Radiant:一个点对点数字资产系统

2022年8月11日
radiantblockchain.org

抽象。Radiant network是一个点对点的数字资产系统，能够实现直接的价值交换，而无需通过一个中心方。最初的比特币[1]协议提供了创建点对点电子现金系统所需的内容，但缺乏验证交易历史的能力，因此不能用于验证数字资产。数字签名和输出限制提供了部分解决方案，但是如果仍然需要可信的第三方来验证数字资产，那么主要的好处就失去了。与比特币类似，辐射式网络需要最小的结构，并将交易的时间戳添加到一个持续的基于哈希的工作证明链中。我们介绍了两种验证数字资产的技术:唯一引用和通用归纳证明系统，它们都在恒定的O(1)时间和空间中运行。可以以任何方式组合输出，而不会损害基于未用完事务输出(UTXO)的架构的固有并行性和性能特征。因此，用户可以随意离开和重新加入Radiant网络，并确保其数字资产的完整性和真实性。

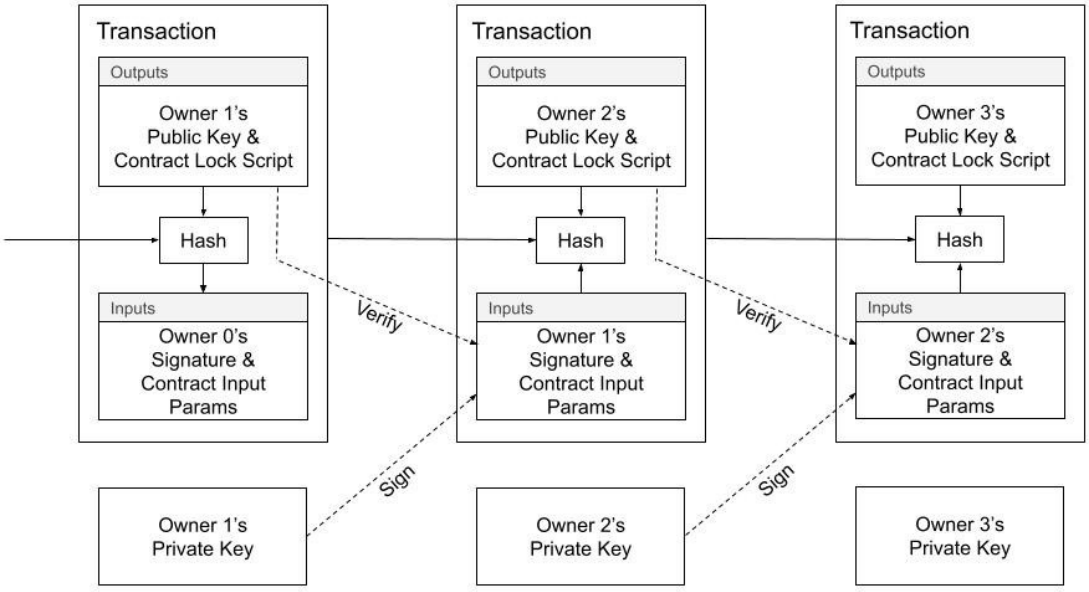
1.介绍

与区块链或数字账本技术(DLT)的商务在许多情况下依赖于作为可信方的发行者和保管者来认证数字资产。虽然这些系统对于类似电子支付的交易来说足够好，但是它们仍然受到高级用途的基于信任的模型的固有弱点的困扰。基于以太坊虚拟机(EVM) [2]的区块链对于各种程序都非常灵活，但是高昂的费用使得微支付应用不切实际。

需要一种可用于数字资产管理系统的低费用、高性能和高级编程能力的电子支付系统。在本文中，我们提出了一个解决区块链缩放和收缩问题的方法，该方法使用了两个新的技术，这两个技术提供了唯一的引用和一个通用的归纳证明系统，这使得跨事务边界的图灵完成[3]程序成为可能。提议的系统是分散的，使用类似比特币的工作验证共识机制，但吞吐量水平明显更高，同时提供与 EVM 区块链相同的灵活性，费用非常低。

