Matter Inc. 白皮书

rev 0.2

目录

目标

资产代币化是区块链社区的一个热门话题，对每种可能的资产进行代币化的进程中，目前还存在经济，技术，监管和认知的障碍。

最容易解释的是经济部分。 如果区块链是用于转移资产的情况下进行记账和执行既定的规则，则交易成本为每笔交易1美元（基于以太坊交易费用限制为50000单位的GAS，GAS价格是40 GWei/GAS和ETH/USD费率500美元/ETH）。 这对于小量大宗交易的资产来说并不是问题，尽管这类交易通常发生在已经拥有现有既定且管理良好的流程的高价值机构交易者之间。

为了大规模地提升资产代币化，我们应该有一个体面的计划，首先使用一整套底层基础设施和技术，以保证代币化过程的信任，并吸引更多传统资产持有者进场。 在接下来的部分中，我们将详细解释。

金融工具及其衍生工具的代币化

在Matter，我们认为传统金融工具和相关资金流的代币化进程是最高优先级别，并为传统世界和加密社区提供巨大的利益。 与其他白皮书相比，我们将尽可能简单地举例。

我们来看看大型贷款组合的代币化过程。 不同投资组合的股票被出售给少数（约10个）大型机构投资者，这些投资者获得固定利率，且很少有次级投资者承担更高的风险但获得浮动（且更高）的利息。

- 例如，每两周（时间间隔可能会有所不同）借款人都可以从最终借款人中获得付款。
- 付款的一部分涵盖贷款利息和贷款部分（本金额）。
- 在这里，我们将跳过关于委托人的部分，仅专注于股息，主要是为了阐述透明和简单。
- 股息（在一些投资组合相关费用之后）在瀑布机制过程中在投资者（主要和次级）之间分配。
- 首先，收集的股息总额在主要投资者之间分配以保证他们的固定收入。 付款按比例分配每个主要投资者。
- 如果股息金额大于支付所有固定收益所需的金额，那么剩余金额将在次级投资者之间**全额分配**，从而弥补其增加的风险，并有可能获得比初级投资者固定利率高得多的利息。
- 如果金额不足，主要投资者的利息应从现金储备或下次收取的付款中支付。 在这种情况下，次级投资者在此付款期间获得零利息。

虽然上述过程简化了，但它说明了未来可能呈现的资产代币化的**起源过程**，因为智能合约可以对投资组合中的原始股票进行记账，并进行必要的计算以符合上述的瀑布机制， 并且还介绍了投资组合的衍生产品 - 相当于加密版本的股息，即智能合约中有一个识别号码，另一方面付款是以法定货币表示和存储在银行帐户中。 在这里，我们看到两个应该详细介绍的独立案例。

智能资产的起源

在上面的示例中，第一步是以智能合约的形式创建等价物组合，其记账功能可以在现有的具有智能合约能力的区块链中有效执行（包含小量计算成本）。限制之一是这种区块链在每次交易的最大计算量（例如，在以太坊这样的限制等同于区块燃料限制），例如，如果股息计算过程比上面解释的更复杂，这样的计算量在智能合约中是没有可能的或者是无效的。 这些问题可以通过zkSNARKS/ZkSTARKs形式的现代密码术或相应章节中涉及的加密经济学方法来解决。 目前它足以说明两个问题：

- 对于某些资产创建智能合约可能是徒劳的，对相关业务功能的完全支持可能既昂贵又不可能。
- 资产代币化产生了衍生（兄弟）资产，这些资产对于市场和社区而言可以更加实用和有趣。

智能资产衍生品

上述贷款代币化的例子产生了非常有趣和实用的工具 - 一种与传统法币挂钩的加密资产。 从经济上看，由于其波动性低（由于挂钩）和流动性高（由于低波动性和微不足道的价格衍生规则），相当于看作一个长期的“稳定币”。 这些资产具有实际应用，并且对于加密社区而言有更大发展空间，因为它们在物理世界和加密世界之间架起了桥梁。 这种衍生资产的所有账本都可以在区块链上进行，而物理世界的参与者会更加愿意接受这种形式的支付，因为其波动性风险大大降低。

我们可以更进一步，通过引入现金流程（由法定货币背书，反过来涵盖该资产的全部发行价值）并使交易成本几乎不变，从而为这种衍生资产带来额外收益。第一部分需要相应的账户实名制/反洗钱机制流程。 后者通过Plasma协议来涵盖。

