



避风港协议

隐私的去中心化金融

核心协议 V3.0

本文旨在记录避风港协议提供的核心功能。本文不涉及其他二层以及后续潜在开发内容，之后将根据具体情况单独处理并列举说明。

介绍

比特币为点对点数字货币铺平了道路。它是第一个成功实现基于可信任的密码学证明的分布式交易账本的数字货币。最近，随着人们意识到许多数字货币中的钱包和转账记录对所有人都是可见的，对转账交易的私密性和隐私币的需求也在增长。避风港是建立与门罗的基础之上，门罗被广泛认为是隐私技术的领导者。因此避风港继承了门罗的所有隐私功能，包括环签名，防弹。避风港通过提供隐私，匿名，合成货币和商品 (xAsset) 扩展了更多的使用功能，这些合成资产只能通过“燃烧”避风港的基础货币-XHV来实现。避风港通水也扩展了门罗的可互换性证明，允许多种类型资产根据其货币价值而不是仅根据交换的硬币数量进行等价交换，创造了第一种完全隐私的合成货币和资产集。

欢迎来到避风港-隐私的去中心化金融。

项目历史

避风港的概念是由两位开发者在2018年初提出的。第一次尝试到达了公开测试阶段，后来由于解决方案的缺点，开发中断以及随后原开发者的毫无进展，使得项目的未来受到怀疑。2019年1月底，几名原避风港社区成员接管了该项目，以期望完成项目，实现离岸存储机制，并建立出支持性的基础设施满足必需的用途，方便在快速增长的数字货币市场中被大规模采用。

避风港协议的主网于2020年7月20日上线，向市场推出了第一款隐私稳定币xUSD。

避风港协议

承诺：1xUSD永远可以兑换价值1美金的XHV。

i. 概念

避风港是一种不可追踪的数字货币，混合了标准市场定价和现实世界资产挂钩的价值存储。它通过单个区块链内的“铸币和燃烧”过程来实现。简单的说，用户可以“燃烧销毁”避风港（XHV）换取等值美元价值的避风港美元（xUSD）。或者，恢复到不稳定状态，用户可以“燃烧销毁”1 xUSD获得1美元等值的XHV。

包括英镑，加元，人民币在内的其他主要法币，包括黄金、白银以及其他备受关注的大宗商品例如原油等，随着开发的进展将会被逐步加入避风港的生态系统内，用户将根据他们的需要选择合适的挂钩机制。

ii. 离岸过程——“铸币和烧币”

避风港使用一种名为“铸币和燃烧”的系统来维持其与资产挂钩的价值关系。在实践中，以合成美元（xUSD）为例，其工作原理如下：鲍勃决定将他的200个避风港币（XHV）放入离岸存储。当用户将XHV放入离岸存储时，他们“燃烧”xhv币，并将这些XHV的当前价值“铸造”成新的xUSD。离岸存储根据所支持的交易所的交易量加权平均值确定避风港币的当前市场价值（以xUSD为单位）。这是通过定价预言机（一种发现真实世界数据并将这些数据提供给区块链的机制）来检索整个避风港生态系统的定价数据并生成定价记录。

如果避风港的当前价值为1美元，离岸储存将通过构造一个特殊的交易来燃烧鲍勃的200个XHV，然后将发送的200个XHV“燃烧掉”并“铸造”生成xUSD，同时XHV的总供应量随之减少。如果XHV的市场价格随后涨到2美元，并且鲍勃决定退出离岸存储，他将收到100个XHV（ $100 * \$2 =$ 当初价值200美金）。

相反，当避风港币的价格下跌到0.5美金，则将铸造出400个避风港币然后发送给鲍勃（ $400 * \$0.5 =$ 当初价值200美金）。显然，使用铸造和烧毁会以动态的方式改变标的资产的流通量。

这创造了与其他数字货币截然不同的有趣的供应方案，读者需要对其仔细琢磨才能充分理解避风港协议的概念。

iii. 离岸存储如何运作？

避风港协议使用“染色币”模型在避风港钱包内实现离岸交易。这是cryptonote协议上第一个实现染色币功能。染色币的概念的定义在比特币网络中是众所周知的，早在2013年这里就有描述：

