

权利要求书

- 1、一种基于区块链智能合约的签名验证方法，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；
- 5 智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令；
- 区块链网络中部署有所述业务智能合约；
- 所述签名验证方法包括：
- 所述区块链网络中的节点获得业务发起交易并广播给其他节点；
- 10 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；
- 该节点通过区块链虚拟机，根据所述业务智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作。
- 2、如权利要求 1 所述的方法，所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据以及用于验证所述业务签名的公钥；或，
- 15 所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据的摘要以及用于验证所述业务签名的公钥；或，
- 所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据，所述业务智能合约包含用于验证所述业务签名的公钥；或，
- 20 所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据的摘要，所述业务智能合约包含用于验证所述业务签名的公钥。
- 3、一种基于区块链智能合约的签名验证方法，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；
- 25 智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约；
- 区块链网络中部署有所述业务智能合约；
- 所述签名验证方法包括：
- 30 所述区块链网络中的节点获得业务发起交易并广播给其他节点；
- 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块

链虚拟机，调用所述业务智能合约；

该节点通过区块链虚拟机，根据所述业务智能合约中的所述 RSA 签名验证智能合约的合约标识，调用所述 RSA 签名验证智能合约；

- 该节点通过区块链虚拟机，根据所述 RSA 签名验证智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

4、一种区块链虚拟机，用于实现权利要求 1~3 任一项所述的方法，其中，

智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令。

- 5、如权利要求 4 所述的区块链虚拟机，所述区块链虚拟机的指令集中还包括至少一个以太坊指令，以太坊指令是以太坊虚拟机的指令集中的指令；

针对所述区块链虚拟机的指令集中包括的每个以太坊指令，所述区块链虚拟机中部署有对应于该以太坊指令的相关逻辑。

6、一种智能合约编译器，用于实现权利要求 1 所述的方法，其中，

- 智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令。

7、如权利要求 6 所述的智能合约编译器，所述智能合约编译器的指令集中还包括至少一个以太坊指令，以太坊指令是以太坊虚拟机的指令集中的指令。

8、一种智能合约编译器，用于实现权利要求 3 所述的方法，其中，

- 智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约。

9、一种区块链系统，包括区块链网络，其中，

- 区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令；区块链网络中部署有所述业务智能合约；

所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

- 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以

对业务签名进行 RSA 签名验证操作。

10、一种区块链系统，包括区块链网络，其中，

区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括
5 所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约；区块链网络中部署有所述业务智能合约；

所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，
10 调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 RSA 签名验证智能合约的合约标识，调用所述 RSA 签名验证智能合约；通过区块链虚拟机，根据所述 RSA 签名验证智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

11、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行
15 的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 1~3 任一项所述的方法。