Brickblock 技术白皮书

Marius Hanne, Jakob Drzazga, Adrian Kizlauskas, Philip Paetz, Martin Mischke

版本 0.9.3, 2017 年 7 月 17 日

目录

请注意，本文件仍然是早期草案; 一些实施细节缺失，有待改善。

本文旨在表现我司愿景的技术面，给读者一种评估我司设计可行性的方法。

我们正在开发一种概念验证实施的流程，并在八月的预售前发布第一个产品。技术实施细节将在决定后立即补充。

我们可接受社会的反馈和建议，并将尽全力彻底评估所有选项，不做草率决定。

摘要

本文件描述了一种建立在 Ethereum，Rootstock 等全球分布式计算网络顶端的智能合约平台。提出的资产证明（PoA）计划将使用户能够无缝交易代币，代表所有 ERC20 兼容市场上不同类型的外国资产。

基本思想是创建一些 PoA 合约，每个合约代表一项不同的外国资产。通过将代币合约与数字信托基金（DTF）相连，代币与外国资产的价值之间将会有近 1：1 的结合。

用户可购买 PoA 代币以换取本币，通过交易或持有本币，获得资产支付的任何股息。

投资者可赎回 PoA 代币，促使 DTF 清算相应的外国资产，并用本币退还当前市价。

1 综述

在供款期，Brickblock 代币（BBT）将在供款者间进行分配。

Brickblock 代币可在任何市场中进行交易，或者被锁定以产生所谓的访问代币（ACT）。

访问代币需支付履行 PoA 合约的费用，并保持长期活跃。

资产证明代币代表可在 Brickblock 平台上交易的某种外国资产。支持这些代币的资产由一个可公开审计的数字信托基金持有。

这些代币均执行 ERC20 规范，并在兼容的第三方市场上无缝交易。

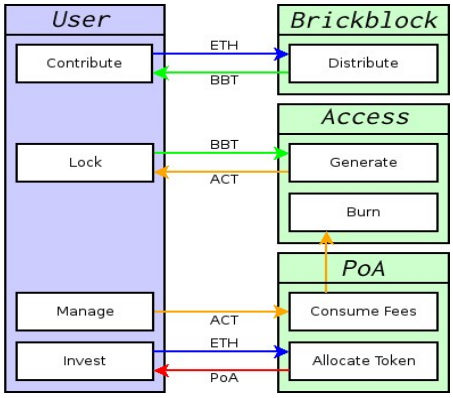

图 1：不同类型的代币以及它们的相互作用

User 用户	
Contribute 贡献	Distribute 分布
Lock 锁定	Access 访问
Manage 管理	Generate 生成
Invest 投资	Burn 销毁
Consume Fees 消费费用	
Allocate Token 分配代币	

2 Brickblock

运行在区块链上的智能合约可代表 Brickblock，该区块链处理经纪人注册并管理个人 PoA 合约。

2.1 Brickblock 代币 (BBT)

Brickblock 合约本身实施一种与 ERC20 兼容的代币，这些将被分发给我们的筹款供款者。

除了可交易外，还需这些代币来生成新的访问代币。

2.2 访问代币 (ACT)

访问代币需支付费用以运行 PoA 合约并保持活跃。它们只能通过将 BBT 锁定到访问代币合约中得以生成。

当 BBT 被锁定时，合约将向发送方账户记录新的 ACT。BBT 被锁定时，生成 ACT 的速率随着时间的推移而提升。然而，生成的 ACT 可随时撤回，这样做会重置生成锁定的 BBT 的年限。

访问代币需运行 PoA 合约的某些功能，并在使用时进行销毁。 PoA 合约将在访问代币合约中注明用户地址以及 ACT 所需的数量。如果用户在账户中具有足够的代币，那么会降低所请求的金额，并允许继续操作。如果余额不足，则会产生例外，从而阻止 PoA 合约执行所需求的功能。

2.3 数字信托基金(DTF)

Brickblock 将建立一个数字信托基金，该基金在托管人投资账户中持有支持 PoA 代币的资产。

托管人将对 DTF 账户中的活动进行公证，并发布证明，以便每个人都能验证所有负债都已核算。

2.4 费用

在使用期中，PoA 合约要求各方以 ACT 的形式支付三种不同类型的费用：创建费、清算费和存款费。

经纪人需支付创作费用，以创建新的 PoA 合约并将其提供给投资者。如果用户希望以本币赎回代币，用户需支付清算费用。

任何有兴趣继续履行合约的人都需支付存款费。如果没有足够兴趣来支付费用，合约中止运行，直到支付足够的费用进行恢复。这将有助于终止过时和不必要的合约，并为经纪人提供额外的奖励，使其具有吸引力。

