区块链技术研究汇报交流(7)

分布式网络 2

刘鹏 · 2018-05-18

共识机制的基础：网络协议

Reference

Wattenhofer, R., *区块链核心算法解析*. 金融科技丛书. 2017, 北京: 机械工业出版社.

溯源： 如果一个网络中的所有计算机都在维护一个变量，那么如何保证一个客户端发出的修改变量的命令能被所有服务器准确执行?

定义：状态复制(State Replication)，对于一组节点，如果所有节点均已相同顺序执行一个（可能是无限的）命令序列c1, c2, …, 则这组节点实现了状态复制。

Paxos算法

票（Ticket）：一张票是一个弱化形式的锁，具备以下性质

- 可重新发布
- 票可以过期

评价：票概念从操作系统的lock中提出，通过一种类似互斥的方式进行读写，保证一个网络中的某个时刻最多只有一个client在进行命令发布，其他client的命令都没有在这个时刻被执行。

Paxos算法

Paxos

客户端（提案者）	服务器（接收者）
初始化	
c //等待执行的命令	$T_{max} = 0$ //当前已经发布的最大票号
t=0 //当前尝试的票号	C = NULL //当前存储的命令
	$T_{store} = 0$ //用来存储命令C的票
阶段1	
1: t = t + 1	
2: 向所有服务器发消息，请求得到编号为t的票	
	3: if t > T_{max} then
	4: T_{max} = t
	5: 回复：ok(T_{store}, C)
	6: end if
7: 阶段2	
8: if 过半数的服务器回复ok then	
9: 选择T_{store}值最大的(T_{store}, C)	
10: if T_{store} > 0 then	
11: c = C	
12: end if	
向这些回复了ok的服务器发送消息:	
13: propose(t, c)	
end if	
	14: if t = T_{max} then
	15: C = c
	16: T_{store} = t
	17: 回复: success
	18: end if

Paxos算法(续)

Paxos

客户端（提案者） 服务器（接收者）

阶段3

19: if 过半数服务器回复success then
20: 向每个服务器发送消息: execute(c)
21: end if