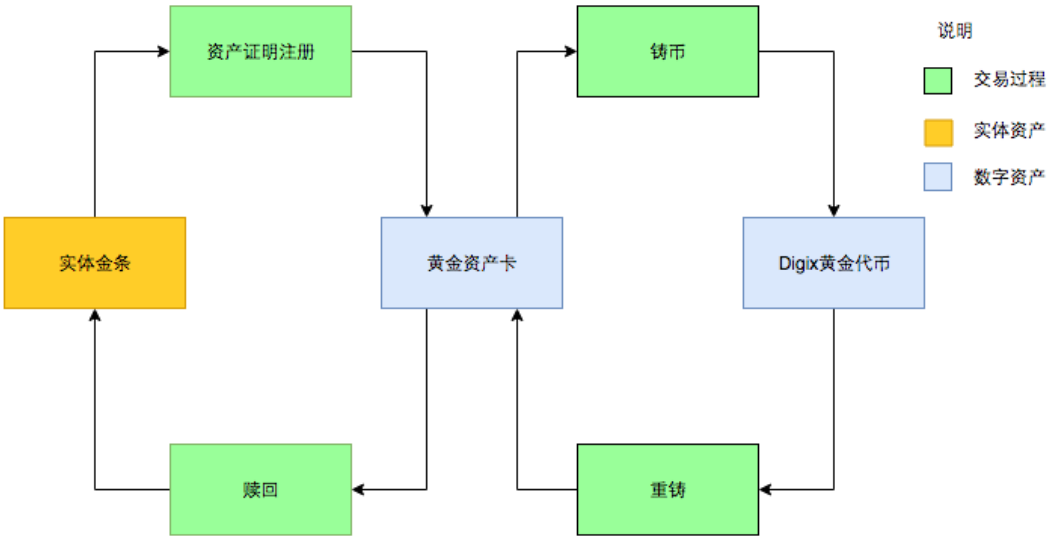
Digix 白皮书：密码学资产中的黄金标准

摘要

Digix 通过它的资产证明（PoA）协议为实体资产代币化和文档化提供了使用实例。PoA 协议利用以太坊和星际文件系统（IPFS） 通过监管链（chain of custody）追踪资产。它实现了开放和公开的资产存在性认证，无需一个中心化数据库。Digix 也提供一个应用程序接口（API），允许其它应用建立在我们的资产代币化服务之上。

技术总览：

产品生命周期:



核心产品

1、资产证明（PoA）资产卡

PoA 资产卡由以下信息构成，被永久性地上传到去中心化数据库：

- 资产卡创建时间戳
- 金条库存单位（SKU）
- 金条序号
- 监管链数字签名（供应商、托管商、审计商）
- 购买收据
- 审计文档
- 存储收据
- 存储费用

PoA 资产卡被保存在以太坊钱包中。

2、Digix 代币（DGX）

DGX 代币通过铸币智能合约生成。每个 DGX 代币代表 1 克黄金，可以细分到 0.001 克。每一个 PoA 资产卡被发送到铸币智能合约时，相应的 DGX 代币就被发行出来。例如，用户发送一个 100 克黄金的 PoA 卡到铸币智能合约，将获得 100 个 DGX 代币。