付费的 ACT 将被销毁，从而取消流通。在使用后，Brickblock 不会再保有或交易 ACT。

2.5 合约的发行与升级

为了实现功能的升级，所有智能合约都将通过与带有固定地址的代理合约进行访问。

在发现错误的情况下，个人合约也可紧急中止。

通过控制升级机制的单一方，我们认识到实际权力下放的部分丧失。然而，BBT 持有人将有能力提出反对意见，从而将任何部署到生产网络的变更进行延迟。

2.6 经纪人注册

经纪人必须经 Brickblock 团队批准，并经过严格的尽职调查程序，才能在平台上进行交易。Brickblock 合约持有一份当前所有活跃经纪人的列表，并允许 Brickblock 管理员进行添加与删除。要在列表中添加经纪人，必须在 ACT 支付费用。

3 资产证明

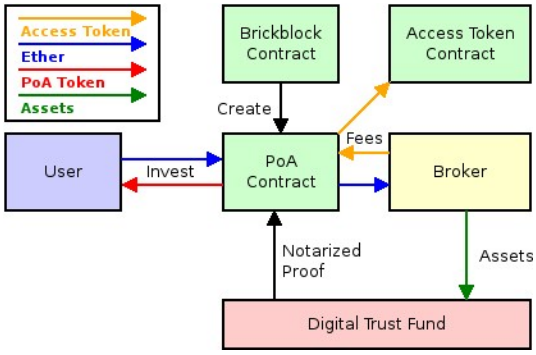

图 2：资产证明方案

Access Token 访问代币
Ether
POA Token: POA 代币
Assets 资产
Brickblock contract : Brickblock 合约
Access Token Contract：访问代币合约
Create 创建
User 用户
invest 投资
POA Contract： POA 合约
Fees 费用
Broker：经纪人
Notarized Proof 公证证明
Digital Trust Fund 数字信托基金

资产证明机制通过在用户、DTF 和经纪人之间建立“信托三角”得以运作，其中需要一份相互信任的智能合约。

用户向合约支付本币。一旦他或她将所需的资产发送到 DTF，经纪人可就这笔款项进行索赔。

DTF 证明智能合约收到资产，该合约向经纪人发放本币，并将新创建的 PoA 代币发送给用户。

用户可相信本合约只有在收到有效的资产证明或退还初始金额时才得以激活。

经纪人同样可委托合约发放资金，并且必须相信 DTF 会将收据凭证发送到合约中。托管人公开提供实际收据凭证，托管人必须值得信赖，不得在任何情况下盗用资金。

与经纪商建立信任之前，DTF 将承担微额信贷，以通过托管人与经纪人进行交换。DTF 将从智能合约而非经纪人手中收到本币，并将其进行转换以支付微额信贷。

托管人公证并发布 DTF 账户的任何交易和余额。这使用户能够独立验证 DTF 的所有负债在任何时间仍然有效。如果不匹配，用户可向 PoA 合约发送欺诈证明，以锁定和中止一切交易。

想要以固定价格即时购买代币的用户可在任意的、ERC20 兼容的、外部代币市场上进行购买。这减轻了获取和处理一篮子不同货币的负担，并允许用户无需等待，以单一货币简单地购买 PoA 代币，尤其是在硬币交易基金（CTF）的情况下。

3.1 创建

在创建新的 PoA 合约时，经纪人会删除参数（见表 1）。

这些字段的内容在不同类型的 PoA 合约之间有所不同，具体情况如下。

例如，CTF 合约通常只需可忽略的最小供应量。因此，无需注资阶段，也无需延期合约，因为新代币一旦创建就立刻被激活。

现实世界资产合约的托管信息是托管人的公钥，用于签署资产证明。加密资产合约需要一份持有不同货币的所有账户的列表。

3.2 激活

为了激活 PoA 合约，必须从通过 DTF 收到资产的托管人处得到有效证明。

对于现实世界资产合约，此证明即是托管人的签名，公证 DTF 的经常账户余额。

对于加密资产合约，证明基于验证在外国区块链中包含资金交易。

如果未在规定的超时时间内收到有效证明，合约将向投资者支付收取的全部资金。

表 1：资产证明合约参数

资产标识	资产的识别，如 ISIN
名字/符号	智能合约生态系统中代币的名称和符号
最低供应量	最低初始资金需求
托管信息	验证托管人证明所需的数据
超时	如果没有达到目标，注资阶段被取消的时间

