

区块的迁移

技术领域

[01]本公开涉及区块链技术领域，具体涉及一种区块的迁移方法和装置。

背景技术

[02]目前提供了一种基于可信执行环境（Trusted Execution Environment，TEE）服务器的区块迁移技术。如果需要从区块链系统中将存储的区块迁移至区块链系统。TEE 服务器会先从区块链系统中拉取待迁移区块，然后，验证获取的待迁移区块的真实性，其中，区块的真实性用于指示区块是否是真正存储在区块链系统中的区块。在 TEE 服务器确认待迁移区块的真实性通过后，可以将待迁移区块存储至区块链系统。当然，在一些情况下，如果需要将区块链系统中的全部区块都迁移至区块链系统，那么可以采用上述方法，逐个将区块链系统中的区块迁移并存储至区块链系统。相应地，用户可以通过区块链系统来查询区块链系统中迁移过来的区块。

[03]在上述迁移方案中，可以通过 TEE 服务器内置的验证逻辑来验证区块的真实性。然而，这种关于区块真实性的验证方式对于用户而言是不可见的，用户无法获知 TEE 服务器内验证区块真实性的验证逻辑包含那些内容，从哪些方面验证了区块的真实性，更甚者，用户无法确定 TEE 服务器有没有对区块的真实性进行验证。因此，用户在很大程度上无法信任利用上述迁移方法来迁移的区块的真实性。

发明内容

[04]有鉴于此，本公开实施例致力于提供一种区块的迁移方法和装置，以提高区块迁移过程中验证区块真实性的方法的透明度。

[05]第一方面，提供一种区块的迁移方法，所述区块为源区块链中待迁移至目标区块链的第一区块，所述方法应用于目标区块链的区块链节点，所述目标区块链上存储有第一智能合约，所述第一智能合约用于对所述源区块链中的区块进行管理，所述方法包括：接收所述第一智能合约的第一调用请求，所述第一调用请求包含所述源区块链中的所述第一区块；利用所述第一智能合约，对所述第一区块的真实性进行验证；如果所述第一区块的真实性验证通过，将所述第一区块存储至所述目标区块链。

[06]第二方面，提供了一种区块的迁移方法，所述区块为源区块链中待迁移至目标区块链的第一区块，所述目标区块链上存储有第一智能合约，所述第一智能合约用于对经由转发设备转发的所述源区块链中的区块进行管理，所述方法应用于所述转发设备，所述方法包括：从所述源区块链中获取所述第一区块；向所述目标区块链节点发送所述第一

智能合约的第一调用请求，所述第一调用请求包含所述第一区块。

[07]第三方面，提供了一种区块的迁移装置，所述区块为源区块链中待迁移至目标区块链的第一区块，所述装置为目标区块链中的区块链节点，所述目标区块链上存储有第一智能合约，所述第一智能合约用于对所述源区块链中的区块进行管理，所述装置包括：接收模块，用于接收所述第一智能合约的第一调用请求，所述第一调用请求包含所述源区块链中的所述第一区块；处理模块，用于利用所述第一智能合约，对所述第一区块的真实性进行验证；所述处理模块，还用于如果所述第一区块的真实性验证通过，将所述第一区块存储至所述目标区块链。

[08]第四方面，提供了一种区块的迁移装置，所述区块为源区块链中待迁移至目标区块链的第一区块，所述目标区块链上存储有第一智能合约，所述第一智能合约用于对经由转发设备转发的所述源区块链中的区块进行管理，所述装置应用于所述转发设备，所述装置包括：获取模块，用于从所述源区块链中获取所述第一区块；发送模块，用于向所述目标区块链节点发送所述第一智能合约的第一调用请求，所述第一调用请求包含所述第一区块。

[09]第五方面，提供一种区块的迁移装置，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器被配置为执行所述可执行代码，以实现如第一方面或第二方面所述的方法。

[10]第六方面，提供一种计算机可读存储介质，其上存储有可执行代码，当所述可执行代码被执行时，能够实现如第一方面或第二方面所述的方法。

[11]第七方面，提供一种计算机程序产品，包括可执行代码，当所述可执行代码被执行时，能够实现如第一方面或第二方面所述的方法。

[12]本公开通过在目标区块链中部署第一智能合约来验证区块的真实性，这样，用户可以通过查询目标区块链中部署的第一智能合约来查看验证区块真实性的验证方法，有利于提高验证方法的透明度，提高用户对迁移过程的信任程度。

附图说明

[13]图 1 为本公开实施例适用的区块链系统的示意图。

[14]图 2 为本公开实施例适用的区块的结构示意图。

[15]图 3 为传统的区块的迁移的场景示意图。

[16]图 4 介绍本公开实施例适用的迁移的场景示意图。

[17]图 5 是本公开实施例的区块的迁移方法的流程图。

[18]图 6 介绍本公开实施例的第一智能合约的示意图。

[19]图 7 是本公开另一实施例的区块的迁移的场景的示意图。

[20]图 8 是本公开另一实施例的区块的迁移方法的流程图。

[21]图 9 是本公开实施例的区块的迁移装置的示意图。

[22]图 10 是本公开实施例的区块的迁移装置的示意图。

[23]图 11 是本公开另一实施例的装置的示意性框图。

具体实施方式

[24]下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本公开一部分实施例，而不是全部的实施例。为了便于理解本公开的方案，下文先结合图 1 介绍本公开适用的区块链系统以及本公开涉及的一些术语。

[25]区块链系统。

[26]图 1 为本公开实施例适用的区块链系统的示意图。图 1 所示的区块链系统 100 包括区块链节点 110 和用户节点 120。

[27]区块链（Blockchain）系统是一个典型的分布式协同系统，多方共同维护一个不断增长的分布式数据记录，这些记录的数据通过密码学技术保护内容和时序，使得任何一方难以篡改、抵赖、造假。

[28]在区块链系统中，数据（例如，交易信息、交易执行结果等）可以以区块（Block）的形式被封装。区块彼此之间可以通过前向的应用彼此链接形成“链”，即区块链。通常，我们将区块链中位于当前区块之前的一个区块称为“上一区块”，将区块链中位于当前区块之后的一个区块称为“后继块”。下文结合图 2 对区块进行介绍，为了简洁，在此不再赘述。

[29]通常，区块链的用户节点 120 可以通过客户端与区块链节点 110 进行通信。在一些情况下，用户节点 120 可以将需要上链的数据，以提交交易（Transaction）的方式发送给关联的一个或多个区块链节点 110。其中，交易可以理解为区块链上的一个事务请求，用来承载具体业务操作数据的结构。