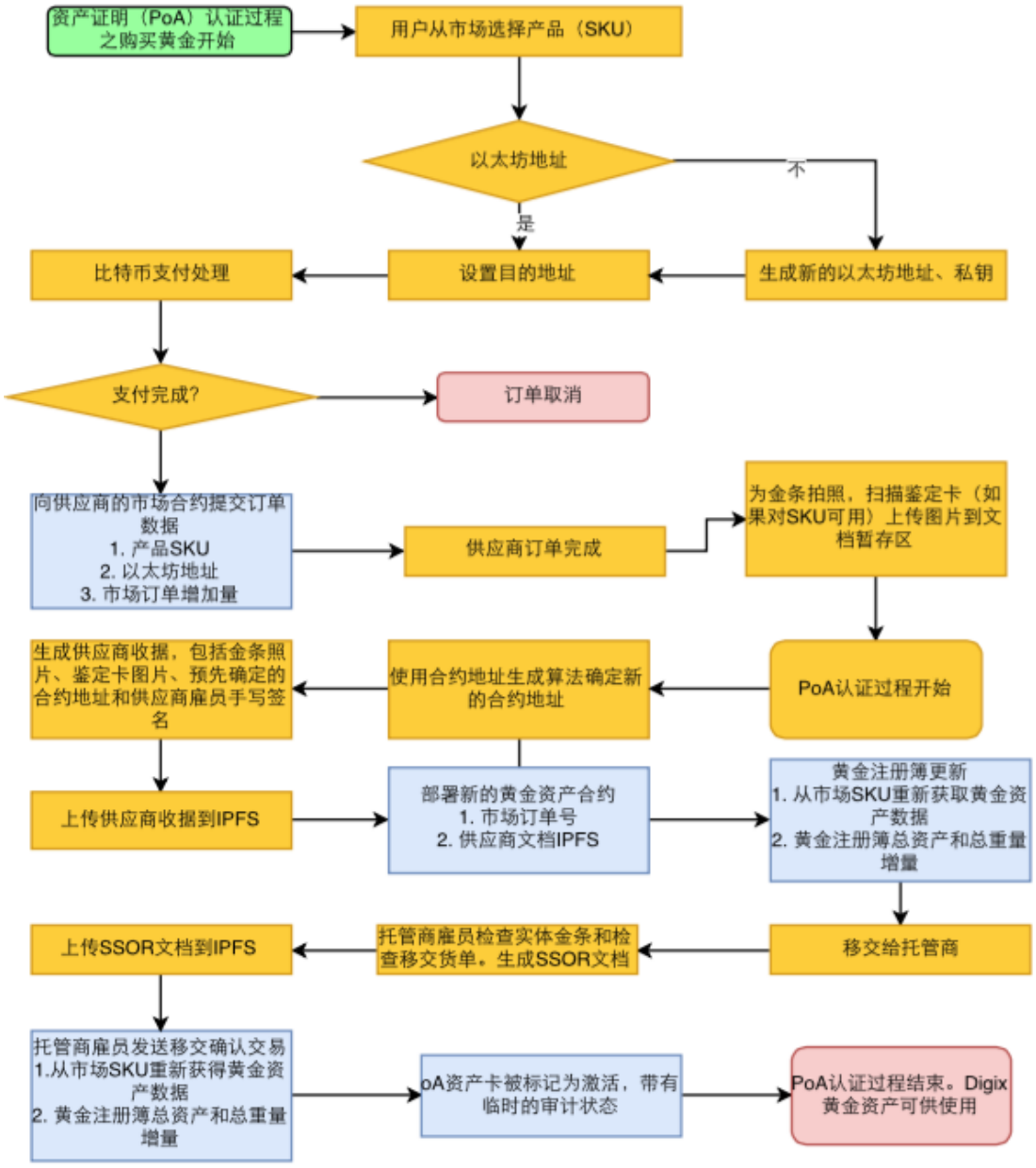
Digix 代币被保管在以太坊钱包。

核心过程

3 个模块过程–Digix 使用它为一项资产提供存在证明和可替代证明，1 个实体资产赎回过程和 1 个鼓励去中心化应用（Dapp）开发过程。这些过程包括以下部分：

1、资产证明（PoA）认证过程在以太坊上记录和提供一项资产的审计跟踪，用以创建 PoA 资产卡。这些资产卡通过来自于监管链参与者（即黄金供应商、托管商、审计商）的连续数字签名获得认证，数字签名进一步通过被提供和上传到 IPFS 所永久保存起来的购买和存储收据证明所确认。

