헤이븐 프로토콜
개인 분산형 금융

코어 프로토콜 v3.0

이 문서는 헤이븐 프로토콜이 제공하는 핵심 기능을 문서화하기 위한 것입니다. 다른 두 번째 단계 기능들은 이 백서에서 포함되지 않으며 사례별로 별도로 다루어질 것입니다.

소개

비트코인은 전자 P2P 통화의 길을 열었습니다. 신뢰에 대한 암호화 증명을 기반으로 분산된 거래 원장을 성공적으로 구현한 최초의 디지털 통화였습니다. 최근에는 많은 암호화폐의 지갑과 거래들이 그것을 보려고 하는 모든 사람에 의해 보여질 수 있다는 사실을 깨달으면서 개인 거래 및 프라이버시 코인에 대한 수요가 증가했습니다. 헤이븐은 개인 정보 보호 기술의 리더로 널리 알려진 모네로 위에 구축되었습니다. 따라서 헤이븐은 링 서명 및 방탄을 포함하여 모네로의 모든 개인 정보 보호 기능을 상속받습니다. 이는 헤이븐의 기본 통화인 XHV 의 "소각"을 통해서만 존재할 수 있는 비공개, 익명, 합성 통화 및 상품 (x 아셋)을 제공하여 기능을 확장합니다. 헤이븐은 또한 모네로의 대체 가능성 증명을 확장하여 여러 자산 유형이 환전된 코인의 수보다는 화폐 가치를 기준으로 동일하게 할 수 있도록하여 최초의 완전 비공개 합성 통화 및 자산 세트를 만듭니다.

헤이븐-개인 분산형 금융에 오신 것을 환영합니다.

프로젝트 역사

헤이븐의 개념은 2018 년 초에 두 명의 개발자에 의해 시작했습니다. 이 첫 번째 시도는 솔루션의 약점, 개발 중단 및 원래 개발자의 후속 진행 미흡으로 미래를 의심하기 전에 공개 테스트넷에 도달했습니다. 2019 년 1 월 말, 원래 헤이븐 커뮤니티 회원들이 프로젝트를 완료하고 오프쇼어 스토리지 메커니즘을 제공하면서, 빠르게 성장하는 암호화폐 시장에 필요한 유틸리티를 대량 채택하기 위한 지원 인프라 구축을 목적으로 프로젝트를 인수했습니다.
헤이븐 프로토콜의 메인넷은 2020 년 7 월 20 일에 성공적으로 출시하여 이의 최초 개인 통화 xUSD 를 시장에 선보였습니다.

헤이븐 프로토콜

약속 : 1 xUSD 는 항상 $ 1.00 상당의 XHV 에 사용할 수 있습니다.

i. 개념

헤이븐은 표준 시장 가격과 실제 고정 자산 가치 스토리지가 혼합된 추적 불가능한 암호 화폐입니다. 이는 단일 블록체인 내에서 '발행과 소각 (Mint and Burn)' 프로세스를 통해 달성됩니다. 가장 간단한 경우, 사용자는 헤이븐 달러 (xUSD) 에 해당하는 USD 가치로 헤이븐 (XHV)을 소각할 수 있습니다. 또는 변동적인 상태로 복원하기 위해 사용자는 $1 USD 상당의 XHV 에 대한 xUSD 를 동일하게 소각할 수 있습니다.

파운드 스털링 (GBP), 유로 (EUR) 및 위안 (CNY)을 포함한 기타 주요 화폐 통화는 물론 은, 금 및 석유와 같은 기타 유명 상품이 시간이 지남에 따라 헤이븐의 생태계에 추가되어 사용자가 필요에 맞는 적절한 페깅 메커니즘을 선택할 수 있도록합니다.

ii. 오프쇼어 절차 -"발행과 소각"

헤이븐은 자산 페그에 대한 가치 관계를 유지하기 위해 "발행과 소각"이라는 시스템을 사용합니다. 실제로 합성 미국 달러 (xUSD)를 예로 사용하면 다음과 같이 설명됩니다. 밥 (Bob) 은 자신의 헤이븐 (XHV) 200 개를 오프쇼어 스토리지에 저장하기로 결정했습니다. 사용자가 XHV 를오프쇼어 스토리지에 넣으면 XHV 코인을 태우고 해당 XHV 의 현재 가치를 새로운 xUSD 로 발행합니다. 오프쇼어 스토리지는 지원되는 환전의 거래량 가중 평균가를 기반으로 해당 헤이븐의 현재 시장 가치를 xUSD 로 결정합니다. 이는 전체 헤이븐 생태계에 대한 가격 데이터를 검색하고 가격 기록을 생성하기 위해 가격 오라클 (실제 데이터를 발견하고 이 데이터를 블록체인에 제공하는 메커니즘)을 사용하여 수행됩니다.

헤이븐의 현재 가치가 $ 1 USD 인 경우 오프쇼어 스토리지는 전송된 200 XHV 가 xUSD 로 소각되고 XHV 의 총 공급이 감소하는 특수 거래를 구성하여 밥의 200 XHV 를 소각할 것입니다. XHV 의 시장 가격이 $ 2 USD 로 이동하고 밥이 자신의 오프쇼어 스토리지에 접속하기로 결정하면 100 XHV (원래 가치에 따라 100 * $ 2 = $ 200 USD)가 반환됩니다.