总而言之，创建一个流动性高的工具，主要是依靠基础经济学（宏观经济学和货币政策领域），在本节中，我们会给出一个简单的解释，阐述可以做什么以及代币化过程如何对多方面有益。

开放证书标准

在区块链与有价值的实体相互操作之时，它需要符合來自传统金融监管机构和实名制/反洗钱机制的所有要求。 在实践中，加密货币交易平台等公司根据其注册国家的法律调整程序。 我们通常认为这种做法是正确和合理的。 但是，我们应该强调，这种限制只应在传统资产和加密资产之间，而加密货币和代币资产本身的交易应该不受限制。 而近期的个人数据泄漏事件已经证实了以下两点需要得到保证：

- 处置个人数据的权利应属于个人数据的所有者，并且仅属于他们。
- 访问个人数据的权利只应授予个人数据所有者授权的服务。

我们的目标是从密码学和数据结构领域引入最佳案例，以改进现有的解决方案。 与其他项目类似，我们希望确保颁发证书（“证书”）应由已被授权的，在现实世界中进行了实名制的程序里进行。 我们将提供格式和描述如何使用区块链上的证书，及其数字快照和智能合约进行储存。 我们认为区块链技术是适用和必要的，原因如下：

- 首先，权利应该由算法而不是特殊个体来授予。
- 用户数据的数字快照可以存储在不可更改的公共存储空间 - 区块链中。 这可以避免审查和欺诈。 任何侵犯隐私的行为都可以被公开。 访问服务和管理个人数据的权利将由算法授予。
- 由数据持有人决定哪些数据可以公开。
- 借助零知识证明，可以在不知道完整用户身份的情况下授予访问权限，并且只能通过用户访问级别的来授予访问权限。 例如，当客户达到足够的资金，我们即可提供服务而无需要要求客户提供准确的资金数字。
- 如果怀疑未经授权访问其证书，证书所有者可以自行撤销证书，而无需随时请求任何特定服务。
- 重现攻击保护在当下是必要的。

我们的解决方案为用户提供选择存储数据的位置 - 他/她可以选择将数据存储在他/她自己的位置，或者通过他/她的意愿将其委托给某人。 通常，对于所有相关方，可以改善处理个人数据的用户体验。

由于实名制是智能合约的关键部分，我们可以将其与Plasma实现紧密集成。 一个例子是基于实名制的白名单过程，用于将资金从Plasma网络提取到父区块链，用于任何其他目的，例如转账或现金支付。 这种逻辑类似于在集中式交换机上进行密码对交易。

建立实名制标准对我们来说是否在经济上有利可图是超出了本文的范围。 尽管如此，它仍然是我们的系统和代币化生态系统中不可或缺的一部分。

Plasma协议实现

Plasma协议最初由Vitalik Buterin和Joseph Poon于2017年8月提出。最新的论文可以在相应的网页（https://plasma.io）上找到。

Plasma协议引入了一个想法，并定义了必要的部分，以允许信任转移，并允许中心化一方以可验证的方式生成区块。 有多种方法可以构建特定的协议案例（有时称为Minimal Viable Plasma，Plasma Cash，More Viable Plasma，Plasma Debit，Plasma XT等），并且很明显可以实现每秒10k+转账速度。 如此巨大的交易速度和集中程度允许每笔交易的成本低于1美分，这完接近加密社区（可转换资产转移）和资产（转移不可替代资产）转移的需要。 人们应该明白，在目前阶段，Plasma不可能实现智能合约，但是它的可验证性使我们推测到，如果结合智能合约功能，将会有很多有趣的用途。
为了进一步解释，我们应该提到Plasma协议的两个基石：

- 可验证性：若中心化操作员以生成了无效区块，没有生产块权限的外部访客不能够给予惩罚。 如果操作员允许零碎的双重花费 - >外部访客应该能够通过提供必要的证据来惩罚操作员。 出于此目的，智能合约需要自动解决此类争议并且需要来自运营商的某种形式的保证金。

- 活力：总要有人监控链上的拜占庭行为。 它可以是监控整个链的大型外部用户（记住，每秒10k个转账）或小用户监控他/她自己的转账以及链的一个小的随机部分。

总而言之，除了协议级别的正确性之外，特定的实现应该提供一些激励机制来吸引大型参与者和小型用户让其参与链上的监控。 对这种机制的讨论超出了这项工作的范围，最简单的是Plasma与其母区块链（智能合约所在的位置）之间的交易的流动性提供机制。

