Bskt：用于创建去中心化代币投资组合的智能合约

D.Que、N.Dalal、Q.Pham 和 J.Tong

v1.0.0 (2018年3月27日)

摘要—Bskt 是用于创建去中心化代币投资组合的一种通用智能合约。它采用 ERC20 代币的形式，实现对一系列以太坊代币的捆绑和拆分。代币所有者对基础代币具有直接的申索权。

任何放弃基础代币的交易方均可创建这些新代币，而任何拥有所发行代币的交易方均可赎回新代币。Bskt 使得投资者能够以较低成本购买以太坊生态系统中的多种代币，并且不会增加保管风险。

I. 简介

Bskt 合约提供了一个容器，用于存储一系列的以太坊 ERC20 代币[1]，且不存在保管风险。Bskt 也可以用作加密代币存储容器的通用框架。

在 2018 年年初，基于以太坊的 ERC20 代币数量超过 600，总市值逾 600 亿美元[2]。随着创建自带加密功能的“安全”代币领域不断取得创新，以及从房地产到股票等现实世界资产的“代币化”浪潮，市场对加密代币的需求可能会持续攀升。

加密代币的疯狂增长催生了新的需求，需要开发一种可轻松存储这些代币的结构体系。

Bskt 与交易所交易基金 (ETF)[3]、单位投资信任基金 (UIT) [4]和房地产投资信托基金 (REIT) 有许多相似之处，它们在全球拥有数万亿[5]资产。与现实世界中一样，这些结构体系可以轻松交易各种资产并降低交易成本。

ETF 的设计旨在使非机构投资者能够以较低成本获得和转移更多元化的权益投资组合。这款以太坊软件解决方案具备同样的优势。

II. 概述

Bskt 是一种以太坊合约，可代表代币持有者管理基础资产。以太坊合约符合 ERC20 标准，其核心是：

- **实例化**自定义 Bskt 按预先指定的基础代币和选定比例；
- **创建** Bskt 代币取代放弃基础代币；
- **赎回**基础代币的 Bskt 代币；以及
- **转移** Bskt 代币的所有权。

Bskt 并非一个新的区块链或协议，而是一种可以配置为存储任意数量基础 ERC20 代币的以太坊合约（请参见图1 中的示例）。新建代币的价值围绕基础代币的价值上下波动。

Bskt 还制定了开放的原子交换标准，以允许升级和投资组合调整。要求用户选择加入，并允许任何开发者提供错误修复或对基础组合进行更改。

由于 Bskt 属于 ERC20 代币，因此新 Bskt 可以由各种基础 Bskt 组成。

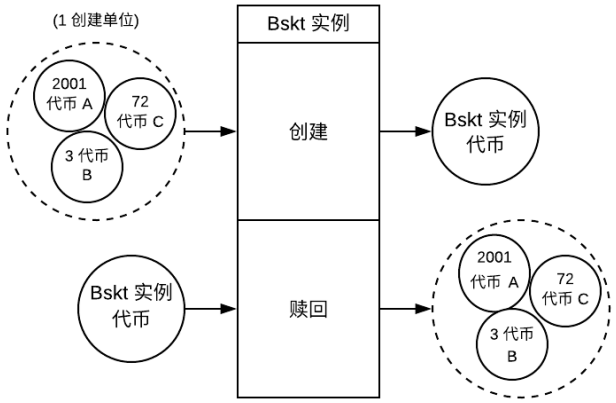

图 1: Bskt 使用说明。上图显示了由代币 A、代币 B 和代币 C 组成的 Bskt 单一部署示例。此合约允许创建和赎回Bskt 代币。

A. 优点

通过使用 Bskt，持有者可以获得以下优势：

- **投资组合多元化**：可以组合许多不同的代币来创建多元化投资组合。
- **访问便捷**：代币通常分布在多个交易所中，并不面向所有投资者。通过 Bskt 则可以轻松访问各种代币。
- **交易费用低**：从交易所先购买所有代币再转移的费用极高；虽然创建 Bskt 实例也需要费用，但通过创建可交易的单位可以降低未来成本。
- **易于转移**：移动许多不同代币是一种十分糟糕的用户体验，并会增加出错的风险。
- **小数金额转移**：可通过 Bskt 将价格高昂、不可交易的代币划分为可管理的单位。

