pay=(type, md, aux) stype=dirp, aux=(pr.pe, amb) type=conp, aux=(pxpe,amt,h,time) Itupe=fulp. aux=(cmal, cpay) (Inputj=(payj, balj, ConPayj), 5j) state= (rnd. (Inputj, oflj. F) stater=(r, [Inputri, srijlj, Fr) (梅: O state中,包含的各节点、存款、名条件部门全额与行徒专 之和与理道内总企和相等 ② State中包含加与个条件系计型同时出现在交易双和系 条件针集合中 ③ State中,各节点的轮次都要不大于state的轮叉和环大孩易对方 的轮次, 若轮次相等则两人吃加冬息相同 图对于stater和stater.risr.则对节点疗来说.在stater中的轮次记为 写,在state,中的轮次记为片见《片·竹 Si VizY.

团

在Stater→Stater, Y>Y1日时. 若包含错误签名的节点加收态,可直接课验证。 若包含的都是节点们签名加收态,只1从讲实节点月的负债者。

以1段设施户、对有发送141轮的状态则custodian片播机户的较次化≤1. 假设在state,中包含的轮收为了。在现在,中包含的轮收为分。

节正字更新,则应该电台分,即分=分。

1847年第,则约4岁且珍公水则如相惊 (3)假设引发送了VH轮级长态,则分为两种偏风。包含5不包含。

岩包含则相约认为这名。此时对抗更新后的收益的歧视图象。

如果的研究,那么更新到144轮、电影相同。

如果路 sousia,则形气锅,>v+180米态,以换客减多较的种鱼

体现在余颗上.可能气的缺乏的效力。造成图的,更多是全颗彩造成图 在条件的上,可能气息的图片 cpay six. 造成图.

若不包含.则是心相同.

```
AuditSin(Stater)
if (! Versig () V! Chech Sum () V! Check Conpay () V! Check Round ()).
    return false
the return true.
Versig (Stater).
  parse Stater as (v. [Input; of ]. Fr)
   if =j,!Verify;(Imput;=j), return false.
   else veturn true
CheckSum (Stater)
   parse Stater as (v. [Inputj.ojlj.Fr)
   parse Inputi as (payi, balj, GonPayi)
   if (Frt = (balj + ± = cpay amt, cpay = ConPay;) + total Value)
        return false
   else return true.
 CheckConpay (state,)
    parse Stater as (v. [Input; of ], Fr)
    parse Input; as (payi, balj, GnPay;)
    if = cpay, set Pi = cpay pr. pj := cpay pe . cpay & (ConPay: () ConPay-)
        veturn false.
    else veturn true.
  Check Round (stater)
     parse Stater as (v. (Input; -sjlj. Fr)
     parse Input; as (payi, balj, GnPayi).
     if = pay j, Pi = pay j. other (Pj).
        (payj. rnd > r) V (payj. rnd > r) V (payj. rnd > payj. rnd)
         V [(pay; .vnd == pay; .vonnd) (pay; + pay;)]
         vetum falæ
     else return true.
```

```
Andit Dou (stater, stater), r'zr.
    if [(r=r) ^ (stater+stater)] V [(r=r+1) ^ (stater+ + update (stater))]
       v [(r'>r+1) /[3], (g+g') / (g'=r)], return fale.
    else neturn true
链上的中的判断.
Audit (proof)
parse proof as (stater, on, stater, or,).
for r in sk, [2]
    if ! Versigeus (stater, 50) / (stater # Best State), stater := 1.
     if Versigous (stater, 50) 1!AuditSin (stater), punish ()
if (staten + 1) 1 (state & + 1) 1! Audit Don (staten, staters)
   punish().
```

```
·杭·斜·迢通,发送最新长态。
 Depart (state, \epsilon). from P<sub>j</sub> at T = if DP = \phi, set deadline := T + \Delta.
     DP:=DPU (Pj)
     Record (state, s).
    emit EventDepart (state).
Kecord (stater, 6). at T.
    assert T< dead line.
    Audit (stater, o. Best State. 1)
    if (r> Bast Round), Best State:= stater, Best Round:=r.
Resolve ( ) at T:
    USSEAL DP + $ A T > deadline
    Best State = Update Con (Best State).
    parse BestState as (r, [Inputj, 1], F).
    of (Cose DP) A (Vj. Confoy = 6),
         send balj to Pj
          send F+G to ous.
          emit Event Close
     else for each Pj EDP APj + Cus,
               if balj=0, send halj to Pj.
               P=P\ (P)
              total Value - = balj.
          Best State = (141, SInput, j, I j, Pjen, F).
          Best Round = 171
          DP:=Ø.
          emit Event Resolve (Best State).
```

```
UpdateCon(state). At T:
   parse state as (r, [Input, oj], f).
   parse each coay as (conp, and pr. pe, amt, h, time)
   if (time >T)
       ConPay pr = ConPaypr \scpay }. ConPay pe = ConPaype \ scpay}
       it pm (h, time), balpe += amt.
        else balpr+=amt
   return (r, [Input], I]j. F).
 Punish ( )
     c=(total Value + G)/(1P1-1)
     send $c to parties in Pexcept cus.
     emit Eventclose
```

```
村、各种面通,发送最新长态.
 Depart (state, 6). from Pj at T:
     if DP = \phi, set deadline := T + \Delta.
     DP:=DPU (PJ)
     Record (state, s).
    emit Event Depart (state).
Keard (stater, 5). at T.
    assert T< deadline.
    Audit (stater, o. Best State, L)
    if (r> Bast Round), Best State:= stater, Best Round:=r.
Resolve ( ) at T:
    assert DP + $p 1 T > deadline
    BestState = UpdateCon(BestState).
    parse BestState as (r, sInputj, 1/j, F).
     if (au & DP) A (Vj. Confoy = $),
         send balj to Pj
         send F+G to ous.
          emit EventClose
     else for each P_j \in DP \land P_j \neq CNS,
              if balj=0, send hali to Pj.
              P=P\ \Pj|.
total Value - = balj.
          Best State= (141, [Input, j, 1 j, plen, F).
          Best Round := 171
          DP:= 0.
         emit Event Resolve (Best State).
```

```
UpdateCon(state). At T:
   parse state as (r, [Inputj, oj]j, f).
   parse each coay as (conp, rnd, pr, pe, amt, h, time)
   if (time >T)
       Contay pr = Contay pr \scpay ]. Contay pe = Contay pe \scpay
        if pm(h,time), balpe += amt.
        else balpr+=amt.
   Veturn (r, [Input_j, \perp]_j, f).
 Punish ( )
     c=(total Value + G)/(1P1-1)
     send $c to parties in Pexcept cus.
    emit Eventclose
```

