

包装的代币

用于将任何资产令牌化的多机构框架

白皮书 v 0.2
2019 年 1 月 24 日

[Kyber](#)
[NetworkBitGo Inc](#)
[共和国议定书](#)

摘要

随着 ERC20 的日益普及，以太坊生态系统中的数字代币已经成为一种重要的资产类别。这些代币拥有区块链和以太坊所拥有的所有优势，在币总数、所有者、铸造、快速确认时间、交易细节和智能合同执行方面都具有透明度。区块链以太坊上的代币可以服务于几种不同的功能；本文将特别关注资产支持或包装的代币。这些代币的价格反映了支持它们的资产的价格，因此它们也可以称为“稳定币”。资产支持的令牌通常以两种不同的方式完成：

- Ethereum 上的一些代币就遵循这种机制，通过智能合约控制供需，从而使代币价格与法定货币保持一致。Dai、Basis、Carbon 和 NuBits 就是这样的例子
- 集中化—资产存储在发布储备证明的组织中。Tether、True USD、USDC (USD)、Digix(黄金)、Globcoin(法定货币的混合货币)和 AAA 储备(政府债券)就是这种情况

包装好的代币遵循集中模式，但它们不是完全依赖于一个机构，而是依赖于在网络中扮演不同角色的机构联合体。本白皮书提出了一个框架，用于通过解决可扩展性、信任、法规和治理方面的挑战来发行资产支持的令牌。我们推出的第一个包装好的代币将是由比特币(BTC)支持的 ERC20 代币，并将恰当地命名为“包装好的 BTC”(WBTC)。与集中解决方案(美元)不同，WBTC 将被完全入账，并在 BTC 链上公布储备证明。

使用 WBTC 不需要额外的二级公用事业/支付代币，也不需要除区块链费用之外的转移费用。WBTC 使用一个简单的联邦治理模型，并努力提升可用性。

使用案例

令牌化

将资产令牌化的行为可以：

- **提高交易速度**
以太坊区块每隔约 15 秒创建一次，您可以在不到 5 分钟的时间内对交易的不可撤销性抱有相当大的信心。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
- **减少中介机构数量**
区块链资产的一个关键好处是无需中介就能进行交易。这可以通过原子交换、分散的交换协议和闪电/raiden 风格的通道来实现。
- **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将密钥从交易所转移到以安全为重点的托管机构，从而降低对手方风险。
- **可用性**
ERC20 标准已被大量机构和产品采用。这为用户提供了多种交易、钱包和 Dapps，供他们在处理令牌化资产时使用。他们还能够全天候快速移动代币。
- **提高透明度**
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、令牌移除事务、令牌持有人数量以及传输规则。这种透明度通常不适用于法定货币、大宗商品和股票等资产。

分散式交易所和 dapps 的流动性

如今，在集中交易所进行的大多数 ERC20 交易都是与 BTC 完成的，而不是与 ETH 完成的。大多数分散的交易所只提供 ETH/Token 交易，不提供 BTC/Token 交易。包装好的代币可以弥补这个缺口，在分散化的交易所提供更多流动性。此外，其他分散的应用程序/协议(如基金、贷款支付)也将受益于获得 BTC 代币可以带来的更大流动性。WBTC 为比特币创造了智能合约的便利条件。

法定代币的好处

法定货币支持的代币为交易员提供了一种将资金存放在加密货币中的安全方式，他们无需担心价格波动。这对于集中和分散交易所的交易员特别有用，因为在这些交易所，没有直接的方式来转移法定货币。法定货币支持的代币也预示着一个

数字加密货币可以取代传统金融。值得注意的是，买方和卖方都可以在电子商务中使用这种技术，而不必担心兑换率或税收(买方需要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

随着加密货币数量的增长，人们开始关注货币交易的某些方面。一些这样的方面是交易吞吐量、隐私、廉价交易费用、智能合同能力以及节点/挖掘者的分散化。有了这个包装好的框架，就可以很容易地在以太坊上表示任何其他加密货币，比如比特币，从而将以太坊区块链的所有功能都用于增强以太坊。其中一个使用情形是能够直接为首次代币发售(ico)提供资金，并在打包的比特币代币存款上铸造代币。将来，中央交易所和其他接受加密货币的机构就不需要维护多个加密货币节点，只需要在以太坊上开发即可。

