共识算法

笔记本:	白皮书		
创建时间:	2019/10/9 10:59	**更新时间:**	2019/10/24 9:32
作者:	jyyhermance@163.com		

FLP定理
在允许节点失效的情况下，纯粹异步系统无法在有限时间内，确保一致性的完成。

CAP定理
分布式计算系统不可能同时确保

- 一致性（所有节点同一时刻数据相同
- 可用性（有限时间内所有请求都能得到回应
- 分区容错性（部分分区故障不影响整体运行

因此必然会削弱某个特性，如
弱化一致性：异步更新
弱化可用性：一旦故障拒绝服务（银行取款机
弱化分区容错性

拜占庭容错 ->（节点按程序逻辑执行，但不保证返回时间）崩溃容错 ->（非健忘）遗漏容错 ->（发生故障后停止响应）崩溃停止容错

Paxos算法
适用于无恶意节点
提议人 提议议案人 审核人 执行人
准备阶段 -- 决定对哪个议案进行投票
提交阶段 -- 确认最终结果

Raft算法
在保证可靠性的同时，简化了Paxos
强Leader共识协议
选举决定leader节点（平票进入睡眠，睡眠结束后重新发起选举），leader节点被定期检测，一旦失效重选。任何写入都经过leader，超过半数节点执行后，leader向上响应。

PBFT算法
容忍小于1/3的节点背叛，非常适合联盟链，但不适用于公有链
pre-prepare prepared committed

PoW（proof of work)
节点自由进出，完全去中心化

1. 向所有节点广播新交易
2. 每个节点把收到的交易放进区块中
3. 每一轮中，一个被随机选中的节点，广播它保留的区块
4. 其他节点验证块中所有交易，无误则接收该区块
5. 其他节点将该区块的哈希值放入下一个它们创建的区块中，表示承认这个区块的正确性

不利原理：付出很大的代价，以向想合作的另一方表达善意

PoS（proof of stake)

参与者预先放一些代币在区块链上，获得对应的利息

1. 持币人成为验证者（validator
2. 根据持币多少，挑选一个验证者给予生成新区块的权利
3. 一定时间内没有成功，就挑选下一个验证者
4. 依此类推，以最长链为准

DPoS（delegated proof of stake)

委托权益人（即，见证人witness）机制，信任少量的诚信节点，提升交易速度和容量

见证人代表权益所有人签署和广播区块链
见证人获取一定的报酬
见证人必须尽量在线，错过一次区块签名活动就会被踢出
权益所有人不喜欢见证人可以卖出权益退场