Wrapped Tokens

包装的代币

A multi-institutional framework for tokenizing any asset

用于将任何资产令牌化的多机构框架

Whitepaper
v0.2 Jan 24th
2019
白皮书 v 0.2
2019 年 1 月 24 日

[Kyber Network](#)
[BitGo Inc](#)
[Republic Protocol](#)

[Kyber
NetworkBitGo
IncRepublic
Protocol](#)

Abstract
摘要

With the rise in popularity of ERC20, digital tokens in the Ethereum ecosystem have emerged as an important asset class. These tokens have all the advantages that blockchains and Ethereum have to offer in terms of transparency in total number of coins, owners, minting, fast confirmation times, transactions details and smart contract execution. Tokens on the Ethereum blockchain can serve several different functions; this paper will specifically focus on asset backed or wrapped tokens. The prices of these tokens reflect the price of the asset backing them and hence they can also be called "stable coins". Asset backed tokens are usually done in two different ways:

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：

- **Algorithmic** - This is a mechanism followed by some tokens on Ethereum where demand and supply are controlled by smart contracts in order to keep the price of the token in line with a fiat currency. Some examples of this are Dai, Basis, Carbon, and NuBits
- 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

- **Centralized** - Assets are stored with an organization which publishes proof of reserves. This is the case with Tether, True USD, USDC (USD), Digix (gold), Globcoin (a mix of fiat currencies), and AAA reserve (governmental bonds)
- 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

Wrapped tokens follow the centralized model, but instead of relying entirely on one institution, they rely on a consortium of institutions performing different roles in the network. This whitepaper proposes a framework for issuing asset backed tokens by addressing challenges with scalability, trust, regulation, and governance. The first wrapped token we launch will be an ERC20 token backed by Bitcoin (BTC) and will be appropriately named, "Wrapped BTC" (WBTC). Unlike centralized solutions (USD), WBTC

will be fully accounted for and proof of reserves posted on the BTC chain.

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。

There is no additional secondary utility/payment token required to use WBTC, and no transfer fees other than blockchain fees. WBTC uses a simple federated governance model and strives to promote usability.

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。

Use Cases
使用案例

Tokenization
令牌化

The act of tokenizing assets can:

将资产令牌化的行为可以：
- Increase speed of transactions
- 提高交易速度

  Ethereum blocks are created every ~15 seconds and it is possible to have a fair deal of confidence in the irrevocability of a transaction in less than 5 minutes. This speed is faster than transacting natively compared to many other assets including Bitcoin, gold, and fiat currencies

  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
- Reduce the number of intermediaries
- 减少中介机构数量

  One of the key benefits of assets on a blockchain is their ability to be transacted without intermediaries. This can be done through atomic swaps, decentralized exchange protocols, and lightning/raiden style channels.

  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。
- Enhance security
- 加强安全

  Tokenization enables users to have full control of private keys of the asset. Users who do not want to hold keys can reduce counterparty risk by moving it from exchanges to a security-focused custodian.

  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。
- Usability
- 可用性

  The ERC20 standard has been adopted by a large number of institutions and products. This provides users with a variety of exchanges, wallets, and Dapps to use while handling their tokenized asset. They also have the ability to move tokens quickly, 24/7.

  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。
- Improve Transparency
- 提高透明度

  The total number of tokens, token creation transactions, token removal transactions, number of token holders, and rules for transfers can be seen on a public block explorer by anyone. This level of transparency is not usually available for assets like fiat currencies, commodities, and stock.

  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。

Liquidity on decentralized exchanges and dapps
分散式交易所和 dapps 的流动性

The majority of ERC20 trading in centralized exchanges today is done with BTC and not ETH. Most decentralized exchanges offer only ETH/Token and not BTC/Token trades. Wrapped tokens can bridge this gap and provide more liquidity on decentralized exchanges. In addition, other decentralized applications/protocols (like funds, lending payments) will also benefit from having access to greater liquidity that a BTC token can bring. WBTC brings the ease of creation of smart contracts to Bitcoin.

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。

Benefits of fiat tokens
法定代币的好处

Tokens backed by fiat currencies offer a safe way for traders to keep their money in a cryptocurrency without having to worry about price fluctuations. This is particularly useful for traders on both centralized and decentralized exchanges where there is no direct way of transferring fiat currencies. Fiat currency backed tokens also promise a world in which a

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

cryptocurrency can replace traditional finance. Notably, it can be used in e-commerce by both buyer and seller without having to worry about conversion rates or taxes (buyers are required to pay capital gains tax calculated at the time of purchase in the US).