关于执行政策的连锁方式

令牌化还提供了一种在链上实施策略的方法。On chain 策略强制执行规则更加透明，并且不依赖于一方来强制执行。根据资产的类型，可能需要执行关于资产转让或交易的规则。例如，证券需要白名单、持有期和身份管理。

常见问题

可量测性

截至 2018 年 1 月，以太坊主网络的最大实际天然气产量上限为每区块 8,000,000 立方米[1]。此限制受硬件和软件限制。虽然提出了几种可伸缩性解决方案，但许多都需要显著的开发提升(状态通道)，或者对于实际应用而言处于开发的早期(等离子体、碎片)。这对 Dapps 和网络用户来说是个问题，因为汽油价格在争端期间飙升(热门 ico、CryptoKitties)。今年早些时候，也就是 7 月份，中国外汇市场的波动造成了空前的交易费上涨[2]。

信任

资产支持的代币通常涉及对持有资产的机构的信任。这与加密货币的精神背道而驰，加密货币旨在将人们对公司运营的信任降到最低。这里要回答的一些关键问题是：

- 现有法律框架是否授权资产持有人持有资产？
- 托管人能否创建任意数量的代币？
- 托管人如何证明拥有托管资产？

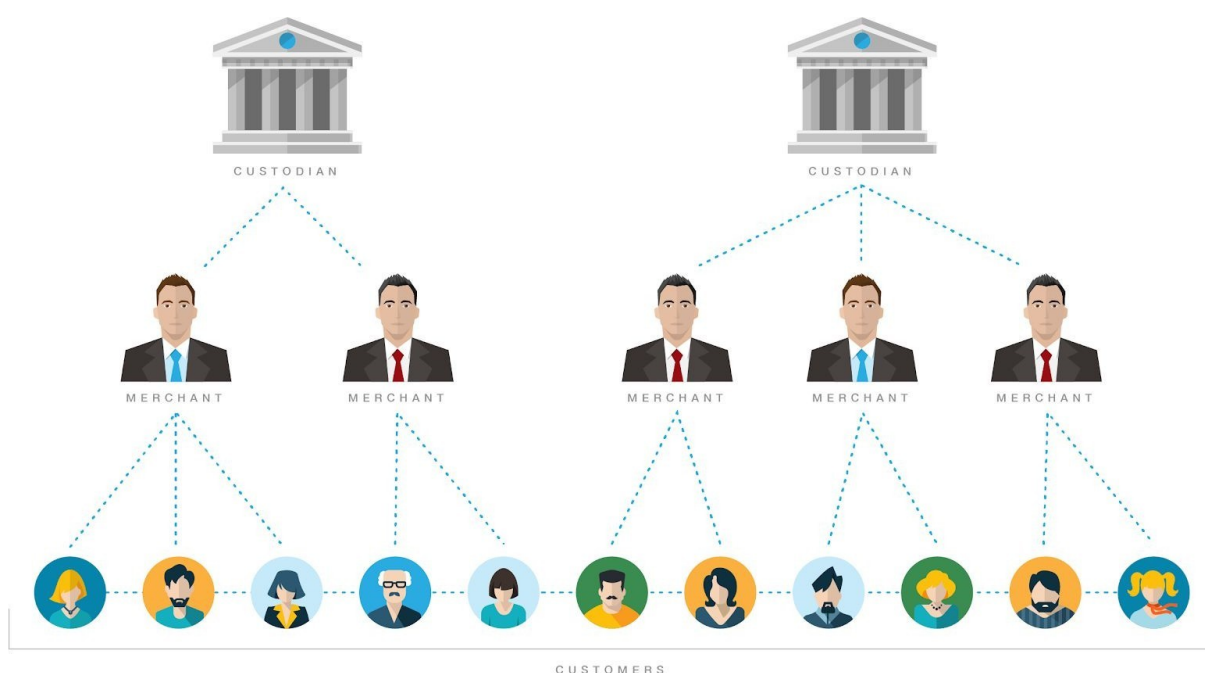
管理

资产支持令牌的保管人需要获得持有资产的许可。本许可证可能因托管人的资产和地理管辖区而异。托管人还必须定期证明自己的外汇储备，因为缺乏 1:1 的支持会损害整个体系。KYC 和 AML 限制也适用于使用资产支持代币的用户。这些限制需要在购买、赎回或转让代币时强制执行。

