(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109450638 A
(43)申请公布日 2019.03.08

(21)申请号 201811236595.5

(22)申请日 2018.10.23

(71)申请人 国科赛思(北京)科技有限公司
地址 100085 北京市海淀区安宁庄西路9号院29号楼5层507室

(72)发明人 李自豪

(74)专利代理机构 北京市商泰律师事务所 11255
代理人 黄晓军

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

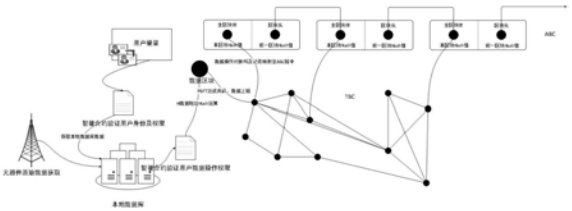
权利要求书2页 说明书11页 附图5页

(54)发明名称

基于区块链的电子元器件数据管理系统及方法

(57)摘要

本发明公开了一种基于区块链的电子元器件数据管理系统,属于通信系统数据管理技术领域,包括账户区块链,用于存储用户基本信息及用户间关系、权限信息;交易区块链,用于存储数据操作信息;注册模块,用于系统初始化和密钥生成,获取用户注册申请后,核实用户身份并完成用户注册,使该用户成为系统合法节点;数据存储模块将数据提供方将电子元器件数据附上数字签名和时间戳进行加密存储至合法节点。本发明存储元器件数据的区块链以联盟链的方式进行部署,节约了存储空间,同时PBFT机制的应用避免了大规模计算;实现了电子元器件整个生命周期所有相关数据的完整性和可追溯性,降低了生产成本缩短了产品装备的研制生产时间和科学研究的任务进程。



CN 109450638 A

1.一种基于区块链的电子元器件数据管理系统,其特征在于,包括:

账户区块链,用于存储用户基本信息及用户间关系、权限信息;

交易区块链,用于存储数据操作信息;

注册模块,用于系统初始化和密钥生成,获取用户注册申请后,核实用户身份并完成用户注册,使该用户成为系统合法节点,所述用户包括数据提供方和数据需求方;

数据存储模块,用于数据提供方将电子元器件数据附上数字签名和时间戳进行加密存储至合法节点。

2.根据权利要求1所述的基于区块链的电子元器件数据管理系统,其特征在于:

所述账户区块链,建立用户索引链,根据不同用户的基本信息通过哈希算法以生成具有唯一标识ID,同时保存该用户的智能合约,完成每一个用户的登记注册和权限设置。

3.根据权利要求1所述的基于区块链的电子元器件数据管理系统,其特征在于:

所述交易区块链,用于建立元器件数据链,将不同用户的电子元器件数据信息存储地址密钥、数据摘要及数据操作操作信息记录至一个区块中,并将该区块的绝对地址与该数据数据提供方建立映射关系,同时将映射结果记录到数据请求方的索引链所在的区块中。

4.一种基于区块链的电子元器件数据管理方法,其特征在于:进行电子元器件数据存储时,该存储过程包括如下步骤:

步骤S110:利用注册模块对系统初始化和用户注册;

步骤S120:上传数据,电子元器件数据提供方将电子元器件数据附上数字签名及时间戳加密存储至本地数据库或云中;

步骤S130:数据操作信息共识;

步骤S140:利用数据存储模块将数据操作记录和数据提供方对应索引映射至账户区块链的合法节点中保存。

5.根据权利要求4所述的基于区块链的电子元器件数据管理方法,其特征在于,所述系统初始化和用户注册具体包括:

通过Boneh-Boyen短签名技术初始化系统,用户申请加入系统,管理员核实其身份并完成基本信息注册后,用户将获取用于加密数据的公钥集合、验证身份唯一性的私钥和证书,成为系统的合法结点。

6.根据权利要求5所述的基于区块链的电子元器件数据管理方法,其特征在于,在步骤S120中,用户登录系统并发送数据上链请求,该请求包含节点i即用户当前使用的证书$Cert_i$和数字签名Sig_i,TBC节点BS_j收到请求后将根据证书和签名核实验证节点身份的合法性和有效性,以确保数据来源真实可靠;当节点身份验证准确无误时,BS_j节点回应其数据上传请求,节点i将使用当前公钥PK_i加密数据保存地址Add_i得到Add_{Enc_i},并集合加密的数字签名和时间戳;最后利用BS_j节点公钥再次加密上述集合,得到最终上传数据Record,BS_j节点验证数据的有效性,如果数据安全有效,则将Record写入BS_j中,具体过程如下:

$$i \to BS_j : \mathrm{Record} = \mathrm{E}_{PK_{BS_j}}\left(Add_{Enc_i} \mid Cert_i \mid Sig_{Enc_i} \mid timestamp_i\right),$$

$$where\ \ Add_{Esc_i} = \mathrm{E}_{PK_i}\left(Add_i \mid timestamp_i\right), \mathrm{Sig}_{Esc_i} = Sign_{SK_i}\left(Add_{Esc_i}\right)$$

其中,i为账户区块链数据请求方节点,BS_j为交易区块链数据提供方节点,$E_{PK_i}(m)$运算

表示使用i的公钥加密信息m，Add_{Enc_i}表示由节点i公钥加密后的数据地址，$Cert_i$表示节点i的证书，Sig_{Enc_i}表示由节点i签名的信息，$timestamp_i$表示节点i的时间戳，Add_i表示节点i存储数据的地址，$Sign_{SK_i}(m)$运算表示使用i的私钥对信息m进行数字签名。

7.根据权利要求6所述的基于区块链的电子元器件数据管理方法，其特征在于，在所述数据操作信息共识过程中，节点BS_j将数据操作广播至临近节点，并由拜占庭容错机制PBFT算法达成共识。

8.根据权利要求4所述的基于区块链的电子元器件数据管理方法，其特征在于，进行电子元器件数据共享操作时，该共享过程包括如下步骤：

步骤S210：数据访问请求；

步骤S220：智能合约执行；

步骤S230：请求数据发送，数据提供方节点N_i将数据地址发送至数据请求方节点N_m中，同时向全网广播操作信息；

步骤S240：访问指定数据，数据请求方节点N_m收到加密的数据地址后，利用自身的私钥进行解密，最后读取数据。

9.根据权利要求8所述的基于区块链的电子元器件数据管理方法，其特征在于，在所述数据访问请求中，数据请求方节点N_m向数据提供方节点N_i发出数据获取请求Req，请求中包含数据访问目的、访问时间和访问次数信息，节点N_i查验节点N_m身份后，针对节点N_m制定访问约束条件Con，授权访问，并将访问约束条件和被访问数据块对应的私钥SK_i发送给对应交易区块链上区块BS_j，如下所示：

$$N_i \rightarrow N_m : \mathrm{Re}q = E_{PK_{N_i}}\left(\mathrm{Request} \mid \mathrm{Cert}_{N_m} \mid timestramp\right)$$

$$N_m \rightarrow BS_j : Message = E_{PK_{BS_j}}\left(Constra\,\mathrm{int}s \mid SK_i \mid PK_{N_m} \mid timestranp \mid Cert_{N_i}\right)。$$

10.根据权利要求9所述的基于区块链的电子元器件数据管理方法，其特征在于，在所述智能合约执行中，节点BS_j验证信息后，执行智能合约，根据节点设定的访问约束条件锁定脚本，并利用节点BS_j的私钥解密数据地址Add_{Enc_i}，同时根据提供的对称密钥SK_i，解密数据地址Add_i，最后使用访问节点N_m的公约对请求数据进行非对称加密，输出结果。