Initialize Best State:=(0, \((\phi, depority.\phi)\pm \]_j, 0) BestRound == 0. P, totalValue = = depositj. Depart() < triggered $Record() \leftarrow triggered, in | | | |$ Resolve() \leftarrow triggered. punish() 一只此内部调用 Updation() 一只红内部调用 Audit() ← thgged 如即何用 Audit Du 把脚调用

pay=(type, rnd, aux) stype=dirp, aux=(pr.pe, amt) type=conp, aux=cpepe,ant, h, time) type=fulp aux=(cmd, cpay) (Input; = (payj, balj, ConPayj), 5;) state=(rnd. [Inputj, 5], F) stater=(r, [Inputrj, sijlj, Fr) 性族: O state中,包含的各节点系数,各条件为时间全额与分类类 之种与强道内总企物相等 ② State中包含的每个条件系付受同时出现在交易双流的 条件村集合中 ③ State中,各节点自5轮次都要不大于State的轮页并且不大致易对方 的轮次,某轮次相等则两人吃加多是相同 ④ 对于state, fo state, risr. 则对节点厅来说.在state中的轮次记为 分, 在states 中的轮次记为时,则(片叶 的)对于27

```
在stater -> stater, r>r+1 时
                                                                                  Blok, AuditSin(Stater)
   艺包含错误签名的节点的状态 可直接被验证
   若回含的都是节点们落名的状态。只从此实节点门的角度看。
                                                                                        if (! Versig () V! Check Sum () V! Check Conpay () V! Check Round ()).
                                                                                       verum false
the return true.
 以1段设节点 Pr 动角发送 Y+1轮割状态 网 custodian 有据的 Pr 68轮次 Yc≤Y.
        假调在的位,中包含的轮收为了。在物也,中包含的轮收为约。
       「若正學更新,则应该电台分,即分二分。
                                                                                        Versig (Stater).
                                                                                          parse Stater as (v. [Input; of 1]. Fr)
        岩不正常,则分子与且片'cr. 即这面相惊
  (1)假设疗发送了VH轮级状态、图1分为两种情况。图65不包含。
                                                                                          if = j,!Verify;(Iqutj-5), return false.
        岩包分则相约认为这名名。此时对方更新后的业态的心块很多。
                                                                                          else veturn true.
            如果抗消灾,那么更新到火料轮、观别相同。
                                                                                        Checksum (stater)
                                                                                          parse Stater as (v. [Input; of 1]. Fr)
           如果吃 sausi 谦,则可能信锅,>v+lps+k态,以换号减实节点的利益
                                                                                           parse Input; as (pay), balj, GnPay;)
             体配在东颗上了举念的铁但这不会影中被实际的转换则与总金配件是自己
                                                                                           if (Frt = (balj + 1 = cpay amb, cpay = Conflag) + total Value)
             在条件村上,可能算为四将 印如湖 违反包
                                                                                               return false
         若不够、网及心相同
                                                                                           else return true
                                                                                         CheckConpay (state,).
           Andit Dou (stater, stater), r'zr.
                                                                                            parse Stater as (v. [Input; oflj. Fr)
             if [(r=r) ^(state,+state,+)] V [(r=r+1) ((state, + Update (state,))]
                                                                                            parse Input; as (payi, balj, GnPay;).
                v[(r'>r+1)^[=j,(15+5')^(15'=r)]], return fale.
             else neturn true
                                                                                            if 3 cpay, set Pi = cpay pr, pj := cpay pe cpay & (ConPay: () ConPay-)
                                                                                               veturn false.
           链上的中的判断
                                                                                            else veturn true
                                                                                          Check Round (stater).
          Audit (proof)
                                                                                             parse Stater as (v. [Input; of lj. Fr)
          parse proof as (stater, on, stater, or,)
                                                                                             parse Input; as (pays, balj, GnPays).
          for r in [ri, ri]
              it!Versigous(stater, 5r) \((stater \neq Best State), stater:=1.
                                                                                             if = pay j, Pi = pay j. other (Pj).
                                                                                               (payj rnd > v) V(payj rnd > v) V(payj rnd > payj rnd)
              of Versigeus (stater, 5v) 1. Audit Sin (stater), punish ()
                                                                                                V [(pay; .vnd == pay; .vonnd) ( (pay; + pay;)]
          if (staten + 1) 1 (state & + 1) 1 ! Audit Dou (staten, staters)
                                                                                                retum falco
             punish ().
                                                                                             else return true.
```