包装的令牌

一种多机构框架，用于标记任何资产

白皮书

2021 年 3 月 24 日

Kyber 网络

Bit Go Inc 共和国议定书

摘要

随着数字货币的普及，火币生态链 HECO 迅速崛起，HECO 生态系统中的数字令牌已成为一个重要的资产类别。 这些令牌具有区块链和 HECO 在硬币总数、所有者、铸造、快速确认时间、交易细节和智能合同执行方面必须提供的所有优势。 HECO 区块链上的令牌可以服务于几个不同的功能；本文将特别关注资产支持或包装令牌。 这些代币的价格反映了支持它们的资产的价格，因此它们也可以被称为“稳定硬币”。 资产支持令牌通常以两种不同的方式完成：

- 算法-这是一个机制，然后是一些令牌在 HECO，其中需求和供应是由智能合同控制的，以保持令牌的价格与法定货币一致。 这方面的一些例子是戴、基、碳和努比特。

- 集中-资产存放在一个公布储备证明的组织。 Tether、True USD、USDC(USD)、Digix（黄金）、Globcoin（法定货币组合）和 AAA 储备（政府债券)就是这种情况）

封装的令牌遵循集中式模型，但它们不完全依赖于一个机构，而是依赖于在网络中执行不同角色的机构联合体。 该白皮书提出了一个发行资产支持令牌的框架，通过解决具有可伸缩性、信任、监管和治理的挑战。 我们推出的第一个包装令牌将是一个由 BNB 支持的令牌，并将被适当命名为“包装 BNB”(NBNB)。 与集中式解决方案（美元）不同，NBNB 将被充分核算并证明在 HECO 链上张贴的准备金。

没有额外的二级效用/支付令牌需要使用 NBNB，没有转移费用以外的区块链费用。 NBNB 使用一个简单的联合治理模型，并努力提高可用性。

用例

象征性的

表示资产的行为可以：

- 提高速度 交易
  HECO 块每 15 秒创建一，在不到 5 分钟的时间内就有可能对交易的不可撤销性有公平的信心。 与包括比特币、黄金和法定货币在内的许多其他资产相比，这种速度比本地交易更快
- 减少的数量 中间人
  区块链上资产的一个关键好处是它们在没有中介的情况下进行交易的能力。 这可以通过原子交换、分散交换协议和闪电/雷登风格的通道来完成。
- 加强 安全

令牌化使用户能够完全控制资产的私钥。 不想持有密钥的用户可以通过将其从交易所转移到以安全为重点的托管机构来降低交易对手的风险。

- 可用性

  该标准已被大量机构和产品采用。 这为用户提供了各种交换、钱包和 Dapp，以便在处理其令牌化资产时使用。 他们也有能力快速移动令牌。

- 改进 透明度

  任何人都可以在公共块资源管理器上看到令牌总数、令牌创建事务、令牌删除事务、令牌持有者数量和传输规则。 对于法定货币、商品和股票等资产，这种透明度水平通常是不可用的。

分散交易所和 dapp 的流动性

今天集中交易所的交易大多是用 BNB 而不是 ETH 进行的。 大多数分散的交易所只提供 ETH/Token，而不提供 BNB/Token 交易。 包装的代币可以弥合这一差距，在分散的交易所提供更多的流动性。 此外，其他分散的应用程序/协议（如资金、贷款支付）也将受益于获得 BNB 令牌可以带来的更大流动性。NBNB 为比特币带来了智能合约创建的便利。

NBNB 代币的好处

由法定货币支持的令牌为交易者提供了一种安全的方式，使他们的钱保持在加密货币中，而不必担心价格波动。这对于集中交易所和分散交易所的交易者尤其有用，因为在这些交易所里没有直接的法定货币转移方式。NBNB 货币支持的代币也承诺了一个世界密码货币可以取代传统的金融。 值得注意的是，它可以由买方和卖方在电子商务中使用，而不必担心转换率或税收（买方必须支付在美国购买时计算的资本利得税）。