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

然而，在cryptonode上的染色币不能以比特币上的相同方式工作，事实上，cryptonode上的染色币概念必须重新设计和塑造。感谢 Nate Eldredge对使用比特币和门罗币实现差异的清晰描述：

“对于比特币，交易的输入和输出之间有了一一对应的关系。假设一笔交易X，它的输出是X1向Alice的地址A发送了1聪，那么大家都同意输出X1被染色并授予了Alice的1977年雪佛兰新星的所有权。如果Alice决定把车给鲍勃，她生成一个新的交易Y，输入指向X1，其唯一的输出Y1向鲍勃的地址B发送1聪。现在鲍勃可以通过生成一个与他地址B相对应的签名来证明他是车的合法主人。

如果Mallory试图通过用输入X1创建一个不同的交易来认领汽车，她将会被发现，因为他不能用Alice的私钥签署该交易，所以它不能被验证。如果Alice试图通过输入X1创造第二个正确签名的交易Z将车给另外一个人，这笔交易将因为双花而被删除，因为在区块链上另外一个消费X1的交易先于它。

对于环签名来说，这种对应关系就被打破了。当创建一个交易时，除了您真正想花费的一个输出（来源于前一个交易的）外，您还可以列出许多其他的输出。你创造了一个签名，证明你被授权花费这些输出列表中的一个，但并没有给出任何关于是哪一個输出的信息。然而，一个相关的算法确保未来任何试图双花该输出的行为都会被注意到并被拒绝。

在上述情况下，如果Alice在她的交易Y上使用了环签名，不仅包括X1，还包括另一个输出Z1，那么她的签名不能证明她有权消费X1（因此是汽车的合法拥有者，可以送人），只能证明她有权获得X1或Z1之一。

此外，Mallory可以创建一个交易M，其中包含了X1和一个他有权消费的其他输出K1。由于她拥有与K1相对应的私钥，她可以正确的签署交易M，但不会清楚是花费X1（会转让汽车的所有权）还是K1（不会转让汽车所有权）。”

上述内容描述了比特币网络内对染色币的看法和实现方式，并且正好的指出，当X1和Z1在初始交易后仍然存在时，这种模式是失败的。然后，避风港的工作方式略有不同，避风港没有Alice，我们也没有Mallory，我们只有鲍勃。

当鲍勃把XHV转换成xUSD时他发送了一笔有两个颜色的交易，X(XHV)和Z(xUSD)。该交易仅以第一种颜色X的数字货币作为输入，同时X和第二种颜色Z作为输出。避风港网络中每笔交易都包含结果（#X,#Z）的两个值，并且对所有交易来说，这两个结果的值中只有一个可以为非零。

因此当鲍勃把他的200个XHV以每个XHV价值1美金的时候转换时，他发出的交易的输入为（200,0），输出值为（0,200）也就是给出的输出为了200xUSD和0XHV。如果XHV的价格变化为每XHV2美金时转换回XHV，那么将会发出交易的输入为（0,200）而输出值为（100,0）也就是给出的输出为100XHV和0xUSD。这样，在交易过程中，交易和UTXO的输入被永久有效实时的销毁了，输出也同时被铸造出来。

这一切都很棒，但是避风港是门罗币的分叉并继承了它所有的安全和匿名特性。而门罗是建立在对任何给定的交易的前提，条件和绝对的确定性上，输入和输出之间的差异为零。任何不满足这个要求的交易都会失败。

在避风港的情况下，门罗币的这一基本要求不可能满足的，事实上，对于XHV和xUSD之间的任何和每一次交换，XHV的价格不是精确的一美元，这一规则完全被打破了，输入和输出不会相等，我们承诺的C^a和C^b之和也是不会相等的，因此src/ringct/rctSigs.cpp verRctSemanticsSimple()将无法通过门罗的测试：

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

这里我们引入了避风港网络的“价值证明”的概念。

感谢门罗研究实验室提供的关于简明可链接环签名和伪造对抗性秘钥的论文[Brandon Goodell, Sarang Noether and Arthur Blue] <https://eprint.iacr.org/2019/654.pdf>，该论文已被用作避风港实现价值证明的一部分。

