

هافن بروتوكول الخاص بالامركزي التمويل

v3.0 الأساسي البروتوكول

تهدف هذه الورقة إلى توثيق الوظيفة الأساسية التي يوفرها بروتوكول Haven. لم يتم تناول وظائف الطبقة الثانية الأخرى في هذه الورقة ، وسيتم تناولها بشكل منفصل على أساس كل حالة على حدة .

المقدمة

مهّد Bitcoin الطريق لمفهوم عملة الند-لند (peer-to-peer) الإلكترونية. كانت أول عملة رقمية تتجح في تنفيذ أداة دفتر الأستاذ الموزع للمعاملات بناءً على شفرة إثبات الثقة. في الآونة الأخيرة ، ومع ادراك الجميع ان كل المحافظ والمعاملات في العديد من العملات المشفرة مكشوفة ومرئية للجميع، زاد الطلب على المعاملات المالية الخاصة وعملات الخصوصية. تم بناء Haven بالاعتماد على سلسلة كتل Monero ، والتي تعتبر رائدة في تكنولوجيا الخصوصية على نطاق واسع. لذلك ترث Haven جميع ميزات خصوصية Monero ، بما في ذلك " توقيعات الحلقة (Ring Signatures) " و" الإثبات المضاد للخصائص " Bulletproofs " Haven . يعزز هذه الوظيفة من خلال توفير عملات وسلع تتميز بالخصوصية ومجهولية المصدر، عملات " اصول الإكس (xAssets) "، والتي لا يمكن أن توجد إلا من خلال " حرق " عملة Haven الأساسية XHV. ايضاً يعزز Haven من دليل " Monero اثبات قابلية التبادل "، عبر تمكين مقايضة مختلف أنواع الأصول بناءً على قيمتها النقدية بدلاً من الاكتفاء بعدد العملات المتداولة ، فجمعها بين الخصوصية المطلقة وتمكين تبادل العملات والأصول الافتراضية يجعلها الاولى من نوعها على الإطلاق

مرحباً بكم في هافن - التمويل اللامركزي الخصوصي.

تاريخ المشروع

بدأ مفهوم Haven من قبل اثنين من المطورين في مطلع عام 2018. وصلت المحاولة الأولى إلى مرحلة الشبكة التجريبية TestNet قبل ظهور نقاط الضعف في الحلول ، وثغرات في التطوير ، وعدم إحراز تقدم لاحقاً من المطورين الأوائل ، مما جعل مستقبل المشروع موضع شك . في أواخر كانون الثاني (يناير 2019)، تولت المشروع مجموعة من أعضاء مجتمع Haven الأصليين برؤية تهدف إلى إستكماله ، وتقديم آلية التخزين الخارجي ، وبناء البنية التحتية اللازمة لتدعيم فرص التبنّي الجماعي لأداة مطلوبة بشدة في سوق العملات المشفرة سريع النمو.

تم إطلاق الشبكة الرئيسية MainNet لبروتوكول Haven بنجاح في 20 يوليو 2020 لتقديم أول عملة مستقرة وخصوصية xUSD.

بروتوكول هافن

الإلتزام: ١ xUSD سيعادل دوماً ما قيمته ١ USD من XHV.

١. المفهوم

Haven هي عملة مشفرة غير قابلة للتعبق مع منصة لتخزين القيمة بمزيج من عملات اصول الاسواق تعكس أسعار السوق القياسية وقيمة الأصول في العالم الحقيقي. يتحقق ذلك من خلال عملية "التعدين-الحرق" — "mint and burn" داخل الكتلة الواحدة. في أبسط الحالات ، يمكن لعملائنا حرق (XHV) Haven مقابل ما يعادله من قيمة بالدولار الأمريكي ليحصل على Haven Dollars (xUSD) وكذلك العكس ، يمكن للمستخدم حرق xUSD مقابل ما قيمته 1 دولار أمريكي من XHV.

العملات الورقية الرئيسية الأخرى بما في ذلك GBP ، EUR و CNY، وكذلك المعادن النفيسة، الفضة والذهب، بالإضافة إلى السلع الأخرى البارزة مثل النفط ستضاف إلى نظام هافن البيئي مع مرور الوقت لتوفير خيارات سعرية أكثر للمستخدمين لتلائم احتياجاتهم.

٢. عملية التخزين الخارجي " - السك والحرق "

يستخدم Haven نظاماً يسمى "السك والحرق" — "Mint and burn" للحفاظ على أسعار مستقرة مقابل قيمة الأصول المعنية. من الناحية العملية ، كالرمز المربوط بالدولار الأمريكي (xUSD) كمثل ، يعمل هذا على النحو التالي: Bob يقرر أن يضع 200 من عملة هافن (XHV) في التخزين الخارجي. عندما يحول XHV إلى المخازن الخارجية Offshore Storage ، فإنه يحرق عملات XHV ويصرف قيمتها حين إذ إلى ما يعادلها من xUSD مسكوكة جديدة. يحدد التخزين الخارجي القيمة السوقية لحظتها (من xUSD بناءً على متوسط السعر المرجح لحجم التداول في البورصات المدعومة. يتم ذلك باستخدام أو راكل التسعير) أداة لجمع قاعدة بيانات تغذي سلسلة الكتل بيانات العالم الواقعي (وذلك لتدعيم بيانات التسعير لنظام هافن البيئي المتكامل لينتج سجلات التسعير.

إذا كانت قيمة XHV Haven حينها 1 دولار أمريكي ، فإن المخزن الخارجي سيحرق 200 XHV الخاصة بـ Bob بمعاملة خصوصية تتم من خلالها عملية الحرق وتعدين xUSD عوضاً عنها، ونتيجة لهذه العملية ينخفض إجمالي المعروض من XHV. إذا ارتفع سعر XHV إلى 2 دولار أمريكي وقرر Bob الدخول إلى مخازنه الخارجية لتحويل ممتلكاته من xUSD إلى XHV مرة أخرى ، فسيحصل على 2 * 100 XHV = 200 دولار أمريكي حسب القيمة الأصلية.