[30]需要说明的是，区块链上所有针对世界状态的变化操作均可以是基于交易来完成的。上述世界状态可以理解为区块链账户的存储状态，包含所有账户的基本存储状态和合约账户的内部存储状态。可以将合约平台理解为一种交易的“状态机”，世界状态描述当前的基本存储状态，经过执行智能合约，世界状态可能发生改变进入另外一个新的世界

状态。

[31]相应地，区块链节点 110 在验证数据的真实性之后，可以通过全网广播的方式将数据广播至每个区块链节点 110。这样，每个区块链节点 110 都记录有全量的、一致的数据。

[32]在一些实现方式中，上述区块链节点 110 可以是具有计算能力的设备，例如，服务器、服务器组、区块链芯片等，其中，服务器组可以是集中式的，也可以是分布式的。在另一些实现方式中，上述服务器还可以是为云平台提供服务的服务器。

[33]在一些实现方式中，上述用户节点 120 可以是具有计算能力的设备，例如，可以是服务器、终端、移动终端等。

[34]区块。

[35]如上文介绍，区块链是一个链式存储结构，区块就是链式存储结构中的数据元素。区块链可以理解为由区块相互连接形成单向链式结构。通常，我们称区块链中的第一个区块为“创始区块”或“初始区块”。

[36]通常，每个区块可以记录有上一个区块的哈希值、当前区块中的交易信息、当前区块的哈希等基础数据。图 2 示出了本公开实施例适用的区块的结构。参见图 2，上述区块 200 可以被分为两部分：区块头 210 和区块体 220。

[37]区块头 210 可以包含当前区块的基本信息，用以保证当前区块能正确的进入区块链。在一些实现方式中，区块头 210 可以记录当前区块的上一区块的区块哈希（Hash）值。目前上一区块的区块哈希值可以记录在区块头 210 中的“prevBlockHash”字段。在另一些实现方式中，上述区块头 210 还可以记录当前区块的区块高度。其中，区块高度简称“块高”，用来识别区块在区块链中的位置。通常，创始区块的块高为 0。

[38]区块体 220 可以用于记录交易信息，包括交易数量和交易数据。

[39]共识机制。

[40]共识机制可以理解为所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。

[41]区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。以比特币为例，采用的是工作量证明，只有在控制了全网超过 51%的记账节点的情况下，才有可能伪造出一条不存在的

记录。当加入区块链的节点足够多的时候，这基本上不可能，从而杜绝了造假的可能。

[42]区块链的自信任主要体现于分布于区块链中的用户无须信任交易的另一方，也无须信任一个中心化的机构，只需要信任区块链协议下的软件系统即可实现交易。这种自信任的前提是区块链的共识机制（consensus），即在一个互不信任的市场中，要想使各节点达成一致的充分必要条件是每个节点出于对自身利益最大化的考虑，都会自发、诚实地遵守协议中预先设定的规则，判断每一笔记录的真实性，最终将判断为真的记录记入区块链之中。换句话说，如果各节点具有各自独立的利益并互相竞争，则这些节点几乎不可能合谋欺骗你，而当节点们在网络中拥有公共信誉时，这一点体现得尤为明显。区块链技术正是运用一套基于共识的数学算法，在机器之间建立“信任”网络，从而通过技术背书而非中心化信用机构来进行全新的信用创造。

[43]现今区块链的共识机制可分为工作量证明机制（Proof Of Work, PoW）、权益证明机制、股份授权证明机制、验证池机制以及实用拜占庭（Practical Byzantine Fault Tolerance, PBFT）。

[44]智能合约（Smart Contracts）。

[45]智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。或者说，智能合约可以理解为部署在计算机系统上的一段程序，当智能合约的触发条件被满足时，智能合约可以被自动地执行。

[46]区块链的出现为智能合约的实现提供了技术支撑。将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障智能合约的存储、读取、执行整个过程透明可跟踪、不可篡改。另一方面，可以由区块链自带的共识算法构建出一套状态机系统，使得智能合约能够高效地运行。

[47]在一些实现方式中，用户可以通过向区块链系统提交交易的方式，调用智能合约，并对智能合约中记录的数据进行设置，并将设置后的智能合约存储在区块链中。相应地，当智能合约的特定条件被触发后，区块链节点可以执行智能合约，并记录智能合约的执行结果，智能合约的执行状态。

[48]目前，各行业乃至行业中某些领域（例如，金融、公益、保险、跨境支付等）会根据自身的产业结构来搭建不同区块链系统，并且在区块链系统上记录该行业或产业中有价值的信息与资产。

[49]然而，在一些场景中，任何一个行业的信息与资产都不可能完全孤立，往往有跨行业协作的业务需求。因此，区块链系统中记录的信息与资产需要在多个区块链系统之间迁移，或者说，区块链系统中存储的区块需要在多个区块链系统之间迁移。这就意味着需要一种“可信连接技术”，能把一个区块链网络中的区块，真实可靠地迁移到另外一

个区块链网络中，并保证在迁移区块的过程中，区块的内容无法被篡改。这样，另外一个区块链网络中的参与方就可以信任被迁移的区块，并利用被迁移的区块进行业务协作了。

[50]在另一些场景中，区块链系统需要升级，但是出于一些原因（例如，升级后的区块链系统不再支持升级前的区块链系统支持的区块格式），无法在存储有区块的情况下进行升级，或者说无法进行在线升级。因此，为了对区块链系统进行升级，需要将该区块链系统中存储的区块迁移至另一个区块链系统中。这也意味着需要一种“可信连接技术”，能把待升级的区块链网络中的区块，真实可靠地迁移到另外一个区块链网络中，并保证在迁移区块的过程中，区块的内容无法被篡改。这样，待升级的区块链网络可以进行升级，同时用户也可以通过另外一个区块链系统继续使用被迁移的区块。

[51]为了满足各个场景中对区块进行跨链迁移的需求，目前提供了一种基于可信执行环境（Trusted Execution Environment，TEE）服务器的区块迁移技术。下文结合图 3 进行介绍。

[52]在图 3 所示的场景中，假设需要从区块链系统 310 中将存储的区块迁移至区块链系统 320。TEE 服务器 330 会先从区块链系统 310 中拉取待迁移区块，然后，验证获取的待迁移区块的真实性，其中，区块的真实性用于指示区块是否是真正存储在区块链系统 310 中的区块。在 TEE 服务器确认待迁移区块的真实性通过后，可以将待迁移区块存储至区块链系统 320。当然，在一些情况下，如果需要将区块链系统 310 中的全部区块都迁移至区块链系统 320，那么可以采用上述方法，逐个将区块链系统 310 中的区块迁移并存储至区块链系统 320。相应地，用户可以通过区块链系统 320 来查询区块链系统 310 中迁移过来的区块。