协议的实施将为代币资产交易提供经济上有效的机制，更重要的是，转移衍生资产。 在我们的提案中，特定的Plasma功能不仅会带来低交易成本，还会提供以下各节中描述的机制。

去中心化交易所

Plasma一个明显可行的方案是用其构建去中心交易所。 使用Plasma协议去中心化交易将需要一些权衡，至少在初始阶段。 区块链中的每笔交易都需要所有者的签名（明确同意交易），同时应该存在一个简单而有效的证明，即交易是正确的还是不正确（在后一种情况下惩罚经营者）。 不幸的是，为传统交易所使用的匹配机制提供这样一个有效的证名并不是琐碎的，用户必须明确同意交易的数量和价格（或留下以先到先得的方式填写的报价）。 尽管如此，这种机制已经被以太坊网络中的去中心化交易所使用，每一笔交易的降价将吸引更多用户使用这种解决方案。

与监督智能合约相结合

任何Plasma功能实现都需要复杂的智能合约才能确保正确性和争议能自动化解决。 人们可以对这种智能合约带来额外的限制，例如仅限于某些用户群限制对特定资产交易的访问。 虽然下面将讨论这种机制的必要性，但首先我们应该举例说明如何实施：

- 有观察员监控Plasma网络。
- 每个以太坊地址都有一个带访问注册表的智能合约（为了便于解释，我们使用以太坊网络作为Plasma实现的父链）和相应的权限。 这可以被视为某种形式的自愿实名制。
- 如果中心化的Plasma操作者在当时在受限制资产上添加交易，而该资产用户并没提供权限，则观察者可以发送证明此事实的转账，并且智能合约将自动从该交易中扣除保证金，并终止Plasma链。

Plasma实施理念是基于善意和用户的完全自由。 任何没有与物理世界等同且不能轻易兑现的资产（在没有某种形式的白名单 / 反洗钱程序下）都可以在Plasma网络中无限制地转移，从而允许加密社区中的用户自由地进行交易并且收费较低。 另一方面，任何可以轻易转换为法定货币的资产只能由自愿接受白名单的用户进行交易。 虽然这种要求可以被视为一种限制，但我们认为这是防止洗钱和非法交易的解决方案。
这种限制的一个明显好处是吸引了大型传统机构参与者和监管机构的注意力。 任何这样的实体都可以成为一个完整的链观察者，并确保其他用户的正确性和链的有效性和活力。 如果在某个时刻，一个完全挂钩的象征化资产衍生品将出现在市场中并具有高流动性并将用于日常支付手段，它还将弥合与实物世界的差距。

Plasma的进一步改进

如上所述，有多种方法可以构建Plasma协议，以及用户可以访问哪些功能。 在这里提到：一个是短期的，一个是长期的开发构想：

- 在短期内，可以在Plasma中实施“机密交易”。 此功能指的是协议的实现，其中用户可以隐藏确切的交易金额，但仍然通过证明没有凭空创造的价值来证明交易的正确性。 对于这样的功能有不同的的方法，例如在Monero和zCash区块链中，我们认为它应该基于Greg Maxwell的原始“机密事务”协议。 人们应该明白，这样的功能可以在以太坊网络中实现，例如，虽然交易价格变得非常大（每次交易需要几百万的GAS。正常交易需要21000个GAS）。

- 从长远来看，人们可以尝试使用现代密码学的优点，例如ZkSNARKs / zKSTARKs来证明块的完整有效性，并减少用户的链监控负担。 虽然它目前还在实验阶段，但进一步研究是实现这一最终目标所必需的。 有关zkSNARKs / zKSTARK的简要说明，请参阅相应章节。

加密货币经济

在本节中，我们将尝试解释什么是加密经济学以及它如何在思维模型中进行某种范式转换。

当智能合约在区块链中执行时（指以太坊网络），我们会尝试将传统的交易逻辑转移到智能合约上。 最好的例子之一是ERC20令牌标准，它定义了一些任意命名的可替换资产的分类账。 但这存在可能甚至很高的计算成本（高于每个事件的最大限制）。 要在区块链中实现这样的过程，可以切换到可证明（并且可高效验证）的计算的方法，其中任何用户可以证明某些输入和输出数据之间的正确关系并且在有效的空间和计算成本中进行（远低于计算费用本身），或者可以引入加密经济步骤流程。
在加密经济步骤流程中，用户不需要证明某些输入和输出数据的正确性，他们只需声明数据是正确的，并为透过交互式或非交互式的程序来完成验证。 人们应该明白，并非每个流程都可以转换为加密经济案例，尽管对所有用户都是有益的。 这是一个简单的例子：

