

注：

非对称加解密算法采用RSA；

对于一对RSA密钥KRN，称其中公钥为KRN pub，私钥为KRN pri；

对称加解密算法采用AES；

AES密钥称为KA；

信息摘要算法采用SHA-256

用户端A的第n次计算任务记为An，如A的第1次计算任务记为A1；

用户端A执行计算任务A1的流程如下：

1.

1.1 : 用户端A生成一对密钥KRA,，将其中公钥KRA pub发送给密钥管理器；

1.2：密钥管理器收到用户端A发来的包含公钥KRA pub的请求后，生成一对新密钥KRS和一个新密钥KA，将新生成的密钥KA用KRA pub加密，KRS pub用KA加密，并对加密后的密文用KRS pri进行加签，返回给用户端A。并且，密钥管理器保存KRA pub与KRS及KA的对应关系。用户端A先用KRA pri对密文解密得到KA，再用KA对密文解密得到KRS pub，而后用KRS pub对密文进行验签，验签成功说明得到的KRS pub和KA可信。

流程1完成后，各模块拥有信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 用户端A | 密钥管理器 | 文件接收器 | 代码运行器 | 区块链记录 |
| KRA,  KRS pub，  KA | KRA pub,  KRS,  KA, |  |  |  |

2.

2.1：

用户端A创建一个任务，该任务名称为task\_name，任务创建时间为create\_time，要执行的代码文件为File，File在用户端的路径为task\_file\_path。对task\_name，create\_time和task\_file\_path拼接而成的字符串生成信息摘要HashA1。

用KRS pub对HashA1和KA进行加密，用KA对代码文件和数据文件File进行加密，，然后将自有的公钥KRA pub，用KRS pub加密的HashA1 encrypted和KAencrypted，用KA加密后的文件Fileencrypted，以及KRA pri对各加密内容的签名，一起发送给文件接收器；

2.2：

文件接收器先用收到的KRA pub对各加密内容验签。

验签成功后，文件接收器用收到的KRA pub从密钥管理器中获取对应的KRS和KA。文件接收器用KRS pri解密KAencrypted，若解密后得到的KA与从密钥管理器获得的KA相同，那么说明本次从用户端A接收的信息确实由用户端A发出。

2.3：

文件接收器用KRS pri解密HashA1 encrypted得到HashA1，用KA解密Fileencrypted进行解密得到File。并且文件接收器向用户端返回信息，表示成功接收该次任务。

流程2完成后，各模块拥有信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 用户端A | 密钥管理器 | 文件接收器 | 代码运行器 | 区块链记录 |
| KRA,  KRS pub，  KA，  File，  HashA1 | KRA pub,  KRS,  KA, | KRA pub,  KRS,  KA,  File,  HashA1 |  |  |

3.

文件接收器将KRA pub，KA，HashA1与File传递到代码运行器。

代码运行器运行File，得到运行结果resultA1，将运行结果用KA加密得到resultA1 encrypted；此外，还记录运行信息run\_infoA1，并对其用KA加密，得到run\_infoA1 encrypted；

流程3完成后，各模块拥有信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 用户端A | 密钥管理器 | 文件接收器 | 代码运行器 | 区块链记录 |
| KRA,  KRS pub，  KA，  File，  HashA1 | KRA pub,  KRS,  KA, | KRA pub,  KRS,  KA,  File,  HashA1 | KRA pub,  KA,  File,  HashA1,  resultA1 encrypted,  run\_infoA1 encrypted |  |

4.

代码运行器将KRA pub，HashA1，resultA1 encrypted和run\_infoA1 encrypted传递到区块链记录。

区块链记录创建新区块记录HashA1，resultA1 encrypted和run\_infoA1 encrypted；并且，维护KRA pub和其每次任务Hash的对应关系，以便计费等操作。

流程4完成后，各模块拥有信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 用户端A | 密钥管理器 | 文件接收器 | 代码运行器 | 区块链记录 |
| KRA,  KRS pub，  KA，  File，  HashA1 | KRA pub,  KRS,  KA, | KRA pub,  KRS,  KA,  File,  HashA1 | KRA pub,  KA,  File,  HashA1,  resultA1 encrypted,  run\_infoA1 encrypted | KRA pub,  HashA1,  resultA1 encrypted,  run\_infoA1 encrypted, |

5.

用户端A用HashA1向区块链记录查询记录着任务A1信息的区块；

区块链记录将记录着HashA1的区块返回给用户端A，用户端A可查看其中的resultA1 encrypted和run\_infoA1 encrypted等信息；

注：用户端A也可以请求同步整个区块链记录到用户端A；

用户端A执行计算任务An (n > 1)时，可省略上述流程1，仅进行23456

流程5完成后，各模块拥有信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 用户端A | 密钥管理器 | 文件接收器 | 代码运行器 | 区块链记录 |
| KRA,  KRS pub，  KA，  File，  HashA1,  resultA1,  run\_infoA1, | KRA pub,  KRS,  KA, |  |  | KRA pub,  HashA1,  resultA1 encrypted,  run\_infoA1 encrypted, |