[53]在上述迁移方案中，可以通过 TEE 服务器内置的验证逻辑来验证区块的真实性。然而，这种关于区块真实性的验证方式对于用户而言是不可见的，用户无法获知 TEE 服务器内验证区块真实性的验证逻辑包含那些内容，从哪些方面验证了区块的真实性，更甚者，用户无法确定 TEE 服务器有没有对区块的真实性进行验证。因此，用户在很大程度上无法信任利用上述迁移方法来迁移的区块的真实性。

[54]为了避免上述问题，提高区块迁移过程中验证区块真实性的方法的透明度，本公开提供了一种区块的迁移方法，在将区块从源区块链迁移至目标区块链的场景下，通过在目标区块链中部署第一智能合约来验证区块的真实性，这样，用户可以通过查询目标区块链中部署的第一智能合约来查看验证区块真实性的验证方法，有利于提高验证方法的透明度，提高用户对迁移过程的信任程度。需要说明的是，为了便于描述，下文将迁移过程中的当前区块称为“第一区块”。

[55]下文在结合图 5 介绍本公开实施例的方法之前，先结合图 4 介绍本公开实施例适用

的迁移场景。需要说明的是，图 4 所示的源区块链 410 和目标区块链 420 可以是图 1 所示的区块链系统中的区块链，相关内容可以参见上文介绍，为了简洁，在此不再赘述。

[56]参见图 4，假设第一区块需要从源区块链 410 迁移至目标区块链 420，且目标区块链 420 上部署有第一智能合约 421，其中，第一智能合约 421 用于对源区块链 410 中的区块进行管理。

[57]图 5 是本公开实施例的区块的迁移方法的流程图。图 5 所示的方法包括步骤 S510 至步骤 S530。图 5 所示的步骤可以由目标区块链 420 中的区块链节点执行。

[58]在步骤 S510 中，接收第一智能合约 421 的第一调用请求。

[59]在一些实现方式中，上述第一调用请求用于请求将第一区块从源区块链 410 迁移至目标区块链 420。上述第一调用请求包含源区块链 410 中的第一区块。

[60]在步骤 S520 中，利用第一智能合约 421，对第一区块的真实性进行验证。

[61]上述第一区块的真实性用于表示第一区块是否为源区块链 410 中存储的区块。在一些实现方式中，可以基于第一区块的合法性，来验证第一区块的真实性。在另一些实现方式中，可以基于第一区块所属的区块链节点的合法性，来验证第一区块的真实性。在另一些实现方式中，可以基于第一区块中的数据内容，来验证第一区块的真实性。下文将详细介绍验证第一区块的真实性的方法，为了简洁，在此不再赘述。

[62]在步骤 S530 中，如果第一区块的真实性验证通过，将第一区块存储至目标区块链 420。

[63]如果第一区块的真实性验证通过，在一定程度上可以认为第一区块为源区块链 410 中存储的区块，此时，可以将第一区块存储在目标区块链 420 中。或者说，将第一区块持久化到目标区块链 420 中。

[64]在一些情况下，上述第一区块的真实性验证可能不通过，也就是说，第一区块可能不是源区块链 410 中存储的区块，此时，可以结束第一智能合约 421 的调用进程。或者说，结束此次第一智能合约 421 的调用。也就是说，上述方法还包括：步骤 S540，如果第一区块的真实性验证未通过，结束第一智能合约 421 的调用进程。

[65]如上文所述，需要对第一区块的真实性进行验证，以确保第一区块是源区块链 410 中的区块。下文分别介绍本公开实施例提供的四种验证第一区块的真实性的方式。

[66]验证方式一、可以基于第一区块是否为己迁移成功的区块的后继块，来验证第一区块的真实性。为了便于描述，下文将已迁移成功的区块称为“第二区块”。

[67]也就是说，目标区块链 420 存储有从源区块链 410 中迁移的第二区块，第二区块在源区块链 410 中为第一区块的上一区块，此时，上述步骤 S520 包括：利用第一智能合

约 421，判断第一区块是否为第二区块的后继块，以对第一区块的真实性进行验证。

[68]如上文关于区块的介绍，如果第一区块为第二区块的后继块时，第一区块的区块头会记录有第二区块的区块哈希值。那么，在一些实现方式中，可以利用第一智能合约 421 记录第二区块的区块哈希值，并将第二区块的区块哈希值与第一区块中记录的第二区块的区块哈希值进行比较，如果第一智能合约 421 中记录的第二区块的区块哈希值，与第一区块中记录的第二区块的区块哈希值相同，可以认为第一区块为第二区块的后继块，即第一区块的真实性验证通过。相反地，如果第一智能合约 421 中记录的第二区块的区块哈希值，与第一区块中记录的第二区块的区块哈希值不相同，可以认为第一区块不是第二区块的后继块，即第一区块的真实性验证不通过。

[69]需要说明的是，上述第一智能合约 421 记录的第二区块的区块哈希值，可以是在迁移第二区块的过程中记录的。例如，可以是下文提及的转发设备在迁移第二区块的过程中获取的，即转发设备从源区块链中拉取第二区块后，将第二区块中的区块哈希值读出，并发送给目标区块链中的第一智能合约 421。

[70]在使用验证方式一验证第一区块的真实性的过程中，如果第一区块为源区块链 410 中的第一个区块，那么可能无法使用上述验证方式一。为了避免这个问题，可以在第一智能合约 421 中记录源区块链 410 的创始块的信息，以便后续源区块链 410 中的其他块可以使用上述验证方式一来验证区块的真实性。在一些实现方式中，可以在第一智能合约 421 初始化的过程中，录入源区块链 410 中创始块的信息。

[71]上述创始块的信息可以包括创始块的区块哈希值。当然，在一些情况下，上述创始块的信息还可以包括创始块的区块内容，以便验证第一智能合约 421 中记录的创始块的区块哈希值是否是基于创始块的区块内容得到的，有利于提高创始块的信息的真实性。

[72]验证方式二、可以基于区块链节点约定的区块哈希值的最大值，来验证第一区块的真实性。

[73]通常，区块链网络中的各个区块链节点会约定一个区块哈希值的最大值，来限制区块链系统中区块的区块哈希值不能超过这个区块哈希值的最大值。基于此，在本公开实施例中，可以利用区块哈希值的最大值，来验证第一区块的真实性。

[74]也就是说，第一智能合约 421 中记录有源区块链 410 中区块链节点约定的区块哈希值的最大值，上述步骤 S520 可以包括利用第一智能合约 421，判断第一区块的区块哈希值是否小于区块哈希值的最大值，以对第一区块的真实性进行验证。