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)。

Interoperability between cryptocurrencies
加密货币之间的互操作性

As we see an expansion in the number of cryptocurrencies today, each one focuses on some aspect of monetary exchange. Some such aspects are transactional throughput, privacy, cheap transaction fees, smart contract ability, and decentralization of nodes/miners. The wrapped framework would make it easy to represent any other cryptocurrency, such as Bitcoin, on Ethereum and thereby enhance it with all the capabilities of the Ethereum blockchain. One such use case is the ability for initial coin offerings (ICOs) to be directly funded and mint tokens on deposits of wrapped Bitcoin tokens. In the future, centralized exchanges and other institutions which accept cryptocurrencies would not need to maintain multiple cryptocurrency nodes and instead could just develop on Ethereum.

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。

On chain ways to enforce policies
关于执行政策的连锁方式

Tokenization also provides a way to enforce policies on chain. On chain policy enforcement makes rules more transparent and doesn't rely on one single party to enforce them. Based on the type of asset, there could be a need to enforce rules on asset transfer or trade. Securities for example require whitelisting, holding periods, and identity management.

令牌化还提供了一种在链上实施策略的方法。On chain 策略强制执行使规则更加透明，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。

Common Issues
常见问题

Scalability
可量测性

As of January 2018, the maximum practical gas limit on Ethereum's mainnet topped out at 8,000,000 gas per block [1]. This limit is both hardware and software-bound. While there are several scalability solutions proposed, many require significant developer lift (state channels), or are too early in development for practical use (plasma, sharding).

This is a problem for Dapps and users of the network because gas prices skyrocket during periods of contention (hot ICOs, CryptoKitties). Earlier this year in July, transactions caused by Chinese exchange Fcoin caused all time high transaction fees [2].

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者提升(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]。

Trust
信任

Asset backed tokens usually involve trust in the institution(s) holding the asset. This goes against the ethos of cryptocurrencies which seeks to minimize need for trust in operations. Some key questions to answer here are:

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：

- Is the asset holder authorized in the existing legal framework to hold the asset?
- 现有法律框架是否授权资产持有人持有资产？
- Can the custodian create an arbitrary amount of tokens?
- 托管人能否创建任意数量的代币？
- How does the custodian prove possession of the asset under custody?
- 托管人如何证明拥有托管资产？

Regulation
管理

Custodians of asset backed tokens need to be licensed to hold the asset. This license may vary based on the asset and geographical jurisdiction of the custodian. Custodians must also prove reserves regularly given that a lack of 1:1 backing would undermine the whole system. KYC and AML restrictions also apply to users engaging in asset backed tokens. These restrictions need to be enforced at the time of purchase, redemption, or transfer of tokens.

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。

Governance
管理

When there are multiple stakeholders in the system, there is a governance challenge with how to handle changes made to the token. Most asset backed tokens are entirely reliant on the asset custodian to make changes to the rules/smart contract governing the token. Usually in the case of ICOs, the issuer of the token has full control of protocol changes. There have been some cases like decentralized autonomous initial coin offerings (DAICOs) where users have voting rights, but they face the challenge of a low voter turnout [3].