Bskt 与 ETF 等传统资产结构体系有些相似之处，但也具有一些明显优势：

- **去中心化**：由于保管由智能合约管理，第三方无法控制或窃取基础代币。
- **透明度和可信度**：Bskt 的持有情况在区块链上完全透明且任何人都可读取。很容易识别抵押不足的 Bskt。
- **易于创建投资组合**：Bskt 允许访问不同的基础代币组合，创建过程简单并且不会产生过多开销。
- **自带加密功能**：与传统金融工具不同，Bskt 属于一种区块链资产，可直接在其基础之上构建基于区块链的智能合约。
- **民主化创建方式**：在传统资产结构体系（如 ETF）

中，只有少数富有的专业投资者可以执行创建和赎回。Bskt 创建单位可比传统资产类别所需的规模小几个数量级。

III. 工作原理

A. 术语

ERC20：ERC20 是一种代币标准。任何实现标准接口的智能合约均视为 ERC20。与本文相关的关键方法如下：

- `transfer` - 允许所有者将代币发送到某地址。
- `approve` - 允许所有者将代币转移至另一买家地址。
- `transferFrom` - 用于转移批准的代币。

基本单位 (BU)：代币或硬币可分割的最小原子单位。以太坊的基本单位是 wei。

小数位数：指用于确定代币基本单位的 ERC20 的 `Decimals` 属性。`Decimals` 通常设置为 18，但可以更改。对于 Bskt，`Decimals` 始终为 18，因此基本单位为 10^{-18}。

Bskt 合约与 Bskt：Bskt 合约是一种通用合约，可通过参数进行部署以创建 Bskt 实例。Bskt 实例可以代表不同投资组合。

创建单位：创建和赎回所需的可分割的最小金额。Bskt 必须以创建单位的倍数创建和赎回。

B. 摘要

可以针对特定列表和比例的基础代币轻松配置 Bskt 合约。部署的合约实例为*Bskt* 实例。Bskt 遵循标准的 ERC20 代币标准。

ERC20 代币名称	代币地址	数量/创建单位 (BU)
代币A	0x86fa0498...78ecfdb0	2001
代币B	0xf230b790...3bed42e2	72
代币C	0xd26114cd...dB8A0C07	3

表 I: Bskt 实例示例。此表显示了用于指定新 Bskt 的关键值。

C. 关键操作

实例化：要新建 Bskt 实例，用户需要指定基础以太坊代币的地址和比例。部署完成后，任何人都可以使用该 Bskt 实例创建或赎回。

创建：`create` 函数允许用户在放弃指定数量的基础代币后铸造代币。该函数需要创建多个预先指定的"创建单位"。来自一个 Bskt 实例的代币不能与另一个 Bskt 实例一起使用，因为它们的基础代币可能不同。

创建过程的工作原理如下：

1) 根据期望金额确定要创建的 Bskt 代币数量。此操作通常可以在一些网站上实现自动化，此类网站可以读取 Bskt 实例的初始化参数，将请求的以太币金额映射为需要的基础代币数量。
2) 获取基础代币（通常在交易所购买）并转移到所控制的地址。
3) 为每个基础代币调用 ERC20 `approve` 函数，以允许 Bskt 访问每个代币的适当金额。
4) 调用 Bskt 的`create` 函数。
   - 使用 ERC20 `transferFrom` 函数，然后为创建者铸造 Bskt 代币。