반대의 상황이 발생하고 헤이븐의 가격이 $ 0.50 로 절반으로 떨어지면 400 XHV 가 발행되어 밥에게 전송됩니다 (원래 가치에 따라 400 * $ 0.50 = $ 200 USD). 따라서 발행과 소각의 사용은 동적 방식으로 기본 자산의 순환 공급을 변경합니다.

이것은 다른 암호화폐와는 매우 다른 흥미로운 공급 시나리오를 생성하며 따라서 독자는 헤이븐 프로토콜의 개념을 완전히 이해하기 위해 철저히 검토해야합니다.

iii. 오프쇼어링의 실제 어떻게 작동하는가?

헤이븐 프로토콜은 '컬러코인'모델을 사용하여 헤이븐 볼트 내에서 오프쇼어 거래를 가능하게 합니다. 이것은 크립토노트 프로토콜에서 컬러코인을 처음으로 구현한 것입니다. 컬러코인의 개념은 비트코인 네트워크 내에서 잘 알려져 있고 정의되었으며 아래 링크에 2013 년까지 설명되어 있습니다:

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

그러나 크립토노트의 컬러코인은 비트코인과 같은 방식으로 작동할 수 없으며 실제로 크립토노트 내의 컬러코인 개념은 재작업되고 재창조 되어야 합니다. 비트코인과 모네로의 사용 구현의 차이점을 명확하게 설명해 준 네이트 엘드레지 (Nate Eldredge) 에게 감사드립니다:

> “비트코인을 사용하면 거래의 입력값과 출력값 간에 일대일 대응이 이루어집니다. 1 사토시 (Satoshi)를 앨리스 (Alice)의 주소 A 로 보내는 출력값 X1 이 있는 거래 X 가 있고 모든 사람들이 출력값 X1 이 색상이 지정되어 앨리스의 1977 쉐비 노바 (Chevy Nova)에 타이틀을 부여한다는 데 동의한다고 가정해 봅시다. 앨리스가 밥에게 자동차를 제공하기로 결정하면 입력값이 X1 을 가리키는 새 거래 Y 를 생성하고 유일한 출력값 Y1 이 밥의 주소 B 에 1 사토시를 보냅니다. 이제 밥은 자신의 주소 B 에 해당하는 서명을 생성하여 그가 자동차의 정당한 소유자임을 증명할 수 있습니다.
>
> 말로리 (Mallory)가 입력값 X1 을 사용하여 다른 거래를 생성해 자동차 소유권을 주장하려 시도하면 그녀는 앨리스의 개인 키로 해당 거래에 서명할 수 없어 인증이 거부되고 발견되게 됩니다. 앨리스가 입력값 X1 을 사용하여 명확히 서명된 두 번째 거래 Z 를 생성하여 타인에게 자동차를 주려고 하면 블록체인에서 X1 을 지출하는 다른 거래가 이미 선행하기 때문에 이를 이중 지출로 감지합니다.
>
> 링 서명을 사용하면 이 관련성이 끊어집니다. 거래를 생성할 때 실제로 지출하고자하는 하나의 출력값 (이전 거래의) 외에 다른 많은 항목을 나열할 수 있습니다. 나열한 출력값 중 하나를 사용할 권한이 있음을 증명하는 서명을 생성하지만 어떤 출력값인지에 대한 정보는 제공하지 않습니다. 그러나 연결 알고리즘이 해당 출력값을 다시 사용하려는 향후 시도를 발견하고 거부하도록 합니다.
>
> 위의 시나리오에서 앨리스가 X1 뿐만 아니라 다른 출력값 Z1 을 포함하여 거래 Y 에 링 서명을 사용하는 경우 그녀의 서명은 그녀가 X1 을 사용할 자격이 있음 (따라서 자동차의 진짜 소유자이며 타인에게 증여할 수 있다) 을 증명하지 못합니다; 단지 그녀가 X1 또는 Z1 에 대한 자격이 있음을 증명할 뿐입니다.
>
> 또한 말로리는 X1 과 그녀가 지출할 자격이 있는 다른 출력값 K1 을 포함하는 거래 M 을 생성할 수 있습니다. 그녀는 K1 에 해당하는 개인 키를 가지고 있기 때문에 거래 M 에 명확히 서명할 수 있지만 X1 (자동차 소유권 전달) 또는 K1 (그렇지 않음)을 소비하는지 여부는 명확하지 않습니다.”

위의 묘사은 비트코인 네트워크 내에서 컬러코인이 인식되고 구현되는 방식을 설명하며, 초기 거래 이후 X1 과 Z1 이 모두 존재하는 경우 이 모델이 실패함을 올바르게 지적합니다. 그러나 헤이븐은 다소 다르게 운영됩니다. 헤이븐에는 앨리스도 말로리도 없습니다. 우리가 가진 건 밥뿐입니다.

밥이 XHV 에서 xUSD 로 전환할 때 X (XHV)와 Z (xUSD)의 두 가지 색상으로 거래를 보냅니다. 거래는 첫 번째 색상 X 의 입력값 코인으로 취하고 X 및 두 번째 색상 Z 의 출력값을 모두 갖습니다. 헤이븐 네트워크 내의 각 거래는 각 목적지 (# X, # Z)에 대해 두 개의 가치를 포함하고, 모든 거래에 대해 이러한 가치 중 오직 하나만 각 목적지에 대해 제로가 아닐 수 있습니다.