管理

当系统中有多个利益相关者时，在如何处理对令牌所做的更改方面存在治理挑战。大多数资产支持的代币完全依赖于资产托管人来更改管理代币的规则/智能合约。通常在 ico 的情况下，令牌的发行者可以完全控制协议更改。也有一些案例，比如分散化的自主式首次代币发售 (DAICOs)，用户拥有投票权，但他们面临的挑战是投票率低[3]。

执行和技术



关键角色

- 保管人——持有资产的机构或一方。在 WBTC 的案例中，这将由 BitGo [4] 扮演。保管人持有铸币代币的钥匙。
- 商户-包裹代币的铸造和焚烧机构或交易方。商家在所包装代币的分发中扮演关键角色。在…的情况下

WBTC，这将发挥最初由凯伯[5]和共和国议定书[6]。每个商家持有密钥以启动新包装代币的铸造和包装代币的燃烧。

- 用户-包装令牌的持有者。用户可以像以太坊生态系统中的任何其他 ERC20 令牌一样，使用包装好的令牌进行传输和交易。
- WBTC DAO 成员-合同变更以及托管人和商户的添加/移除将由多重签名合同控制。多重签署合约的金钥持有人将由机构持有，作为 WBTC DAO 的一部分。

托管人与商家交换资产以换取包装好的代币。这是通过两种不同类型的交易来实现的：铸造(创建包装代币)和燃烧(减少包装代币的供应)。这些交易将公开提供，任何人都可以通过 block explorer 查看。在初始交换之后，商家的目标是保持包装好的代币的缓冲区，以便他们可以与用户交换代币。两步铸币过程有助于减少用户获取包装好的代币所需的时间，因为铸币和燃烧是更耗时的过程。