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]。

Implementation and Technology
执行和技术
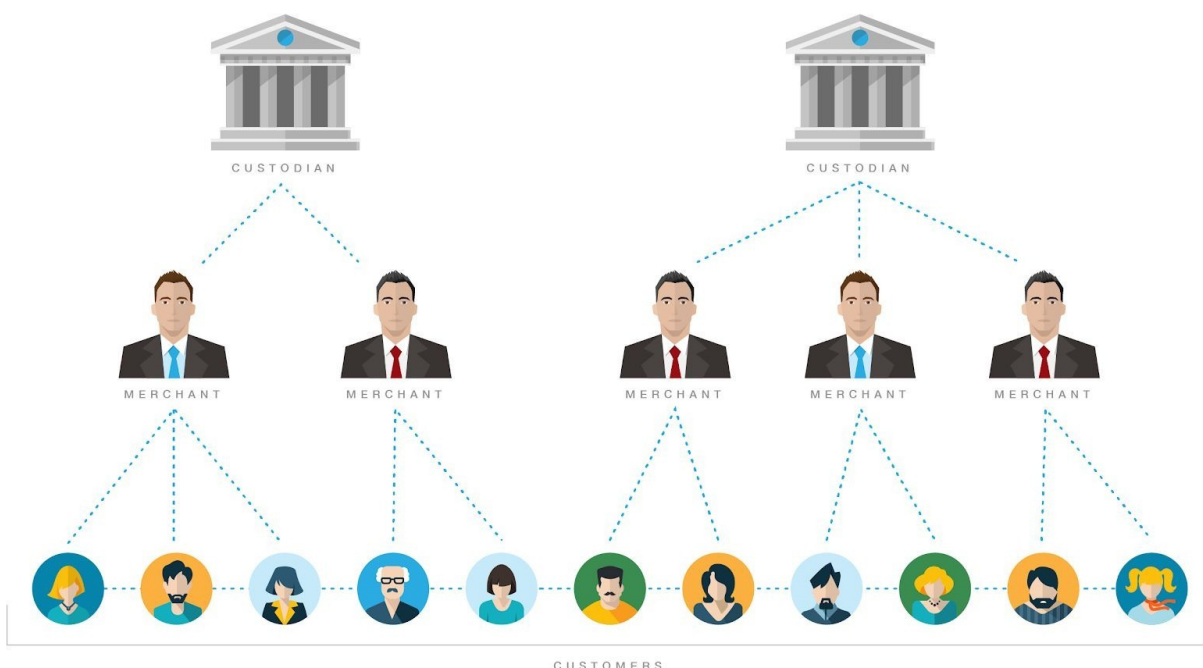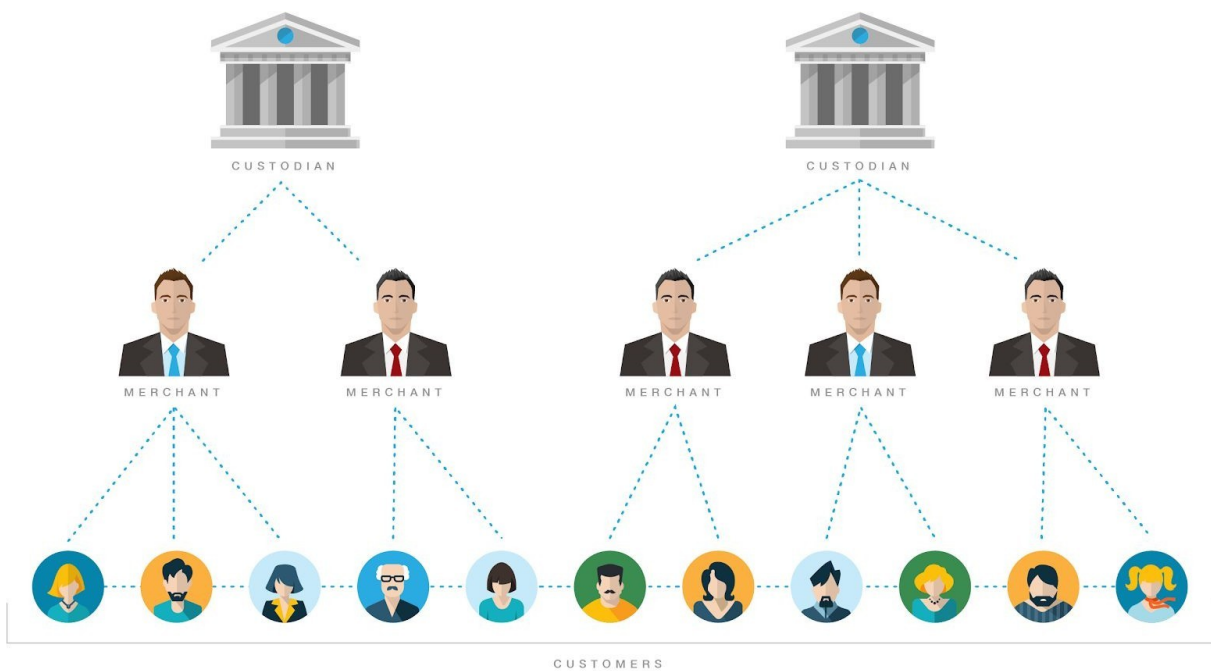
Key Roles
关键角色

- Custodian - The institution or party who holds the asset. In the case of WBTC, this will be played by BitGo [4]. Custodians hold the keys to mint tokens.
- 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。
- Merchant - The institution or party to which wrapped tokens will be minted to and burnt from. Merchants play a key role in distribution of the wrapped token. In the case of
- 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, this will be played initially by Kyber [5] and Republic Protocol [6]. Each merchant holds a key to initiate minting of new wrapped tokens and burning of wrapped tokens.