在论文的早期草案中，作者提出了一个“玩具”模型，他们创造了一种染色币，在两种染色币之间有固定的锚定：类似美元和便士之间1:100的兑换比例，并展示了使用CLSAG来实现这一目标。其过程如下：

1. 通过确定一个常数 ξ 和一些常数 γ_C, γ_D 为 $1, 2, \dots, 2^{\xi-1}$, 来确定交换汇率 (在本例中 $\gamma_C = 100$ 以及 $\gamma_D = 1$).
2. 改变承诺结构，使每一项承诺变成一对相应染色的承诺 C 和 D.
3. 从 Prove 中创建一个证明范围来覆盖 C 和 D 的值。这里 C 和 D 扮演的 Z_j 点的角色，P 是交易协议所需要的额外数据。
4. 当以下条件得到满足时我们判定一个简单的交易秘钥是有效的：
 - a. 每个输入的环成员 $(X_i, C_i, D_i, P_i) \in Q$ 有一个有效的证明范围 P_i 使得 $\text{Ver}(P_i) = 1$; 以及
 - b. 每一个输出的证明范围 $P \circ k$ 有效使得 $\text{Ver}(P \circ k) = 1$; 以及
 - c. 对于修改过的环 $pk = X_1 X_2 \dots X_n Z_1 Z_2 \dots Z_n$ 签名 σ 通过 2-CLSAG 验证, $\text{Verify}(m, pk, \sigma) = 1$.

这样做的效果是交易的签名不再承诺为零，而是承诺有差额——这个差额就是这个交易根据输入和输出创造的“代币”数量的差异。如果一个用户把 1 美金兑换成 100 便士，那么差额就是 99——也就是新铸币的数量。这个模型的工作原理是，为了让发送者使用差额签名，用户必须同时知道作为输入的硬币的数量（只有这些输入的私钥持有者才能知道），而且他们必须使用 100:1 的正确汇率，所有的防弹协议持有两种染色值。这么做，他们可以正确的使用输入和输出之间的差值进行签名，交易就会生效。

在考虑避风港铸币和烧币系统时，上述模型有一个重大缺陷。它需要一个固定的汇率。固定的，交易双方都知道的，以及其他所有交易验证者都知道的固定的汇率。这就给我们带来了一个问题，这个模型是行不通的，因为从定义上看，要把一个不稳定的资产跟一个稳定资产锚定，必须改变的就是汇率。

iv. 价值证明

要使上述染色币模型在浮动汇率的情况下正常工作，我们需要：

1. 获得大家都认可并无法更改的价格信息的方法，以便在任何时候，兑换交易都可以使用可被验证的价格。
2. 根据该价格将输入转换成输出的方法。
3. 验证交易发送方是否满足与任何其他cryptonote交易相同要求的方法，即他们知道所有输入的密钥，然后可以使用汇率进行转换，并签署具有正确差额的交易。
4. 验证商定的价格确实已应用于兑换中，但不向验证者透露任何数额的方法。

定价细节从真实世界的定价提供商（即定价预言机）获得，并且价格记录将在一个新的区块生成时创建。价格记录包含了当新的区块被挖出时每个Xasset锚定的汇率（相对XHV的）。价格信息每隔30秒钟更新一次，并根据避风港守护进程的请求显示。价格记录由挖到该区块的矿工将其打包进该区块的区块头中。

通过在每个区块中打包这些信息，协议保证了交易价值不能被篡改或改变——区块链保证了价格信息不可改变的。如果在当前价格记录的30秒生命周期内，有多个区块被成功挖出来，则同一个记录将被包含进多个区块中。

价格记录包含了以下汇率（都是以XHV为基准），以及一些保留空间以便将来增加数据和提供数据的预言机签名。一个价格记录的例子如下：

```
{
  "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
  }
}
```

价格记录示例: [Carbon](#)

2/ 避风港在上面（Bob）的例子使用承诺对而不是单个承诺值来实现。这也是门罗实验室的玩具例子中使用的方法。

3/ 避风港交易使用了上面所讲的CLSAG以及配对防弹签名。但是，我们不像玩具例子中那样使用差值进行签名。我们使用原始承诺的零值来签名，我们的承诺是价值的零差异。

