

基于区块链的数据处理方法和装置

5 相关申请的交叉引用

本专利申请要求于 2021 年 01 月 04 日提交的、申请号为 202110002609.2、发明名称为“基于区块链的数据处理方法和装置”的中国专利申请的优先权，该申请的全文以引用的方式并入本申请中。

10 技术领域

本申请的实施例涉及计算机技术领域，具体涉及区块链技术领域，尤其涉及基于区块链的数据处理方法和装置。

背景技术

- 15 区块链技术诞生于中本聪提出的比特币系统，其本质是一个共享数据库，具有去中心化、不可篡改、公开透明等优点。智能合约是 1997 年由 Szabo 提出的理念，在区块链系统中，智能合约是运行在区块链数据库上的一段可执行的具有逻辑顺序的计算机程序，可以满足其源代码中预定义的条件时自行执行。由于智能合约可以在无可信第三方的情况下自动执行的特性，其降低了互不信任的多个合约参与方之间的信任成本。

然而，目前在区块链系统中，修改智能合约代码，需要重新编译区块链节点代码并重新启动区块链服务，增加了运维人员的工作量，增大了系统出错的几率。

25 发明内容

本申请提供了一种基于区块链的数据处理方法、装置、设备以及存储介质。

- 根据本申请的第一方面，提供了一种基于区块链的数据处理方法，该方法包括：响应于接收到区块链网络中请求节点发送的合约部署请求，获取合约部署请求对应的合约文件，其中，合约文件基于对合约部署请求对
- 30

应的智能合约进行内容扩展而生成，智能合约为区块链中可自动执行的业务代码；基于合约文件的解析结果和区块链账本，对合约文件进行验证，其中，验证用于表征对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证，区块链账本通过预先执行合约部署的交易而生成；响应于

5 合约文件验证成功，根据合约文件，确定与合约部署请求对应的智能合约。

在一些实施例中，基于合约文件的解析结果和区块链账本，对合约文件进行验证，包括：对合约文件进行内容解析，得到合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包和合约文件的密钥包，其中，密钥包通过对请求节点进行加密运

10 算而生成；基于合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，对合约文件进行验证。

在一些实施例中，基于合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，对合约文件进行验证，包括：根据合约文件的密钥包，对合约文件进行密钥验证，其中，验证用于表征对请求节点的公私钥对进行验证；根据合约参与方的签名数据包，对合约的参与方进行验证；查询区块链账本，得到合约部署请求对应的各方法的方法名和与合约部署请求对应的各方法对应的参数信息，并根据得到的方法名和参数信息，对合约

15 文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包进行验证；根据合约文件的密钥验证结果、合约的参与方的验证结果、合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包的验证结果，确定合约文件是否验证成功。

在一些实施例中，区块链账本的生成过程如下：响应于接收到请求节点发送的合约部署的交易请求，广播交易请求至区块链网络，并基于交易请求报文对交易进行验证，其中，交易请求报文包括：合约部署请求对应的各方法的方法数据包、与合约部署请求对应的各方法对应的参数数据包、合约文件的哈希值和合约文件的位置信息；响应于交易验证通过，根据合约部署请求对应的各方法的方法数据包、与合约部署请求对应的各方法对

25

应的参数数据包、合约文件的哈希值和合约文件的位置信息，生成与交易请求对应的区块；基于共识机制，将区块写入区块链账本，生成写入后的区块链账本。

5 在一些实施例中，获取合约部署请求对应的合约文件，包括：基于区块链账本中合约文件的位置信息，获取与合约文件的位置信息对应的合约文件。

在一些实施例中，方法名数据包基于第一加密算法对方法名进行加密而生成；和/或，参数数据包基于第二加密算法对参数进行加密而生成。

10 在一些实施例中，基于合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包，对合约文件进行验证，包括：基于方法名数据包的密文，对合约文件进行验证；和/或，基于参数数据包的密文，对合约文件进行验证。

在一些实施例中，方法还包括：将智能合约部署于区块链中，以使当业务触发调用条件时，执行智能合约。

15 在一些实施例中，方法还包括：响应于合约文件验证失败，结束合约部署请求。

根据本申请的第二方面，提供了一种基于区块链的数据处理装置，装置包括：获取单元，被配置成响应于接收到区块链网络中请求节点发送的合约部署请求，获取合约部署请求对应的合约文件，其中，合约文件基于
20 对合约部署请求对应的智能合约进行内容扩展而生成，智能合约为区块链中可自动执行的业务代码；验证单元，被配置成基于合约文件的解析结果和区块链账本，对合约文件进行验证，其中，验证用于表征对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证，区块链账本通过预先执行合约部署的交易而生成；确定单元，被配置成响应于合约文件验证
25 成功，根据合约文件，确定与合约部署请求对应的智能合约。

在一些实施例中，验证单元，包括：内容解析模块，被配置成对合约文件进行内容解析，得到合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包和合约文件的密钥包，其中，密钥包通过对请求节点进行加密运算而生成；验证模块，被配