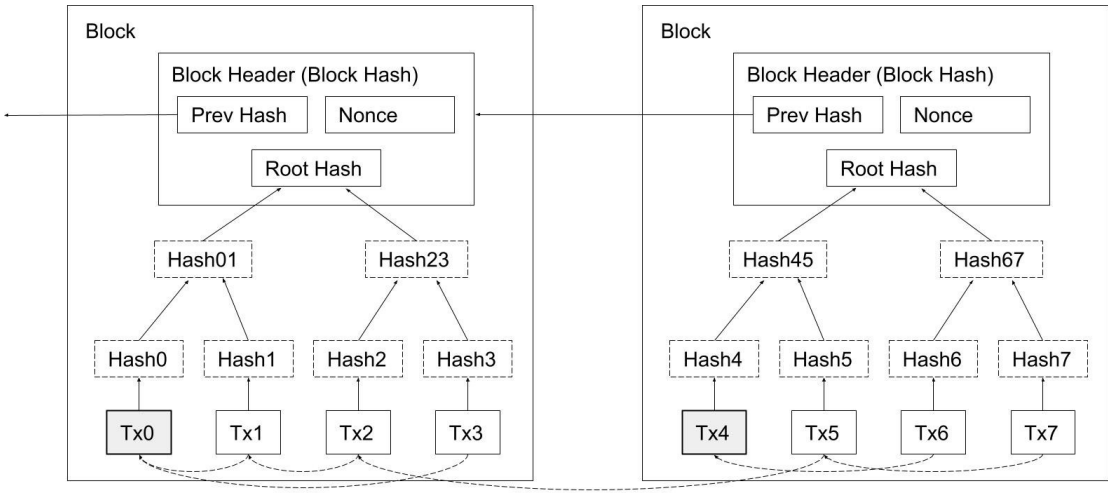
2. 处理

类似于比特币，我们把一个电子币定义为一串数字签名。Radiant 中的交易不同之处在于，除了解锁硬币所需的输入参数之外，每个所有者还通过对前一交易的散列进行数字签名来将硬币转移给下一个所有者。除了用户定义的任何其他规则之外，事务还创建新的输出锁定约束，其可以包括下一个所有者的公钥。



图表 1。光彩夺目的交易。

为了验证没有发生重复花费，我们使用分布式时间戳服务器，使用基于哈希的工作证明系统来组织规范的历史，以确定哪个事务最先到达。事务被组织成块。按照惯例，块中的第一个交易称为“coinbase 交易”，是一个特殊的交易，它启动块的创建者拥有的新硬币。块被链接在一起，并将事务组织成一棵 Merkle 树[4]。除了第一个交易之外，所有交易都必须参考形成有向非循环图(DAG)的前一个交易，其中所有硬币最终都连接回一个区块开始处的至少一个特殊交易。



