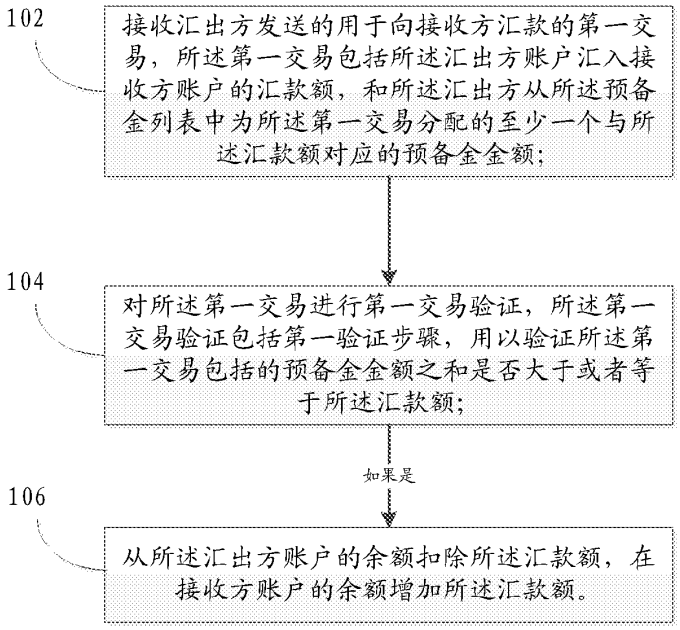
102
接收汇出方发送的用于向接收方汇款的第一交易，所述第一交易包括所述汇出方账户汇入接收方账户的汇款额，和所述汇出方从所述预备金列表中为所述第一交易分配的至少一个与所述汇款额对应的预备金金额；
104
对所述第一交易进行第一交易验证，所述第一交易验证包括第一验证步骤，用以验证所述第一交易包括的预备金金额之和是否大于或者等于所述汇款额；
如果是
106
从所述汇出方账户的余额扣除所述汇款额，在接收方账户的余额增加所述汇款额。

图 1

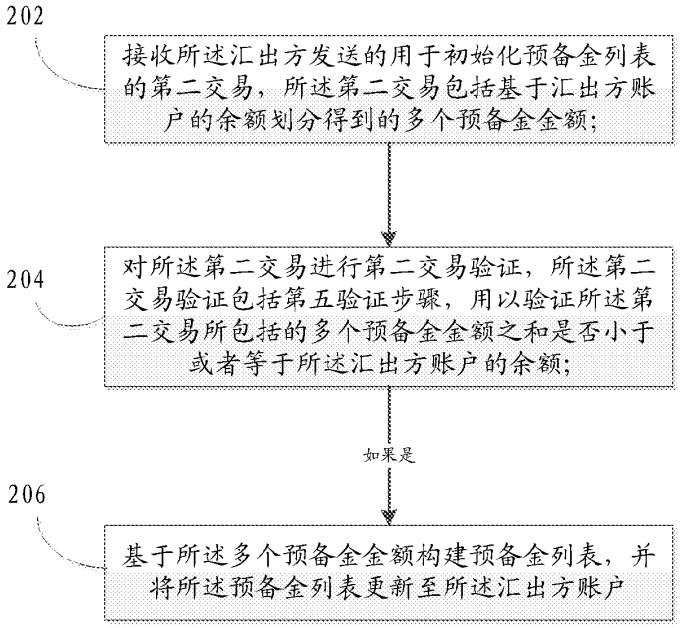
202
接收所述汇出方发送的用于初始化预备金列表的第二交易，所述第二交易包括基于汇出方账户的余额划分得到的多个预备金金额；
204
对所述第二交易进行第二交易验证，所述第二交易验证包括第五验证步骤，用以验证所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方账户的余额；
如果是
206
基于所述多个预备金金额构建预备金列表，并将所述预备金列表更新至所述汇出方账户