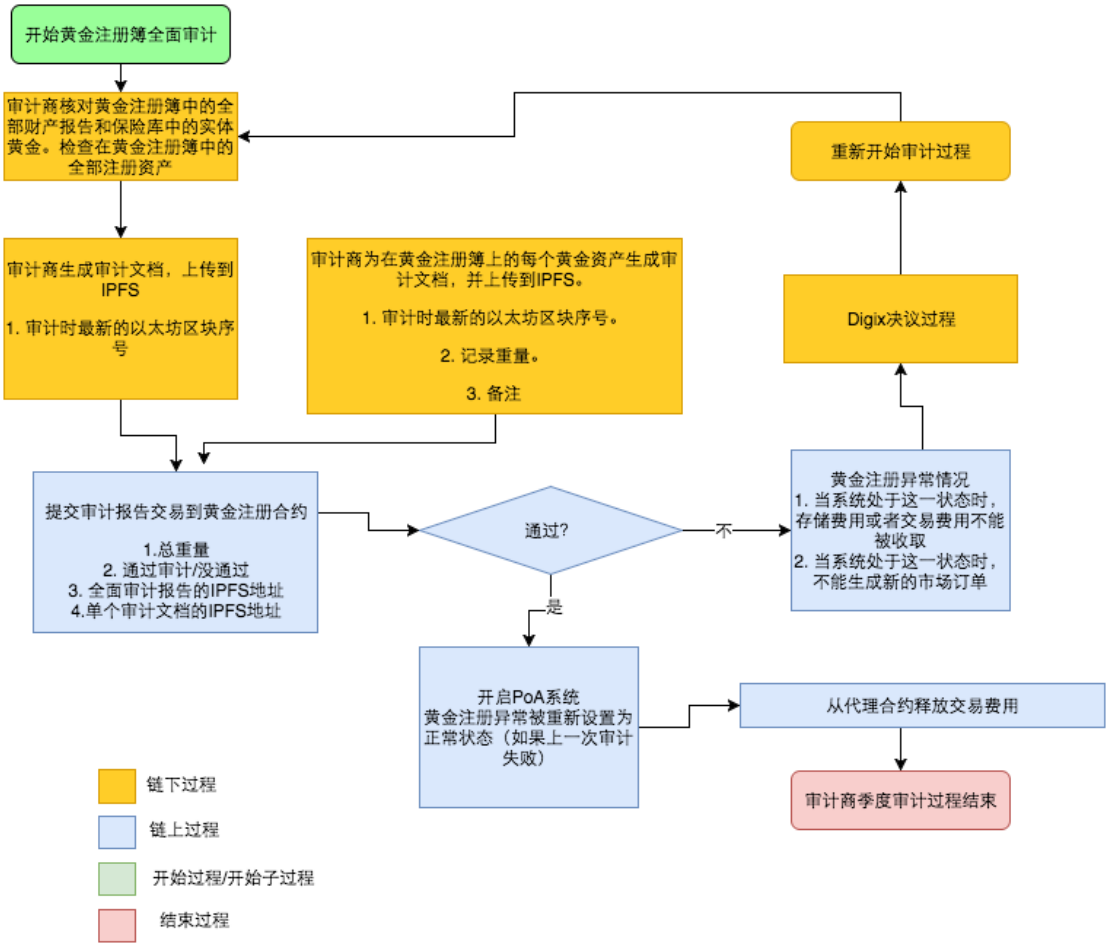
图表 ｉ ：Digix 资产注册过程



（注：上图第一个菱形中文字应为：以太坊地址，使用现有的地址？）

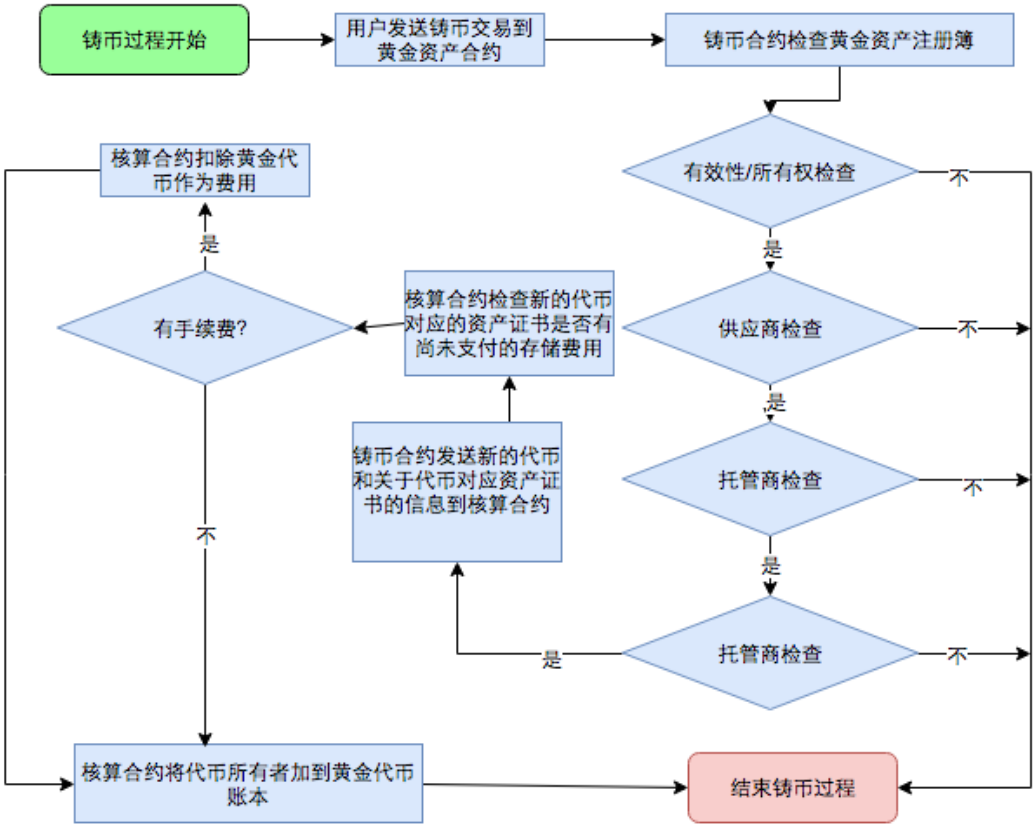
PoA 认证包括一个定期审计子过程，如图表 ii 所示。

图表 ii：审计过程



2、**铸币智能合约**，创建可替代的 DGX 代币，它接受或持有 PoA 资产卡，向用户返回 DGX 代币。