لكن إن حدث العكس وانخفض سعر Haven XHV إلى النصف، أي إلى 0.50 دولار، فسيتم سك (تعدين) 400 XHV وإرسالها إلى Bob (400 * 0.50 = 200 دولار أمريكي حسب القيمة الأصلية). (من الواضح أن استخدام بروتوكول السك والحرق يغير من وتيرة العرض المتداول للأصول الأساسية بطريقة ديناميكية.

يؤدي هذا إلى إنشاء سيناريوهات توريد مثيرة للاهتمام - تختلف تماماً عن العملات المشفرة الأخرى - والتي تحتاج إلى مراجعة بدقة من قبل القراء لفهم مفهوم بروتوكول Haven بالكامل.

٣. كيف تعمل المخازن الخارجية في الواقع؟

يتيح بروتوكول Haven إجراء المعاملات الخارجية داخل "مخازن هافن" Haven Vault باستخدام نموذج "العملة الملونة" "coloured coin". يعتبر أول تطبيق عملي للعملات الملونة على بروتوكول "الملحوظات المشفرة" — "CryptoNote". مفهوم العملات الملونة معروف ومُعَرَّف جيداً من خلال شبكة البتكوين ، وذلك منذ عام 2013 اطلع عليه هنا:

<https://www.coindesk.com/colored-coins-paint-sophertain-future-for-bitcoin>

ومع ذلك ، لا يمكن أن تعمل العملات الملونة على الكريبتونوت -الملحوظات المشفرة- بنفس طريقة عمل البتكوين ، وفي الواقع يجب إعادة صياغة مفهوم العملات وإعادة تصورها داخل بروتوكول مريبتونوت. الشكر لـ Nate Eldredge لهذا الوصف الواضح للفروق بين التنفيذ باستخدام بتكوين ومينيرو:

"مع Bitcoin ، هناك تطابق واحد لواحد (one to one) بين مدخلات ومخرجات المعاملات "input-output" لنفترض أن هناك معاملة X بمخرجات X1 يرسل 1 satoshi إلى عنوان Alice A ، وبوافق الجميع على أن الناتج X1 ملون بحيث يمنح Alice حق ملكية سيارة 1977 Chevy Nova. إذا قرر Alice إعطاء السيارة إلى Bob ، فإنها تنشئ معاملة جديدة Y ، بإدخال يشير إلى X1 ، ومخرجه الوحيد Y1 يرسل 1 ساتوشي إلى عنوان Bob B. الآن يستطيع بوب إثبات ذلك ، من خلال إنشاء توقيع يتوافق مع عنوانه B - ليكون المالك الشرعي للسيارة.

تأثير ذلك هو أن الصفقة لم يتم توقيعها مع الالتزام بالصر ، ولكن الالتزام بالفرق - وهذا الاختلاف هو الفرق في عدد "العملات / الرموز" التي تنشئها هذه المعاملة بناءً على المدخلات والمخرجات. إذا كان المستخدم يستبدل 1 دولاراً أمريكياً مقابل 100 بنس ، فسيكون الفرق 99 - عدد العملات الجديدة المسكوكة. يعمل هذا النموذج لكون المرسل يقوم بالتوقيع باستخدام الفارق ، يجب أن يعرف المستخدم كلاً من عدد العملات المستخدمة كمدخلات (والتي لا يعرفها سوى مالك المفتاح الخاص لتلك المدخلات) (ويجب أن يستخدم سعر الصرف الصحيح لـ 1:100، مع كل متطلبات الاثبات المضاد للبرصاص "bulletproofs" تحمل اسعار الألوان الممكنة. وبالقيام بذلك ، يمكن التوقيع بشكل صحيح باستخدام الفرق بين المدخلات والمخرجات ليتم التحقق من صحة المعاملة.

يحتوي النموذج أعلاه على عيب رئيسي واحد عند التفكير في نظام "هافن السك والحرق". Haven mint and burn. يتطلب سعر صرف ثابت. ثابت ومعروف من قبل كل اطراف المعاملة ، وأيضاً ثابت ومعروف لدى جميع مدققي المعاملة. هذا يخلق مشكلة بالنسبة لنا ، لن يعمل هذا النموذج لأنه محكوم بتعريف ربط الأصول المتقلبة بأخرى مستقرة ، سعر الصرف متقلب ومتغير دائماً.

٤. إثبات القيمة.

لجعل نموذج العملات الملونة أعلاه يعمل بسعر صرف متغير، يتطلب:

- طريقة لجمع معلومات التسعير المتفق عليها وغير القابلة للتغيير ، بحيث يمكن لمعاملة التبادل في أي وقت استخدام سعر يمكن التحقق من صحته
- كطريقة لتحويل المدخلات إلى مخرجات بناءً على هذا السعر
- طريقة للتحقق من أن مرسل المعاملة يفي بنفس المتطلبات مثل أي معاملة أخرى من نوع "الملحوظات المشفرة" - cryptonote أي أنه يعرف المفتاح السري للمدخلات المستخدمة ، وبالتالي يمكنه التحويل باستخدام سعر الصرف وتوقيع معاملة مع اختلاف صحيح
- طريقة للتحقق من أن السعر المتفق عليه قد تم تطبيقه بالفعل على البورصة ، دون الكشف للمدققين أي مبالغ خاصة.

يتم الحصول على مواد التسعير من مزود بيانات التسعير من العالم الحقيقي الى الافتراضي) مثل أوراقك التسعير (ويتم إنشاء سجل تسعير استعداداً لحل كتلة جديدة. تحتوي سجلات التسعير على أسعار الصرف) مقابل (XHV لكل من حزم "اصول الإكس - xAsset" في وقت تعدين الكتلة. يتم تحديث معلومات التسعير كل 30 ثانية ، ويتم تقديمها إلى برنامج Haven daemon عند الطلب. يتم تضمين سجلات تسعير سلسلة الكتل في كل رأس كتلة عن طريق قيام المعدن بحل (فتح) تلك الكتلة.