3.3 交易

所有 PoA 代币都与任何其他代币一样，可在 ERC20 兼容的外部市场上进行交易。

3.4 股息支付

当 PoA 合约追踪的资产产生任何股息时，DTF 将将其转换为本币，并发送到 PoA 合约中，分配给所有代币持有人。随后，用户可随时索要利润。

3.5 偿还

用户可在任何时候用本币兑换活跃的 PoA 代币当前的市价。

为此，用户必须先使用 Brickblock 完成强制性的“了解客户（KYC）”流程。

当用户将 PoA 代币发送回合约时，他们将以本币形式接收追踪资产当前的市值。合约将通知提供所需的本币 DTF，并通过经纪人清算适当数量的份额。

3.6 延期

为了扩展 PoA 合约的资产基础，可创建一份实施与母公司合约相同的新资金回收的分包合约。激活后，分包合约将向其母公司发送资产证明，促其对新余额进行合并。

请注意，只有当新的融资周期自身具有最低供应限制时，这种做法才有必要。在大多数情况下，当 DTF 获取必要的附加资产时，用户可简单地从合约中购买新的代币。

3.7 欺诈证明

DTF 的所有负债将被公示，允许每个人发现差异来向 PoA 合约证明该事实。

当合约收到有效的欺诈证明时，它会自动锁定并中止活动。

除非合约在一定时间内提供新的有效的资产证明，否则会自动破坏所有代币，使其失效。

合约再次解锁后，可恢复正常运行。

4 现实世界资产基金

现实世界资产基金合约由交易所交易基金（ETF）和房地产基金（REF）等外国资产构成。

4.1 资金

PoA 合约最初向投资者出售代币以换取本币，直到达成规定的融资目标。

4.2 失败

如果在规定的时间范围内未达到资金目标，或者激活超时，则合约进入失败阶段。

投资者可将其购买的 PoA 代币发回至合约中，收到本币作为补偿。

4.3 待办

如果达成资金目标，合约进入待办阶段，并告知经纪人对外国资产进行担保。

经纪人对外国资产进行担保，并将其转移至 DTF 与托管人的账户。托管人将对 DTF 账户中的所有交易以及相应的 PoA 合约地址进行公证与发布。

托管人将通过加密签署由以下内容组成的声明启动 PoA 合约：

地址 合约的地址

ISIN 外国资产识别

数量 股份转让数量

4.4 激活

如果证明有效，合约将进入激活阶段。如果合约在一定时间内未被激活，则进入失败阶段。

合约证实签署的声明均包含预期数据，并具有托管人的有效签名。为此，它首先从记忆中重新创建预期的报表数据，然后将该数据与接收的签名结合使用以恢复签名地址。如果复原的地址与托管人的地址吻合，则可同时证明数据正确，签名确实由托管人所写。如果声明数据与保管人用于创建签名的信息不同，则复原出不同的地址，合同也不会被激活。

PoA 合约通知经纪人他或她的资金被清算。经纪人现在可从 PoA 合约中申请报销，并将收到筹集的本币。

4.5 股息支付

每当追踪资产产生股息时，股息将被转换为本币，并发送到 PoA 合约中。

投资者随时可要求分红。

4.6 偿还

投资者可按照追踪资产的当前市场价格赎回 PoA 代币。

发回合约的代币被销毁，DTF 要求经纪人清算相关资产。

DTF 将收到的资金转换成本币，并将其发送至合约中供用户索赔。

4.7 延期

经纪人可决定扩大现有 PoA 合约的资产基数。

为此，PoA 合约创建了一个新实例，它将通过之前描述的相同的融资与激活过程运行。它也将自然地与其母公司合约共享某些属性，如 ISIN 和 Symbol。

一旦分包合约完成融资，它就进入了吸收阶段，而母公司合约则将代币余额进行合并。由于分包合约与母公司合约遵循完全相同的规则，母公司合约可接受新的代币，可与本币进行有效互换。

