EASH 稳定币白皮书

目录

1. 背景

随着数字货币在人气指数和投资者兴趣方面持续飙升，其应用范围也越来越广。但数字货币价格的波动，阻碍了它们作为交换媒介和记账单位的使用。比特币和以太等流行的数字资产太不稳定，无法用作日常货币。比特币的价值经常会出现大幅波动，一天内上涨或下跌多达 25%的波动。

一种常见的解决方案是创建一个有稳定价值的代币（称为“ 稳定币 ”），以固定的 1：1 汇率换取指定的法定货币，如美元，然后由发行人将加密代币分配给客户。 由于美元是一种比较理想的交换媒介，以及全球公认的记账单位，所以目前它是稳定币较为理想的锚定物。

市面上已经提出了几种盯住法定货币的稳定币，例如 USDT、GUSD、Base Coin、Maker Dao 等。这其中又包含中心化解决方案的和有抵押担保的解决方案。

这些稳定币大多是基于以太坊平台上发行的 ERC20 代币。为了扩展以太零生态平台的应用，我们在以太零平台上实现发行了稳定币--EASH，它是一种抵押品支持的加密货币，锚定美元价格，可以实现 1：1 兑换，其价值相对于美元是稳定的。

2. 创造、赎回、交易

EASH 是以太零平台上发行的 ERC20 代币，以 ETZ 抵押担保生成，可以在以太零系统中转移。创建、赎回、交易的功能通过智能合约实现。

任何人都可以利用他们的以太零资产在 EASH 平台上生成 EASH。一旦生成，EASH 可以与任何其他加密货币相同的方式使用，它可以自由发送给其他人，用作

商品和服务的付款，或作为长期储蓄持有。EASH 的产生创造了一个强大的分散保证金交易平台，为稳定币的应用提供系统平台支撑。

2.1.**抵押 ETZ 获取 EASH**

用户首先向智能合约发送交易以创建抵押头寸，其中包用于生成 EASH 的抵押品 ETZ，并获得相对应数量的 EASH。并且同时，抵押合约累积等量的债务，锁定他们无法获得抵押品直到支付未偿还的债务。

抵押比例设定为 1：1。抵押的价格参考 ETZ 的实时价格，格参考各主流交易平台价格的加权平均，采用最接近成交价格的平均值进行抵押。

示例：

Allice 手里有 10 万个 ETZ，当前 ETZ 的价格是 0.3USD/ETZ。那么 Allice 可以将这个 10 万个 ETZ 抵押在智能合约中，获取 10 万*0.3=3 万个 EASH。

2.2.**赎回 ETZ**

用户可以通过向合约发送交易，将抵押品回收到自己的钱包中，不受以太零价格涨跌的影响。抵押过以太零的地址通过智能合约记录，相同的地址可以用合约初始约定的抵押价格解除抵押，获取原先抵押数量的以太零。抵押单持有时间超过三个月才可以赎回。

用户在赎回页面检索到他们自己的抵押头寸，可以选择一张抵押单全部赎回，也可以选择一张抵押单的部分赎回。

示例：

Alice 手里有 10 万个 ETZ，以 0.3USD/ETZ 的价格获得了 3 万个 EASH，那么 Alice 就获得了一份抵押单，她在任何时间都可以用 0.3USD/ETZ 的价格赎回这张抵押单。

假设 Alice 赎回全部的 3 万个 EASH，她将会得到 3 万/0.3=10 万个 ETZ。

假设 Alice 赎回 1.5 个 EASH，她将会得到 1.5/0.3*=5 万个 ETZ。剩余部分的抵押单继续存在，Alice 还有权利继续赎回剩余部分的 EASH。

2.3.做市商

只有做市商才能抵押和赎回 EASH，做市商的门槛是抵押 10 万个 ETZ，当抵押超过 10 万个 ETZ 时，自动升级为做市商。做市商抵押得到 EASH，每 10 天解锁总量的 1/10，到 100 天结束时，抵押得到的 EASH 全部解锁可以交易。