من خلال تضمين هذه المعلومات في كل كتلة ، يضمن البروتوكول عدم إمكانية التلاعب بقيمة المعاملة أو تغييرها بأي شكل من الأشكال - تضمن سلسلة الكتل أن معلومات التسعير غير قابلة للتغيير. إذا تم استخراج عدة كتل بنجاح خلال 30 ثانية من عمر سجل التسعير الحالي ، فسيتم تضمين نفس السجل في كتل متعددة.

يحتوي سجل التسعير على معدلات التحويل التالية) جميعها مقابل (XHV، بالإضافة إلى بعض المساحة المحجوزة للإضافات المستقبلية وتوقيع أوراقك الذي يوفر البيانات. وهنا سجل التسعير النموذجي:

```

{
  "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":"9dcc4cd4f862dd5731f9142614fd4fd6c7f795d3c1b07923092abfb25e70a9941498134022ea1958ce07b704930c6891204fc7ce0366742529c559b6c15c72b2",
    "timestamp":1598523249
  }
}

```

مثال سجل التسعير: الكريون

2 / تقوم Haven بهذا في المثال أعلاه [ببوب [باستخدام أزواج الالتزام بدلاً من قيم الالتزام الفردية. هذه أيضاً هي الطريقة المستخدمة في مثال اللعبة من مختبرات أبحاث Monero.

3 / يتم توقيع معاملات Haven باستخدام CLSAG وخوارزميات الإثبات المضاد للرصاص المزدوجة كما هو موضح أعلاه. ومع ذلك، فإننا لا نوقع باستخدام الفروق كما في مثال اللعبة. نوقع باستخدام الالتزام الأصلي بالقيم الصغيرة. التزامنا هو عدم وجود فرق في القيمة.

4 / هنا حيث تتعقد الأمور. لفهم كيفية قيام Haven بالتحقق من صحة المعاملات أو رفضها باستخدام إثبات القيمة يتطلب القليل من العمل المسبق وبعض الفهم لخوارزميات المفتاح العام، وكيفية استخدام Cryptonote لعمليات Elliptic Curve والنقاط للتحقق من صحة كميات المدخلات والمخرجات.

تمر كل معاملة من خلال الوظيفة $verRctSemanticsSimple()$ التي تجمع جميع مدخلات ومخرجات المعاملة للتحقق من تساوي النتائج. على الرغم من أن القيم في هذه المرحلة مشفرة تماماً وتم تمثيلها كنقاط Elliptic Curve ['EC'] بدلاً من الأرقام الحقيقية، إلا أن هذه المبالغ لا تزال تعمل بسبب خصائص الحساب النمطي والطريقة المحددة لاختيار /إنشاء نقاط Monero's EC.

باختصار، على الرغم من أن الأرقام مشفرة، إلا أنها لا تزال تحتفظ بخصائص معينة - تبقى الاختلافات بينها (داخل مساحة EC) صالحة، وبالتالي سيظل الاختلاف الصفري عبارة عن فرق صفري كونه التزامات مضافة.

بعبارة أخرى، إذا كانت لدينا معاملة بمدخلات مكونة من $1, \dots, a_j$ ومخرجات مكونة من $1, \dots, b_k$ ، فعندها يتوقع الرقيب ما يلي:

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

بالنسبة ل Haven، ستستمر عمليات تحويل XHV و xUSD، ولكنها غير صحيحة بتاتاً بالنسبة للبورصات الأخرى.

لذلك، عند إعادة استخدام بعض الرموز من الأعلى، دعونا نحدد الثوابت C, γ ، D, γ كسعر الصرف لمعاملة واحدة، يتم توفير سعر الصرف هذا من خلال أوراق التسعير الخاص بنا. والآن مع الالتزامات المقترنة بمجموعة الإثباتات لدينا C ، D على التوالي. لإثبات المساواة في القيمة، نطلب أن يساوي مجموع قيمة المدخلات مجموع قيمة المخرجات.

وبذلك، هكذا سيبدو التحقق من صحتها:

حيث $\lambda C, \lambda D$ تشير إلى أن القيم الموضوعه بين قوسين يتم جمعها بناءً على أسعار الصرف الخاصة بكل منها (C) ، (D) تشير إلى التزامات المدخلات ، (C')، (D') تشير إلى اثبات المخرجات ، و fxG تدل على الرسوم المدفوعة.

5. تسعير الأوراكل

للتزود ببيانات من العالم الحقيقي ، تستخدم البلوكشين بنية تسمى "أوراكل blockchain oracle". "هو مصدر معلومات تابع لجهة خارجية وظيفته الوحيدة هي توفير البيانات لسلسلة الكتل"

المصدر: <https://www.mycryptopedia.com/blockchain-oracles-explained/>

في الإعداد الأول لـ Haven والعديد من التصميمات اللاحقة منذ ذلك الوقت ، كان إنشاء أوراكل آمن ودقيق وذو كفاءة عالية يعتبر مفتاحاً لنجاح البروتوكول. ومع إنشاء ونجاح مزودين مثل Chainlink، والتي تم تصميمها فقط لتوفير وظائف أوراكل كمصدر بيانات مستقل ولا مركزي ، أصبح من الواضح أن إنشاء أوراكل بنفسنا وخاص بهافن ليس فكرة جيدة، ليس فقط غير ضروري ، ولكنه ضار وغير مرغوب به أيضاً لأن من شأن ذلك زيادة مركزية شبكة هافن في أكثر فصولها أهمية - الا وهو التسعير.

مع اخذ المبررات اعلاه، بدلاً من انشاء اوراكل لشبكتنا، هافن بروتوكول عقدت شراكة مع Chainlink للتزود بمنتجاتهم خدمات قاعدة بيانات التسعير -اوراكل-. ويمكن الاطلاع على تفاصيل أوراكل Chainlink لـ XHV / USD أدناه:

المصدر: <https://feeds.chain.link/xhv-usd>

Haven تؤمن بضرورة بناء ادوات تسعير مرنة وذات كفاءة منذ البداية، فلذلك لن نعتمد على مزود خدمات أوراكل واحد فقط ، بل نسعى لتمكين زيادة عدد المزودين او تبديلهم بشكل مستمر لضمان تسعير افضل واكثر دقة يتحسن مع مرور الوقت بشكل مستدام لتعزيز الثقة.

