Digix's Whitepaper: The Gold Standard in Crypto-Assets (English ／ 中文)

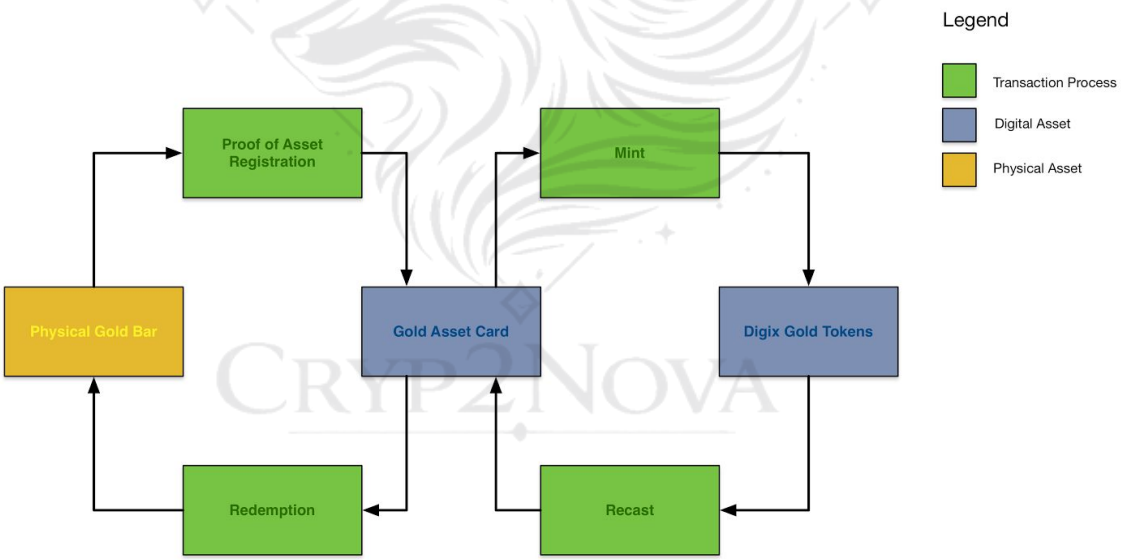
prepared by:
Anthony C. Eufemio <ace@dgx.io>
Kai C. Chng <kcchng@dgx.io>
Shaun Djie <shaundjie@dgx.io>
January 2016
Version 1.03

Abstract

Digix provides a use case for the tokenisation and documentation of physical assets through its **Proof of Asset (PoA)** protocol. The PoA protocol utilises Ethereum[1] and the InterPlanetary Files System (IPFS)[2] to track an asset through its chain of custody. This allows for the open and public verification of an asset's existence without a centralised database. Digix also offers an API allowing other applications to be built on top of our asset tokenisation service.

Technical Overview:

Product Life Cycle



[1] "[English] White Paper · ethereum/wiki Wiki · GitHub." 2014. 29 Dec. 2015
[2] Benet, Juan. (September 11 2015) "The IPFS Project - How it works". IPFS

Archived copy · cryp2nova.com

Key Products

1. **Proof of Asset (PoA) Asset Cards**

   PoA Asset Cards consist of the below information permanently uploaded onto the decentralised database:

- Time Stamp of card creation
- SKU of the gold bar
- Bar Serial number
- Chain of Custody digital signatures (Vendor, Custodian, Auditor)
- Purchase Receipt
- Audit Documentation
- Depository Receipt
- Storage fees due

   PoA Asset Cards are kept in an Ethereum Wallet.

2. **Digix Tokens (DGX)**

   Dgx Tokens are minted via a Minter Smart Contract. Each DGX token represents 1g of Gold and divisible to 0.001g. For every PoA Card that is sent to the Minter Smart Contract, DGX tokens will be issued in return. For instance, a 100g PoA Card sent to the Minter Smart Contract returns 100 DGX tokens to the user.

   Digix Tokens are held in an Ethereum Wallet.

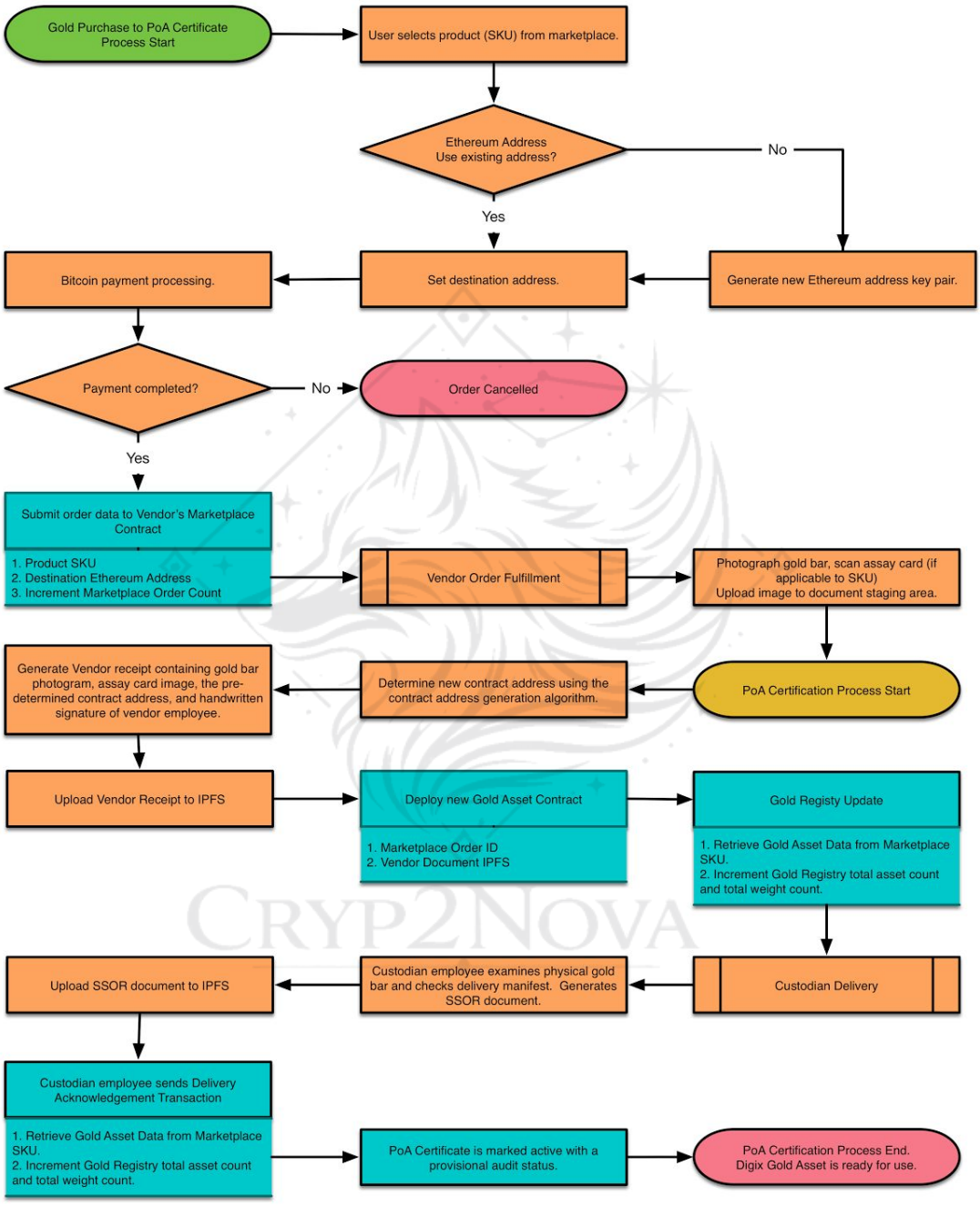
Key Processes

There are 3 modular processes that Digix uses to provide a proof of existence and fungibility for an asset, 1 for redemption of physical assets, and 1 that encourages Ðapp Development. Those processes consist of:

1. **Proof of Asset (PoA) Verification** process which records and provides an audit trail of an asset on Ethereum to create PoA Asset Cards. The asset cards are certified using sequential digital signatures from the entities in the chain of custody, namely, the **Vendor, Custodian**, **Auditor**, which are further validated with proof of purchase and depository receipts provided and uploaded onto IPFS for permanent record (Fig i).

Archived copy · cryp2nova.com

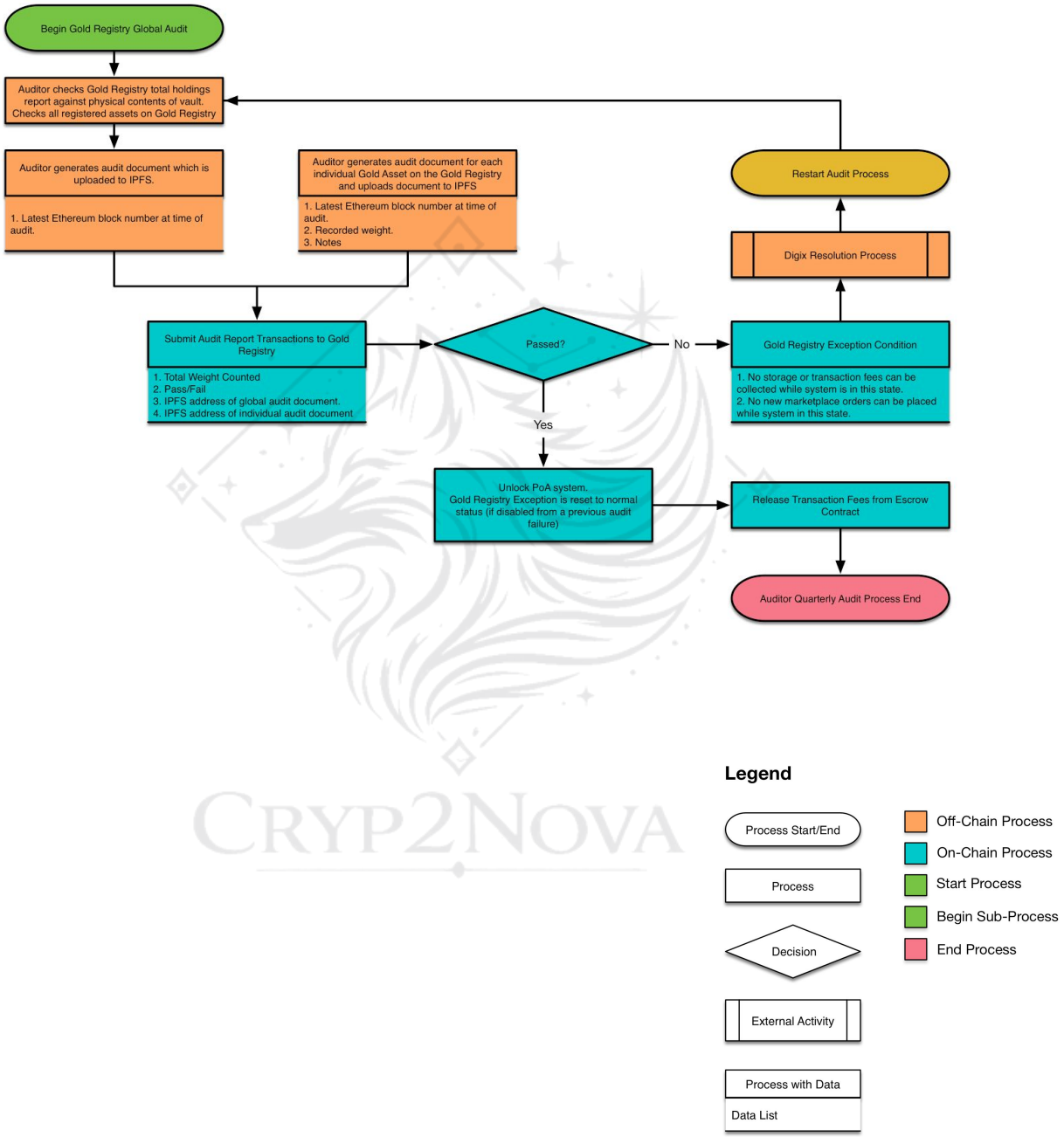
Figure i: Digix Asset Registration Process



Archived copy · cryp2nova.com

The PoA Verification contains a sub process for regular audits as shown in (Fig ii).