4/ 这是它变的复杂的地方。要了解避风港如何使用价值证明来验证或拒绝交易。需要一点点的前期工作和对公钥算法的一些理解，以及Cryptonote如何使用椭圆曲线操作和点来验证输入和输出金额。

每笔交易都会经过函数`verRctSemanticsSimple()`对交易的所有输入和输出进行求和，检查结果是否相等。虽然在这个阶段，价值是完全加密的，并以椭圆曲线[‘EC’]点而不是实数来表示，但由于模块化算术特性以及门罗的EC点选择/生成的特性，让这些求和仍然可行。

简而言之，虽然数字是加密的，但它们仍然持有一定属性——他们之间的差值（在EC空间内）仍然有效，因此零差值仍然会是零差值因为承诺是叠加的。

换句话说，如果我们的交易的输入包含金额 a_1, \dots, a_j 以及输出的金额为 b_1, \dots, b_k , 那么观察者有理由期待:

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

对避风港来说适用于XHV, xUSD的转账者，但对兑换来说，这是完全错误的。

所以，重新适用上面的一些符号，让我们定义常数 γ_C, γ_D 作为一个单一交易的兑换汇率，这个汇率由我们的预言机提供。那么现在承诺在我们的证明范围内分别被配对为 (C, D) 。为了证明价值相等，我们要求输入的价值之和等于输出的价值之和。

我们现在的验证是这样的：

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

其中 λ_C, λ_D 表示括号内的数值根据各自 k 的汇率相加。 (C, D) 表示输入承诺， (C', D') 表示输出承诺。然后 $f_C G$ 表示支付的费用

v. 喂价预言机

为了从现实世界中获取数据，区块链使用了“预言机”的构造。“一个区块链预言机是一个第三方信息源，其唯一功能是向区块链提供数据。”

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

建立一个安全、准确以及高效的预言机被认为是协议成功的关键。不过，自从Chainlink等服务的创建和成功以来，他们的设计纯粹是为了提供作为独立数据源的预言机功能，现在很明显，不仅不需要在避风港系统中单独建立一个预言机，而且这样做也是不合适的。这样做会使转换方程最重要的部分——定价变的更中心化。

考虑到这一点，避风港协议与Chainlink合作，以利用他们的预言机网络来处理 and 提供价格数据。下面是Chainlink的XHV/USD的预言机：

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

避风港认为，从一开始就建立灵活的价格发现是至关重要的，避风港永远不会仅仅依赖一个预言机系统，而是能够随着时间的推移增加，更换和去掉预言机，以确保避风港使用现在和未来最佳的数据。

供应量场景

XHV是一个纯工作量证明（PoW）数字货币，其排放曲线与门罗币一致，最初可开采量为1840万枚，一旦开采出1840万枚，就会产生少量尾流量。

在数字货币市场，这是一个标准，非常容易理解的供应量场景。一旦避风港的离岸存储功能发布，上述数据将继续适用于挖矿奖励，但不再定义XHV的实际流通量，因为“铸币和燃烧”如前所述一般将流通量变成动态的。

此外，当未来xAssets（除了xUSD之外）上线以后，XHV的流通量不再能用来定义避风港生态系统的市值了。为此，有必要考虑所有xAssets的价值以及XHV本身的价值。

