedaan met behulp van een prijsorakel. Dit is een mechanisme om gegevens uit de echte wereld te lezen en deze gegevens beschikbaar te maken voor een blockchain. De prijsgegevens worden door het orakel voor het volledige Haven-ecosysteem opgehaald en prijsgegevens worden gecreëerd en vastgelegd in de blockchain.

Als de huidige waarde van XHV $ 1 USD is, zal de offshore-opslag Bob's 200 XHV verbranden door een speciale transactie te creëren waarbij de 200 XHV die door Bob werden verzonden vervolgens worden 'verbrand' en worden omgezet in xUSD. Hierdoor neemt het totale aanbod van XHV af. Als de marktprijs van XHV vervolgens naar $ 2 USD beweegt en Bob besluit om zijn xUSD uit de offshore opslag te halen, krijgt hij 100 XHV terug (100 * $ 2 = $ 200 USD volgens de oorspronkelijke waarde).

Als het tegenovergestelde gebeurt en de prijs van XHV halveert naar $ 0,50, dan worden 400 XHV gecreëerd en vervolgens naar Bob gestuurd (400 * $ 0,50 = $ 200 USD volgens de oorspronkelijke waarde). Het gebruik van *mint* en *burn* verandert dus het circulerend aanbod van de onderliggende activa op een dynamische wijze.

Dit creëert intrigerende aanbodsscenario's - wezenlijk anders dan die van andere cryptovaluta - die grondig door lezers moeten worden beschouwd om het concept van het Haven Protocol volledig te begrijpen.

iii. Hoe werkt offshoring eigenlijk?

Het Haven-protocol maakt offshore-transacties binnen de *Haven Vault* mogelijk met behulp van een 'coloured coin' oftewel een 'gekleurde munt'-model. Het is de eerste werkende implementatie van gekleurde munten op het Cryptonote-protocol. Het concept van gekleurde munten is goed bekend en gedefinieerd binnen het Bitcoin-netwerk, en wordt hier al in 2013 beschreven:

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

Gekleurde munten op het Cryptonote-protocol kunnen echter niet op dezelfde manier werken als bij Bitcoin en in feite moet het concept van gekleurde munten binnen het Cryptonote-protocol worden

herdacht en opnieuw worden uitgewerkt. Met dank aan Nate Eldredge voor deze duidelijke beschrijving van de verschillen tussen het implementeren op Bitcoin en Monero:

> *"Bij Bitcoin is er een één-op-één overeenkomst tussen invoer en uitvoer van transacties. Stel dat er een transactie X is met een output X1 die 1 satoshi naar Alice's adres A stuurt, en iedereen is het erover eens dat output X1 zo gekleurd is dat het de titel verleent aan Alice's Chevy Nova uit 1977. Als Alice besluit de auto aan Bob te geven, maakt ze een nieuwe transactie Y aan, met een invoer die naar X1 wijst, en wiens enige uitvoer Y1 1 satoshi naar het adres B van Bob stuurt. Nu kan Bob dit bewijzen door een handtekening te maken die overeenkomt met zijn adres B, dat hij de rechtmatige eigenaar van de auto is.*
>
> *Als Mallory de auto probeert te claimen door een andere transactie te maken met invoer X1, zal ze ontdekt worden, omdat ze die transactie niet kan ondertekenen met de privésleutel van Alice, waardoor de transactie niet kan worden geverifieerd. Als Alice de auto aan iemand anders probeert te geven door een tweede correct ondertekende transactie Z te maken met invoer X1, dan wordt dit gedetecteerd als een dubbele uitgave omdat een andere transactie die X1 uitgeeft, eraan voorafgaat in de blockchain.*
>
> *Met ringhandtekeningen wordt deze correspondentie verbroken. Bij het aanmaken van een transactie kunt u naast de ene output (van een eerdere transactie) die u werkelijk wilt uitgeven, nog vele andere vermelden. U maakt een handtekening die bewijst dat u gemachtigd bent om een van de vermelde outputs te besteden, maar u geeft geen informatie over welke het was. Een koppelingsalgoritme zorgt er echter voor dat elke toekomstige poging om die output opnieuw te besteden, wordt opgemerkt en afgewezen.*
> *Als Alice in het bovenstaande scenario een ringsignatuur gebruikt op haar transactie Y, inclusief niet alleen X1 maar een andere output Z1, dan zal haar handtekening niet bewijzen dat ze het recht heeft om X1 uit te geven (en daarom de rechtmatige eigenaar van de auto is en de auto derhalve kan overdragen); het bewijst alleen dat ze recht heeft op X1 of Z1. Verder zou Mallory een transactie M kunnen creëren die X1 bevat en een andere output K1 die ze mag uitgeven. Aangezien ze de privésleutel heeft die overeenkomt met K1, kan ze de transactie M correct ondertekenen, maar het zal niet duidelijk zijn of ze X1 uitgeeft (welke de titel van de auto zou overdragen) of K1 (waarmee de auto niet kan worden overgedragen). "*

Het bovenstaande beschrijft de manier waarop gekleurde munten kunnen worden geïmplementeerd binnen het Bitcoin-netwerk en wijst er terecht op dat dit model faalt wanneer zowel X1 als Z1 nog bestaan na de eerste transactie. Haven werkt op een andere manier. Haven heeft geen Alice en ook geen Mallory. Het enige dat wij hebben is Bob.