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。

- User - The holders of the wrapped token. Users can use wrapped tokens to transfer and transact like any other ERC20 token in the Ethereum ecosystem.
- 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 member - Contract changes and addition/removal of custodians and merchants will be controlled by a multi-signature contract. Holders of the keys to the multi-sig contract will be held by institutions as part of the WBTC DAO.
- 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。

Custodians exchange assets for wrapped tokens with merchants. This is done through two different types of transactions; minting (creation of wrapped tokens) and burning (reducing supply of wrapped tokens). These transactions will be available publicly and can be viewed by anyone through a block explorer. After the initial exchange, merchants aim to maintain a buffer of wrapped tokens so that they can exchange it with users. The two-step minting process helps reduce the time it takes for users to get wrapped tokens, as minting and burning are more time consuming processes.

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。

Custodian wallet setup
托管钱包设置

Custodians are expected to have a pooled wallet for all merchants. The wallet will use

托管机构应该为所有商户提供一个共享钱包。钱包会用

multi-signature with all keys controlled by the custodian. The wallet will only be able to send to the whitelisted merchant address on chain. All minting and burning transactions are expected to be done within 48 hours of submission to the custodian. Note that in case of multiple custodians, a single wallet might not have enough funds to redeem all pending wrapped tokens.

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。
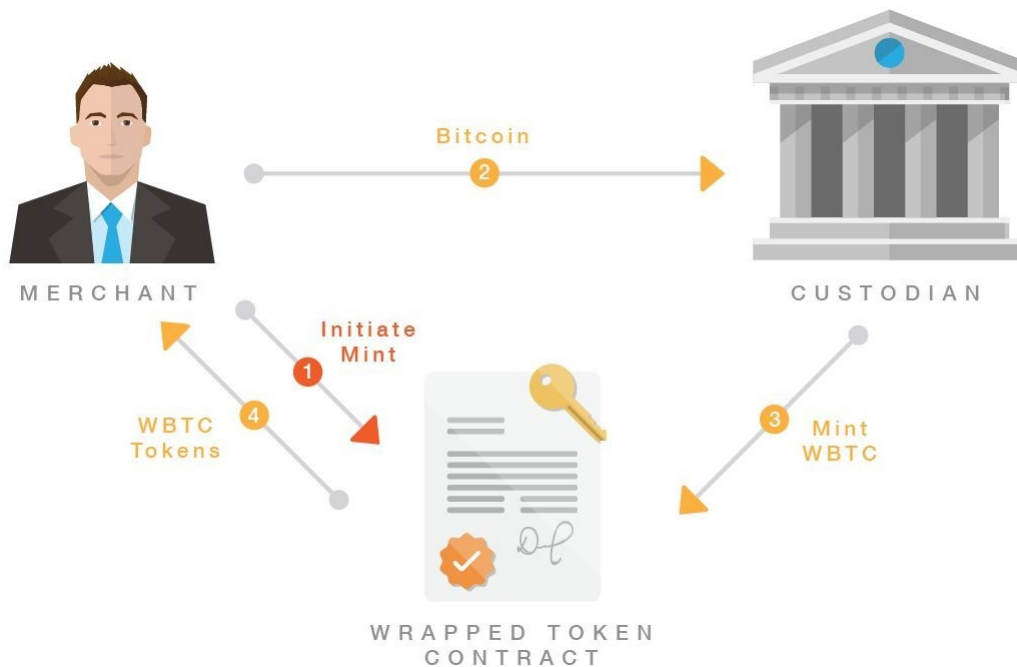
Minting
铸造

Minting refers to the process of creating new wrapped tokens. Minting in the wrapped framework has to be done by a custodian, but needs to be "initiated" by a merchant.

It is important to note that minting does not involve the user. It is a set of transactions done between the merchant and the custodian.

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。

Sequence of minting events for WBTC

WBTC 铸币事件顺序

- Merchant initiates a transaction to authorize the custodian to mint X WBTC to the merchant's address on the Ethereum chain.