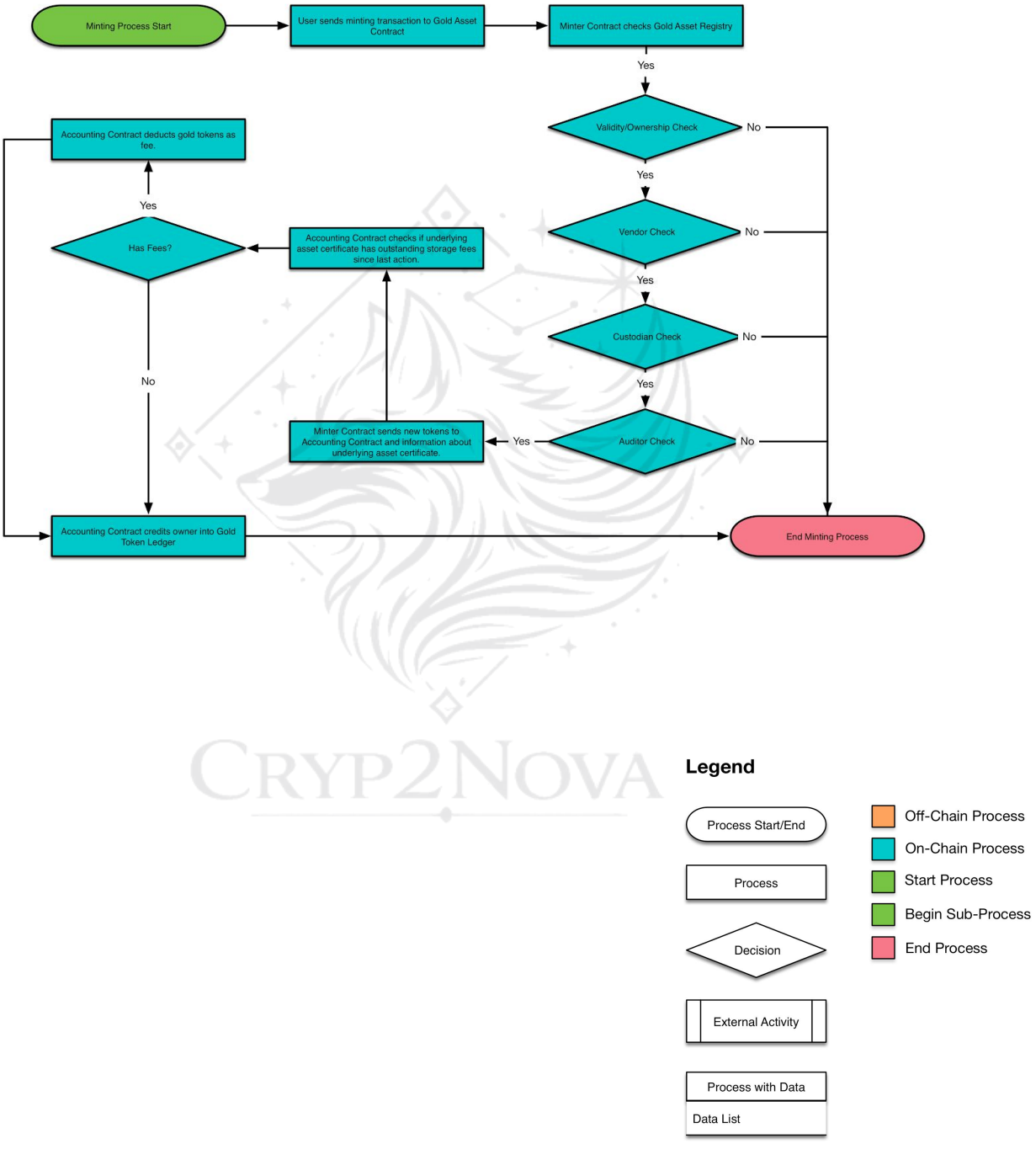
Figure ii: Audit Process



Archived copy · cryp2nova.com

2. **Minter Smart Contract** to create fungible DGX tokens, that accepts or holds PoA Asset Cards in exchange for DGX tokens (Fig iii).

Figure iii: Minting Digix Gold Asset Cards into Digix Gold Tokens

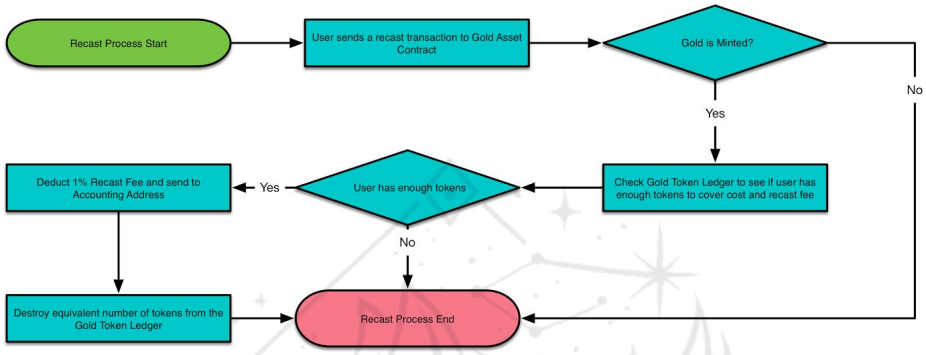


CRYP2NOVA

Archived copy · cryp2nova.com

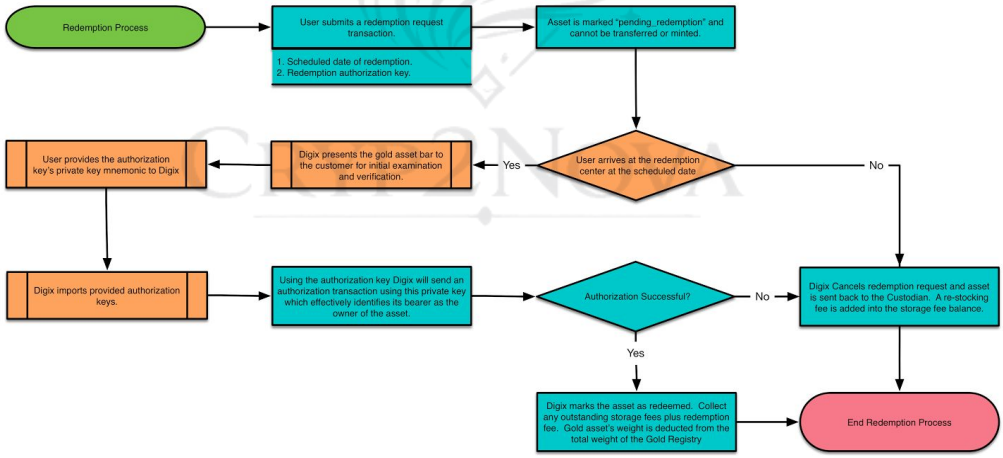
3. **Recaster Smart Contract**, which is used to exchange DGX tokens back into PoA Asset cards. (Fig iv).

Figure iv: Recasting Digix Gold Tokens into Digix Gold Asset Cards



4. **Redemption Process**, for redeeming physical gold bar with PoA Asset cards. (Fig V).