我们的预期是，只有高级用户和套利者才会创建或赎回bkst 实例代币，大多数用户只是转移代币而已。将提供开源工具来简化创建/赎回流程。

赎回：`redeem` 函数首先根据指定金额销毁代币，然后使用 ERC20 的 `transfer` 函数将基础代币转移给赎回者。

redeem 可以选择带上额外的参数`tokensToSkip`，以指定要跳过的基础代币。鉴于目前许多以太坊代币都具有可暂停性，同时考虑到要降低 ERC20 代币恶意干扰 Bskt 的风险，此参数十分有用。

例如，一旦暂停，许多受欢迎的代币将无法转移。其团队计划在移至自己的区块链时尽快永久停止代币。下表显示了一些重要代币及其计划暂停日期：

名称	`approve`	`transfer`	`transferFrom`	暂停日期
EOS	可暂停	可暂停	可暂停	2018 年6 月1 日
ICON	可暂停	可暂停	可暂停	2018 年3 月x 日
Augur	确定	可暂停	可暂停	不适用

表 II: 此表显示了关键的ERC20 操作是否可暂停，以及某些重要代币的预计暂停日期。

如果没有跳过列表，那么一个代币转移失败可能使其他所有代币永久无法赎回。我们通过允许用户指定要跳过的代币来缓解此问题。这样可以以锁定跳过的代币为代价，防止其他代币被锁定。只应在基础代币失败并阻止赎回时使用跳过列表功能。

暂停（仅限所有者）：合约所有者可以暂停 `create` 操作。这样做的目的是允许弃用旧Bskt，同时允许持有者通过 `redeem` 来访问基础代币。

提取（未来版本提供，仅限所有者）：可能需要从最初创建的包中移除一个或多个基础代币。例如，基础 ERC20 创建者可以在他们准备启动其本地区块链时锁定其代币。

Bskt 合约所有者可以通过提取单个代币将其从包中分离开来（请参见图2），而不会要求所有持有者在新 Bskt 实例发行后赎回其代币。此过程可确保 Bskt 持有者保持全程保管。

此操作的结果是持有者拥有两个代币：不包含所提取代币的更新后代币和已提取的代币。可以认领提取的代币并将其转移到别处。

超额资金回收（仅限所有者）：在一些情况下，第三方可能会在合约中留下超额资金：

- 用户直接向合约发送 ERC20 代币，而无需依次使用 ERC20 的 `approve` 和 Bskt 的 create。
- 用户直接向 Bskt 合约发送 Bskt 代币，而不是使用 `redeem`。
- 用户在 redeem 函数中使用 `tokensToSkip`，但这些跳过的代币可以稍后转移。
- 用户将以太币发送给合约。

在任何情况下，合约所有者均可通过 `withdrawExcessToken` 和 `withdrawEther` 获得超额资金和代币。

原子交换：流通性 Bskt 可能需要更改以应用升级、合约的安全修复或对代币组合的调整。为了实现此功能，支持以新 Bskt 换旧 Bskt（请参见图3）。

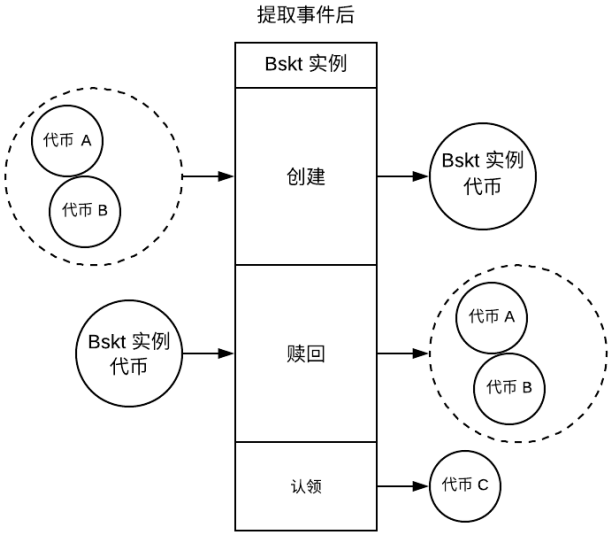

图 2: 从 Bskt 实例中提取代币 C 后，`create` 将不再需要该代币，并且也无法通过 `redeem` 赎回该代币。系统会记录所有权的快照，因此只有在提取之前拥有 Bskt 代币的交易方才能认领代币 C。