[75]在一些实现方式中，可以利用第一智能合约 421 将第二区块的区块哈希值与区块哈希值的最大值进行比较，如果第二区块的区块哈希值小于区块哈希值的最大值，可以认为第一区块的区块哈希值满足源区块链 410 中区块链节点的约定，则第一区块的真实性

验证通过。相反地，第二区块的区块哈希值大于区块哈希值的最大值，可以认为第一区块的区块哈希值不满足源区块链 410 中区块链节点的约定，即第一区块的真实性验证不通过。

[76]需要说明的是，上述第一智能合约 421 记录的区块哈希值的最大值，可以是在第一智能合约 421 初始化的过程中录入的。

[77]验证方式三、可以基于源区块链中第一区块所属的区块链节点，来验证第一区块的真实性。

[78]也就是说，源区块链 410 中存储第一区块的区块链节点为第一区块链节点，第一区块为经过第一区块所属的区块链节点数字签名后的区块，第一智能合约 421 中记录有第一区块链节点的公钥。上述步骤 S520 可以包括：利用第一智能合约 421，基于第一区块链节点的公钥，判断第一区块的数字签名是否为第一区块链节点的数字签名，以对第一区块的真实性进行验证。

[79]在一些实现方式中，调用第一智能合约 421 时还可以向第一智能合约 421 告知待迁移的第一区块在源区块链中所属的区块链节点，即上文中的第一区块链节点。这样，第一智能合约 421 可以基于记录的第一区块链节点的公钥以及第一区块上的数字签名，来验证第一区块的真实性。如果第一智能合约 421 记录的第一区块链节点的公钥与第一区块上的数字签名匹配，可以认为第一区块为第一区块链节点传输的区块，则第一区块的真实性验证通过。相反地，如果第一智能合约 421 记录的第一区块链节点的公钥与第一区块上的数字签名不匹配，可以认为第一区块不是第一区块链节点传输的区块，则第一区块的真实性验证不通过。

[80]需要说明的是，上述源区块链中第一区块链节点的公钥，可以是在第一智能合约 421 初始化的过程中录入的。

[81]在另一些实现方式中，第一智能合约 421 还可以记录有源区块链中的部分或全部区块链节点的公钥，以便在对不同区块链节点的区块进行迁移的过程中，验证区块的真实性。当然，上述部分或全部区块链节点的公钥也可以是在第一智能合约 421 初始化的过程中录入的。

[82]验证方式四、基于源区块链中的其他区块链节点存储的区块的交易信息，对第一区块的真实性进行验证。

[83]在实际情况中，源区块链 410 中可能存在区块链分叉的情况，也就是说，存在有多个记录不同交易信息的区块争夺同一块高的位置的情况。但仅会有一个区块争夺到该块高的位置，并被整个源区块链 410 中的区块链节点所共识。例如，源区块链 410 中有区块 1 和区块 2 同时在竞争块高 2 的位置，并且区块 1 记录有交易 1、交易 3、交易 5 的

内容, 区块 2 记录有交易 2、交易 4、交易 6 的内容。最后, 仅区块 1 争夺到区块 2 的位置, 并被源区块链 410 中的全部区块链节点所共识。

[84]在上述场景中, 区块 2 虽然没有被源区块链 410 中的全部区块链节点所共识, 但是区块 2 的区块哈希值是小于源区块链 410 中约定的区块哈希值的最大值, 并且区块 2 中会记录块高 1 位置的区块的区块哈希值, 如果此时, 区块 2 所属的区块链节点作恶, 对区块 2 进行数据签名, 并迁移到目标区块链节点 420 后, 使用上述验证方式一至验证方式三中任意一种验证方式对区块 2 的真实性进行验证, 得到的验证结果都会是通过。这种情况, 上述验证方式是无法验证出区块 2 其实并不是源区块链 410 中被共识的区块。

[85]因此, 为了提高区块真实性验证的准确性。本公开实施例还提供一种区块真实性的验证方式四。即, 第一智能合约 421 中记录有源区块链 410 中第二区块链节点存储的第三区块的第一交易信息, 且在源区块链 410 中第三区块的块高与第一区块的块高相同。上述步骤 S520 还包括: 利用第一智能合约 421, 对第一交易信息与第一区块记录的交易信息进行比对, 以对第一区块的真实性进行验证。

[86]如果第一交易信息与第一区块记录的交易信息的内容相同, 可以理解为, 第一区块是源区块链 410 中经过共识的区块, 则第一区块的真实性验证通过。相反地, 如果第一交易信息与第一区块记录的交易信息的内容不同, 可以理解为, 第一区块是没有经过源区块链节点 410 共识的区块, 则第一区块的真实性验证不通过。

[87]需要说明的是, 上述第一交易信息和/或第一区块记录的交易信息可以是在对应区块的迁移过程中获取的。例如, 第一交易信息可以是下文中的转发设备在迁移第三区块的过程中获取的, 即转发设备从源区块链中拉取第三区块后, 将第三区块中的第一交易信息读出, 并发送给目标区块链中的第一智能合约 421。相应地, 第一区块记录的交易信息也可以是下文中的转发设备在迁移第一区块的过程中获取的, 即转发设备从源区块链中拉取第一区块后, 将第一区块中的交易信息读出, 并发送给目标区块链中的第一智能合约 421。

[88]通常, 为了进一步提高对区块真实性进行验证的准确率, 可以利用第一智能合约 421, 对源区块链中各个区块链节点中存储的相应位置的区块记录的交易信息进行对比, 只有当预设数量的区块链节点存储的相应位置的区块中的交易信息相同时, 才会认定记录该交易信息的区块为源区块链 410 中共识的区块, 那么该区块的真实性验证通过。上述相应位置的区块可以理解为是块高相同的区块。

[89]例如, 在第一智能合约 421 中规定当源区块链 410 中有三分之一的区块链节点存储的相应位置的区块记录的交易信息相同, 那么可以认为记录该交易信息的区块是经过共识的。假设源区块链 410 中总共有 3000 个区块链节点, 区块 3 的块高为 4, 此时, 基于第一智能合约 421 的规定, 如果源区块链 410 中的 1000 个区块链节点中, 块高为 4 的

区块 3 记录的交易信息完全相同，那么可以认为记录该交易信息的区块 3 即为源区块链 410 中的真实区块，即区块的真实性验证通过。

[90]需要说明的是，如果未达到预设数量的区块链节点的对比过程中，出现了记录交易信息不同的多个区块，并且该区块的块高相同，此时，可以将这多个区块记录的内容都保留，并且在后续其他区块链节点中的相应区块进行验证的过程中，分别记录具有不同交易信息的区块对应的数量，直到记录某一交易信息的区块对应的区块链节点的数量达到上述预设数量，那么认为具有该交易信息的区块的真实性验证通过。

