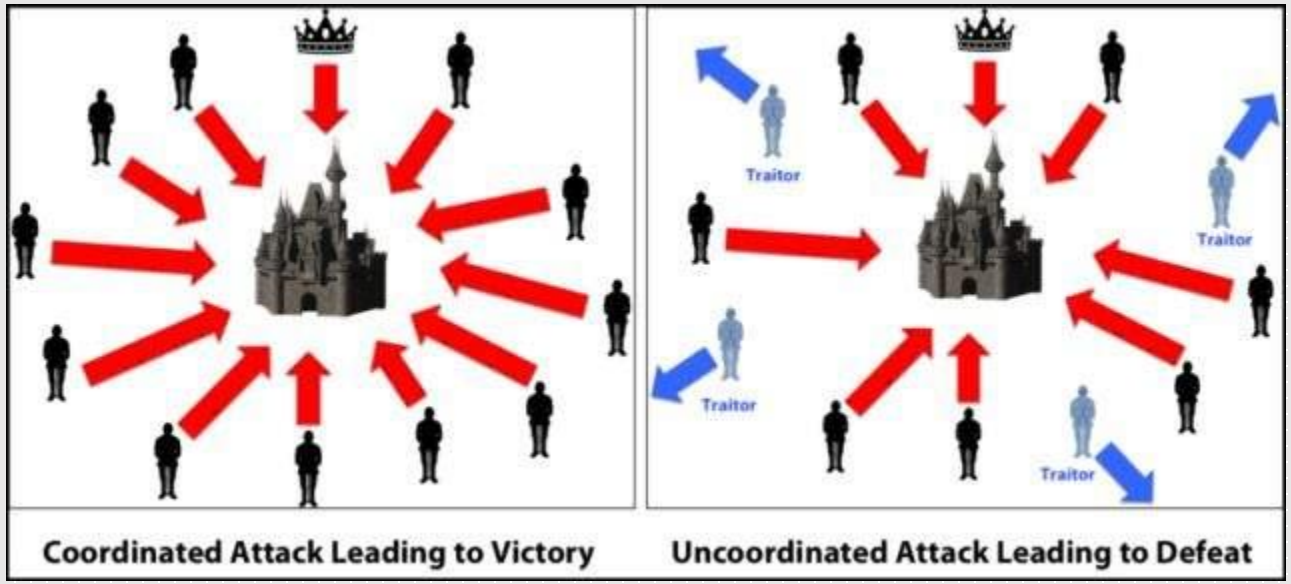
3.5 拜占庭将军问题

01 故事背景

拜占庭是曾经的东罗马帝国的首都。当时的拜占庭罗马帝国国土辽阔，所以用于防御和保卫国家的军队们都被分散安排在各处，军队与军队之间分隔很远，每支队伍的将军之间只能靠信差来传递消息。

在这个背景下，战争爆发了。拜占庭帝国所有军队的将军们为了帝国的利益，必须达成一致的共识，决定是否要去攻打某一支敌军。

02 拜占庭将军问题



但是，因为将军们在地理上是分散的，而且在军队内有可能存有叛徒和敌军的间谍，他们的活动会左右将军们的决定，扰乱整体军队的秩序。这些客观因素的存在可能会导致在进行共识时，结果并不代表大多数人的意见。那么在已知有成员谋反的情况下，其余忠诚的将军如何不受叛徒的影响达成一致的协议，就是拜占庭将军问题要讨论的重点。

03 拜占庭将军问题

拜占庭将军问题就是讨论，在可能出现消息丢失和错误的不可靠信道上，如何通过消息传递的方式达到一致性，且最后的共识应当是可靠的。

拜占庭问题出现的前提和背景：

- 将军们在地理上的分散；
- 叛徒的存在。

04 拜占庭将军问题与区块链

拜占庭将军问题		区块链
分散的军队	→	分布式数据库，节点具有分散性
达成攻打某一支敌军的共识	→	节点要达成共识
存在叛徒	→	存在恶意节点
寻求在有叛徒存在的情况下，仍然能够达成一致性的方法。	→	在有恶意节点存在的情况下，达成节点间的一致，并使得最终的结果是可靠的。

05 叛徒对共识的影响

- 叛徒可以通过某些方式欺骗忠诚的将军，使他们采取进攻行动；
- 促成一个不是所有将军都同意的决定，如当将军们不希望进攻时促成进攻行动
- 迷惑某些忠诚的将军，使他们无法做出决定

如果叛徒达到了这些目的之一，使得总数超过半数的将军违背了本来的决策结果，这样最终的结果就会和本来共识结果相反，这样任何攻击行动的结果都是注定要失败的。

06 如何解决拜占庭将军问题

- 第一，要让所有忠诚的接受命令的将军接收相同的命令。在区块链系统中，就是要使得恶意结点的错误消息不会被区块链其他结点所接收；
- 第二是要实现“如果发送命令的将军是忠诚的，那么所有忠诚的接收命令的将军遵守所接收的命令”。在区块链中，如果消息发布者发布的区块是合法的，那么其他所有结点都会把它加入到自己本地的区块链中。

只选择“忠诚的将军”作为发布者以及保证恶意发布者发布的消息不会被接受。

07 解决方法

- PoW算法：它要求节点完成一定的工作量才有可能得到发布区块的权利，这也就是提高了恶意节点造假的成本——它必须做第一个完成证明的节点，而这需要很高的算力，一旦没有成功，就是白白消耗算力。
- PBFT算法：实用拜占庭容错算法。