图 3: Bskt 实例代币通过升级合约提供的原子交换进行升级。旧 Bskt v1 代币换为新 Bskt v2 代币。

合约所有者操作：为了确保代币所有者始终持有保管权，只为合约所有者预留一些特定操作。在 Bskt 合约中，可以暂停 `create` 以允许弃用，并且可以提取超额资金。合约所有者不能收集基础"预留"代币或阻止转移操作。

D. 重要参数

地址：Bskt 通过指定基础代币的地址进行配置。

数量：以基本单位表示的一个创建单位所需的基础代币数量。可通过此参数设置初始投资组合分配并确定单个 Bskt 的价格。

所有数量均必须用无符号整数表示。数量根据创建单位进行计算，并进行相应优化，使 Bskt 能够尽可能多地保留可分割性。

创建单位：Bskt 必须以创建单位的倍数创建和赎回。分配创建单位约束以防止出现小数金额的基础代币。可通过此参数将其定义为无符号整数，同时可避免精度损失。

Bskt 最小可按照 1 个基本单位(10^{-18}) 的金额进行转移，这意味着可以按创建单位的分数量转移。与现实世界的 ETF 不同，创建单位通常是很小的数字（通常小于$0.01).

创建单位根据以下约束进行计算：

- 目标价格
- 投资组合分配
- 基础代币可分割性
- 基础代币价格
- 所有代币数量必须为自然数的要求
- Bskt 可分割性的最大化

创建单位的计算公式如下：

$$\Gamma s \propto UM = 10^{18-\lfloor log(min_i(p_i)) \rfloor}$$

表III 通过一则示例给出了最佳说明。

IV. 实现

请注意：作为本白皮书的一部分，我们将使用 *MIT* 许可证发布 *Bskt* 合约 *v1*。所有代码和文档均按原样提供，并且可能存在错误。

在 GitHub [7] 上提供了我们的 Bskt 实现。Bskt 投资组合测试实例已部署到 mainnet，并且可以在我们的 repo 中找到。

V. 安全性

由于 Bskt 高度倚重 `approve`、`transfer` 和 `transferFrom` 的 ERC20 功能，因此安全性取决于这些功能的实现方式。部署 ERC20 代币的团队通常会对这些功能进行修改。

在创建新 Bskt 实例时，部署团队应确保审核所有基础代币合约，以确保无法实施恶意或意外行为。

A. 拒绝服务

由于 `create` 和 `redeem` 的同步性质，如果某个代币的某项操作失败，将会阻止整个操作的运行。

这种操作可能是善意的（例如，暂停代币以进行本地代币空投升级），也可能是恶意的（例如，某基础代币意图通过锁定代币来进行劫持）。在对最受欢迎的代币合约进行审计之后，我们发现，最可能导致 `transfer` 或 `transferFrom` 失败的方式是代币所有者是否决定将其暂停。

作为一种保障机制，可使用上文描述的跳过列表功能保护 `redeem`。

然而遗憾的是，`create` 无法通过跳过列表获得保护。因此，如果某基础代币暂停，将无法再新建 Bskt。

Bskt 实例创建者和持有者均应验证基础代币是否能与 *Bskt* 一起使用。并非所有 *ERC20* 代币都可以与 *Bskt* 一起使用。

VI. 未来产品

资产代币化：其他区块链和资产（如证券和财产）的代币化将使Bskt 能够创建更多种类的 Bskt 投资组合。例如，Bskt 可以包括比特币、NEO 和 Nano 以及 ERC20 代币。

