

地址的生成方法、区块链信息的处理方法以及相关设备

本申请要求于 2020 年 10 月 31 日提交中国专利局、申请号为 202011196897.1、发明名称为“地址的生成方法、区块链信息的处理方法以及相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机技术领域，尤其涉及一种地址的生成方法、区块链信息的处理方法以及相关设备。

背景技术

区块链本质上是一个去中心化的数据库，它依靠密码学和数学巧妙的分布式算法，在无法建立信任关系的互联网上，无需借助任何第三方中心的介入就可以使参与者达成共识，以极低的成本解决了信任与价值的可靠传递难题，基于区块链的分布式身份和数据管理平台是未来数字世界的发展趋势。

区块链虽然以其公开、透明、不可篡改的特性备受大家的信赖，但是正是由于其公开、透明的性质，使得其隐私问题成为了最受大家关注的问题。例如对于基于区块链的供应链应用，公开于区块链上的交易内容会涉及买卖双方和商品信息，这些信息都是敏感信息。一个生产商并不想别人知道他的零售商都是谁，一个零售商不想别人知道他的客户是谁。

为了解决上述问题，可以在每次交易过程中，商品的接收方均使用一个新的公钥地址，这样从第三方来看，就无法将多个公钥地址关联到一个人，从而能够达到保护隐私的效果。但这需要接收方存储并管理多个公私钥对，管理难度高。

发明内容

本申请实施例提供了一种地址的生成方法、区块链信息的处理方法以及相关设备，用于验证的共享密钥也可以通过第一区块链节点的公钥和第二区块链节点的第一私钥生成，也即接收方也可以生成共享密钥，以对交易信息进行验证，接收方无需存储并管理多个公私钥对，降低了管理难度。

为解决上述技术问题，本申请实施例提供以下技术方案：

第一方面，本申请实施例提供一种地址的生成方法，可用于区块链领域中。方法包括：第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥；其中，第一区块链节点的私钥为第一区块链节点的固定密钥，第二区块链节点的第一公钥为第二区块链节点的固定密钥。第一区块链节点根据共享密钥和第一交易内容生成第二区块链节点的临时的第一公钥地址，由于该第一公钥地址仅在第一区块链节点向第二区块链节点发送第一交易信息时使用，所以将第一公钥地址称为临时的公钥地址，也可以称为一次性的公钥地址。第一区块链节点将第一交易信息写入区块链，也即第一区块链节点将第一交易信息上链，第一交易信息包括第一区块链节点的公钥地址（也即交易发送方的公钥地址）、第一公钥地址（也即交易接收方的公钥地址）和第一交易内容。其中，第一交易内

-2-

容为第一区块链节点和第二区块链节点之间的当前交易的内容，第一交易内容中包括时间戳，用于指示第一交易内容所指向的交易的时间。若第一交易内容所指向的交易是由第一区块链节点首创的，则无论第一区块链节点拥有一套固定密钥，还是拥有两套固定密钥，第一区块链节点的公钥地址均为根据第一区块链节点的长期公钥生成的。若第一交易内容所指向的交易为第三区块链节点转移给第一区块链节点的，则第一区块链节点的公钥地址与该第一公钥地址类似，为第三区块链节点为第一区块链节点生成的临时公钥地址。写入区块链的第一交易信息由第二区块链节点根据第一公钥地址进行验证，第一公钥地址需要利用共享密钥进行验证，共享密钥在第二区块链节点处通过第一区块链节点的公钥和第二区块链节点的第一私钥生成。

本实现方式中，由于第一交易信息的公钥地址是根据共享密钥和第一交易内容生成的，而不同交易中的交易内容是不同的，则区块链上的每个交易信息的公钥地址都是一次性的，从而可以很好的保护接收方的隐私；且共享密钥也可以通过第一区块链节点的公钥和第二区块链节点的第一私钥生成，也即接收方也可以生成共享密钥，并根据共享密钥和第一交易内容生成第一交易信息的公钥地址，以对交易信息进行验证，接收方无需存储并管理多个公私钥对，降低了管理难度。

在第一方面的一种可能实现方式中，第一区块链节点根据共享密钥和第一交易内容生成第一交易信息的第一公钥地址，包括：第一区块链节点根据共享密钥和第一交易内容生成临时的第二私钥；其中，由于与不同交易对应的交易内容不同，则根据不同的交易内容生成的私钥不同，所以第二私钥为一次性的，或者说第二私钥为临时的，而不是固定的。需要说明的是，第二私钥为生成第二区块链节点的一次性公钥地址的过程中所产生的密钥，并不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密。第一区块链节点根据第二私钥和第二区块链节点的第二公钥生成临时的第三公钥，并根据该临时的第三公钥生成第二区块链节点的临时的第一公钥地址。需要说明的是，第三公钥的作用与第二私钥的功能类似，均为生成第二区块链节点的一次性公钥地址的过程中所生成的密钥，并不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密。无论第二区块链节点拥有一套固定密钥还是两套固定密钥，第二区块链节点的第二公钥均为第二区块链节点的长期公钥。

本申请实施例中，根据第二私钥和第二区块链节点的第二公钥生成第一公钥地址，则需要借助第二区块链节点的第三私钥才能够生成花费第一交易信息中的产品时所使用的私钥，从而避免了第一区块链节点在将第一交易信息中的产品转移给第二区块链节点之后，还能够花费第一交易信息中的产品，以保证了第二区块链节点的财产的安全性，也包括了区块链上交易的稳定性。

在第一方面的一种可能实现方式中，第一区块链节点根据共享密钥和第一交易内容生成第二私钥，包括：第一区块链节点将共享密钥和第一交易内容进行组合，得到第一组合结果，对第一组合结果进行哈希运算，以生成第二私钥。组合的方式包括但不限于拼接、异/或运算、相加等；采用的哈希函数包括但不限于 SHA256、SHA512 或其他哈希函数。本申请实施例中，提供了生成第二私钥的具体实现方式，操作简单，易于实现。

在第一方面的一种可能实现方式中，第一区块链节点根据第二私钥和第二区块链节点的第二公钥生成第一公钥地址，包括：第一区块链节点在椭圆曲线的公钥密码体系中，根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥；并在椭圆曲线的公钥密码体系的约束下，根据临时的第三公钥，生成临时的第一公钥地址。或者，第一区块链节点在离散对数的公钥密码体系中，根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥；并在离散对数的公钥密码体系的约束下，根据临时的第三公钥，生成临时的第一公钥地址。

本申请实施例中，无论是在椭圆曲线的公钥密码体系下，还是在离散对数的公钥密码体系下，均能根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，并根据临时的第三公钥，生成临时的第一公钥地址，扩展了本方案的应用场景。

在第一方面的一种可能实现方式中，第一区块链节点在椭圆曲线的公钥密码体系中，根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，包括：第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与生成元 G （也即椭圆曲线群的生成元）进行点乘，可以生成临时的公钥 R ，进而将临时的公钥 R 与第二区块链节点的第二公钥 B 相加，以生成临时的第三公钥 T ，也即临时的第三公钥 $T=R+B$ 。

在第一方面的一种可能实现方式中，第一区块链节点在椭圆曲线的公钥密码体系中，根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，包括：第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与生成元 G （也即椭圆曲线群的生成元）进行点乘，可以生成临时的公钥 R ，进而将临时的公钥 R 与第二区块链节点的第二公钥 B 相减，以生成临时的第三公钥 T ，也即临时的第三公钥 $T=R-B$ 。

在第一方面的一种可能实现方式中，第一区块链节点在椭圆曲线的公钥密码体系中，根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，包括：第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与第二区块链节点的第二公钥 B 相乘，以生成临时的第三公钥 T ，也即临时的第三公钥 $T=r \cdot B$ 。

在第一方面的一种可能实现方式中，第一区块链节点在椭圆曲线的公钥密码体系中，根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，包括：第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 的倒数与第二区块链节点的第二公钥 B 相乘，以生成临时的第三公钥 T 。

在第一方面的一种可能实现方式中，第一区块链节点在离散对数的公钥密码体系中，根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，包括：第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与第二区块链节点的第二公钥 B 进行指数运算，以生成临时的第三公钥 T ；其中，第二区块链节点的第二公钥 B 为前述指数运算的底数，临时的第二私钥 r 为前述指数运算的指数。

在第一方面的一种可能实现方式中，第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥，包括以下两项中的任一项：在椭圆曲线的公钥密码体系中，第一区块链节点将第一区块链节点的私钥与第二区块链节点的第一公钥进行点乘，得到共享密钥。或者，在离散对数的公钥密码体系中，第一区块链节点根据第一区块

-4-

链节点的私钥和第二区块链节点的第一公钥，进行指数运算，得到共享密钥，第二区块链节点的第一公钥为指数运算中的底数，第一区块链节点的私钥为指数运算中的指数。

本申请实施例中，分别公开了在椭圆曲线的公钥密码体系和离散对数的公钥密码体系下，共享密钥的生成方式，扩展了本方案的应用场景。

5 在第一方面的一种可能实现方式中，第一区块链节点和第二区块链节点均仅拥有一套固定密钥，一套固定密钥中包括一个长期私钥和一个长期公钥；第一区块链节点的私钥指的是第一区块链节点的长期私钥，第二区块链节点的第一公钥指的是第二区块链节点的长期公钥，第一区块链节点的公钥指的是第一区块链节点的长期公钥，第二区块链节点的第一私钥指的是第二区块链节点的长期私钥。或者，第一区块链节点和第二区块链节点均拥有两套固定密钥，两套固定密钥包括第一套固定密钥和第二套固定密钥，第一套固定密钥包括一个长期私钥和一个长期公钥，第二套固定密钥包括一个扫描私钥和一个扫描公钥，第一区块链节点的私钥为第一区块链节点的长期私钥，第二区块链节点的第一公钥为第二区块链节点的扫描公钥，第一区块链节点的公钥为第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的扫描私钥。

15 本申请实施例中，提供的区块链信息的处理方法不仅可以适用于区块链节点仅拥有一套固定密钥的情况，而且还适用于区块链拥有两套固定密钥的情况，扩展了本方案的应用场景。

第二方面，本申请实施例提供了一种区块链信息的处理方法，可用于区块链领域中。方法包括：第二区块链节点根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥；其中，第一区块链节点的公钥为第一区块链节点的固定密钥，第二区块链节点的第一私钥为第二区块链节点的固定密钥。第二区块链节点对区块链上的至少一个交易信息进行读取，在至少一个交易信息中存在第一交易信息的情况下，确定第一交易内容指向的交易为交易成功；也即第二区块链节点需要对区块链上的每个交易信息进行读取，以逐个判断区块链上的每个交易信息中是否为第一交易信息。第一交易信息包括第一区块链节点的公钥地址、第一交易内容和第二区块链节点的第一公钥地址；第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，第一公钥地址能够根据共享密钥和第一交易内容生成。具体的，针对判断一个交易信息是否为第一交易信息的过程。第二区块链节点在读取到一个交易信息之后，会获取该交易信息中的交易内容，并根据生成的共享密钥和获取到的交易内容，生成一个临时的公钥地址，具体生成方式与生成临时的第一公钥地址的方式一致。进而判断第一公钥地址与该交易信息中的携带的接收方的公钥地址是否一致，若一致，则视为该交易信息为第一交易信息，若不一致，则视为该交易信息不是第一交易信息。

30 在第二方面的一种可能实现方式中，第二区块链节点根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥，包括：第二区块链节点在椭圆曲线的公钥密码体系中，将第一区块链节点的公钥和第二区块链节点的第一私钥进行点乘，得到共享密钥。或者，第二区块链节点在离散对数的公钥密码体系中，根据第一区块链节点的公钥和第二区块链节点的第一私钥，进行指数运算，第一区块链节点的公钥为指数运算中的底数，第

二区块链节点的第一私钥为指数运算中的指数。

在第二方面的一种可能实现方式中，方法还包括：第二区块链节点在确定第一交易信息指向的交易为交易成功的情况下，当第二区块链节点需要花费第一交易信息中的产品时，第二区块链节点根据共享密钥和第一交易内容，生成第二私钥，根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的临时的第四私钥，第四私钥用于花费第一交易信息中的产品。第二区块链节点的第三私钥是第二区块链节点的固定密钥，无论第二区块链节点包括一套固定密钥还是两套固定密钥，第二区块链节点的第三私钥均为第二区块链节点的长期私钥。本申请实施例中，提供了当第二区块链节点想要花费第一交易信息中的产品时，生成花费第一交易信息中的产品的私钥的具体生成方式，扩展了本方案的应用场景，且增加了本方案的完整性。

在第二方面的一种可能实现方式中，第二区块链节点根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的第四私钥，包括：在椭圆曲线的公钥密码体系中，第二区块链节点根据将第二私钥 r 与第二区块链节点的第三私钥 b 相加，得到第一相加结果，将第一相加结果与生成元的阶 q 进行求余运算，得到第二区块链节点的临时的第四私钥，也即临时的第四私钥 $t = (r+b) \bmod q$ 。

在第二方面的一种可能实现方式中，第二区块链节点根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的第四私钥，包括：在椭圆曲线的公钥密码体系中，第二区块链节点将第二私钥 r 与第二区块链节点的第三私钥 b 相减，得到第一相减结果，将第一相减结果与生成元的阶 q 进行求余运算，得到第二区块链节点的临时的第四私钥，也即临时的第四私钥 $t = (r-b) \bmod q$ 。

在第二方面的一种可能实现方式中，第二区块链节点根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的第四私钥，包括：在椭圆曲线的公钥密码体系中，第二区块链节点将第二私钥 r 与第二区块链节点的第三私钥 b 相乘，将前述相乘结果与生成元的阶 q 进行求余运算，得到第二区块链节点的临时的第四私钥，也即临时的第四私钥 $t = (rb) \bmod q$ 。