基于区块链的电子元器件数据管理系统及方法

技术领域

[0001] 本发明涉及通信系统数据管理技术领域，具体涉及一种基于区块链的电子元器件数据管理系统及管理方法。

背景技术

[0002] 目前在电子元器件选用、采购、监制验收、筛选复验、失效分析阶段元器件质量管理缺乏统一的标准和规范，同时信息不连通、不对称，各部门机构间缺少有效、顺畅的信息共享，针对科研院所、生产厂商等元器件数据信息封闭、不流通等问题，现有的技术方案一般包括：(1)各个机构、部门独自开发管理私有的数据存储系统，用户通过调用API获取各个部门的数据；(2)各个部门、机构将拥有的数据上传至中心平台统一管理，用户通过访问平台获取相关数据。

[0003] 现有数据分享方式(1)中各个部门数据独立保存，各部门间数据互不连通，存在数据孤岛问题，而且各个部门需要独立维护其API，成本较高。此外，由于数据标准规范不统一，各个部门、各个机构执行独立的规范标准，这将导致数据规范性差，流通慢。

[0004] 现有数据分享方式(2)虽然一定程度上解决了数据孤岛的问题，然而数据中心化问题又随之凸显，电子数据的安全性、隐私性受到威胁。此外，相关部门分享了核心数据，然而往往无法从数据中心获取价值数据，信息不对称问题愈发严重。当存在多个中心平台时，他们相互间往往存在一定的竞争关系，各平台为保证客户存量，也通常会互不兼容，数据间互不共享。现有的技术方案对于隐私和数据安全的要求均不能得到很好的保证和满足。

发明内容

[0005] 本发明的目的在于提供一种基于区块链的电子元器件数据管理系统，以解决上述背景技术中存在的技术问题。

[0006] 为了实现上述目的，本发明采取了如下技术方案：

[0007] 本发明提供一种基于区块链的电子元器件数据管理系统，该系统包括：

[0008] 账户区块链，用于存储用户基本信息及用户间关系、权限信息；

[0009] 交易区块链，用于存储数据操作信息；

[0010] 注册模块，用于系统初始化和密钥生成，获取用户注册申请后，核实用户身份并完成用户注册，使该用户成为系统合法节点，所述用户包括数据提供方和数据需求方；

[0011] 数据存储模块，用于数据提供方将电子元器件数据附上数字签名和时间戳进行加密存储至合法节点。

[0012] 进一步的，所述账户区块链建立用户索引链，根据不同用户的基本信息通过哈希算法以生成具有唯一标识ID，同时保存该用户的智能合约，完成每一个用户的登记注册和权限设置。

[0013] 进一步的，所述交易区块链建立元器件数据链，将不同用户的电子元器件数据信息存储地址密钥、数据摘要及数据操作操作信息记录至一个区块中，并将该区块的绝对地

址与该数据数据提供方建立映射关系，同时将映射结果记录到数据请求方的索引链所在的区块中。

[0014] 进一步的，进行电子元器件数据存储时，该存储过程包括如下步骤：

[0015] 步骤S110：系统初始化和用户注册；

[0016] 步骤S120：上传数据，电子元器件数据提供方将电子元器件数据附上数字签名及时间戳加密存储至本地数据库或云中；

[0017] 步骤S130：数据操作信息共识；

[0018] 步骤S140：将数据操作记录和数据提供方对应索引映射至账户区块链的合法节点中保存。

[0019] 进一步的，所述系统初始化和用户注册具体包括：

[0020] 通过Boneh-Boyen短签名技术初始化系统，用户申请加入系统，管理员核实其身份并完成基本信息注册后，用户将获取用于加密数据的公钥集合、验证身份唯一性的私钥和证书，成为系统的合法结点。

[0021] 进一步的，在步骤S120中，用户登录系统并发送数据上链请求，该请求包含节点i即用户当前使用的证书$Cert_i$和数字签名Sig_i，TBC节点BS_j收到请求后将根据证书和签名核实验证节点身份的合法性和有效性，以确保数据来源真实可靠；当节点身份验证准确无误时，BS_j节点回应其数据上传请求，节点i将使用当前公钥PK_i加密数据保存地址Add_i得到Add_{Enc_i}，并集合加密的数字签名和时间戳；最后利用BS_j节点公钥再次加密上述集合，得到最终上传数据Record，BS_j节点验证数据的有效性，如果数据安全有效，则将Record写入BS_j中，具体过程如下：

[0022] $$i \to BS_j : \mathrm{Record} = \mathrm{E}_{PK_{BS_j}}\left(Add_{Enc_i} \mid Cert_i \mid Sig_{Enc_i} \mid timestamp_i\right),$$

[0023] $$where\ \ Add_{Esc_i} = \mathrm{E}_{PK_i}\left(Add_i \mid timestamp_i\right), \mathrm{Sig}_{Esc_i} = Sign_{SK_i}\left(Add_{Esc_i}\right)$$

[0024] 其中，i为账户区块链数据请求方节点，BS_j为交易区块链数据提供方节点，$E_{PK_i}(m)$运算表示使用i的公钥加密信息m，Add_{Enc_i}表示由节点i公钥加密后的数据地址，$Cert_i$表示节点i的证书，Sig_{Enc_i}表示由节点i签名的信息，$timestamp_i$表示节点i的时间戳，Add_i表示节点i存储数据的地址，$Sign_{SK_i}(\mathrm{m})$运算表示使用i的私钥对信息m进行数字签名。

[0025] 进一步的，在所述数据操作信息共识过程中，节点BS_j将数据操作广播至临近节点，并由拜占庭容错机制PBFT算法达成共识。

[0026] 进一步的，进行电子元器件数据共享操作时，该共享过程包括如下步骤：

[0027] 步骤S210：数据访问请求；

[0028] 步骤S220：智能合约执行；

[0029] 步骤S230：请求数据发送，数据提供方节点N_i将数据地址发送至数据请求方节点N_m中，同时向全网广播操作信息；

[0030] 步骤S240：访问指定数据，数据请求方节点N_m收到加密的数据地址后，利用自身的私钥进行解密，最后读取数据。

[0031] 进一步的，在所述数据访问请求中，数据请求方节点N_m向数据提供方节点节点N_i发出数据获取请求Req，请求中包含数据访问目的、访问时间和访问次数信息，节点N_i查验节

点N_m身份后，针对节点N_m制定访问约束条件Con，授权访问，并将访问约束条件和被访问数据块对应的私钥SK_i发送给对应交易区块链上区块BS_j，如下所示：

[0032] $$N_i \rightarrow N_m : \mathrm{Re}q = E_{PK_{N_i}}\left(\mathrm{Request} \mid \mathrm{Cert}_{N_m} \mid timestramp\right)$$

[0033] $$N_m \rightarrow BS_j : Message = E_{PK_{BS_j}}\left(Constra\,\mathrm{int}s \mid SK_i \mid PK_{N_m} \mid timestranp \mid Cert_{N_i}\right)。$$

[0034] 进一步的，在所述智能合约执行中，节点BS_j验证信息后，执行智能合约，根据节点设定的访问约束条件锁定脚本，并利用节点BS_j的私钥解密数据地址Add_{Enc_i}，同时根据提供的对称密钥SK_i，解密数据地址Add_i，最后使用访问节点N_m的公约对请求数据进行非对称加密，输出结果。

[0035] 本发明有益效果：能更好的利用现有硬件资源，存储元器件数据的区块链以联盟链的方式进行部署，节约了存储空间；实现了电子元器件整个生命周期所有相关数据的完整性、可靠性和可追溯性，降低了生产成本，缩短了产品装备的研制生产时间和科学研究的任务进程。