置成基于合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，对合约文件进行验证。

在一些实施例中，验证模块，包括：第一验证子模块，被配置成根据
5 合约文件的密钥包，对合约文件进行密钥验证，其中，验证用于表征对请求节点的公私钥对进行验证；第二验证子模块，被配置成根据合约参与方的签名数据包，对合约的参与方进行验证；第三验证子模块，被配置成查询区块链账本，得到合约部署请求对应的各方法的方法名和与合约部署请求对应的各方法对应的参数信息，并根据得到的方法名和参数信息，对合
10 约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包进行验证；确定子模块，被配置成根据合约文件的密钥验证结果、合约的参与方的验证结果、合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包的验证结果，确定合约文件是否验证成功。

在一些实施例中，区块链账本利用如下模块生成：交易验证模块，被
15 配置成响应于接收到请求节点发送的合约部署的交易请求，广播交易请求至区块链网络，并基于交易请求报文对交易进行验证，其中，交易请求报文包括：合约部署请求对应的各方法的方法数据包、与合约部署请求对应的各方法对应的参数数据包、合约文件的哈希值和合约文件的位置信息；生成模块，被配置成响应于交易验证通过，根据合约部署请求对应的各方法的方法数据包、与合约部署请求对应的各方法对应的参数数据包、合
20 约文件的哈希值和合约文件的位置信息，生成与交易请求对应的区块；写入模块，被配置成基于共识机制，将区块写入区块链账本，生成写入后的区块链账本。

在一些实施例中，获取单元进一步被配置成基于区块链账本中合约文
25 件的位置信息，获取与合约文件的位置信息对应的合约文件。

在一些实施例中，内容解析模块中的方法名数据包基于第一加密算法对方法名进行加密而生成；和/或，内容解析模块中的参数数据包基于第二加密算法对参数进行加密而生成。

在一些实施例中，验证模块进一步被配置成基于方法名数据包的密文，

对合约文件进行验证；和/或，基于参数数据包的密文，对合约文件进行验证。

在一些实施例中，装置还包括：部署单元，被配置成将智能合约部署于区块链中，以使当业务触发调用条件时，执行智能合约。

- 5 在一些实施例中，装置还包括：结束单元，被配置成响应于合约文件验证失败，结束合约部署请求。

根据本申请的第三方面，提供了一种电子设备，包括：至少一个处理器；以及与至少一个处理器通信连接的存储器；其中，存储器存储有可被至少一个处理器执行的指令，指令被至少一个处理器执行，以使至少一个
10 处理器能够执行如第一方面中任一实现方式描述的方法。

根据本申请的第四方面，本申请提供了一种存储有计算机指令的非瞬态计算机可读存储介质，其特征在于，计算机指令用于使计算机执行如第一方面中任一实现方式描述的方法。

- 应当理解，本部分所描述的内容并非旨在标识本申请的实施例的关键
15 或重要特征，也不用于限制本申请的范围。本申请的其它特征将通过以下的说明书而变得容易理解。

附图说明

附图用于更好地理解本方案，不构成对本申请的限定。

- 20 图1是根据本申请的基于区块链的数据处理方法的第一实施例的示意图；

图2是可以实现本申请实施例的基于区块链的数据处理方法的场景图；

图3是根据本申请的基于区块链的数据处理方法的第二实施例的示意图；

- 25 图4是根据本申请的基于区块链的数据处理装置的一个实施例的结构示意图；

图5是用来实现本申请实施例的基于区块链的数据处理方法的电子设备的框图。

- 30 具体实施方式

以下结合附图对本申请的示范性实施例做出说明，其中包括本申请实施例的各种细节以助于理解，应当将它们认为仅仅是示范性的。因此，本领域普通技术人员应当认识到，可以对这里描述的实施例做出各种改变和修改，而不会背离本申请的范围和精神。同样，为了清楚和简明，以下的描述中省略了对公知功能和结构的描述。

需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

根据本申请的技术采用响应于接收到区块链网络中请求节点发送的合约部署请求，获取合约部署请求对应的合约文件，其中，合约文件基于对合约部署请求对应的智能合约进行内容扩展而生成，基于合约文件的解析结果和区块链账本，对合约文件进行验证，响应于合约文件验证成功，根据合约文件，确定与合约部署请求对应的智能合约，实现了通过扩展智能合约文件（ELF 文件）的文件格式，动态加载智能合约文件，而无需重启区块链节点即可运行新的智能合约。通过扩展智能合约 ELF 文件的文件类型，对智能合约二进制本身进行了安全控制，达到安全的动态加载智能合约的目的。区块链账本通过预先执行合约部署的交易而生成，实现了智能合约方法和参数可以动态设置，而限制智能合约的实现方法和模板，具有更大的灵活性。验证基于对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证，避免了现有技术中通过引入第三方密钥中心带来的安全风险和密钥泄漏的可能性，保证了合约的部署者和批准者的不可否认性和完整性。