Wanneer Bob XHV converteert naar xUSD, dan stuurt hij een transactie met twee 'kleuren', X (XHV) en Z (xUSD). De transactie heeft als input munten van alleen de eerste kleur X, en heeft outputs van zowel X als de tweede kleur Z. Elke transactie binnen het Haven-netwerk bevat twee waarden voor elke bestemming (# X, # Z), en voor alle transacties kan slechts één van deze waarden voor elke bestemming anders dan nul zijn.

Dus wanneer Bob zijn 200 XHV converteert tegen een prijs van $ 1,00 per XHV, stuurt hij een transactie met invoer van (200,0) en bestemmingswaarden van (0,200) wat een uitvoer oplevert van 200 xUSD en 0 XHV. Als de prijs van XHV dan veranderd naar $ 2,00 per XHV, dan zou de conversie terug naar XHV een transactie verzenden met inputs van (0,200) en bestemmingswaarden van (100,0), hetgeen een output oplevert van 100 XHV en 0 xUSD. Op deze manier worden inputs voor transacties en UTXO's permanent en effectief atomair en in realtime verbrand tijdens het transactieproces en worden outputs op dezelfde manier gecreëerd.

Omdat Haven een afsplitsing is van Monero erft het ook al die beveiligings- en anonimiteitskenmerken van Monero. Monero is gebouwd op de premisse, voorwaarde en absolute

zekerheid dat voor een bepaalde transactie het verschil tussen inputs en outputs altijd nul is. Elke transactie die niet aan dit vereiste voldoet, zal altijd mislukken.

In het geval van Haven kan dit fundamentele aspect van Monero echter geen stand houden. Voor elke conversie tussen XHV en xUSD waar de prijs van XHV niet precies $ 1,00 is, is deze regel volledig onhoudbaar; inputs en outputs zullen namelijk niet gelijk zijn, noch zullen onze toezeggingssommen van Ca en Cb en bijgevolg src / ringct / rctSigs.cpp verRctSemanticsSimple () de Monero-test kunnen doorstaan voor:

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

Hier introduceren we het concept binnen het Haven-netwerk van '*Proof of Value*'.

Dank gaat uit naar het Monero Research Lab voor hun paper over "Concise Linkable Ring Signatures and Forgery Against Adversarial Keys" door Brandon Goodell, Sarang Noether en Arthur Blue https://eprint.iacr.org/2019/654.pdf. Dit document is gebruikt als onderdeel van de Haven-implementatie van *Proof of Value*.

In een vroege versie van het document stelden de auteurs een 'speelgoed'-model voor waarbij ze een gekleurde valuta creëren met een vaste koppeling tussen twee kleuren: dollars en centen met een omrekeningskoers van 100: 1, en lieten zij zien hoe dit kan worden gedaan met CLSAG. Het proces is als volgt:

> 1. Definieer een conversieratio door een constante ξ en enkele constanten γC, γD op 1, 2, te bepalen. . . , 2 ξ − 1, (in dit voorbeeld γC = 100 en γD = 1).
> 2. Wijzig de verbintenisstructuur zodat elke verbintenis nu een paar verbintenissen C en D is voor hun overeenkomstige kleuren
> 3. Maak een bereikbewijs van Bewijs dat de waarden van zowel C als D dekt. Hier spelen C en D de rol van de Zj-punten, en P zijn aanvullende gegevens die nodig zijn voor het transactieprotocol.
> 4. Een eenvoudige transactiesleutel is geldig als aan de volgende voorwaarden wordt voldaan:
>
> a. elke inputring lid (Xi, Ci, Di, Pi) ∈ Q heeft een geldig bereikbewijs Pi dus Ver (Pi) = 1; en
> b. elk uitgangsbereik bewijs P 0 k is geldig dus Ver (P 0 k) = 1; en
> c. voor de gewijzigde ring pk = X1 X2 · · · Xn Z1 Z2 · · · Zn de handtekening σ slaagt voor de 2-CLSAG verificatie, Verifieer (m, pk, σ) = 1.