- 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。
- The merchant sends the custodian X BTC.
- 商家派托管人 X BTC。
- Custodian waits for 6 confirmations of the BTC transaction
- 托管人等待 6 份 BTC 交易确认书
- Custodian creates a transaction to mint X new WBTC tokens on the Ethereum chain
- 托管人创建一个交易，在以太坊链上铸造 X 个新的 WBTC 代币

KYC, AML & Bitcoin

1

WBTC Tokens

2

CUSTOMER

MERCHANT

Sequence of events for users to receive WBTC tokens

用户接收 WBTC 令牌的事件序列

- User requests wrapped tokens from a merchant
- 用户向商家请求包装好的代币
- The merchant does the required AML, KYC procedures and gets identification information from the user
- 商户执行所需的 AML、KYC 程序，并从用户处获取身份信息
- The user and merchant perform an [atomic swap](#), or use a trusted exchange with the merchant receiving Bitcoin and the user receiving WBTC
- 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

Burning

燃烧的

Burning refers to the action of redeeming BTC for WBTC tokens. Only merchant addresses can burn wrapped tokens. In order to do so, the 'burn' function is called in the contract with the amount of tokens to be burnt on the Ethereum chain. By doing so, the amount is deducted from the merchant's WBTC balance (on chain) and the supply of WBTC is reduced.

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。

MERCHANT   BTC Transaction ①   CUSTODIAN

Burn ②

Confirm Burn ③

WRAPPED TOKEN CONTRACT

`

`
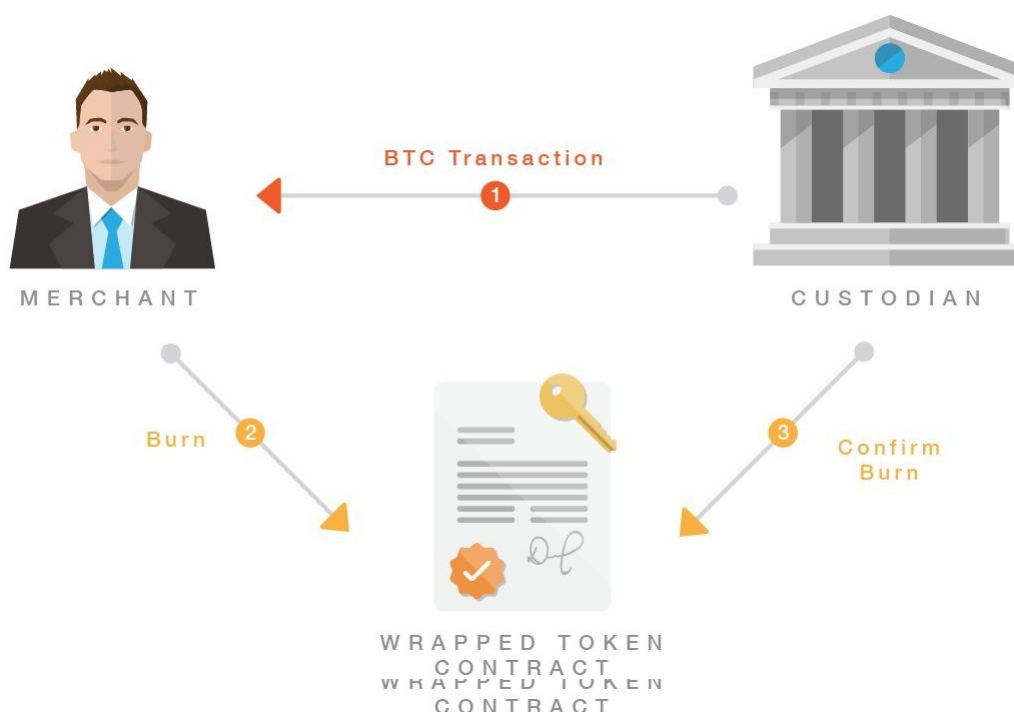
Sequence of events for burning WBTC tokens
用于燃烧 WBTC 代币的事件序列

- The merchant creates a burn transaction, burning X WBTC tokens
- 商家创建一个烧钱交易，烧钱 X WBTC 代币
- Custodian waits for 25 block confirmations of the ETH transaction
- 托管人等待 ETH 交易的 25 个块确认
- Custodian releases X BTC to the merchants Bitcoin address
- 托管人向商户的比特币地址释放 X BTC
- Custodian makes an ethereum transaction marking the burn request as completed
- 托管人进行以太坊交易，将刻录请求标记为已完成

Sequence of events for users to receive Bitcoins
用户接收比特币的事件顺序

- User requests the redemption of tokens from a merchant

- 用户向商家请求兑换代币

- The merchant does the required AML, KYC procedures and gets identification information from user

- 商户执行所需的 AML、KYC 程序，并从用户处获取身份信息
- The user and merchant perform an <u>atomic swap</u>, or use a trusted exchange where the user receives Bitcoin and the merchant receives WBTC tokens

- 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

On Chain transfer restrictions
关于链转移限制

Based on the token, there could be restrictions in place for the transfer of tokens. For WBTC, there will be no restrictions on transfers.