سيناريوهات التوريد (العرض)

XHV هي عملة إثبات عمل (PoW) خالصة بخصائص مماثلة لـ Monero، ويبلغ إجمالي العرض القابل للتعيين 18.4 مليون ومذيل بالقليل من المسكوكات بمجرد ان يتم تعدين تلك الـ 18.4 مليون قطعة.

هذا سيناريو توريد قياسي ومفهوم جيداً في سوق العملات المشفرة. الآن بعد أن أصبحت ميزة التخزين الخارجي في Haven مباشرة على الشبكة الرئيسية ، تستمر الأرقام المذكورة أعلاه في تطبيق مكافآت التعدين ، ولكنها لم تعد تحدد العرض المتداول الفعلي لـ XHV لأن خوارزميات السك والحرق سيغيران ذلك ديناميكياً، كما تم استعراضه مسبقاً.

بالإضافة إلى ذلك ، بمجرد نشر أصول الإكس (xAssets) (وغيرها) على الشبكة ، لن يبقى العرض المتداول لـ XHV يحدد القيمة السوقية الإجمالية لنظام هافن البيئي. لهذا ، من الضروري مراعاة القيمة التراكمية للأصول الإكس المحتفظ بها بالإضافة إلى XHV نفسه.

يمكن التعبير عن ذلك على أنه HNV أو Haven Network Value وسيتم حسابه على النحو التالي:

$$HNV = \text{سعر} * XHV \text{ العرض المتداول} + (\text{العرض المتداول لـ } xUSD)$$

يمكن بسهولة إضافة أصول الإكس xAssets الأخرى إلى المعادلة عند إدراجها في شبكة هافن.

لفهم العرض المستقبلي المحتمل لـ XHV وتأثير هذا العرض على النظام البيئي لـ Haven، يتم تقديم السيناريوهات الجزئية عالية المستوى التالية.

تشمل المتغيرات التي تم أخذها في الاعتبار في هذه السيناريوهات ما يلي:

- الزيادة في إجمالي القيمة السوقية في دورة السوق الصاعدة (بما في ذلك الثور)
- الانخفاض في إجمالي القيمة السوقية في دورة هبوط السوق (dec_Bear)
- النسبة المئوية لعملة XHV المرسل والمخزنة في الخارج في نهاية دورة السوق الصاعدة (perc_offBull)
- النسبة المئوية لعملة (xAsset باستخدام xUSD كمثال) تم إعادة شحنها إلى XHV في نهاية دورة السوق الهابطة (perc_onBear)
- النسبة المئوية لقيمة ATH المحلية لـ XHV خلال دورة صعودية هي متوسط جميع قيم المعاملات الخارجية (على سبيل المثال ، إذا كان ATH المحلي لـ XHV هو 2.00 دولار ، فإن 80٪ من هذا ATH هو 1.60 دولار وستكون هذه هي القيمة المستخدمة في هذه سيناريوهات النقل إلى الخارج إذا تم استخدام 80٪ لهذا المتغير (perc_LATH))
- النسبة المئوية لقيمة ATH المحلية لـ XHV ضمن دورة هابطة هي متوسط جميع قيم المعاملات الداخلية (perc_LATL) .§
- *ملاحظة: يمكن النظر إلى هذه القيم لـ 5 و 6 على أنها مدى دقة المتداولين عند توقع قمم وقيعان الأسواق.
- مؤشر تقلب XHV - تُستخدم هذه القيمة لمحاكاة مدى ارتباط تقلب XHV بالمقارنة مع تقلبات B itcoins القيمة 1 تساوي تقلب البيتكوين ، 0.5 تمثل نصف التقلب ، 2 هي ضعف التقلب إلخ.

السيناريو 1

التوسع في توريد XHV

في هذا السيناريو ، نستخدم قيمًا من شأنها زيادة المعروض من XHV في السوق مع مرور الوقت.