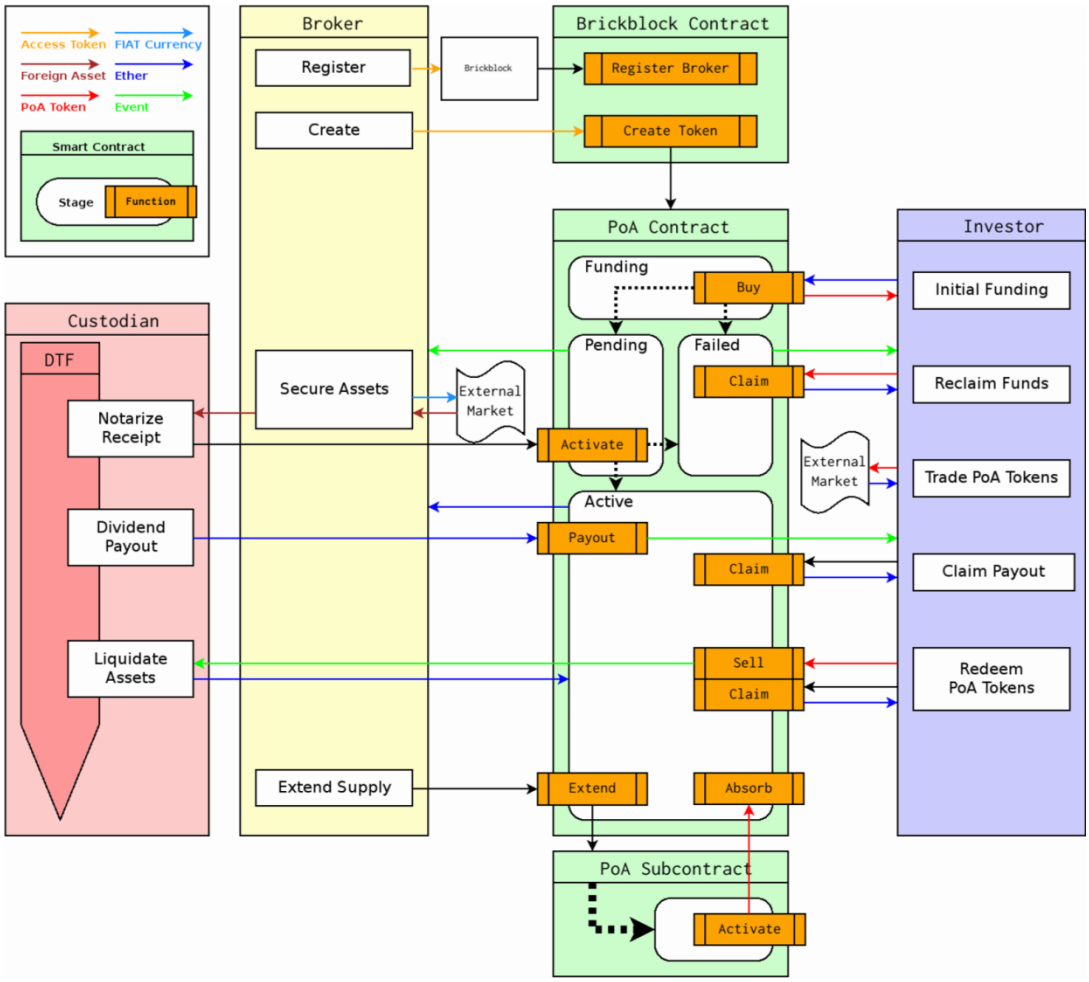

图 3：ETF / REF 的资产证明代币周期

Access Token ：访问代币
FIAT Currency ： FIAT 货币
Broker ： 经纪人
Brickblock contract： Brickblock 合约
Foreign Asset： 外国资产
Register ：注册人
Brickblock
Register Broker：注册经纪人
POA Token： POA 代币
Event ：事件
Create： 创建
Create Token：创建代币
Smart contract：智能合约
Stage Function：阶段功能
POA contract： POA 合约
Investor ： 投资者
Funding ：融资
Buy：购买
Initial Funding：初始融资
Custodian：托管人
Secure Assets ： 担保资产
External Market ： 外部市场
Pending ： 待办
Failed：失败
Notarize Receipt ：公证收据
Claim：索赔
Activate：激活
Reclaim Funds：回收资金
External Market：外部市场
Trade POA Token：交易 POA 代币
Dividend Payout ：股息支付
Active：活跃的
Payout：支付
Claim：索赔
Claim Payout：理赔
Liquidate Assets：清算资产
Sell：出售
Claim：索赔
Redeem POA Token：回收 POA 代币
Extend Supply：扩大供应
Extend：扩大
Absorb：吸收
POA Subcontract ：POA 子合约
activate 激活