[0036] 本发明附加的方面和优点将在下面的描述中部分给出，这些将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0037] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0038] 图1为本发明实施例所述的账户区块链和交易区块链组织架构图。

[0039] 图2为本发明实施例所述的区块链元器件数据管理系统采用联盟链的方式的组织结构图。

[0040] 图3为本发明实施例所述的账户区块链的创世区块结构图。

[0041] 图4为本发明实施例所述的账户区块链的增加区块结构图。

[0042] 图5为本发明实施例所述的拜占庭容错机制共识原理示意图。

[0043] 图6为本发明实施例所述的电子元器件防伪溯源流程示意图。

[0044] 图7为本发明实施例所述的电子元器件数据管理系统工作原理流程示意图。

具体实施方式

[0045] 下面详细叙述本发明的实施方式，所述实施方式的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过附图描述的实施方式是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0046] 本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件和/或它们的组。应该理解，这里使用的“连接”

或“耦接”可以包括无线连接或耦接，使用的措辞“和/或”包括一个或更多个相关联的列出项的任一单元和全部组合。

[0047] 本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语(包括技术术语和科学术语)具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样定义，不会用理想化或过于正式的含义来解释。

[0048] 为便于理解本发明，下面结合附图以具体实施例对本发明作进一步解释说明，且具体实施例并不构成对本发明实施例的限定。

[0049] 本领域技术人员应该理解，附图只是实施例的示意图，附图中的部件并不一定是实施本发明所必须的。

[0050] 实施例

[0051] 如图1所示，本发明实施例提供一种基于区块链的电子元器件数据管理系统，该系统采用双链的结构组织管理数据，所有数据提供方及参与机构均可以和其他单位互相交换数据而保证隐私，至少包括账户区块链和交易区块链两种区块链。

[0052] ①账户区块链(Account Blockchain，ABC)：仅存储账户基本信息及账户关系、权限信息，不存储具体数据和交易即数据的操作(读取数据、写入数据等)信息。

[0053] ②交易区块链(Trading Blockchain，TBC)：仅存储交易即数据的操作(读取数据、写入数据等)信息。

[0054] 账户区块链(ABC)负责建立用户索引链，根据不同用户(生产商、采购方、第三方机构等)的基本信息通过哈希算法以生成具有唯一标识ID，同时保存该用户的关系合约、总结合约等，完成每一个用户的登记注册和权限设置。以实现用户查询、建块等功能。该链上账户信息共享，这使得信息难以篡改。同时，账户区块链也提供可扩展性，即：当区块链处理大小超过限制，可以被分割成多个子链，由不同机器上托管以保持平衡的工作量。

[0055] 交易区块链(TBC)负责建立元器件数据链，将不同机构的元器件数据信息存储地址密钥、数据摘要及不同机构数据上传、提取等操作信息记录至一个区块中，并将该区块的绝对地址与该数据所属用户、机构建立映射关系，同时将映射结果记录到对应的用户、机构索引链(ABC)所在的区块中。交易区块链负责建块、执行和记录交易(数据操作)。该链仅仅是用作交易和结算的通道(或场所)，其不保存双方的账户信息。此外，厂商和第三方机构的数据均加密保存至可信的服务器或云端，而在交易区块链中仅保存该数据的加密地址和数据摘要，这样只有获得授权的用户才能获取数据，同时每个机构都可以拥有自己的账户和区块链，只有当需要获取数据时，才共享至区块链上。

[0056] 如图2所示，区块链元器件数据管理系统采用联盟链的方式进行组织架构，该架构主要包括以下5个层次，分别为：数据存储层、数据连接层(网络层)、共识层、合约层及应用层。

[0057] 在数据层设计中，用户账户区块链(ABC)是记录该用户拥有或参与元器件数据交换活动的所有操作信息，该信息与元器件全生命周期内各阶段的相关活动(生产制造、检测、物流等)和用户、机构的数据操作(读取、写入)有关。

[0058] ABC区块链包含两个部分：起始区块和增加区块，每一个区块均包含前一个区块的Hash值已连接成链，建立起始区块后，写入数据的地址和数据操作行为等相关信息将会以

增加块的方式加入至区块链中。

[0059] 其中，起始区块(创世区块)保存用户的基本注册信息，用以识别验证用户，确定用户的数据操作、访问权限等。如图3所示，创世区块包括区块头和区块主体，区块头包括版本号、时间戳、前一区块哈希值和Merkle根。版本号将记录区块版本号和该区块建立所参照的规则(如安卓8.0、ios11.3)。时间戳将记录该区块创建时间，以保证历史信息可追溯、不可篡改。前一区块哈希值将各区块串连接成链。Merkle根为Merkle树的哈希值，Merkle树由所有记录的哈希值构成，为树状结构。区块主体包括用户信息摘要哈希值、用户公钥、用户签名。用户信息摘要记录用户身份信息同时确定该用户操作数据的权限。用户公钥作为公开用户身份的唯一标识可将其理解为用户账号地址，用以加密数据信息，操作数据。通过用户公开的公钥对其签名进行解密，得到用户的身份信息。私钥签名主要用以相互验证、确认对方身份。

[0060] 增加区块主要用于记录与该用户有关的元器件数据操作信息等。该区块的构成如图4所示。增加区块大体结构与创世区块类似，唯一不同之处在于该区块主体部分主要由数据操作信息(读取、写入数据)摘要哈希值构成的Merkle树组成，其中，数据操作信息主要由交易区块链(TBC)中由该用户发起、参与或涉及该用户的数据操作映射而来。用户签名是指该数据操作者的数字签名。

[0061] TBC区块链其创世区块和增加区块的结构与ABC区块链类似，在此不再赘述。TBC区块链即数据操作区块链并不保存用户的信息和数据操作双方的账户信息而只记录数据操作行为(读取、写入等)和操作数据的加密地址。因此，TBC区块链并不存储与元器件有关的任何数据。数据拥有者一般将数据存储至可信的脱链数据库或云中，同时附上自己的数字签名、时间戳，本地数据库根据数字签名核实用户的备案信息，确定写入数据用户身份的真实性和有效性，只有当核实有效时，数据库才认为写入的数据合法，合法性得到确认后，利用SHA256哈希算法加密数据保存地址，并将地址保存至区块中。该过程用以保证数据的真实、有效性，同时确定数据的唯一所有权。此外，该数据中还将提供数据所有者公钥加密数据的Hash值，用户在获取数据后根据数据所有者公布的公钥对数据进行Hash运算，并与提供的Hash值进行对比，以确保数据不可篡改、删除、真实可信。只将数据的保存地址经加密后保存至区块中，这种数据脱链分布式存储方式能确保数据更加安全，同时确保数据拥有者获得数据的绝对掌控权。其他用户或第三方机构若要操作数据必须经过身份验证，确认数据操作权限，才能获取数据地址操作数据。该行为也将被记录至TBC区块中，同时映射至数据操作双方ABC区块中，在双方ABC区块中将保存数据操作记录。由于区块链采用冗余方式进行存储，而元器件全生命周期数据具有数据量大、数据结构复杂的特点，因此采用区块链技术存储所有数据并不适合，同时区块链技术在大规模数据分析计算的情况下，也不能适应复杂事务的处理。因此数据脱链存储，有利于区块链的轻量化，容易部署。