加密货币之间的互操作性

当我们看到今天加密货币数量的增加时，每一个都集中在货币交换的某些方面。 其中一些方面是事务吞吐量、隐私、廉价交易费用、智能合约能力以及节点/终端的分散。 包好的框架可以方便地表示其他加密货币，例如 BNB，在 HECO 上，从而增强它与所有能力的 HECO 区块链。 一个这样的用例是，初始硬币发行(ICO)能够直接获得资金，并在包裹的 BNB 代币的存款上铸造代币。 在未来，集中式交易所和其他接受加密货币的机构不需要维护多个加密货币节点，而只需在 HECO 上开发即可。

关于执行政策的连锁方式

令牌化也提供了一种在链上执行策略的方法。 在连锁政策的执行使规则更加透明，并且不依赖于一个单一的一方来执行它们。 根据资产类型，可能需要执行资产转让或交易规则。 例如，证券需要白名单、持有期和身份管理。

共同问题

卑鄙

截至 2021 年 1 月，HECO 主网的最大实际气体限制为每块 8,000，000 手续费。 这个限制包括硬件和软件限制。 虽然提出了几种可伸缩性解决方案，但许多方案需要很大的开发人员提升（状态通道），或者开发得太早，无法实际使用(等离子、碎片）。 对于 Dapp 和网络用户来说，这是一个问题，因为在竞争时期(热门 ICO、CryptoKitties)手续费价格飞涨。