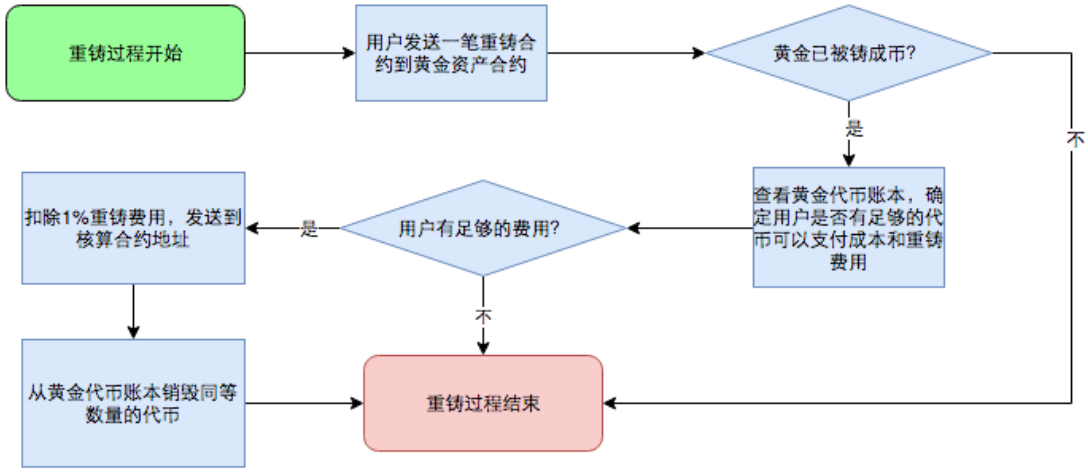
图表 iii：将 Digix 黄金资产卡铸为 Digix 黄金代币



（注：右边第四个菱形中的文字应为：审计商检查）

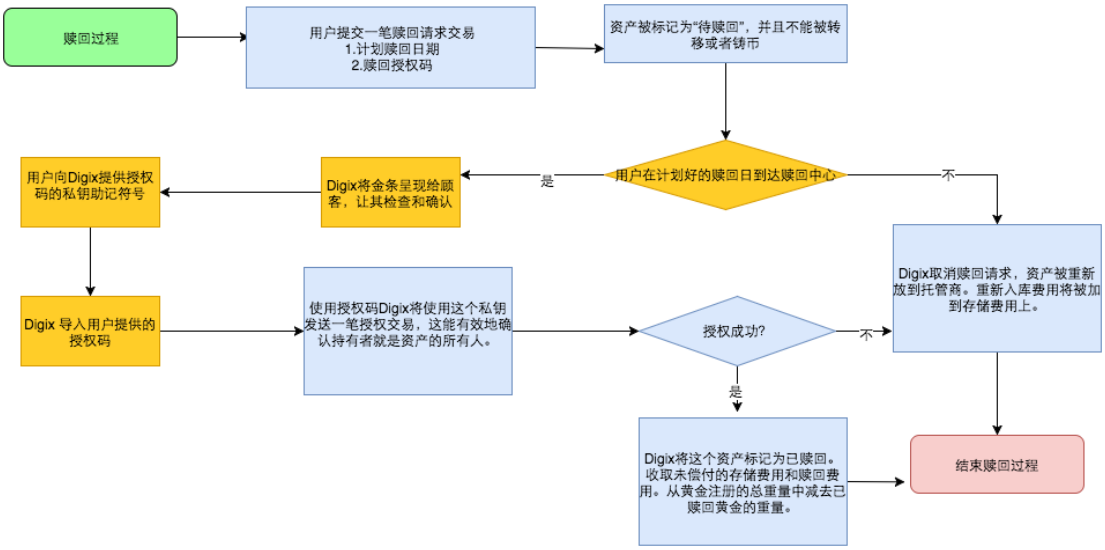
3、**重铸智能合约**，将 DGX 代币重铸为 PoA 资产卡。（图表 iv）