[0062] 在数据连接层中，在元器件区块链的数据连接层中，元器件数据链采用P2P技术组织各个节点，与传统的中心化网络模式相比，P2P网络中各个节点平等，不存在中心化的服务器，对于元器件数据的大规模泄露有很好的防范作用。同时去中心化的分布式数据存储方式也提高了整个系统的冗余性和稳定性。

[0063] 数据连接层将所有的元器件数据库操作信息构建成一条区块链，该区块链以联合区块链的方式进行部署。PBFT拜占庭容错算法参与共识更新的过程，其他用户节点可以访

问区块链。区块链的不可篡改性，保证了数据连接层的数据的真实性，所有状态的改变都可以溯源，以确保用户权限和用户数据操作的有效性。因此，通过数据连接层的数据操作都是安全可靠的。在进行数据操作过程中，可以利用区块链技术验证交易的有效性和交易账户身份的有效性。首先根据数据操作请求方的公钥和签名验证数据请求方身份，同时根据关系合约核实其权限，当核实通过后主节点收到请求后将消息向从节点广播，达成一致后数据请求方将获得数据存储地址并完成数据操作。

[0064] 数据操作区块链(TBC)其数据连接层存储的所有对元器件数据库或云平台的操作记录(读取或写入数据)，与加密货币中区块链存储交易记录的本质是相同的，均详细记录了数据状态的变化。所以数据连接层的区块链的增加方式可以按照加密货币的方式进行，即以固定时间间隔的方式进行增加。数据连接层中数据操作双方达成一致，完成交易(数据操作)的另一个重要部分即是智能合约，智能合约由区块链状态改变时而触发从而实现对数据的操作，并保证数据操作真实、有效。

[0065] 而对于账户区块链(ABC)其每个用户、科研院所、第三方机构等其信息单独成链。以方便元器件信息的查找、防伪溯源。

[0066] 在共识层设计中，共识层是数据链中各节点达成一致的策略和方法，该方法解决了在不可信信道上传输可信信息、价值转移的问题，达到了去中心化背景下节点互相信任的状态。传统的工作量证明(POW)需要进行数学运算获取记账权，消耗较高的资源，可监管性也比较差，达成共识依赖于全网的共同参与，一般用于数字货币交易的公有链中。对于联盟链或私有链，其共识方法主要包括权益证明和拜占庭容错，此方法相比于工作量证明，减少了资源消耗，提高了性能。

[0067] 权益证明机制(DPOS)的主要思想是节点记账权的易获得度与节点持有利益正相关。该方法允许所有的股东节点都具有投票权，通过公平民主的方式票选出101个权益代表。并可以在后续过程中根据代表的表现自由重投选票。该方法有效地降低了参与记账节点的数量，实现了快速共识验证。DPOS的基本工作思路为本领域技术人员都能够清楚了解的现有技术，在此不再赘述。

[0068] 另一种共识机制——实用拜占庭容错机制(PBFT)是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。该机制将拜占庭协议的运行复杂度从指数级别降低至多项式级别，使拜占庭协议在分布式系统中的应用成为可能。

[0069] PBFT要求共同维护一个状态，所有节点采取的行动一致。为此，需要运行三类基本协议，包括一致性协议、检查点协议和视图更换协议。其中主要关注支持系统日常运行的一致性协议。一致性协议至少包含若干个阶段：请求、广播数据区块和响应。根据协议设计的不同，可能包含相互交互，审计、验证等阶段。其共识过程如图5所示。

[0070] 其中，Leader为主节点、BS1～BSn为从节点。每一个用户的请求需要经过5个阶段，通过采用两次两两交互的方式在服务器达成一致之后再执行用户的请求。由于用户不能从服务器端获得任何服务器运行状态的信息，PBFT中主节点是否发生错误只能由服务器监测。如果服务器在一段时间内都不能完成用户的请求，则会触发视图更换协议。该机制最多可以容忍三分之一的节点错误。其共识过程如下：

[0071] Step1.主节点(Leader)收集各从节点的数据集合整合为一个新的数据区块，附上

主节点的数字签名和新数据区块的哈希值以备审查验证,同时主节点向各从节点广播新生成数据区块以待查验。

[0072] Step2.从节点接收到数据区块后,根据其区块哈希值和数字签名等信息验证数据区块的合法性和正确性,并把审计结果附上各自对应的数字签名广播至其它邻近从节点,以实现节点间的相互监督和共同查验。

[0073] Step3.从节点接收并汇总其他从节点审计结果后与自身的审计结果进行对比,并向主节点发送回复信息,这个回复包含该从节点自身的审计结果,收到的所有审计结果,审计对比的结论以及对应的数字签名。

[0074] Step4.主节点汇总所有来自从节点的审计回复。如果全部数据集合器都赞同当前数据区块的合法性和有效性,主节点将把该数据区块、参与审计的从节点证书集合以及对应的数字签名整合发送至所有从节点。此后,该数据区块将以时间先后的顺序存储在链中。

[0075] Step5.假若有部分从节点不赞同当前的审计结果,主节点将分析和查验这些从节点的审计结果。必要时,主节点重新发送该数据区块给这部分从节点进行第二次审计,如果从节点不赞同,将采取少数服从多数的原则,超过一定比例的从节点赞同该数据区块,则将该数据区块按Step4方式加载到数据存储区块链中。同时,主节点将进一步分析个别不赞同从节点的审计结果,判断这些节点是否存在恶意行为,并及时把恶意节点进行处理。此步骤有利于及时发现并剔除非法恶意节点,从而保证系统的安全稳定运行。

[0076] 对比于POS机制,PBFT机制可以脱离数字货币运转,PBFT算法共识结点由业务的参与方或者监管方组成,安全性与隐私性由业务相关方保证。共识的延时大约在2～5秒,能基本满足实时处理的要求,而且其共识效率高。对于节点数目较少且环境较为封闭的联盟链,PBFT共识机制能取得不错的效果。因此,我们采用拜占庭容错机制进行区块共识。

[0077] 在合约层设计中,继承了比特币区块链的设计,封装区块链系统的各类脚本代码、算法。可以利用脚本代码规定数据的操作、分享方式及各项细节,通过合约的脚本技术,可以保证数据操作等行为的顺利进行。该合约层主要包括:登记合约、关系合约和总结合约。

[0078] (1)登记合约。登记合约主要记录用户、不同机构的基本信息以及用户类型(元器件生产商、元器件采购方、第三方科研机构等等),用以管理账户身份,确定用户数据操作权限。区块链账户的身份信息都是通过椭圆加密算法由用户公钥生成的私钥进行加密,这可能与现有的ID形式不相符合。登记合约将用户真实身份和其区块链账号做映射,合约中的编码可以允许新身份的注册及现有映射的改变。此外,登记合约也将用户身份与相应的关系合约做映射,用以管理相关用户的数据权限。

[0079] (2)关系合约。关系合约用于实现数据操作权限设置和访问控制。每个元器件的信息记录可能在其生命周期内会由不同的机构进行提供、管理,每个机构组织也将会拥有、管理不同元器件的数据,关系合约就是对用户和各机构间一对一的关系进行说明的合约,该合约将定义一系列数据指针和相关访问权限,通过指针可以访问不同用户所拥有的数据库地址,数据的访问权限主要通过数据库检索指令来约束,不同权限的用户可以使用的数据检索指令也将不同。在具体实现时用户权限可以通过设置用户角色确定(例如元器件采购用户有权限获取元器件制造商关于该元器件的部分生产信息和所有元器件的检测数据,用以监管元器件质量,避免二次筛选,缩短任务周期、减少成本等),或为每位用户、机构院所开发简单的图形界面工具,由用户在界面上对拥有数据进行权限管理,实现人机的友好交、

