

一种区块链的交易方法和装置

技术领域

[01] 本说明书涉及计算机网络技术领域，尤其涉及一种区块链的交易方法和装置。

背景技术

- 5 [02] 区块链技术，也被称之为分布式账本技术，是一种由若干台计算设备共同参与“记账”，共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性，使得区块链技术已在众多的领域中广泛的进行应用。

发明内容

- 10 [03] 针对以上提出的区块链技术现状，本说明书提供了一种区块链的交易方法，所述交易发起方的账户对应多个公钥，所述方法包括：
- [04] 接收所述发起方节点设备发送的目标交易，所述目标交易包括交易内容和所述账户的若干公钥对应的私钥基于至少部分的所述交易内容而作的数字签名；
- [05] 验证所述目标交易，以在所述验证通过后根据所述区块链的共识规则将所述目标交易收录于所述区块链的分布式数据库，其中，所述验证包括验证所述数字签名是否合法。
- 15 [06] 在又一示出的实施例中，所述账户中的多个公钥分别对应预设交易权重；
- [07] 所述验证还包括验证作出合法数字签名的私钥对应的公钥的预设交易权重之和是否满足预设权重阈值。
- [08] 在又一示出的实施例中，所述交易内容包括所述预设权重阈值。
- 20 [09] 在又一示出的实施例中，所述交易内容还包括所述账户的若干公钥对应的目标交易权重，所述若干公钥对应的目标交易权重不大于所述若干公钥在所述账户中对应的预设交易权重；
- [10] 所述验证作出合法数字签名的私钥对应的公钥的预设交易权重之和是否满足预设权重阈值，包括：

[11]验证作出合法数字签名的私钥对应的公钥的目标交易权重之和是否满足预设权重阈值。

[12]在又一示出的实施例中，所述交易发起方的账户的标识为基于所述发起方的名称获得的唯一性标识。

5 [13]相应的，本说明书还提供了一种区块链的交易装置，所述交易发起方的账户对应多个公钥，所述装置包括：

[14]接收单元，接收所述发起方节点设备发送的目标交易，所述目标交易包括交易内容和所述账户的若干公钥对应的私钥基于至少部分的所述交易内容而作的数字签名；

10 [15]验证单元，验证所述目标交易，以在所述验证通过后根据所述区块链的共识规则将所述目标交易收录于所述区块链的分布式数据库，其中，所述验证包括验证所述数字签名是否合法。

[16]在又一示出的实施例中，所述账户中的多个公钥分别对应预设交易权重；

[17]所述验证单元：

15 [18]验证作出合法数字签名的私钥对应的公钥的预设交易权重之和是否满足预设权重阈值。

[19]在又一示出的实施例中，所述交易内容包括所述预设权重阈值。

[20]在又一示出的实施例中，所述交易内容还包括所述账户的若干公钥对应的目标交易权重，所述若干公钥对应的目标交易权重不大于所述若干公钥在所述账户中对应的预设交易权重；

20 [21]所述验证单元：

[22]验证作出合法数字签名的私钥对应的公钥的目标交易权重之和是否满足预设权重阈值。

[23]在又一示出的实施例中，所述交易发起方的账户的标识为基于所述发起方的名称获得的唯一性标识。

25 [24]本说明书还提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述区块链的交易方法所述的步骤。

[25]本说明书还提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述区块链的交易方法所述的步骤。

- [26]由以上技术方案可见，本说明书提供的区块链的交易方法及装置，用户账户可以对应多个公钥（或公私钥对），不仅可以有效降低账户丢失的风险，而且对应任何一笔交易，上述多个公钥（或公私钥对）背后的实体可以通过数字签名的方式实现投票解决，使得每一笔账户发起的交易都是多方共识后的结果，因此基于以上技术方案的账户体系在多方合作场景中有很大的应用空间。