图 1 示出了根据本申请的基于区块链的数据处理方法的第一实施例的示意图 100。该基于区块链的数据处理方法，包括以下步骤：

步骤 101，响应于接收到区块链网络中请求节点发送的合约部署请求，获取合约部署请求对应的合约文件。

在本实施例中，在区块链网络中，当执行主体（例如智能合约服务端）接收到请求节点发送的合约部署请求时，可以通过有线连接或无线连接的方式获取合约部署请求对应的合约文件。合约文件可以基于对合约部署请求对应的智能合约进行内容扩展而生成，合约文件的文件类型可以为智能

合约文件（ELF 文件）扩展后的 ELFext，智能合约为区块链中可自动执行的业务代码。需要指出的是，上述无线连接方式可以包括但不限于 3G、4G、5G 连接、WiFi 连接、蓝牙连接、WiMAX 连接、Zigbee 连接、UWB（ultra wideband）连接、以及其他现在已知或将来开发的无线连接方式。

5 进一步说明，智能合约代码进行编译后，以 ELF 文件格式存在，当业务触发了调用条件的时候，自动执行 ELF 文件代码逻辑。为了保证 ELF 文件的不可篡改，以及体现区块链参与方对本合约的统一共识，需要在原 ELF 文件格式基础上添加自定义的属性，称为附加属性，附属属性包含以下内容：加密的方法名数据包、各方法对应的加密的参数数据包、合约参与方签名的签名数据包、合约文件的密钥包和智能合约密文包。对于方法名数据包，使用 3DES 算法的 CBC 模式对方法名进行加密运算。对于参数数据包，使用 3DES 算法的 CBC 模式对方法的参数进行加密。对于签名数据包，智能合约参与方对智能合约二进制文件使用各自私钥进行签名生成签名值列表。对于合约文件的密钥包，工作密钥为系统随机数，使用
10 区块链节点公钥进行运算，还需要计算密钥的 CRC32 值，为后续使用进行校验。对于智能合约密文包，对智能合约的二进制流进行对称算法的加密运算，在智能合约流转过程中保证了智能合约的保密性。以上作为附加属性，写入到 ELF 文件的附加属性区域中，形成自定义的 ELFext 文件。

15 步骤 102，基于合约文件的解析结果和区块链账本，对合约文件进行验证。

20 在本实施例中，执行主体可以对步骤 101 获得的合约文件进行解析，基于解析得到的结果和区块链账本中相应信息，对合约文件进行验证。验证可以表征对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证，区块链账本通过预先执行合约部署的交易而生成。

25 在一些可选的实现方式中，区块链账本的生成过程如下：响应于接收到请求节点发送的合约部署的交易请求，广播交易请求至区块链网络，并基于交易请求报文对交易进行身份验证，其中，交易请求报文包括：合约部署请求对应的各方法的方法数据包、与合约部署请求对应的各方法对应的参数数据包、合约文件的哈希值和合约文件的位置信息；响应于交易验证通过，根据合约部署请求对应的各方法的方法数据包、与合约部署请求
30

对应的各方法对应的参数数据包、合约文件的哈希值和合约文件的位置信息,生成与交易请求对应的区块;基于共识机制,将区块写入区块链账本,生成写入后的区块链账本。通过对区块链账本进行更新,实现了智能合约方法和参数的动态设置和下发,使智能合约的实现具有更大的灵活性;智能合约经过了区块链共识方的确认,在后续的合约部署环节,以这个交易产生的区块链账本为基准,对动态合约的方法和参数以及摘要值进行验证,保证了动态合约的不可否认性和完整性。

步骤 103, 响应于合约文件验证成功, 根据合约文件, 确定与合约部署请求对应的智能合约。

10 在本实施例中, 当执行主体确定合约文件验证成功后, 可以对合约文件进行解析, 得到合约文件中与合约部署请求对应的智能合约。

需要说明的是, 上述区块链系统中智能合约的部署是目前广泛研究和应用的是公知技术, 在此不再赘述。

继续参见图 2, 本实施例的基于区块链的数据处理方法 200 运行于服务平台 201 中。当服务平台 201 接收到区块链网络中请求节点发送的合约部署请求后, 获取合约部署请求对应的合约文件 202, 然后服务平台 201 基于合约文件的解析结果和区块链账本, 对合约文件进行验证 203, 最后当服务平台 201 确定合约文件验证成功后, 根据合约文件, 确定与合约部署请求对应的智能合约 204。其中, 合约文件基于对合约部署请求对应的智能合约进行内容扩展而生成, 验证用于表征对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证, 区块链账本通过预先执行合约部署的交易而生成。