$$\%inc_Bull = 2500$$

$$\%dec_Bear = 85$$

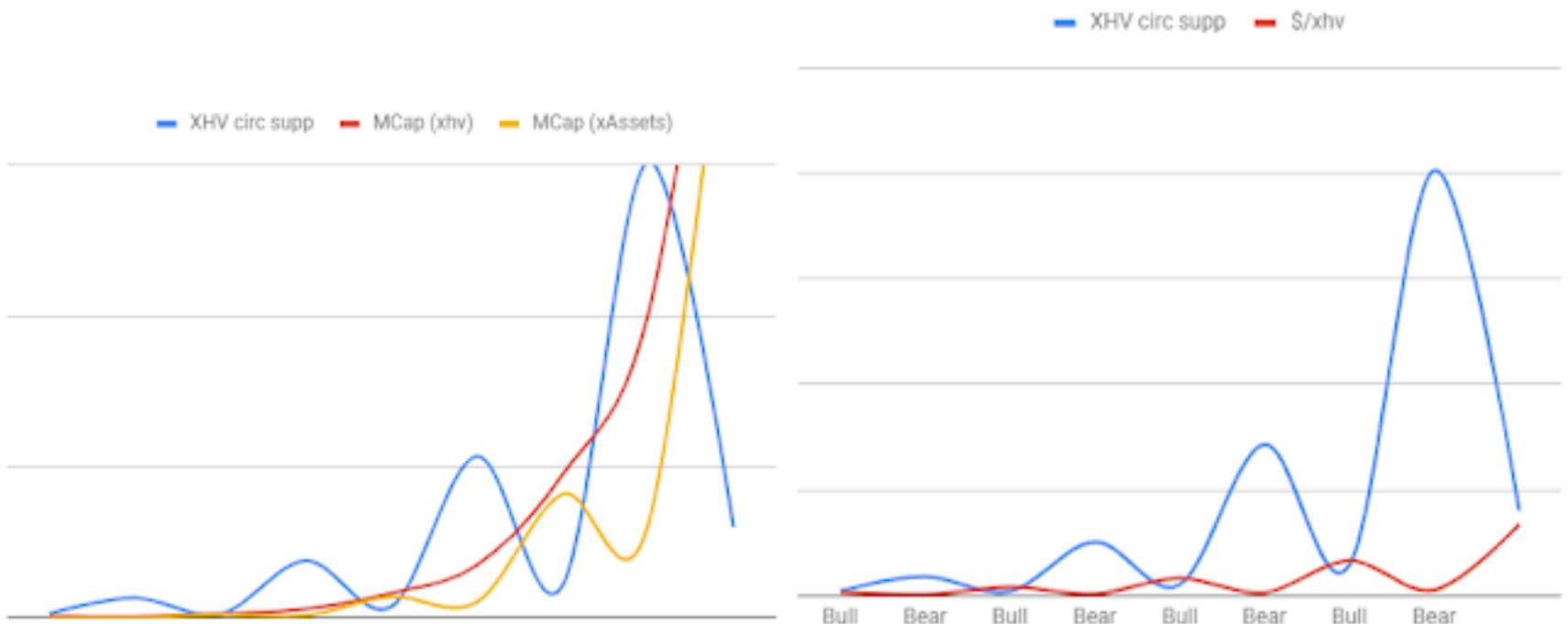
$$\%perc_offBull = 80$$

$$\%perc_onBear = 75$$

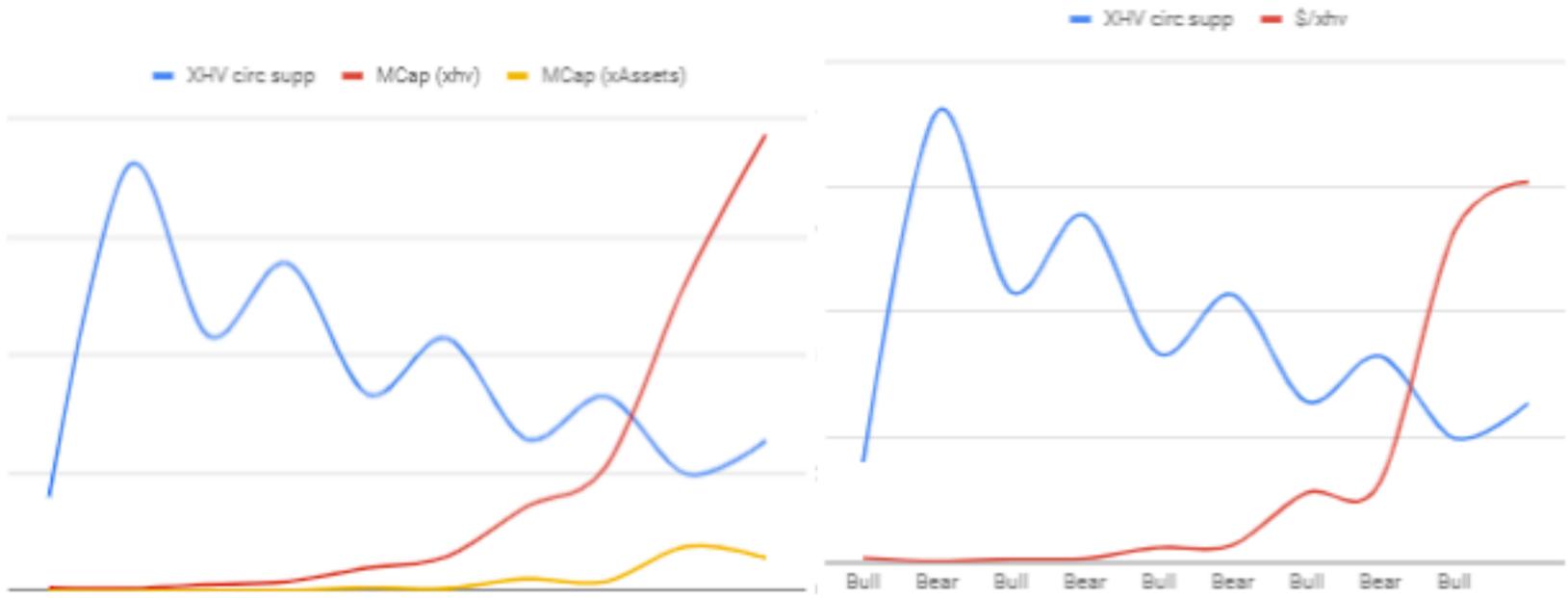
$$\%perc_LATH = 90$$

$$\%perc_LATL = 10$$

$$iVol = 1.0$$



كما يتضح من هذا النموذج استخدام المخازن الخارجية ثقيل للغاية ودقة تداول عالية ، فإن استخدام وظائف المخازن الخارجية في سيناريو التوسع يحافظ على سعر XHV ضعيفاً ، ولكن بمرور الوقت يزيد من القيمة السوقية لكل من XHV ونظام Haven البيئي ككل. هذا السيناريو مقبول للنظام البيئي لأنه يقلل من تقلب سعر XHV ، والذي بدوره يغير الأنماط الموضحة ويخرج السيناريو من التوسع ، إلى التوازن) أو حتى الانكماش (كما يمكن رؤيته في الرسوم البيانية أدناه حيث التغيير الوحيد للأسعار المستخدمة أعلاه هو iVol (0.5).