따라서 밥이 자신의 200 XHV 를 XHV 당 $1.00 의 가격으로 변환할 때 입력값이 (200,0) 이고 대상 가치가 (0,200) 인 거래를 전송하여 200 xUSD 및 0 XHV 의 출력값을 제공합니다. XHV 의 가격이 XHV 당 $2 로 이동할 때 XHV 로 다시 전환하면 입력값이 (0,200)이고 대상 가치가 (100,0) 인 거래가 전송되어 100 XHV 및 0 xUSD 가 출력값이 됩니다. 이러한 방식으로 거래 및 UTXO 에 대한 입력값은 거래 과정 중 즉시 산산이 가루가 되어 효과적으로 영구 소각되고 출력값은 유사하게 발행됩니다.

이것은 모두 훌륭하지만 헤이븐은 모네로의 포크이며 모든 보안 및 익명성 기능을 상속합니다. 모네로는 주어진 거래에 대한 전제, 조건 및 절대 보증을 기반으로

구축되었습니다. 입력값과 출력값의 차이는 제로입니다. 이 요구 사항을 충족하지 않는 모든 거래는 항상 실패합니다.

헤이븐의 경우, 모네로의 이 근본적인 측면은 사실일 수가 없습니다. 사실 XHV 의 가격이 정확히 $1.00 가 아닌 XHV 와 xUSD 사이의 모든 거래에 대해 이 규칙은 완전히 깨지고 입력값과 출력값이 동일하지 않을 것입니다. C^a 와 C^b 의 커미트먼트 합계도 같지 않을 것이고 결과적으로 src / ringct / rctSigs.cpp verRctSemanticsSimple ()도 다음의 모네로 테스트에 실패할 것입니다.

$$\sum_i C_i'^a - \sum_t C^b_t = 0$$

여기서는 '가치 증명'이라는 헤이븐 네트워크의 개념을 소개합니다.

헤이븐의 가치 증명 구현의 일부로 사용된 간결한 연결이 가능한 링 서명 및 상대 키에 대한 위조에 관한 논문 [브랜든 구델, 사랑 노에더, 아서 블루] https://eprint.iacr.org/2019/654.pdf ['논문']을 발표한 모네로 연구소에 감사드립니다.

'논문'의 초기 초안에서 작가들은 두 가지 색상 사이에 고정된 페그로 컬러 통화를 만들어 낸 '장난감'모델을 제안했습니다: 100 : 1 환율로 달러와 페니를 환전하고 CLSAG 를 사용하여 이것이 어떻게 수행되는지 보여줍니다. 과정은 아래와 같습니다:

1. 상수 ξ와 1, 2, . . . , 2 ξ−1 에서 일부 상수 ɣC, ɣD 를 결정하여 환율을 정의한다 (이 예시에서는 ɣC = 100 및 ɣD = 1).
2. 이제 각 커미트먼트가 해당 색상에 대한 커미트먼트 C 와 D 의 쌍이 되도록 커미트먼트 구조를 변경한다.
3. 프르브 (Prove) 에서 C 와 D 의 값을 모두 포함하는 범위 증명을 만든다. 여기서 C 와 D 는 Zj 포인트의 역할을 하고 P 는 거래 프로토콜에 필요한 추가 데이터이다.
4. 다음 사항이 충족되면 간단한 거래 키가 유효하다고 말한다.
    a. 모든 입력값 링 멤버 (Xi, Ci, Di, Pi) ∈ Q 에는 유효한 범위 증명 Pi 가 있으므로 Ver (Pi) = 1;
    b. 모든 출력값 범위 증명 P o k 가 유효하므로 Ver (P o k) = 1;
    c. 수정된 링의 경우 pk = X1 X2 · · · Xn Z1 Z2 · · · Zn 서명 σ는 2-CLSAG 검증을 통과하므로 Verify (m, pk, σ) = 1.

이것의 효과는 거래가 제로에 대한 커미트먼트가 아니라 차이에 대한 커미트먼트로 서명된다는 것입니다. 그 차이는 이 거래가 입력값과 출력값을 기반으로 생성하는 '코인 / 토큰' 수의 차이입니다. 사용자가 1 달러를 100 페니로 환전했다면 차액은 99 - 발행된 새로운 코인의 수 - 가 될 것입니다. 이 모델은 발신자가 그 차이를 이용하여 서명을 하기위해 사용자가 입력값으로 사용한 코인의 수 (해당 입력에 대한 개인 키 보유자만 알 수 있음)를 모두 알아야하고, 가능한 두 가지 색상의 값을 모두 보유한 모든 방탄과 함께 100 : 1 의 올바른 환율을 사용해야 하기 때문에 작동됩니다. 이렇게하면 입력값과 출력값의 차이를 사용하여 올바르게 서명할 수 있으며 거래의 유효성이 검사됩니다.

위의 모델은 헤이븐 발행과 소각 시스템을 고려할 때 한 가지 주요 결함이 있습니다. 고정 환율이 필요합니다. 거래의 양측에 의해 고정되고 알고 있으며, 또한 거래의 모든 검증인이 고정하고 알고 있습니다. 이것은 우리에게 문제를 야기시키며, 또한 이 모델은 정의에 따르면 변동성 자산을 안정된 자산으로 고정하기 위해 환율 변경이 필수적이기 때문에 작동되지 않습니다.

iv. 가치 증명

위의 컬러코인 모델을 가변 환율로 작동하려면 다음이 필요합니다.