本申请的上述实施例提供的基于区块链的数据处理方法采用响应于接收到区块链网络中请求节点发送的合约部署请求, 获取合约部署请求对应的合约文件, 其中, 合约文件基于对合约部署请求对应的智能合约进行内容扩展而生成, 基于合约文件的解析结果和区块链账本, 对合约文件进行验证, 响应于合约文件验证成功, 根据合约文件, 确定与合约部署请求对应的智能合约, 实现了通过扩展智能合约文件的文件格式, 动态加载智能合约文件, 而无需重启区块链节点即可运行新的智能合约。通过扩展智能合约文件的文件类型, 对智能合约二进制本身进行了安全控制, 达到安

全的动态加载智能合约的目的。区块链账本通过预先执行合约部署的交易而生成，实现了智能合约方法和参数可以动态设置，而限制智能合约的实现方法和模板，具有更大的灵活性。验证基于对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证，避免了现有技术中通过引入第三
5 方密钥中心带来的安全风险和密钥泄漏的可能性，保证了合约的部署者和批准者的不可否认性和完整性。

进一步参考图 3，其示出了基于区块链的数据处理方法的第二实施例的示意图 300。该方法的流程包括以下步骤：

步骤 301，响应于接收到区块链网络中请求节点发送的合约部署请求，
10 获取合约部署请求对应的合约文件。

在本实施例的一些可选的实现方式中，获取合约部署请求对应的合约文件，包括：基于区块链账本中合约文件的位置信息，获取与合约文件的位置信息对应的合约文件。实现准确快速地查询合约文件。

步骤 302，对合约文件进行内容解析，得到合约文件中各方法的方法
15 名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包和合约文件的密钥包。

在本实施中，执行主体可以对合约文件进行内容解析，得到解析后的合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包和合约文件的密钥包。密钥包通过对请求节
20 点进行加密运算而生成。

在本实施例的一些可选的实现方式中，方法名数据包基于第一加密算法对方法名进行加密而生成；和/或，参数数据包基于第二加密算法对参数进行加密而生成。第一加密算法和第二加密算法即可以相同也可以不同。通过对数据包进行加密，使得智能合约不易被篡改，增加了信息传输的安全
25 性。

步骤 303，基于合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，对合约文件进行验证。

在本实施中，执行主体可以基于合约文件中各方法的方法名数据包、

与合约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，利用预先设定的验证方法对合约文件进行验证。验证用于表征对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证，区块链账本通过预先执行合约部署的交易而生成。

- 5 在本实施例的一些可选的实现方式中，基于合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，对合约文件进行验证，包括：根据合约文件的密钥包，对合约文件进行密钥验证，其中，验证用于表征对请求节点的公私钥对进行验证；根据合约参与方的签名数据包，对合约的参与方进行验证；查询区块链账本，得到合约部署请求对应的各方法的方法名和与合约部署请求对应的各方法对应的参数信息，并根据得到的方法名和参数信息，对合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包进行验证；根据合约文件的密钥验证结果、合约的参与方的验证结果、合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包的验证结果，确定合约文件是否验证成功。经多方/
- 10 多维度验证，更安全地保证了智能合约的不可否认性，完整性和保密性。

- 在本实施例的一些可选的实现方式中，基于合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包，对合约文件进行验证，包括：基于方法名数据包的密文，对合约文件进行验证；和/或，基于参数数据包包的密文，对合约文件进行验证。进一步保证了智能合约的保密性。
- 20 在本实施例的一些可选的实现方式中，基于合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包，对合约文件进行验证，包括：基于合约文件中智能合约文件的密文，对合约文件进行验证。进一步保证了智能合约的保密性。

- 步骤 304，响应于合约文件验证成功，根据合约文件，确定与合约部署请求对应的智能合约。
- 25 在本实施例的一些可选的实现方式中，方法还包括：将智能合约部署于区块链中。实现了智能合约的部署，以使当业务触发调用条件时，根据用户实际的调用参数，执行智能合约。

在本实施例的一些可选的实现方式中，方法还包括：响应于合约文件验证失败，结束合约部署请求。节省了系统资源，提高了系统处理效率。

在本实施例中，步骤 301 和 304 的具体操作与图 1 所示的实施例中的步骤 101 和 103 的操作基本相同，在此不再赘述。

5 从图 3 中可以看出，与图 1 对应的实施例相比，本实施例中的基于区块链的数据处理方法的示意图 300 采用对合约文件进行内容解析，得到合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包和合约文件的密钥包，其中，密钥包通过对请求节点进行加密运算而生成；基于合约文件中各方法的方法名数据包、与合
10 约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，对合约文件进行验证，通过对区块链节点进行身份验证和对合约文件的密文进行验证的双重验证，在保证智能合约的不可否认性和完整性的同时，还保证了合约的保密性。

进一步参考图 4，作为对上述图 1~3 所示方法的实现，本申请提供了一种基于区块链的数据处理装置的一个实施例，该装置实施例与图 1 所示的方法实施例相对应，该装置具体可以应用于各种电子设备中。
15