[91]例如，采用上述验证方式四，对源区块链 410 中的第一个区块链节点中的区块 2 进行真实性验证时，区块 2 记录的交易信息为交易信息 1。采用上述验证方式四，对源区块链 410 中的第二个区块链节点中的区块 2 进行真实性验证时，区块 2 记录的交易信息为交易信息 2。此时，由于并不知道源区块链中其他区块链节点存储的区块 2 记录的交易信息，可以分别保留交易信息 1 和交易信息 2，并在后续对源区块链 410 中的其他区块链节点中的区块 2 的真实性进行验证的过程中，记录每个交易信息的区块对应的区块链节点的数量，并在区块链节点的数量达到预设数量之后，将该交易信息的区块 2 作为源区块链 410 中记录的真实区块，即该区块的真实性验证通过。

[92]需要说明的是，上述源区块链中节点的总数量和/或上述预设数量，可以是在第一智能合约 421 的初始化过程中设定的。当然，上述参数也可以是在调用第一智能合约 421 的过程中指定的，本公开实施例对此不作限定。

[93]另外，上述预设数量可以基于源区块链中的共识机制指定，例如，源区块链 410 中采用的共识机制为 PBFT 时，上述预设数量可以是源区块链 410 中区块链节点总数的三分之一。又例如，采用的共识机制为 PoW 时，上述预设数量可以是源区块链 410 中区块链节点总数的二分之一。当然，在本公开实施例中，上述预设数量还可以是基于经验设定的，本公开实施例对此不作限定。

[94]在上文中分别介绍了验证方式一至验证方式四，需要说明的是，在本公开实施例中，上述四种验证方式还可以相互结合使用，例如，验证方式一和验证方式二可以结合使用。又例如，验证方式一、验证方式三以及验证方式四也可以结合使用。为了简洁，本公开实施例在此不再一一列举。另外，为了便于理解，下文将结合图 8 介绍上述 4 种验证方式结合使用的方法流程。

[95]另外，还需要说明的是，在上述四种验证方式还可以相互结合使用的情况中，本公开实施例对上述验证方式之间的先后顺序不作限定。例如，验证条件一可以先于验证条件二。又例如，验证条件三可以先于验证条件二。

[96]为了便于用户查询源区块链 410 中的区块，可以在第一智能合约 421 中设置查询接

口, 以便目标区块链 420 的用户调用。即, 上述方法还包括: 从目标区块链 420 的用户节点接收第一智能合约 421 的第二调用请求, 第二调用请求用于查询目标区块链 420 中存储的源区块链 410 中的区块。

[97]需要说明的是, 上述目标区块链 420 中存储的源区块链 410 中的区块可以是经过上文区块的真实性验证的区块。在一些实现方式中, 为了防止源区块链 410 中存在区块链分叉, 将源区块链中分叉后的较短的链上的区块 (即未经过共识) 迁移至目标区块链, 导致用户在目标区块链上查询到较短的链上的区块, 可以在第一智能合约 421 中设置等到块高为 N 的区块通过真实性验证过程后, 再为源区块链中块高为 $(N-i)$ 的区块提供上述查询服务, 以确保查询的可靠性。其中, N, i 为正整数, 且 N 大于 i 。在一些情况下, 根据经验可以将上述 i 设置为 6。也就是说, 这种待块高为 i 的区块通过真实性验证后, 再来提供块高为 $N-i$ 的区块的查询服务, 有利于降低用户查到上述较短的链上的区块的可能性。

[98]为了便于理解, 下文结合图 6 介绍本公开实施例的第一智能合约的内容。图 6 是本公开实施例中第一智能合约的示意图。参见图 6, 第一智能合约可以包括传输块 (通过 “transferBlock” 表示) 接口以及查询块 (通过 “queryBlock” 表示) 接口。

[99]上述传输块接口可以用于上传源区块链 410 中的区块。也就是说, 上文中的第一调用请求可以理解为调用了该传输块接口。在调用传输块接口时, 除了需要指定待上传区块 (通过 “Block” 表示), 还需要指定存储该区块的区块链节点 (通过 “node” 表示)。

[100]上述查询块接口可以用于查询已通过真实性验证的区块。也就是说, 上文中的第二调用请求可以理解为调用了该查询块接口。在调用查询块接口时, 需要指定待查询区块的索引 (通过 “blockNumber” 表示)。

[101]第一智能合约的持久化数据包括区块列表 (通过 “List<Block>” 表示)、源区块链中的区块链节点信息 (通过 “Map<node, NodeInfo>” 表示)。其中, 该列表中记录有已通过真实性验证的区块。区块链节点信息可以包括区块链节点的标识 (通过 “node” 表示), 以及区块链节点的公钥 (通过 “NodeInfo” 表示)。

[102]在一些实现方式中, 源区块链 410 和目标区块链 420 之间无法直接通信, 来迁移第一区块, 此时, 可以在源区块链 410 和目标区块链 420 之间设置转发者来将第一区块从源区块链 410 中迁移至目标区块链 420。即该转发设备从源区块链 410 获取待迁移的区块, 然后, 转发设备向目标区块链 420 的区块链节点发送上述第一调用请求。因此, 上述步骤 S510 可以包括从转发设备接收第一智能合约 421 的第一调用请求, 转发设备用于将第一区块从源区块链 410 迁移至目标区块链 420。

[103]在一些实现方式中, 转发设备可以采用拉块解析的方式从源区块链 410 中获取第一

区块。在另一些实现方式中，转发设备可以通过调用目标区块链 420 的某个区块链节点的区块查询接口，来获取第一区块。本公开实施例对转发设备获取第一区块的方式不作限定。

[104]在另一些实现方式中，上述转发设备可以是具有处理功能的设备，例如，可以是服务器、终端设备、矿机等。需要说明的是，在本公开实施例中，由于利用第一智能合约来对第一区块的真实性进行验证，以确保目标区块链中记录的区块的真实性。相对于传统的区块迁移方案而言，本公开实施例的方案对转发设备是不是 TEE 服务器并没有那么强的依赖性。当然，如果为了进一步提高区块迁移过程中的安全性，也可以配置转发设备为 TEE 服务器。

[105]为了避免转发设备作恶导致区块迁移失败，可以在源区块链 410 和目标区块链 420 之间设置多个转发设备，来将第一区块从源区块链 410 迁移至目标区块链 420。当然，如果考虑到节约成本等问题，也可以在源区块链 410 和目标区块链 420 之间设置一个转发设备。