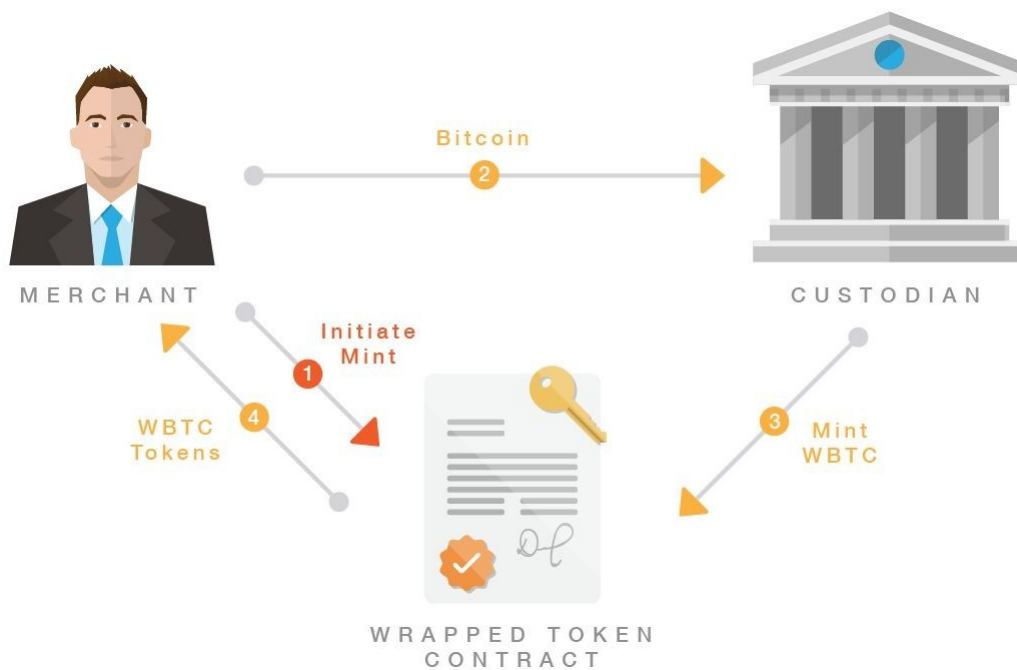
托管钱包设置

托管机构应该为所有商户提供一个共享钱包。钱包会用

由托管人控制所有密钥的多重签名。钱包将只能发送到链上的白名单商家地址。所有铸币和焚烧交易预计将在提交给托管人后 48 小时内完成。请注意，在多个保管人的情况下，单个钱包可能没有足够的资金来赎回所有挂起的包装代币。

铸造

铸币指的是创建新的包装代币的过程。在包装好的框架内进行铸币必须由托管人完成，但必须由商家“发起”。重要的是要注意，铸币不涉及用户。这是商人和托管人之间的一组交易。



WBTC 铸币事件顺序

- 商家发起交易以授权托管人将 X WBTC 铸币到以太坊链上的商家地址。
- 商家派托管人 X BTC。
- 托管人等待 6 份 BTC 交易确认书
- 托管人创建一个交易，在以太坊链上铸造 X 个新的 WBTC 代币

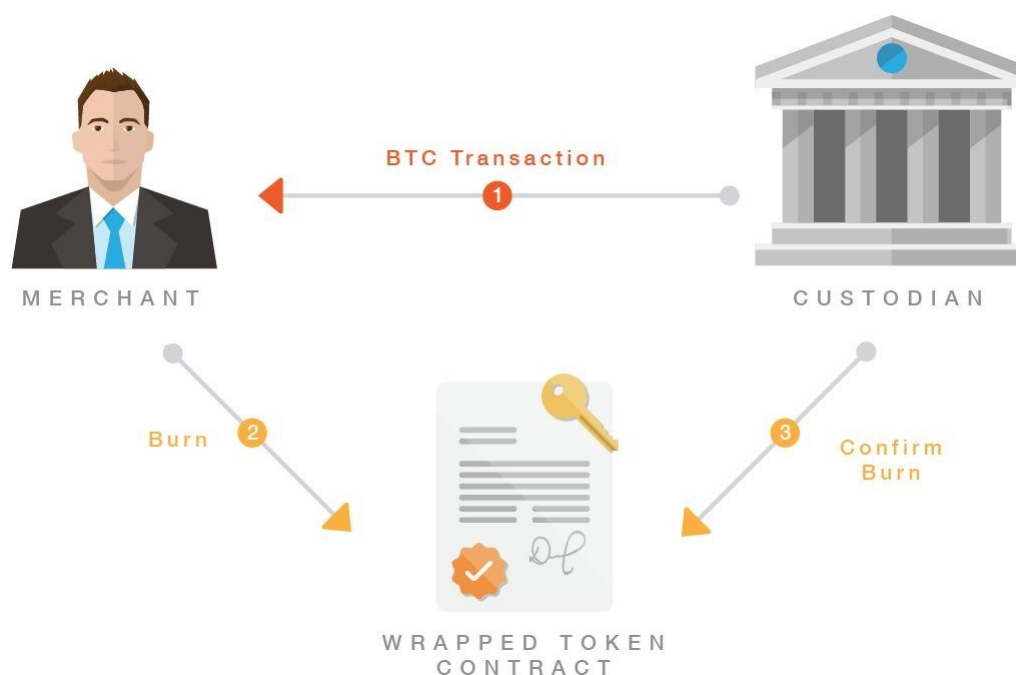


用户接收 WBTC 令牌的事件序列

- 用户向商家请求包装好的代币
- 商户执行所需的 AML、KYC 程序，并从用户处获取身份信息
- 用户和商家执行原子交换，或者使用可信交换，商家接收比特币，用户接收 WBTC

燃烧的

焚烧指的是用 BTC 换取 WBTC 代币的行为。只有商家地址才能烧掉包装好的代币。为此，会在合约中使用 Ethereum 链上要燃烧的代币数量调用“burn”函数。通过这样做，该金额从商家的 WBTC 余额中扣除(在链上)，WBTC 的供应减少。