2.4.EASH 交易

普通用户可以通过交易来购买或出售 EASH，维持 EASH 交易的流动性。交易价格按照 ETZ 的实时价格来计算。

示例：

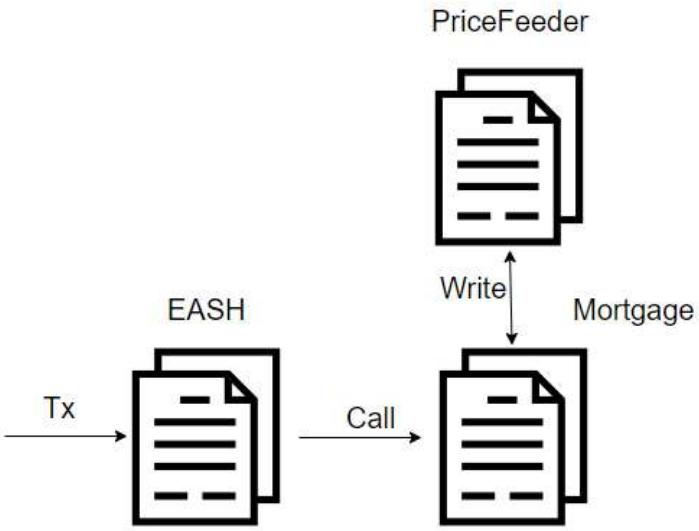
Alice 手里有 10 个 EASH，当前 ETZ 价格为 0.3USD/ETZ，而 Alice 手里没有任何抵押单。那么她可以通过交易的方式，将 EASH 兑换成 ETZ。

如果选择兑换，Alice 将会得到 10/0.3=33.33 个 ETZ。

3. 合约设计

合约架构

我们通过建立一个彼此合作的智能合约系统来实现 EASH 抵押系统，在下面更详细描述。系统的核心部件是 EASH 合约，负责在太零平台实现符合以 ERC20 标准的稳定币发行，Mortgage 和 PriceFeeder 合约分别负责抵押和喂价。合约提供了代币持有者可以与之交互，并执行诸如转移代币和查看代币余额等操作的接口。



价格测定

价格测定的方案采用从多个价格源测定，然后进行投票选举的方案，保证了链上价格的稳定性和安全性。

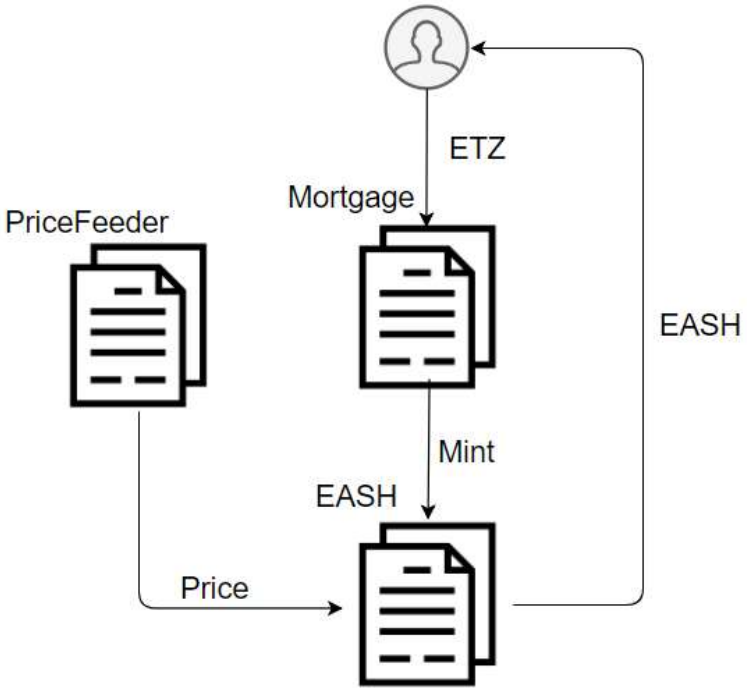
如下，有五个价格源提供价格，这五个价格提供者分布在不同的服务器上，合约中采用最接近的三个价格的平均值作为测定的价格。这样即使其中的两个价格源出现问题，系统还是能正常运转。