السيناريو 2

الانكماش في توريد XHV

في هذا السيناريو ، يتم استخدام القيم التي تؤدي عمداً إلى حدوث انكماش في العرض المتداول لـ XHV.

$$\%inc_Bull = 2500$$

$$\%dec_Bear = 85$$

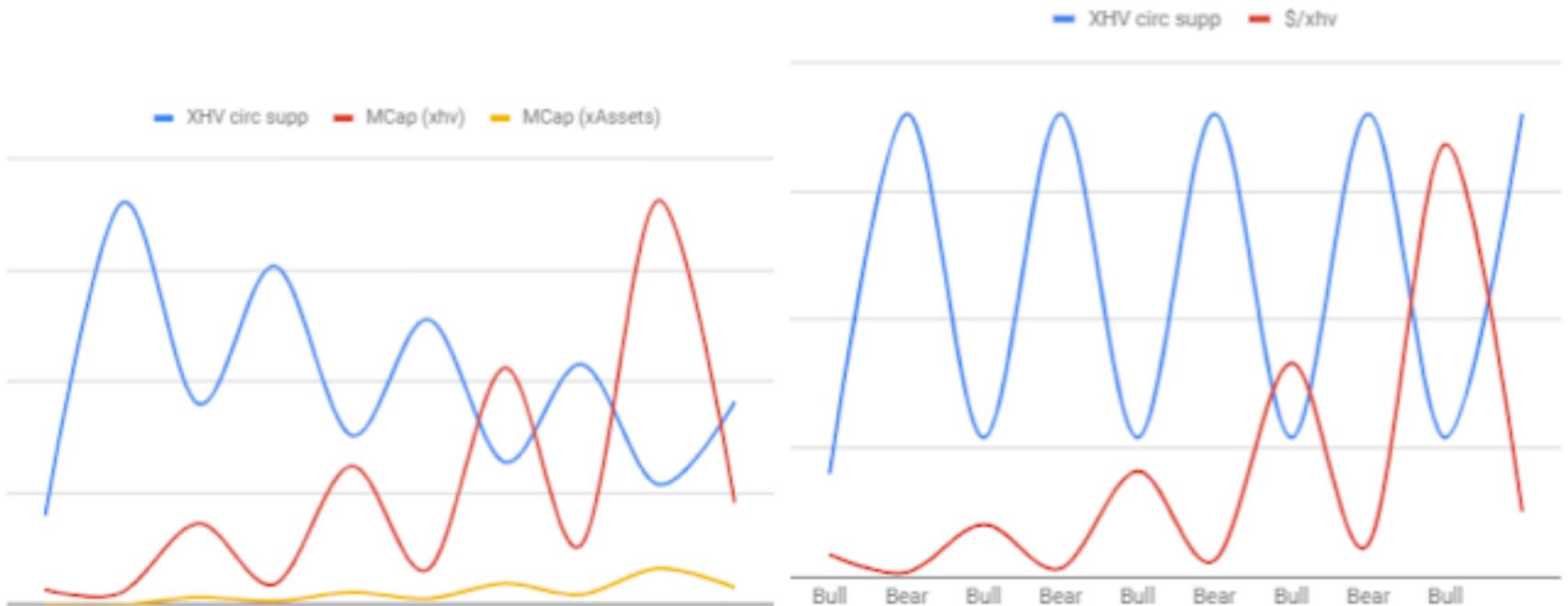
$$\%perc_offBull = 50$$

$$\%perc_onBear = 48$$

$$\%perc_LATH = 60$$

$$\%perc_LATL = 40$$

$$iVol = 1.0$$



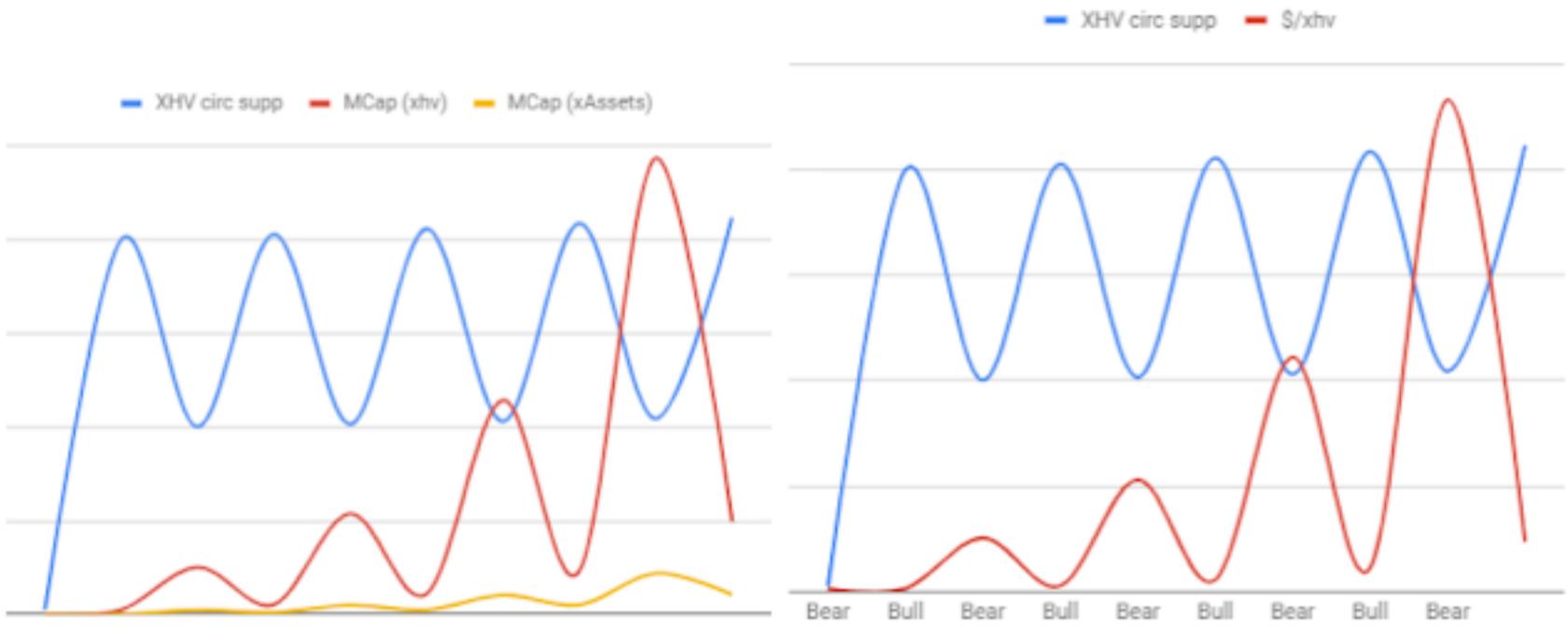
كما يمكن رؤيته في سيناريو الانكماش ، يزداد سعر XHV في التقلب ، مما يخلق تأثيراً معاكساً لسيناريو التوسع بمرور الوقت وسيحرك النمط من الانكماش إلى التوازن أو التوسع.