Figure V: Digix Gold Redemption and Token Based User Identification

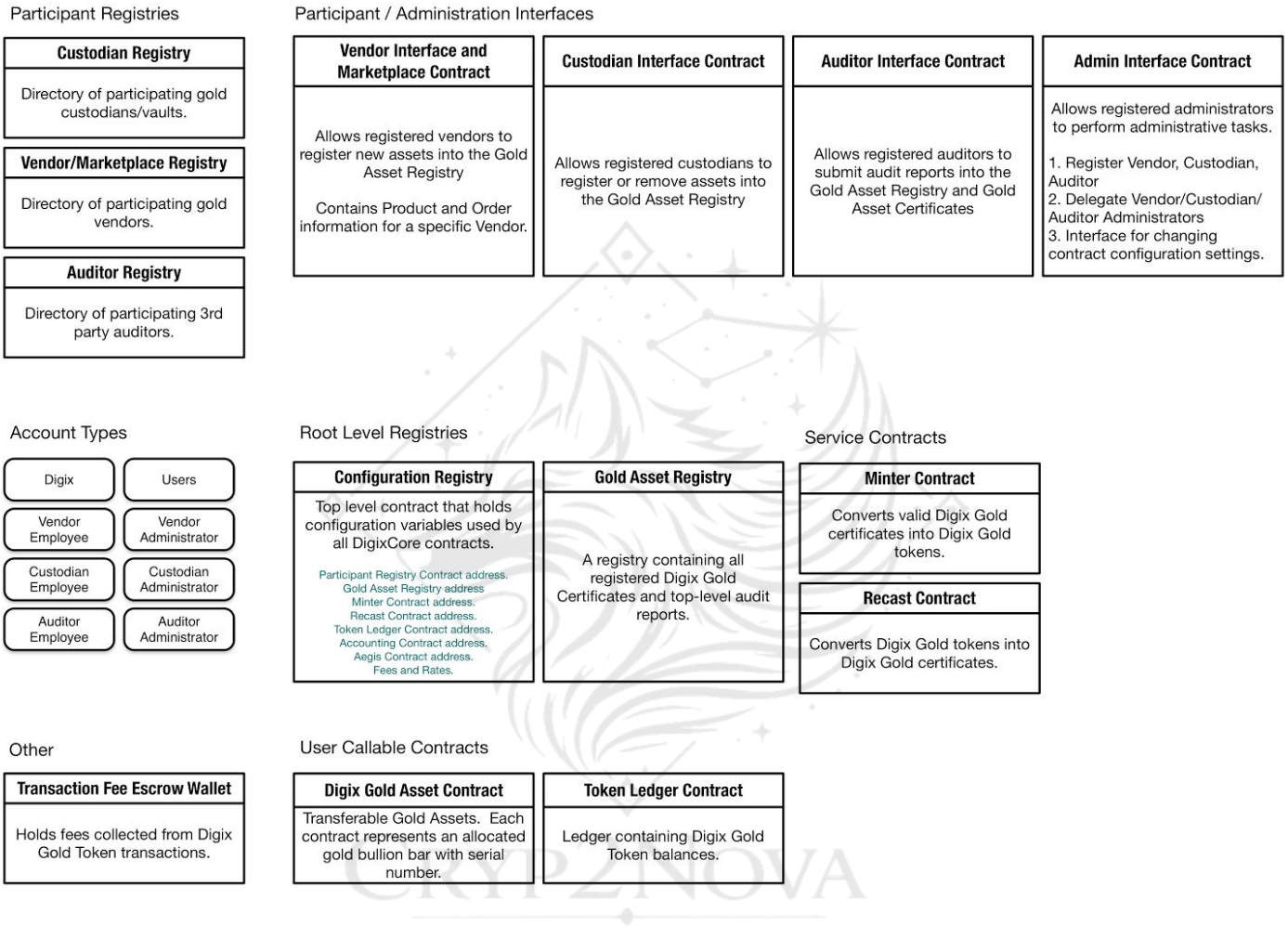


5. **Generic I/O Contracts,** allowing developers to utilize PoA Cards or DGX tokens for Đapp development.

Archived copy · cryp2nova.com

Ethereum Smart Contracts Stack

The diagram below shows the individual Digix smart contracts deployed on the Ethereum blockchain that make up the core processes above.



Archived copy · cryp2nova.com

Digix's Proof of Asset Participants
(Blockchain Oracle Entities)

Asset Vendor

ValueMax Singapore, a publicly listed company, supplies London Bullion Market Association (LBMA[3]) certified gold bullion bars through the Digix Marketplace. Established in 1988, they provide pawnbroking services, retail and trading of pre-owned jewellery, gold and luxury timepieces.

Independent Auditor

Bureau Veritas Inspectorate will carry out quarterly checks on the quality and quantity at our custodian vault to ensure accounting is upheld. They are a multinational group with capabilities in an extensive range of commodities, providing independent inspection, sampling and testing services of precious metals.

Every gold bullion is rigorously tested with precision instruments at Audit. We perform such measurements using Ultrasonic Gauge Measurements (UTM) and densometers. UTM is a method of performing non-destructive measurement (gauging) of the local thickness of a solid element basing on the time taken by the ultrasound wave to return to the surface. Densometers are devices that measure the density of objects with water displacement.

Participating Custodian Vault

Malca-Amit's state of the art facility near Singapore Changi International Airport is located in the Le Freeport of Singapore, a 25,000 sqm high-security and climate-controlled facility featuring cutting edge security technologies enhanced by green building engineering.

CRYP2NOVA

Multi-party Trust Mechanism

The Digix system relies on multiple independent participants to provide a transparent platform for the tokenization of physical assets. We can assume that miners in a Proof of Work based crypto-currency system will act rationally, that is, that they would act in a way to maximize and protect their long term profits by performing their role of transaction verification. We assume that a cartel of rational miners would not collude to perform double spending attacks as such attacks would cause reputational damage to the entire system. We must therefore assume that in the Digix system which is the tri-party system consisting of asset providing vendors, the asset custodian in charge of storing and securing the asset from theft, and the auditor in charge of

[3] "LBMA - FAQs". The London Bullion Market Association.

Archived copy · cryp2nova.com

ensuring the authenticity of the reported assets in custody are all acting in a rational manner who are trying to maximize their profits from the fees that they collect for their service.

Mitigating Potential Points of Failure with Real World Governance

Dishonest Entities and collusion in the chain of custody

Digix works with entities in jurisdictions that provide stringent regulatory oversight and corporate governance. The entities we have engaged with are either publicly listed or well known in the industry for providing their niche service. Each entity that we have engaged with performs a separate function to prevent cheating. For instance, the asset vendor for physical assets cannot also be the asset custodian. The interest in the service has to be independent of one another. While the risk of collusion is a real possibility, it is at the cost of severe reputational and legal damages to the colluding participants. As these entities provide similar other services to other customers and such reputational and legal damages to their core business would be detrimental to their business, we can make a fair assumption that they will act in a rational manner.

Key Benefits

No centralised database management of Crypto Asset records

All chain of custody information is fully managed by the Ethereum blockchain. This blockchain ledger is immutable with data upload taking significantly less time than on the Bitcoin blockchain.[4]

No Web-based log-in

There is no web form log-in. Users will download desktop clients from Digix. The application itself can also be compiled from source on Github and is publicly auditable.[5] There is significantly less chance of a Man in the Middle attack compared to traditional user web-based log-in.[5]

Secure Cold Storage of Crypto-Assets

Digix's Aegis Vaults is a cold storage wallet custodial service for crypto-assets and crypto currencies on Ethereum.

Perpetual Existence of Digital Assets

[4] CryptoBond. (September 16, 2015) Why Is Ethereum Different to Bitcoin. CryptoCompare
[5] Hjemlvik, Erik. (March 27, 2011) Network Security Blog. "Network Forensic Analysis of SSL MITM Attacks". NETRESEC

Archived copy · cryp2nova.com

All asset data is recorded on the blockchain and exists indefinitely. Even if Digix folds, every proof generated can be verified and are admissible in a court of law in the applicable jurisdiction.