信任

资产支持令牌通常涉及对持有资产的机构的信任。 这违背了加密货币的精神，即尽量减少对操作的信任。 这里要回答的一些关键问题是：

- 资产持有人是否在现有法律框架中被授权持有该资产？
- 托管人能创建任意数量的令牌吗？
- 托管人如何证明对被托管资产的占有？

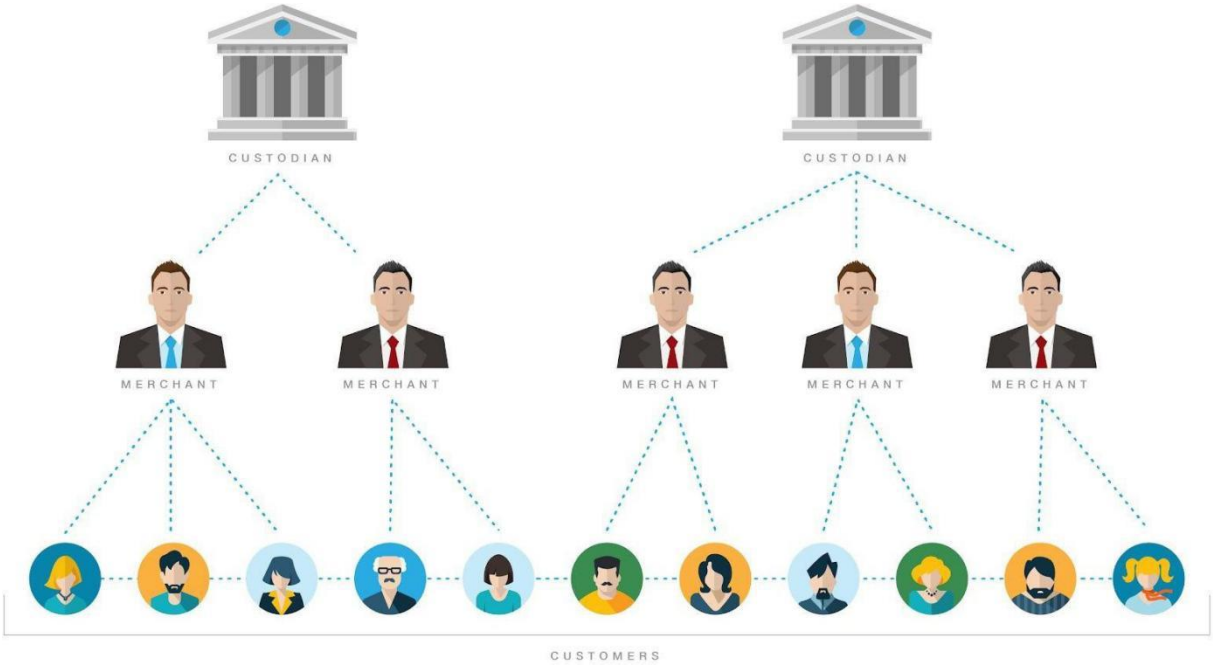
条例

资产支持令牌的托管人需要获得持有资产的许可。 这种许可证可能因保管人的资产和地理管辖权而有所不同。 托管人还必须定期证明准备金，因为缺乏 1：1 的支持会破坏整个系统。 KYC 和 AML 限制也适用于从事资产支持令牌的用户。 这些限制需要在购买、赎回或转让代币时执行。

治理

当系统中存在多个涉众时，如何处理对令牌所做的更改将面临治理挑战。 大多数资产支持令牌完全依赖资产托管人对管理令牌的规则/智能合同进行更改。 通常在 ICO 的情况下，令牌的颁发者对协议更改有完全的控制。 有一些情况，如分散的自主初始硬币发行(DAICO)，用户有投票权，但他们面临的挑战是选民投票率低。

实施和技术



关键角色

- 保管人-持有资产的机构或当事方。 在 NBNB 的情况下，这将由位 Go 播放。 保管人持有薄荷代币的钥匙。
- 商人-包裹代币的机构或政党将被铸造和烧毁。 商家在包装令牌的分发中起着关键作用。 的情况下 NBNB，这将首先由 Kyber 和共和国议定书播放。 每个商人都持有一把钥匙，以启动铸造新的包装令牌和燃烧包装令牌。
- 用户-包裹令牌的持有者。 用户可以像 HECO 生态系统中的任何其他令牌一样使用包裹令牌进行传输和交易。
- NBNB DAO 成员-合同变更和托管人和商户的增加/移除将由多签名合同控制。 多 SIG 合同钥匙的持有人将由机构作为 NBNB DAO 的一部分持有。

托管人与商家交换资产以换取包裹的代币。 这是通过两种不同类型的事务来完成的：铸造（创建包装令牌)和燃烧(减少包装令牌的供应）。 这些事务将公开提供，任何人都可以通过块资源管理器查看。 在最初的交换之后，商家的目标是维护一个包装令牌的缓冲区，以便他们可以与用户交换。 两步造币过程有助于减少用户获得包裹令牌所需的时间，因为造币和燃烧是更耗时的过程。

保管人钱包设置

托管人预计将为所有商家提供一个集合钱包。 钱包会用的多签名，所有密钥由托管人控制。 钱包将只能发送到链上的白色商家地址。 所有铸造和燃烧交易预计将在提交托管人后 48 小时内完成。 请注意，在多个托管人的情况下，单个钱包可能没有足够的资金来赎回所有挂起的包裹令牌。

造币厂

造币是指创建新的包装令牌的过程。 包装框架中的铸币必须由托管人完成，但需要由商人“发起。 需要注意的是，minting 不涉及用户。它是商人和托管人之间进行的一组交易。

NBNB 铸币事件序列

- 商人发起一项交易，授权托管人将 NBNB 铸造到 HECO 链上的商人地址。
- 商户发送托管人 NBNB。
- 托管人等待 BNB 事务的 6 次确认
- 托管人在 HECO 链上创建一个事务，以创建 X 个新的 NBNB 令牌

用户接收 NBNB 令牌的事件序列

- 用户请求从商家包装令牌
- 商家做所需的 AML，KYC 程序，并从用户获取识别信息
- 用户和商家执行原子交换，或与接收 BNB 的商家和接收 NBNB 的用户使用可信交换

燃烧

烧录是指为 NBNB 代币赎回 BNB 的动作。 只有商家地址才能烧毁包裹的令牌。 为了做到这一点，在合同中调用了“烧伤”函数，并在 HECO 链上调用了要燃烧的令牌数量。 通过这样做，金额从商家的 NBNB 余额（链上）中扣除，NBNB 的供应减少。