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。

Governance
管理

The wrapped token contract is governed by a multisig contract in which signatures are required from DAO members in order to add/remove members. All custodians and merchants will be DAO members, but other institutions can also be included as a member without having a custodian or merchant role. An "M of N" signature signature will be used in the contract where M is the required number of signatures in the multisig contract and N is the total number of members. The values of M and N will be decided mutually between members keeping in mind security as well as the ease of adding/removing members.

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。

Side chain for wrapped tokens
包裹代币的侧链

Initially, WBTC will be launched on the Ethereum mainnet chain. The mainnet chain is easily accessible and usable as there are a network of exchanges, block explorers, wallets, and other Dapps on it. One of the key benefits of tokenization, is cheap transactional cost. But with gaining popularity of Ethereum and increased Dapp creation, transaction costs of wrapped tokens could rise to the point where it is not cheap to do so on the main chain. The collaboration of multiple institutions in the wrapped framework enables the ability to deploy a practical scalable solution to increase transactional throughput.

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。

This can be done through the use of a pegged sidechain, using existing software ([parity-bridge](#)) run among DAO members. The chain will run on it's own proof of authority network [7] using the Aura consensus algorithm [8]. Blocks will be created every 4 seconds predictably and in a performant manner. Currently, there is already such a chain (Kovan testnet) and it has been in operation since March 2017. Wrapped tokens will be pegged between the main and side chain by creating a 2-way multi-sig wallet on mainnet and on the sidechain. Side chains provide much needed scalability on ethereum. Some benefits of a side chain for trading and transferring wrapped tokens are:

这可以通过使用挂钩侧链、使用现有软件([parity-bridge](#)

- Scaling with minimal development costs (same EVM)
- 以最小的开发成本进行扩展(相同的 EVM)
- Dedicated, increased throughput - seperate blockchain on separate hardware and potential proof of authority (PoA) advantages (faster blocks)
- 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)
- Easy to support in existing clients and wallets
- 在现有客户和钱包中易于支持
- Chain is free from other "noisy neighbors"
- 连锁超市摆脱了其他"吵闹的邻居"
- Minimal transactional cost (to prevent spam)
- 最小的交易成本(防止垃圾邮件)

Validators (block generators) will be chosen from wrapped partners and other trusted parties who will be geographically distributed and represent several different domiciles / governments. Validators will also maintain the 2-way peg between the main and side chain. To peg the value of wrapped tokens on both chains, we propose a multi-signature contract to be used on the mainnet and the sidechain.

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。

- To send from Ethereum mainnet to Ethereum sidechain:
- 要从以太坊 mainnet 发送到以太坊侧链:
  - Send from mainnet address to the federated mainnet multi-sig address
  - 从 mainnet 地址发送到联邦 mainnet 多签名地址
    - It is recommended to send the amount while calling the "sendToSidechain" method on the multi-sig address, specifying as the argument the destination address on the sidechain
    - 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
    - If sent without a method, the destination address on the sidechain will be assumed to be the same as the source address
    - 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
  - An event is generated on the mainnet to record the send
  - 在 mainnet 上生成一个事件来记录发送

- ○ Federated signers "lock" tokens on mainnet
- ○ 联合签名者在 mainnet 上"锁定"令牌
- ○ After a "confirmation period", multisig authorities on the sidechain can validate the send event on the mainnet and disburse the amount to the destination address on the sidechain, less transaction fees
- ○ 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
- To send from ETH sidechain to ETH mainnet:
- 从 ETH 侧链向 ETH mainnet 发送：
  - ○ Identical (symmetric)
  - ○ 相同(对称)

WBTC will be the first asset on the sidechain and will use a combination of these components working together to create an ecosystem:
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：

- Node Software and Configuration
- 节点软件和配置
- Block Explorer
- 区块总管
- Wallet Providers
- 钱包提供商

- Block Validators
- 区块验证器
- Multi-sig Authorities
- 多重签署机构

Incentivization
激励

Transactions will be charged at the minimal starting gas price of 1 Gwei to cover running block validators and to prevent spam on the sidechain. Validators can also be incentivized off chain for each Dapp or have block rewards. Details of distribution/management of Ether on the sidechain are still to be determined.

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。

Atomic Swap
原子交换

Atomic swaps can be used between merchants and users in order to exchange WBTC and BTC. If the user would like to receive WBTC or BTC more quickly, a trusted method of exchange could also be done through the merchants.