用于燃烧 WBTC 代币的事件序列

- 商家创建一个烧钱交易，烧钱 X WBTC 代币
- 托管人等待 ETH 交易的 25 个块确认
- 托管人向商户的比特币地址释放 X BTC
- 托管人进行以太坊交易，将刻录请求标记为已完成



用户接收比特币的事件顺序

- 用户向商家请求兑换代币
- 商户执行所需的 AML、KYC 程序，并从用户处获取身份信息
- 用户和商家执行原子交换，或者使用可信交换，其中用户接收比特币而商家接收 WBTC 代币

关于链转移限制

基于令牌，可能存在对令牌传输的适当限制。对 WBTC 而言，转让将不受任何限制。

管理

包装的令牌协定由 multisig 协定管理，其中需要 DAO 成员的签名才能添加/删除成员。所有托管人和商户都将是 DAO 成员，但其他机构也可以包含为成员，而不具有托管人或商户角色。“M of N” 签名将用于合同，其中 M 是多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，同时考虑到安全性以及添加/删除成员的便利性。

包裹代币的侧链

最初，WBTC 将在以太坊主网络链上推出。mainnet 链很容易访问和使用，因为上面有一个交易所、区块探险者、钱包和其他 Dapps 的网络。令牌化的关键优势之一是交易成本低廉。但随着以太坊的普及和 Dapp 创建量的增加，包装好的代币的交易成本可能会上升到在主链上交易不便宜的地步。多个机构在包装框架中的协作使得能够部署实用的可扩展解决方案来提高事务吞吐量。

这可以通过使用挂钩侧链、使用现有软件([parity-bridge](#))在 DAO 成员之间运行。它将使用 Aura 一致性算法 [8] 在自己的权威证明网络 [7] 上运行。区块将每 4 秒创建一次，可预测，并以性能的方式。目前，已经有了这样一个链(Kovan testnet)，并从 2017 年 3 月开始运作。通过在 mainnet 和侧链上创建一个双向多 sig 钱包，包装好的代币将被挂钩在主链和侧链之间。侧链为以太坊提供了亟需的可扩展性。交易和转移包装代币的侧链的一些好处是：

- 以最小的开发成本进行扩展(相同的 EVM)
- 专用、提高的吞吐量—在单独的硬件上实现单独的区块链以及潜在的授权证明 (PoA) 优势 (更快的区块)
- 在现有客户和钱包中易于支持
- 连锁超市摆脱了其他“吵闹的邻居”
- 最小的交易成本(防止垃圾邮件)

验证方(区块生成器)将从包装好的合作伙伴和其他受信任方中进行选择，这些合作伙伴和其他受信任方将分布在不同的地区并代表多个不同的注册地/政府。验证者也将保持主链和侧链之间的双向挂钩。为了将包装好的代币的价值绑定在这两个链上，我们提出了一个在 mainnet 和 sidechain 上使用的多重签名合约。

- 要从以太坊 mainnet 发送到以太坊侧链：
 - 从 mainnet 地址发送到联邦 mainnet 多签名地址
 - 建议在多签名地址上调用“sendToSidechain”方法时发送金额，并指定侧链上的目标地址作为参数
 - 如果在没有方法的情况下发送，则假定侧链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
 - 联合签名者在 mainnet 上“锁定”令牌
 - 在“确认期”之后，侧链上的 multisig 机构可以在 mainnet 上验证 send 事件，并将金额支付给侧链上的目的地址，减去交易费用
- 从 ETH 侧链向 ETH mainnet 发送：
 - 相同(对称)

WBTC 将成为侧链上的第一个资产，并将结合使用这些组件，共同创建一个生态系统：

- 节点软件和配置
- 区块总管
- 钱包提供商

- 区块验证器
- 多重签署机构

激励

为了保护正在运行的区块验证器并防止侧链上的垃圾邮件，交易将按最低起始汽油价格 1 Gwei 收取费用。对于每一个 Dapp，验证者也可以被链外激励或者获得区块奖励。醚在侧链上的分销/管理详情仍有待确定。