这里可以用HNV或者避风港网络价值来表示，计算方式如下：

$$\text{HNV} = (\text{XHV价格} \times \text{流通量}) + \text{xUSD流通量}$$

当其他的xAssets被加入到网络中能简单的加入到计算中。

要了解未来XHV供应量的趋势和供应量对避风港生态带来的影响，提出了以下高层次的宏观场景

这些场景中考虑的变量包括：

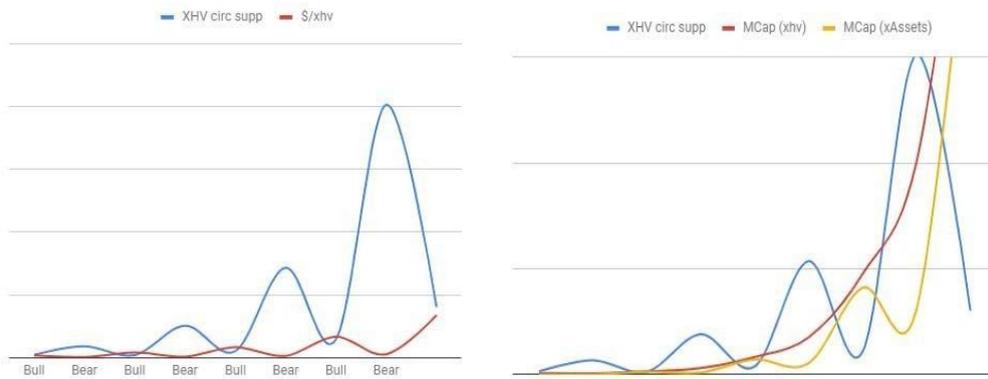
1. 牛市周期中总市值的增长情况（inc_Bull）
2. 熊市周期中总市值的减少情况（dec_Bear）
3. 牛市周期末尾XHV币离岸并储存百分比（perc_offBull）
4. 熊市周期末尾xAsset（以xUSD为例）返回XHV币的百分比（perc_onBear）
5. 所有离岸交易价值的平均值在牛市周期里XHV最高价的百分比（例如，如果XHV本次牛市最高价是2美金，80%的最高价就是1.6美金，如果我们使用80%作为这个场景中的变量的话，那么我们将1.6美金作为这次离岸价格的平均值）（perc_Lath）
6. 熊市周期里XHV的最低价格百分比，即所有该周期内回岸交易价值的平均值（perc_LATL）§
 - a. **注意：5和6的值可以被视为交易者在预测行情市场的顶部和底部的准确程度。*
7. 波动率指数-该指数用于模拟XHV的波动与比特币波动的相关性。值1表示等于btc波动，0.5表示btc波动的一半，2表示2倍的波动等等。（iVol）

场景1

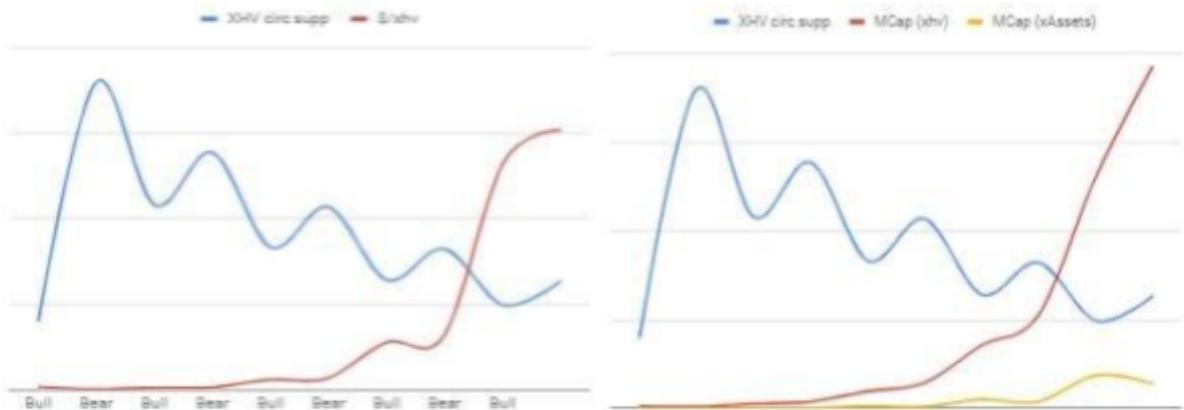
XHV供应增加

在这个场景下，我们使用的值将随着时间的推移增加市场上XHV的供应。

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



从这个高频的离岸使用和高交易准确性模型中可以看出，在增加场景中使用离岸功能可以保持XHV价格在较低水平，但随着时间推移，XHV和避风港整个生态系统的市值都会增加。这种情况对生态系统是可以接受的，因为它降低了XHV价格的波动性，这反过来改变了所显示的模式，从而摆脱了增加场景，并进入了均衡（甚至减少）。入下图所示，唯一变化是使用的iVol值为（0.5）