1. 합의되고 변경 불가능한 가격 정보를 수집하는 방법으로, 주어진 시간에 환전 거래가 검증 가능한 가격을 사용할 수 있음.
2. 그 가격을 기준으로 입력값을 출력값으로 변환하는 방법
3. 거래 발신자가 다른 크립토노트 거래와 동일한 요구 사항을 충족하는지 확인하는 방법-즉, 사용된 입력값에 대한 비밀 키를 알고 있으므로 환율을 사용하여 변환하고 정확한 차이로 거래에 서명할 수 있음
4. 검증인에게 금액을 공개하지 않고 합의된 가격이 실제로 환전에 적용되었는지 검증하는 방법

가격 정보는 실제 가격 책정 공급자 (즉, 가격 책정 오라클)로부터 얻어지며, 새로운 블록이 해결될 준비를 위해 가격 기록이 생성됩니다. 가격 기록에는 블록이 채굴되는 시점의 각 x 아셋 페그에 대한 환율 (XHV 대비)이 포함됩니다. 가격 정보는 30 초 간격으로 업데이트되며 요청시 헤이븐 데몬에 제공됩니다. 가격 기록은 특정 블록을 해결하는 채굴자가 모든 블록 헤더의 블록체인에 포함됩니다.

이 정보를 모든 블록에 포함함으로써 프로토콜은 거래 가치가 어떤 식으로든 변조되거나 변경될 수 없음을 보장합니다. 블록체인은 가격 정보가 변경 불가능함을 보장합니다. 현재 가격 책정 기록의 30 초 동안 여러 블록이 성공적으로 채굴되면 동일한 기록이 여러 블록에 포함됩니다.

가격 기록에는 다음과 같은 전환율 (모두 XHV 기준)과 향후 추가를 위한 일부 예약된 공간 및 데이터를 제공하는 오라클의 서명이 포함됩니다. 예시적인 가격 기록은 다음과 같습니다:

가격 기록 예 : *Carbon*

2 /헤이븐은 위의 [밥]의 예에서 단일 커미트먼트 가치가 아닌 커미트먼트 쌍을 사용하여 이를 수행합니다. 이것은 또한 모네로 연구소의 장난감 예제에서 사용된 방법입니다.

3 / 헤이븐 거래는 위에서 설명한대로 CLSAG 와 쌍을 이루는 방탄을 사용하여 서명됩니다. 그러나 우리는 장난감 예제에서와 같이 차이를 사용하여 서명하지 않습니다. 우리는 제로 가치에 대한 원래의 커미트먼트를 사용하여 서명합니다. 우리의 커미트먼트는 가치 차이를 제로로 만드는 것입니다.

4 / 여기서부터 복잡해지기 시작합니다. 헤이븐이 가치 증명을 사용하여 거래를 검증하거나 거부하는 방법을 이해하려면 약간의 사전 작업과 공개 키 알고리즘, 크립토노트가 입력값과 출력값을 검증하기 위해 타원 곡선 작업 및 포인트를 사용하는 방법에 대한 이해가 필요합니다.

모든 거래는 결과가 동일한지 확인하기 위해 거래의 모든 입력값과 출력값을 합산하는 함수 verRctSemanticsSimple ()을 통과합니다. 이 단계에서는 값이 완전히 암호화되어 실수가 아닌 타원 곡선 ['EC'] 점으로 표시되지만 모듈식 산술의 속성과 모네로의 EC 점이 선택/생성되는 특정 방식으로 인해 이러한 합계는 여전히 작동합니다.

요컨대, 숫자는 암호화되어 있지만 여전히 특정 속성을 유지합니다. 이들 간의 차이 (EC 공간 내에서)는 여전히 유효하므로 커미트먼트가 가산되기 때문에 차이가 제로이면 여전히 차이가 제로가 됩니다.

즉, a1, ..., aj 양을 포함하는 입력값과 b1, ..., bk 양을 포함하는 출력값으로 거래를 수행한 경우 관찰자는 다음과 같이 정당하게 기대할 수 있습니다.

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

헤이븐의 경우 이것은 XHV 전송 및 xUSD 전송에 대해 여전히 작동하지만 환전의 경우 이것은 완전히 올바르지 않습니다.

따라서 위의 일부 표기법을 다시 사용하여 단일 거래의 환율로 상수 ɣC, ɣD 를 정의해 봅시다. 해당 환율은 가격 책정 오라클에서 제공되었습니다. 그리고 이제 우리의 범위 증명에서 쌍을 이루는 커미트먼트는 각각 (C, D)입니다. 가치의 동등성을 증명하기 위해 입력값의 합이 출력값의 합과 같아야 합니다.

이제 우리의 검증 내용은 다음과 같습니다:

$$\lambda C \left(\sum_i C_i - f_c G - \sum_k C'_k \right) = 1/\lambda D \left(\sum_i D_i - f_D G' - \sum_k D'_k \right)$$

여기서 λC, λD 는 괄호 안의 값이 각각의 환율에 따라 합산됨을 나타냅니다. (C, D)는 입력값 커미트먼트를, (C ', D')는 출력값 커미트먼트를, fxG 는 지불된 수수료를 나타냅니다.

v. 오라클 가격 책정

실제 세계에서 데이터를 검색하기 위해 블록체인은 "오라클"이라는 구조를 사용합니다. "블록체인 오라클은 블록체인에 데이터를 제공하는 유일한 기능을 가진 제 삼자 정보 소스입니다."

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

그 이후로 헤이븐의 첫 번째 되풀이와 여러 후속 설계에서 안전하고 정확하며 고성능의 오라클 생성이 프로토콜 성공의 열쇠로 간주되었습니다. 그러나 순수하게 오라클 기능을 독립적인 데이터 소스로 제공하도록 설계된 체인링크와 같은 서비스의 생성과 성공으로 인해 이제는 헤이븐 시스템에 구축할 필요가 없는 별도의 오라클일 뿐만 아니라 그렇게하는 것은 바람직하지 않습니다. 그렇게하면 전환 방정식에서 가장 중요한 부분인 가격 책정의 중앙 집중화가 증가합니다.