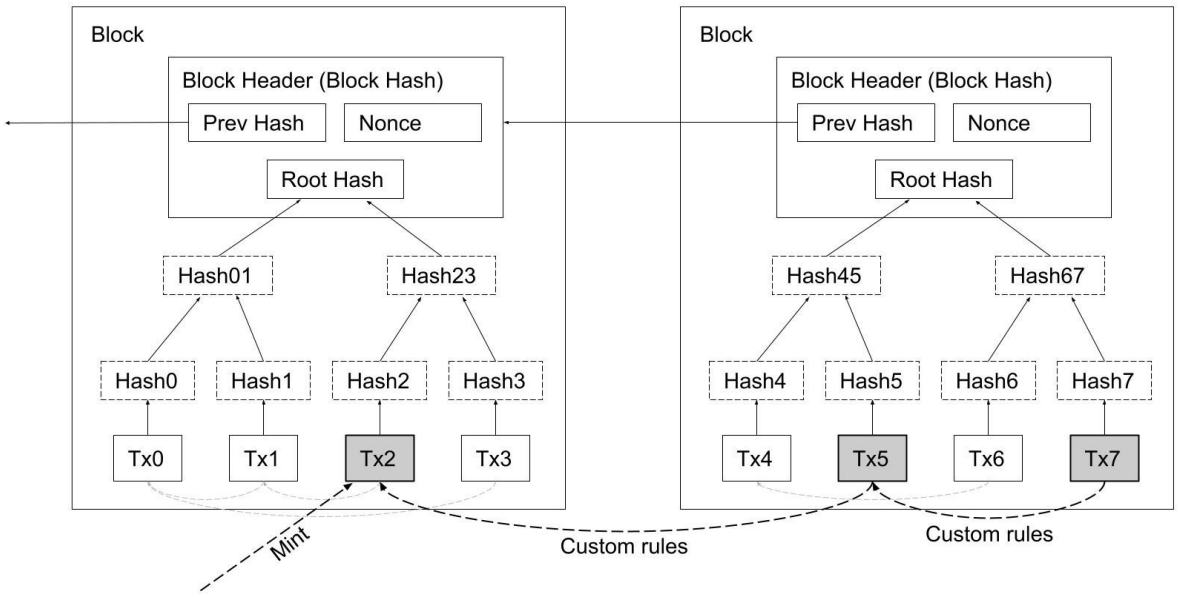
> 图表 2。块状结构；事务被组织成一棵 Merkle 树。

在数字资产的背景下，这种设计的问题在于，只有一种类型的硬币或数字资产，而没有用户定义的硬币(或数字资产类型)的概念。该设计对于在本地账户单位中的类似电子支付的交易来说足够好，但是它不能立即将其自身用于其他类型的硬币或数字资产。一种常见的解决方案是引入诸如事务索引器之类的服务，该服务监视特殊数据序列的事务，以表示数字资产的创建。这种解决方案的问题是数字资产的命运，取决于运行服务的公司，每笔交易都需要分类，并以有效的方式为用户提供服务，就像网络上任何其他可信的服务一样。

我们需要一种方法，让用户指示自定义硬币类型的创建，但不依赖于用于数据呈现的可信服务。

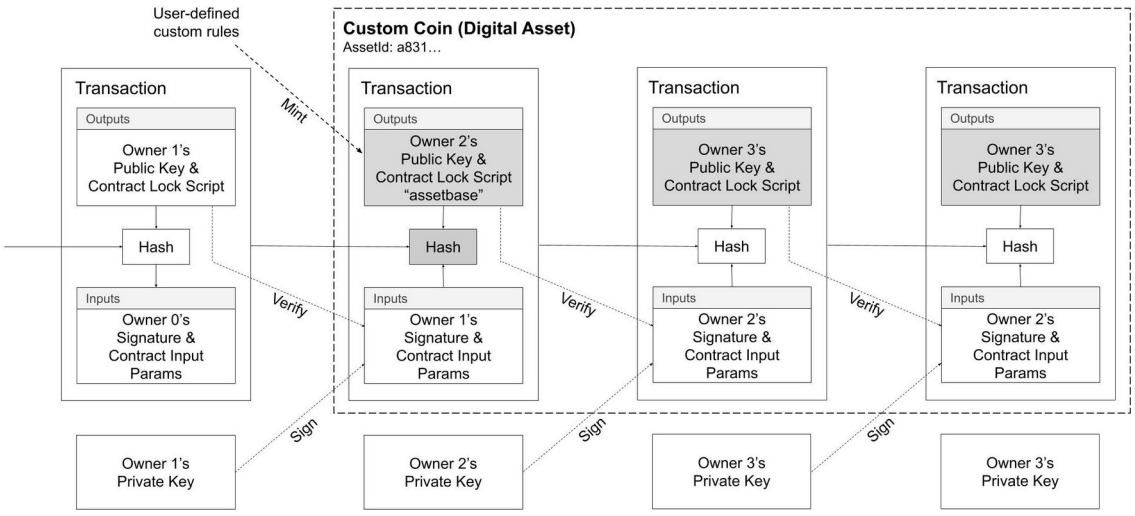
3. 数字资产

我们将自定义电子硬币或数字资产定义为一系列数字签名。数字资产是一种用户定义的硬币类型，使用特殊的交易标记(称为“资产基础交易”)来创建或铸造数字资产。与向系统注入新硬币的 coinbase 交易类似，assetbase 交易在电子硬币的生命周期内用唯一的 36 字节标识符对其进行着色或标记。定制电子硬币覆盖在基础硬币类型的顶部，并且以类似的方式起作用。assetbase 事务可以出现在块中的任何地方，并且可以执行预先决定的任何自定义规则和约束。