减轻用户的认知负担。

[0080] (3)总结合约。总结合约用于管理各用户和其所有关系合约的映射,即该合约为用户登记合约和关系合约间的桥梁。用户的登记合约中将保存一张列表,该列表将记录总结合约的地址,只需访问用户的登记合约便可以链接至用户的总结合约。此外,用户登记合约还将存有总结合约的状态,用于表示关系合约中的权限是否被用户确认。

[0081] 如图6所示,根据合约层的设计,在应用层设计中,可以满足各科研院所、第三方机构等对数据采集和交换的需求。通过多用户参与制定智能合约、P2P网络扩散、链上代码自动执行相关程序,用户和各机构可以放心的实现数据交换、分享。同时根据业务需求和现有的行业痛点,利用获取所得数据进行分析、挖掘、操作,开发相应的程序、软件,如元器件防伪溯源、元器件质量管理、元器件供应链管理、元器件库存管理等等。

[0082] 用户或科研院所登录账户并请求查看元器件各阶段详细数据,此时将触发用户登记智能合约。智能合约将验证用户身份的有效性,即首先根据用户公布公钥解密使用私钥加密的数字签名,确定用户身份。身份合法、有效后再向连接层的区块进行权限验证,此时触发总结合约及关系合约。如果权限验证合法、有效,则查询用户所申请的该部分数据读取权限是否开放,开放则允许用户获取TBC链中的数据地址,读取数据。若该部分数据查询操作没有对用户开放,则用户将向数据所有者提出权限申请,待所有者回复。若所有者回复同意,则用户获得数据访问权限,否则放弃本次操作。待用户获得数据后,即可查看数据,判断数据真实性。同时根据数据所有者签名核实数据的真实来源,根据时间戳获取各阶段元器件数据的历史信息,以达到防伪溯源的目的。

[0083] 2.2.6元器件区块链系统的运行过程

[0084] 元器件区块链的运行遵循智能合约约定规则。智能合约是一套以数字形式定义的承诺,从本质上讲,智能合约是一个运行在安全环境下(去中心化的计算机网络)的计算机程序,合约协议的工作原理类似于其它计算机程序的if-then语句。智能合约只是以这种方式与真实世界的资产进行交互。当一个预先编好的条件被触发时,智能合约执行相应的合同条款。其与共识机制、点对点网络、Merkle树以及数据库技术构成区块链这样一种低成本、高可靠的基础设施。在满足合约执行的促发条件下,智能合约智能化自动执行数据访问和共享请求,依据定义好的约束条件执行数据输出、数据共享等操作。其元器件数据区块链运行主要包括数据存储与数据读取。

[0085] 如图7所示,该系统在数据存储操作中,主要包括以下几个步骤:

[0086] Step1.系统初始化和密钥生成。这里我们使用Boneh-Boyen短签名技术初始化系统。首先用户申请加入系统,管理员核实其身份并完成基本信息注册后,用户将获取用于加密数据的公钥集合、验证身份唯一性的私钥和证书,记为$\{PK_i,SK_i,CertL_i\}$,成为系统的合法结点。

[0087] Step2.上传数据。从制造生产至淘汰报废各阶段由物联网设备(IoT)收集元器件数据,并附上数字签名及时间戳加密存储至本地数据库或云中。用户登录系统并发送数据上链请求,该请求包含节点i即用户当前使用的证书$Cert_i$和数字签名Sig_i,TBC节点BS_j收到请求后将根据证书和签名核实验证节点身份的合法性和有效性,以确保数据来源真实可靠。当节点身份验证准确无误时,BS_j节点回应其数据上传请求。此时,节点i将使用当前公钥PK_i加密数据保存地址Add_i得到Add_{Enc_i},并集合加密的数字签名和时间戳。最后利用BS_j节

点公钥再次加密上述集合,得到最终上传数据Record,BS_j节点验证数据的有效性,如果数据安全有效,则将Record写入BS_j中,具体过程如下:

[0088] $$i \to BS_j : \mathrm{Re}cord = \mathrm{E}_{PK_{BS_j}}\left(Add_{Enc_i} \mid Cert_i \mid Sig_{Enc_i} \mid timestamp_i\right),$$

[0089] $$where\ \ Add_{Esc_i} = \mathrm{E}_{PK_i}\left(Add_i \mid timestamp_i\right), \mathrm{Sig}_{Esc_i} = Sign_{SK_i}\left(Add_{Esc_i}\right)$$

[0090] 上式中,i为账户区块链ABC请求节点,BS_j为交易区块链TBC记录节点,$E_{PK_i}(m)$运算表示使用i的公钥加密信息m,Add_{Enc_i}表示由节点i公钥加密后的数据地址,$Cert_i$表示节点i的证书,Sig_{Enc_i}表示由节点i签名的信息,$timestamp_i$表示节点i的时间戳,Add_i表示节点i存储数据的地址,$Sign_{SK_i}(\mathrm{m})$运算表示使用i的私钥对信息m进行数字签名。

[0091] Step3.数据操作信息共识过程。节点BS_j将数据操作广播至临近节点,并由PBFT算法达成共识,其具体过程参见2.3节,在此不再赘述。

[0092] Step4.将上述数据操作记录和节点BS_j对应索引映射至ABC区块链节点i中,保存。

[0093] 在数据共享操作中,存储在交易区块链(TBC)上的数据地址已被数据真正的拥有者使用不同的私钥进行加密处理,而数据拥有者有权控制并有选择性的公开部分数据进行共享。各节点间的数据共享操作通过执行智能合约的脚本文件来实现。数据拥有者有权设定数据共享的对象、共享数据的范围、共享的时间及次数等约束条件,通过计算机语言代替法律文件约束其他访问者的行为,保证数据共享的安全性和有效性。

[0094] 数据共享智能合约脚本主要包括锁定脚本和解锁脚本。锁定脚本规定共享数据输出的阻碍条件,解锁脚本定义数据输出的执行条件。其数据共享流程主要流程为:当节点N_m向节点N_i发出数据共享请求时,节点N_i首先验证节点N_m的身份,与N_m达成共识后,节点N_i将制定访问约束条件(数据访问范围、访问时间、访问次数等),然后智能合约根据节点N_i所拥有的私钥将数据解密,并根据约束条件输出对应结果,最后利用节点N_m所提供的公钥对数据进行加密,将加密结果传输给节点N_m。节点N_m利用自身私钥进行解密,获取数据。具体步骤如下所述:

[0095] Step1.数据访问请求。节点N_m向节点N_i发出数据获取请求Req,请求中包含数据访问目的,时间和次数等相关信息。节点N_i查验节点N_m身份后,针对节点N_m制定访问约束条件Con(数据共享范围、时效、次数等),授权访问,并将这些条件和被访问数据块对应的私钥SK_i发送给对应TBC链上区块BS_j,如下所示:

[0096] $$N_i \to N_m : \mathrm{Re}q = E_{PK_{N_i}}\left(\mathrm{Request} \mid \mathrm{Cert}_{N_m} \mid timestramp\right)$$

[0097] $$N_m \to BS_j : Message = E_{PK_{BS_j}}\left(Constra\,\mathrm{int}s \mid SK_i \mid PK_{N_m} \mid timestranp \mid Cert_{N_i}\right)$$

[0098] Step2.智能合约执行。节点BS_j验证信息后,执行智能合约,根据节点设定的访问约束条件锁定脚本,并利用节点BS_j的私钥解密数据地址Add_{Enc_i},同时根据提供的对称密钥SK_i,解密数据地址Add_i。最后使用访问节点N_m的公约对请求数据进行非对称加密,输出结果。