Ex post facto Incentivization Mechanism

The Proof of Asset process requires that regular quarterly or more frequent audits to be performed by a 3rd party auditor on the entire collection of gold assets held at the custodian vaults. The auditor performs a complete audit of each gold bar which includes verification of its authenticity, weight, and physical examination to detect anomalies or defects. The auditor submits a record on the Gold Registry contract for each and every single bar that has been audited, which contains an IPFS reference to a signed paper documentation, the auditor's Ethereum identity, and a pass or fail result.

Digix receives its revenues through the collection of transaction fees paid in the form of Digix gold tokens. These tokens are held in an escrow contract which can only release the tokens to a specified address after the successful completion of a 3rd party audit.

Generic I/O Contracts and Đapp Development Opportunities

The generic I/O contract provided at Digix allows developers to utilize PoA Asset Cards or Digix tokens for Đapp development and event logging. Our vision is to create an ecosystem for developers to utilize DGX tokens as a framework for various Đapp developments. Code samples will be provided on our Github.

Wealth Inheritance

Dead man's switch can be built as a service to allow wealth to be passed on in the form of Crypto Assets to the mentioned Ethereum address under the Digix system.

Gamification

In legal jurisdictions, DGX tokens can be used like bitcoin to facilitate in game currency or as gaming tokens.[6] The PoA protocol can also be used for the issuance of digital gaming assets.[7]

Escrow

DGX tokens can provide a better and less volatile store of value for Escrow services on the blockchain.

---

[6] Farivar, Cyrus (January 22, 2013). "Bitcoin-based casino rakes in more than $500,000 profit in six months". Ars Technica.
[7] Addison, Ian. (December 22, 2015) "Game-changers FreeMyVunk and Digix allow video gamers ..." IB Times.

Archived copy · cryp2nova.com

Crowdfunding

A Đapp can provide crowdfunding opportunities with crypto-currencies and crypto-assets, or offer convertibility of cryptocurrencies to DGX tokens as a hedge to price volatility.

Gold Backed Crypto Currency Developments

Cryptocurrencies can stake a portion of its value with DGX Gold tokens and Gold Assets, backing its value with Gold.

Crypto Exchanges and Wealth Management Đapps

When exchanges integrate DGX tokens as a cryptocurrency pair, they will be able to offer a gold hedge to cryptocurrencies as part of their service offering. Wealth management services that adjusts your cryptocurrency / crypto asset holdings can be developed to manage an individual's crypto financial risk profile.

P2P Lending and Microfinance

Đapps can utilize DGX Gold for peer to peer lending. A borrower can call for funding through a Đapp based on his risk profile and reputation and negotiate a rate of return on the borrowed funds. Interest / yield payments can be serviced at regular intervals with a penalty system in place for late payments. This has already been done with bitcoin[8], but due to the price volatility of cryptocurrencies, lenders may lose more of their asset value than what can be earned from the interest during the period of the loan. The price stability of DGX Gold Tokens can facilitate the adoption rate of such services.

Collateral services

Privately held assets can be safely and efficiently used as collateral without going through lengthy verification process to ascertain an asset's existence and authenticity.

Conclusion

Digix will provide a transparent, audit friendly, safe protocol that leverages the full potential of Ethereum's decentralized consensus ecosystem and IPFS to facilitate crypto assets on the blockchain.

---

[8] Shieber, Jonathan (June 5, 2014). "BTCJam Brings Its Bitcoin-Based Lending Service To Emerging Markets". TechCrunch.

Archived copy · cryp2nova.com

Digix白皮书：密码学资产中的黄金标准

prepared by:

Anthony C. Eufemio <ace@dgx.io>

Kai C. Chng <kcchng@dgx.io>

Shaun Djie <shaundjie@dgx.io>

V1.02

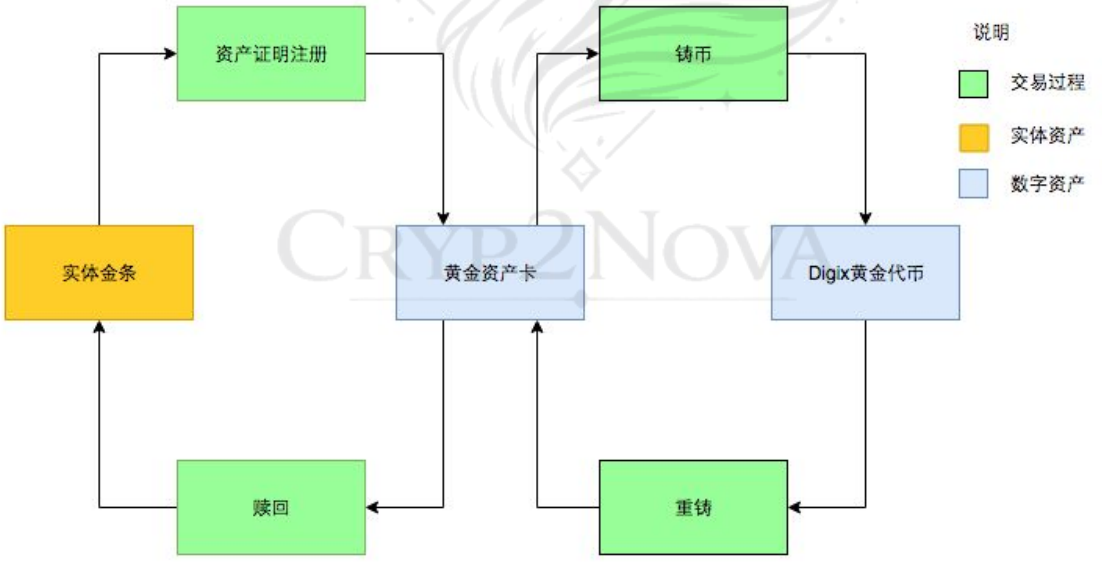
翻译：Ethfans--少平

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[9]和星际文件系统（IPFS）[10] 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:



[9] **[英文] 白皮书· ethereum/wiki Wiki · GitHub. " 2014. 29 Dec. 2015**

[10] B enet, Juan. (September 11 2015) " IPFS项目：它是如何运行的". IPFS

Archived copy · cryp2nova.com

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

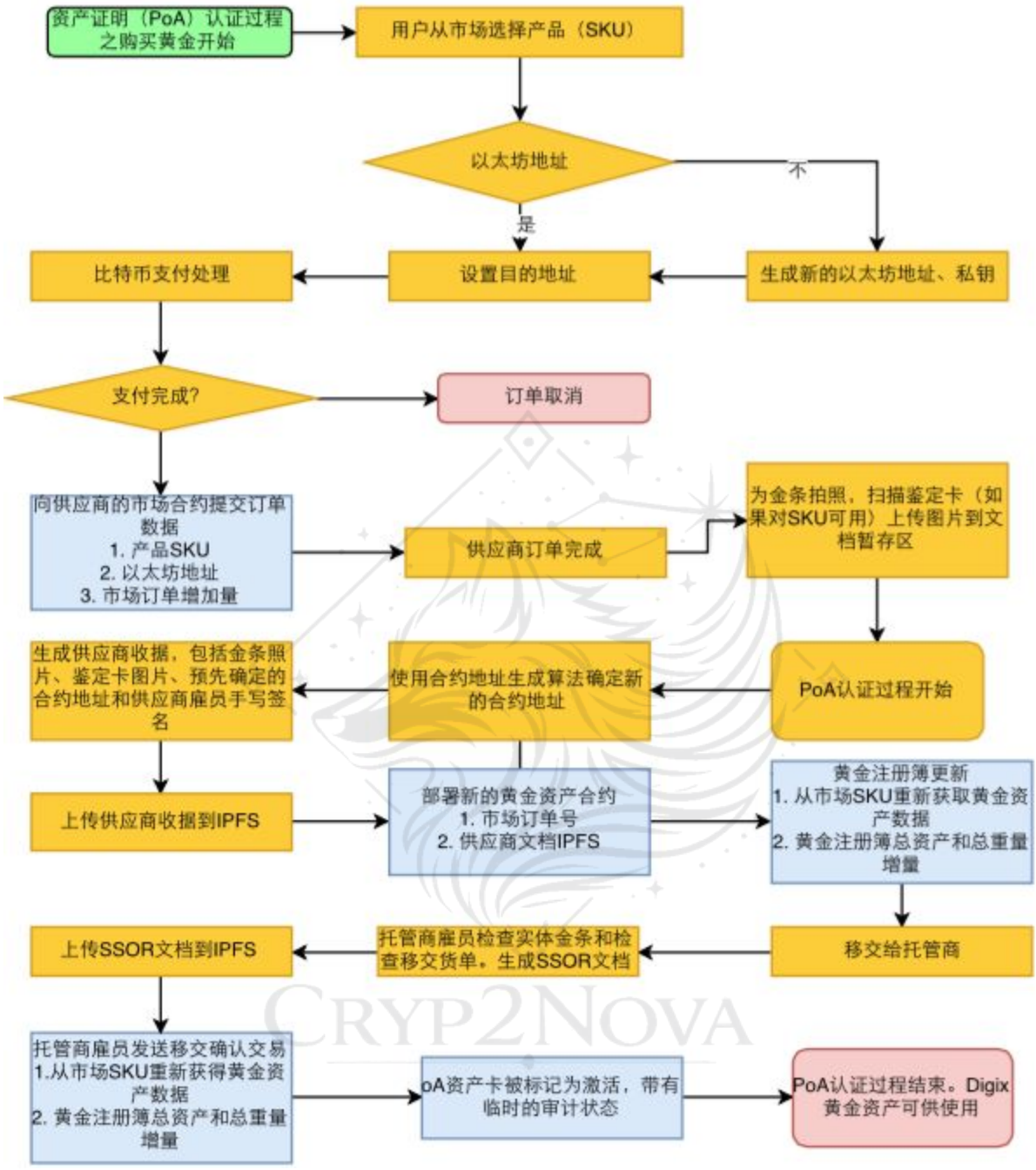
3个模块过程—Digix使用它为一项资产提供存在证明和可替代证明，1个实体资产赎回过程和1个鼓励去中心化应用（Dapp）开发过程。这些过程包括以下部分：