> 图表 3。代表用户定义的硬币类型或数字资产的交易。

为此，我们需要创建一个稳定的唯一标识符和交易机制来跟踪硬币类型(数字资产)的真实性。该系统的用户需要证明定制硬币类型不是伪造的，并且准确地表示数字资产。

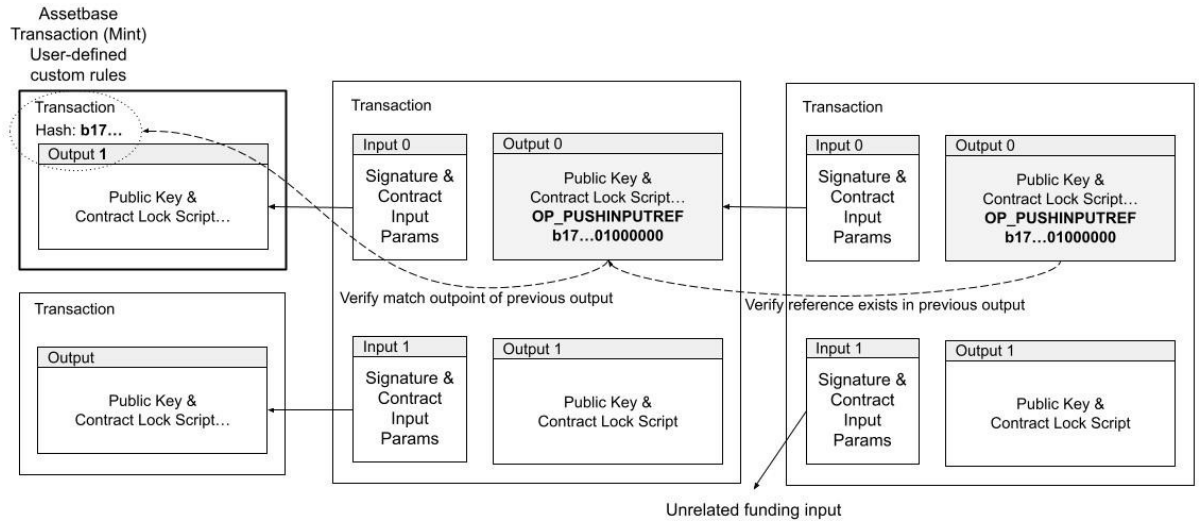


> 图表 4。自定义用户定义的硬币类型是从一个特殊的铸币交易定义的。唯一的标识符用于对硬币类型进行分类。

4. 唯一标识符

为了实现硬币类型的唯一标识符，我们使用一种特殊的标记事务，称为“资产基础事务”，它充当数字签名链的起点(mint)。我们重新使用交易标识符和输出索引(称为“输出点”)作为硬币类型的唯一标识符，而不是要求唯一标识符的新数据结构。确保输出点(36 字节)是随机的和全局唯一的。

名为 OP_PUSHINPUTREF 的编程指令用于将引用附加到输出。该指令只接受一个 36 字节的参数，该参数必须匹配 1)正在使用的输出之一的 outpoint，或者 2)相同的 36 字节值已经出现在正在使用的输出之一的先前指定的 OP_PUSHINPUTREF 中。任何给定值出现在事务输出中的唯一方式是，通过某个祖先事务，它匹配来自初始 minting assetbase 事务的 outpoint。指定值不满足任一条件的交易无效。