图表 iv：将 Digix 黄金代币重铸为 Digix 黄金资产卡



4、**赎回过程**，利用 PoA 资产卡赎回实体金条。（图表 v）

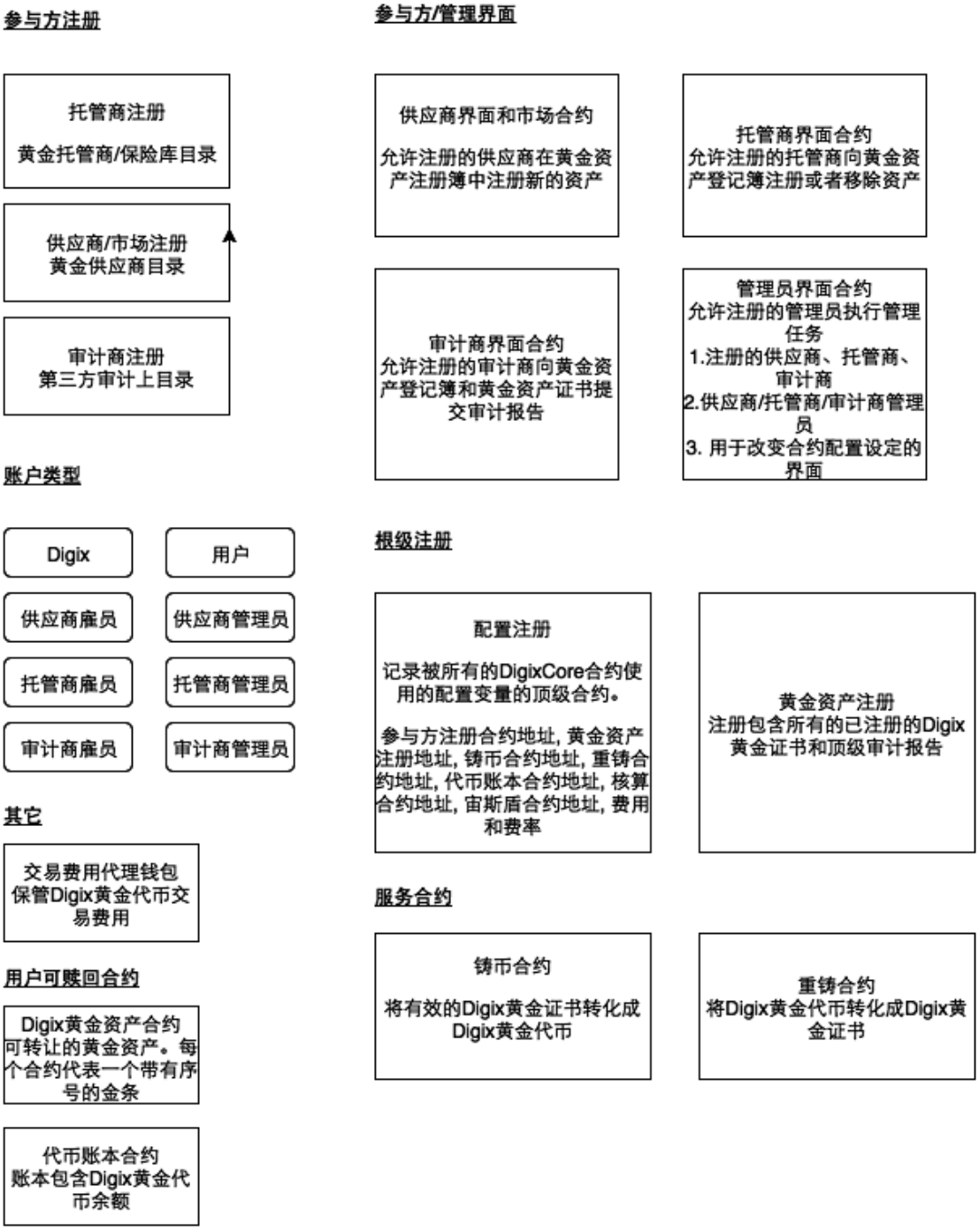
图表 V：Digix 黄金赎回和基于代币的用户身份证明



5、**通用输入/输出（I/O）合约**，运行开发者利用 PoA 资产卡或者 DGX 代币进行去中心化应用（Dapp）开发。

以太坊智能合约栈。

下面的图表展示了包含以上过程的 Digix 智能合约如何部署在以太坊区块链上。



Digix 资产证明参与者

（区块链线下实体）

资产供应商

ValueMax 新加坡是一家上市公司，在 Digix 市场上提供伦敦金银市场协会（LBMA）认可的金条。ValueMax 新加坡成立于 1988 年，他们提供典当服务和二手珠宝、黄金、名表的零售和交易服务。

独立审计商

Bureau Veritas Inspectorate 将对我们的黄金托管商库存金条的重量和质量进行季度审计，确保 DGX 代币有实体黄金支撑。他们是一家跨国集团，涉足多个商品领域，为贵金属提供独立的检查、取样和检测服务。

每个金条在审计时都将被用机密检查设备严格地检测。我们使用超声波计量器（UTM）和密度计执行这些检测。UTM 是一种基于超声波返回物体表面所用时间测量物体局部厚度的无损测量方式。密度计是使用排水量测量物体密度的设备。