이를 염두에두고 헤이븐 프로토콜은 가격 데이터의 처리 및 제공을 위해 오라클 네트워크를 활용하기 위해 체인링크와 협력했습니다. XHV / USD 용 체인링크 오라클은 아래에서 확인할 수 있습니다.

자료 출처 : https://feeds.chain.link/xhv-usd

헤이븐은 처음부터 가격 책정 검색에 유연성을 구축하는 것이 중요하며, 따라서 하나의 오라클 시스템에만 의존하지 않고 시간이 지남에 따라 오라클을 추가, 교체 및 제거하여 헤이븐이 현재와 미래에 동급 최강의 데이터를 사용하도록 할 수 있습니다.

공급 시나리오

XHV 는 Monero 와 동일한 배출 곡선을 가진 순수 작업 증명 (PoW) 코인으로, 초기 채굴 가능 공급량은 1,840 만 개이며, 그 1,840 만 코인이 채굴되면 소량의 꼬리가 배출됩니다.

이것은 암호 화폐 시장에서 잘 알려진 표준 공급 시나리오입니다. 이제 헤이븐의 오프쇼어 스토리지 기능이 메인넷에 게시되었으므로 위의 수치는 채굴 보상에 계속 적용되지만 이전에 논의한 바와 같이 발행과 소각이 동적으로 이를 변경하기 때문에 더 이상 XHV 의 실제 순환 공급을 정의하지 않습니다.

또한, xUSD 이외의 x 아셋들이 네트워크에 추가되면 XHV 의 순환 공급이 더 이상 헤이븐 생태계의 총 시가 총액을 정의하지 않습니다. 이 때문에 보유한 x 아셋들의 누적 가치와 XHV 자체를 고려할 필요가 있습니다.

이는 HNV 또는 헤이븐 네트워크 가치로 표현될 수 있으며 다음과 같이 계산됩니다. HNV = (XHV 가격 * 순환 공급) + xUSD 순환 공급
추가 x 아셋은 네트워크에 추가될 때 계산에 쉽게 더해 질 수 있습니다.

XHV 의 잠재적인 미래 공급과 해당 공급이 헤이븐 생태계에 미치는 영향을 이해하기 위해 다음과 같은 높은 수준의 매크로 시나리오가 제시됩니다.

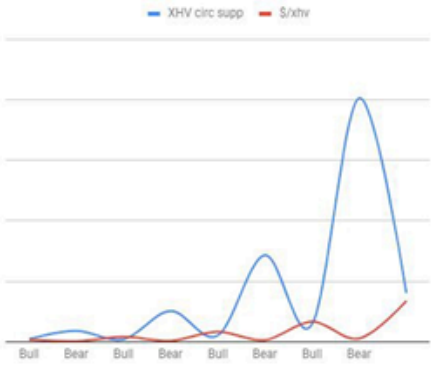
시나리오에서 고려되는 변수는 다음과 같습니다.

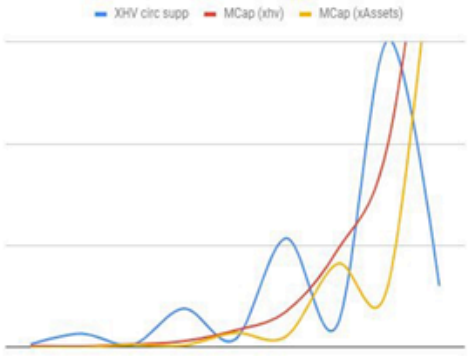
1. 불 마켓 사이클에서 총 시가 총액 증가 (inc_Bull)
2. 베어 마켓 사이클에서 총 시가 총액의 감소 (dec_Bear)
3. 강세시장 주기가 끝날 때 오프쇼어에 보내지고 저장되는 XHV 코인의 % (perc_offBull)
4. 약세시장 주기가 끝날 때 XHV 로 다시 온쇼어된 x 아셋 (예 : xUSD 사용) 코인의 % (perc_onBear)
5. 모든 오프쇼어 거래 값들의 평균인 불 사이클 내에 XHV 의 로컬 ATH 값의 % (예 : XHV 에 대한 로컬 ATH 가 $2.00 이면 해당 ATH 의 80 %는 $1.60 이고 이 변수에 80%가 사용되는 경우 오프쇼어링을 위해 이러한 시나리오에서 사용되는 값이된다.) (perc_LATH)
6. 모든 온쇼어 거래 값들의 평균인 베어 사이클 내에 XHV 의 로컬 ATL 값의 %. (perc_LATL) §
    a. 참고 : 5 및 6 에 대한 이러한 값은 시장의 최고점과 최저점을 예측할 때 거래자가 얼마나 정확한지 볼 수 있다.
7. XHV 변동성 지수 - 이 값은 비트코인 변동성과 비교하여 XHV 의 변동성이 얼마나 상관 관계가 있는지 시뮬레이션하는 데 사용된다. 1 의 값은 BTC 변동성, 0.5 는 '변동성의 절반', 2 는 변동성의 두 배 등.