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。

Once KYC is completed, the steps for users to atomically swap BTC for WBTC with the merchant are:
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：
- User generates a secret and a hash of it is provided to the merchant off chain. The user and the merchant also agree on other swapping details such as receive addresses (ETH and BTC)
- 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)
- The user creates a Bitcoin HTLC (Hashed Time Lock Contract) using the merchant's Bitcoin address, user's refund address, secret hash, and expiration time. This is used to create a P2SH address which the user funds with X 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
- After 6 confirmations, the merchant will create an HTLC contract on Ethereum, by using the user's Ethereum address, merchant's refund address, secret hash, and expiration time. The merchant then transfers X WBTC to the atomic swap contract.
- 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。
- The user reveals the secret in order to move X WBTC from the atomic swap contract to the user's Ethereum address

- 为了将 X WBTC 从原子交换合约移动到用户的以太坊地址，用户揭示了这个秘密
- The merchant uses the secret in order to move Bitcoin funds from the P2SH address
- 商家使用该秘密从 P2SH 地址转移比特币资金
- If the user does not claim the WBTC within the expiration time, the transaction does not go through and the user can claim the BTC back
- 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

Some important things to note here:
这里要注意一些重要的事情：

- In order to deploy the atomic swap contract and send WBTC to it, there are transaction fees involved. Hence, the user will have to pay an atomic swap fee before initiating a swap.
- 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。
- Atomic swaps take time and multiple transactions on both the BTC and ETH chain. The user may have the option of doing a trusted swap in which BTC is transferred to the merchant address and after 6 confirmations on the bitcoin network, the merchant sends WBTC to the user. This involves trust in the merchant, but it is quicker and cheaper.
- 原子互换需要时间，BTC 和 ETH 两个链上的多个交易。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 vs Atomic Swaps
WBTC 与原子互换

Atomic swaps can be performed without WBTC for users which only want to perform a

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 trade. They can be done on a decentralized exchange outlined through a mechanism by the Komodo platform [9]. However, it is important to note that WBTC provides a representation of BTC on the ETH chain, which is required for DAPPs and the ecosystem to interact with. A few other tradeoffs to consider while comparing atomic swaps with WBTC:

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：

- They require price discovery to be done by whoever does the atomic swap. In wrapped tokens price discovery only needs to be done while trading on a decentralized exchange after having already obtained WBTC.
- 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。
- Requires atomic swap technology to be supported by existing wallets and decentralized exchanges. Wrapped BTC will be available for use in any ERC20 supported wallet.
- 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。
- They are really slow because every transactions is as slow as multiple confirmations on the ETH chain and then the Bitcoin chain (as opposed to WBTC, where the initial minting/tokenization is slow but after creation it's easily tradable on the ETH chain)
- 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)
- Doing an atomic swap on a decentralized exchange requires a separate deposit and a atomic swap fee as well. This is inconvenient each time users want to swap currencies.
- 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。

Fees
费用

Transfers of WBTC between users will have no cost apart from network fees. There are three ways in which different parties in the network can earn fees:

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：

- Custodian fees: This is taken by the custodian at the time when a merchant mints or burns wrapped tokens.
- 托管费：由托管人在商户铸币或焚烧包裹的代币时收取。
- Merchant fees: This is taken by the merchant who the user exchanges wrapped tokens with for the asset.
- 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。
- Sidechain transaction fees: This fee is predominantly aimed at preventing spam on the sidechain. This is shared equally among all institutions running nodes on the sidechain.
- 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。

Legal Binding
法律约束力

Contract between custodians and merchants
托管人与商户之间的合约

The process of minting and burning tokens does not involve the user and is between trusted institutions. Merchants are required to hold the identity information of the user securely.

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。
Custodians are required to publish details of assets under custody quarterly and perform minting/burning duties in a timely manner. Failure to meet these criteria can lead to removal from the network.
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。

It is to be noted that there can be multiple custodians in the network, but this comes at the cost of increasing the risk involved in the network. A model where custodianship is shared by different institutions holding keys to a multi-sig wallet is also possible in the future. Though operationally, minting/burning/auditing would require more coordination and time. A security breach among any of the custodians would cause the loss of trust and could lead to mass withdrawals. A security breach with a merchant is much less severe as all outstanding tokens will still be backed up by custodians, but instead could lead to a loss of KYC/AML user data.