托管商保险库

MalcaAmit 的现代化设备靠近新加坡樟宜国际机场，位于新加坡自由港，它是一个面积达 25000 平方米的高度安全和可空调控制温度的保险库，以通过绿色建筑工程实现的最前沿安全技术著称。

多方信任机制

Digix 依赖多方独立的参与者为实体资产代币化提供一个透明的平台。我们可以假定基于工作量证明（PoW）的密码学货币系统中的矿工将理性行动，即他们将通过履行交易确认职责，实现收益最大化和保护他们的长期利润。我们假设，理性矿工的垄断联盟将不会合谋进行双花攻击，因为这样的攻击将造成整个系统的声誉受损。我们因此假设 Digix 系统中三个参与方--负责提供黄金的供应商、负责保管和保证资产安全的托管商、负责保证托管商资产的真实性，都将以理性的方式行事，通过收取服务费用实现利用最大化。

利用现实世界的管理解决潜在的单点故障

监管链上不诚实的参与者和共谋

Digix 与提供严格监管和公司管理的公司合作。我们的合作公司不是上市公司就是因他们的专业服务而在行业知名的公司。为了方式欺诈，我们的合作每个公司只能从事一种只能。例如，实体资产供应商不能再充当资产托管商。一项服务的利益必须独立另一项服务。尽管共谋的风险是真实存在的，但是对于共谋者来说，信誉和法律成本是极高的。因为这些公司还为其他顾客提供类似的其它服务，核心业务的信