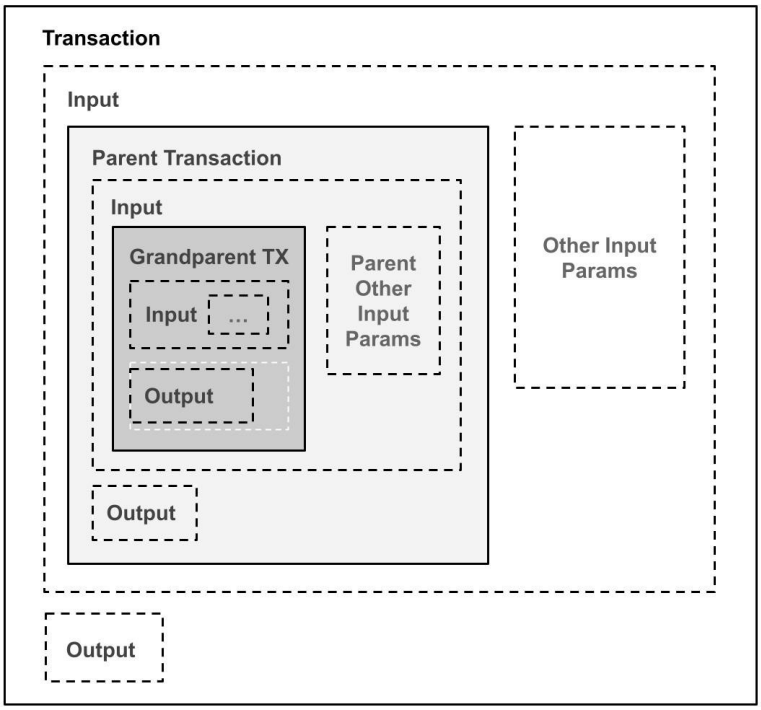


> 图表 5。唯一标识符通过匹配正在使用的一个输出的输出点来初始化，然后只要至少一个正在使用的输出在脚本体中包含相同的唯一标识符，就维护唯一标识符。

这个简单的编程指令提供了一个唯一的标识符，可以用作创建高级规则的稳定参考。例如，不同的硬币类型，数字资产，现在可以依赖于其他硬币类型。由于所有数据都是事务本地的，通过其直接的父输入事务，客户端和服务很容易在 O(1)恒定的时间和空间内验证数字资产的真实性，从而避免了对可信服务的需要。

5. 归纳法证明

可以用另一种方式创建唯一标识符，也可以使用修改的事务散列算法提供数学归纳[5]证明的机制。通过允许输入脚本接受正在使用的父事务，规则可以验证父事务及其祖父事务是否符合所需的规则。显而易见的问题是，随着父事务的每个完整副本的嵌入，会出现指数级的大小爆炸，从而阻碍了该技术的实际应用。所需要的是一种压缩事务的方法，以便可以使用固定大小的数据结构来导出事务散列，而不需要完整的事务内容。



> 图表 6。完全父交易验证，通过将完全父交易嵌入到导致交易规模指数增长的输入中进行数学归纳证明。

我们可以通过修改比特币中使用的交易哈希算法来实现这一点，其中从序列化交易中计算出双重 sha-256 摘要，将其修改为新版本，首先汇总交易内容以获得哈希。我们引入交易哈希算法版本 3，以区别于比特币中版本 1 和版本 2 的使用。该过程是将事务的每个字段或组件散列为中间散列，该中间散列可用作固定大小的输入，从而避免事务大小的指数增长。