Het effect hiervan is dat de transactie niet wordt ondertekend met een verbintenis tot nul, maar een verbintenis tot een verschil - dat verschil is het verschil in aantal 'munten / tokens' dat deze transactie creëert op basis van inputs en outputs. Als een gebruiker 1 USD inwisselt voor 100 centen, zou het verschil 99 zijn – nl. het aantal nieuwe munten dat wordt gecreëerd. Dit model werkt omdat indien een afzender wil ondertekenen met het verschil, dan dient hij zowel het aantal munten dat als invoer wordt gebruikt (hetgeen alleen de houder van de privésleutel voor die invoer kan weten) als de juiste wisselkoers van 100: 1 te gebruiken, waarbij alle *bulletproofs* de waarden van beide mogelijke kleuren moet bevatten. Door dit te doen, kunnen ze geldig ondertekenen door het verschil tussen in- en uitvoer, waardoor de transactie zal worden gevalideerd.

Echter, het *mint* en *burn*-mechanisme van Haven in ogenschouw nemend bevat het bovenstaande model één grote fout. Het vereist een namelijk een vaste wisselkoers; een vaste en bekende koers bij beide partijen van de transactie, en ook vast en bekend bij alle *validators* van de transactie. Dit zorgt voor een probleem waardoor het model niet zal functioneren aangezien bij de koppeling van een stabiele munt aan een volatiele, hetgeen zal dienen te veranderen per definitie de wisselkoers zal zijn.

iv. Proof of Value / *bewijs van waarde*

Om het bovenstaande model van gekleurde munten te laten functioneren met een variabele wisselkoers, moet voldaan worden aan de volgende voorwaarden:

1. er moet een manier zijn om overeengekomen en onveranderlijke prijsinformatie te verzamelen, zodat op elk moment een omwisseltransactie gebruik kan maken van een prijs die kan worden gevalideerd;
2. er moet een manier zijn om inputs om te zetten in outputs op basis van die prijs;
3. er moet een manier zijn om te valideren dat de afzender van een transactie aan dezelfde vereisten voldoet als elke andere cryptonote-transactie - namelijk dat ze de geheime sleutel van de gebruikte input kennen en derhalve kunnen converteren met behulp van een wisselkoers en de transactie kunnen ondertekenen met een correct verschil;
4. er moet een manier zijn om te valideren dat de overeengekomen prijs inderdaad is toegepast op de conversie, zonder enige bedragen aan *validators* bekend te maken.

Prijsinformatie wordt verkregen van een echte prijsaanbieder (d.w.z. een prijsorakel) en er wordt een prijsrecord aangemaakt ter voorbereiding op een nieuw blok dat wordt opgelost. Deze prijsrecords bevatten de wisselkoersen (tegen XHV) voor elk van de xAsset-koppelingen op het moment dat het blok wordt gedolven. De prijsinformatie wordt met tussenpozen van 30 seconden bijgewerkt en op verzoek aan de Haven-daemon gepresenteerd. Prijsrecords worden in elke block-header in de blockchain verwerkt door de *miner* die dat specifieke blok oplost.

Door deze informatie in elk blok op te nemen, garandeert het protocol dat er op geen enkele manier met de transactiewaarde kan worden geknoeid of dat deze kan worden gewijzigd - de blockchain garandeert dat de prijsinformatie onveranderlijk is. Als meerdere blokken met succes zijn gewonnen binnen de levensduur van 30 seconden van het huidige prijsrecord, wordt hetzelfde record in meerdere blokken opgenomen.