如图 4 所示，本实施例的基于区块链的数据处理装置 400 包括：获取单元 401、验证单元 402 和确定单元 403，其中，获取单元，被配置成响应于接收到区块链网络中请求节点发送的合约部署请求，获取合约部署请求对应的合约文件，其中，合约文件基于对合约部署请求对应的智能合约进行内容扩展而生成，智能合约为区块链中可自动执行的业务代码；验证单元，被配置成基于合约文件的解析结果和区块链账本，对合约文件进行验证，其中，验证用于表征对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证，区块链账本通过预先执行合约部署的交易而生成；
20 确定单元，被配置成响应于合约文件验证成功，根据合约文件，确定与合约部署请求对应的智能合约。
25

在本实施例中，基于区块链的数据处理装置 400 的获取单元 401、验证单元 402 和确定单元 403 的具体处理及其所带来的技术效果可分别参考图 1 对应的实施例中的步骤 101 到步骤 103 的相关说明，在此不再赘述。

在本实施例的一些可选的实现方式中，验证单元，包括：内容解析模块，被配置成对合约文件进行内容解析，得到合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包和合约文件的密钥包，其中，密钥包通过对请求节点进行加密运算而生成；验证模块，被配置成基于合约文件中各方法的方法名数据包、与合约文件中各方法对应的参数数据包、合约参与方的签名数据包、合约文件的密钥包和区块链账本，对合约文件进行验证。

在本实施例的一些可选的实现方式中，验证模块，包括：第一验证子模块，被配置成根据合约文件的密钥包，对合约文件进行密钥验证，其中，验证用于表征对请求节点的公私钥对进行验证；第二验证子模块，被配置成根据合约参与方的签名数据包，对合约的参与方进行验证；第三验证子模块，被配置成查询区块链账本，得到合约部署请求对应的各方法的方法名和与合约部署请求对应的各方法对应的参数信息，并根据得到的方法名和参数信息，对合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包进行验证；确定子模块，被配置成根据合约文件的密钥验证结果、合约的参与方的验证结果、合约文件中各方法的方法名数据包和与合约文件中各方法对应的参数数据包的验证结果，确定合约文件是否验证成功。

在本实施例的一些可选的实现方式中，区块链账本利用如下模块生成：交易验证模块，被配置成响应于接收到请求节点发送的合约部署的交易请求，广播交易请求至区块链网络，并基于交易请求报文对交易进行验证，其中，交易请求报文包括：合约部署请求对应的各方法的方法数据包、与合约部署请求对应的各方法对应的参数数据包、合约文件的哈希值和合约文件的位置信息；生成模块，被配置成响应于交易验证通过，根据合约部署请求对应的各方法的方法数据包、与合约部署请求对应的各方法对应的参数数据包、合约文件的哈希值和合约文件的位置信息，生成与交易请求对应的区块；写入模块，被配置成基于共识机制，将区块写入区块链账本，生成写入后的区块链账本。

在本实施例的一些可选的实现方式中，获取单元进一步被配置成基于

区块链账本中合约文件的位置信息，获取与合约文件的位置信息对应的合约文件。

在本实施例的一些可选的实现方式中，内容解析模块中的方法名数据包基于第一加密算法对方法名进行加密而生成；和/或，内容解析模块中的
5 参数数据包基于第二加密算法对参数进行加密而生成。

在本实施例的一些可选的实现方式中，验证模块进一步被配置成基于方法名数据包的密文，对合约文件进行验证；和/或，基于参数数据包的密文，对合约文件进行验证。

在本实施例的一些可选的实现方式中，装置还包括：部署单元，被配置成将智能合约部署于区块链中，以使当业务触发调用条件时，执行智能
10 合约。

在本实施例的一些可选的实现方式中，装置还包括：结束单元，被配置成响应于合约文件验证失败，结束合约部署请求。

根据本申请的实施例，本申请还提供了一种电子设备和一种可读存储
15 介质。

如图 5 所示，是根据本申请实施例的基于区块链的数据处理方法的电子设备的框图。电子设备旨在表示各种形式的数字计算机，诸如，膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动
20 装置，诸如，个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例，并且不意在限制本文中描述的和/或者要求的本申请的实现。

如图 5 所示，该电子设备包括：一个或多个处理器 501、存储器 502，以及用于连接各部件的接口，包括高速接口和低速接口。各个部件利用不同的总线互相连接，并且可以被安装在公共主板上或者根据需要以其它方式安装。处理器可以对在电子设备内执行的指令进行处理，包括存储在存储器中或者存储器上以在外部输入/输出装置（诸如，耦合至接口的显示设备）上显示 GUI 的图形信息的指令。在其它实施方式中，若需要，可以将
25 多个处理器和/或多条总线与多个存储器和多个存储器一起使用。同样，可以连接多个电子设备，各个设备提供部分必要的操作（例如，作为服务器
30

阵列、一组刀片式服务器、或者多处理器系统)。图 5 中以一个处理器 501 为例。

存储器 502 即为本申请所提供的非瞬时计算机可读存储介质。其中，存储器存储有可由至少一个处理器执行的指令，以使至少一个处理器执行本申请所提供的基于区块链的数据处理方法。本申请的非瞬时计算机可读存储介质存储计算机指令，该计算机指令用于使计算机执行本申请所提供的基于区块链的数据处理方法。