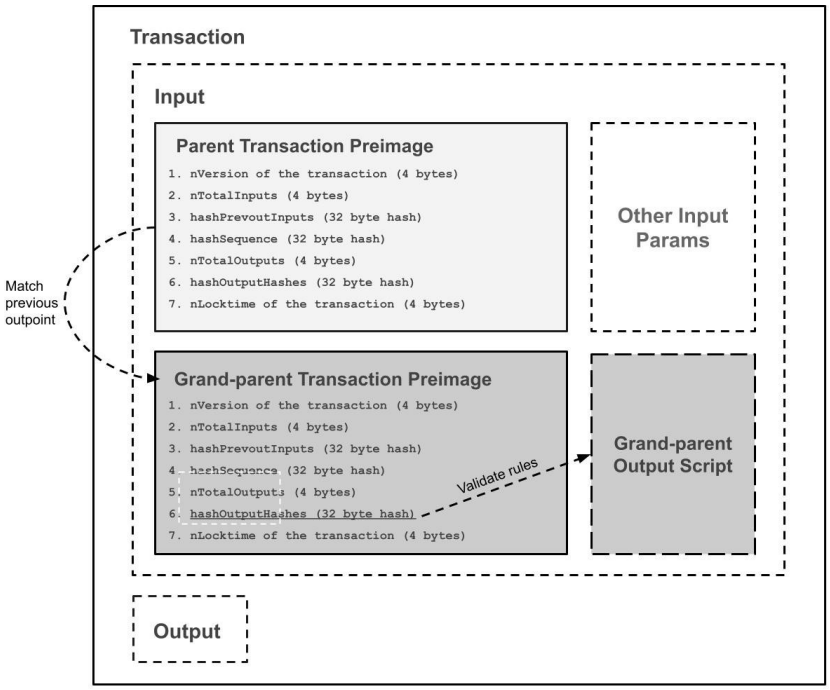
我们使用事务的以下组件将有关事务的信息压缩到一个固定的 112 字节数据结构中，该数据结构是一个预映像，然后再对其进行双重 sha-256 哈希处理，最终获得事务哈希。

事务版本 3 哈希原像字段:

> - 事务的转换（= 3）（4 字节小端）
> - nTotalInputs （4 字节小端）
> - hashPrevoutInputs （32 字节哈希）

- 哈希序列（32 字节哈希）
- nTotalOutputs （4 字节小端）
- hashOutputHashes （32 字节哈希）
- 事务的 nLocktime 字节小端）

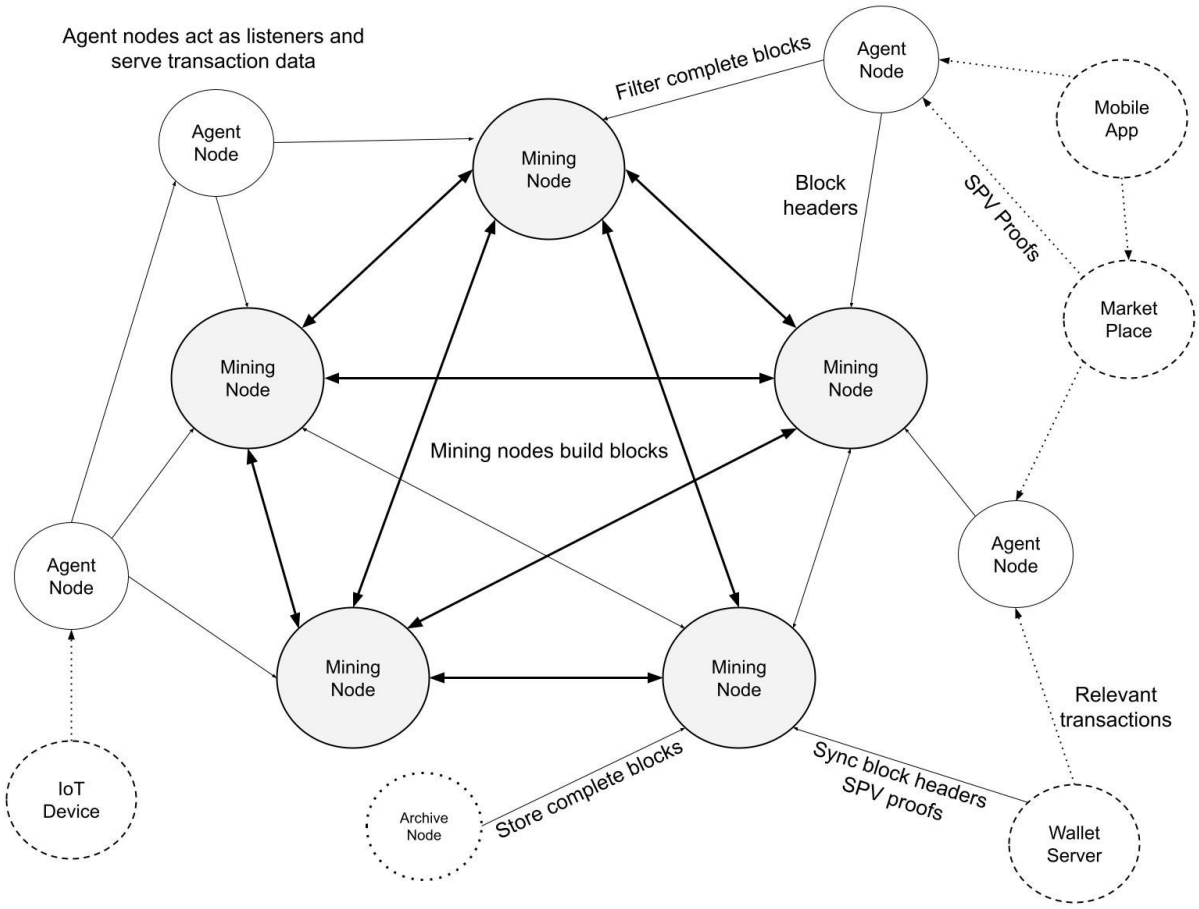
通过对版本 3 事务使用事务散列算法，我们能够在数学归纳证明的每个步骤中嵌入父事务和祖父事务，以防止事务大小增加，并且能够根据需要实施任何规则和约束。