시나리오 1

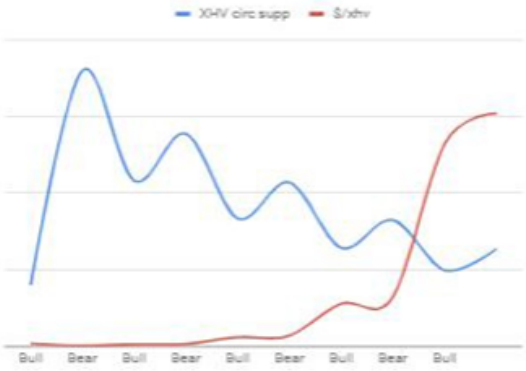
XHV 공급 확대
이 시나리오에서는 시간이 지남에 따라 시장에서 XHV 공급을 증가시킬 값을 사용합니다.

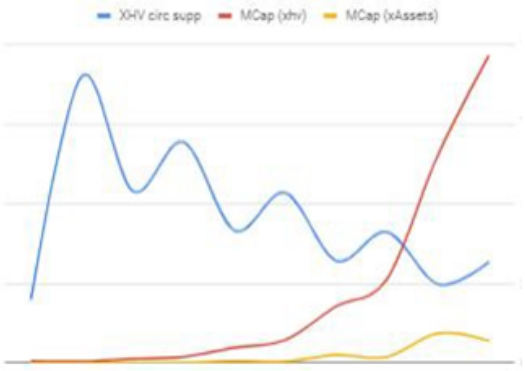
inc_Bull = 2500%
dec_Bear = 85%
perc_offBull = 80%
perc_onBear = 75%
perc_LATH = 90%
perc_LATL = 10%
iVol = 1.0





극도로 많은 오프쇼어 사용과 높은 거래 정확도의 이 모델에서 볼 수 있듯이 확장 시나리오에서 오프쇼어 기능을 사용하면 XHV 의 가격이 낮아지지만 시간이 지남에 따라 XHV 와 헤이븐 생태계 전체의 시가 총액이 증가합니다. 이 시나리오는 XHV 가격의 변동성을 낮추고 결과적으로 표시된 패턴을 변경하고 시나리오를 확장에서 벗어나, 위에서 사용된 값의 유일한 변경 사항이 iVol (0.5) 인 아래 차트에서 볼 수 있듯이 평형 (또는 축소)으로 이동하기 때문에 생태계에서 받아 들일 수 있습니다.

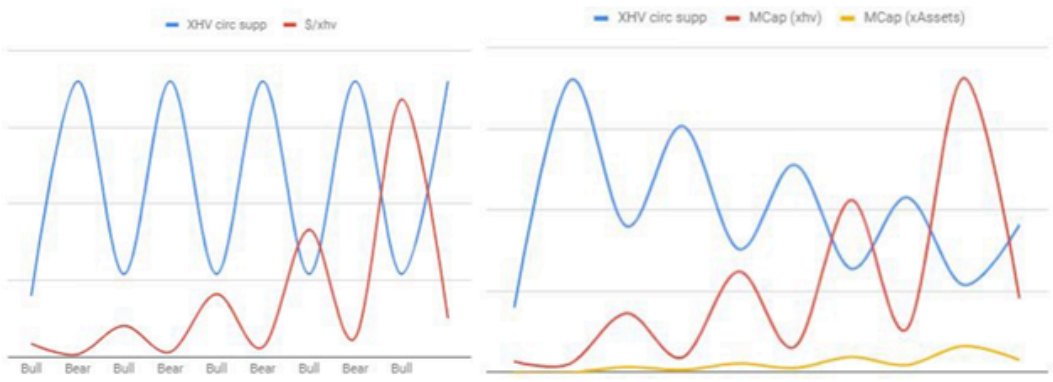




시나리오 2

XHV 공급의 수축
이 시나리오에서는 XHV 의 순환 공급에 의도적으로 디플레이션을 생성하는 값이 사용됩니다.

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



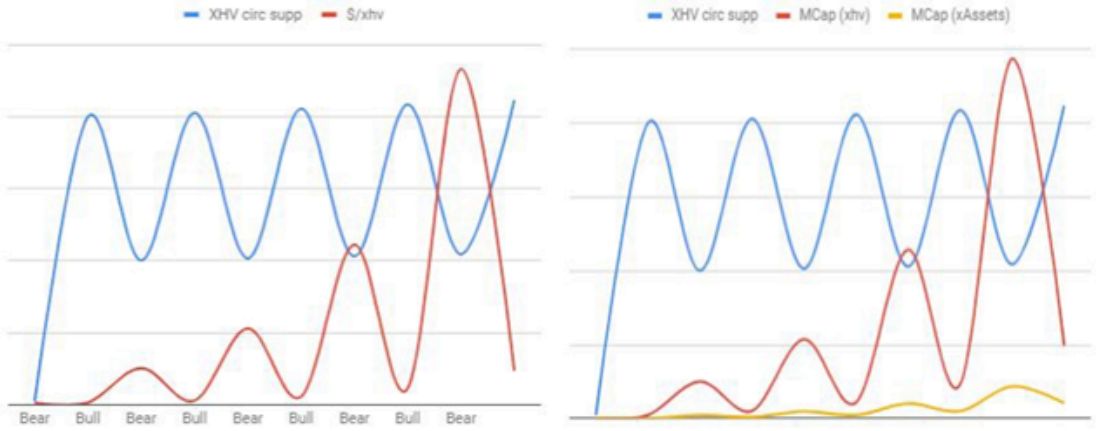
수축 시나리오에서 볼 수 있듯이 XHV 의 가격은 변동성에서 증가하여 시간이 지남에 따라 확장 시나리오와 반대 효과를 생성하며 패턴이 수축에서 균형 또는 확장으로 이동합니다.