- Alice希望对Bob进行交易兴趣，其中输入数据是I，输出数据的权益是O
- 这里会出现交互式或非交互式流程，允许用户肯定地证明输出数据O是输入数据I的正确值。
- Alice在本地（在家用电脑或手机设备上）从I计算O并将事件发送到智能合约，其中声明了以下内容：
    - Alice有输入数据I的计算结果
    - Alice计算了输出数据O
    - Alice声明O是I的有效输出
    - Alice愿意通过某些抵押X支持她的声明
    - X的值高于上述证明程序的成本
    - X立即转入合同，并且可以在Y小时内由Alice兑换

- 在Y小时期间，任何观察者（Bob）都可以验证O是I的有效输出，如果发现存在差异，他/她可以与Alice进行争议程序，如果证明存在差异，则Bob取得X，并且Alice的交易被视为无效。

为了确保加密性的有效性，网络中需要高度“活跃”，尽可能多的监控终端，因为许多交易都可能引发争议。

这是Matter令牌发挥作用的时候。 如果使用Matter代币支付抵押品，我们可以引入额外的限制。

- 如果用户Bob成功地对Alice的交易提出异议，他会像往常一样收到抵押品
- 即使没人监控网络，Matter也有责任对无效交易提出异议
- 如果没人在允许的时间段内（包括我们）对Alice的交易提出异议，并且在稍后的某个时间点，Alice的交易仍然被证明是无效的，那么这个事件的证明者将从Matter那里扣除保证金，这被视为特殊情况

通过承担额外的负担，我们试图通过经济机制为网络带来活力。 为了避免作弊，“我们自己证明我们错过了一笔交易”并收回保证金，只有一半会被支付给证明人，而另一半则被摧毁。

Matter代币的直接应用

我们生态系统中，任何产品都应该无差别对待，但我们建议对某些应用执行以下流程：

- 在Plasma中使用令牌转账作为付费的平均值。 如果其中涉及大量资产，价格有大波动性的，要么我们必须实施复杂的监控系统，根据转账原生面额（例如，一些ERC20令牌）提供适当的费用，或者使用我们的代币作为费用。
- 颁发实名证书需要在一个（或多个）中与提供商进行交互，管辖过程和付款可以通过不同方式支付。
- 如果某些衍生资产触发了现金支付程序，则需要支付一定的佣金应以Matter Inc.代币或资产的原始面额支付。

零知识证明算法 zkSNARKs / zKSTARKS简要概述

人们已经熟悉zkSNARKs以及zCash区块链用于匿名交易的实际用途。 虽然它是零知识非交互式证明，但可以尝试用以下形式的陈述来解释它（而Alice和Bob又来了）：

- Alice想要证明她已经正确地做了一些计算
- Alice想以极高的概率说服Bob（天文学上接近1）
- 虽然Alice所做的计算量可能很大，但她只提供了计算过程中的少量结果（全套通常称为“见证”，而Alice只公开一些“公共”参数）
- Alice和Bob同意计算的性质（直到最后的标志！）
- 为了实现她的目标，Alice提供基于zkSNARK协议的证明
- 作为奖励，Bob没有学到任何关于她的计算的任何中间结果。 它对我们的目的来说并不重要，但在某些情况下可以派上用场
- Alice的证明大小始终是恒定的并且事先已知，并且验证成本始终是恒定的并且事先已知

正如人们可以看到zkSNARKs的有效利用，主要是验证了最后一段信息是恒定的大小和恒定的验证成本。 这种程序可以代替加密经济学用于交易期间的一些复杂计算的方法，代价是高得多的证明准备成本而不仅仅是从相应的输入I计算输出O。它甚至可以在交易期间与加密经济学混合使用，当时未经证明，但可以为日后解决争议时作为记录！