[106]在一些实现方式中，为了鼓励转发设备将区块从源区块链 410 迁移至目标区块链 420，可以设置奖励机制。在一些实现方式中，可以通过链上的方式来奖励转发设备。例如，可以链上账户（例如，创建第一智能合约的账户）中存储奖励金，并基于每个转发设备的迁移成功率和/或迁移成功的区块数量，来将账户中的奖励金分发给转发设备对应的链上账户。本公开对上述奖励机制所参照的因素不作具体限定，例如，还可以基于转发设备调用第一智能合约的次数，来分配奖励金。

[107]在另一些实现方式中，还可以通过链下的方式来奖励转发设备。例如，可以在链上记录每个转发设备的迁移成功率和/或迁移成功的区块数量，然后基于这些记录，在链下将奖励金发给转发设备对应的链下账户。本公开对上述奖励机制所参照的因素不作具体限定，例如，还可以基于转发设备调用第一智能合约的次数，来分配奖励金。

[108]上文结合图 1 至图 6 介绍了本公开实施例的方法，为了便于理解，下文结合图 7 至图 8 以迁移区块 1 为例，介绍本公开实施例的区块迁移方法流程。参见图 7，假设区块 1 存储在源区块链 710 中的区块链节点 1，且区块 1 的块高为 2。转发设备 730 用于将区块 1 从源区块链 710 迁移中至目标区块链 720。相应地，目标区块链 720 中部署有智能合约 1，智能合约 1 用于对源区块链 710 中的区块进行管理。

[109]图 8 是本公开另一实施例的区块的迁移方法的流程图。图 8 所示的方法包括步骤 S810 至步骤 S820。

[110]在步骤 S810 中，在目标区块链 720 中初始化智能合约 1。

[111]上述初始化智能合约 1 的过程包括在智能合约 1 中记录源区块链 710 的创始块信息、

源区块链 710 的所有区块链节点信息以及源区块链 710 约定的区块哈希值的最大值。其中，创始块信息可以包括创始块的区块哈希值以及创始块区块内容。区块链节点信息包括区块链节点的标识、以及区块链节点的公钥。

[112]在步骤 S820 中，转发设备 730 从源区块链中的区块链节点 1 处获取区块 1。

[113]在一些实现方式中，转发设备 730 可以通过调用区块链节点 1 的区块查询接口，来查询得到区块 1。相应地，可以获取区块 1 中的全量交易信息。另外，区块 1 是经由区块链节点 1 采用私钥进行数字签名的区块。

[114]在步骤 S830 中，转发设备 730 将向目标区块链 720 中的区块链节点发送智能合约 1 的调用请求 1。

[115]在一些实现方式中，转发设备 730 可以通过调用请求 1 来调用智能合约 1 的传输块接口，以将区块 1 发送目标区块链 720。

[116]在步骤 S840 中，目标区块链 720 的区块链节点利用智能合约 1 对区块 1 的真实性进行验证。

[117]在一些实现方式中，区块链节点利用智能合约 1 基于验证方式一，验证区块 1 是否为区块 0 的后继块。其中区块 0 为源区块链 710 中区块 1 的上一块。如果区块 1 为区块 0 的后继块，则采用验证方式二继续验证区块 1 的真实性。如果区块 1 不是区块 0 的后继块，则结束此次智能合约 1 的调用。

[118]如果区块 1 为区块 0 的后继块，采用验证方式二，来验证区块 1 的区块哈希值是不是小于源区块链 710 约定的区块哈希值的最大值。如果区块 1 的区块哈希值小于区块哈希值的最大值，则采用验证方式三继续验证区块 1 的真实性。如果区块 1 的区块哈希值大于或等于区块哈希值的最大值，则结束此次智能合约 1 的调用。

[119]如果区块 1 的区块哈希值小于区块哈希值的最大值，采用验证方式三，来验证区块 1 所属的区块链节点是不是区块链节点 1。如果区块 1 的数字签名与区块链节点 1 的公钥匹配，则采用验证方式四继续验证区块 1 的真实性。如果区块 1 的数字签名与区块链节点 1 的公钥不匹配，则结束此次智能合约 1 的调用。

[120]如果区块 1 的数字签名与区块链节点 1 的公钥匹配，采用验证方式四，来验证区块 1 中的交易信息与区块 1' 中记录的交易信息是否相同。其中，区块 1' 是源区块链 710 中区块链节点 2 中存储的与区块 1 具有相同块高的区块，并且，区块 1' 已经通过区块的真实性验证过程。如果区块 1 记录的交易信息与区块 1' 中记录的交易信息相同，则区块 1 的真实性验证通过，执行步骤 S850。如果区块 1 记录的交易信息与区块 1' 中记录的交易信息不同，则结束此次智能合约 1 的调用。

[121]在步骤 S850 中, 将第一区块持久化至目标区块链 420 的智能合约 1 中。

[122]在步骤 S860 中, 目标区块链 720 的区块链节点利用智能合约 1 进行查询, 以确认是不是收到了源区块链 710 中预设数量的区块链节点发送的各自存储的区块 1。

[123]如果是, 可以理解为区块 1 在源区块链 710 中是经过共识的区块, 则执行步骤 S870。如果不是, 则等待转发设备 730 继续迁移源区块链 710 中其他区块链节点存储的区块 1, 即步骤 S880。

[124]在步骤 S870 中, 在智能合约 1 中将已经共识的区块的块高+1, 并且在智能合约 1 中将区块 1 添加在区块列表中。

[125]需要说明的是, 上文结合图 4 至图 5 介绍了本公开实施例中转发某一区块的过程, 如果要迁移源区块链中的全部区块, 可以利用上述过程循环执行, 直到源区块链中的全部区块迁移完成。为了简洁, 在此不再具体赘述。

[126]另外, 如上文介绍, 在验证区块真实性的过程中, 需要维护某一区块包含的全量交易信息, 以便于执行验证方式四。需要说明的是, 为了节约存储空间, 在区块记录的交易信息相同的情况下, 可以仅记录一份区块的全量数据。当然, 在本公开实施例中, 也可以记录源区块链中每个区块链节点存储的区块的交易信息。

[127]上文结合图 1 至图 8, 详细描述了本公开的方法实施例, 下面结合图 9 至图 11, 详细描述本公开的装置实施例。应理解, 方法实施例的描述与装置实施例的描述相互对应, 因此, 未详细描述的部分可以参见前面方法实施例。

[128]图 9 是本公开实施例的区块的迁移装置的示意图。其中, 区块为源区块链中待迁移至目标区块链的第一区块, 所述装置为目标区块链中的区块链节点, 所述目标区块链上存储有第一智能合约, 所述第一智能合约用于对所述源区块链中的区块进行管理, 所述装置 900 包括: 接收模块 910 以及处理模块 920。