附图说明

- [27]图1为本说明书所提供的一实施例所示的区块链的交易方法的流程图；
- 10 [28]图2为本说明书一示例性实施例提供的用户账户在区块链分布式数据库中的状态示意图；
- [29]图3为本说明书所提供的一实施例提供的区块链的交易装置的示意图；
- [30]图4为运行本说明书所提供的区块链的交易装置实施例的一种硬件结构图。

具体实施方式

- 15 [31]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。
- 20 [32]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。
- 25 [33]传统区块链的用户账户通常对应有一个有效的公钥（或一对有效的公钥-私钥对），上述有效的公钥被显示在区块链用户的账户状态中，或以其他形式存储在区块链的分布式数据库中，且可被区块链上的任一节点设备获得；与上述有效的公钥对应的私钥则保

存在用户节点设备的本地数据库或其他硬件终端中，以供用户进行数字签名或其他与私钥相关的加密或解密操作。当保存上述私钥的文件或硬件终端遗失或失密后，上述区块链账户则不能再被该用户使用以发起任何交易，甚至上述区块链账户内的虚拟资源也可能会被盗取。

- 5 [34]基于以上现有技术中存在的问题，如图1所示，本说明书一示意性实施例提供了一种区块链的交易方法，所述交易发起方的账户对应有多个公钥，所述多个公钥由多个私钥生成。

- 10 [35]本实施例所述的区块链，具体可指一个各节点设备通过共识机制达成的、具有分布式数据存储结构的P2P网络系统，该区块链内的数据分布在时间上相连的一个个“区块（block）”之内，后一区块包含前一区块的数据摘要，且根据具体的共识机制（如POW、POS、DPOS或PBFT等）的不同，达成全部或部分节点设备的数据全备份。本领域的技术人员熟知，由于区块链系统在相应共识机制下运行，已收录至区块链数据库内的数据很难被任意的节点篡改，例如采用Pow共识的区块链，至少需要全网51%算力的攻击才有可能篡改已有数据，因此区块链系统有着其他中心化数据库系统所法比拟的保证
15 数据安全、防攻击篡改的特性。

[36]值得注意的是，本说明书所述的节点设备，不仅可包括备份有区块链的分布式数据库的全量数据的全节点设备，还可包括备份有区块链的分布式数据库的部分数据的轻节点设备，以及其他的终端设备或客户端，在本说明书中不做限定。

- 20 [37]本实施例所述的交易发起方的账户对应有多个公钥，由于公钥与私钥也是一一对应关系，所述上述“交易发起方的账户对应有多个公钥”也可被理解为“交易发起方的账户对应有多个公钥-私钥对”。上述交易发起方的账户对应的多个公钥或公钥-私钥对可以作为该交易发起方用户的多个备用身份，以防止个别私钥遗失或失密，保证账户安全；也可以作为该交易发起方用户相关或管理的多个实体身份，由该多个实体共同代表上述交易发起方用户。

- 25 [38]上述公钥-私钥的生成算法在此不作限定，可以由私钥基于非对称加密算法（如RSA或椭圆曲线算法等）计算得出相应的公钥，也可以是基于加密算法共同得出的一对密钥等。

[39]本领域的技术人员熟知，公钥作为可公开的密钥，可以被存储在区块链的分布式数据库中，或显示在区块链的用户账户状态中；而相应的私钥则可存储在交易发起方用户

的节点设备的本地数据库中。在本实施例中，为保证私钥的安全性，防止遗失或失密，上述多个公钥对应的多个私钥可以保存在多个不同的节点设备的本地数据库或硬件终端中；尤其是当上述多个公钥（或公钥-私钥对）代表该交易发起方用户相关或管理的多个实体身份时，为保证上述多个实体公平决策，上述多个私钥更应保存在上述多个实体所在的节点设备的本地数据库中，或多个硬件终端中，由上述多个实体各自持有。