السيناريو 3

التوازن في العرض XHV

في هذا السيناريو ، يتم تعيين المتغيرات المتوقعة باستخدام استهلاك متوسط للمخازن الخارجية ودقة تداول متوسطة. كنقطة مركزية بين السيناريوهين الآخرين ، يمكن التوقع أن يتم تنفيذ هذا السيناريو بشكل متكرر بمرور الوقت ، مع سيناريوهات توسع وانكماش تتجه نحو التوازن.

$$\begin{aligned}\%inc_Bull &= 2500 \\ \%dec_Bear &= 85 \\ \%perc_offBull &= 70 \\ \%perc_onBear &= 50 \\ \%perc_LATH &= 60 \\ \%perc_LATL &= 40 \\ iVol &= 1\end{aligned}$$



في الختام ، في حين لا يمكن التنبؤ بتوقيت حدوث السيناريوهات ، تم تصميم البروتوكول للتكيف مع ظروف مستويات الاستخدام المتغيرة عن طريق توسيع وتعاقب توريد XHV مباشرة من خلال إجراءات المستخدم ، ما يخلق منحنى بياني سلس وجديد وفريد من نوعه يعكس السلوكيات الطبيعية للمستخدمين.

الاستقرار والاقتصاد

يتطلب بروتوكول السك والحرق القليل لبعريضة مبسطة؛ مجرد سعر معروف لإجراء التحويل ، والقدرة على تحويل نوع واحد من الأصول إلى الآخر على نفس السلسلة بذات معدل التحويل.

بكلمة اوضح، إنه مفهوم بسيط للغاية. ومع ذلك ، فإن أبسط المفاهيم في بعض الأحيان يكون من الصعب فهمها بشكل كامل ، ولضمان أن النظام البيئي لها فن يستخدم نموذجاً اقتصادياً قوياً ، يجب معالجة بعض التحديات.

- شفافية التوريد
- التلاعب بالأسعار على أساس الصرف
- إثبات قيمة الأصول المستقرة والحفاظ عليها في نظام بيئي خوارزمي لإثبات العمل.
- احتمالية "الجرى في البنك" خلال فترات تقلبات السوق الأوسع

سيتم التعامل مع هذه التحديات واحداً تلو الآخر:

شفافية التوريد

اعتمد المفهوم الأصلي لـ Haven على وجود إمداد متداول غير معروف لـ XHV و xAssets. كان السبب في ذلك هو منع التلاعب بالشبكة من قبل كبار مالكي XHV أو xAssets (الحيثان).

بعد قدر كبير من الدراسة والنقاش المجتمعي والتشاور مع المستشارين والخبراء ، تقرر أن وجود توريد متداول شفاف سيكون مفيداً للشبكة بالطرق التالية:

- ان يسمح بمراقبة أكثر كفاءة لشبكة Haven، مما يعني أنه يمكن اكتشاف محاولات التهرب والتلاعب على نطاق واسع والتخفيف من حدتها بشكل أسرع.
- يمنح المستخدمين ثقة أكبر للدخول إلى شبكة Haven مع القدرة على عرض عدد XHV و xAssets المتداولة في أي لحظة.
- يسمح برؤية أكبر وبالتالي تحليل أكبر على مواقع مقاييس العملات. نتيجة لذلك ، لضمان الدقة والوضوح ، سيتم إنشاء كل معاملة سك وحرق بطريقة يمكن اكتشاف المبالغ من خلال تحليل blockchain، وعرضها في مستكشفات كتل Haven. سيسمح ذلك للمستخدمين بالحفاظ على مستويات Monero القياسية لإخفاء الهوية وخصوصية عنوان المحفظة مع السماح برؤية واضحة للعرض المتداول.

أصبح عرض كل نوع من الأصول مرتباً الآن ويمكن رؤيته هنا:

<https://explorer.havenprotocol.org/supply>

احتكار اسعار الصرف

نظراً لطبيعة خوارزميات السك والحرق ، تلتزم هافن منذ فترة طويلة بأن 1xUSD سيكون دائماً قابلاً للاسترداد مقابل 1 دولار أمريكي من "XHV، وإجراء تسوية الأسعار للمتوسطات المتحركة ضمن نظام تسعير هافن ، يلزم اتخاذ تدابير معينة لضمان تحجيم التناقضات بين أسعار الصرف والتحويلات للمخازن الخارجية و الداخلية.

يتم تحقيق هذا التحجيم عبر الاختيار حسب افضلية معاملات المستخدمين. سيتم فرض رسوم أعلى على المعاملات ذات الأفضلية الأعلى ، مع الحد الأدنى لأوقات القفل المفتوح ، مقارنة بالمعاملات ذات الأفضلية المنخفضة مع أوقات إلغاء القفل المغلق) حيث تميل الرسوم إلى ما يقرب من الصفر).

منذ الإطلاق الأول ، كان المساهمون في Haven يراقبون ويحللون البيانات المكتسبة من النشاط خلال الشهر الأول من الاستخدام الفعلي. منذ بداية هافن ، تم استبدال هيكل الرسوم الأصلي بنهج أبسط وأكثر صرامة لضمان دقة الشبكة على المدى القصير بينما يكون توزيع الرموز مع المالكين الأوائل. بمرور الوقت ، تتصور هافن أن الرسوم وهياكلها ستتطلب إعادة النظر والتعديل للعمل جنباً إلى جنب مع نضج شبكة هافن. سيتم نشر هيكل الرسوم الكامل لشبكة Haven جنباً إلى جنب مع هذه الورقة ، والاحتفاظ بها للرجوع إليها في جميع الأوقات على موقع بروتوكول Haven. <https://havenprotocol.org/fees>

تتمثل إحدى المشكلات المتعلقة بالعديد من منتجات DeFi الحالية في أنه يجب أن يكون لديك رمز مميز معين في محفظتك من أجل التعامل مع منتج آخر. ينتج عن ذلك التعامل مع اصول ليست ضرورية والاحتفاظ بها دون اسباب منطقية.