在第二方面的一种可能实现方式中，第二区块链节点根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的第四私钥，包括：在椭圆曲线的公钥密码体系中，第二区块链节点根据临时的第二私钥 r ，第二私钥 r 的倒数与第二区块链节点的第三私钥 b 相乘，将相乘结果与生成元的阶 q 进行求余运算，得到第二区块链节点的临时的第四私钥。

在第二方面的一种可能实现方式中，第二区块链节点根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的第四私钥，包括：在离散对数的公钥密码体系中，第二区块链节点将临时的第二私钥 r 与第二区块链节点的第三私钥 b 进行指数运算，得到第一运算结果；第三私钥 b 为前述指数运算的底数，第二私钥 r 为前述指数运算的指数。第二区块链节点将第一运算结果与生成元的阶 q 进行求余运算，得到第二区块链节点的临时的第四私钥。

在第二方面的一种可能实现方式中，第一区块链节点和第二区块链节点均仅拥有一套固定密钥，一套固定密钥中包括一个长期私钥和一个长期公钥，第一区块链节点的公钥为

第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的长期私钥。或者，第一区块链节点和第二区块链节点均拥有两套固定密钥，两套固定密钥包括第一套固定密钥和第二套固定密钥，第一套固定密钥包括一个长期私钥和一个长期公钥，第二套固定密钥包括一个扫描私钥和一个扫描公钥，第一区块链节点的公钥为第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的扫描私钥。

对于本申请实施例第二方面以及第二方面的各种可能实现方式中名词的概念、具体实现步骤以及每种可能实现方式所带来的有益效果，均可以参考第一方面中各种可能的实现方式中的描述，此处不再一一赘述。

第三方面，本申请实施例提供了一种地址的生成方法，可用于区块链领域中。方法包括：第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥；第一区块链节点随机生成临时的第五私钥，并根据临时的第五私钥生成第二区块链节点的临时的第二公钥地址；第五私钥为生成第二区块链节点的一次性公钥地址的过程中所产生的私钥，并不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密；由于该第二公钥地址仅在第一区块链节点向第二区块链节点发送第二交易信息时使用，所以将第二公钥地址称为临时的公钥地址，也可以称为一次性的公钥地址。第一区块链节点采用共享密钥对第五私钥进行对称加密，得到加密后的第五私钥；对称加密的算法包括但不限于数据加密标准、3 数据加密标准、高级加密标准等。第一区块链节点将第二交易信息写入区块链，第二交易信息包括第一区块链节点的公钥地址（也即交易发送方的公钥地址）、第二公钥地址（也即交易接收方的公钥地址）、第一交易内容和加密后的第五私钥。其中，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，写入区块链的第二交易信息由第二区块链节点根据第二公钥地址进行验证，第二公钥为根据第五私钥生成，加密后的第五私钥需要利用共享密钥进行对称解密，共享密钥在第二区块链节点处通过第一区块链节点的公钥和第二区块链节点的第一私钥生成。

本申请实施例中，在隐藏交易接收方的真实地址的前提下，提供了交易接收方无需存储并管理多个公私钥对的又一实现方案，提高了本方案的实现灵活性。

在第三方面的一种可能实现方式中，第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥，包括以下两项中的任一项：第一区块链节点在椭圆曲线的公钥密码体系中，将第一区块链节点的私钥与第二区块链节点的第一公钥进行点乘，得到共享密钥。或者，第一区块链节点在离散对数的公钥密码体系中，根据第一区块链节点的私钥和第二区块链节点的第一公钥，进行指数运算，第二区块链节点的第一公钥为指数运算中的底数，第一区块链节点的私钥为指数运算中的指数。

在第三方面的一种可能实现方式中，第一区块链节点根据第五私钥生成第二区块链节点的第二公钥地址，包括：第一区块链节点根据第五私钥和第二区块链节点的第二公钥，生成临时的第四私钥，根据临时的第四私钥，生成第二区块链的临时的第二公钥地址；临时的第四公钥为生成第二区块链节点的第二公钥地址的过程中产生的密钥，既不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密。

对于本申请实施例第三方面以及第三方面的各种可能实现方式中名词的概念、具体实

现步骤以及每种可能实现方式所带来的有益效果，均可以参考第一方面中各种可能的实现方式中的描述，此处不再一一赘述。

第四方面，本申请实施例提供了一种区块链信息的处理方法，可用于区块链领域中。方法包括：第二区块链节点根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥；第二区块链节点对区块链上的至少一个交易信息进行读取，在至少一个交易信息中存在第二交易信息的情况下，确定第一交易内容指向的交易为交易成功，也即第二区块链节点需要对区块链上的每个交易信息进行读取，以逐个判断区块链上的每个交易信息中是否为第二交易信息。其中，第二交易信息包括第一区块链节点的公钥地址、第二区块链节点的第二公钥地址、第一交易内容和加密后的第五私钥；第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，加密后的第五私钥能够通过共享密钥解密，第二公钥地址能够根据第五私钥生成。具体的，针对判断一个交易信息是否为第二交易信息的过程。第二区块链节点在读取到一个交易信息之后，会利用生成的共享密钥对加密后的密钥进行解密，进而根据解密结果生成临时的公钥地址，生成临时的公钥地址的方式与生成临时的第二公钥地址的方式一致，并判断生成的公钥地址是否与获取的交易信息中包括的交易接收方的公钥地址一致，若一致，则证明读取到的交易信息为第二交易信息，若不一致，则证明读取到的交易信息不是第二交易信息。

在第四方面的一种可能实现方式中，第二区块链节点根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥，包括：第二区块链节点在椭圆曲线的公钥密码体系中，将第一区块链节点的公钥和第二区块链节点的第一私钥进行点乘，得到共享密钥。或者，第二区块链节点在离散对数的公钥密码体系中，根据第一区块链节点的公钥和第二区块链节点的第一私钥，进行指数运算，第一区块链节点的公钥为指数运算中的底数，第二区块链节点的第一私钥为指数运算中的指数。

在第四方面的一种可能实现方式中，方法还包括：第二区块链节点根据临时的第五私钥和第二区块链节点的第三私钥，生成第二区块链节点的临时的第六私钥，第六私钥用于花费第二交易信息中的产品。

对于本申请实施例第四方面以及第四方面的各种可能实现方式中名词的概念、具体实现步骤以及每种可能实现方式所带来的有益效果，均可以参考第二方面中各种可能的实现方式中的描述，此处不再一一赘述。

第五方面，本申请实施例提供了一种地址的生成装置，可用于区块链领域中。地址的生成装置应用于第一区块链节点，装置包括：生成模块，用于根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥；生成模块，还用于根据共享密钥和第一交易内容生成第二区块链节点的第一公钥地址；写入模块，用于将第一交易信息写入区块链，第一交易信息包括第一区块链节点的公钥地址、第一公钥地址和第一交易内容。其中，第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间的交易的内容，写入区块链的第一交易信息由第二区块链节点根据第一公钥地址进行验证，第一公钥地址需要利用共享密钥进行验证，共享密钥在第二区块链节点处

通过第一区块链节点的公钥和第二区块链节点的第一私钥生成。

本申请实施例的第五方面中，地址的生成装置还可以执行第一方面以及第一方面的各种可能实现方式中由第一区块链节点执行的步骤，对于第五方面以及第五方面的部分可能实现方式中名词的概念、具体实现步骤以及每种可能实现方式所带来的有益效果，均可以
5 参考第一方面中各种可能的实现方式中的描述，此处不再一一赘述。

第六方面，本申请实施例提供了一种区块链信息的处理装置，可用于区块链领域中。区块链信息的处理装置应用于第二区块链节点，装置包括：生成模块，用于根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥；读取模块，用于对区块链上的至少一个交易信息进行读取；确定模块，用于在至少一个交易信息中存在第一交易信息的情况下，确定第一交易内容指向的交易为交易成功，第一交易信息包括第一区块链节点的公钥地址、第一交易内容和第二区块链节点的第一公钥地址。其中，第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，第一公钥地址能够根据共享密钥和第一交易内容生成。
10

本申请实施例的第六方面中，区块链信息的处理装置还可以执行第二方面以及第二方面的各种可能实现方式中由第二区块链节点执行的步骤，对于第六方面以及第六方面的部分可能实现方式中名词的概念、具体实现步骤以及每种可能实现方式所带来的有益效果，均可以参考第二方面中各种可能的实现方式中的描述，此处不再一一赘述。
15

第七方面，本申请实施例提供了一种地址的生成装置，可用于区块链领域中。装置应用于第一区块链节点，装置包括：生成模块，用于根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥；生成模块，还用于随机生成第五私钥，并根据第五私钥生成第二区块链节点的第二公钥地址；加密模块，用于采用共享密钥对第五私钥进行对称加密，得到加密后的第五私钥；写入模块，用于将第二交易信息写入区块链，第二交易信息包括第一区块链节点的公钥地址、第二公钥地址、第一交易内容和加密后的第五私钥。其中，第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，加密后的第五私钥需要利用共享密钥进行解密，共享密钥在第二区块链节点处通过第一区块链节点的公钥和第二区块链节点的第一私钥生成。
20
25

本申请实施例的第七方面中，地址的生成装置还可以执行第三方面以及第三方面的各种可能实现方式中由第一区块链节点执行的步骤，对于第七方面以及第七方面的部分可能实现方式中名词的概念、具体实现步骤以及每种可能实现方式所带来的有益效果，均可以
30 参考第三方面中各种可能的实现方式中的描述，此处不再一一赘述。

第八方面，本申请实施例提供了一种区块链信息的处理装置，可用于区块链领域中。区块链信息的处理装置应用于第二区块链节点，装置包括：生成模块，用于根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥；读取模块，用于对区块链上的至少一个交易信息进行读取；确定模块，用于在至少一个交易信息中存在第二交易信息的情况下，确定第一交易内容指向的交易为交易成功，第二交易信息包括第一区块链节点的公钥地址、第二区块链节点的第二公钥地址、第一交易内容和加密后的第五私钥。其中，第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二
35

区块链节点之间交易的内容，写入区块链的第二交易信息由第二区块链节点根据第二公钥地址进行验证，加密后的第五私钥能够通过共享密钥解密，第二公钥地址能够根据第五私钥生成。

本申请实施例的第八方面中，区块链信息的处理装置还可以执行第四方面的各种可能实现方式中由第二区块链节点执行的步骤，对于本申请实施例第八方面以及第八方面的部分可能实现方式中名词的概念、具体实现步骤以及每种可能实现方式所带来的有益效果，均可以参考第四方面中各种可能的实现方式中的描述，此处不再一一赘述。

第九方面，本申请实施例提供了一种计算机程序，当其在计算机上运行时，使得计算机执行上述第一方面或第三方面所述的地址的生成方法，或者，使得计算机执行上述第二方面或第四方面所述的区块链信息的处理方法。

第十方面，本申请实施例提供了一种区块链节点，包括处理器，所述处理器与所述存储器耦合；所述存储器，用于存储程序；所述处理器，用于执行所述存储器中的程序，使得所述区块链节点执行如上述第一方面或第三方面所述的地址的生成方法，或者，使得所述区块链节点执行如上述第二方面或第四方面所述的区块链信息的处理方法。

第十一方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行上述第一方面或第三方面所述的地址的生成方法，或者，使得计算机执行上述第二方面或第四方面所述的区块链信息的处理方法。

第十二方面，本申请实施例提供了一种电路系统，所述电路系统包括处理电路，所述处理电路配置为执行上述第一方面或第三方面所述的地址的生成方法，或者，所述处理电路配置为执行上述第二方面或第四方面所述的区块链信息的处理方法。

第十三方面，本申请实施例提供了一种芯片系统，该芯片系统包括处理器，用于支持实现上述方面中所涉及的功能，例如，发送或处理上述方法中所涉及的数据和/或信息。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器，用于保存服务器或通讯设备必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包括芯片和其他分立器件。

附图说明

图1为本申请实施例提供的区块链信息的处理方法的一种流程示意图；

图2为本申请实施例提供的区块链信息的处理方法的另一种流程示意图；

图3为本申请实施例提供的区块链信息的处理方法的又一种流程示意图；

图4为本申请实施例提供的区块链信息的处理方法的再一种流程示意图；

图5为本申请实施例提供的区块链信息的处理方法的又一种流程示意图；

图6为本申请实施例提供的区块链信息的处理方法的再一种流程示意图；

图7为本申请实施例提供的区块链信息的处理方法的又一种流程示意图；

图8为本申请实施例提供的区块链信息的处理方法的再一种流程示意图；

图9为本申请实施例提供的地址的生成装置的一种结构示意图；

图 10 为本申请实施例提供的区块链信息的处理装置的一种流程示意图；

图 11 为本申请实施例提供的地址的生成装置的另一种结构示意图；

图 12 为本申请实施例提供的区块链信息的处理装置的另一种流程示意图；

图 13 为本申请实施例提供的区块链节点的一种结构示意图。

5

具体实施方式

本申请实施例提供了一种地址的生成方法、区块链信息的处理方法以及相关设备，用于验证的共享密钥也可以通过第一区块链节点的公钥和第二区块链节点的第一私钥生成，也即接收方也可以生成共享密钥，以对交易信息进行验证，接收方无需存储并管理多个公私钥对，降低了管理难度。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，这仅仅是描述本申请的实施例中对相同属性的对象在描述时所采用的区分方式。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，以便包含一系列单元的过程、方法、系统、产品或设备不必限于那些单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它单元。

下面结合附图，对本申请的实施例进行描述。本领域普通技术人员可知，随着技术的发展和场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

本申请实施例可应用于区块链技术中，特别是交易发送方想要隐藏交易接收方的真实身份的场景中。作为示例，例如生产商并不想别人知道他的零售商都是谁，再例如零售商不想别人知道他的客户是谁等，此处不对本申请实施例的应用场景进行穷举。在对本申请实施例提供的区块链信息的处理方法的详细实现方案进行介绍之前，先对本申请实施例涉及到的一些基本概念进行介绍。