[40]如图 1 所示，上述区块链的交易方法包括：

[41]步骤 102，接收所述发起方节点设备发送的目标交易，所述目标交易包括交易内容和所述账户的若干公钥对应的私钥基于至少部分的所述交易内容而作的数字签名。

[42]在本说明书中所描述的交易（transaction），是指用户通过区块链的节点设备创建，并需要最终发布至区块链的分布式数据库中的一笔数据。其中，区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔任意的数据：例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求；又如，在账户型的区块链中，该交易还可以是用户向区块链发送的、用以更改用户的账户状态的数据（如账户余额等）。因此，只要是用户向区块链的分布式数据库发布的任意数据，无论该任意数据被保存在区块的区块体、区块头还是其他位置，均可属于本发明所述的“交易”。

[43]上述账户的若干公钥对应的私钥基于至少部分的所述交易内容而作的数字签名，可以是上述账户的一个公钥对应的私钥基于至少部分的所述交易内容而作的一个数字签名，也可以是上述账户的多个公钥对应的私钥基于至少部分的所述交易内容而作的多重数字签名。上述多重数字签名可以是上述多个私钥基于至少部分的上述交易内容分别所作的多个数字签名；也可以是上述多个私钥按照预设的签名顺序、基于其上一私钥所作的数字签名而叠加所作的数字签名；也可以兼顾上述两种签名方式，上述多个私钥的一部分私钥分别做多个数字签名，一部分私钥进行按照预设的签名顺序、基于其上一私钥所作的数字签名而叠加进行数字签名，还可以是按照其他预设的签名顺序或方式进行的数字签名，在此不做限定。上述多重数字签名既可以是由上述交易发起方账户对应的所有私钥作出的，也可以是由上述交易发起方账户对应的部分私钥作出的，在此也不做限

定。

[44]另外值得注意的是，上述目标交易的交易内容部分在一些特殊的业务场景下可以为空，即不在目标交易中显示；而数字签名部分则是上述账户的至少一个公钥对应的私钥基于未在目标交易中显示的交易内容而作出的。

- 5 [45]步骤 104，验证所述目标交易，以在所述验证通过后根据所述区块链的共识规则将所述目标交易收录于所述区块链的分布式数据库，其中，所述验证包括验证所述数字签名是否合法。

- 10 [46]基于上述区块链协议的关于交易验证规则的具体设置，区块链的节点设备对上述目标交易的验证至少可以包括对上述目标交易包括的数字签名的合法性进行验证，上述合法性验证通常可包括验证上述数字签名的签名方公钥是否隶属于上述交易发起方的账户，上述数字签名是否按照预设的签名顺序进行签署，上述数字签名是否基于上述交易内容而获得，等等，以确保该目标交易是由交易发起方用户或交易发起方账户中若干公钥对应的实体生成并发送的，防止其他方的恶意篡改或攻击。上述对目标交易的验证还可包括对目标交易的数据内容格式验证、该交易是否为重放交易等等，在此不作限定。

- 15 [47]上述区块链所基于的共识规则不同，将上述通过验证的目标交易收录于区块链的分布式数据库中的具体过程也不尽相同。在一示出的实施例，所述将上述通过验证的目标交易收录于区块链的分布式数据库中的具体过程，包括：

[48]所述区块链中具有记账权限的节点将通过验证的所述目标交易加入到候选区块；

[49]从所述具有记账权限的节点中确定满足所述区块链共识规则的共识记账节点；

- 20 [50]所述共识记账节点向所述区块链的节点广播所述候选区块；

[51]在所述候选区块通过所述区块链符合预设数量的节点的验证认可后，所述候选区块被视为最新区块，加入到所述区块链的分布式数据库中。

- [52]在上述的实施例，具有记账权限的节点是指具有生成候选区块权限的节点。根据所述区块链的共识规则，可从上述对所述候选区块具有记账权限的节点中确定共识记账节点，上述共识规则可以包括工作量证明机制（PoW）、或权利证明机制（PoS）、或股份授权证明机制（DPoS）、或拜占庭容错算法规则（PBFT）、或区块链协议规定的其他具体的共识规则。
- 25