誉和合法性受损对他们是有害无利的，我们可以做一个合理的假设，他们将以理性的方式行事。

核心益处

没有中心化数据管理加密资产记录

所有的监管链信息完全由以太坊区块链管理。这个区块链账本以永久上传数据，花费的时间也明显少于在比特币区块链上传数据。

没有基于网页的登陆

没有网页形式的登陆。用户将从 Digix 下载桌面客户端。这个应用也可以从 Github 上的源代码编译出来，公开可审计。与传统的基于网页的用户登陆相比，Digix 的用户登陆方式极大地降低了中间人攻击。

安全的加密资产冷存储

Digix 的宙斯盾保险库是以太坊上面的密码学资产和密码学货币的冷存储钱包托管服务。

数字资产永久存在

所有的资产都被记录在区块链上，永久存在。即使 Digix 倒闭，已经生成的每个证明在可适用的司法辖区可以被法庭承认和采纳。

事后激励机制

资产证明过程要求常规的季度审计或者更加频繁的审计需要由第三方审计商执行，审计商需要对托管商保险库中所有的黄金资产进行审计。审计商对每个金条进行一次完整审计，包括核实金条的真实性、重量和物理检测，以检测异常和不合格品。审计商为已经审计过的每个金条在黄金登记合约上提交一份记录，该记录包含对签字的纸质文档的一个 IPFS 引用、审计商在以太坊上的身份信息和是否通过审计。

Digix 通过交易费用获得收入，交易费是用 Digix 黄金代币支付的。这些代币被保存在一个代理合约，只有经过第三方审计后这些代币可以被发送到一个特定地址。

通用输入/输出（I/O）合约和去中心化应用（Dapp）开发机会

Digix 提供的通用 I/O 合约允许开发者将 PoA 资产卡或者 Digix 代币进行于 Dapp 开发和事件记录。我们的愿景是为开发者创建一个生态系

统，将 DGX 代币用作各种各样的 Dapp 开发的架构。代码例子将在我们的 Github 上提供。

财富继承

去世用户的财产转移可以被做成一项服务，允许财富以密码学资产的形式被转移到 Digix 系统中被提到的以太坊地址。

博彩

在司法辖区，DGX 黄金代币可以像比特币一样，被用作博彩货币或者博彩代币。PoA 协议也可以被用于数字博彩资产的发行 7。

代理

DGX 代币可以区块链上的代理服务提供一个更好的、波动更小的价值储存手段。

众筹

Dapp 利用密码学货币和密码学资产可以提供众筹机会，或者将密码学货币转换为 DGX 代币，对冲价格波动。

由黄金支持的密码学货币开发

密码学货币可以利用 DGX 黄金代币和黄金资产支持它的部分价值。

交易所和财富管理 Dapp

当交易所整合 DGX 代币作为密码学货币交易对的一方时，它们将能够为密码学货币提供与黄金对冲的服务。开发能够调整你的密码学货币/密码学资产的比例财富管理服务，管理个人的密码学金融资产风险。

点对点（P2P）借贷和微金融

App 可以将 DGX 黄金代币应用到 P2P 借贷。借款人可以通过一个基于他的风险组合和信誉的 Dapp 寻找资金，并和出借人商定一个资金回报率。利息/收益支付可以每隔一段时间付一次，还要有一套惩罚系统，支付迟了要收到惩罚。这些已经在比特币上实现了，但是由于密码学货币的价格波动，在债务期出借人损失的资产价值可能比获得的利息价值更多。在 DGX 黄金代币的价格稳定将促成这些服务的应用。

抵押服务

私人持有的资产可以安全有效地被用作抵押品，不用通过冗长的认证过程确定一项资产的存在性和真实性。

结论

Digix 将提供一个透明、对审计友好、安全的协议，该协议利用以太坊的去中心化共识系统和 IPFS 的全部潜力在区块链上实现密码学资产。

原文：https://digix.io/whitepaper.pdf

作者： Anthony C. Eufemio ace@dgx.io Kai C. Chng kcchng@dgx.io Shaun Djie shaundjie@dgx.io

译者：@shaoping