1、区块链技术

区块链技术是一种不依赖第三方、通过自身分布式节点进行网络数据的存储、验证、传递和交流的一种技术方案。区块链能够记录点对点网络中的数据，每个参与方都可以使用共识算法，查看区块链上的数据并验证/拒绝数据。被验证通过的数据将作为一个“区块”进入账本，储存在按时间顺序排列且无法更改的“链条”上。区块链严格定义上被划分为 3 种类型：公有链、私有链和联盟链。

公有链是对所有人公开，用户不需要注册和授权就能够匿名访问网络和区块，任何人都可以自由加入和退出网络，并参与记账和交易。公有链是真正完全意义上的去中心化区块链，它通过密码学（非对称加密）算法保证了交易的安全性和不可篡改性，在陌生的网络环境中，建立了互信和共识机制。在公有链中共识机制一般是工作量证明（POW）和权益证明（POS）。公有链又被称为非许可链，即不需要验证身份即可参与一切网络活动。目前比特币、以太坊、大多数山寨币以及智能合约都是建立在公有链上，其中公有链的始祖是比特币区块链。公有链适用于数字货币、电子商务、互联网金融、知识产权等应用场景。

私有链对单独的个人或实体开放，仅在私有组织（例如公司内部）使用，私有链上的

读写权限，参与记账的权限都由私有组织来制定。例如企业内部的办公审批和财务审计、政府行业的预算和执行等。

联盟链仅限于联盟成员，因其只针对成员开放全部或部分功能，所以联盟链上的读写权限、以及记账规则都按联盟规则来“私人定制”。联盟链上的共识过程由预先选好的节点控制，一般来说，他适用于机构间的交易、结算、或清算等 B2B 场景。例如人民银行开发一个基于联盟链的结算、清算系统，工建中农等银行作为联盟成员加入这个系统，获得相应的授权，就可以实时进行不同银行之间的实时结算、清算。联盟链几乎不采用工作量证明共识机制而是采用权益证明或实用拜占庭容错 (practical byzantine fault tolerance, PBTF) 等共识算法。联盟链由参与成员机构共同维护，并提供了对参与成员的管理、认证、授权、监控、审计等全套安全管理功能。

2、智能合约

智能合约是以区块链技术为基础，能够自我执行的条约；一旦满足条件，就可以自动触发行为或付款。智能合约是一段代码和数据的集合，可以部署在区块链上运行。智能合约更像是 JAVA 程序，JAVA 程序通过 JAVA 虚拟机将代码解释字节进行执行，以太坊的智能合约通过以太坊虚拟机 (EVM) 解释成字节码进行执行。智能合约有自己的账户，在时间或事件的驱动下能自动执行一些功能，如可以在相互之间传递信息，修改区块链的状态例如账户信息等。

3、非对称加密 (asymmetric cryptography)

非对称加密是一种密码学算法类型，在这种密码学方法中，需要一对密钥，分别为公钥和私钥。前述两个密钥数学相关，用某用户密钥加密后所得的信息，只能用该用户的解密密钥才能解密。如果知道了公钥，并不能计算出私钥。私钥由密钥对所有者持有，不可公布，公钥是密钥对持有者公布给他人的。公钥用来给数据加密，用公钥加密的数据只能使用私钥解密。

为了解决上述问题，本申请实施例提供了一种区块链信息的处理方法，能够为交易接收方生成临时的公钥地址，交易发送方在与相同的交易接收方进行不同的交易时，交易接收方的公钥地址均不同，从而无法通过交易接收方的公钥地址来指向交易接收方的真实身份，以实现隐藏交易接收方的真实身份的场景区的目的。且交易接收方无需长期存储该临时的公钥地址，以避免提高交易接收方的管理难度。

本申请实施例中，先结合图 1 和图 2 对本申请实施例提供的区块链信息的处理方法进行大体介绍。图 1 和图 2 分别为本申请实施例提供的区块链信息的处理方法的两种流程示意图，图 1 和图 2 中均以交易发送方和交易接收方仅拥有一套固定密钥为例。在一种实现方式中，请先参阅图 1，图 1 中示出的实现方式为利用共享密钥来生成第二区块链节点的临时的公钥地址。具体的，A1、第一区块链节点（也即交易发送方）根据第一区块链节点的私钥和第二区块链节点（也即交易接收方）的第一公钥生成共享密钥。A2、在每次交易中，第一区块链节点根据该共享密钥和第一交易内容（也即交易发送方和交易接收方之间的交易内容），生成第二区块链节点的临时的公钥地址。A3、第一区块链节点将第一交易信息上链，第一交易信息包括第一区块链节点的公钥地址、第一公钥地址和第一交易内容。

- 12 -

A4、第二区块链节点根据第二区块链节点的第一私钥和第一区块链节点的公钥生成共享密钥。A5、第二区块链节点读取区块链上的多个交易信息，以根据该共享密钥，逐个判断该多个交易信息中是否存在第一交易信息；其中，第一交易信息包括第一区块链节点的公钥地址、第一公钥地址和第一交易内容，第一区块链节点的公钥地址属于第一区块链节点，
5 第一交易内容为第一区块链节点和第二区块链节点之间的交易的内容，第一公钥地址需要利用共享密钥和第一交易内容进行验证。A6、在第二区块链节点确定多个交易信息中存在第一交易信息的情况下，确定第一交易信息指向的交易成功；在第二区块链节点确定多个交易信息中不存在第一交易信息的情况下，确定第一交易信息指向的交易失败。由于每次交易过程中为第二区块链节点生成的临时的公钥地址为根据第一交易内容生成的，而不同交易中的交易内容是不同的，所以保证了该临时的公钥地址为一次性的，不能够指向某个特定的交易接收方。且第二区块链无需存储多余的临时公钥或临时私钥等，就可以完成对交易信息的验证，避免提高交易接收方的管理难度。

在另一种实现方式中，请参阅图 2，B1、第一区块链节点（也即交易发送方）根据第一区块链节点的私钥和第二区块链节点（也即交易接收方）的第一公钥生成共享密钥。B2、
15 在每次交易中，第一区块链节点随机生成一个临时的第五私钥，并根据临时的第五私钥生成第二区块链节点的公钥地址。B3、第一区块链节点利用共享密钥对第五私钥进行加密，以生成加密后的第五私钥。B4、第一区块链节点将第二交易信息上链，第二交易信息包括第一区块链节点的公钥地址、第二区块链节点的第二公钥地址、第一交易内容和加密后的第五私钥。B5、第二区块链节点根据第二区块链节点的第一私钥和第一区块链节点的公钥生成共享密钥。B6、第二区块链节点读取区块链上的多个交易信息，以根据该共享密钥，逐个判断该多个交易信息中是否存在第二交易信息；其中，第二交易信息包括第一区块链节点的公钥地址、第二公钥地址、第一交易内容和加密后的第五私钥，加密后的第五私钥能够通过共享密钥解密，第二公钥地址能够根据第五私钥生成，也即能够利用生成的共享密钥来验证获取到的交易信息是否为第二交易信息。B7、在第二区块链节点确定多个交易
20 信息中存在第二交易信息的情况下，确定第二交易信息指向的交易成功。由于每次交易过程中为第二区块链节点生成的临时的公钥地址为根据随机生成的第五私钥生成的，保证了该临时的公钥地址是一次性的，不能够指向某个特定的交易接收方。且第二区块链无需存储多余的临时公钥或临时私钥等，就可以完成对交易信息的验证，避免提高交易接收方的管理难度。

30 由于上述两种实现方式的具体流程有所不同，以下分别对前述两种情况进行详细介绍。

一、共享密钥用于生成第一公钥地址

本申请实施例中，请参阅图 3，图 3 为本申请实施例提供的区块链信息的处理方法的一种流程示意图，本申请实施例提供的区块链信息的处理方法可以包括：

35 301、第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥。

本申请实施例中，第一区块链节点能够获取到第一区块链节点的私钥和第二区块链节点的第一公钥，根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥

(derive shared key)。其中，第一区块链节点和第二区块链节点为区块链上的两个区块链节点，第一区块链节点为交易的发送方，第二区块链节点为交易的接收方。共享密钥也可以称为对称密钥或对称共享密钥，第二区块链节点也能够根据第一区块链节点的公钥和第二区块链节点的第一私钥生成。

5 进一步地，在一种情况下，第一区块链节点和第二区块链节点均仅拥有一套固定密钥 (single-key scheme)，一套固定密钥中包括一个长期私钥和一个长期公钥；第一区块链节点的私钥指的是第一区块链节点的长期私钥，第二区块链节点的第一公钥指的是第二区块链节点的长期公钥，第一区块链节点的公钥指的是第一区块链节点的长期公钥，第二区块链节点的第一私钥指的是第二区块链节点的长期私钥。

10 在另一种情况下，第一区块链节点和第二区块链节点均拥有两套固定密钥 (Dual-Key scheme)，两套固定密钥包括第一套固定密钥和第二套固定密钥，第一套固定密钥包括一个长期私钥和一个长期公钥，第二套固定密钥包括一个扫描 (scanning) 私钥和一个扫描公钥，在本情况下，长期私钥也可以称为花费 (spending) 私钥，长期公钥也可以称为花费公钥；第一区块链节点的私钥为第一区块链节点的长期私钥，第二区块链节点的第一公钥为第二区块链节点的扫描公钥，第一区块链节点的公钥指的是第一区块链节点的长期公钥，第二区块链节点的第一私钥指的是第二区块链节点的扫描私钥。本申请实施例中，提供的区块链信息的处理方法不仅可以适用于区块链节点仅拥有一套固定密钥的情况，而且还适用于区块链拥有两套固定密钥的情况，扩展了本方案的应用场景。

20 具体的，在一种实现方式中，在椭圆曲线的公钥密码体系中，第一区块链节点基于静态的迪菲-赫尔曼 (Diffie-Hellman) 算法，将第一区块链节点的私钥与第二区块链节点的第一公钥进行点乘，得到共享密钥。为更直观地理解本方案，以下以第二区块链节点拥有两套固定的密钥为例，公开了第一区块链节点在椭圆曲线的公钥密码体系中，生成共享密钥的公式的一个示例：

$$S=a.D=ad.G(1)$$

25 其中，S 代表共享密钥，a 代表第一区块链节点的私钥，D 代表第二区块链节点的第一公钥 (也即第二区块链节点的扫描公钥)，D 是由第二区块链节点的第一私钥 d (也即第二区块链节点的扫描私钥) 与生成元 (generator, G) 点乘得到，G 代表椭圆曲线群的生成元，也可以称为椭圆曲线上的基点。需要说明的是，虽然用户看来第一区块链节点的私钥和第二区块链节点的第一公钥均表现为包括字母、数字的密钥，但对于计算机而言，均可以通过二进制编码的方式进行表示。

30 在另一种实现方式中，在离散对数的公钥密码体系中，第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥，进行指数运算，得到共享密钥。其中，第二区块链节点的第一公钥为指数运算中的底数，第一区块链节点的私钥为指数运算中的指数。

35 进一步地，在离散对数的公钥密码体系中，第二区块链节点的第一公钥为第二区块链节点的第一私钥与生成元 G 进行指数运算得到，生成元 G 为指数运算中的底数，第二区块链节点的第一私钥为指数运算中的指数。在离散对数的公钥密码体系中，生成元 G 代表的为整数群的生成元或素数群的生成元。

本申请实施例中，分别公开了在椭圆曲线的公钥密码体系和离散对数的公钥密码体系下，共享密钥的生成方式，扩展了本方案的应用场景。

302、第一区块链节点根据共享密钥和第一交易内容生成第二私钥。

本申请的一些实施例中，第一区块链节点在生成共享密钥之后，可以根据共享密钥和第一交易内容生成临时的第二私钥（generate temporary private key）。其中，由于与不同交易对应的交易内容不同，则根据不同的交易内容生成的私钥不同，所以第二私钥为一次性的，或者说第二私钥为临时的，而不是固定的。需要说明的是，第二私钥为生成第二区块链节点的一次性公钥地址的过程中所产生的密钥，并不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密。

具体的，第一区块链节点将共享密钥和第一交易内容（Txcontents）进行组合，得到第一组合结果；对第一组合结果进行哈希运算，以生成第二私钥。其中，第一交易内容指的是第一区块链节点与第二区块链节点当前交易的交易内容，第一交易内容中包括时间戳，用于指示第一交易内容所指向的交易的时间，作为示例，例如第一交易内容可以为“转移3个比特币”、“卖出两箱奇异果”、“卖出一辆汽车”等等，此处不做穷举。组合的方式包括但不限于拼接、异/或运算、相加等；采用的哈希函数包括但不限于 SHA256、SHA512等，此处不对组合的方式以及采用的哈希函数进行穷举。本申请实施例中，提供了生成第二私钥的具体实现方式，操作简单，易于实现。

为更直观地理解本方案，以下生成第二私钥的公式的一个示例：

$$r = \text{Hash}(\text{Txcontents}, S) \quad (2)$$

其中，r 代表第二私钥，Txcontents 代表第一交易内容，S 代表共享密钥，Txcontents，S 代表将第一交易内容与共享密钥进行拼接，需要说明的是，式（2）仅为一个示例，不用于限定本方案。

303、第一区块链节点根据第二私钥生成第二区块链节点的第一公钥地址。

本申请实施例中，第一区块链节点在生成第二私钥之后，可以根据临时的第二私钥生成临时的第三公钥（generate temporary public key），进而根据临时的第三公钥，生成第二区块链节点的临时的第一公钥地址。需要说明的是，第三公钥的作用与第二私钥的功能类似，均为生成第二区块链节点的一次性公钥地址的过程中所生成的密钥，并不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密。由于该第一公钥地址仅在第一区块链节点向第二区块链节点发送第一交易信息时使用，所以将第一公钥地址称为临时的公钥地址，也可以称为一次性的公钥地址。