[53]上述实施例提供的区块链的交易方法，用户账户可以对应多个公钥（或公私钥对），

不仅可以有效降低账户丢失的风险，而且对应任何一笔交易，上述多个公钥（或公私钥对）背后的用户或实体可以通过多重签名的方式实现投票解决，使得每一笔账户发起的交易都是多方共识后的结果，因此基于以上技术方案的账户体系在多方合作场景中有很大的应用空间。

- 5 [54]在又一示出的实施例中，上述交易发起方账户还为其对应的多个公钥（或公钥-私钥对）对应设置了预设交易权重，用以表征每个公钥（或公钥-私钥对）所代表的实体在代表上述交易发起方用户决策中的表决权权重。上述预设交易权重在用户的区块链账户状态中可以用百分比表示，也可以用其他数值或指数或因数表示。

- 10 [55]相应的，该目标交易应对应设置一预设权重阈值，以在对目标交易的验证中，查验作出合法数字签名的私钥（或该私钥对应的公钥）对应的预设交易权重之和是否满足预设权重阈值：满足时通过该项验证。上述合法性数字签名对应的交易权重之和大于预设的权重阈值，表示在该账户中同意该目标交易的交易内容的公钥或实体所占的决策权重之和大于预设的阈值，则该交易内容应被通过。上述为账户中的多个公钥设置相应的预设交易权重，体现了该多个公钥所代表的多个实体的决策分量或表决能力，上述决策分量或表决能力通过该多个实体利用相应的私钥对目标交易的交易内容所作的合法数字签名得以体现，因此本技术方案在该区块链账户进行去中心化决策中有着广泛的应用。

- 15 [56]设置上述预设权重阈值的方式可以有多种，例如区块链系统可在底层协议代码中为目标交易设置权重阈值，不同类型的目标交易可以设置不同的预设权重阈值；或者区块链用户可为自身账户发出的每个目标交易分别设置预设权重阈值，还可将每个目标交易对应的预设权重阈值收录在交易内容中等方式，在此不做限定。

[57]图2示意了本说明书一示例性实施例中提供的用户账户在区块链分布式数据库中的状态，其中，Nonce 为防止重放攻击而严格随发出交易递增的交易序列号；Balance 为账户持有的虚拟资源的数量；CodeHash 为该账号智能合约代码摘要值；PublicKey：为账户对应的公钥；StorageHash 为账户状态内容组成的默克尔树根的哈希值。

- 25 [58]如图2所示，该用户账户内对应应有多个公钥：公钥1至6，且上述公钥1至6分别对应应有预设交易权重：10%，10%，20%，20%，30%，10%。可选的，上述公钥1至6的预设交易权重还可以表示为：1,1,2,2,3,1 或 a,a,2a,2a,3a,a 等各种形式。

[59]例如，当一目标交易的交易内容中包含的预设权重阈值为70%或7或7a时，如果在目标交易中查验到作出合法性数字签名的私钥对应的公钥为公钥1至5，由于公钥1至

5 的权重之和为 90%或 9 或 9a, 大于上述预设权重阈值, 则对该目标交易的决策权重的验证应通过。

[60]在又一示出的实施方式中, 为保证上述区块链账户所对应的多个实体在进行交易或决策时的灵活性, 所述交易内容还可包括所述账户的若干公钥对应的目标交易权重; 而且为了保证决策的公平性, 所述每个公钥对应的目标交易权重不大于所述每个公钥在所述账户中对应的预设交易权重, 亦即对上述目标交易作出数字签名的多个实体, 可以在该目标交易中体现出特定的决策权重, 但是为公平起见, 每个实体为目标交易所体现的特定的决策权重不能大于经区块链节点共识所确定的用户区块链账户中所规定的预设交易权重。

