拜占庭故障是LeslieLambert提出的点对点通信中的基本问题。这意味着在有消息丢失的不可靠信道上试图通过消息传递来实现一致性是不可能的。

拜占庭位于土耳其伊斯坦布尔，是东罗马帝国的首都。由于当时拜占庭罗马帝国疆域辽阔，为了达到防御的目的，各军相隔甚远，将军只能通过信使传递消息。在战争时期拜占庭军队中所有的将军和副官都必须达成共识，在攻击敌人之前决定是否有胜算&#039；s营。但军中可能有汉奸、敌特，将军们的决策会扰乱全军的秩序。在达成共识的过程中，结果不代表大多数人的意见。这时，拜占庭的问题就形成了，在已知成员反叛的情况下，其他忠诚的将军如何在不受叛徒影响的情况下达成协议。

拜占庭一般问题是协议问题。拜占庭帝国军队的将军们必须一致决定是否攻击敌人。问题是这些将军地理位置分散，其中有叛徒。。汉奸可以随意行动，以达到以下目的：欺骗一些将领采取进攻行动；促成并非所有将军都同意的决定，例如在将军们不想进攻时促成进攻；或者迷惑一些将军，这样他们就可以&#039；不要做决定。如果叛徒达到了其中一个目标，，任何攻击的结果都是注定要失败的，只有达成完整协议的努力才能取得胜利。

拜占庭假设是现实世界的模型。由于硬件错误、网络拥塞或断开以及恶意攻击，，计算机和网络可能会出现不可预测的行为。

区块链轻松解决了这个问题。它增加了信息传输的成本，降低了信息传输的速率，增加了一个随机元素，使得某个时刻只有一个将军可以广播信息。。这里所说的成本是&quot工作量证明&quot基于随机哈希算法的区块链系统。哈希算法所做的是计算输入，得到一串64位的随机数和字母。

区块链系统计算的输入数据是指节点发送的当前时点的全部总账。目前，计算机的计算能力能够实时计算单个哈希值，但区块链系统只接受前13个字符为0的哈希值作为&quot工作量证明&quot。前13个字符为0的哈希值非常罕见，整个网络要花10分钟才能在数以亿计的数据中找到一个。在计算出一个有效的哈希值之前，网络中已经产生了无数的无效值这是&quot工作量证明&quot降低信息传输速率，使整个系统顺利运行。

拜占庭将军问题中，第一个广播信息的将军是第一台找到有效哈希值的计算机。只要其他将军收到并验证了这个有效的哈希值和附加到它的信息，他们就只能用新信息更新他们的总帐副本，然后重新计算哈希值。。下一个计算有效哈希值的将军可以把他的更新信息附加到有效哈希值上，广播给大家。然后哈希计算大赛从新的起点开始。由于网络信息的不断同步，网络上的所有计算机都使用相同版本的总账。

比特币区块链系统找到有效哈希值的时间间隔是10分钟，由算法设定。算法难度每两周调整一次，保证间隔10分钟，不多不少。每10分钟一次。总账信息将在区块链更新，并在全网同步一次。因此，分散的交易记录在所有网络上的计算机之间进行协调和同步。

&quot；拜占庭一般问题&quot可以进一步扩展到各个领域。当人们在网上交易数据时。，总是习惯性的依赖强大的第三方平台进行信任保障。但是，这些第三方解决人&#039；的信任问题逐渐失效，因为总有黑客可以抓住第三方平台的漏洞进行金融诈骗。。&quot叛徒&quot在&quot拜占庭一般问题&quot是&quot骗子&quot在互联网金融交易中。如果第三方平台有很大的漏洞，或者为了避免太多的步骤而去掉了第三方信托机构，那么&quot叛徒&quot将使用信息来&quot作弊&quot没有第三方信托机构的担保。。而不用花费大量的时间和资源去发现这个&quot叛徒&quot，使交易双方互相信任，进行正常交易的方法就是区块链。

当个人用户在区块链系统中发起交易时，他们将使用私钥和公钥对交易进行签名。嵌入在比特币系统中的标准公钥扮演着加密工具的角色。与拜占庭一般问题相对应，加密工具是用于签名和验证消息的印章。

因此，哈希算法对信息传输速率和加密工具的限制，使得区块链成为一个没有信任的数据交互系统。在区块链上，一系列交易、时间约定、域名记录、政治投票系统或任何其它需要建立分布式协议的地方。参与者可以达成一致。

互联网中的拜占庭一般问题是指在信道传输的过程中，某些节点可能会因为工作量过大或者某些恶意攻击而难以实现信息同步。在1999年，米格尔卡斯特罗(Miguel Castro)和芭芭拉利斯科夫(BarbaraLiskov)提出了拜占庭容错算法，认为如果系统中有三分之二的节点正常工作，就可以保证系统的一致性和正确性。。后来，中本聪提出了比特币的工作量证明机制和非对称加密算法，为拜占庭一般问题提供了新的解决方案。

拜占庭容错算法假设有n个将军和t个叛徒。当n=3，t=1时。这个时候，甲、乙、丙中有一个是汉奸。如果A下达了进攻的命令，但是叛徒B让C撤退，那么C就无法做出判断；如果叛徒B发出一个&quot攻击&quot命令发送给A和一个&quot撤退&quot此时，C、A和C的命令将不一致。因此，当叛徒的数量大于或等于1/3时，拜占庭问题就无法解决。同样，假设网络节点总数为n，恶意节点数为t，只有当Ngt=3T1，即当网络中正常节点数至少为(2/3)N时，问题就可以解决了。，从而保证信息的一致性。在网络通信可靠的情况下，拜占庭容错算法可以在一定程度上解决节点故障问题，使系统达成共识。

工作负载证明(PoW)机制假设一般A首先发出&quot攻击&quot命令并附上自己的

签名。如果其他将军接到后打算进攻，就听从A将军的指挥和自己的签名。如果A给出了&quot攻击&quot但是&#039；t执行，其他将领可以判断A为汉奸，并以此来辨别信息的对错。以同样的方式；以类似的方式，多个参与节点会通过一系列工作得到一个结果，第一个得到结果的节点会广播全网。如果结果正确，其他节点会将结果添加到自己的账簿中，以便为下一笔交易做准备。。黑客要破坏网络安全或发布虚假区块，必须有51%以上的计算能力，代价远远大于收益。因此，使用该机制可以减少错误信息的可能性，并使系统更快地达成共识。

非对称加密算法非对称加密算法的加密和解密需要两个不同的密钥，——公钥和私钥，一般成对出现。如果A要给B发消息，A需要用B&#039加密消息；s的公钥，B需要用自己的私钥解密消息。。如果B想表明身份，可以写a&quot签名文本&quot用他的私人密钥广播出去。其他人可以根据B&#039验证他的身份；的公钥。由于身份和签名是不可伪造的，非对称加密算法保证了传输过程的私密性和签名不完全可信的问题。