具体的，第一区块链节点根据第二私钥和第二区块链节点的第二公钥，生成第二区块链节点的第一公钥地址。其中，无论在第二区块链节点仅拥有一套固定密钥的情况下，还是在第二区块链节点拥有两套固定密钥的情况下，第二区块链节点的第二公钥均为第二区块链节点的长期公钥。进一步地，若第二区块链节点仅拥有一套固定密钥，则第二区块链节点的第一公钥和第二区块链节点的第二公钥可以为同一密钥。若第二区块链节点拥有两套固定密钥，则第二区块链节点的第一公钥和第二区块链节点的第二公钥可以为不同的密钥，第二区块链节点的第一公钥为第二区块链节点的扫描公钥，第二区块链节点的第二公

钥为第二区块链节点的长期公钥。

本申请实施例中，根据第二私钥和第二区块链节点的第二公钥生成第一公钥地址，则需要借助第二区块链节点的第三私钥才能够生成花费第一交易信息中的产品时所使用的私钥，从而避免了第一区块链节点在将第一交易信息中的产品转移给第二区块链节点之后，还能够花费第一交易信息中的产品，以保证了第二区块链节点的财产的安全性，也包括了区块链上交易的稳定性。

更具体的，在一种情况中，步骤 303 可以包括：在椭圆曲线的公钥密码体系中，第一区块链节点根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，并根据临时的第三公钥，生成临时的第一公钥地址。

进一步地，在一种实现方式中，在椭圆曲线的公钥密码体系中，第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与生成元 G （也即椭圆曲线群的生成元）进行点乘，可以生成临时的公钥 R ，进而将临时的公钥 R 与第二区块链节点的第二公钥 B 相加，以生成临时的第三公钥 T ，也即临时的第三公钥 $T=R+B$ ，进而在椭圆曲线的公钥密码体系的约束下，根据临时的第三公钥 T 生成第一公钥地址。

在另一种实现方式中，在椭圆曲线的公钥密码体系中，第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与生成元 G （也即椭圆曲线群的生成元）进行点乘，可以生成临时的公钥 R ，进而将临时的公钥 R 与第二区块链节点的第二公钥 B 相减，以生成临时的第三公钥 T ，也即临时的第三公钥 $T=R-B$ ，进而在椭圆曲线的公钥密码体系的约束下，根据临时的第三公钥 T 生成第一公钥地址。

在另一种实现方式中，在椭圆曲线的公钥密码体系中，第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与第二区块链节点的第二公钥 B 相乘，以生成临时的第三公钥 T ，也即临时的第三公钥 $T=r.B$ ，进而在椭圆曲线的公钥密码体系的约束下，根据临时的第三公钥 T 生成第一公钥地址。

在另一种实现方式中，在椭圆曲线的公钥密码体系中，第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 的倒数与第二区块链节点的第二公钥 B 相乘，以生成临时的第三公钥 T ，进而在椭圆曲线的公钥密码体系的约束下，根据临时的第三公钥 T 生成第一公钥地址等等，此处不对在椭圆曲线的公钥密码体系中，生成第一公钥地址的方式进行穷举，应理解，此处举例仅为进一步理解本方案，不用于限定本方案。

在另一种情况中，步骤 303 可以包括：在离散对数的公钥密码体系中，第一区块链节点根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，并根据临时的第三公钥，生成临时的第一公钥地址。

进一步地，在一种实现方式中，第一区块链节点根据临时的第二私钥 r ，将临时的第二私钥 r 与第二区块链节点的第二公钥 B 进行指数运算，以生成临时的第三公钥 T ；其中，第二区块链节点的第二公钥 B 为前述指数运算的底数，临时的第二私钥 r 为前述指数运算的指数。进而在离散对数的公钥密码体系的约束下，根据临时的第三公钥 T 生成第一公钥地址等等，此处不对在离散对数的公钥密码体系中，生成第一公钥地址的方式进行穷举，应理解，此处举例仅为进一步理解本方案，不用于限定本方案。

本申请实施例中，无论是在椭圆曲线的公钥密码体系下，还是在离散对数的公钥密码体系下，均能根据临时的第二私钥和第二区块链节点的第二公钥，生成临时的第三公钥，并根据临时的第三公钥，生成临时的第一公钥地址，扩展了本方案的应用场景。

5 304、第一区块链节点将第一交易信息写入区块链，第一交易信息包括第一区块链节点的公钥地址、第一公钥地址和第一交易内容。

本申请实施例中，第一区块链节点在为第二区块链节点生成一次性的第一公钥地址之后，会将第一交易信息写入区块链，也即将第一交易信息上链。其中，第一交易信息包括第一区块链节点的公钥地址（也即字段 **Input** 的内容为交易发送方的公钥地址）、第一公钥地址（也即字段 **Output** 的内容为交易接收方的公钥地址）和第一交易内容。

10 进一步地，第一区块链节点的公钥地址属于第一区块链节点，若第一交易内容所指向的交易是由第一区块链节点首创的，则无论第一区块链节点拥有一套固定密钥，还是拥有两套固定密钥，第一区块链节点的公钥地址均为根据第一区块链节点的长期公钥生成的。若第一交易内容所指向的交易为第三区块链节点转移给第一区块链节点的，则第一区块链节点的公钥地址为第三区块链节点为第一区块链节点生成的临时公钥地址，具体临时公钥地址的生成方式可参阅上述步骤 301 至 303 中的描述，此处不做赘述。第一交易内容的含义可参阅上述步骤 302 中的描述，此处不做赘述。

写入区块链的第一交易信息由第二区块链节点根据第一公钥地址进行验证，第一公钥地址需要利用共享密钥进行验证，共享密钥能够通过第一区块链节点的公钥和第二区块链节点的第三私钥生成，也即第二区块链节点能够自主生成前述共享密钥。

20 305、第二区块链节点根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥。

本申请实施例中，第二区块链节点能够获取到第一区块链节点的公钥和第二区块链节点的第一私钥，第二区块链节点根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥。其中，在一种情况下，第一区块链节点和第二区块链节点均仅拥有一套固定密钥，一套固定密钥中包括一个长期私钥和一个长期公钥，则第一区块链节点的公钥指的是第一区块链节点的长期公钥，第二区块链节点的第一私钥指的是第二区块链节点的长期私钥。

30 在另一种情况下，第一区块链节点和第二区块链节点均拥有两套固定密钥，两套固定密钥包括第一套固定密钥和第二套固定密钥，第一套固定密钥包括一个长期私钥和一个长期公钥，第二套固定密钥包括一个扫描私钥和一个扫描公钥。与步骤 301 对应的，第一区块链节点的公钥为第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的扫描私钥。

具体的，与步骤 301 对应的，在一种实现方式中，在椭圆曲线的公钥密码体系中，第二区块链节点基于静态的迪菲-赫尔曼算法，将第一区块链节点的公钥和第二区块链节点的第一私钥进行点乘，得到共享密钥。为更直观地理解本方案，以下以第二区块链节点拥有两套私钥为例，公开第二区块链节点在椭圆曲线的公钥密码体系中，生成共享密钥的公式的一个示例：

$$S=d.A=da.G \quad (3)$$

其中，S 代表共享密钥，d 代表第二区块链节点的第一私钥（也即第二区块链节点的扫描私钥），A 代表第一区块链节点的公钥，A 是由第一区块链节点的私钥 a 与生成元(generator, G) 点乘得到，G 代表椭圆曲线群的生成元，也可以称为椭圆曲线上的基点，则第二区块链节点也可以生成共享密钥，需要说明的是，虽然用户看来第二区块链节点的第一私钥和第一区块链节点的公钥均表现为包括字母、数字的密钥，但对于计算机而言，均可以通过二进制编码的方式进行表示。

在另一种实现方式中，在离散对数的公钥密码体系中，根据第一区块链节点的公钥和第二区块链节点的第一私钥，进行指数运算，第一区块链节点的公钥为指数运算中的底数，第二区块链节点的第一私钥为指数运算中的指数。

进一步地，在离散对数的公钥密码体系中，第一区块链节点的公钥为第一区块链节点的私钥与生成元 G 进行指数运算得到，生成元 G 为指数运算中的底数，第一区块链节点的私钥为指数运算中的指数。在离散对数的公钥密码体系中，生成元 G 代表的为整数群的生成元或素数群的生成元。

306、第二区块链节点对区块链上的至少一个交易信息进行读取，并判断区块链上的至少一个交易信息中是否存在第一交易信息，若存在，则确定第一交易内容指向的交易为交易成功；若不存在，则确定第一交易内容指向的交易为交易失败。

本申请实施例中，第二区块链节点需要遍历区块链节点上的所有交易信息，也即需要对区块链上的每个交易信息进行读取，以逐个判断区块链上的每个交易信息中是否为第一交易信息，也即判断区块链上的至少一个交易信息中是否存在第一交易信息。在区块链上的至少一个交易信息中存在第一交易信息的情况下，确定第一交易内容指向的交易为交易成功；在区块链上的至少一个交易信息中不存在第一交易信息的情况下，确定第一交易内容指向的交易为交易失败。

其中，区块链节点上的每个交易信息中均包括交易发送方的公钥地址（也即字段 Input 中的内容）、交易内容和交易接收方的公钥地址（也即字段 Output 中的内容）。第一交易信息包括第一区块链节点的公钥地址、第一交易内容和第二区块链节点的第一公钥地址；第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，第一公钥地址能够根据共享密钥和第一交易内容生成。也即第一交易信息的特点在于，第二区块链节点能够根据生成的共享密钥和交易信息中的交易内容，生成交易接收方的公钥地址。

具体的，针对判断区块链上的至少一个交易信息中的任一个交易信息是否为第一交易信息的过程。第二区块链节点在读取到一个交易信息之后，会获取该交易信息中的交易内容，并根据步骤 305 中生成的共享密钥和获取到的交易内容，生成一个临时的公钥地址，具体生成方式与步骤 302 和 303 中生成第一公钥地址的方式一致，此处不做赘述。进而判断该临时的公钥地址与该交易信息中的携带的接收方的公钥地址是否一致，若一致，则视为该交易信息为第一交易信息，若不一致，则视为该交易信息不是第一交易信息。

第二区块链节点对区块链上的每个交易信息均执行上述操作，以判断区块链上的每个

交易信息是否为第一交易信息。

307、第二区块链节点根据共享密钥和第一交易内容，生成第二私钥。

本申请实施例中，第二区块链节点在确定第一交易信息指向的交易为交易成功的情况下，当第二区块链节点需要花费第一交易信息中的产品时，还需要生成用于花费第一交易信息中的产品的临时的第四私钥，该临时的第四私钥与临时的第一公钥地址对应，也即该第四私钥需要能够在椭圆曲线的公钥密码体系的约束下，或者，在离散对数的公钥密码体系中的约束下，能够直接生成临时的第一公钥地址。

具体的，第二区块链节点生成临时的第四私钥的方式与第一区块链节点生成临时的第一公钥地址的方式对应。第二区块链节点需要先根据共享密钥和第一交易内容，生成第二私钥。具体实现方式与步骤 302 中第一区块链节点生成第二私钥的步骤一致，第二私钥的含义与步骤 302 中第二私钥的含义一致，均可参阅上述步骤 302 中的描述，此处不做赘述。

308、第二区块链节点根据第二私钥，生成第二区块链节点的第四私钥，第四私钥用于花费第一交易信息中的产品。

本申请实施例中，第二区块链节点根据第二私钥，生成第二区块链节点的临时的第四私钥，由于该临时的第四私钥需要与临时的第一公钥地址对应，则第二区块链节点生成第四私钥的方式，需要与步骤 303 中第一区块链节点生成第一公钥地址的方式对应。

具体的，在一种实现方式中，第二区块链节点根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的临时的第四私钥。

更具体的，在一种情况中，步骤 308 可以包括：在椭圆曲线的公钥密码体系中，第二区块链节点根据临时的第二私钥和第二区块链节点的第三私钥（也即第二区块链节点的长期私钥），生成第二区块链节点的临时的第四私钥。其中，无论第二区块链节点包括一套固定密钥，还是两套固定密钥，第二区块链节点的第三私钥指的均为第二区块链节点的长期私钥。

进一步地，与步骤 303 对应，在一种实现方式中，在椭圆曲线的公钥密码体系中，第二区块链节点根据临时的第二私钥 r ，第二私钥 r 与第二区块链节点的第三私钥 b 相加，得到第一相加结果，将第一相加结果与 q 进行求余运算，得到第二区块链节点的临时的第四私钥。其中，求余运算也可以称为取余或者取模运算；在椭圆曲线的公钥密码体系中， q 代表生成元的阶（order）。也即临时的第四私钥 $t = (r+b) \bmod q$ 。

在另一种实现方式中，在椭圆曲线的公钥密码体系中，第二区块链节点根据临时的第二私钥 r ，第二私钥 r 与第二区块链节点的第三私钥 b 相减，得到第一相减结果，将第一相减结果与 q 进行求余运算，得到第二区块链节点的临时的第四私钥，也即临时的第四私钥 $t = (r-b) \bmod q$ 。

在另一种实现方式中，在椭圆曲线的公钥密码体系中，第二区块链节点根据临时的第二私钥 r ，第二私钥 r 与第二区块链节点的第三私钥 b 相乘，将前述相乘结果与 q 进行求余运算，得到第二区块链节点的临时的第四私钥，也即临时的第四私钥 $t = (rb) \bmod q$ 。

在另一种实现方式中，在椭圆曲线的公钥密码体系中，第二区块链节点根据临时的第二私钥 r ，第二私钥 r 的倒数与第二区块链节点的第三私钥 b 相乘，将前述相乘结果与 q 进