图 2

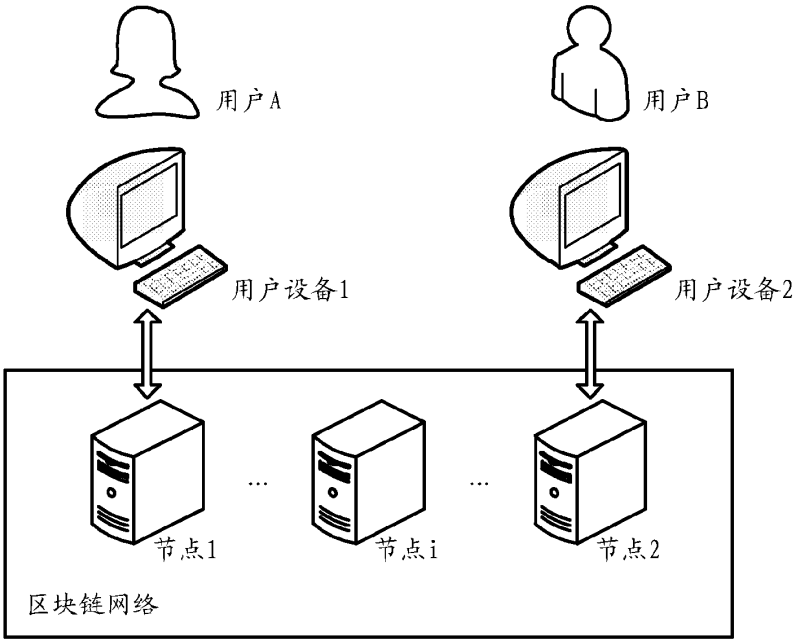

图 3

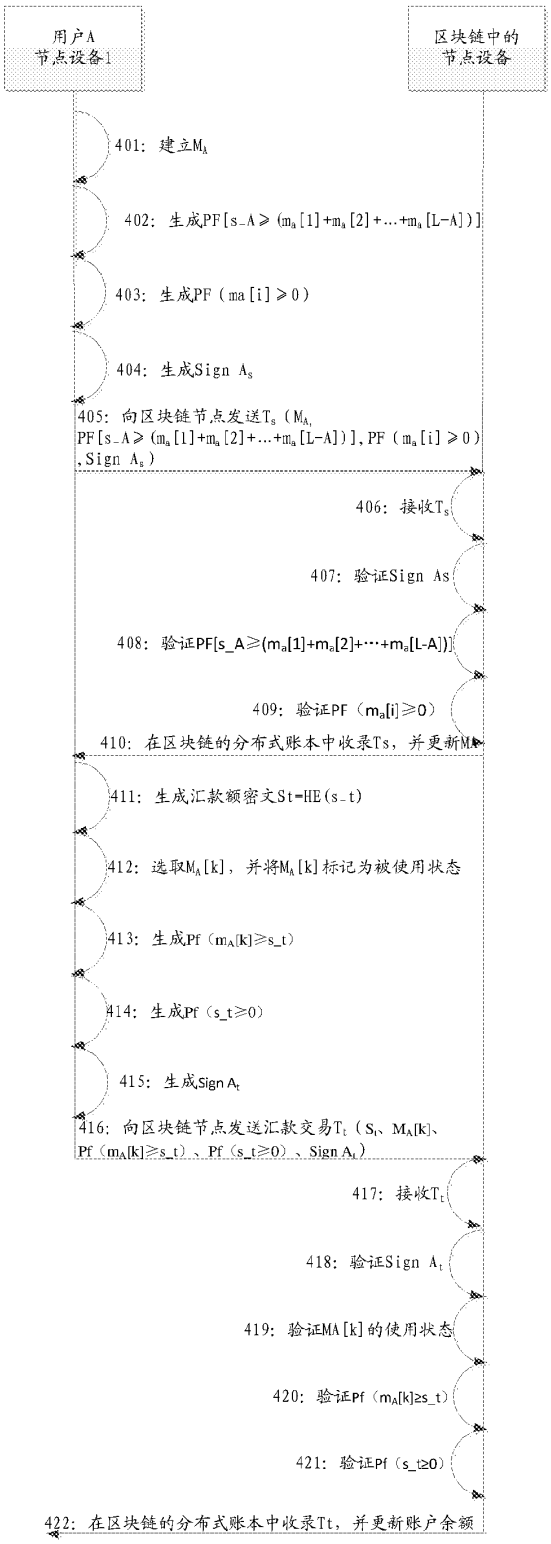
用户A
节点设备1
区块链中的
节点设备
401：建立M_A
402：生成PF[s_A≥(m_a[1]+m_a[2]+…+m_a[L-A])]
403：生成PF（ma[i]≥0）
404：生成Sign A_s
405：向区块链节点发送T_s（M_A，PF[s_A≥(m_a[1]+m_a[2]+…+m_a[L-A])]，PF（m_a[i]≥0）、Sign A_s）
406：接收T_s
407：验证Sign As
408：验证PF[s_A≥(m_a[1]+m_a[2]+…+m_a[L-A])]
409：验证PF（m_a[i]≥0）
410：在区块链的分布式账本中收录Ts，并更新MA
411：生成汇款额密文St=HE(s_t)
412：选取M_A[k]，并将M_A[k]标记为被使用状态
413：生成Pf（m_A[k]≥s_t）
414：生成Pf（s_t≥0）
415：生成Sign A_t
416：向区块链节点发送汇款交易T_t（S_t、M_A[k]、Pf（m_A[k]≥s_t）、Pf（s_t≥0）、Sign A_t）
417：接收T_t
418：验证Sign A_t
419：验证MA[k]的使用状态
420：验证Pf（m_A[k]≥s_t）
421：验证Pf（s_t≥0）
422：在区块链的分布式账本中收录Tt，并更新账户余额

图 4

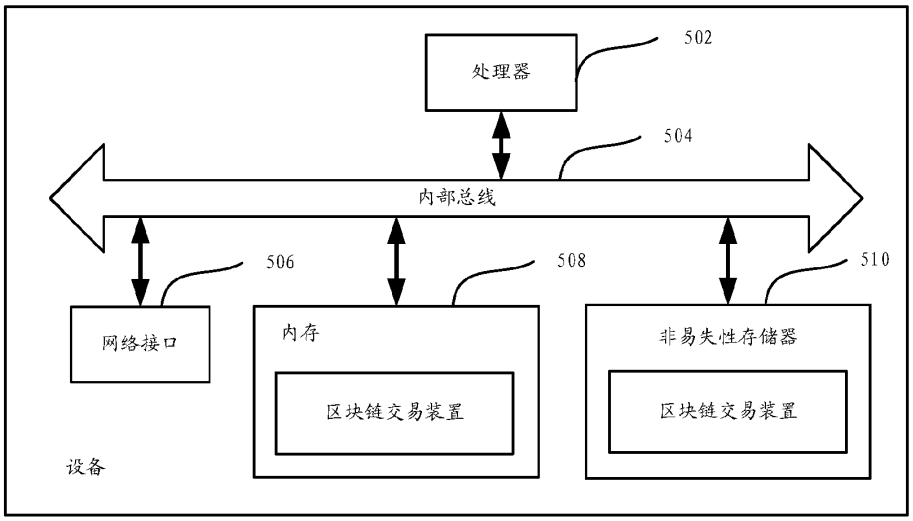
处理器
502
504
内部总线
506
508
510
网络接口
内存
区块链交易装置
非易失性存储器
区块链交易装置
设备

图 5

装置60
接收单元602
第一交易验证单元604
账户更新单元606

图 6