存储器 502 作为一种非瞬时计算机可读存储介质，可用于存储非瞬时软件程序、非瞬时计算机可执行程序以及模块，如本申请实施例中的基于区块链的数据处理方法对应的程序指令/模块(例如，附图 4 所示的获取单元 401、验证单元 402 和确定单元 403)。处理器 501 通过运行存储在存储器 502 中的非瞬时软件程序、指令以及模块，从而执行服务器的各种功能应用以及数据处理，即实现上述方法实施例中的基于区块链的数据处理方法。

存储器 502 可以包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需要的应用程序；存储数据区可存储根据基于区块链的数据处理电子设备的使用所创建的数据等。此外，存储器 502 可以包括高速随机存取存储器，还可以包括非瞬时存储器，例如至少一个磁盘存储器件、闪存器件、或其他非瞬时固态存储器件。在一些实施例中，存储器 502 可选包括相对于处理器 501 远程设置的存储器，这些远程存储器可以通过网络连接至基于区块链的数据处理电子设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

基于区块链的数据处理方法的电子设备还可以包括：输入装置 503 和输出装置 504。处理器 501、存储器 502、输入装置 503 和输出装置 504 可以通过总线或者其他方式连接，图 5 中以通过总线连接为例。

输入装置 503 可接收输入的数字或字符信息，以及产生与基于区块链的数据处理电子设备的用户设置以及功能控制有关的键信号输入，例如触摸屏、小键盘、鼠标、轨迹板、触摸板、指示杆、一个或者多个鼠标按钮、轨迹球、操纵杆等输入装置。输出装置 504 可以包括显示设备、辅助照明装置(例如，LED)和触觉反馈装置(例如，振动电机)等。该显示设备

可以包括但不限于，液晶显示器（LCD）、发光二极管（LED）显示器和等离子体显示器。在一些实施方式中，显示设备可以是触摸屏。

此处描述的系统和技术各种实施方式可以在数字电子电路系统、集成电路系统、专用 ASIC（专用集成电路）、计算机硬件、固件、软件、
5 和/或它们的组合中实现。这些各种实施方式可以包括：实施在一个或者多个计算机程序中，该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，该可编程处理器可以是专用或者通用可编程处理器，可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令，并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。
10

这些计算程序（也称作程序、软件、软件应用、或者代码）包括可编程处理器的机器指令，并且可以利用高级过程和/或面向对象的编程语言、和/或汇编/机器语言来实施这些计算程序。如本文使用的，术语“机器可读介质”和“计算机可读介质”指的是用于将机器指令和/或数据提供给可
15 编程处理器的任何计算机程序产品、设备、和/或装置（例如，磁盘、光盘、存储器、可编程逻辑装置（PLD）），包括，接收作为机器可读信号的机器指令的机器可读介质。术语“机器可读信号”指的是用于将机器指令和/或数据提供给可编程处理器的任何信号。

为了提供与用户的交互，可以在计算机上实施此处描述的系统和技术，
20 该计算机具有：用于向用户显示信息的显示装置（例如，CRT（阴极射线管）或者 LCD（液晶显示器）监视器）；以及键盘和指向装置（例如，鼠标或者轨迹球），用户可以通过该键盘和该指向装置来将输入提供给计算机。其它种类的装置还可以用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的传感反馈（例如，视觉反馈、听觉反馈、或者触觉反馈）；并且可以用任何形式（包括声输入、语音输入或者、触觉输入）
25 来接收来自用户的输入。

可以将此处描述的系统和技术实施在包括后台部件的计算系统（例如，作为数据服务器）、或者包括中间件部件的计算系统（例如，应用服务器）、或者包括前端部件的计算系统（例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处
30

描述的系统和技术实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如,通信网络)来将系统的部件相互连接。通信网络的示例包括:局域网(LAN)、广域网(WAN)和互联网。

- 5 计算机系统可以包括客户端和服务端。客户端和服务端一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务端的关系。

- 根据本申请实施例的技术方案采用响应于接收到区块链网络中请求节点发送的合约部署请求,获取合约部署请求对应的合约文件,其中,合约文件基于对合约部署请求对应的智能合约进行内容扩展而生成,基于合约文件的解析结果和区块链账本,对合约文件进行验证,响应于合约文件验证成功,根据合约文件,确定与合约部署请求对应的智能合约,实现了通过扩展智能合约文件(ELF文件)的文件格式,动态加载智能合约文件,而无需重启区块链节点即可运行新的智能合约。通过扩展智能合约 ELF
- 10 文件的文件类型,对智能合约二进制本身进行了安全控制,达到安全的动态加载智能合约的目的。区块链账本通过预先执行合约部署的交易而生成,实现了智能合约方法和参数可以动态设置,而限制智能合约的实现方法和模板,具有更大的灵活性。验证基于对合约文件的密钥、合约文件的内容和合约参与方的签名进行验证,避免了现有技术中通过引入第三方密钥中心带来的安全风险和密钥泄漏的可能性,保证了合约的部署者和批准者的不可否认性和完整性。
- 15
- 20