行求余运算，得到第二区块链节点的临时的第四私钥等等。

上述种种实现方式的举例均仅为方便理解本方案，不用于限定本方案，需要说明的是，在上述种种实现方式中，在椭圆曲线的公钥密码体系中，需要满足，生成的临时的第四私钥 t 点乘生成元 G 之后，需要等于步骤 303 中生成的临时的第三公钥 T 。

5 在另一种情况中，步骤 308 可以包括：在离散对数的公钥密码体系中，第二区块链节点根据临时的第二私钥和第二区块链节点的第三私钥（也即第二区块链节点的长期私钥），生成第二区块链节点的临时的第四私钥。其中，无论第二区块链节点包括一套固定密钥，还是两套固定密钥，第二区块链节点的第三私钥指的均为第二区块链节点的长期私钥。

10 进一步地，与步骤 303 对应，在一种实现方式中，在离散对数的公钥密码体系中，第二区块链节点将临时的第二私钥 r 与第二区块链节点的第三私钥 b 进行指数运算，得到第一运算结果；第三私钥 b 为前述指数运算的底数，第二私钥 r 为前述指数运算的指数。第二区块链节点将第一运算结果与 q 进行求余运算，得到第二区块链节点的临时的第四私钥。其中，在离散对数的公钥密码体系中， q 代表生成元的阶（order）。

15 上述种种实现方式的举例均仅为方便理解本方案，不用于限定本方案，需要说明的是，在上述种种实现方式中，在离散对数的公钥密码体系中，需要满足，生成的临时的第四私钥 t 与生成元 G 进行指数运算之后，需要等于步骤 303 中生成的临时的第三公钥 T 。

本申请实施例中，提供了当第二区块链节点想要花费第一交易信息中的产品时，生成花费第一交易信息中的产品的私钥的具体生成方式，扩展了本方案的应用场景，且增加了本方案的完整性。

20 为更直观地理解本方案，请参阅图 4 和图 5，图 4 和图 5 分别示出了本申请实施例提供的区块链信息的处理方法的两种流程示意图。图 4 和图 5 均以在椭圆曲线的公钥密码体系下为例；图 4 和图 5 的区别在于，图 4 以第一区块链节点和第二区块链节点均仅拥有一套固定密钥为例，图 5 以第一区块链节点和第二区块链节点均拥有两套固定密钥为例。先参阅图 4，第一区块链节点中配置有长期私钥 a 和长期公钥 A ，第二区块链节点中配置有长期私钥 b 和长期公钥 B 。C1、第一区块链节点通过将 a 与 B 进行点乘，生成共享密钥 S 。C2、第一区块链节点将第一交易内容与 S 进行拼接，并对拼接结果进行哈希运算，以生成临时的第二私钥 r 。C3、第一区块链节点将 r 与 G 进行点乘，并将点乘结果与 B 相加，以生成临时的第三公钥 T ，也即 $T=r \cdot G+B=R+B$ ，临时的第三公钥 T 用于生成第二区块链节点的临时的第一公钥地址。C4、第一区块链节点将第一交易信息上链，第一交易信息包括第一区块链节点的公钥地址（也即交易发送方的公钥地址）、第二区块链节点的临时的第一公钥地址（也即交易接收方的公钥地址）和第一交易内容。C5、第二区块链节点通过将 b 与 A 进行点乘，生成共享密钥 S 。C6、第二区块链节点在读取到区块链上的一个交易信息之后，将读取到的交易内容（Txcontents1）与 S 进行拼接，并对拼接结果进行哈希运算，以生成临时的私钥 $r1$ 。需要说明的是，若当前读取的交易信息为第一交易信息，则 Txcontents1 与 Txcontents 相同，且 $r1$ 与 r 相同；若当前读取的交易信息不是第一交易信息，则 Txcontents1 与 Txcontents 不同，且 $r1$ 与 r 不同。C7、第二区块链节点将 $r1$ 与 G 进行点乘，并将点乘结果与 B 相加，得到相加结果，将计算到的相加结果与读取到交易信息中携带的交易接收

25

30

35

方的公钥地址进行对比，以判断计算到的相加结果与读取到的交易接收方的公钥地址是否相同，若相同，则证明读取到的交易信息为第一交易信息，也即证明第一交易信息指向的交易成功；若区块链上的所有交易信息均不是第一交易信息，则证明第一交易信息执行的交易失败。C8、在第一交易信息指向的交易成功的情况下，当第二区块链节点想要花费第一交易信息中的产品时，还会根据第二私钥，生成第二区块链节点的第四私钥，第四私钥用于花费第一交易信息中的产品， t 点乘 G 之后需要等于 T ，也即 $t = (r+b) \bmod q$ 。

请再参阅图 5，第一区块链节点配置有长期私钥 a 和长期公钥 A ，第二区块链节点中配置有长期私钥 b 、长期公钥 B 、扫描私钥 d 和扫描公钥 D 。D1、第一区块链节点通过将 a 与 D 进行点乘，生成共享密钥 S 。D2、第一区块链节点将第一交易内容与 S 进行拼接，并对拼接结果进行哈希运算，以生成临时的第二私钥 r 。D3、第一区块链节点将 r 与 B 进行点乘，以生成临时的第三公钥 T ，临时的第三公钥 T 用于生成第二区块链节点的临时的第一公钥地址。D4、第一区块链节点将第一交易信息上链，第一交易信息包括第一区块链节点的公钥地址（也即交易发送方的公钥地址）、第二区块链节点的临时的第一公钥地址（也即交易接收方的公钥地址）和第一交易内容。D5、第二区块链节点通过将 d 与 A 进行点乘，生成共享密钥 S 。D6、第二区块链节点在读取到区块链上的一个交易信息之后，将读取到的交易内容（ $Txcontents1$ ）与 S 进行拼接，并对拼接结果进行哈希运算，以生成临时的私钥 $r1$ 。D7、第二区块链节点将 $r1$ 与 B 进行点乘，判断计算到的点乘结果与读取到的交易接收方的公钥地址是否相同，若相同，则证明读取到的交易信息为第一交易信息，也即证明第一交易信息指向的交易成功；若区块链上的所有交易信息均不是第一交易信息，则证明第一交易信息执行的交易失败。D8、在第一交易信息指向的交易成功的情况下，当第二区块链节点想要花费第一交易信息中的产品时，还会根据第二私钥，生成第二区块链节点的第四私钥，第四私钥用于花费第一交易信息中的产品， t 点乘 G 之后需要等于 T ，也即 $t = (rb) \bmod q$ 。需要说明的是，图 4 和图 5 中的举例均仅为方便理解本方案，不用于限定本方案。

本申请实施例中，由于第一交易信息的公钥地址是根据共享密钥和第一交易内容生成的，而不同交易中的交易内容是不同的，则区块链上的每个交易信息的公钥地址都是一次性的，从而可以很好的保护接收方的隐私；且共享密钥也可以通过第一区块链节点的公钥和第二区块链节点的第一私钥生成，也即接收方也可以生成共享密钥，并根据共享密钥和第一交易内容生成第一交易信息的公钥地址，以对交易信息进行验证，接收方无需存储并管理多个公私钥对，降低了管理难度。且不需要更改写入区块链的交易信息的格式，降低了本方案带来的技术更新的难度。

二、共享密钥用于加密第五私钥

本申请实施例中，请参阅图 6，图 6 为本申请实施例提供的区块链信息的处理方法的一种流程示意图，本申请实施例提供的区块链信息的处理方法可以包括：

601、第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥。

本申请实施例中，第一区块链节点执行步骤 601 的具体实现方式与图 3 对应实施例中

步骤 301 的具体实现方式类似，可参阅图 3 中的描述，此处不做赘述。

602、第一区块链节点随机生成第五私钥。

本申请的一些实施例中，第一区块链节点随机生成第五私钥。其中，第五私钥也是临时的一次性的私钥，第五私钥的作用与图 3 对应实施例中第二私钥的作用类似，第五私钥为生成第二区块链节点的一次性公钥地址的过程中所产生的私钥，并不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密。

需要说明的是，本申请实施例不限定步骤 601 和 602 的执行顺序，可以先执行步骤 601，再执行步骤 602，也可以先执行步骤 602，再执行步骤 601，还可以同时执行步骤 601 和步骤 602。

603、第一区块链节点根据第五私钥生成第二区块链节点的第二公钥地址。

本申请实施例中，第一区块链节点在随机生成第五私钥之后，会根据第五私钥生成临时的第四公钥，进而根据临时的第四公钥生成第二区块链节点的临时的第二公钥地址。其中，临时的第四公钥的含义与图 3 对应实施例中临时的第三公钥的含义类似，作用相同，为生成第二区块链节点的第二公钥地址的过程中产生的密钥，既不归属于第一区块链节点，也不归属于第二区块链节点，也不需要任何交易信息进行解密。

具体的，第一区块链节点根据第五私钥和第二区块链节点的第二公钥生成临时的第四公钥，进而根据临时的第四公钥生成第二区块链节点的临时的第二公钥地址。

其中，第二区块链节点的第二公钥地址的概念和第二区块链节点的第二公钥的概念均可以参阅图 3 对应各个实施例的描述，第一区块链节点执行步骤 603 的具体实现方式与图 3 对应实施例中步骤 303 的具体实现方式类似，区别仅在于将图 3 对应实施例中步骤 303 中的第二私钥替换为步骤 603 中的第五私钥，具体实现方式以及带来的有益效果可参阅图 3 中的描述，此处不做赘述。

604、第一区块链节点采用共享密钥对第五私钥进行对称加密，得到加密后的第五私钥。

本申请的一些实施例中，第一区块链节点会利用步骤 601 生成的共享密钥对第五私钥进行对称加密，以得到加密后的第五私钥。其中，加密后的第五私钥可以表示为 $En(h, S)$ ， h 代表随机生成的第五私钥， S 代表共享密钥， $En(h, S)$ 代表利用共享密钥对 h 进行对称加密。对称加密的算法指的是加密和解密使用相同密钥的加密算法，对称加密的算法包括但不限于数据加密标准 (DES, data encryption standard)、3 数据加密标准 (3DES, triple data encryption standard)、高级加密标准 (AES, advanced encryption standard) 或其他对称加密算法等等，此处不一一列举，具体采用哪种对称加密的算法，可结合实际情况灵活选择，此处不做限定。

需要说明的是，本申请实施例不限定步骤 603 和 604 的执行顺序，可以先执行步骤 603，再执行步骤 604，也可以先执行步骤 604，再执行步骤 603，还可以同时执行步骤 603 和步骤 604。

605、第一区块链节点将第二交易信息写入区块链，第二交易信息包括第一区块链节点的公钥地址、第二公钥地址、第一交易内容和加密后的第五私钥。

本申请的一些实施例中，第一区块链节点将第二交易信息写入区块链，也即将第二交

易信息上链。其中，第二交易信息包括第一区块链节点的公钥地址、第二公钥地址（也即第二区块链节点的临时公钥地址）、第一交易内容和加密后的第五私钥，也即第二交易信息的格式为字段 **Input** 的内容为第一区块链节点的公钥地址（也即交易发送方的公钥地址）、字段 **Output** 的内容为第二区块链节点的第二公钥地址（也即交易接收方的公钥地址）、字段交易内容的内容为第一交易内容和加密后的第五私钥，字段交易内容可以表示为
5 (Txcontents, En (h, S))。

进一步地，第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，写入区块链的第二交易信息由第二区块链节点根据第二公钥地址进行验证，第二公钥地址为根据第五私钥生成，加密后的第五私钥需要利用共享密钥进行解密，共享密钥在第二区块链节点处通过第一区块链节点的公钥和第二区块链节点的第一私钥生成。
10

606、第二区块链节点根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥。

本申请实施例中，第一区块链节点执行步骤 606 的具体实现方式与图 3 对应实施例中步骤 305 的具体实现方式类似，可参阅图 5 中的描述，此处不做赘述。
15

607、第二区块链节点对区块链上的至少一个交易信息进行读取，并判断区块链上的至少一个交易信息中是否存在第二交易信息，若存在，则确定第一交易内容指向的交易为交易成功；若不存在，则确定第一交易内容指向的交易为交易失败。

本申请实施例中，第二区块链节点需要遍历区块链节点上的所有交易信息，也即需要对区块链上的每个交易信息进行读取，以逐个判断区块链上的每个交易信息中是否为第二交易信息，也即判断区块链上的至少一个交易信息中是否存在第二交易信息。在区块链上的至少一个交易信息中存在第二交易信息的情况下，确定第一交易内容指向的交易为交易成功；在区块链上的至少一个交易信息中不存在第二交易信息的情况下，确定第一交易内容指向的交易为交易失败。
20

其中，区块链节点上的每个交易信息中均包括交易发送方的公钥地址（也即字段 **Input** 中的内容）、交易接收方的公钥地址（也即字段 **Output** 中的内容）、交易发送方和交易接收方之间的交易内容以及加密后的第五私钥。第二交易信息包括第一区块链节点的公钥地址、第二区块链节点的第二公钥地址、第一交易内容和加密后的第五私钥，加密后的第五私钥能够通过第二区块链节点生成的共享密钥解密，第二公钥地址能够根据第五私钥生成。
25

具体的，针对判断区块链上的至少一个交易信息中的任一个交易信息是否为第二交易信息的过程。第二区块链节点在读取到一个交易信息之后，会利用生成的共享密钥对加密后的密钥进行解密，进而采用步骤 603 中的方式，根据解密结果生成公钥地址，并判断生成的公钥地址是否与获取的交易信息中包括的交易接收方的公钥地址一致，若一致，则证明读取到的交易信息为第二交易信息，若不一致，则证明读取到的交易信息不是第二交易信息。
30
35