抵押赎回

用户抵押产生 EASH 的过程为，调用 Mortgage 合约，并向合约发送 ETZ。Mortgage 作为授权的可信合约，调用 EASH 代币合约，增发对应数量 EASH，然后将增发的 EASH 发送到用户账户地址。增发的数量根据喂价合约 PriceFeeder 提供的价格，通过如下公式计算：

$$\mathrm{EASH}_{amount} = \mathrm{ETZ}_{amount} * Price$$

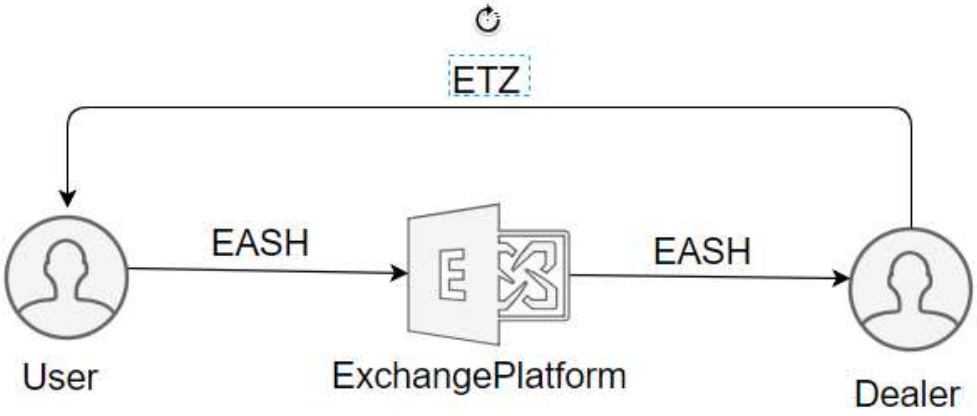
赎回是相反的过程，将用户账户地址里的 EASH 销毁，然后将锁定的 ETZ 返回给用户账户。



交易

用户通过其他途径得到的 EASH 可以进行交易，交易通过法定的交易商完成，用户将 EASH 传递给交易商，然后得到对应价值的 ETZ。获得 ETZ 的数量通过如下公式计算：

$$\mathrm{ETZ}_{amount} = \mathrm{EASH}_{amount}/Price$$



4. 风险控制

用户抵押获取了 EASH，当 ETZ 升值的情况下，用户赎回抵押合约时能赎回同等数量的 ETZ，享受 ETZ 升值带来的红利。当 ETZ 价格下跌的情况下，也需要承担部分价格下跌带来的损失。假设极端情况，ETZ 突然发生市场崩溃，并且合约中最终包含的债务超过其抵押品的价值，则以太零基金会向平台注入 ETZ，保证 EASH 币值的稳定。

这样链上进行抵押结算的稳定币更为透明安全，不用担心它的背后没有对等数量的资产来支撑 EASH 的价格。

5. 合约保障

对于合约系统中的某些高风险行为，系统中设计了分级审批机制。系统中的每个智能合约都要求托管人批准。 托管人可以是另一个智能合约。A 托管人可以查看另一名托管人 B，此 B 托管人可能会继续查看下一名托管人 C，依此类推，从而形成监管链或 “托管关系” 。

系统实现了以下安全功能：

1） 离线密钥：高风险操作的密钥在专有的冷存储系统中脱机存储。

2） 密钥生成：密钥是在硬件安全模块（HSM）上生成，存储和管理的。 我们只使用 HSM，每个“签名者 ” 的技术规格已达到 FIPS PUB 140-2 Level 3 或更高等级。

3） 双重控制（多重签名）：高风险行为需要至少两名签名者的批准（即多重签名）。 我们利用 N 个中 M 成员要签署的设计方案，选择了 M = 2，这同时提供了安全性和容错 。

6. 应用示例

任何人都可以使用 EASH 系统，不受任何注册限制，下面给出 EASH 应用场景的示例。

示例：抵押消费

Tinna 需要贷款，因此她决定生成 10 万 EASH。她将价值为 10 万 EASH 的 ETZ 锁定到抵押合约，并用它来产生 10 万 EASH。100EASH 立即直接发送到她的账户。Tinna 可以将部分 EASH 用来消费，到电商平台购买商品。如果她决定在一年后取回他抵押的 ETZ，那么合约将发送给她对应的 ETZ。