- 应该理解,可以使用上面所示的各种形式的流程,重新排序、增加或删除步骤。例如,本申请中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行,只要能够实现本申请公开的技术方案所期望的结果,本文在此不进行限制。
- 25

上述具体实施方式,并不构成对本申请保护范围的限制。本领域技术人员应该明白的是,根据设计要求和因素,可以进行各种修改、组合、子组合和替代。任何在本申请的精神和原则之内所作的修改、等同替换和改进等,均应包含在本申请保护范围之内。

权 利 要 求

1. 一种基于区块链的数据处理方法，所述方法包括：
响应于接收到区块链网络中请求节点发送的合约部署请求，获取所述合约部署请求对应的合约文件，其中，所述合约文件基于对所述合约部署请求对应的智能合约进行内容扩展而生成，所述智能合约
5 为所述区块链中可自动执行的业务代码；
基于所述合约文件的解析结果和所述区块链账本，对所述合约文件进行验证，其中，所述验证用于表征对所述合约文件的密钥、
10 所述合约文件的内容和所述合约参与方的签名进行验证，所述区块链账本通过预先执行所述合约部署的交易而生成；以及
响应于所述合约文件验证成功，根据所述合约文件，确定与所述合约部署请求对应的智能合约。
- 15 2. 根据权利要求 1 所述方法，其中，所述基于所述合约文件的解析结果和所述区块链账本，对所述合约文件进行验证，包括：
对所述合约文件进行内容解析，得到所述合约文件中各方法的方法名数据包、与所述合约文件中各方法对应的参数数据包、所述合约参与方的签名数据包和所述合约文件的密钥包，其中，所述密
20 钥包通过对所述请求节点进行加密运算而生成；以及
基于所述合约文件中各方法的方法名数据包、与所述合约文件中各方法对应的参数数据包、所述合约参与方的签名数据包、所述合约文件的密钥包和所述区块链账本，对所述合约文件进行验证。
- 25 3. 根据权利要求 2 所述方法，其中，所述基于所述合约文件中各方法的方法名数据包、与所述合约文件中各方法对应的参数数据包、所述合约参与方的签名数据包、所述合约文件的密钥包和所述区块链账本，对所述合约文件进行验证，包括：
根据所述合约文件的密钥包，对所述合约文件进行密钥验证，
30 其中，所述验证用于表征对所述请求节点的公私钥对进行验证；

根据所述合约参与方的签名数据包, 对所述合约的参与方进行验证;

5 查询所述区块链账本, 得到所述合约部署请求对应的各方法的方法名和与所述合约部署请求对应的各方法对应的参数信息, 并根据得到的所述方法名和所述参数信息, 对所述合约文件中各方法的方法名数据包和与所述合约文件中各方法对应的参数数据包进行验证; 以及

10 根据所述合约文件的密钥验证结果、所述合约的参与方的验证结果、所述合约文件中各方法的方法名数据包和与所述合约文件中各方法对应的参数数据包的验证结果, 确定所述合约文件是否验证成功。

4. 根据权利要求 1 所述方法, 其中, 所述区块链账本的生成过程如下:

15 响应于接收到所述请求节点发送的所述合约部署的交易请求, 广播所述交易请求至所述区块链网络, 并基于所述交易请求报文对所述交易进行验证, 其中, 所述交易请求报文包括: 所述合约部署请求对应的各方法的方法数据包、与所述合约部署请求对应的各方法对应的参数数据包、所述合约文件的哈希值和所述合约文件的位置信息;

20 响应于所述交易验证通过, 根据所述合约部署请求对应的各方法的方法数据包、与所述合约部署请求对应的各方法对应的参数数据包、所述合约文件的哈希值和所述合约文件的位置信息, 生成与所述交易请求对应的区块; 以及

25 基于共识机制, 将所述区块写入所述区块链账本, 生成写入后的所述区块链账本。

5. 根据权利要求 4 所述方法, 其中, 所述获取所述合约部署请求对应的合约文件, 包括:

30 基于所述区块链账本中所述合约文件的位置信息, 获取与所述

合约文件的位置信息对应的合约文件。

6. 根据权利要求 2 所述方法，其中，所述方法名数据包基于第一加密算法对所述方法名进行加密而生成；和/或，所述参数数据包
5 基于第二加密算法对所述参数进行加密而生成。