시나리오 3

XHV 공급의 평형

이 시나리오에서 예측 변수는 중간 정도의 오프쇼어 사용 및 중간 정도의 거래 정확도로 설정됩니다. 다른 두 시나리오 사이의 핵심으로 확장 및 축소 시나리오가 모두 균형을 이루는 경향이 있는 이 시나리오가 시간이 지남에 따라 반복적으로 진행될 것으로 예상할 수 있습니다.

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



결론적으로, 어떤 시나리오가 어떤 특정 시간에 진행될지 예측할 수는 없지만, 이 프로토콜은 사용자 작업을 통해 직접 XHV 공급을 확대 및 축소하여 변화하는 사용 수준에 적응하도록 설계되어 순전히 자연 및 유기적 사용에서 새롭고 고유한 공급 곡선을 만듭니다.

안정성과 경제성

발행와 소각은 기본적인 형태로 실행하기 위해 거의 아무것도 필요로 하지 않습니다; 단지, 변환을 수행할 알려진 가격 및 해당 변환율로 동일한 체인에서 한 유형의 자산을 다른 유형으로 변환하는 능력.

분명한 것은 매우 단순한 개념입니다. 즉, 가장 단순한 개념은 때로는 완전히 이해하기 가장 어렵고 헤이븐 생태계가 강력한 경제 모델을 사용하도록 보장하려면 특정 당면 과제를 해결해야 합니다.

1. 투명성 제공
2. 환전 기반 가격 조작
3. 작업 증명 (PoW) 알고리즘 생태계에서 합성 자산의 가치 증명 및 유지
4. 시장 변동성이 확대되는 기간 동안 '예금 인출 소동'의 가능성

이러한 문제는 한 번에 하나씩 해결됩니다:

공급 투명성

헤이븐의 원래 개념은 XHV 및 x 아셋의 알 수 없는 순환 공급을 기반으로 했습니다. 그 이유는 XHV 또는 x 아셋의 대규모 보유자가 네트워크를 조작하는 것을 방지하기 위함이었습니다.

많은 고민과, 커뮤니티 토론 및 전문 고문과의 협의 끝에 투명한 순환 공급이 실제로 다음과 같은 방식으로 네트워크에 도움이 될 것이라고 결정했습니다.

- 헤이븐 네트워크를 보다 효율적으로 모니터링할 수 있다. 즉, 시도된 공격과 대규모 조작을 훨씬 빠르게 감지하고 완화할 수 있다.
- 주어진 순간에 유통되는 XHV 및 x 아셋의 수를 볼 수 있는 능력을 통해 사용자가 헤이븐 네트워크에 확신을 가지고 입장할 수 있다.
- 더 큰 가시성을 제공하므로 코인 메트릭 웹 사이트에 대한 더 큰 분석이 가능하다. 결과적으로 정확성과 가시성을 보장하기 위해 각 발행 및 소각 거래는 블록체인 분석을 통해 금액을 발견할 수 있는 방식으로 생성되고 헤이븐 블록 익스플로러에 표시된다. 이를 통해 사용자는 표준 모네로 수준의 익명성 및 지갑 주소 개인 정보를 유지하면서 순환 공급을 명확하게 볼 수 있다.

이제 각 자산 유형의 공급이 표시되며 아래 링크에서 볼 수 있습니다:
https://explorer.havenprotocol.org/supply

환전 기반 가격 조작

발행과 소각의 특성, "1 xUSD 는 항상 $1 상당의 XHV 에 상환될 것"이라는 헤이븐의 오랜 약속 그리고 헤이븐의 가격 책정 시스템 내에서 이동 평균의 가격 완화 조치로 말미암아 환전 가격과 오프쇼어/온쇼어 전환율 간의 불일치를 최소화하기 위해 특정 조치가 필요합니다.

이 최소화는 사용자가 거래 우선 순위를 선택할 수 있도록하여 수행됩니다. 잠금 해제 시간이 최소인 높은 우선 순위 거래는 잠금 해제 시간이 긴 낮은 우선 순위 거래 (수수료가 거의 제로에 가까운 경향이 있음)보다 높은 수수료가 부과됩니다.

첫 출시 이후 헤이븐 기여자들은 실제 사용 첫 달 동안 활동에서 얻은 데이터를 모니터링하고 분석해 왔습니다. 최초 출시 이후, 토큰 분배는 초기 보유자와 함께하는 동안 네트워크 상태를 단기적으로 보장하기 위해 원래 수수료 구조가 훨씬 더 간단하고 엄격한 체계로 대체되었습니다. 시간이 지남에 따라 헤이븐은 수수료와 구조가 헤이븐 네트워크의 성숙도와 함께 작동하기 위해 재검토 및 변경이 필요할 것으로 예상합니다. 헤이븐 네트워크의 전체 수수료 구조는 이 백서와 함께 발행되고 항상 참조를 위해 헤이븐 프로토콜 웹 사이트에 게시되어 유지됩니다. https://havenprotocol.org/fees

많은 기존 DeFi 제품의 문제 중 하나는 다른 거래에서 거래하려면 지갑에 특정 토큰이 있어야한다는 것입니다. 이로 인해 불필요한 마찰과 비용이 발생할 수 있습니다.