[0099] Step3.请求数据发送。数据被请求节点N_i将数据地址发送至数据请求节点N_m中,同时向全网广播操作信息。

[0100] Step4.访问指定数据。数据请求节点N_m收到加密的数据地址后，利用自身的私钥进行解密，最后读取数据。

[0101] 综上，本发明的具体实施例中，首先，元器件区块链系统的结构设计仅是从软件层面的逻辑结构出发，对于现有的硬件设施并未有较大改变，因此其能很好的运行和部署在现有的硬件设备、操作系统上，能够更好的利用现有的硬件资源。现有的大多数区块链技术以开源社区的方式进行维护，在技术的使用上是免费的，这样可以减少软件授权费用，同时存储元器件数据的区块链以联盟链的方式进行部署，一定程度上克服了区块链中分布式分布需要大量存储空间的缺点。元器件区块链系统可以实现元器件从生产制造到报废淘汰整个生命周期所有相关数据的完整性、可靠性和可追溯性，其带来的效益是多方的、广泛的。通过该系统可以提高元器件的质量，减少元器件生产、管理、维护的支出，还可以在数据的基础上开发各类应用系统，加快元器件的研制。

[0102] 联盟链采用分布式数据脱链存储方法来保证数据的安全存储，其不依赖于全局可信的第三方实体，节点间采用端到端的通信方式，分布式存储数据，从而避免了传统中心化数据存储方法的中心节点容易遭受集中式恶意攻击的风险。这种非中心化的脱链存储系统具有良好的可扩展性和可靠性。

[0103] 联盟链系统数据存储过程使用不同的非对称密钥对不同时间采集的数据进行加密，最大可能性保证数据安全储。此外，该盟链采用智能合约的方式执行数据共享，约束了节点的访问条件，限制节点随意访问数据的权限，使得数据的真正拥有者能掌握并控制数据的访问权限和开放程度。

[0104] 利用拜占庭容错机制，所有的加密数据由预选的节点执行公开审计和验证工作，从而保证数据的合法性和真实有效性。

[0105] 通过共识机制，这些被攻击的数据也会被其它节点在审计和查验数据时发现问题。对于预选的节点而言，预选的节点间采用PBFT共识机制，不妨设全网存在f个恶意节点，只需预选节点数目n满足$n>3f+1$，便可抵御f个预选节点发起的恶意篡改数据攻击，保证数据的合法性与真实性。假如设全网存在100个预选节点，且预选节点成为恶意节点的概率为1/2。根据上述分析内容可知，需要同时存在33个恶意节点才能成功发起数据篡改攻击。因此在此条件下，恶意节点篡改数据的成功率仅为$1/2^{33}$。

[0106] 联盟链分布式的本质特性联合数字签名技术保证攻击者无法假扮成某个合法实体来干扰无线网络数据存储。存储在联盟链上的元数据是通过节点密钥加密后在上链的，除非攻击者窃取到节点全部的非对称加密密钥，否则无法获得完整数据，进而去伪造这些数据。

[0107] 在PBFT共识算法中，系统主要的能耗包括主从节点间的广播数据区块操作与节点收到数据后的校验操作。不妨设联盟链每30分钟执行一次共识算法，n个预选节点则需要进行n^2+n-2次广播操作以及n^2+2n-2次验证操作。查阅相关资料知每个数据区块大小为1M，每个节点执行广播操作平均需要0.9J能量，验证操作需要0.03J能量。则100个预选节点每小时执行PBFT共识机制耗能约为18KJ，即其功率为5W。因此，PBFT耗能数量级并不大，即使全网节点数目增加，本系统预选节点数目取值不变，PBFT共识机制的能耗相对固定。因此该技术能耗较低，方案现实可行。。

[0108] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本发明可

借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例或者实施例的某些部分所述的方法。

[0109] 以上所述，仅为本发明较佳的具体实施方式，但本发明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发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