Een prijsoverzicht bevat de volgende wisselkoersen (allemaal tegen XHV), evenals enige gereserveerde ruimte voor toekomstige toevoegingen en de handtekening van het orakel dat de gegevens verstrekt. Een voorbeeld van een prijsrecord is:


```
{
   "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 doet dit in het bovenstaande voorbeeld [Bob] met behulp van *commitment*-paren in plaats van enkele *commitment*-waarden. Deze methode wordt ook gebruikt in het speelgoedvoorbeeld van de onderzoekslaboratoria van Monero.

3 / Haven-transacties worden ondertekend met CLSAG en gepaarde *bulletproofs* zoals hierboven beschreven. De transactie wordt echter niet ondertekend met het verschil zoals in het speelgoedvoorbeeld. We ondertekenen met de oorspronkelijke *commitment* tot nulwaarden. Onze *commitment* is om een verschil in waarde van nul te bereiken.

4 / Hier wordt het ingewikkeld. Om te begrijpen hoe Haven transacties valideert of weigert met behulp van een bewijs van waarde, is een beetje voorwerk en enig begrip van *Public Key*-algoritmen vereist alsmede van hoe *Cryptonote Elliptic Curve*-bewerkingen en -punten gebruikt om in- en uitvoerbedragen te valideren.

Elke transactie passeert de functie verRctSemanticsSimple () die alle inputs en outputs van een transactie optelt om te controleren of de resultaten gelijk zijn. Hoewel de waarden in dit stadium volledig versleuteld zijn en worden weergegeven als Elliptic Curve ['EC'] -punten in plaats van reële getallen, werken deze sommen nog steeds vanwege de eigenschappen van modulaire wiskunde en de specifieke manier waarop Monero's EC-punten worden gekozen / gegenereerd.

Kortom, hoewel de cijfers gecodeerd zijn, hebben ze nog steeds bepaalde eigenschappen - de verschillen tussen hen (binnen de EC-ruimte) zijn nog steeds geldig, en dus zal een nulverschil nog steeds een nulverschil zijn, omdat *commitments* additief zijn.

Met andere woorden, als we een transactie hadden met inputs die waardes a1, ..., aj bevatten en outputs met waardes b1, ..., bk, dan zou een waarnemer terecht verwachten dat:

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

Voor Haven zou dit nog steeds werken voor XHV-overschrijvingen en xUSD-overschrijvingen, maar voor conversies zal dit niet werken.

Dus, gebruikmakend van de notatie van hierboven, laten we de constanten γC, γD definiëren als de conversieratio voor een enkele transactie, welke wordt geleverd door ons prijsorakel. En nu met toezeggingen gepaard in ons assortiment, bewijzen respectievelijk (C, D). Om de gelijkheid van waarde te bewijzen, eisen we dat de som van de waarde van de inputs gelijk is aan de som van de waarde van de outputs.

Onze validatie ziet er nu uit als:

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

Waar λC, λD betekenen dat de waarden tussen haakjes worden opgeteld op basis van hun respectievelijke conversiepercentages. (C, D) duiden inputverbintenissen aan, (C ', D') duiden outputverbintenissen aan, en 〖fxG〗 _ duidt de betaalde kosten aan.

v. Orakels om de prijs te bepalen

Om gegevens uit de echte wereld op te halen, gebruiken blockchains een constructie die een 'orakel' wordt genoemd. "Een blockchain-orakel is een informatiebron van een derde partij die als enige functie heeft om gegevens aan blockchains te leveren"

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

In de eerste versie van Haven en in verschillende daaropvolgende ontwerpen sinds die tijd, werd het creëren van een veilig, nauwkeurig en goed presterend orakel beschouwd als de sleutel tot het succes van het protocol. Sinds de oprichting en het succes van diensten zoals Chainlink, die puur zijn ontworpen om orakelfuncties als onafhankelijke gegevensbron aan te bieden, is het nu duidelijk dat er niet alleen geen apart orakel hoeft te worden ingebouwd in het Haven-systeem maar ook dat het onwenselijk is om dit te doen. De reden hiervoor is dat dit de centralisatie van het belangrijkste deel van de conversievergelijking – de prijsstelling – zal vergroten.