헤이븐 거래는 이체되는 통화로 수수료를 부과함으로써 이를 극복합니다. 이것은 아래 표에 나와 있습니다:

거래 유형	수수료 유형	지불 가능한 수수료
XHV 이체	표준 tx 수수료	XHV
xUSD 이체	표준 tx 수수료	xUSD
XHV -> xUSD 환전	환전 수수료+ 표준 tx 수수료	XHV
xUSD -> XHV 환전	환전 수수료+표준 tx 수수료	xUSD

작업 증명 (PoW) 알고리즘 생태계에서 합성 자산의 가치 증명 및 유지

알고리즘 합성 자산의 가장 큰 과제 중 하나이자 가장 자주 묻는 질문 중 하나는 "진정한 가치"또는 "가치의 근원"이라는 개념에 집중되어 있습니다. "어떻게 뒷받침하는 담보물이 없는데 xUSD 가 1 달러의 가치가 있다고 주장할 수 있는가?"라고 사용자들이 자주 질문합니다.

이 질문에 답을 얻고 이해가 되면 (xUSD 는 다양하고 적절한 양의 XHV 에 의해 "간접적으로 뒷받침됨") XHV 자체의 공급 및 유동성에 대한 질문에 집중합니다. XHV 공급은 위에서 설명한 것처럼 오프쇼어 거래로 인해 변동하기 때문에 공급 확대 및 축소 사례 모두 잠재적으로 전체 생태계의 역학을 변화시킵니다.

암호 화폐 시장의 주기적 특성을 고려할 때 두 경우 모두 발생할 가능성이 높습니다. 이것은 예상되고 또한 바람직합니다. 순환 공급의 변동은 XHV 가격에 더 큰 변동성을 만들지 않고 xUSD 공급의 확장 및 축소를 허용하는 데 절대적으로 필요합니다.

시장 변동성이 확대되는 기간 동안 '예금 인출 소동'의 가능성

모든 상품의 상승하는 시장주기 ('불 마켓') 동안 트레이더는 종종 안정적인 옵션 대신 변동성이 있는 자산을 선호하는데 그 반대의 경우도 마찬가지입니다. USDT 와 같이 전통적으로 '뒷받침된'스테이블코인의 경우 지원되는 금액은 뒷받침된 암호화폐의 안정성에 핵심입니다. '시장'가치에서 '뒷받침된'가치의 편차는 사용자에게 실질적인 위험을 초래하고, 암호 화폐가 추적해야하는 자산에 대해 뒷받침되지 않은 가치 및 페그 손실 가능성이 있는 상황을 만듭니다.

헤이븐은 발행과 소각 그리고 컬러코인을 사용하기 때문에 이 문제를 겪지 않습니다.

사용자는 항상 모든 상황에서 1 xUSD 를 $ 1 상당의 XHV 에 사용할 수 있습니다. 이 페그는 절대 부러지지 않습니다.

헤이븐 프로토콜은 컬러코인 모델을 사용하여 구현되기 때문에 xUSD 뿐만 아니라 'x 아셋'이라고 부르는 다양한 자산 및 상품도 지원할 수 있습니다. 이를 통해 XHV 자체가 하나가 아닌 개인 합성 자산 모음의 담보물이 될 수 있으며, 가능한 페깅 메커니즘을 확장하고 프로토콜을 암호화폐 사용자에게 진정한 사용 사례와 가치를 가진 플랫폼으로 전환할 수 있습니다.

헤이븐 팀 소개

헤이븐 팀은 개발자와 기여자의 커뮤니티 집단이므로 모든 당사자의 의견과 기여를 환영합니다.

핵심 개발 팀은 다음과 같습니다.

원래 개발자로부터 코인의 관리 및 개발을 인수한 이래 커뮤니티는 헤이븐의 약속을 이행하고 암호 화폐 환경의 중요한 부분의 채택을 추진하는 것을 사명으로 삼은 여러 고문, 컨설턴트 및 기술 업계 전문가의 지속적인 지원과 지도의 혜택을 받았습니다. 이 분들의 지속적인 지원과 의견에 진심으로 감사드립니다.

핵심 개발 팀 :

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

데이비드는 제품 제공 및 전략에 중점을 둔 경력 기술자이며 지난 20 년 동안 주요 영국 기업 및 여러 기술 스타트업에서 고위직을 역임했습니다. 수학, 암호화 기술 및 소프트웨어 개발에 대한 배경 지식을 가진 데이비드는 기술 제공 및 대규모 지배구조 모두에서 상당한 경험을 헤이븐에 제공합니다.

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

닐은 전담 풀 스택 소프트웨어 설계자이자 개발자입니다. X86 어셈블러, C ++, 자바, PHP 및 자바스크립에서 20 년 이상의 개발 경험을 보유한 닐은 지난 18 년 동안 암호화 소프트웨어를 설계하고 구축했습니다.

@마티 (익명)

마티는 다양한 프레임워크에 대한 경험이 있는 프런트 엔드 개발자이며 헤이븐 지갑 및 웹사이트에 대한 그의 작업을 통해 이를 전면에 내 세웁니다.

@피에르 라피트 (익명)

피에르는 제품 디자인 전문가이며 헤이븐 제품 포트폴리오에서 모든 사용자 여정과 사용자 인터페이스 (UI) 를 만듭니다. 피에르는 경험이 풍부한 프런트 엔드 암호화 개발자이며 헤이븐에 오랫동안 기여했으며 개발의 사용자 경험/ 사용자 인터페이스 (UX / UI) 측면을 이끌고 팀의 사용자 경험 (UX) 비전을 현실화 할 것입니다.