结论

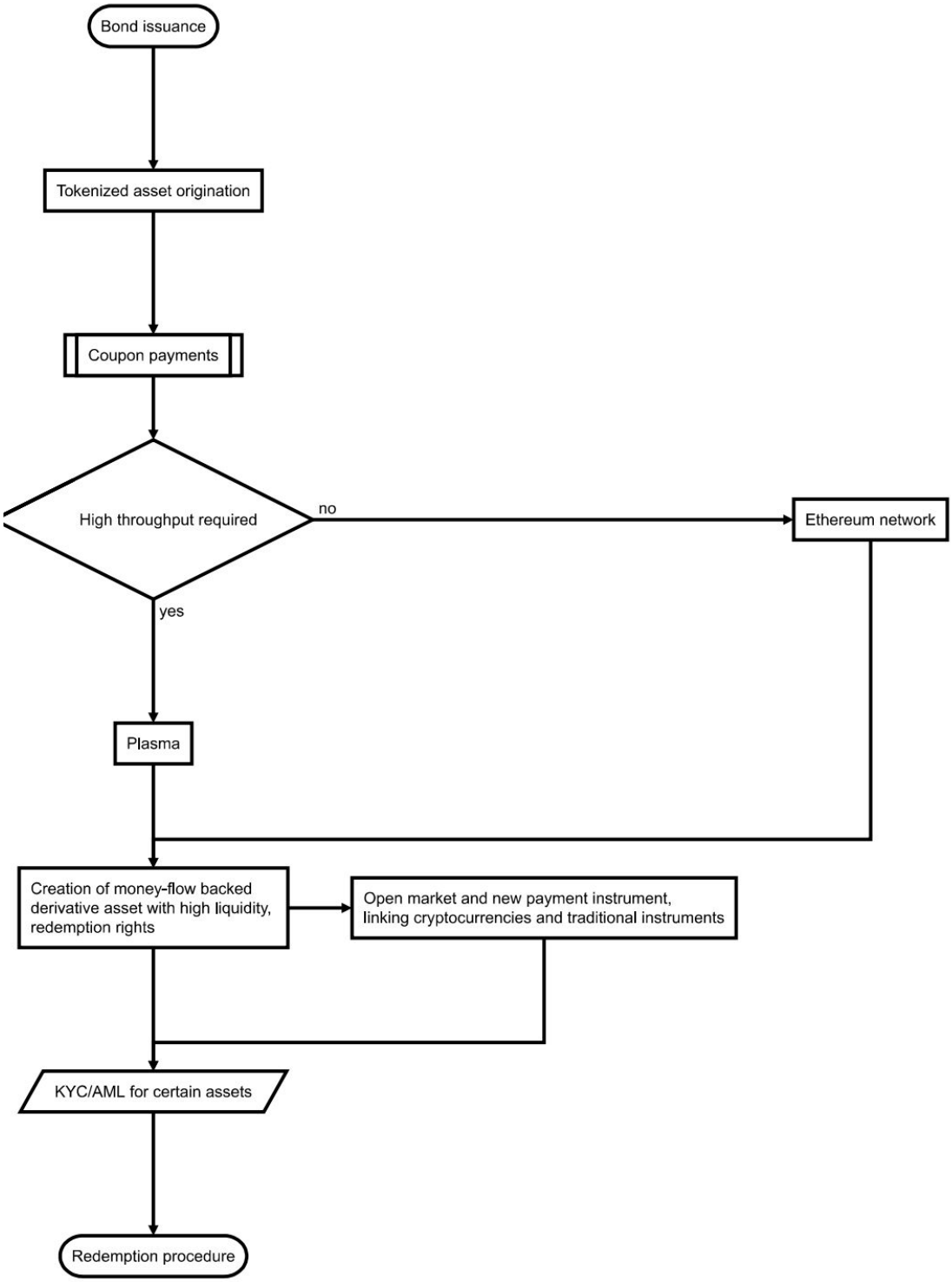
长文短结论，我们不是号召大家“购买我们的代币”，而是希望尽可能解释我们的目标。

Matter主要是一个工程师团队，我们相信系统（包括加密经济！）应该是自洽的，经济上合理的，实用的并且具有很好的用户体验。虽然许多公司试图参与资产代币化或快速进入区块链的世界，但我们倾向更加谦虚并尝试构建一个系统，其中具有巨大吞吐量的Plasma可以辅佐许多实际的事务。我们想先将某类型资产代币化。这类型资产将为代币化过程带来案例和信任，并且（我们希望它）通过适当的现金流出机制，产生具有透明定价，高流动性和与真实世界的明显联系的新一代“稳定币”。为了做到这一点，我们在这篇简短（不是300页）的白皮书中向您介绍了我们的想法，试图使所有这些解释尽可能简单和琐碎，并且从实践方面也有Plasma实施和投资组合试点的经验代币化 - 否则我们永远无法快速向您解释。