Met dit in gedachten heeft Haven Protocol samengewerkt met Chainlink om hun oracle-netwerk te gebruiken voor de verwerking en levering van prijsgegevens. De Chainlink-orakels voor XHV / USD zijn hieronder te zien

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

Het Haven-team is van mening dat het essentieel is om vanaf het begin flexibiliteit in de prijsbepaling in te bouwen en zal daarom niet alleen afhankelijk zijn van één Oracle-systeem, maar zal in staat zijn om na verloop van tijd andere orakels toe te voegen, te ruilen en te verwijderen om ervoor te zorgen dat Haven, nu en ook in de toekomst, de beste gegevens tot haar beschikking heeft.

Aanbodscenario's

XHV is een pure *Proof-of-Work* (PoW) - munt met dezelfde emissiecurve als Monero. Het heeft een initiële mijnbare voorraad van 18,4 miljoen munten en een kleine *tail*emissie zodra die initiële 18,4 miljoen munten zijn gedolven.

Dit is een standaard en welbekend aanbodscenario in de cryptocurrency-markt. Nu Haven's offshore-opslagfunctie live is op het mainnet, blijven de bovenstaande getallen van toepassing op de beloningen voor miners. Ze kwantificeren echter niet langer de feitelijke circulerende hoeveelheid van XHV, aangezien de hoeveelheid door *mint* en *burn* dynamisch zal veranderen, zoals eerder besproken.

Daarnaast bepaalt het circulerende aanbod van XHV niet langer de totale marktkapitalisatie van het Haven-ecosysteem, zodra er meer xAssets (buiten xUSD) live zijn op het netwerk. Hiervoor is het noodzakelijk om zowel de cumulatieve waarde van xAssets als XHV zelf in ogenschouw te nemen.

Deze waarde kan worden uitgedrukt als HNV of Haven netwerkwaarde en wordt als volgt berekend:

*HNV = (XHV-prijs * circulerend aanbod) + xUSD circulerend aanbod*

Extra xAssets kunnen eenvoudig aan de berekening worden toegevoegd wanneer ze aan het netwerk worden toegevoegd.

Om het potentiële toekomstige aanbod van XHV en het effect van dat aanbod op het Haven-ecosysteem te begrijpen, worden de volgende macroscenario's gepresenteerd.

Variabelen die in deze scenario's worden overwogen, zijn onder andere:

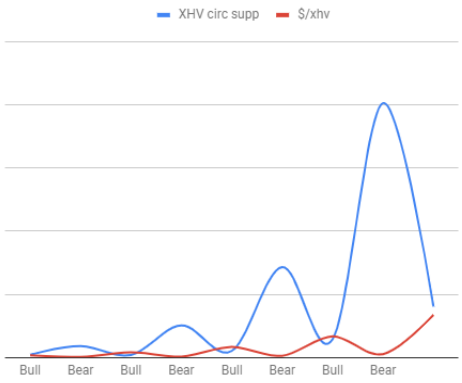
1. De toename van de totale marktkapitalisatie in een stijgende markt = bullmarkt cyclus (inc_Bull)
2. De afname van de totale marktkapitalisatie in een dalende markt = bearmarkt cyclus (dec_Bear)
3. Het percentage van XHV-munten dat is verzonden naar en offshore is opgeslagen aan het einde van een bullmarktcyclus (perc_offBull)
4. Het percentage van xAssets (met xUSD als voorbeeld) munten die terug naar XHV zijn geconverteerd aan het einde van een bearmarkt cyclus (perc_onBear)
5. Het percentage van de lokale ATH-waarde van XHV binnen een bullmarkt cyclus dat het gemiddelde is van alle offshore transactiewaarden (bijv. als de lokale ATH van XHV $ 2,00 is, dan is 80% van die ATH $ 1,60 en zou dit de gebruikte waarde zijn in deze scenario's voor offshoring als 80% wordt gebruikt voor deze variabele) (perc_LATH)
6. Het percentage van de lokale ATL-waarde van XHV binnen een bearmarkt cyclus dat het gemiddelde is van alle onshore transactiewaarden. (perc_LATL) §
    a. Opmerking: de waarden onder punten 5 en 6 kunnen worden gezien als hoe nauwkeurig handelaren zijn in het voorspellen van toppen en bodems van markten.*
7. XHV-volatiliteitsindex - deze waarde wordt gebruikt om te simuleren hoe gecorreleerd de volatiliteit van XHV zou kunnen zijn in vergelijking met de volatiliteit van Bitcoins. Een waarde van 1 is gelijk aan BTC-volatiliteit, 0,5 is 'half zo volatiel ', 2 is twee keer zo volatiel enz.

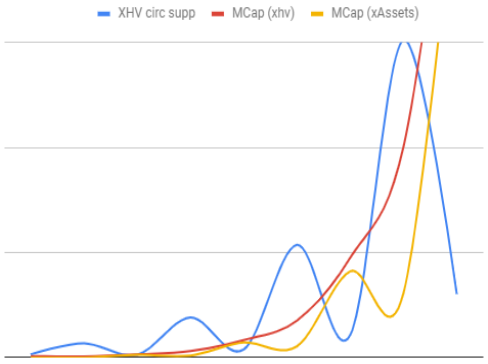
Scenario 1

Expansie van XHV aanbod

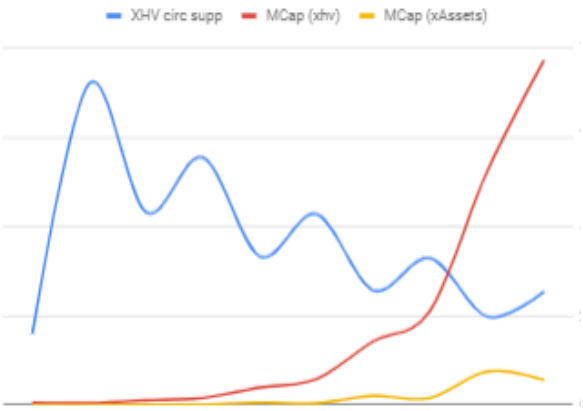
In dit scenario gebruiken wij waarden die het aanbod van XHV in de markt op ten duur zullen doen laten toenemen.