再平衡：Bskt 可以编制再平衡规则，以便定期对投资组合进行调整。主动和被动管理均支持。用户必须选择加入一次，但此后不必执行任何操作来将其 Bskt 再平衡。

代币	市值	价格	小数位数	分配	价值 /Bskt	数量 /Bskt	数量 /Bskt (BU)	最佳 创建单位	数量/ 创建单位(BU)	
代币A	$5,027,187	$4.61	18	48.11%	$2.41	0.5217	5.22E+17	不适用	5,217,270,035,202	参考书目
代币B	$2,739,853	$8.18	6	26.22%	$1.31	0.1602	1.60E+05	不适用	2	
代币C	$2,681,325	$4.94	12	25.66%	$1.28	0.2598	2.60E+11	不适用	2,597,843	
总计	$10,448,365			100%	$5.00			1.00E+13		

表 III: 此表显示了以目标价格 5 美元为例派生创建单位的过程。市值、价格和小数位数均基于代币进行输入。分配指的是代币占投资组合的市值加权百分比。价值/Bskt 指 1 个 Bskt 所需的代币的价值。数量/Bskt 是达到所需价值需要的代币数量。数量/Bskt (BU) 与最后一列相同，但以基本单位表示。最佳创建单位基于前一列计算，并针对 Bskt 可分割性进行优化。数量/创建单位 (BU) 是构成创建单位所需的最终数量。这些值均用于初始化 Bskt 实例。请参见示例电子表格[6] 查看所用的全部公式。

VII. 现有产品

分组资产这一理念是金融和早期加密货币项目的共同主题。在金融领域，ETF 和 UIT 是广泛使用的产品，可以让投资者轻松便宜地购买分组资产。我们的主要贡献是提供一个功能完美、经过测试的以太坊合约用于捆绑代币，同时认识到以太坊目前的一些关键故障状态。

A. *Crypto20*

与 Bskt 类似，Crypto20 是代表基础加密代币（包括许多非以太坊代币）所有权的 ERC20 代币。与 Bskt 不同的是，基础资产由一方保管，要求持有者信任 Crypto20。

B. {*Set*}

{Set} 协议提供了捆绑 ERC20 代币的框架。它与 Bskt 有许多相似之处，包括带创建和赎回方法的智能合约以及合约保管。Bskt 的关键性附加功能克服了现实世界中的使用难题，例如：1) 在赎回时提供跳过功能以缓解基础代币的暂停问题，2) 提供提取功能以从现有 Bskt 中移除代币，3) 原子交换框架，以及 4) 允许转移小数金额的最佳创建单位派生方法。

References

[1] Vitalik Buterin Fabian Vogelsteller. *EIP 20*. URL: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md. (accessed: 03.13.2018).

[2] CoinMarketCap. *Token Market Capitalizations*. URL: https://coinmarketcap.com/tokens/. (accessed: 01.15.2018).

[3] Community. *Exchange traded fund*. URL: https://en.wikipedia.org/wiki/Exchange-traded_fund. (accessed: 03.13.2018).

[4] Community. *Unit investment trust*. URL: %https://en.wikipedia.org/wiki/Unit_investment_trust. (accessed: 03.13.2018).

[5] Ryan Vlastelica. *ETFs shattered their growth records in 2017*. URL: https://marketwatch.com/story/etfs-shattered-their-growth-records-in-2017-2017-12-11. (accessed: 03.13.2018).

[6] Cryptofin. *Example creation unit derivation*. URL: https://docs.google.com/spreadsheets/d/1-VEg4ilDsTDRoFscdh-F1bNQIcWG2KLJfIyH3iScOxA. (accessed: 03.25.2018).

[7] Cryptofin. *Bskt*. URL: https://github.com/cryptofinlabs/bskt. (accessed: 03.21.2018).