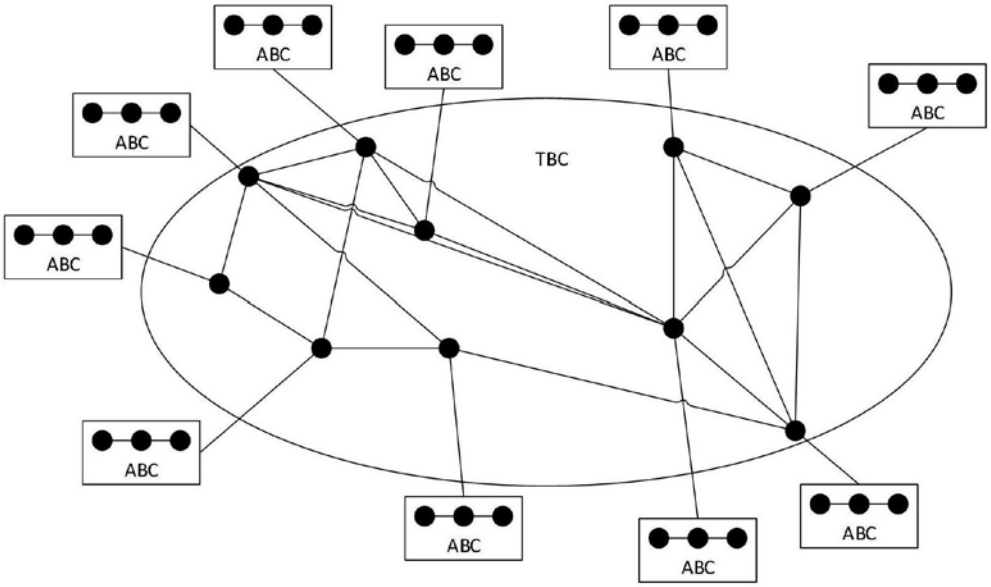


图1

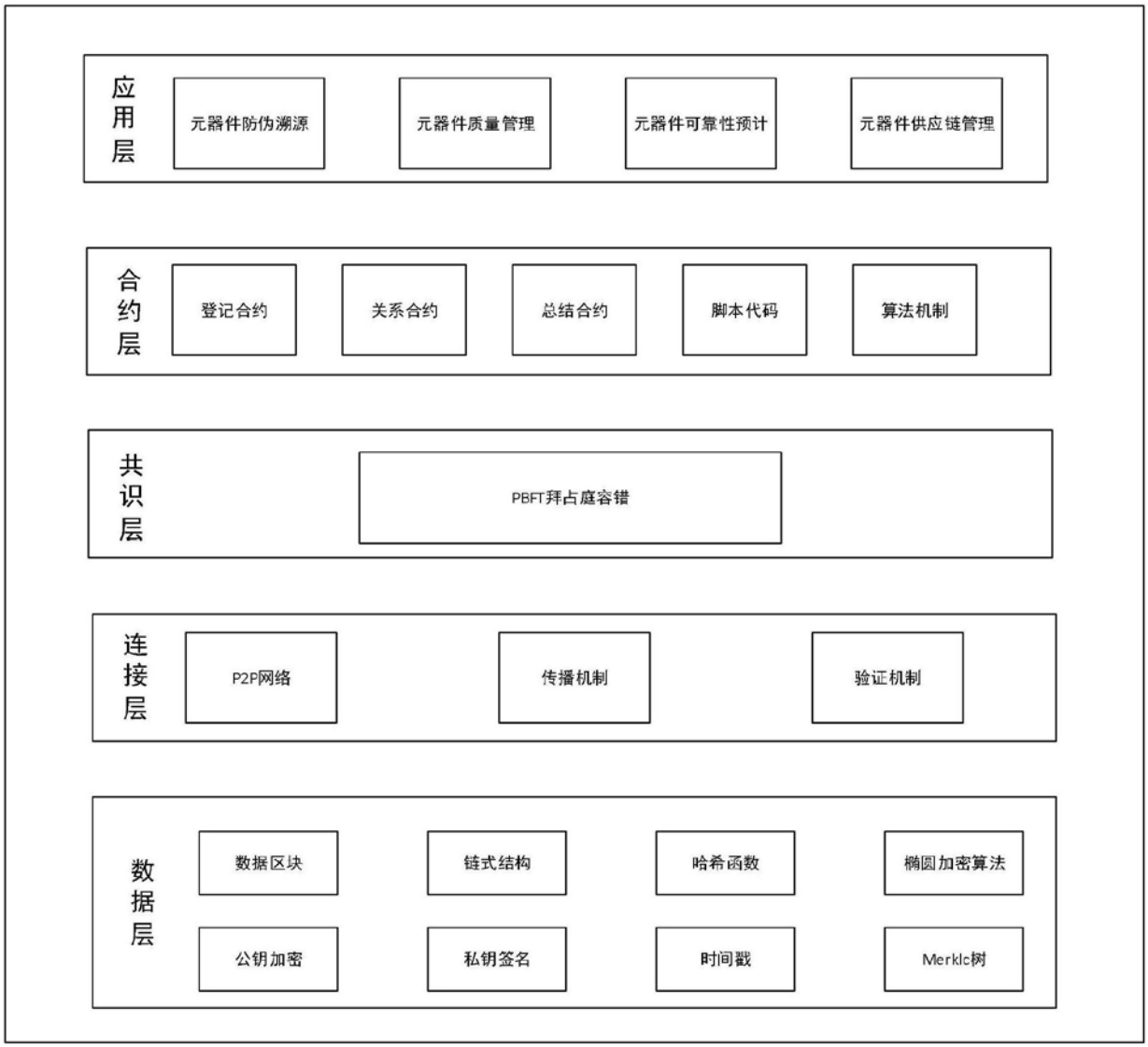

应用层
元器件防伪溯源
元器件质量管理
元器件可靠性预计
元器件供应链管理
合约层
登记合约
关系合约
总结合约
脚本代码
算法机制
共识层
PBFT拜占庭容错
连接层
P2P网络
传播机制
验证机制
数据层
数据区块
链式结构
哈希函数
椭圆加密算法
公钥加密
私钥签名
时间戳
Merkle树

图2

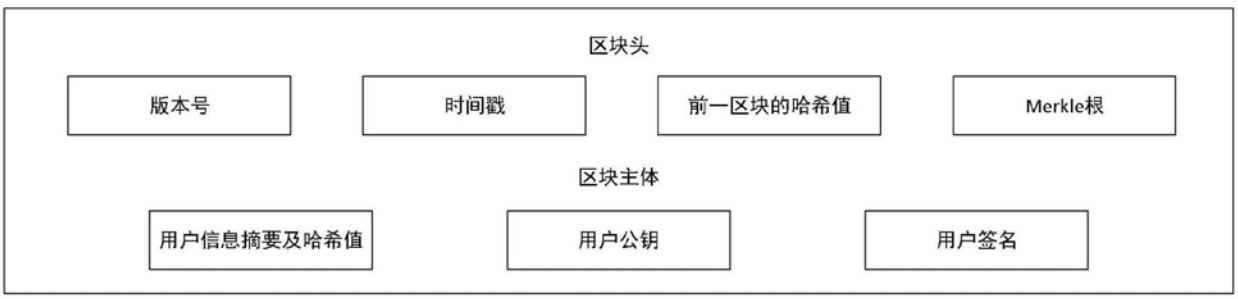

区块头
版本号
时间戳
前一区块的哈希值
Merkle根
区块主体
用户信息摘要及哈希值
用户公钥
用户签名

图3

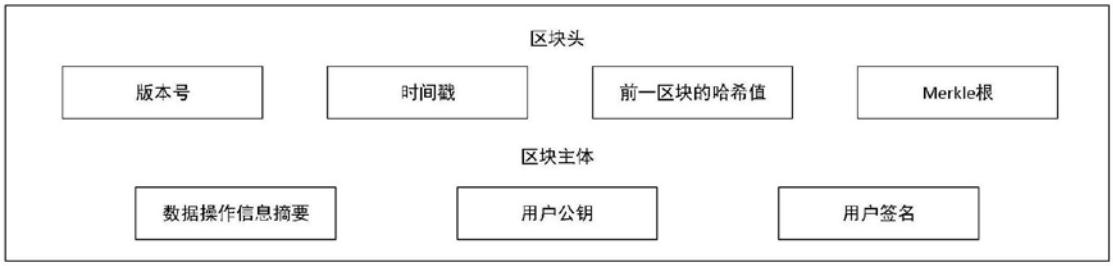

区块头
版本号
时间戳
前一区块的哈希值
Merkle根
区块主体
数据操作信息摘要
用户公钥
用户签名

图4

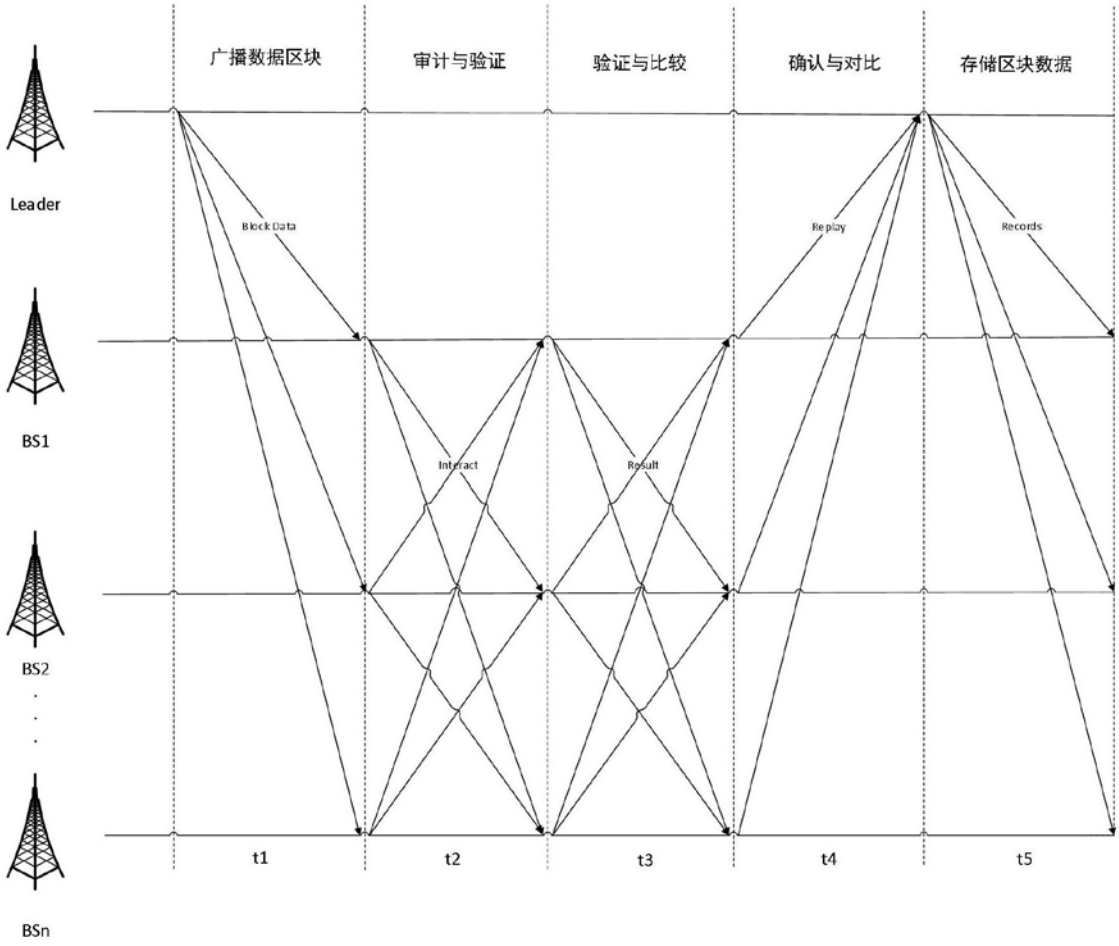

广播数据区块
审计与验证
验证与比较
确认与对比
存储区块数据
Leader
BS1
BS2
BSn
Block Data
Interact
Result
Replay
Records
t1
t2
t3
t4
t5