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





Zoals te zien is in dit model van extreem hoog offshore-gebruik en hoge handelsnauwkeurigheid, houdt het gebruik van de offshore-functionaliteit in dit uitbreidingsscenario de prijs van XHV laag. Na verloop van tijd echter zal het de marktkapitalisatie van zowel XHV als van het Haven-ecosysteem als geheel doen toenemen. Dit scenario is acceptabel voor het ecosysteem omdat het de volatiliteit van de XHV-prijs verlaagt, wat op zijn beurt de weergegeven patronen verandert en het scenario uit expansie en uiteindelijk in evenwicht (of zelfs samentrekking) zal brengen, hetgeen te zien is in de onderstaande grafieken. De enige verandering in de hierboven gebruikte waarden is die van iVol (0,5).

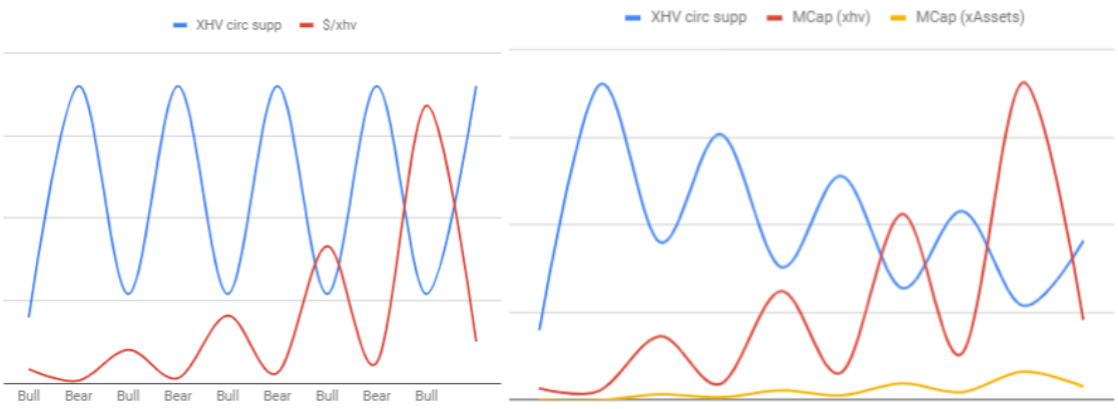


Scenario 2

Krimp van het XHV aanbod

In dit scenario worden waarden gebruikt die opzettelijk deflatie van de circulerende hoeveelheid XHV teweeg brengen.

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



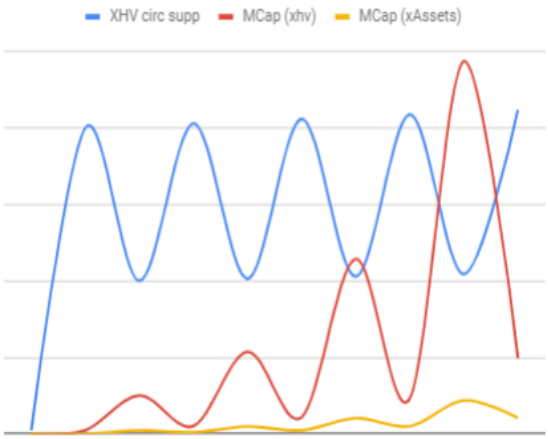
Zoals wij kunnen zien in dit krimpscenario, zal de volatiliteit van de prijs van XHV toenemen, waardoor na verloop van tijd het tegenovergestelde effect van het uitbreidingsscenario zal ontstaan en het patroon zal verschuiven van krimp naar evenwicht of expansie.

Scenario 3

Evenwicht in het aanbod van XHV

In dit scenario worden waarden gebruikt die passen bij een middelgroot gebruik van de offshore functionaliteit en gemiddelde handelsnauwkeurigheid. Doordat dit scenario zich in het centrum tussen de twee andere hierboven beschreven scenario's bevindt, is het de verwachting dat dit scenario zich in de loop van de tijd herhaaldelijk zal afspelen, met scenario's van expansie en krimp die beiden neigen naar evenwicht.

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



Concluderend is niet te garanderen welk scenario zich op welk specifiek moment zal voordoen. Het protocol is echter ontworpen om zich aan te passen aan de veranderde gebruiksniveaus door de expansie en krimp van het aanbod van XHV door middel van acties van de gebruiker, waardoor een nieuwe en unieke aanbodcurve ontstaat puur als gevolg van natuurlijk en organisch gebruik van het protocol.

Stabiliteit en economie

Het *mint* en *burn* principe heeft in de basis weinig nodig; slechts een bekende prijs waartegen de conversie moet worden uitgevoerd en de mogelijkheid om een bepaald type actief om te wisselen tegen een ander type actief op dezelfde blockchain.

Om het voor de hand liggende te verklaren; het is een relatief simpel concept. Dat gezegd hebbende, zelfs de meest eenvoudige concepten zijn soms het moeilijkst om ze volledig te doorgronden. Om ervoor te zorgen dat het Haven-ecosysteem een robuust economisch model gebruikt, moeten bepaalde uitdagingen worden overwonnen.

1. Transparantie van het aanbod.
2. Manipulatie van de prijs op exchanges.
3. Bewijs en behoud van waarde van de synthetische activa in een *PoW*-algoritmisch ecosysteem.
4. De mogelijkheid van een *bankrun* gedurende periodes van hoge volatiliteit op de cryptomarkt.

Deze uitdagingen zullen één voor één nader uiteen worden gezet:

Transparantie van het aanbod

Het oorspronkelijke concept van Haven was gebaseerd op een onbekend circulerend aanbod van XHV en xAssets. De reden hierachter was om manipulatie van het netwerk door grote bezitters van XHV of xAssets te voorkomen.

Na veel beraad, discussie in de gemeenschap en overleg met deskundige adviseurs, werd besloten dat het hebben van een transparant circulerend aanbod op de volgende manieren daadwerkelijk gunstig zou zijn voor het netwerk:

- Het zorgt voor een efficiëntere monitoring van het Haven-netwerk, hetgeen tot gevolg heeft dat pogingen tot aanvallen en grootschalige manipulatie veel sneller kunnen worden gedetecteerd en kunnen worden tegengegaan.