7. 根据权利要求 6 所述方法，其中，所述基于所述合约文件中各方法的方法名数据包和与所述合约文件中各方法对应的参数数据包，对所述合约文件进行验证，包括：

10 基于所述方法名数据包的密文，对所述合约文件进行验证；和/或，基于所述参数数据包的密文，对所述合约文件进行验证。

8. 根据权利要求 1 所述方法，还包括：

15 将所述智能合约部署于所述区块链中，以使当业务触发调用条件时，执行所述智能合约。

9. 根据权利要求 1 所述方法，还包括：

响应于所述合约文件验证失败，结束所述合约部署请求。

20 10. 一种基于区块链的数据处理装置，所述装置包括：

获取单元，被配置成响应于接收到区块链网络中请求节点发送的合约部署请求，获取所述合约部署请求对应的合约文件，其中，所述合约文件基于对所述合约部署请求对应的智能合约进行内容扩展而生成，所述智能合约为所述区块链中可自动执行的业务代码；

25 验证单元，被配置成基于所述合约文件的解析结果和所述区块链账本，对所述合约文件进行验证，其中，所述验证用于表征对所述合约文件的密钥、所述合约文件的内容和所述合约参与方的签名进行验证，所述区块链账本通过预先执行所述合约部署的交易而生成；以及

30 确定单元，被配置成响应于所述合约文件验证成功，根据所述

合约文件，确定与所述合约部署请求对应的智能合约。

11. 根据权利要求 10 所述装置，其中，所述验证单元，包括：

5 内容解析模块，被配置成对所述合约文件进行内容解析，得到所述合约文件中各方法的方法名数据包、与所述合约文件中各方法对应的参数数据包、所述合约参与方的签名数据包和所述合约文件的密钥包，其中，所述密钥包通过对所述请求节点进行加密运算而生成；以及

10 验证模块，被配置成基于所述合约文件中各方法的方法名数据包、与所述合约文件中各方法对应的参数数据包、所述合约参与方的签名数据包、所述合约文件的密钥包和所述区块链账本，对所述合约文件进行验证。

12. 根据权利要求 11 所述装置，其中，所述验证模块，包括：

15 第一验证子模块，被配置成根据所述合约文件的密钥包，对所述合约文件进行密钥验证，其中，所述验证用于表征对所述请求节点的公私钥对进行验证；

第二验证子模块，被配置成根据所述合约参与方的签名数据包，对所述合约的参与方进行验证；

20 第三验证子模块，被配置成查询所述区块链账本，得到所述合约部署请求对应的各方法的方法名和与所述合约部署请求对应的各方法对应的参数信息，并根据得到的所述方法名和所述参数信息，对所述合约文件中各方法的方法名数据包和与所述合约文件中各方法对应的参数数据包进行验证；以及

25 确定子模块，被配置成根据所述合约文件的密钥验证结果、所述合约的参与方的验证结果、所述合约文件中各方法的方法名数据包和与所述合约文件中各方法对应的参数数据包的验证结果，确定所述合约文件是否验证成功。

30 13. 根据权利要求 10 所述装置，其中，所述区块链账本利用如

下模块生成:

交易验证模块, 被配置成响应于接收到所述请求节点发送的所述合约部署的交易请求, 广播所述交易请求至所述区块链网络, 并基于所述交易请求报文对所述交易进行验证, 其中, 所述交易请求
5 报文包括: 所述合约部署请求对应的各方法的方法数据包、与所述合约部署请求对应的各方法对应的参数数据包、所述合约文件的哈希值和所述合约文件的位置信息;

生成模块, 被配置成响应于所述交易验证通过, 根据所述合约部署请求对应的各方法的方法数据包、与所述合约部署请求对应的
10 各方法对应的参数数据包、所述合约文件的哈希值和所述合约文件的位置信息, 生成与所述交易请求对应的区块; 以及

写入模块, 被配置成基于共识机制, 将所述区块写入所述区块链账本, 生成写入后的所述区块链账本。

15 14. 根据权利要求 13 所述装置, 其中, 所述获取单元进一步被配置成基于所述区块链账本中所述合约文件的位置信息, 获取与所述合约文件的位置信息对应的合约文件。

20 15. 根据权利要求 11 所述装置, 其中, 所述内容解析模块中的所述方法名数据包基于第一加密算法对所述方法名进行加密而生成; 和/或, 所述内容解析模块中的所述参数数据包基于第二加密算法对所述参数进行加密而生成。

25 16. 根据权利要求 15 所述装置, 其中, 所述验证模块进一步被配置成基于所述方法名数据包的密文, 对所述合约文件进行验证; 和/或, 基于所述参数数据包的密文, 对所述合约文件进行验证。

17. 根据权利要求 10 所述装置, 还包括:

30 部署单元, 被配置成将所述智能合约部署于所述区块链中, 以使当业务触发调用条件时, 执行所述智能合约。

18. 根据权利要求 10 所述装置，还包括：

结束单元，被配置成响应于所述合约文件验证失败，结束所述合约部署请求。

5

19. 一种电子设备，其特征在于，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

10 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求 1-9 中任一项所述的方法。

20. 一种存储有计算机指令的非瞬时计算机可读存储介质，其

15 特征在于，所述计算机指令用于使所述计算机执行权利要求 1-9 中任一项所述的方法。