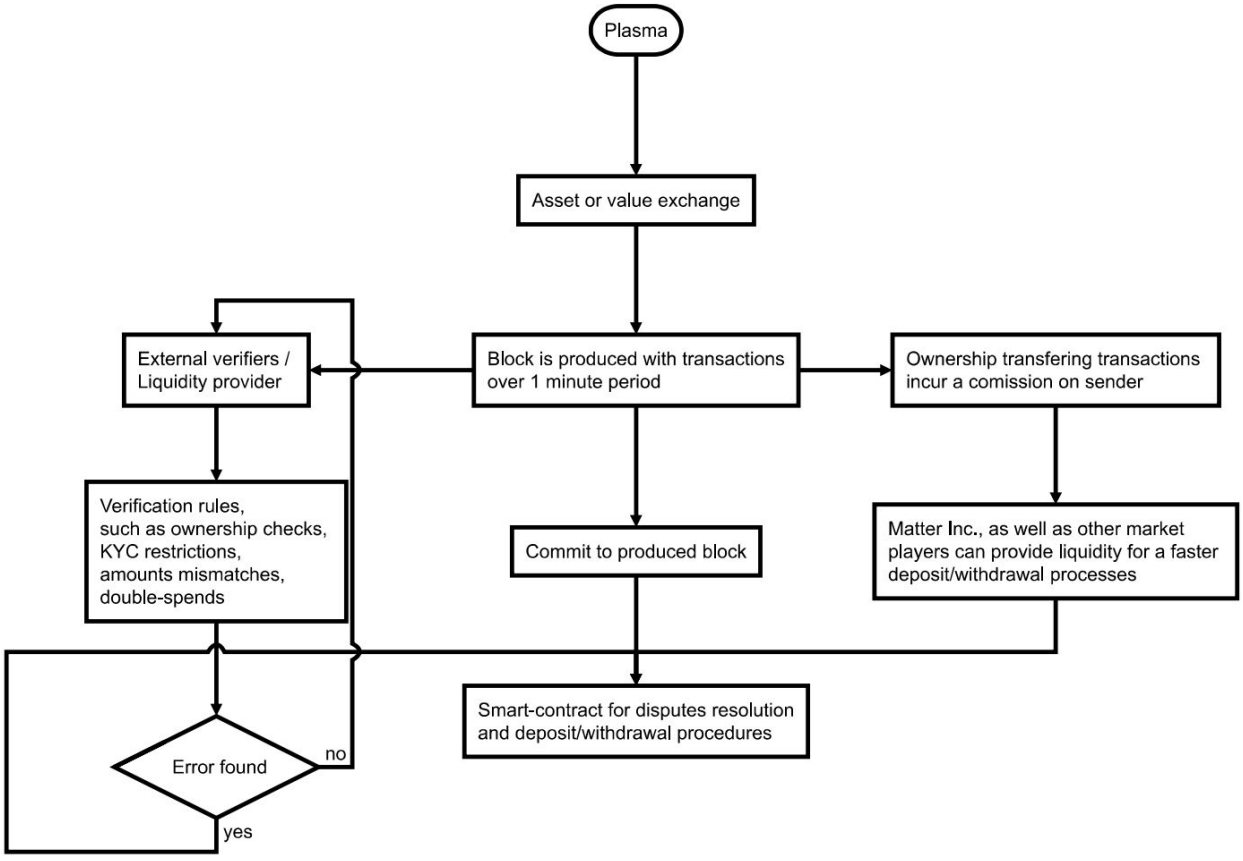
无名氏

附录

建议的债券代币化流程图的示例



Plasma实施结构


Plasma
Asset or value exchange
External verifiers / Liquidity provider
Block is produced with transactions over 1 minute period
Ownership transfering transactions incur a comission on sender
Verification rules, such as ownership checks, KYC restrictions, amounts mismatches, double-spends
Commit to produced block
Matter Inc., as well as other market players can provide liquidity for a faster deposit/withdrawal processes
Smart-contract for disputes resolution and deposit/withdrawal procedures
Error found
no
yes