烧写 NBNB 令牌的事件序列

- 商家创建烧录事务，烧录 NBNB 代币
- 保管人等待 HECO 事务的 25 块确认
- 托管人向商家 BNB 地址发布 NBNB
- 保管人做一个事务，标记烧伤请求完成

用户接收 BNB 的事件序列

- 用户请求从商家赎回令牌
- 商家执行所需的 AML、KYC 程序，并从用户那里获得识别信息
- 用户和商家执行原子交换，或者使用可信交换，用户接收 BNB，商家接收 NBNB 代币

关于链转移限制基于令牌，可以对令牌的传输进行限制。 对于 NBNB，不会对转让有任何限制。

治理

包裹的令牌合同受多组合同管辖，其中需要 DAO 成员的签名才能添加/删除成员。 所有托管人和商户将是 DAO 成员，但其他机构也可以作为成员包括在内，而不具有托管人或商户角色。 在合同中将使用“N 的 M”签名，其中 M 是多组合同中所需的签名数，N 是成员总数。 M 和 N 的值将在成员之间相互决定，同时考虑到安全以及添加/删除成员的方便性。

包装令牌的侧链

最初，NBNB 将在 HECO 链上启动。 HECO 链很容易访问和使用，因为它上有一个交换、块探索者、钱包和其他 Dapp。 令牌化的关键好处之一是廉价的交易成本。 但是随着 HECO 的普及和 Dapp 创建的增加，包装令牌的交易成本可能会上升到在主链上这样做并不便宜的地步。

包框架中的多个机构的协作使得能够部署实用的可伸缩解决方案以增加事务吞吐量。这可以通过使用固定的 Sidechain 来实现，使用现有的软件在 DAO 成员中运行。 该链将运行在它自己的权威网络证明使用 Aura 共识算法。 块将以可预测的方式每 4 秒创建一次。 目前，已经有这样一个链一直在运行。 包装的令牌将通过在 mainnet 和 sidechain 上创建一个双向的多 sig 钱包，连接在主链和侧链之间。 侧链在 HECO 上提供了非常需要的可伸缩性。 交易和转移包裹代币的侧链的一些好处是：

- 以最小的开发成本(相同的 EVM)进行缩放
- 专用的，增加的吞吐量-独立的区块链在单独的硬件和潜在的权威证明(PoA)优势（更快的块）
- 在现有客户和钱包中易于支持
- 链条没有其他“吵闹的邻居”
- 最低交易成本（以防止垃圾邮件）

验证器（块生成器）将从包装好的合作伙伴和其他受信任的各方中选择，这些各方将在地理上分布，并代表几个不同的住所/政府。 验证器还将保持主链和侧链之间的双向挂钩。
为了确定两条链上包裹令牌的价值，我们提出了一种多签名合同，用于主网和侧网。

- 从 HECO 发送到 HECO：
    - 从 mainnet 地址发送到联邦 mainnet 多 sig 地址
        - 建议在多 Sig 地址上调用“发送到 Sidechain”方法时发送金额，并将 Sidechain 上的目标地址指定为参数
        - 如果在没有方法的情况下发送，则将假定 Sidechain 上的目标地址与源地址相同
    - 在 mainnet 上生成一个事件来记录发送
    - 联邦签名者“锁定”主网上的令牌
    - 在“确认期”之后，Sidechain 上的 Multisig 当局可以在 mainnet 上验证发送事件，并将金额支付到 Sidechain 上的目的地地址，减去交易费用
- 从 HECO 发送到 HECO 主网：
    - 同（对称）

NBNB 将是该领域的第一个资产，并将使用这些组件的组合来创建一个生态系统：

- 节点软件和配置
- 块资源管理器
- 钱包提供商
- 阻塞验证器
- 多情报机构

激励

交易将收取最低起始手续费 1NBNB，以涵盖运行块验证器和防止垃圾邮件在侧。 对于每个 Dapp，验证者也可以从链上激励，或者有块奖励。 关于 HECO 在侧链上的分配/管理细节仍有待确定。