第二区块链节点对区块链上的每个交易信息均执行上述操作，以判断区块链上的每个交易信息是否为第二交易信息。

608、第二区块链节点根据第五私钥，生成第二区块链节点的第六私钥，第六私钥用于花费第二交易信息中的产品。

本申请实施例中，第二区块链节点在确定第二交易信息指向的交易为交易成功的情况下，当第二区块链节点需要花费第二交易信息中的产品时，还需要生成用于花费第二交易信息中的产品的临时的第六私钥，该临时的第六私钥与临时的第二公钥地址对应，也即该第六私钥需要能够在椭圆曲线的公钥密码体系的约束下，或者，在离散对数的公钥密码体系中的约束下，能够直接生成临时的第二公钥地址。

具体的，第二区块链节点根据第五私钥和第二区块链节点的第三私钥，生成第二区块链节点的临时的第六私钥。

更具体的，在一种情况中，步骤 608 可以包括：在椭圆曲线的公钥密码体系中，第二区块链节点根据临时的第五私钥和第二区块链节点的第三私钥（也即第二区块链节点的长期私钥），生成第二区块链节点的临时的第六私钥。具体实现方式可参阅图 3 对应实施例中步骤 308 中的描述，区别在于将步骤 308 中的第二私钥替换为步骤 608 中的第五私钥，需要说明的是，在椭圆曲线的公钥密码体系中，需要满足，生成的临时的第六私钥点乘生成元 G 之后，需要等于步骤 603 中生成的临时的第四公钥。

在另一种情况中，步骤 608 可以包括：在离散对数的公钥密码体系中，第二区块链节点根据临时的第五私钥和第二区块链节点的第三私钥（也即第二区块链节点的长期私钥），生成第二区块链节点的临时的第六私钥。具体实现方式可参阅图 3 对应实施例中步骤 308 中的描述，区别在于将步骤 308 中的第二私钥替换为步骤 608 中的第五私钥，需要说明的是，在离散对数的公钥密码体系中，需要满足，生成的临时的第六私钥与生成元 G 进行指数运算之后，需要等于步骤 603 中生成的临时的第四公钥。

为更直观地理解本方案，请参阅图 7 和图 8，图 7 和图 8 分别示出了本申请实施例提供的区块链信息的处理方法的两种流程示意图。图 7 和图 8 均以在椭圆曲线的公钥密码体系下为例；图 7 和图 8 的区别在于，图 7 以第一区块链节点和第二区块链节点均仅拥有一套固定密钥为例，图 8 以第一区块链节点和第二区块链节点均拥有两套固定密钥为例。先参阅图 7，第一区块链节点中配置有长期私钥 a 和长期公钥 A，第二区块链节点中配置有长期私钥 b 和长期公钥 B。E1、第一区块链节点通过将 a 与 B 进行点乘，生成共享密钥 S。E2、第一区块链节点随机生成临时的第五私钥 h。E3、第一区块链节点将 h 与 G 进行点乘，并将点乘结果与 B 相加，以生成临时的第三公钥 M，临时的第三公钥 M 用于生成第二区块链节点的临时的第二公钥地址。E4、第一区块链节点采用共享密钥对第五私钥进行对称加密，得到加密后的第五私钥。E5、第一区块链节点将第二交易信息上链，第二交易信息包括第一区块链节点的公钥地址（也即交易发送方的公钥地址）、第二区块链节点的临时的第二公钥地址（也即交易接收方的公钥地址）、第一交易内容和加密后的第五私钥。E6、第二区块链节点通过将 b 与 A 进行点乘，生成共享密钥 S。E7、第二区块链节点在读取到区块链上的一个交易信息之后，通过共享密钥对读取到的交易信息中加密后的私钥进行解密，得到解密结果 h1。需要说明的是，若当前读取的交易信息为第二交易信息，则 h1 与 h 相同；若当前读取的交易信息不是第二交易信息，则 h1 与 h 不同。E8、第二区块链节点将

h1 与 G 进行点乘, 并将点乘结果与 B 相加, 得到相加结果, 将计算到的相加结果与读取到交易信息中携带的交易接收方的公钥地址进行对比, 以判断计算到的相加结果与读取到的交易接收方的公钥地址是否相同, 若相同, 则证明读取到的交易信息为第二交易信息, 也即证明第二交易信息指向的交易成功; 若区块链上的所有交易信息均不是第二交易信息, 5 则证明第二交易信息执行的交易失败。E9、在第二交易信息指向的交易成功的情况下, 当第二区块链节点想要花费第二交易信息中的产品时, 还会根据第二私钥, 生成第二区块链节点的第六私钥, 第六私钥用于花费第二交易信息中的产品, m 点乘 G 之后需要等于 M, 也即 $m = (h+b) \bmod q$ 。

10 请继续参阅图 8, 图 8 与图 7 的区别在于, 第一, 图 8 中的第二区块链节点配置有长期私钥 b、长期公钥 B、扫描私钥 d 和扫描公钥 D。对应的, 步骤 F1 中, 第一区块链节点通过将 a 与 D 进行点乘, 生成共享密钥 S; 步骤 F6 中, 第二区块链节点通过将 d 与 A 进行点乘, 生成共享密钥 S。第二, 步骤 F3 中, 第一区块链节点将 h 与 B 进行点乘, 以生成临时的第四公钥 M, 对应的, 步骤 F8 中, 第二区块链节点将 h1 与 B 进行点乘, 判断计算到的点乘结果与读取到的交易接收方的公钥地址是否相同, 且在步骤 F9 中, 为了保证第六私钥 m 与 G 点乘后等于第四公钥 M, $m = (hb) \bmod q$ 。图 8 中剩余步骤的描述均可参阅上述图 7 中的介绍, 此处不做赘述。需要说明的是, 图 7 和图 8 中的举例均仅为方便理解本方案, 不用于限定本方案。

本申请实施例中, 在隐藏交易接收方的真实地址的前提下, 提供了交易接收方无需存储并管理多个公私钥对的又一实现方案, 提高了本方案的实现灵活性。

20 在图 1 至图 8 所对应的实施例的基础上, 为了更好的实施本申请实施例的上述方案, 下面还提供用于实施上述方案的相关设备。具体参阅图 9, 图 9 为本申请实施例提供的地址的生成装置的一种结构示意图。地址的生成装置 900 应用于第一区块链节点, 地址的生成装置 900 包括生成模块 901 和写入模块 902。其中, 生成模块 901, 用于根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥; 生成模块 901, 还用于根据共享密钥和第一交易内容生成第二区块链节点的第一公钥地址; 写入模块 902, 用于将第一交易信息写入区块链, 第一交易信息包括第一区块链节点的公钥地址、第一公钥地址和第一交易内容。其中, 第一交易内容为第一区块链节点和第二区块链节点之间的交易的内容, 写入区块链的第一交易信息由第二区块链节点根据第一公钥地址进行验证, 第一公钥地址需要利用共享密钥进行验证, 共享密钥在第二区块链节点处通过第一区块链节点的公钥和 25 第二区块链节点的第一私钥生成。

在一种可能的设计中, 生成模块 901, 具体用于根据共享密钥和第一交易内容生成第二私钥, 根据第二私钥和第二区块链节点的第二公钥生成第一公钥地址。

在一种可能的设计中, 生成模块 901, 具体用于将共享密钥和第一交易内容进行组合, 得到第一组合结果, 对第一组合结果进行哈希运算, 以生成第二私钥。

35 在一种可能的设计中, 生成模块 901, 具体用于: 在椭圆曲线的公钥密码体系中, 根据第二私钥和第二区块链节点的第二公钥, 生成第三公钥, 并根据第三公钥, 生成第一公钥地址; 或者, 在离散对数的公钥密码体系中, 根据第二私钥和第二区块链节点的第二公

钥，生成第三公钥，并根据第三公钥，生成第一公钥地址。

在一种可能的设计中，生成模块 901，具体用于执行以下两项中的任一项：在椭圆曲线的公钥密码体系中，将第一区块链节点的私钥与第二区块链节点的第一公钥进行点乘，得到共享密钥；或者，在离散对数的公钥密码体系中，根据第一区块链节点的私钥和第二区块链节点的第一公钥，进行指数运算，得到共享密钥，第二区块链节点的第一公钥为指数运算中的底数，第一区块链节点的私钥为指数运算中的指数。

在一种可能的设计中，第一区块链节点和第二区块链节点均仅拥有一套固定密钥，一套固定密钥中包括一个长期私钥和一个长期公钥，第一区块链节点的私钥为第一区块链节点的长期私钥，第二区块链节点的第一公钥为第二区块链节点的长期公钥，第一区块链节点的公钥为第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的长期私钥。或者，第一区块链节点和第二区块链节点均拥有两套固定密钥，两套固定密钥包括第一套固定密钥和第二套固定密钥，第一套固定密钥包括一个长期私钥和一个长期公钥，第二套固定密钥包括一个扫描私钥和一个扫描公钥，第一区块链节点的私钥为第一区块链节点的长期私钥，第二区块链节点的第一公钥为第二区块链节点的扫描公钥，第一区块链节点的公钥为第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的扫描私钥。

需要说明的是，地址的生成装置 900 中各模块/单元之间的信息交互、执行过程等内容，与本申请中图 3 至图 5 对应的各个方法实施例基于同一构思，具体内容可参见本申请前述所示的方法实施例中的叙述，此处不再赘述。

本申请实施例还提供一种区块链信息的处理装置，请参阅图 10，图 10 为本申请实施例提供的区块链信息的处理装置的一种结构示意图。区块链信息的处理装置 1000 应用于第二区块链节点，区块链信息的处理装置 1000 包括生成模块 1001、读取模块 1002 和确定模块 1003。其中，生成模块 1001，用于根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥；读取模块 1002，用于对区块链上的至少一个交易信息进行读取；确定模块 1003，用于在至少一个交易信息中存在第一交易信息的情况下，确定第一交易内容指向的交易为交易成功，第一交易信息包括第一区块链节点的公钥地址、第一交易内容和第二区块链节点的第一公钥地址。其中，第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易的内容，第一公钥地址能够根据共享密钥和第一交易内容生成。

在一种可能的设计中，生成模块 1001，具体用于：在椭圆曲线的公钥密码体系中，将第一区块链节点的公钥和第二区块链节点的第一私钥进行点乘，得到共享密钥；或者，在离散对数的公钥密码体系中，根据第一区块链节点的公钥和第二区块链节点的第一私钥，进行指数运算，第一区块链节点的公钥为指数运算中的底数，第二区块链节点的第一私钥为指数运算中的指数。

在一种可能的设计中，生成模块 1001，还用于根据共享密钥和第一交易内容，生成第二私钥；生成模块 1001，还用于根据第二私钥和第二区块链节点的第三私钥，生成第二区块链节点的第四私钥，第四私钥用于花费第一交易信息中的产品。

在一种可能的设计中，第一区块链节点和第二区块链节点均仅拥有一套固定密钥，一套固定密钥中包括一个长期私钥和一个长期公钥，第一区块链节点的公钥为第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的长期私钥。或者，第一区块链节点和第二区块链节点均拥有两套固定密钥，两套固定密钥包括第一套固定密钥和
5 第二套固定密钥，第一套固定密钥包括一个长期私钥和一个长期公钥，第二套固定密钥包括一个扫描私钥和一个扫描公钥，第一区块链节点的公钥为第一区块链节点的长期公钥，第二区块链节点的第一私钥为第二区块链节点的扫描私钥。

需要说明的是，区块链信息的处理装置 1000 中各模块/单元之间的信息交互、执行过程等内容，与本申请中图 3 至图 5 对应的各个方法实施例基于同一构思，具体内容可参见
10 本申请前述所示的方法实施例中的叙述，此处不再赘述。

本申请实施例还提供一种地址的生成装置，具体参阅图 11，图 11 为本申请实施例提供的地址的生成装置的一种结构示意图。地址的生成装置 1100 应用于第一区块链节点，地址的生成装置 1100 包括生成模块 1101、加密模块 1102、和写入模块 1103。其中，生成模块 1101，用于根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥；生成
15 模块 1101，还用于随机生成第五私钥，并根据第五私钥生成第二区块链节点的第二公钥地址；加密模块 1102，用于采用共享密钥对第五私钥进行对称加密，得到加密后的第五私钥；写入模块 1103，用于将第二交易信息写入区块链，第二交易信息包括第一区块链节点的公钥地址、第二公钥地址、第一交易内容和加密后的第五私钥。其中，第一区块链节点的公钥地址属于第一区块链节点，第一交易内容为第一区块链节点和第二区块链节点之间交易
20 的内容，写入区块链的第二交易信息由第二区块链节点根据第二公钥地址进行验证，第二公钥地址为根据第五私钥生成，加密后的第五私钥需要利用共享密钥进行解密，共享密钥在第二区块链节点处通过第一区块链节点的公钥和第二区块链节点的第一私钥生成。

在一种可能的设计中，生成模块 1101，具体用于执行以下两项中的任一项：在椭圆曲线的公钥密码体系中，将第一区块链节点的私钥与第二区块链节点的第一公钥进行点乘，
25 得到共享密钥；或者，在离散对数的公钥密码体系中，根据第一区块链节点的私钥和第二区块链节点的第一公钥，进行指数运算，第二区块链节点的第一公钥为指数运算中的底数，第一区块链节点的私钥为指数运算中的指数。

在一种可能的设计中，生成模块 1101，具体用于根据第五私钥和第二区块链节点的第二公钥，生成第二公钥地址。

需要说明的是，地址的生成装置 1100 中各模块/单元之间的信息交互、执行过程等内容，与本申请中图 6 至图 8 对应的各个方法实施例基于同一构思，具体内容可参见本申请
30 前述所示的方法实施例中的叙述，此处不再赘述。

本申请实施例还提供一种区块链信息的处理装置，请参阅图 12，图 12 为本申请实施例提供的区块链信息的处理装置的一种结构示意图。区块链信息的处理装置 1200 应用于第二区块链节点，区块链信息的处理装置 1200 包括生成模块 1201、读取模块 1202 和确定模
35 块 1203。其中，生成模块 1201，用于根据第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥；读取模块 1202，用于对区块链上的至少一个交易信息进行读取；确定