[129]接收模块 910, 用于接收所述第一智能合约的第一调用请求, 所述第一调用请求包含所述源区块链中的所述第一区块; 处理模块 920, 用于利用所述第一智能合约, 对所述第一区块的真实性进行验证; 所述处理模块 920, 还用于如果所述第一区块的真实性验证通过, 将所述第一区块存储至所述目标区块链。

[130]在一种可能的实现方式中, 所述目标区块链存储有从所述源区块链中迁移的第二区块, 所述第二区块在所述源区块链中为所述第一区块的上一区块, 所述处理模块, 还用于利用所述第一智能合约, 判断所述第一区块是否为所述第二区块的后继块, 以对所述第一区块的真实性进行验证。

[131]在一种可能的实现方式中, 所述第一智能合约中记录有所述源区块链中区块链节点

约定的区块哈希值的最大值,所述处理模块,还用于利用所述第一智能合约,判断所述第一区块的区块哈希值是否小于所述区块哈希值的最大值,以对所述第一区块的真实性进行验证。

[132]在一种可能的实现方式中,所述源区块链中存储所述第一区块的区块链节点为第一区块链节点,所述第一区块为经过所述第一区块所属的区块链节点数字签名后的区块,所述第一智能合约中记录有所述第一区块链节点的公钥,所述处理模块,还用于利用所述第一智能合约,基于所述第一区块链节点的公钥,判断所述第一区块的数字签名是否为所述第一区块链节点的数字签名,以对所述第一区块的真实性进行验证。

[133]在一种可能的实现方式中,所述第一智能合约中记录有所述源区块链中第二区块链节点存储的第三区块的第一交易信息,在所述源区块链中所述第三区块的块高与所述第一区块的块高相同,所述处理模块,还用于利用所述第一智能合约,对所述第一交易信息与所述第一区块记录的交易信息进行比对,以对所述第一区块的真实性进行验证。

[134]在一种可能的实现方式中,所述接收模块,还用于从所述目标区块链的用户节点接收所述第一智能合约的第二调用请求,所述第二调用请求用于查询所述目标区块链中存储的所述源区块链中的区块。

[135]在一种可能的实现方式中,所述接收模块,还用于从转发设备接收所述第一智能合约的所述第一调用请求,所述转发设备用于将所述第一区块从所述源区块链迁移至所述目标区块链。

[136]在一种可能的实现方式中,所述转发设备为多个转发设备中的一个,所述多个转发设备用于将所述第一区块从所述源区块链迁移至所述目标区块链。

[137]在一种可能的实现方式中,所述处理模块,还用于如果所述第一区块的真实性验证未通过,结束所述第一智能合约的调用进程。

[138]图 10 是本公开实施例的区块的迁移装置的示意图。其中,区块为源区块链中待迁移至目标区块链的第一区块,所述目标区块链上存储有第一智能合约,所述第一智能合约用于对经由转发设备转发的所述源区块链中的区块进行管理。图 10 所述装置 1000 应用于所述转发设备,包括获取模块 1010 以及发送模块 1020。

[139]获取模块 1010,用于从所述源区块链中获取所述第一区块;发送模块 1020,用于向所述目标区块链节点发送所述第一智能合约的第一调用请求,所述第一调用请求包含所述第一区块。

[140]图 11 是本公开另一实施例的装置的示意性框图。图 11 所示的装置 1100 可以包括存储器 1110、处理器 1120、输入/输出接口 1130、收发机 1140。其中,存储器 1110、处理器 1120、输入/输出接口 1130 和收发机 1140 通过内部连接通路相连,该存储器 1110

用于存储指令，该处理器 1120 用于执行该存储器 1110 存储的指令，以控制输入/输出接口 1130 接收输入的数据和信息，输出操作结果等数据，并控制收发机 1140 发送信号。

[141]所述处理器 1120，用于确定用于传输调度请求 SR 的专用的传输资源；所述收发机 1140，用于在所述确定单元确定的所述专用的传输资源上向网络设备发送所述 SR。

[142]应理解，在本公开实施例中，该处理器 1120 可以采用通用的中央处理器（central processing unit, CPU），微处理器，应用专用集成电路（application specific integrated circuit, ASIC），或者一个或多个集成电路，用于执行相关程序，以实现本公开实施例所提供的技术方案。

[143]还应理解，收发机 1140 又称通信接口，使用例如但不限于收发器一类的收发装置，来实现终端 1100 与其他设备或通信网络之间的通信。

[144]该存储器 1110 可以包括只读存储器和随机存取存储器，并向处理器 1120 提供指令和数据。处理器 1120 的一部分还可以包括非易失性随机存取存储器。例如，处理器 1120 还可以存储设备类型的信息。

[145]在实现过程中，上述方法的各步骤可以通过处理器 1120 中的硬件的集成逻辑电路或者软件形式的指令完成。结合本公开实施例所公开的用于请求上行传输资源的方法可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1110，处理器 1120 读取存储器 1110 中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

[146]应理解，本公开实施例中，该处理器可以为中央处理单元（central processing unit, CPU），该处理器还可以是其他通用处理器、数字信号处理器（digital signal processor, DSP）、专用集成电路（application specific integrated circuit, ASIC）、现成可编程门阵列（field programmable gate array, FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[147]应理解，在本公开实施例中，“与 A 相应的 B”表示 B 与 A 相关联，根据 A 可以确定 B。但还应理解，根据 A 确定 B 并不意味着仅仅根据 A 确定 B，还可以根据 A 和/或其它信息确定 B。

[148]应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[149]应理解，在本公开的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本公开实施例的实施过程构成任何限定。

[150]在本公开所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[151]所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[152]另外，在本公开各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[153]在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本公开实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber Line，DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够读取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，数字通用光盘（digital video disc，DVD））或者半导体介质（例如，固态硬盘（solid state disk，SSD））等。

[154]以上所述，仅为本公开的具体实施方式，但本公开的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本公开揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本公开的保护范围之内。因此，本公开的保护范围应以所述权利要求的保护范围为准。

权利要求书

1、一种区块的迁移方法，所述区块为源区块链中待迁移至目标区块链的第一区块，所述方法应用于目标区块链的区块链节点，所述目标区块链上存储有第一智能合约，所述第一智能合约用于对所述源区块链中的区块进行管理，