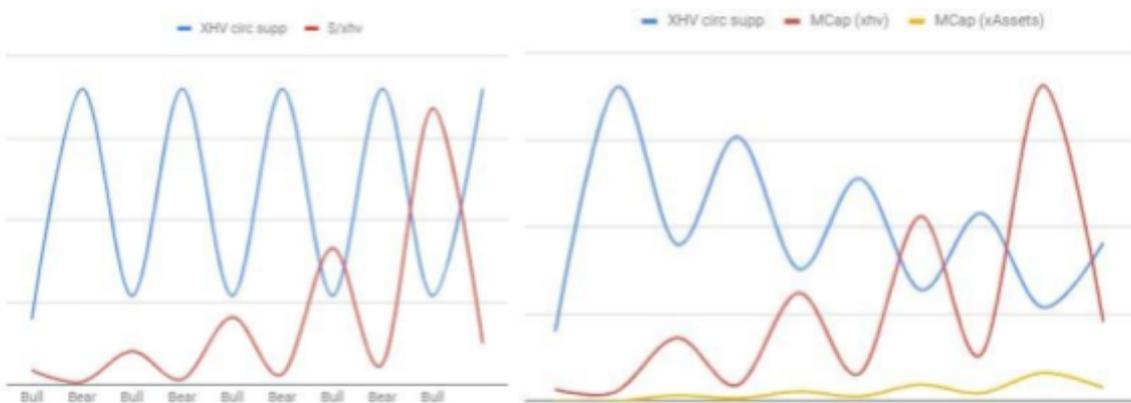


场景2

XHV供应减少

在这种情况下，使用的值会使XHV的循环供应中产生通货紧缩。

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



正如在减少情景中可以看到的那样，xhv的价格波动性增加，随着时间的推移，会产生与减少情景相反的效果，并将模式从通缩转向均衡或增加。

场景3

XHV供应平衡

在这个情况下，预测变量的设置具有中等的离岸使用频率和中等的交易精度。作为其他两种情况的中间情况，人们可以预期，随着时间的推移，这种情况会反复上演，增加和减少的情况都会区域平衡。

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



总之，我们无法预测在任何给定情景下会发生什么，随着时间的推移，该协议旨在直接通过用户的行为直接增加和减少HXV的供应量，而适应不断变化的使用水平，从而创造出一条源于自然和有机使用的独特供应曲线。

稳定性和经济学

需要很少的条件就可以以基本形式实施铸币和燃烧，只需要知道执行兑换的价格，以及可以在同一条链上把一种资产以这个兑换比例兑换成另一个资产的能力。

显而易见，这是一个非常简单的概念。这就是说，最简单的概念有时候是最难完全理解的，为了确保避风港生态系统使用强大的经济模型，我们必须解决以下挑战：

1. 供应量透明性
2. 基于交换价格的操控
3. 证明和维护在PoW算法生态系统中合成资产的价值
4. 在市场大范围波动期间“挤兑银行”的可能性

这些挑战将逐一解决：

供应量透明性

避风港最初的概念是基于XHV和xAsset流通供应为未知的。这样的理由是为了防止XHV或xAssets的大户操控网络。

经过慎重考虑，社区讨论以及与专家顾问的协商，决定建立透明的流通量，实际上对网络有以下好处：

- 它可以更有效的监控避风港网络，这意味着可以更快的发现和缓解企图攻击和大规模操纵币价的行为。
- 它可以让用户在任何时候查看该时刻的XHV和xAssets的流通数量，这会让他们更有信心加入避风港网络。
- 它能让货币标准网站中获得更好的可见性和可分析性。因此，为了确保准确性和可见性，每个铸币和烧币交易创建以后，将可以通过区块链分析来发现其数量，然后在避风港区块链浏览器中显示出来。这样可以让用户保持标准的门罗匿名性和钱包地址的隐私水平，同时允许清晰的查看流通量。

各种类型资产的流通量都可以在这里看到：

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

基于交换价格的操控

基于铸币和烧币的性质，避风港长期以来的承诺是“1xUSD永远可以兑换价值1美金的XHV”，并且避风港的定价系统利用移动平均价格来保证价格变化平滑，因此需要采取一定的措施来最大限度的确保减少交易交换价格和离岸/在岸兑换价格之间的差异。