- Het geeft gebruikers meer vertrouwen om het Haven-netwerk te betreden met de mogelijkheid om het aantal XHV en xAssets dat op elk moment in omloop is te bekijken.
- Het zorgt voor een grotere zichtbaarheid en daardoor voor een betere analyse op websites die gegevens over de cryptomarkt verzamelen en publiceren. Als gevolg hiervan, om de nauwkeurigheid en zichtbaarheid te garanderen, wordt elke *mint- en burn*-transactie zo gecreëerd dat de bedragen detecteerbaar zijn door analyse van de blockchain en worden weergegeven in de Haven block explorers. Hierdoor kunnen gebruikers standaard Monero-niveaus van anonimiteit en wallet adres privacy behouden, terwijl ze een duidelijk zicht hebben op het circulerende aanbod.

Het aanbod van elk activatype is nu zichtbaar en kan hier worden bekeken:
https://explorer.havenprotocol.org/supply

Manipulatie van de prijs op exchanges

Vanwege de aard van het *mint* en *burn* principe, de langdurige belofte van Haven dat "1 xUSD altijd inwisselbaar is voor $ 1 aan XHV" en de prijsafvlakkende actie van voortschrijdende gemiddelden binnen het prijsstelsel van Haven, zijn bepaalde maatregelen vereist om ervoor te zorgen dat discrepanties tussen wisselkoersen en off / onshore conversies worden geminimaliseerd.

Deze minimalisatie wordt uitgevoerd door de gebruiker een keuze van transactieprioriteit te bieden. Voor transacties met een hoge prioriteit en derhalve met minimale ontgrendelingstijden, wordt een hogere vergoeding in rekening gebracht dan voor transacties met een lage prioriteit met langere ontgrendelingstijden (waarbij de te betalen vergoeding bijna nul zal zijn).

Sinds de eerste lancering hebben Haven-gebruikers de gegevens die zijn verkregen door activiteit gedurende de eerste maanden van gebruik in de echte wereld gevolgd en geanalyseerd. Sinds de eerste lancering is de oorspronkelijke vergoedingsstructuur vervangen door een veel eenvoudiger en stringenter schema om de gezondheid van het netwerk op korte termijn te garanderen, terwijl de tokendistributie voornamelijk bij de vroege houders ligt. Haven voorziet dat in de loop van de tijd vergoedingen en hun structuren opnieuw moeten worden bezien en zullen moeten worden aangepast om te kunnen blijven functioneren met een volwassen Haven-netwerk. De volledige vergoedingenstructuur voor het Haven-netwerk zal naast dit document worden gepubliceerd en te allen tijde ter referentie worden bijgehouden op de Haven Protocol-website.
https://havenprotocol.org/fees

Een van de problemen met veel bestaande DeFi-producten is dat u een bepaald token in uw wallet moet hebben om transacties in een andere valuta te kunnen uitvoeren. Dit kan onnodige wrijving en kosten veroorzaken, louter om van het protocol gebruik te kunnen maken.

Haven-transacties verhelpen dit probleem door de kosten in rekening te brengen in de valuta die wordt verzonden. Dit wordt weergegeven in de onderstaande tabel:

Transactietype	Type vergoeding	Vergoeding te betalen in:
XHV overschrijving	standaard tx vergoeding	XHV
xUSD overschrijving	standaard tx vergoeding	xUSD
XHV -> xUSD conversie	conversiekosten + standaard tx vergoeding	XHV
xUSD -> XHV conversie	conversiekosten + standaard tx vergoeding	xUSD

Bewijs en behoud van waarde van de synthetische activa in een PoW-algoritmisch ecosysteem.

Een van de grootste uitdagingen van algoritmische synthetische activa, evenals één van de meest gestelde vragen, is gecentreerd rond het concept van *'daadwerkelijke waarde*' of *'bron van waarde'*. Vragen als *'hoe kun je claimen dat xUSD $ 1 waard is als er geen onderpand voor is?*' worden vaak gesteld door gebruikers.

Zodra die vraag is beantwoord en het antwoord is begrepen (xUSD wordt "indirect ondersteund" door een variërende en toepasselijke hoeveelheid XHV), richten gebruikers zich vervolgens op vragen over