10 [61]相应的, 在执行对所述目标交易的决策权重验证时, 应验证作出合法数字签名的私钥对应的公钥的目标交易权重之和是否满足预设权重阈值, 在满足时, 上述目标交易通过该项验证。

[62]传统区块链系统的账户标识 (即账户地址) 由无具体语意的若干字节 (例如以太坊是 20 字节) 表示的, 并且账户和私钥、公钥存在严格的数学递推关系: 传统区块链系统通过非对称加密算法生成公钥-私钥对, 私钥可以推出公钥, 账户地址再通过公钥计算得到。以以太坊为例, 以太坊的账户地址是通过 Keccak-256 哈希算法基于公钥得到的 20 字节编码, 并用 40 位 16 进制表示, 诸如这种格式: 0x9bA5552cCc83A65A84CFE389B50bb1D4E8AdF9。这种格式对使用者是极不友好的, 毫无任何语意的账户地址不仅易容被遗忘, 而且在具体的业务场景中加大了使用的复杂性。

[63]在本说明书提供的上述一个或多个实施例中, 交易发起方的区块链账户对应多个公钥 (或公钥-私钥对), 每个公钥 (或公钥-私钥对) 可以代表与该交易发起方用户相关的一个实体, 以使该交易发起方用户可以代表一个机构、组织、公司、家庭等等。相比于传统的区块链账户, 上述各实施例中用户的区块链账户已经可以与特定的公钥解耦, 因此本说明书提供的各实施例中, 交易发起方的区块链账户标识可以选用一些更加用户友好的表达, 例如, 所述交易发起方的账户的标识为基于所述发起方的名称获得的唯一性标识, 以方便记忆及使用上述发起方账户, 如图 2 所示的用户的账户名称 (或者可称为账户地址等其他账户标识) ant financial; 又如, 上述账户标识也可能是基于所述发起方的名称而作出的数字摘要等等, 在此不做限定。

30 [64]与上述流程实现对应, 本说明书的实施例还提供了一种区块链的交易装置。该装置

可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为逻辑意义上的装置，是通过所在设备的 CPU(Central Process Unit, 中央处理器)将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，除了图 4 所示的 CPU、内存以及存储器之外，网络风险业务的实现装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件，和/或用于实现网络通信功能的板卡等其他硬件。

[65]图 3 所示为一种区块链的交易装置 30，所述交易发起方的账户对应有多个公钥，所述装置 30 包括：

[66]接收单元 302，接收所述发起方节点设备发送的目标交易，所述目标交易包括交易内容和所述账户的若干公钥对应的私钥基于至少部分的所述交易内容而作的数字签名；

10 [67]验证单元 304，验证所述目标交易，以在所述验证通过后根据所述区块链的共识规则将所述目标交易收录于所述区块链的分布式数据库，其中，所述验证包括验证所述数字签名是否合法。

[68]在又一示出的实施例中，所述账户中的多个公钥分别对应有预设交易权重；

[69]所述验证单元 304：

15 [70]验证作出合法数字签名的私钥对应的公钥的预设交易权重之和是否满足预设权重阈值。

[71]在又一示出的实施例中，所述交易内容包括所述预设权重阈值。

[72]在又一示出的实施例中，所述交易内容还包括所述账户的若干公钥对应的目标交易权重，所述若干公钥对应的目标交易权重不大于所述若干公钥在所述账户中对应的预设交易权重；

20

[73]所述验证单元 304：

[74]验证作出合法数字签名的私钥对应的公钥的目标交易权重之和是否满足预设权重阈值。

[75]在又一示出的实施例中，所述交易发起方的账户的标识为基于所述发起方的名称获得的唯一性标识。

25

[76]上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，相关之处参见方法实施例的部分说明即可，在此不再赘述。

[77]以上所描述的装置实施例仅仅是示意性的，其中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模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部单元或模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