模块 1203, 用于在至少一个交易信息中存在第二交易信息的情况下, 确定第一交易内容指向的交易为交易成功, 第二交易信息包括第一区块链节点的公钥地址、第二区块链节点的第二公钥地址、第一交易内容和加密后的第五私钥。其中, 第一区块链节点的公钥地址属于第一区块链节点, 第一交易内容为第一区块链节点和第二区块链节点之间交易的内容, 加密后的第五私钥能够通过共享密钥解密, 第二公钥地址能够根据第五私钥生成。

在一种可能的设计中, 生成模块 1201, 具体用于执行以下两项中的任一项: 在椭圆曲线的公钥密码体系中, 将第一区块链节点的公钥和第二区块链节点的第一私钥进行点乘, 得到共享密钥; 或者, 在离散对数的公钥密码体系中, 根据第一区块链节点的公钥和第二区块链节点的第一私钥, 进行指数运算, 第一区块链节点的公钥为指数运算中的底数, 第二区块链节点的第一私钥为指数运算中的指数。

在一种可能的设计中, 生成模块 1201, 还用于根据第五私钥和第二区块链节点的第三私钥, 生成第二区块链节点的第六私钥, 第六私钥用于花费第二交易信息中的产品。

需要说明的是, 区块链信息的处理装置 1200 中各模块/单元之间的信息交互、执行过程等内容, 与本申请中图 6 至图 8 对应的各个方法实施例基于同一构思, 具体内容可参见本申请前述所示的方法实施例中的叙述, 此处不再赘述。

本申请实施例还提供了一种区块链节点, 请参阅图 13, 图 13 为本申请实施例提供的区块链节点的一种结构示意图。其中, 区块链节点 1300 上可以部署有图 3 至图 5 对应实施例中所描述的第一区块链节点, 用于实现图 9 对应实施例中地址的生成装置 900 的功能。或者, 区块链节点 1300 上可以部署有图 3 至图 5 对应实施例中所描述的第二区块链节点, 用于实现图 10 对应实施例中区块链信息的处理装置 1000 的功能。或者, 区块链节点 1300 上可以部署有图 6 至图 8 对应实施例中所描述的第一区块链节点, 用于实现图 11 对应实施例中地址的生成装置 1100 的功能。或者, 区块链节点 1300 上可以部署有图 6 至图 8 对应实施例中所描述的第二区块链节点, 用于实现图 12 对应实施例中区块链信息的处理装置 1200 的功能。

具体的, 区块链节点 1300 包括: 接收器 1301、发射器 1302、处理器 1303 和存储器 1304 (其中区块链节点 1300 中的处理器 1303 的数量可以一个或多个, 图 13 中以一个处理器为例), 其中, 处理器 1303 可以包括应用处理器 13031 和通信处理器 13032。在本申请实施例的一些实施例中, 接收器 1301、发射器 1302、处理器 1303 和存储器 1304 可通过总线或其它方式连接。

存储器 1304 可以包括只读存储器和随机存取存储器, 并向处理器 1303 提供指令和数据。存储器 1304 的一部分还可以包括非易失性随机存取存储器 (non-volatile random access memory, NVRAM)。存储器 1304 存储有处理器和操作指令、可执行模块或者数据结构, 或者它们的子集, 或者它们的扩展集, 其中, 操作指令可包括各种操作指令, 用于实现各种操作。

处理器 1303 控制数据生成装置的操作。具体的应用中, 数据生成装置的各个组件通过总线系统耦合在一起, 其中总线系统除包括数据总线之外, 还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见, 在图中将各种总线都称为总线系统。

上述本申请实施例揭示的方法可以应用于处理器 1303 中，或者由处理器 1303 实现。处理器 1303 可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 1303 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 1303 可以是通用处理器、数字信号处理器（digital signal processing, DSP）、微处理器或微控制器，还可进一步包括专用集成电路（application specific integrated circuit, ASIC）、现场可编程门阵列（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。该处理器 1303 可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码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 1304，处理器 1303 读取存储器 1304 中的信息，结合其硬件完成上述方法的步骤。

接收器 1301 可用于接收输入的数字或字符信息，以及产生与数据生成装置的相关设置以及功能控制有关的信号输入。发射器 1302 可用于通过第一接口输出数字或字符信息，发射器 1302 还可用于通过第一接口向磁盘组发送指令，以修改磁盘组中的数据，发射器 1302 还可以包括显示屏等显示设备。

本申请实施例中，在一种情况下，应用处理器 13031，用于实现图 3 至图 5 对应实施例中第一区块链节点的功能。对于应用处理器 13031 执行图 3 至图 5 对应实施例中第一区块链节点的功能的具体实现方式以及带来的有益效果，均可以参考图 3 至图 5 对应的各个方法实施例中的叙述，此处不再一一赘述。

在另一种情况下，应用处理器 13031，用于实现图 3 至图 5 对应实施例中第二区块链节点的功能。对于应用处理器 13031 执行图 3 至图 5 对应实施例中第二区块链节点的功能的具体实现方式以及带来的有益效果，均可以参考图 3 至图 5 对应的各个方法实施例中的叙述，此处不再一一赘述。

在一种情况下，应用处理器 13031，用于实现图 6 至图 8 对应实施例中第一区块链节点的功能。对于应用处理器 13031 执行图 6 至图 8 对应实施例中第一区块链节点的功能的具体实现方式以及带来的有益效果，均可以参考图 6 至图 8 对应的各个方法实施例中的叙述，此处不再一一赘述。

在另一种情况下，应用处理器 13031，用于实现图 6 至图 8 对应实施例中第二区块链节点的功能。对于应用处理器 13031 执行图 6 至图 8 对应实施例中第二区块链节点的功能的具体实现方式以及带来的有益效果，均可以参考图 6 至图 8 对应的各个方法实施例中的叙述，此处不再一一赘述。

本申请实施例中还提供一种计算机可读存储介质，该计算机可读存储介质中存储有程序，当其在计算机上运行时，使得计算机执行如前述图 3 至图 5 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如前述图 3 至图 5 所示实施例描述的方法中第二区块链节点所执行的步骤。

本申请实施例中还提供一种计算机可读存储介质，该计算机可读存储介质中存储有程序，当其在计算机上运行时，使得计算机执行如前述图 6 至图 8 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如前述图 6 至图 8 所示实施例描述的方法中第二区块链节点所执行的步骤。

5 本申请实施例中还提供一种计算机程序，当其在计算机上运行时，使得计算机执行如前述图 3 至图 5 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如前述图 3 至图 5 所示实施例描述的方法中第二区块链节点所执行的步骤。

本申请实施例中还提供一种计算机程序，当其在计算机上运行时，使得计算机执行如前述图 6 至图 8 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如前述图 6 至图 8 所示实施例描述的方法中第二区块链节点所执行的步骤。

10 本申请实施例中还提供一种电路系统，所述电路系统包括处理电路，所述处理电路配置为执行如前述图 3 至图 5 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如前述图 3 至图 5 所示实施例描述的方法中第二区块链节点所执行的步骤。

本申请实施例中还提供一种电路系统，所述电路系统包括处理电路，所述处理电路配置为执行如前述图 6 至图 8 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如前述图 6 至图 8 所示实施例描述的方法中第二区块链节点所执行的步骤。

本申请实施例提供的相关设备具体可以为芯片，芯片包括：处理单元和通讯单元，所述处理单元例如可以是处理器，所述通讯单元例如可以是输入/输出接口、管脚或电路等。该处理单元可执行存储单元存储的计算机执行指令，以使芯片执行上述前述图 3 至图 5 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如上述图 3 至图 5 所示实施例描述的方法中第二区块链节点所执行的步骤，或者，执行上述前述图 6 至图 8 所示实施例描述的方法中第一区块链节点所执行的步骤，或者，执行如上述图 6 至图 8 所示实施例描述的方法中第二区块链节点所执行的步骤。可选地，所述存储单元为所述芯片内的存储单元，如寄存器、缓存等，所述存储单元还可以是所述无线接入设备端内的位于所述芯片外部的存储单元，如只读存储器（read-only memory，ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory，RAM）等。

25 其中，上述任一处提到的处理器，可以是一个通用中央处理器，微处理器，ASIC，或一个或多个用于控制上述方法的程序执行的集成电路。

另外需说明的是，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30 需要选择其中的部分或者全部模块来实现本实施例方案的目的。另外，本申请提供的装置实施例附图中，模块之间的连接关系表示它们之间具有通讯连接，具体可以实现为一条或多条通讯总线或信号线。

35 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现，当然也可以通过专用硬件包括专用集成电路、专用 CLU、专用存储器、专用元器件等来实现。一般情况下，凡由计算机程序完成的功能都可以很容

易地用相应的硬件来实现,而且,用来实现同一功能的具体硬件结构也可以是多种多样的,例如模拟电路、数字电路或专用电路等。但是,对本申请而言更多情况下软件程序实现是更佳的实施方式。基于这样的理解,本申请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,该计算机软件产品存储在可读取的存储介质中,如计算机的软盘、U 盘、移动硬盘、ROM、RAM、磁碟或者光盘等,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)执行本申请各个实施例所述的方法。

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的形式实现。

所述计算机程序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申请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(如同轴电缆、光纤、数字用户线(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存储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,DVD)、或者半导体介质(例如固态硬盘(Solid State Disk, SSD))等。

权 利 要 求

1.一种地址的生成方法，其特征在于，所述方法应用于第一区块链节点，所述方法包括：

根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥生成共享密钥；

5 根据所述共享密钥和第一交易内容生成第二区块链节点的第一公钥地址；

将第一交易信息写入区块链，所述第一交易信息包括所述第一区块链节点的公钥地址、所述第一公钥地址和所述第一交易内容；

其中，所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间的交易的内容，写入区块链的所述第一交易信息由所述第二区块链节点根据所述第一公钥地址进行验证，所述第一公钥地址需要利用所述共享密钥进行验证，所述共享密钥在所述第二区块链节点处通过所述第一区块链节点的公钥和所述第二区块链节点的第一私钥生成。

2.根据权利要求 1 所述的方法，其特征在于，所述根据所述共享密钥和第一交易内容生成第一交易信息的第一公钥地址，包括：

根据所述共享密钥和所述第一交易内容生成第二私钥；

15 根据所述第二私钥和所述第二区块链节点的第二公钥生成所述第一公钥地址。

3.根据权利要求 2 所述的方法，其特征在于，所述根据所述共享密钥和所述第一交易内容生成第二私钥，包括：

将所述共享密钥和所述第一交易内容进行组合，得到第一组合结果；

对所述第一组合结果进行哈希运算，以生成所述第二私钥。

20 4.根据权利要求 2 所述的方法，其特征在于，所述根据所述第二私钥和所述第二区块链节点的第二公钥生成所述第一公钥地址，包括：

在椭圆曲线的公钥密码体系中，根据所述第二私钥和所述第二区块链节点的第二公钥，生成第三公钥，并根据所述第三公钥，生成所述第一公钥地址；或者，

25 在离散对数的公钥密码体系中，根据所述第二私钥和所述第二区块链节点的第二公钥，生成第三公钥，并根据所述第三公钥，生成所述第一公钥地址。

5.根据权利要求 1 至 4 任一项所述的方法，其特征在于，所述根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥生成共享密钥，包括：

在椭圆曲线的公钥密码体系中，将所述第一区块链节点的私钥与所述第二区块链节点的第一公钥进行点乘，得到所述共享密钥；或者，

30 在离散对数的公钥密码体系中，根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥，进行指数运算，得到所述共享密钥，所述第二区块链节点的第一公钥为所述指数运算中的底数，所述第一区块链节点的私钥为所述指数运算中的指数。

6.根据权利要求 1 至 4 任一项所述的方法，其特征在于，

35 所述第一区块链节点和所述第二区块链节点均仅拥有一套固定密钥，所述一套固定密钥中包括一个长期私钥和一个长期公钥，所述第一区块链节点的私钥为所述第一区块链节点的长期私钥，所述第二区块链节点的第一公钥为所述第二区块链节点的长期公钥，所述第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私

- 32 -

钥为所述第二区块链节点的长期私钥；或者，

所述第一区块链节点和所述第二区块链节点均拥有两套固定密钥，所述两套固定密钥包括第一套固定密钥和第二套固定密钥，所述第一套固定密钥包括一个长期私钥和一个长期公钥，所述第二套固定密钥包括一个扫描私钥和一个扫描公钥，所述第一区块链节点的私钥为所述第一区块链节点的长期私钥，所述第二区块链节点的第一公钥为所述第二区块链节点的扫描公钥，所述第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私钥为所述第二区块链节点的扫描私钥。

7.一种区块链信息的处理方法，其特征在于，所述方法应用于第二区块链节点，所述方法包括：

10 根据第一区块链节点的公钥和所述第二区块链节点的第一私钥生成共享密钥；

对区块链上的至少一个交易信息进行读取；

在所述第二区块链节点确定所述至少一个交易信息中存在第一交易信息的情况下，确定第一交易内容指向的交易为交易成功，所述第一交易信息包括所述第一区块链节点的公钥地址、所述第一交易内容和所述第二区块链节点的第一公钥地址；

15 其中，所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间交易的内容，所述第一公钥地址为根据所述共享密钥和所述第一交易内容生成。

8.根据权利要求 7 所述的方法，其特征在于，所述根据第一区块链节点的公钥和所述第二区块链节点的第一私钥生成共享密钥，包括：

20 在椭圆曲线的公钥密码体系中，将所述第一区块链节点的公钥和所述第二区块链节点的第一私钥进行点乘，得到所述共享密钥；或者，

在离散对数的公钥密码体系中，根据所述第一区块链节点的公钥和所述第二区块链节点的第一私钥，进行指数运算，所述第一区块链节点的公钥为所述指数运算中的底数，所述第二区块链节点的第一私钥为所述指数运算中的指数。