这个最小化是通过允许用户选择交易优先级来实现的。优先级越高的交易，解锁时间最短，将比解锁时间长，优先级低的交易（费用将趋近于0）收取更高的费用。

自从首次上线以来，避风港贡献者们一直在监测和分析从第一个月实际使用中得到的数据。自首次推出以来，原有的费率结构已被一个简单得多，更严格的方案所取代，以确保网络短期内的健康发展，同时保护早期的持有者。随着时间的推移，避风港的费率结构设计将需要重新审视和改变，与避风港网络一起变的更成熟。避风港网络的完整费率结构将与本文一起发布，并在官网上随时维护以供参考：<https://havenprotocol.org/fees>

许多现有DeFi产品的问题之一是，你必须在钱包里有一个特定的代币，才能转账其他的类型的币。这可能会在使用中造成不必要的摩擦和成本。

避风港交易通过以发送的货币为收费币种收取费用来接这以问题。如下表所示：

转账类型	收费种类	费用支付使用:
XHV转账	标准转账费用	XHV
xUSD转账	标准转账费用	xUSD
XHV -> xUSD 转换	转换费 + 标准转账费	XHV
xUSD -> XHV转换	转换费 + 标准转账费	xUSD

证明和维护在PoW算法生态系统中合成资产的价值

算法合成资产的最大挑战之一，也是最常被问到的问题之一，是围绕着“真实价值”或者“价值来源”的概念。类似“当xUSD没有抵押品支持时，你怎么能说它值1美金？”这样的问题经常被用户提及。

一旦这个问题得到了答案和理解（xUSD是由不同的和适量的XHV“间接支持”），用户就会关注有关XHV本身的供应量和流动性的问题。由于如上所述，XHV供应量将因为离岸交易产生波动，供应量的扩大和收缩的情况都可能改变整个生态系统的动态。

考虑到数字货币市场的周期性，这两种情况出现的可能性很大。这既是可预料并可以接受的。流量的波动绝对需要允许xUSD供应量的增加和缩减而不对XHV的价格造成过大的波动。

在市场大范围波动期间“挤兑银行”的可能性

在任何商品的上升市场周期（“牛市”）中，交易者通常会离开稳定的选择而选择波动性的资产，反之亦然。对于传统“背书”的稳定币比如USDT，背书货币量是被背书数字货币稳定性的关键。任何“背书”价值和“市场”价值的偏离都会给用户带来真正的危险，会造成一种情况，即有可能出现无背书的价值，并与该数字货币应该追踪的任何背书资产的脱锚。

因为避风港使用铸币和烧币以及染色币，所以不会有这类问题。

任何时候，任何情况下，用户可以将1xUSD兑换成等值一美元的XHV，这个锚定永远不会被破坏。

由于避风港协议是使用染色币模型实现的，因此它不仅能支持xUSD，还能支持一系列我们称之为“xAsset”的其他资产和商品。这使得XHV本身不仅可以成为一种，而是一套隐私合成资产的抵押物，扩展了锚定机制的可能，并将协议变成了一个对数字货币用户具有真正用例和价值的平台。

W避风港团队都有谁？

避风港团队是一个由开发者和贡献者组成的社区集体，因此欢迎所有人的投入和贡献。

核心开发团队名单如下。

自从从原开发团队接过项目的管理和开发工作以来，社区受益于几位以实现避风港的承诺作为自己使命的顾问，咨询师和技术行业专业人士的持续支持和指导，并推动数字货币领域这一重要部分的被接受。非常感谢这些人的持续支持和投入。

核心开发团队：

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

作为一名专注于产品战略和交付的职业技术专家，David在过去20年中曾在英国的大型企业和多家科技创业公司中担任高级职位。他拥有数学、加密技术和软件开发的背景，他为避风港带来了技术交付和大规模管理方面的丰富经验。

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

Neil是一名专业的全栈软件构架师和开发人员。Neil在X86汇编器、C++、Java、PHP和Javascript方面有超过20年的开发经验，在过去18年里，他一直致力于设计和构建加密软件。

@Marty (anonymous)

Marty是一名拥有众多构架方面经验的前端设计师，他在避风港钱包和网站上的工作将这一点发挥的淋漓尽致。

@Pierre Lafitte (anonymous)

Pierre是一名产品设计专家，负责创建避风港产品组合中的所有用户体验和UI。Pierre是一名经验丰富的前端加密开发人员，是避风港的长期贡献者，他将领导UX/UI方面的开发，并将团队的UX愿景变为现实。