5 [78]上述实施例阐明的装置、单元、模块，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

10 [79]与上述方法实施例相对应，本说明书的实施例还提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中区块链的交易方法的各个步骤。对区块链的交易方法的各个步骤的详细描述请参见之前的内容，不再重复。

[80]与上述方法实施例相对应，本说明书的实施例还提供了一种计算机可读存储介质，
15 该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中所述的区块链的交易方法的各个步骤。对区块链的交易方法的各个步骤的详细描述请参见之前的内容，不再重复。

[81]以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的
20 范围之内。

[82]在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[83]内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的
25 示例。

[84]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。

[85]计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储

器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带, 磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算设备访问的信息。按照本文中的界定, 计算机可读介质不包括暂存电脑可读媒体(transitory media), 如调制的数据信号和载波。

[86]还需要说明的是, 术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含, 从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素, 而且还包括没有明确列出的其他要素, 或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下, 由语句“包括一个...”限定的要素, 并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[87]本领域技术人员应明白, 本说明书的实施例可提供为方法、系统或计算机程序产品。因此, 本说明书的实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且, 本说明书的实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

权利要求书

1、一种区块链的交易方法，所述交易发起方的账户对应有多个公钥，所述方法包括：

接收所述发起方节点设备发送的目标交易，所述目标交易包括交易内容和所述账户的若干公钥对应的私钥基于至少部分的所述交易内容而作的数字签名；

验证所述目标交易，以在所述验证通过后根据所述区块链的共识规则将所述目标交易收录于所述区块链的分布式数据库，其中，所述验证包括验证所述数字签名是否合法。

2、根据权利要求1所述的方法，所述账户中的多个公钥分别对应有预设交易权重；所述验证还包括验证作出合法数字签名的私钥对应的公钥的预设交易权重之和是否满足预设权重阈值。

3、根据权利要求2所述的方法，所述交易内容包括所述预设权重阈值。

4、根据权利要求2或3所述的方法，所述交易内容还包括所述账户的若干公钥对应的目标交易权重，所述若干公钥对应的目标交易权重不大于所述若干公钥在所述账户中对应的预设交易权重；

所述验证作出合法数字签名的私钥对应的公钥的预设交易权重之和是否满足预设权重阈值，包括：

验证作出合法数字签名的私钥对应的公钥的目标交易权重之和是否满足预设权重阈值。

5、根据权利要求1所述的方法，所述交易发起方的账户的标识为基于所述发起方的名称获得的唯一性标识。

6、一种区块链的交易装置，所述交易发起方的账户对应有多个公钥，所述装置包括：

接收单元，接收所述发起方节点设备发送的目标交易，所述目标交易包括交易内容和所述账户的若干公钥对应的私钥基于至少部分的所述交易内容而作的数字签名；

验证单元，验证所述目标交易，以在所述验证通过后根据所述区块链的共识规则将所述目标交易收录于所述区块链的分布式数据库，其中，所述验证包括验证所述数字签名是否合法。

7、根据权利要求6所述的装置，所述账户中的多个公钥分别对应有预设交易权重；所述验证单元：

验证作出合法数字签名的私钥对应的公钥的预设交易权重之和是否满足预设权重阈值。

8、根据权利要求 7 所述的装置，所述交易内容包括所述预设权重阈值。

9、根据权利要求 7 或 8 所述的装置，所述交易内容还包括所述账户的若干公钥对应的目标交易权重，所述若干公钥对应的目标交易权重不大于所述若干公钥在所述账户中对应的预设交易权重；

5 所述验证单元：

验证作出合法数字签名的私钥对应的公钥的目标交易权重之和是否满足预设权重阈值。

10、根据权利要求 6 所述的装置，所述交易发起方的账户的标识为基于所述发起方的名称获得的唯一性标识。

10 11、一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 1 到 5 任意一项所述的方法。

12、一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求 1 到 5 任意一项所述的方法。