图表 7。压缩的父事务验证，数学归纳证明，通过嵌入父和曾祖父的事务哈希版本 3 原像数据结构来执行任意规则和约束。

6. 网络

网络拓扑是一个几乎完整的图，其中每个挖掘节点都连接到每个其他挖掘节点。运行网络的步骤与比特币相同，不同的节点类型有所区别:挖掘节点、代理节点、存档节点。挖掘节点是数据块的主动发布者，并与所有其他节点保持一致，归档节点提供历史数据块数据，而代理节点旨在过滤数据块并跟踪它们所服务的应用程序感兴趣的事务。存档和代理节点可以在同一对等网络上运行，但不会产生数据块。诸如档案和代理节点之类的非挖掘节点有时被称为“监听器节点”，以区分它们在网络中的角色。



图表 8。挖掘节点连接良好，构建在彼此的块之上。归档节点存储完整的数据块，用于历史分析和引导目的。代理节点是监听器节点，用于过滤和存储事务以服务于客户端。

挖掘节点在其他挖掘节点之间很好地连接成一个几乎完整的图。他们的工作是建立在彼此的区块之上，并维护最近几百个区块的共识，并维护 UTXO 集以防止重复支出。

代理节点只需要存储交易的子集，例如，特定的硬币类型或数字资产。即使对于大块，代理节点也可以通过引用或特定的字节序列快速过滤事务，然后存储这些事务以通过应用程序编程接口提供服务。在协作代理之间，可以为每个块中匹配预定模式的事务公开宣布 Merkle 树根散列，以向其他代理和消费者发信号通知该代理已经处理了哪些事务。

归档节点用于为各种应用程序(包括数据仓库、分析和机器学习)创建整个数据块的备份副本。由于归档节点不直接参与挖掘，因此它不需要与挖掘或代理节点相同的实时性能和带宽要求。

7. 计算

我们考虑辐射式网络持续增长的情况，以及它对挖掘、存档和代理节点的处理要求所带来的影响。相比之下，在撰写本文时，比特币区块链有大约 8300 万个未用完的交易输出，总共有大约 6 GB 的必要数据来防止双重花费。只需要由挖掘节点保存最近的几百个块，而较旧的块可以从归档节点获得。对于代理节点，有必要保留与它们所服务的应用程序相关的未用事务输出的相关分区，缩放是带宽而不是存储需求的函数。