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，但可能会导致丢失 KYC/AML 用户数据。

Trust model
信任模型

In some sense custodians are trusted in the wrapped framework, as assets could be stolen or they might not honour the one-to-one backing. However, the wrapped framework aims to minimize this trust in a few ways:

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：

- Quarterly audits will be conducted by external third parties to verify that all wrapped tokens minted have an equal amount of asset stored among all custodians. In the case of WBTC, proof of reserves can be shown by publishing signatures from the addresses which bitcoin is stored in.
- 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。
- Custodians will not be able to mint tokens on their own, but would instead require the initiation of a merchant in order to do so. Hence creation of new tokens involves both the custodian and the merchant.
- 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。
- The user is insulated from interacting with the custodian through a set of merchant institutions. An individual merchant does not need to be trusted, but instead all merchants together would need to be.
- 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。
- Existing credibility of the institutions involved is at stake for all the institutions involved with the framework.
- 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。

Transparency

透明度

There will be full transparency in the functioning of the wrapped token. All key details of the network will be reflected in a dashboard, some of which are:

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：

- Names and details of institutions performing different roles in the network
- 在网络中扮演不同角色的机构名称和详细信息
- Status of mint and burn orders (pending, processing, cancelled, complete)
- mint 和 burn 订单的状态(待定、正在处理、已取消、已完成)
- Total amount of BTC stored by custodians
- 托管人存储的 BTC 总额
- Total amount of WBTC in the network (Will be the same or slightly lower than BTC stored)
- WBTC 在网络中的总金额(将与 BTC 存储的金额相同或略低)
- Quarterly audits in the form of transactions which prove that the custodian has the keys to the Bitcoin
- 以交易形式进行季度审计，证明托管人拥有比特币的密钥
- Merchant and Custodians ethereum addresses
- 商户及托管人以太坊地址
- The Bitcoin address associated with each merchant, controlled by the custodian
- 与每个商家相关联的比特币地址，由托管人控制
- Links to the open source token contract code / deployed contract on a block explorer
- 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

An example of what the dashboard might look like:

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

Page 1 of 504

Conclusion

结论

Through wrapped tokens, we propose a solution to make assets interchangeable and representable on the Ethereum chain. Global liquidity, increased fractional ownership, smart contract programmability and reduction in transaction fees are some of the key benefits of tokenization. WBTC will be the first such token, enabling Dapps easy access to Bitcoin. All transactions, contracts and audits will be publicly viewable to maintain transparency and enable

trust in the network. The framework also provides a way in which multiple institutions in the cryptocurrency space can perform different roles to get past common issues faced by asset backed tokens.

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。

Glossary

词汇表

<u>Custodian</u> - The institution or party who holds the asset. In the case of WBTC, this will be played by BitGo. Custodians hold the keys to mint tokens.

<u>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。</u>

<u>Merchant</u> - The institution or party to which wrapped tokens will be minted to and burnt from. Merchants play a key role in distribution of the wrapped token. In the case of WBTC, this will be played initially by Kyber and Republic Protocol. Each merchant holds a key to approve minting of new wrapped tokens and burn wrapped tokens.
<u>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。</u>

<u>User</u> - The holders of the wrapped token. Users can use wrapped tokens to transfer and transact like any other ERC20 token in the ethereum ecosystem.
<u>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。</u>

<u>KYC (Know your customer)</u> - FINCEN and OFAC Required Guidelines pursuant to which institutions must seek information in order to confirm that customers are not subject to OFAC sanctions, violate any Bank Secrecy Act rules or are otherwise potentially engaged in money laundering activities.
<u>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。</u>

<u>AML (Anti money laundering)</u> - Rules and regulations enforced by regulatory authorities (including the Department of Treasury in the US) to target and combat illicit source of funds which may be laundered.
<u>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。</u>

<u>WBTC (Wrapped Bitcoin)</u> - An ERC20 token on ethereum backed 1:1 by Bitcoin.
<u>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。</u>

References

参考

[1] - https://etherscan.io/chart/gaslimit

[2] -https://etherscan.io/chart/gaslimit

[3] - https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/

[4] -https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/

[5] - https://cointelegraph.com/explained/what-is-a-daico-explained

[6] -https://cointelegraph.com/explained/what-is-a-daico-explained

[7] - https://www.bitgo.com

[8] -https://www.bitgo.com

[9] - https://https://kyber.network

[10]   - https://https://kyber.network

[11]   - https://republicprotocol.com

[12]   -https://republicprotocol.com

[13]   - https://paritytech.github.io/wiki/Proof-of-Authority-Chains

[14]   -https://paritytech.github.io/wiki/Proof-of-Authority-Chains

[15]   - https://wiki.parity.io/Aura

[16]   -https://wiki.parity.io/Aura

[17]   - https://komodoplatform.com/atomic-swaps/

[18]   - https://komodoplatform.com/atomic-swaps/