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

CRYP2NOVA

Archived copy · cryp2nova.com

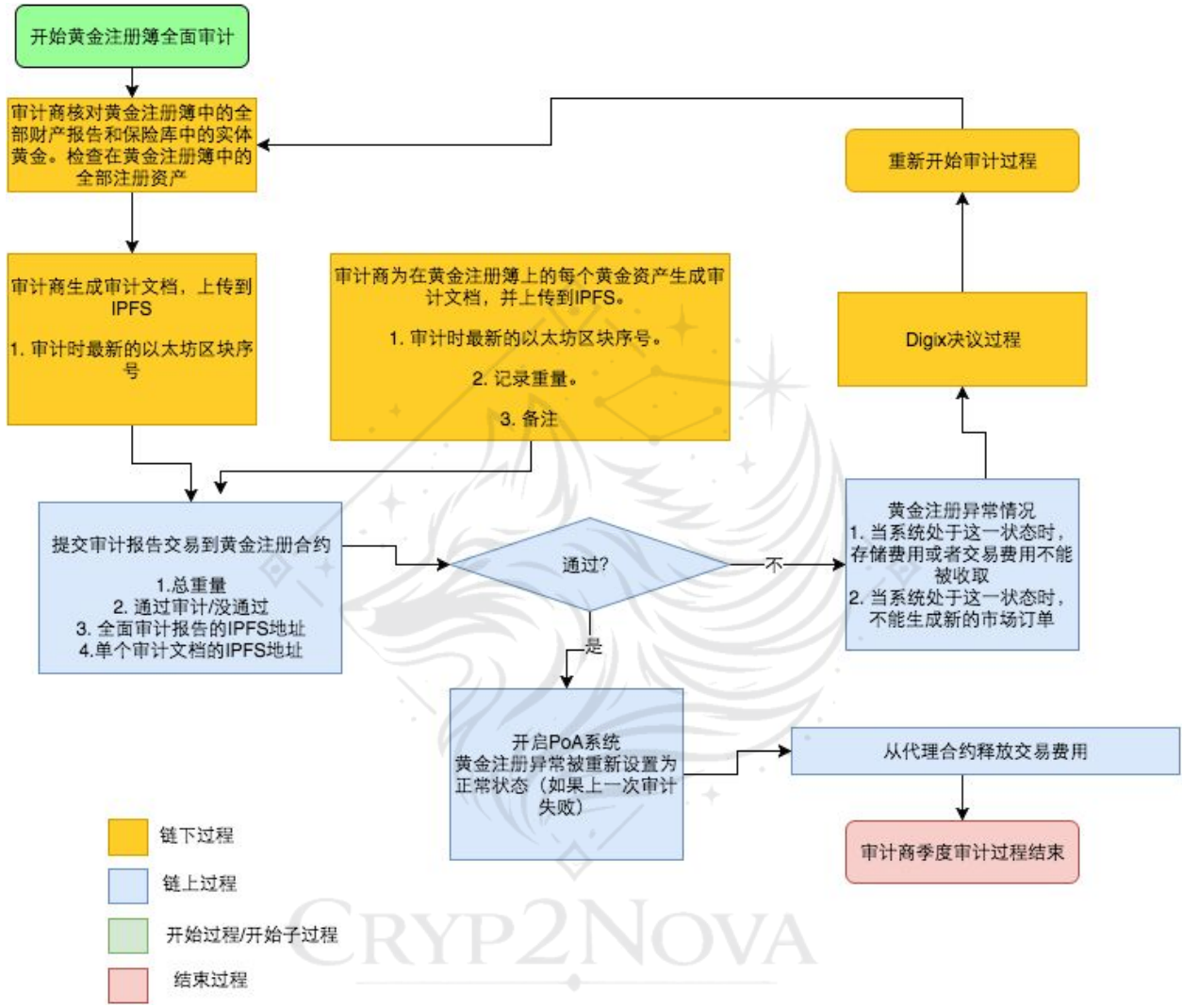


CRYP2NOVA

Archived copy · cryp2nova.com

PoA认证包括一个定期审计子过程，如图表ii所示。

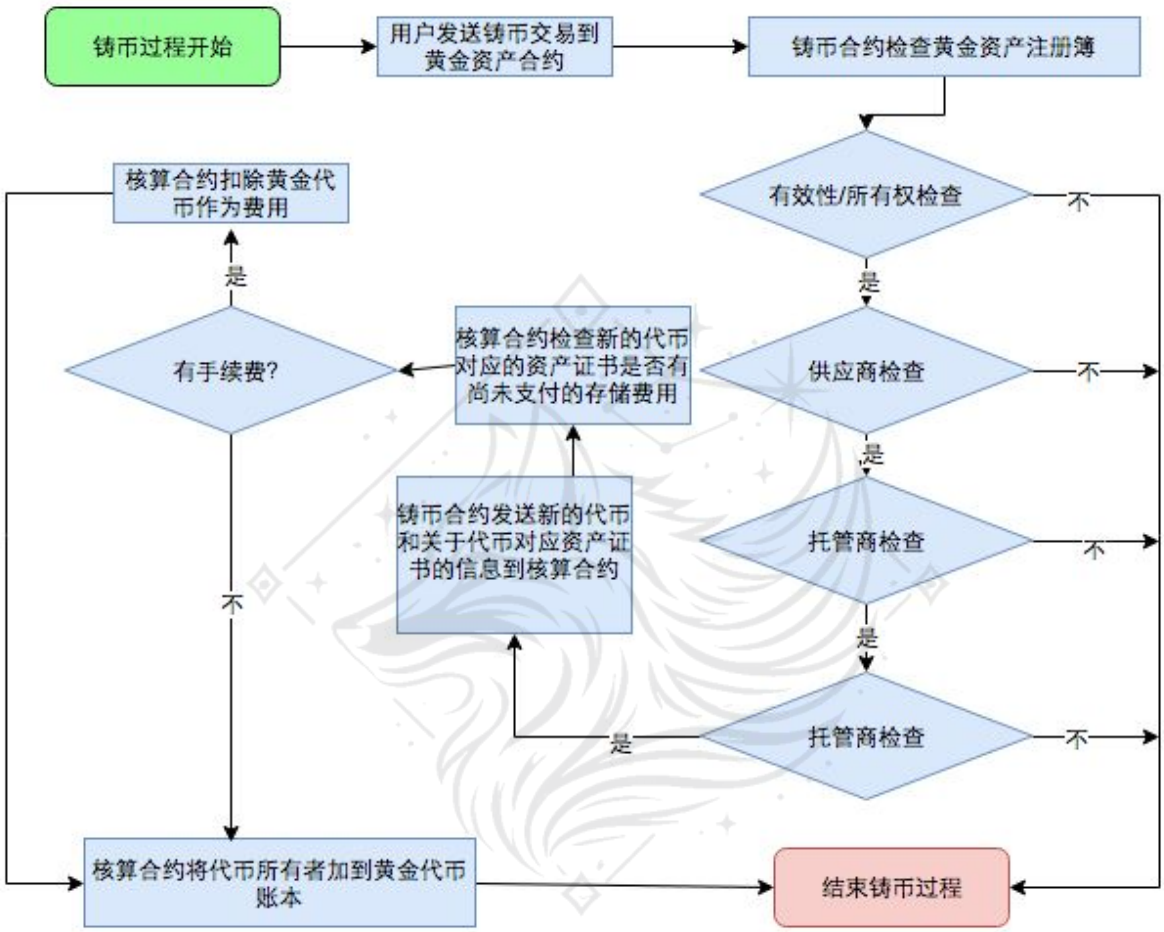
图表ii：审计过程



Archived copy · cryp2nova.com

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

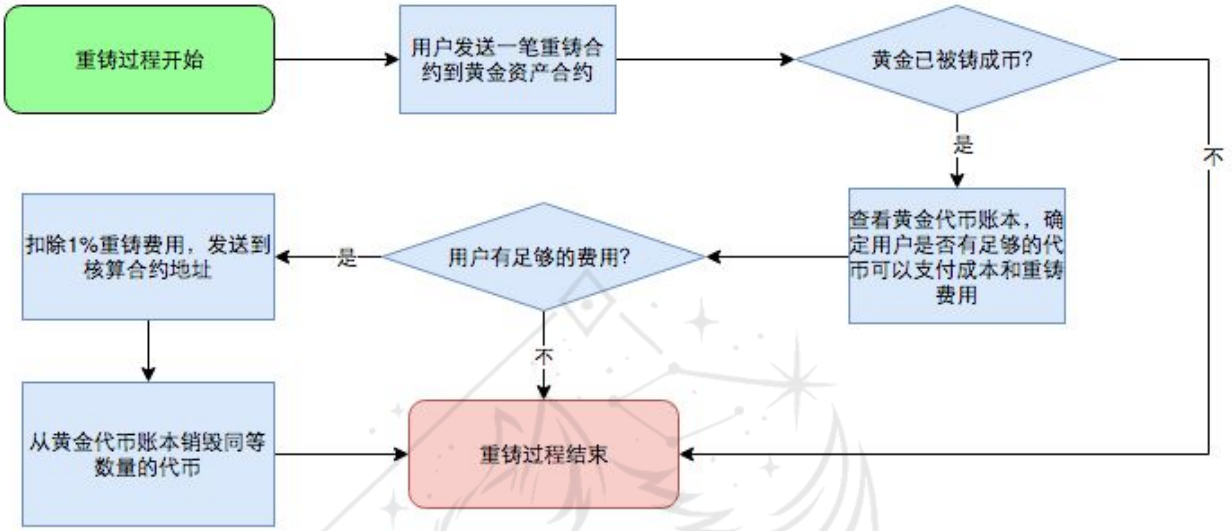


CRYP2NOVA

Archived copy · cryp2nova.com

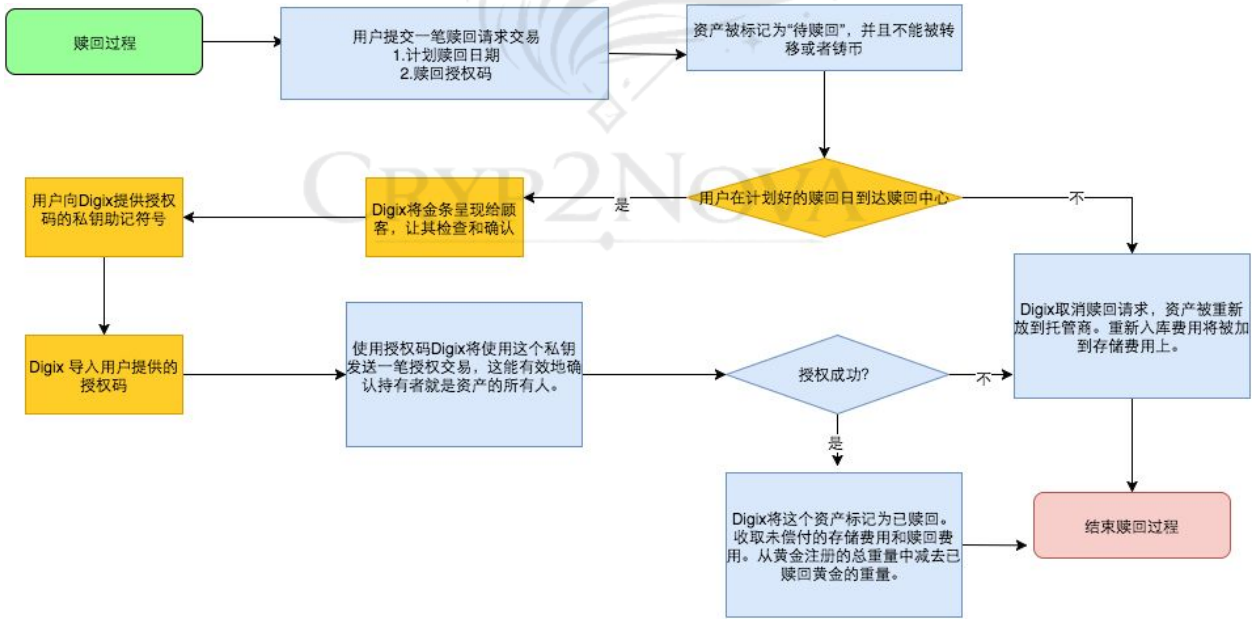
3 重铸智能合约，将DGX代币重铸为PoA资产卡。（图表iv）

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）

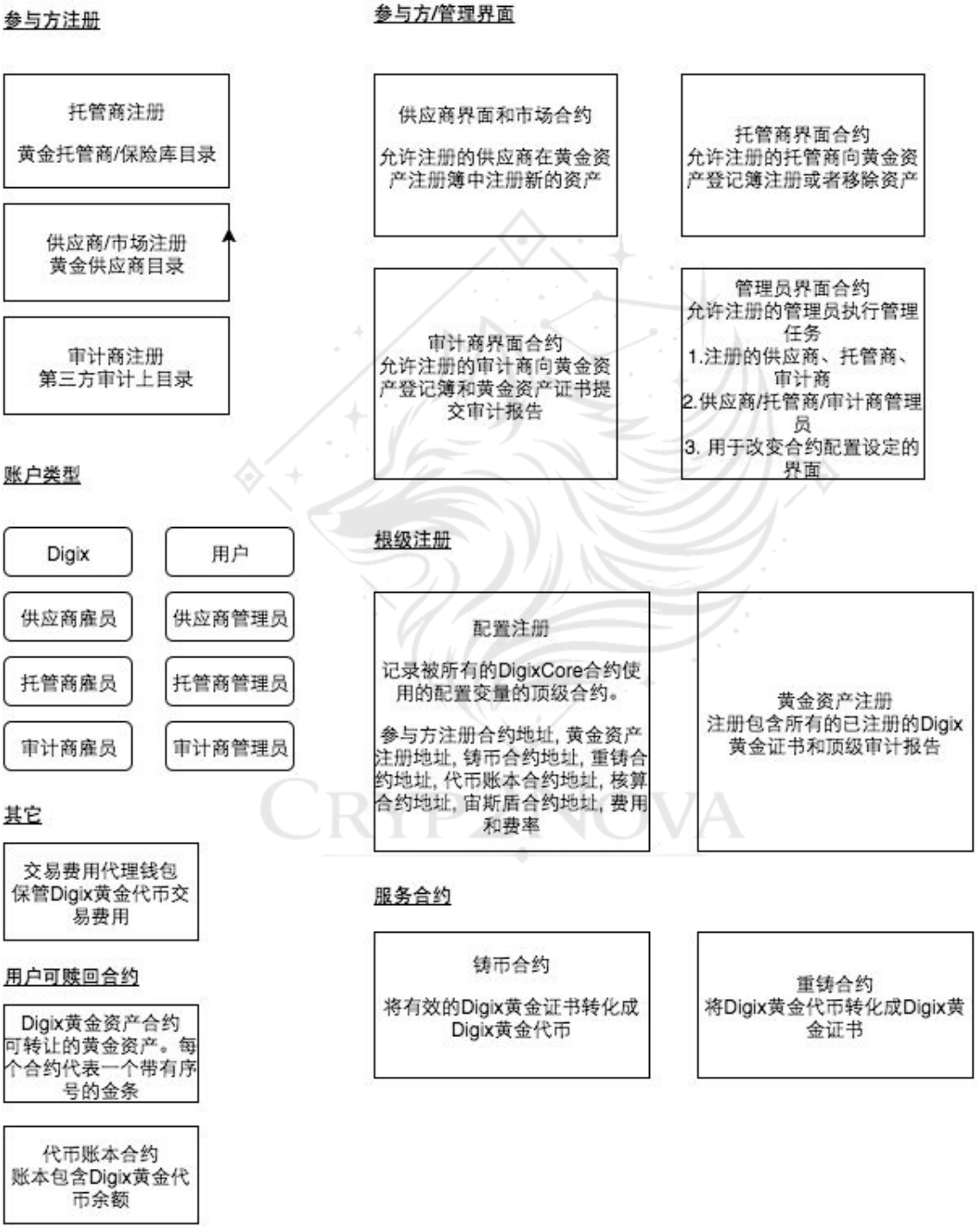
图表V：Digix黄金赎回和基于代币的用户身份证明



Archived copy · cryp2nova.com

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。



Archived copy · cryp2nova.com

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[11]）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

[11] **“ LBMA常见问题". l伦敦金银市场协会。**

Archived copy · cryp2nova.com

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[12]。

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[13]。

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

[12] **CryptoBond. (September 16, 2015)为什么以太坊不同于比特币？. CryptoCompare**

[13] **Hjemlvik, Erik. (March 27, 2011) 网络安全博客. "SSL MITM攻击的网络分析". NETRESEC**

Archived copy · cryp2nova.com

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[14]。PoA协议也可以被用于数字博彩资产的发行[15]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。

---

[14] **Farivar, Cyrus (January 22, 2013). " Bitcoinbased casino rakes in more than $500,000 profit in six months". Ars Technica.**

[15] **Addison, Ian. (December 22, 2015) " Gamechangers FreeMyVunk and Digix allow video gamers ..." I B Times.**

Archived copy · cryp2nova.com

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[16]，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。

[16] **Shieber, Jonathan (June 5, 2014). "BTCJam Brings Its BitcoinBased Lending Service To Emerging Markets". TechCrunch.**

Archived copy · cryp2nova.com