原子交换

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

一旦 KYC 完成，用户原子性地将 BTC 交换为与商家的 WBTC 的步骤是：

- 用户生成秘密，并且其散列被提供给商家脱离链。用户和商家还就其他交换细节达成一致，例如接收地址 (ETH 和 BTC)
- 用户使用商家的比特币地址、用户的退款地址、秘密散列和到期时间创建比特币 HTLC (散列时间锁定合约)。这用于创建一个 P2SH 地址，用户用 X BTC 为其提供资金
- 在 6 次确认之后，商家将使用用户的以太坊地址、商家的退款地址、秘密散列和到期时间在以太坊上创建 HTLC 合同。然后，商家将 X WBTC 转移到原子互换合约。
- 为了将 X WBTC 从原子交换合约移动到用户的以太坊地址，用户揭示了秘密
- 商家使用该秘密从 P2SH 地址转移比特币资金
- 如果用户在到期时间内没有要求 WBTC，则交易不通过，用户可以要求收回 BTC

这里要注意一些重要的事情：

- 为了部署原子互换合约并把 WBTC 送到它那里，涉及交易费。因此，用户将不得不在启动交换之前支付原子交换费用。
- 原子掉期交易需要时间，在 BTC 和 ETH 两个链上需要多次交易。用户可以具有进行可信交换的选项，其中 BTC 被转移到商家地址，并且在比特币网络上的 6 次确认之后，商家将 WBTC 发送给用户。这涉及到对商家的信任，但它更快、更便宜。

WBTC 与原子互换

对于只希望执行的用户，可以在没有 WBTC 的情况下执行原子交换 BTC-ETH 贸易。它们可以通过科莫多平台[9]提出的机制在一个分散的交易所内完成。然而，值得注意的是，WBTC 在 ETH 链上提供了 BTC 的代表，这是 DAPPs 和生态系统相互作用所需要的。比较原子交换和 WBTC 时，还需要考虑其他一些权衡：

- 他们要求进行原子互换的人都要发现价格。在包装好的代币中，价格发现只需要在获得 WBTC 后在分散的交易所进行交易时进行。
- 要求原子交换技术得到现有钱包和分散化交易所的支持。包装 BTC 将可用于任何 ERC20 支持的钱包。
- 他们真的很慢，因为每一笔交易都慢得像 ETH 链上的多次确认，然后是比特币链（与 WBTC 相反，那里的初始铸造/令牌化很慢，但创建后可以在 ETH 链上轻松交易）
- 在分散的交易所进行原子互换需要单独的存款和原子互换费用。这在每次用户想要交换货币时都是不方便的。

费用

除了网络费用外，用户之间的 WBTC 转账没有任何费用。网络中的不同方可以通过以下三种方式赚取费用：

- 托管费：由托管人在商户铸币或焚烧包裹的代币时收取。
- 商户费用：这是由用户用其交换包裹代币的商户收取的资产费用。
- 侧链交易费：此费用主要用于防止侧链上的垃圾邮件。这在侧链上运行节点的所有机构之间平等地共享。

法律约束力

托管人与商户之间的合约

铸造和燃烧代币的过程不涉及用户，而是在可信机构之间进行。商家需要安全地持有用户的身份信息。托管人须按季度公布托管资产的详细资料，并及时履行铸币/烧钱职责。未能满足这些标准可能会导致从网络中删除。

应当指出，网络中可能有多个托管人，但这是以增加网络所涉及的风险为代价的。持有多重签名钱包密钥的不同机构共享托管权的模式在未来也是可能的。虽然在操作上，铸造/燃烧/审计将需要更多的协调和时间。任何一位托管人的安全漏洞都将导致信任的丧失，并可能导致大规模提款。与商家发生安全漏洞的严重性要低得多，因为所有未完成的代币仍将由托管人备份，但会导致丢失 KYC/AML 用户数据。