出于我们的目的，我们假设每 5 分钟将有 3 GB 大小的数据块被打上时间戳并分布在网络中，即每秒约 20，000 个事务，平均事务大小为 500 字节，即每个数据块约 6，000，000 个事务。我们表明，对于每种类型的节点，网络能够充分扩展以满足全球需求。这相当于地球上 80 亿人口中的每 5 天就有 1 笔交易。

挖掘节点

挖掘节点是唯一建立在彼此块之上的节点类型。为了保持一致，同步未用完的事务输出(UTXO)集就足够了，并且只维护大约最后一百个块。在撰写本文时，高性能商用固态硬盘能够实现 120，000 以上的 IOPS，280 GB 的成本约为 500 美元，每秒能够处理约 20，000 次交易(假设每次交易有 2 个输入和 2 个输出)。对输入有 2 次读取，对输入有 2 次更新，对新输出有 2 次写入:120，000 / 6 = 20，000 事务/秒。

存档节点

存档节点提供历史块数据，适用于机器学习、分析和数据仓库应用。存档节点可以补充挖掘节点的引导，并在 UTXO 集合上运行定期一致性检查。在撰写本文时，18 TB 的商用硬盘的价格约为
350 美元。假设每 5 分钟 3 GB 的数据等于每天 732 GB 的数据存储需求，即每月约 22 TB。一年的硬件成本是 15 个硬盘，容量为 18 TB，每年的增量成本为 5，000 美元。

代理节点

代理节点在节点类型中最容易扩展，因为它们只处理它们所服务的应用程序的相关事务类型。因此，代理节点的范围可以从 web 服务器到具有有限处理和存储能力的轻量级物联网设备，但仍能保持 3 GB 数据块或每秒 20，000 次交易。例如，一家公司可能希望跟踪作为数字资产创建的忠诚度积分的使用情况，因此只需从每个区块中选择一小部分与该硬币类型的唯一标识符匹配的交易更新。

在撰写本文时，一款商业计算设备 Raspberry Pi 4 的售价约为 275 美元，它拥有一个四核 1.5 GHZ 处理器和 4 GB RAM，可用于快速过滤和丢弃不相关的事务，每核处理 5000 个事务。当然，这只是一个例子，说明处理大型块是多么合理，在一个典型的 web 应用程序中可能有更多的可用内核。

前 25 个国家的中值带宽速度超过 100 MBPS，或大约 10mb/秒下载，许多互联网服务提供商提供无限下载。每 5 分钟 3 GB 数据块的带宽需求约为 10mb/秒，每月总计 22 TB。还可以创建代理节点的层次结构，以过滤带宽容量较低的代理节点的总带宽需求。

8. 结论

我们提出了一种不依赖信任的数字资产管理系统。我们从由数字签名构成的硬币的基本构件开始，数字签名提供了对所有权的强大控制。从所需的规则和激励出发，我们介绍了两种在恒定的 O(1)时间和空间中认证和跟踪数字资产的新方法。这两种方法独立地提供了一个通用的数学归纳证明系统，该系统可以对任何可能的数字资产配置进行编码。该系统在交易范围内和交易范围内都是完整的，不需要二级层。Radiant 是一种突破性的设计，它提供了未用完事务输出(UTXO)区块链的性能和并行性优势，但具有基于以太坊虚拟机(EVM)的基于帐户的区块链的收缩能力。

参考

[1] 中本聪，“比特币:点对点电子现金系统”网址 https://bitcoin.org/bitcoin.pdf，2009.

[2] 以太坊:下一代智能合约和分散应用平台。统一资源定位器 https://ethereum.org/en/whitepaper/，2014.

[3] 维基百科贡献者。“图灵完备性。”维基百科，免费的百科全书。维基百科，免费的百科全书，网址 https://en.wikipedia.org/wiki/Turing_completeness，2022 年 7 月 21 日

[4] R.C. Merkle，“公钥密码系统的协议”，正在进行中。1980 年安全和隐私研讨会，IEEE 计算机学会，122-133 页，1980 年 4 月。

[5] 大英百科全书编辑。“数学归纳法。”大英百科全书，网址 https://www.britannica.com/science/mathematical-induction，2018