**Selfish mining strategy**

p : relative hashrate of the honest miners

q : relative hashrate of the attacker

**Action**

* Override

i = Nb de block de la Blockchain official

If nb of block on the fork (= j) > i then publish i+1 bock

* Wait

Mine secretly on top of the last block of the fork

* Match : feasible if ( \*)

If the nb of official block =I and nb of block in the fork >= I then publish i blocks

(\*) gama != 0 and honest miners just discovered a new block

Alpha : vitesse de validation des honnêtes mineurs ( initialement to/p )

If gama = 0, state space = N\*2 ={ (i,j) / I E N, j E N }

Start : (i,j)= (0)

End: (i,j)= (0)

(i,j)= (0,0) 🡪 “wait”

(i,j)= (1,0) 🡪 “abandon”

(i,j)= (0,1) 🡪 “wait”

(i,j)= (0,2) 🡪 “wait” ?

(i,j)= (1,1) 🡪 “wait”

(i,j)= (2,1) 🡪 “abandon”

(i,j)= (1,2) 🡪 “override”

J=i+1 🡪 override

j> i+ 1 🡪 wait

Change of state = > reward for the attacker and for the honest miners

Attacker wins i +1 if action = “override”

Instruction

* Input
  + n : nb attack cycles
  + q : relative hashrate
  + gamma : connectivity
* Output
  + M : nb of official blocks mined after n attack cycles
  + R : nb of official blocks mined by the attacker after n attack cycles
  + Tnb of honest blocks mines by the honest miners after n attack cycles
  + average number of official blocks mined during 1 attack cycle
  + average number of official blocks mined by the attacker during 1 attack cycle
  + O : nb of orphan blocks
  + of % orphan blocks
  + nb of difficulty adjustment
  + T : time it has taken to repeat n attack cycles
  + Revenue ration of the miner = (R/T) \* t0
  + Long-term apparent hash rate = R/M
  + t0 = 600 sec