图5

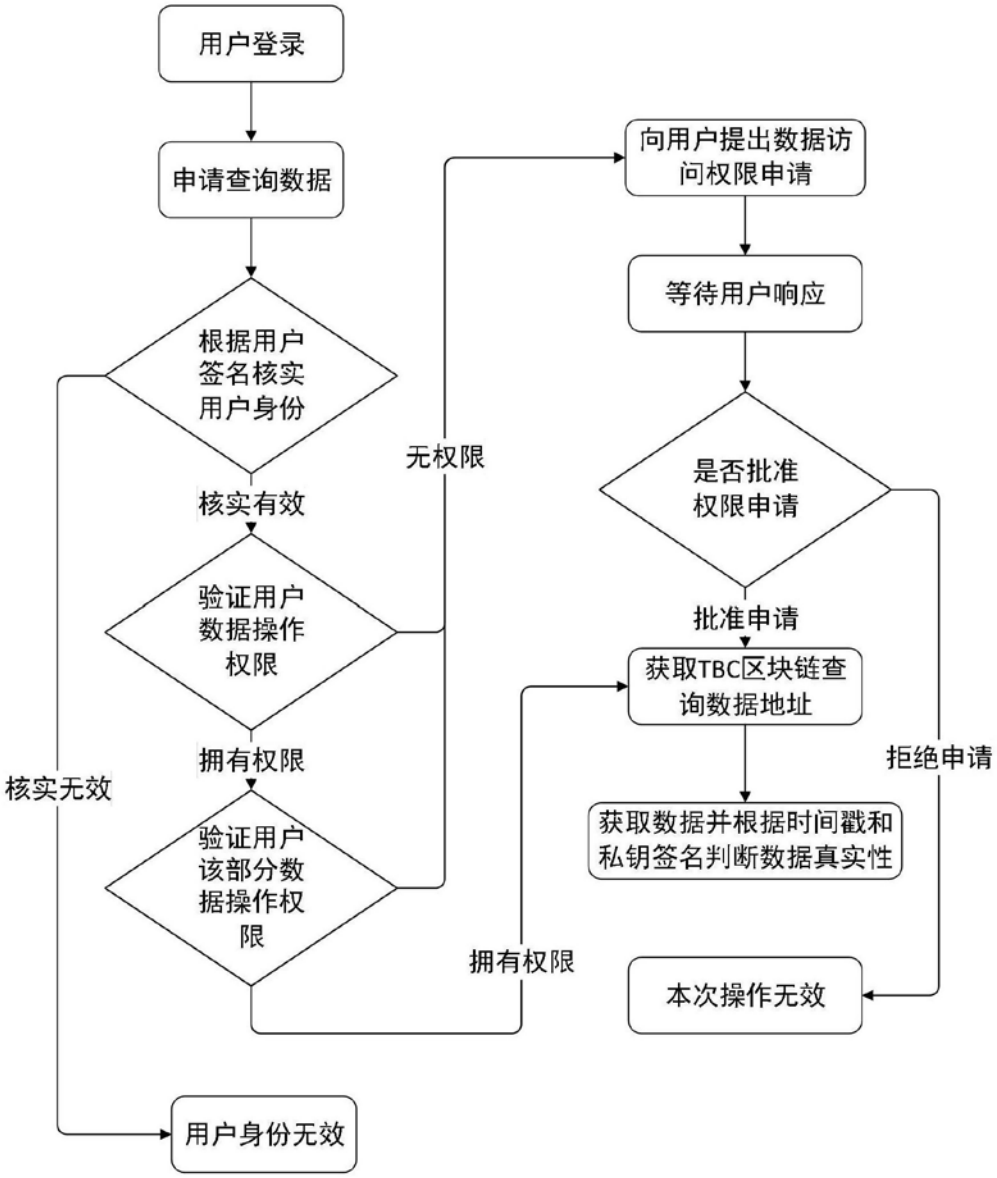

用户登录
申请查询数据
根据用户签名核实用户身份
核实有效
验证用户数据操作权限
拥有权限
验证用户该部分数据操作权限
核实无效
用户身份无效
无权限
向用户提出数据访问权限申请
等待用户响应
是否批准权限申请
批准申请
获取TBC区块链查询数据地址
获取数据并根据时间戳和私钥签名判断数据真实性
拒绝申请
本次操作无效
拥有权限

图6

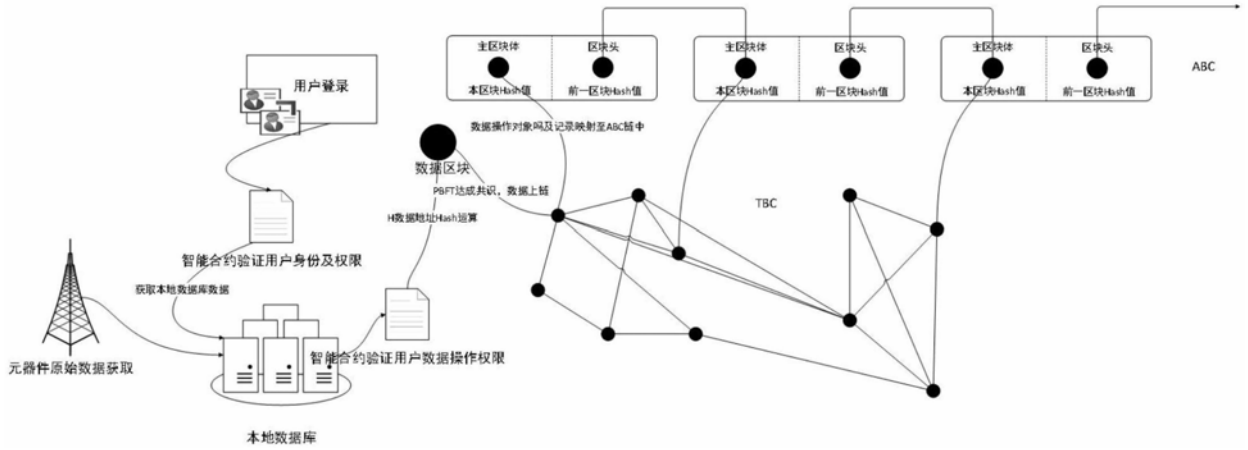

主区块体
区块头
本区块Hash值
前一区块Hash值
ABC
用户登录
数据操作对象吗及记录映射至ABC链中
数据区块
PBFT达成共识，数据上链
H数据地址Hash运算
TBC
智能合约验证用户身份及权限
获取本地数据库数据
元器件原始数据获取
智能合约验证用户数据操作权限
本地数据库

图7