所述方法包括：

接收所述第一智能合约的第一调用请求，所述第一调用请求包含所述源区块链中的所述第一区块；

利用所述第一智能合约，对所述第一区块的真实性进行验证；

如果所述第一区块的真实性验证通过，将所述第一区块存储至所述目标区块链。

2、如权利要求 1 所述的方法，所述目标区块链存储有从所述源区块链中迁移的第二区块，所述第二区块在所述源区块链中为所述第一区块的上一区块，

所述利用所述第一智能合约，对所述第一区块的真实性进行验证，包括：

利用所述第一智能合约，判断所述第一区块是否为所述第二区块的后继块，以对所述第一区块的真实性进行验证。

3、如权利要求 1 或 2 所述的方法，所述第一智能合约中记录有所述源区块链中区块链节点约定的区块哈希值的最大值，

所述利用所述第一智能合约，对所述第一区块的真实性进行验证，包括：

利用所述第一智能合约，判断所述第一区块的区块哈希值是否小于所述区块哈希值的最大值，以对所述第一区块的真实性进行验证。

4、如权利要求 1-3 中任一项所述的方法，所述源区块链中存储所述第一区块的区块链节点为第一区块链节点，所述第一区块为经过所述第一区块所属的区块链节点数字签名后的区块，所述第一智能合约中记录有所述第一区块链节点的公钥，

所述利用所述第一智能合约，对所述第一区块的真实性进行验证，包括：

利用所述第一智能合约，基于所述第一区块链节点的公钥，判断所述第一区块的数字签名是否为所述第一区块链节点的数字签名，以对所述第一区块的真实性进行验证。

5、如权利要求 1-4 中任一项所述的方法，所述第一智能合约中记录有所述源区块链中第二区块链节点存储的第三区块的第一交易信息，在所述源区块链中所述第三区块的块高与所述第一区块的块高相同，

所述利用所述第一智能合约，对所述第一区块的真实性进行验证，包括：

利用所述第一智能合约，对所述第一交易信息与所述第一区块记录的交易信息进行比对，以对所述第一区块的真实性进行验证。

6、如权利要求 1-5 中任一项所述的方法，所述方法还包括：

从所述目标区块链的用户节点接收所述第一智能合约的第二调用请求，所述第二调用请求用于查询所述目标区块链中存储的所述源区块链中的区块。

7、如权利要求 1-6 中任一项所述的方法，所述接收所述第一智能合约的第一调用请求，包括：

从转发设备接收所述第一智能合约的所述第一调用请求，所述转发设备用于将所述第一区块从所述源区块链迁移至所述目标区块链。

8、如权利要求 7 所述的方法，所述转发设备为多个转发设备中的一个，所述多个转发设备用于将所述第一区块从所述源区块链迁移至所述目标区块链。

9、如权利要求 1-8 中任一项所述的方法，所述方法还包括：

如果所述第一区块的真实性验证未通过，结束所述第一智能合约的调用进程。

10、一种区块的迁移方法，所述区块为源区块链中待迁移至目标区块链的第一区块，所述目标区块链上存储有第一智能合约，所述第一智能合约用于对经由转发设备转发的所述源区块链中的区块进行管理，所述方法应用于所述转发设备，

所述方法包括：

从所述源区块链中获取所述第一区块；

向所述目标区块链节点发送所述第一智能合约的第一调用请求，所述第一调用请求包含所述第一区块。

11、一种区块的迁移装置，所述区块为源区块链中待迁移至目标区块链的第一区块，所述装置为目标区块链中的区块链节点，所述目标区块链上存储有第一智能合约，所述第一智能合约用于对所述源区块链中的区块进行管理，

所述装置包括：

接收模块，用于接收所述第一智能合约的第一调用请求，所述第一调用请求包含所述源区块链中的所述第一区块；

处理模块，用于利用所述第一智能合约，对所述第一区块的真实性进行验证；

所述处理模块，还用于如果所述第一区块的真实性验证通过，将所述第一区块存储至所述目标区块链。

12、如权利要求 11 所述的装置，所述目标区块链存储有从所述源区块链中迁移的第二区块，所述第二区块在所述源区块链中为所述第一区块的上一区块，

所述处理模块，还用于利用所述第一智能合约，判断所述第一区块是否为所述第二区块的后继块，以对所述第一区块的真实性进行验证。

13、如权利要求 11 或 12 所述的装置，所述第一智能合约中记录有所述源区块链中区块链节点约定的区块哈希值的最大值，

所述处理模块，还用于利用所述第一智能合约，判断所述第一区块的区块哈希值是否小于所述区块哈希值的最大值，以对所述第一区块的真实性进行验证。

14、如权利要求 11-13 中任一项所述的装置，所述源区块链中存储所述第一区块的区块链节点为第一区块链节点，所述第一区块为经过所述第一区块所属的区块链节点数

字签名后的区块, 所述第一智能合约中记录有所述第一区块链节点的公钥,

所述处理模块, 还用于利用所述第一智能合约, 基于所述第一区块链节点的公钥, 判断所述第一区块的数字签名是否为所述第一区块链节点的数字签名, 以对所述第一区块的真实性进行验证。

15、如权利要求 11-14 中任一项所述的装置, 所述第一智能合约中记录有所述源区块链中第二区块链节点存储的第三区块的第一交易信息, 在所述源区块链中所述第三区块的块高与所述第一区块的块高相同,

所述处理模块, 还用于利用所述第一智能合约, 对所述第一交易信息与所述第一区块记录的交易信息进行比对, 以对所述第一区块的真实性进行验证。

16、如权利要求 11-15 中任一项所述的装置, 所述接收模块, 还用于

从所述目标区块链的用户节点接收所述第一智能合约的第二调用请求, 所述第二调用请求用于查询所述目标区块链中存储的所述源区块链中的区块。

17、如权利要求 11-16 中任一项所述的装置, 所述接收模块, 还用于从转发设备接收所述第一智能合约的所述第一调用请求, 所述转发设备用于将所述第一区块从所述源区块链迁移至所述目标区块链。

18、如权利要求 17 所述的装置, 所述转发设备为多个转发设备中的一个, 所述多个转发设备用于将所述第一区块从所述源区块链迁移至所述目标区块链。

19、如权利要求 11-18 中任一项所述的装置, 所述处理模块, 还用于如果所述第一区块的真实性验证未通过, 结束所述第一智能合约的调用进程。

20、一种区块的迁移装置, 所述区块为源区块链中待迁移至目标区块链的第一区块, 所述目标区块链上存储有第一智能合约, 所述第一智能合约用于对经由转发设备转发的所述源区块链中的区块进行管理, 所述装置应用于所述转发设备,

所述装置包括:

获取模块, 用于从所述源区块链中获取所述第一区块;

发送模块, 用于向所述目标区块链节点发送所述第一智能合约的第一调用请求, 所述第一调用请求包含所述第一区块。

21、一种区块的迁移装置, 包括存储器和处理器, 所述存储器中存储有可执行代码, 所述处理器被配置为执行所述可执行代码, 以实现权利要求 1-9 中任一项所述的方法。

22、一种区块的迁移装置, 包括存储器和处理器, 所述存储器中存储有可执行代码, 所述处理器被配置为执行所述可执行代码, 以实现权利要求 10 所述的方法。