معاملات Haven تصلح ذلك عن طريق فرض الرسوم بالعملة التي يتم إرسالها. ويظهر ذلك في الجدول أدناه:

نوع المعاملة	نوع الرسوم	الرسوم واجبة في: السداد في:
XHV نقل	القياسية TX رسوم	XHV
xUSD تحويل	القياسية TX رسوم	xUSD
XHV -> تبادل xUSD	+ رسوم الصرف رسوم الصرف القياسية	XHV
xUSD -> تبادل XHV	+ رسوم التبادل e القياسية tx رسوم	xUSD

إثبات قيمة الأصول المركبة والحفاظ عليها في نظام بيئي خوارزمي قائم على إثبات العمل

أحد أكبر التحديات التي تواجه خوارزميات الأصول المركبة ، بالإضافة إلى أحد الأسئلة الأكثر شيوعاً ، حول مفهوم "القيمة الحقيقية" أو "مصدر القيمة". أسئلة مثل "كيف يمكنك ضمان أن xUSD تساوي دولاراً واحداً وهي غير مدعومة بالدولار؟" تساؤل بدر من الكثيرين.

بمجرد الإجابة على هذا السؤال وفهمه (يتم "دعم xUSD بشكل غير مباشر" بكمية من XHV متغيرة حسب القيمة)، يركز المستخدمون بعد ذلك على الأسئلة حول العرض والسيولة لـ XHV نفسها. نظراً لأن العرض XHV سيتقلب بسبب المعاملات الخارجية كما هو موضح أعلاه ، فمن المحتمل أن تتغير حالات التوسع والانكماش في العرض لديناميكيات النظام البيئي بأكمله.

في جميع الاحتمالات ، مع الأخذ بالاعتبار الطبيعة الدورية لأسواق العملات المشفرة ، فإن احتمال ظهور كلتا الحالتين وارد جداً. هذا متوقع ومرغوب فيه. التقلبات في العرض المتداول مطلوبة للسماح بالتوسع والانكماش في عرض xUSD دون إحداث تقلبات أكبر في سعر XHV.

احتمالية "التهافت على النظام البنكي" خلال فترات تقلبات السوق الحادة

خلال الدورات السعرية الصاعدة ("سوق صاعد القيمة") (لأي سلعة ، غالباً ما يترك المتداولون خيارات مستقرة لصالح الأصول المتقلبة ، والعكس صحيح. مع أي عملة مستقرة تقليدية "مدعومة" مثل USDT، فإن مقدار الدعم هو مفتاح استقرار العملة المشفرة المدعومة. أي انحراف للقيمة "المدعومة" عن القيمة "السوقية" يخلق خطراً حقيقياً على المستخدمين ، ويخلق حالة احتمالية لقيمة غير مدعومة ، وغياب الارتباط بأي أصول من المفترض أن تتبعه العملة المشفرة بفقد قيمتها بقدر مماثل.

لا تعاني هافن من هذه المشكلة بسبب استخدامها خوارزمية "السك والحروق" وخوارزمية "العملات الملونة".

في جميع الأوقات ، وفي جميع الحالات ، يمكن للمستخدم استرداد 1 x USD مقابل 1 دولار بقيمة XHV. هذه قاعدة لن تنكسر أبداً.

نظراً لأن بروتوكول Haven يتم تنفيذه باستخدام خوارزميات الرموز الملونة ، فهو قادر على دعم، ليس فقط xUSD، ولكن أيضاً مجموعة من الأصول والسلع الأخرى التي نطلق عليها "أصول الإكس" — "xAssets". يسمح هذا لـ XHV بأن يصبح ضماناً ليس فقط لواحد ، ولكن لمجموعة من الأصول الخصوصية ، مما يوسع آليات الربط الممكنة ويحول البروتوكول إلى نظام أساسي مع حالة استخدام حقيقية وقيمة مضافة لمستخدمي العملات المشفرة.

من نحن، فريق هافن؟

فريق هافن هو مجموعة من المطورين والمساهمين ، وبناءً على ذلك، هافن يرحب بجميع المنضمين والمساهمين من أي طرف.

وهنا سرد عن فريق المطورين الأساسي.

منذ تولي إدارة وتطوير العملة من المطورين الأصليين ، استفاد المجتمع من الدعم المستمر والتوجيه للعديد من المستشارين والخبراء والمتخصصين في صناعة التكنولوجيا الذين جعلوا مهمتهم هي الإيفاء وتحقيق وعد Haven ، ودفع تبنيتها من هذا الجزء الحيوي من مجتمع العملة المشفرة. إن الدعم المستمر من هؤلاء الأفراد موضع تقدير كبير.

فريق التطوير الأساسي:

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

ديفيد هو تقني المهنية مع التركيز على تقديم المنتجات والاستراتيجية، أنه تقلد مناصب عليا في تخصص الشركات في المملكة المتحدة والشركات الناشئة التكنولوجية متعددة على مدى السنوات ال 20 الماضية. مع خلفية في الرياضيات وتكنولوجيا التشفير وتطوير البرمجيات ، يجلب David خبرة كبيرة في كل من التسليم الفني والحكومة واسعة النطاق إلى Haven.

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

نيل هو مهندس ومطور برمجيات مكثس متكامل. مع أكثر من 20 عامًا من الخبرة في التطوير في X86 Assembler و ++C و Java و PHP و Javascript، أمضى Neil آخر 8 سنوات في تصميم وبناء برامج التشفير.

@Marty (anonymous)

مارتي هو مطور واجهات أمامية لديه خبرة في العديد من الأطر ، ويبرز ذلك من خلال عمله على محافظ ومواقع Haven.

@Pierre Lafitte (anonymous)

بيير هو متخصص في تصميم المنتجات ، ويقوم بإنشاء جميع رحلات المستخدم وواجهة المستخدم في مجموعة منتجات Haven. بيير هو مطور تشفير من ذوي الخبرة في Front End ، وهو مساهم لفترة طويلة في Haven وسيقود جانب UX / UI من التطوير ويحول رؤى UX للفريق إلى الواقع.