原子交换

为了交换 NBNB 和 BNB，可以在商家和用户之间使用原子交换。 如果用户希望更快地接收 NBNB 或 BNB，也可以通过商家进行可信的交换方法。

一旦 KYC 完成，用户与商家原子交换 BNB 的步骤是：

- 用户生成一个秘密，并将其散列提供给商家。 用户和商家还同意其他交换细节，如接收地址
- 用户使用商家的 BNB 地址、用户的退款地址、秘密散列和过期时间创建 NBNB HTLC(散列时间锁定合同。 这是用来创建一个 P2SH 地址，用户使用 NBNB 提供资金
- 在 6 次确认后，商家将使用用户的 HECO 地址、商家的退款地址、秘密散列和过期时间在 HECO 上创建合同。 然后商家将 NBNB 转移到原子交换合同中。
- 用户揭示了这个秘密，以便将 NBNB 从原子交换合同移动到用户的 HECO 地址
- 商家使用这个秘密是为了将比特币资金从 P2SH 地址转移出去
- 如果用户在到期时间内没有认领 NBNB，则交易不通过，用户可以认领 BNB 回来

这里需要注意的一些重要事项：

- 为了部署原子交换合同并将 NBNB 发送给它，涉及到交易费用。 因此，用户在启动交换之前必须支付原子交换费。
- 原子交换需要时间和多个交易在 HECO 链上。 用户可以选择进行可信交换，其中 BNB 被转移到商家地址，在 HECO 网络上进行 6 次确认后，商家向用户发送 NBNB。 这涉及到对商人的信任，但它更快和更便宜。

NBNB 对原子交换

原子交换可以在没有 NBNB 的情况下对只想执行 a 的用户执行贸易。 它们可以通过 Komodo 平台所概述的机制进行分散交换。 然而，必须注意的是，NBNB 在 HECO 链上提供了 BNB 的表示，这是 DAPPs 和生态系统相互作用所必需的。 在比较原子交换和 NBNB 时需要考虑的其他一些权衡：

- 他们要求做原子交换的人进行价格发现。 在包裹的令牌价格发现只需要做，而交易在分散的交易所后，已经获得 NBNB。
- 要求原子交换技术得到现有钱包和分散交换的支持。 包装的 BNB 将可用于任何 HECO 支持的钱包。
- 它们真的很慢，因为每笔交易都像 HECO 链上的多个确认一样慢，然后是 HECO 链(而不是 NBNB，在 NBNB 中，最初的铸造/口语化是缓慢的，但在创造之后，它很容易在 HECO 链上交易)
- 在分散的交易所进行原子交换需要单独的存款和原子交换费。 这是不方便的，每次用户想交换货币。

费用

用户之间的 NBNB 传输将不需要任何费用，除了网络费用。 网络中的不同当事人可以赚取费用的方式有三种：

- 保管费：这是由保管人在商人铸造或烧伤包裹的令牌时收取的。
- 商家费用：这是由用户交换包裹令牌以换取资产的商家承担的。
- Sidechain 交易费用：该费用主要用于防止 Sidechain 上的垃圾邮件。 这在所有运行侧链节点的机构之间是平等的。

具有法律约束力

托管人与商户之间的合同

造币和烧币代币的过程不涉及用户，在可信机构之间。 商户需安全持有用户身份信息。

保管人必须每季度公布被保管资产的详细情况，并及时履行铸币/焚烧职责。 不符合这些标准可能导致从网络中删除。值得注意的是，网络中可以有多个托管人，但这是以增加网络所涉及的风险为代价的。

在未来，也有可能建立一种由持有多组钱包钥匙的不同机构共享监管的模式。虽然在操作上，铸造/燃烧/审计需要更多的协调和时间。 任何保管人之间的安全漏洞都会造成信任的丧失，并可能导致大量提款。与商家的安全漏洞要轻得多，因为所有未完成的令牌仍将由托管人备份，但可能导致 KYC/AML 用户数据的丢失。