9.根据权利要求 7 或 8 所述的方法，其特征在于，所述方法还包括：

25 根据所述共享密钥和所述第一交易内容，生成第二私钥；

根据所述第二私钥和所述第二区块链节点的第三私钥，生成所述第二区块链节点的第四私钥，所述第四私钥用于花费所述第一交易信息中的产品。

10.根据权利要求 7 或 8 所述的方法，其特征在于，

30 所述第一区块链节点和所述第二区块链节点均仅拥有一套固定密钥，所述一套固定密钥中包括一个长期私钥和一个长期公钥，所述第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私钥为所述第二区块链节点的长期私钥；或者，

所述第一区块链节点和所述第二区块链节点均拥有两套固定密钥，所述两套固定密钥包括第一套固定密钥和第二套固定密钥，所述第一套固定密钥包括一个长期私钥和一个长期公钥，所述第二套固定密钥包括一个扫描私钥和一个扫描公钥，所述第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私钥为所述第二区块链节点的扫描私钥。

11.一种地址的生成方法，其特征在于，所述方法应用于第一区块链节点，所述方法包

括:

根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥生成共享密钥;
随机生成第五私钥, 并根据所述第五私钥生成第二区块链节点的第二公钥地址;
采用所述共享密钥对所述第五私钥进行对称加密, 得到加密后的第五私钥;

- 5 将所述第二交易信息写入区块链, 所述第二交易信息包括所述第一区块链节点的公钥地址、所述第二公钥地址、第一交易内容和所述加密后的第五私钥;

其中, 所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间交易的内容, 写入区块链的所述第二交易信息由所述第二区块链节点根据所述第二公钥地址进行验证, 所述加密后的第五私钥需要利用所述共享密钥进行解密, 所述共享密钥在所述第二区块链节点处通过所述第一区块链节点的公钥和所述第二区块链节点的第一私钥生成。

10

12. 根据权利要求 11 所述的方法, 其特征在于, 所述根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥生成共享密钥, 包括:

在椭圆曲线的公钥密码体系中, 将所述第一区块链节点的私钥与所述第二区块链节点的第一公钥进行点乘, 得到所述共享密钥; 或者,

- 15 在离散对数的公钥密码体系中, 根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥, 进行指数运算, 所述第二区块链节点的第一公钥为所述指数运算中的底数, 所述第一区块链节点的私钥为所述指数运算中的指数。

13. 根据权利要求 11 或 12 所述的方法, 其特征在于, 所述根据所述第五私钥生成第二区块链节点的第二公钥地址, 包括:

- 20 根据所述第五私钥和所述第二区块链节点的第二公钥, 生成所述第二公钥地址。

14. 一种区块链信息的处理方法, 其特征在于, 所述方法应用于第二区块链节点, 所述方法包括:

根据第一区块链节点的公钥和所述第二区块链节点的第一私钥生成共享密钥;
对区块链上的至少一个交易信息进行读取;

- 25 在所述第二区块链节点确定至少一个交易信息中存在第二交易信息的情况下, 确定第一交易内容指向的交易为交易成功, 所述第二交易信息包括所述第一区块链节点的公钥地址、所述第二区块链节点的第二公钥地址、所述第一交易内容和所述加密后的第五私钥;

其中, 所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间交易的内容, 所述加密后的第五私钥通过所述共享密钥解密, 所述第二公钥地址为根据所述第五私钥生成。

30

15. 根据权利要求 14 所述的方法, 其特征在于, 所述根据第一区块链节点的公钥和所述第二区块链节点的第一私钥生成共享密钥, 包括:

在椭圆曲线的公钥密码体系中, 将所述第一区块链节点的公钥和所述第二区块链节点的第一私钥进行点乘, 得到所述共享密钥; 或者,

- 35 在离散对数的公钥密码体系中, 根据所述第一区块链节点的公钥和所述第二区块链节点的第一私钥, 进行指数运算, 所述第一区块链节点的公钥为所述指数运算中的底数, 所述第二区块链节点的第一私钥为所述指数运算中的指数。

16.根据权利要求 14 或 15 所述的方法，其特征在于，所述方法还包括：

根据所述第五私钥和所述第二区块链节点的第三私钥，生成所述第二区块链节点的第六私钥，所述第六私钥用于花费所述第二交易信息中的产品。

17.一种地址的生成装置，其特征在于，所述装置应用于第一区块链节点，所述装置包
5 括：

生成模块，用于根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥生成共享密钥；

所述生成模块，还用于根据所述共享密钥和第一交易内容生成第二区块链节点的第一公钥地址；

10 写入模块，用于将第一交易信息写入区块链，所述第一交易信息包括所述第一区块链节点的公钥地址、所述第一公钥地址和所述第一交易内容；

其中，所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间的交易的内容，写入区块链的所述第一交易信息由所述第二区块链节点根据所述第一公钥地址进行验证，所述第一公钥地址需要利用所述共享密钥进行验证，所述共享密钥在所述第二区块链节点处通过所述第一区块链节点的公钥和所述第二区块链节点的第一私钥生成。
15

18.根据权利要求 17 所述的装置，其特征在于，

所述生成模块，具体用于根据所述共享密钥和所述第一交易内容生成第二私钥，根据所述第二私钥和所述第二区块链节点的第二公钥生成所述第一公钥地址。

19.根据权利要求 18 所述的装置，其特征在于，

20 所述生成模块，具体用于将所述共享密钥和所述第一交易内容进行组合，得到第一组合结果，对所述第一组合结果进行哈希运算，以生成所述第二私钥。

20.根据权利要求 18 所述的装置，其特征在于，所述生成模块，具体用于：

在椭圆曲线的公钥密码体系中，根据所述第二私钥和所述第二区块链节点的第二公钥，生成第三公钥，并根据所述第三公钥，生成所述第一公钥地址；或者，

25 在离散对数的公钥密码体系中，根据所述第二私钥和所述第二区块链节点的第二公钥，生成第三公钥，并根据所述第三公钥，生成所述第一公钥地址。

21.根据权利要求 17 至 20 任一项所述的装置，其特征在于，

所述生成模块，具体用于：

30 在椭圆曲线的公钥密码体系中，将所述第一区块链节点的私钥与所述第二区块链节点的第一公钥进行点乘，得到所述共享密钥；或者，

在离散对数的公钥密码体系中，根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥，进行指数运算，得到所述共享密钥，所述第二区块链节点的第一公钥为所述指数运算中的底数，所述第一区块链节点的私钥为所述指数运算中的指数。

22.根据权利要求 17 至 20 任一项所述的装置，其特征在于，

35 所述第一区块链节点和所述第二区块链节点均仅拥有一套固定密钥，所述一套固定密钥中包括一个长期私钥和一个长期公钥，所述第一区块链节点的私钥为所述第一区块链节点的长期私钥，所述第二区块链节点的第一公钥为所述第二区块链节点的长期公钥，所述

— 35 —

第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私钥为所述第二区块链节点的长期私钥；或者，

所述第一区块链节点和所述第二区块链节点均拥有两套固定密钥，所述两套固定密钥包括第一套固定密钥和第二套固定密钥，所述第一套固定密钥包括一个长期私钥和一个长期公钥，所述第二套固定密钥包括一个扫描私钥和一个扫描公钥，所述第一区块链节点的私钥为所述第一区块链节点的长期私钥，所述第二区块链节点的第一公钥为所述第二区块链节点的扫描公钥，所述第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私钥为所述第二区块链节点的扫描私钥。

23.一种区块链信息的处理装置，其特征在于，所述装置应用于第二区块链节点，所述装置包括：

生成模块，用于根据第一区块链节点的公钥和所述第二区块链节点的第一私钥生成共享密钥；

读取模块，用于对区块链上的至少一个交易信息进行读取；

确定模块，用于在所述至少一个交易信息中存在第一交易信息的情况下，确定第一交易内容指向的交易为交易成功，所述第一交易信息包括所述第一区块链节点的公钥地址、第一交易内容和所述第二区块链节点的第一公钥地址；

其中，所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间交易的内容，所述第一公钥地址能够根据所述共享密钥和所述第一交易内容生成。

24.根据权利要求 23 所述的装置，其特征在于，所述生成模块，具体用于：

在椭圆曲线的公钥密码体系中，将所述第一区块链节点的公钥和所述第二区块链节点的第一私钥进行点乘，得到所述共享密钥；或者，

在离散对数的公钥密码体系中，根据所述第一区块链节点的公钥和所述第二区块链节点的第一私钥，进行指数运算，所述第一区块链节点的公钥为所述指数运算中的底数，所述第二区块链节点的第一私钥为所述指数运算中的指数。

25.根据权利要求 23 或 24 所述的装置，其特征在于，

所述生成模块，还用于根据所述共享密钥和所述第一交易内容，生成第二私钥；

所述生成模块，还用于根据所述第二私钥和所述第二区块链节点的第三私钥，生成所述第二区块链节点的第四私钥，所述第四私钥用于花费所述第一交易信息中的产品。

26.根据权利要求 23 或 24 所述的装置，其特征在于，

所述第一区块链节点和所述第二区块链节点均仅拥有一套固定密钥，所述一套固定密钥中包括一个长期私钥和一个长期公钥，所述第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私钥为所述第二区块链节点的长期私钥；或者，

所述第一区块链节点和所述第二区块链节点均拥有两套固定密钥，所述两套固定密钥包括第一套固定密钥和第二套固定密钥，所述第一套固定密钥包括一个长期私钥和一个长期公钥，所述第二套固定密钥包括一个扫描私钥和一个扫描公钥，所述第一区块链节点的公钥为所述第一区块链节点的长期公钥，所述第二区块链节点的第一私钥为所述第二区块链节点的扫描私钥。

27.一种地址的生成装置，其特征在于，所述装置应用于第一区块链节点，所述装置包括：

生成模块，用于根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥生成共享密钥；

5 所述生成模块，还用于随机生成第五私钥，并根据所述第五私钥生成第二区块链节点的第二公钥地址；

加密模块，用于采用所述共享密钥对所述第五私钥进行对称加密，得到加密后的第五私钥；

10 写入模块，用于将所述第二交易信息写入区块链，所述第二交易信息包括所述第一区块链节点的公钥地址、所述第二公钥地址、第一交易内容和所述加密后的第五私钥；

其中，所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间交易的内容，写入区块链的所述第二交易信息由所述第二区块链节点根据所述第二公钥地址进行验证，所述加密后的第五私钥需要利用所述共享密钥进行解密，所述共享密钥在所述第二区块链节点处通过所述第一区块链节点的公钥和所述第二区块链节点的第一私钥生成。

15 28.根据权利要求 27 所述的装置，其特征在于，所述生成模块，具体用于：

在椭圆曲线的公钥密码体系中，将所述第一区块链节点的私钥与所述第二区块链节点的第一公钥进行点乘，得到所述共享密钥；或者，

20 在离散对数的公钥密码体系中，根据所述第一区块链节点的私钥和所述第二区块链节点的第一公钥，进行指数运算，所述第二区块链节点的第一公钥为所述指数运算中的底数，所述所述第一区块链节点的私钥为所述指数运算中的指数。

29.根据权利要求 27 或 28 所述的装置，其特征在于，

所述生成模块，具体用于根据所述第五私钥和所述第二区块链节点的第二公钥，生成所述第二公钥地址。

25 30.一种区块链信息的处理装置，其特征在于，所述装置应用于第二区块链节点，所述装置包括：

生成模块，用于根据第一区块链节点的公钥和所述第二区块链节点的第一私钥生成共享密钥；

读取模块，用于对区块链上的至少一个交易信息进行读取；

30 确定模块，用于在所述至少一个交易信息中存在第二交易信息的情况下，确定第一交易内容指向的交易为交易成功，所述第二交易信息包括所述第一区块链节点的公钥地址、所述第二区块链节点的第二公钥地址、所述第一交易内容和所述加密后的第五私钥；

其中，所述第一交易内容为所述第一区块链节点和所述第二区块链节点之间交易的内容，所述加密后的第五私钥为通过所述共享密钥解密，所述第二公钥地址为根据所述第五私钥生成。

35 31.根据权利要求 30 所述的装置，其特征在于，所述生成模块，具体用于：

在椭圆曲线的公钥密码体系中，将所述第一区块链节点的公钥和所述第二区块链节点的第一私钥进行点乘，得到所述共享密钥；或者，

—37—

在离散对数的公钥密码体系中，根据所述第一区块链节点的公钥和所述第二区块链节点的第一私钥，进行指数运算，所述第一区块链节点的公钥为所述指数运算中的底数，所述第二区块链节点的第一私钥为所述指数运算中的指数。

32.根据权利要求 30 或 31 所述的装置，其特征在于，

5 所述生成模块，还用于根据所述第五私钥和所述第二区块链节点的第三私钥，生成所述第二区块链节点的第六私钥，所述第六私钥用于花费所述第二交易信息中的产品。

33.一种计算机程序，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 1 至 6 中任一项所述的方法，或者，使得计算机执行如权利要求 7 至 10 任一项所述的方法，或者，使得计算机执行如权利要求 11 至 13 任一项所述的方法，或者，使得计算机执行如权利要求 14 至 16 任一项所述的方法。

10 34.一种区块链节点，其特征在于，包括处理器，所述处理器与所述存储器耦合；
所述存储器，用于存储程序；

所述处理器，用于执行所述存储器中的程序，使得所述区块链节点执行如权利要求 1 至 6 中任一项所述的方法，或者，使得所述区块链节点执行如权利要求 7 至 10 任一项所述的方法，或者，使得所述区块链节点执行如权利要求 11 至 13 任一项所述的方法，或者，使得所述区块链节点执行如权利要求 14 至 16 任一项所述的方法。