信任模型

从某种意义上说，托管人在包装好的框架内是可信的，因为资产可能会被盗，或者他们可能不会兑现一对一的担保。不过，包装好的框架旨在以几种方式最小化这种信任：

- 外部第三方将进行季度审计，以验证所有铸造的包装代币在所有托管人之间存储的资产量是否相等。就 WBTC 而言，可以通过公布比特币存储地址的签名来证明其储量。
- 托管人将不能自己铸造代币，而是要求启动一个商人这样做。因此，新代币的创建涉及托管人和商家两者。
- 用户通过一组商家机构与托管人交互隔离。单个商家不需要被信任，而是所有商家一起需要被信任。
- 对参与该框架的所有机构而言，所涉机构的现有信誉都处于危险之中。













透明度

包装的令牌的功能将完全透明。网络的所有关键细节都将反映在仪表板中，其中包括：

- 在网络中扮演不同角色的机构名称和详细信息
- mint 和 burn 订单的状态(待定、正在处理、已取消、已完成)
- 托管人存储的 BTC 总额
- WBTC 在网络中的总金额(将与 BTC 存储的金额相同或略低)
- 以交易形式进行季度审计，证明托管人拥有比特币的密钥
- 商户及托管人以太坊地址
- 与每个商家相关联的比特币地址，由托管人控制
- 指向块资源管理器上的开源令牌协定代码/已部署协定的链接

仪表板可能是什么样子的示例：

ORDER BOOK

NETWORK		CUSTODY	
 34,234 WBTC		 34,263 BTC (\$4,434,411 USD)	
ACTION	DATE	MERCHANT	VALUE (WBTC)
	1/3/19 — 6:45:39	Kyber	312.95
	1/1/19 — 14:14:35	Kyber	92.00
	1/1/19 — 8:12:24	Republic Protocol	399.29
	12/31/18 — 23:01:47	Kyber	2,100.37
	12/30/18 — 12:15:51	Republic Protocol	50.50
	12/29/18 — 3:24:20	Republic Protocol	100.60
	12/29/18 — 1:59:01	Kyber	42.16
	12/27/18 — 17:04:54	Kyber	10.00
	12/25/18 — 14:45:31	Kyber	3.00
	12/21/18 — 2:01:45	Republic Protocol	14.20

<< < Page 1 of 504 > >>

结论

通过包装令牌，我们提出了一个解决方案，使资产在以太坊链上可互换和可表示。全球流动性、更高的部分所有权、智能合同可编程性和交易费用的减少是代币化的一些关键优势。WBTC 将成为第一个这样的代币，使 Dapps 能够方便地获得比特币。所有交易、合同和审计都将是公开可见的，以保持透明度并实现对网络的信任。该框架还提供了一种方式，在这种方式下，加密货币领域的多个机构可以扮演不同的角色，从而克服资产支持代币面临的常见问题。

词汇表

保管人——持有资产的机构或一方。就 WBTC 而言，这将由 BitGo 来扮演。保管人持有铸币代币的钥匙。

商户-包裹代币的铸造和焚烧机构或交易方。商家在所包装代币的分发中扮演关键角色。就 WBTC 而言，这将首先由 Kyber 和 Republic Protocol 扮演。每个商家持有用于批准铸造新的包装代币和燃烧包装代币的密钥。

用户-包装令牌的持有者。用户可以像以太坊生态系统中的任何其他 ERC20 令牌一样，使用包装好的令牌进行传输和交易。

KYC(了解你的客户)-金融犯罪执法网和 OFAC 所需准则，根据这些准则，各机构必须寻求信息，以确认客户不受 OFAC 制裁，没有违反《银行保密法》的任何规则，或有可能从事洗钱活动。

AML(反洗钱)-监管机构(包括美国财政部)执行的规则和法规，旨在针对和打击可能被洗钱的非法资金来源。

WBTC(包装好的比特币)——以太坊上的一枚 ERC20 代币，以 1:1 的比例由比特币支持。

参考

- [1] -<https://etherscan.io/chart/gaslimit>
- [2] -<https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/>
- [3] -<https://cointelegraph.com/explained/what-is-a-daico-explained>
- [4] -<https://www.bitgo.com>
- [5] - <https://kyber.network>
- [6] -<https://republicprotocol.com>
- [7] -<https://paritytech.github.io/wiki/Proof-of-Authority-Chains>
- [8] -<https://wiki.parity.io/Aura>
- [9] -<https://komodoplatform.com/atomic-swaps/>