het aanbod van en de liquiditeit van XHV zelf. Aangezien het aanbod van XHV zal fluctueren als gevolg van offshore-transacties zoals hierboven is beschreven, veranderen zowel de gevallen van expansie van het aanbod als krimp van het aanbod mogelijk de dynamiek van het gehele ecosysteem.

Rekening houdend met de cyclische aard van cryptocurrency-markten, is de kans dat beide gevallen zich voordoen waarschijnlijk groot. Dit is zowel te verwachten alsook wenselijk. Schommelingen in het circulerende aanbod zijn absoluut noodzakelijk om uitbreiding en inkrimping van het xUSD-aanbod mogelijk te maken zonder een steeds grotere volatiliteit in de prijs van XHV te creëren.

De mogelijkheid van een bankrun

Tijdens stijgende marktcycli ('bullmarkten') in welke grondstof dan ook, laten handelaren vaak stabiele opties liggen ten gunste van volatiele activa, en vice versa in dalende markten. Bij elke traditioneel 'gedekte' stablecoin zoals USDT, is de hoeveelheid dekking de sleutel tot de stabiliteit van de gedekte cryptocurrency. Elke afwijking van 'gedekte' waarde van 'markt'waarde creëert een reëel gevaar voor gebruikers, en creëert een situatie waarin er een potentieel is voor niet-gedekte waarde, en verlies van de koppeling met welk actief de cryptocurrency ook zou moeten volgen.

Haven heeft dit probleem niet door het gebruik van *mint* en *burn* en gekleurde munten.

Een gebruiker kan te allen tijde en in alle situaties 1 xUSD inwisselen voor $ 1 aan XHV. Deze koppeling zal nooit breken.

Aangezien Haven Protocol wordt geïmplementeerd met behulp van een gekleurd muntenmodel, kan het niet alleen xUSD ondersteunen, maar ook een reeks andere activa en goederen die we 'xAssets' noemen. Hierdoor kan XHV zelf het onderpand worden voor niet alleen één, maar ook voor een hele reeks anonieme-synthetische activa, waardoor de mogelijke koppel-mechanismen worden uitgebreid en het protocol wordt omgezet in een platform met een echte use-case en waarde voor gebruikers van cryptocurrency.

Wie zijn het Haven team?

Het Haven team bestaat uit een gemeenschap van ontwikkelaars en donateurs en verwelkomt derhalve alle input en bijdragen van iedere partij.

De kernleden van het ontwikkelingsteam staan hieronder vermeld.

Sinds de overname van het beheer en de ontwikkeling van Haven van de oorspronkelijke ontwikkelaars, heeft de gemeenschap geprofiteerd van de voortdurende steun en begeleiding van verschillende adviseurs, consultants en professionals in de technologie-industrie die het tot hun missie hebben gemaakt om de belofte van Haven te verwezenlijken en de adoptie van dit essentiële gedeelte van het cryptocurrencylandschap te stimuleren. De voortdurende steun en inbreng van deze personen wordt enorm gewaardeerd.

Kernleden van het ontwikkelingsteam:

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

David heeft een langdurige loopbaan in de technologie met een speciale focus op productlevering en strategie. De afgelopen twintig jaar heeft hij verschillende seniorposities bekleed bij grote Britse bedrijven en meerdere technologie startups. David heeft een achtergrond in de wiskunde, encryptietechnologie en softwareontwikkeling. Hij brengt aanzienlijke technische en bestuurlijke ervaring met zich mee.

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

Neil is een toegewijde full-stack software-architect en -ontwikkelaar. Met meer dan 20 jaar ontwikkelingservaring in X86 Assembler, C ++, Java, PHP en Javascript, heeft Neil de afgelopen 18 jaar cryptografische software ontworpen en gebouwd.

@Marty (anoniem)

Marty is een front-end developer met ervaring in een veelheid aan frameworks en brengt dit naar voren in zijn werk aan de Haven wallets en websites.

@Pierre Lafitte (anoniem)

Pierre is een productontwerpspecialist en creëert alle gebruikerservaringen en UI's in de Haven-productportfolio. Pierre is een ervaren front-end crypto-ontwikkelaar, levert een lange tijd bijdrages aan Haven en zal de UX / UI-kant van de ontwikkeling leiden en de UX-visies van het team in de praktijk brengen.