5 加密基金

加密基金合约由不同加密货币或代币组成的资金，比如 Bitcoin, Litecoin，Dash，Ethereum，Golem，甚至 BBT 或 ACT 本身。

有三种类型的合约，硬币交易基金（CTF），硬币管理基金（CMF）和自主硬币基金（ACF）。

用户可购买 PoA 代币，代表一定数量的外币或本币、代币。

这些资金可为根据预先确定的一套规则运作的消极 CTF 或积极 CMF，由担保或无担保市场的经纪人进行交易。

未来，我们希望增加完全自主的硬币资金，实现合约内的所有交易。

5.1 消极的硬币交易基金 (CTF)

根据预定义的一套规则，消极硬币交易基金合约由不同加密货币组成。

通过改变创建和赎回篮子的构成，合约调整持有量以适应变化的市场。

托管人答复当前篮子组合的询价单（RFQ）。

5.2 硬币管理基金 (CMF)

硬币管理基金合约将允许基金经理在第三方市场对账户中收到的资金进行交易。

用户可用任何货币进行支付，基金经理将其转换为所需的组合。

5.2.1 担保账户

Brickblock 将提供担保账户，基金经理可在经验证可信赖的交易所进行交易。这些账户的功能有限，只可用于交易。提款只能返回到 DTF 中。这将使信用较差的基金经理以受控的方式提供服务，以建立追踪记录并重获信誉。

5.2.2 无担保账户

为了向既定的基金经理提供灵活度，他们需表现良好，可允许他们自行交易。向他们提供完整的资金所有权，并通过他们选择的方式进行管理。如果条件支持，基金经理可选择提供资产证明，但这并不是强制性的。

用户将始终关注账户和担保投资的基金经理的类型，并将这些信息纳入风险计算。

将来，Brickblock 将为托管账户或值得信赖的基金经理提供保险。

5.2.3 股息

如果基金产生股息，则由基金经理收取，转换为本币，并发送到合约中。在任何时间，代币持有者都可收到通知并申请一定份额。

5.2.4 偿还

投资者可随时兑换代币，将其寄回合约中。基金经理将清算头寸，将其转换成本币，并将其发送至用户要求的合约中。

5.3 自主的硬币基金 (ACF)

我们还想跨多个区块链自主探究全自动合约交易。在实现多数加密货币之间的可靠双向挂钩之前，唯一的选择是通过第三方交易所进行交易。该合约可与 Shapehiftbot 等 API 进行连接，自行交换货币。

为了给交易机器人创建一个市场，我们允许用户提交按照智能合约实施的交易算法和市场模型。开发人员可提供结果，用户可评估表现并投资于优选合约。

6 兼容性

所有代币合约将与 ERC20 规范兼容，这使得在兼容的交易所和钱包中进行交易显得微不足道。

我们正在评估在合约的发现与升级中面临的几个选择，并希望与其他项目一起找到一个共同的解决方案。

智能合约可通过 BTCRelay 等简化支付验证（SPV）确定比特币和派生区块链。

尚未决定基本智能合约引擎。我们目前正在基于 Ethereum 区块链构建原型，并评估 Rootstock,Tezos 和 EOS 等可比较系统。

7 术语表

资产基数：由 PoA 合约管理的外国资产金额。

托管人：持有 DTF 外国资产组合的值得信赖的组织。

数字信托基金（DTF）：一个监管严格的金融机构，代表投资者合法拥有资产。

外国资产：存在于 Ethereum 生态系统之外的资产，即不是 Ether，而是 REFs，ETFs 或 CTFs。

本币：一种以区块链接平台为源头的货币，如 Ethereum 的 Ether（ETH）。

PoA 代币：如同 ERC20 的智能代币，代表与某外国资产相同的价值。