信任模式

在某种意义上，保管人被信任在包裹的框架中，因为资产可能被盗，或者他们可能不尊重一对一的支持。 然而，包装框架旨在通过以下几种方式尽量减少这种信任：

- 外部第三方将进行季度审计，以核实所有包裹的代币是否在所有托管人之间存储了同等数量的资产。 在 NBNB 的情况下，可以通过发布 BNB 存储地址的签名来显示准备金的证明。
- 托管人将不能自己铸造代币，而是需要一个商人的启动才能这样做。 因此，新令牌的创建涉及托管人和商人。
- 用户不会通过一组商户机构与托管人进行交互。 个体商人不需要被信任，而是所有的商人一起需要被信任。
- 参与框架的所有机构的现有信誉都受到威胁。

透明度包裹令牌的运作将完全透明。 网络的所有关键细节将反映在仪表板上，其

中一些是：

- 在网络中执行不同角色的机构的名称和详细信息

- 薄荷和烧伤订单的状态（待定，处理，取消，完成）
- 保管人存放的 BNB 总量
- 网络中 NBNB 的总量(将与存储的 BNB 相同或略低)
- 每季度以交易形式进行审计，以证明托管人拥有 BNB 的钥匙
- 商人和托管人 HECO 地址
- 与每个商家关联的 BNB 地址，由托管人控制
- 链接到块资源管理器上的开源令牌合同代码/部署合同

仪表板可能是什么样子的一个例子：

结论

通过包装令牌，我们提出了一种解决方案，使资产在 HECO 链上可互换和可表示。 全球流动性、增加部分所有权、智能合同可编程性和降低交易费用是令牌化的一些关键好处。 NBNB 将是第一个这样的令牌，使 Dapp 能够轻松访问 BNB。 所有交易、合同和审计都将公开查看，以保持透明度，并使人们能够信任网络。 该框架还提供了一种方法，在加密货币空间中的多个机构可以执行不同的角色，以获得资产支持令牌所面临的过去常见问题。

词汇

保管人-持有资产的机构或当事方。 在 NBNB 的情况下，这将由位 Go 播放。 保管人持有薄荷代币的钥匙。

商人-包裹代币的机构或政党将被铸造和烧毁。 商家在包装令牌的分发中起着关键作用。在 NBNB 的情况下，这将首先由 Kyber 和共和国议定书发挥作用。 每个商家持有一个密钥，以批准铸造新的包装令牌和燃烧包装令牌。

用户-包裹令牌的持有者。 用户可以像 HECO 生态系统中的任何其他 HECO 令牌一样使用包裹令牌进行传输和交易。

KYC（了解你的客户）-FINCEN 和 OFAC 所需的准则，根据这些准则，机构必须寻求信息，以确认客户不受 OFAC 制裁，违反任何银行保密法规则，或以其他方式可能从事洗钱活动。

反洗钱（反洗钱)----监管当局(包括美国财政部）为打击可能被洗钱的非法资金来源而实施的规则和条例。

NBNB（包装 BNB）--一个 HECO 令牌在 HECO 支持 1：1 对标 BNB。

发行与分配

NBNB 总发行量 10 亿，其中 2 个亿用于 USDT 挖矿产出，5 个亿用本币挖矿，3 个亿分配给团队和用户奖励，采用销毁机制，销毁到 1 个亿后，1:1 对标 BNB。

团队介绍

NBNB 由原 WBTC 团队打造。WBTC 团队曾经构建全球最大下载引擎，其核心成员在云计算、分布式计算、区块链等领域具备深厚的技术实力。其中，李金波为迅雷原技术合伙人、CTO；李峰为迅雷原首席科学家；邹胜龙为迅雷原董事长兼 CEO，程浩为迅雷原总裁，张玉波为迅雷原高级副总裁，他们均是全球分布式计算以及去中心化共享计算的旗帜性人物。

技术团队

NBNB 团队的技术专家来自全球顶尖公司。

管理团队

NBNB 管理团队人才济济，在区块链技术开发、市值管理和团队运营方面有着深厚经验。

顾问团队

NBNB 顾问团队来自于全球区块链联盟的顶尖人士和风投机构。