今天，我刷卡买了一杯爽口的抹茶拿铁。刷完卡，店家很笃定地为我做了这杯饮料。商户确信这笔交易已经成功了，钱不会再原路返回到我的卡上，而是妥妥地进入他们的户头。换句话说，购买已经终结。不过实际上，信用卡的交易非常复杂，信用卡交易需要在60天时才能最终完成，小额交易商家还可以接受刷卡消费，但大额交易，更愿意接受支票或电汇。只有现金交易可即时实现「终结」。在区块链的场景中，终结性「finality」是指一旦提交到区块链，所有格式正确的区块都不会被撤销。当用户进行交易时，他们希望一旦其交易通过，交易就不会被任意更改或回滚。因此，在设计区块链共识协议时，终结性就显得至关重要。区块被撤销可能会带来数百万美元的损失，或者对去中心化应用程序中的基本操作造成影响。因此，理解终结性对于构建稳健的区块链平台、选择在何种平台之上开发应用程序至关重要。在目前基于中本聪共识的系统中，51%攻击和私下进行的采矿行为有可能允许区块被撤销，从而威胁到系统的健康。例如，如果一个恶意行动者能够积累51%的采矿力量，他可以进行双花攻击。有些协议提供了概率上的「终结性」，而其他协议则可以保证绝对的「终结性」。对「终结性」进行分类「概率上的终结性」是指，基于区块链的协议提供的终结性，比特币的中本聪共识就属于此类。在这种情况下，包含交易的区块在链中下沉越深，交易不被回滚的概率就越大。区块越深，包含该区块的分叉越可能是最长的链条。这就是为什么在比特币区块链上，我们会建议等到一个交易获得六个区块确认时再确定其真实性，也就是说，等上大约一个小时的时间再完成交易，这样就能确保交易被回滚的可能性非常低了。「绝对终结性」是指基于实用拜占庭容错PBFT的协议提供的终结性，Tendermint是其中的代表。在这种情况下，交易一旦包含在区块中并添加到区块链上，就会立即被认为已经最终完成。在这种情况下，领先者将提出一个区块，而验证委员会需要在批准这个区块方面达成多数一致。还有一种「经济终结性」的概念，在这种概念中，一个区块的回滚成本会非常高昂。在使用削减机制比如Casper FFG和Tendermint的权益证明PoS系统中，如果一个股权持有人在两个区块上双重标记，他们的整个股权都可能被削减，也要是说，他们要为损害终结性付出极其昂贵的代价。例如，如果一个网络上有100个股权持有人，每个人都已经投入了100万美元，那么现有的股份总额就是1亿美元。如果在同一高度提出了两个区块，比如B和B'，66%的股权持有人投票给B 6600万美元，66%的人投给B'6600万美元，那么至少33%的股权持有人存有恶意，而这意味着损失至少为3300万美元。

CAP定理和终结性虽然看起来绝对终结性比概率上的终结性更可取，但是在进行挑选时，仍然存在一些基本的权衡。在考虑概率和基于拜占庭容错BFT的终结性之间进行权衡时，使用Eric Brewer的「CAP定理」很有用。CAP定理指出，在分区的情况下，分布式系统只能要么保留一致性，要么保留可用性。保留一致性的系统宁可中止，也不会允许不准确的交易通过。而保留可用性的系统会允许不准确的交易通过，自身也会继续存在。偏好一致性的系统提供拜占庭容错终结性，而偏好可用性的系统提供概率上的终结性。在进行支付时，用户经常会选择概率上终结性的协议，这就是为什么许多基于有向无环图DAG、支持可用性，而非一致性的协议，会把重点放在支持支付上。然而，许多区块链平台提供的不仅仅是支付功能，还包括由智能合约支持的DApp。不同的DApp在最终性方面可能有不同的偏好：那些需要可用性的DApp，如果交易在哪怕并不准确时也总是能够通过，会更偏好概率上终结性的方式；倾向于一致性的DApp，在出现不准确的交易时整个应用程序为之中止，这也是可取的，这种应用会更偏好绝对终结性的方式。所以说，终结性从根本上影响用户体验。PoS共识中的终结性以下是我们对一些主要的PoS平台进行的分析；TendermintTendermint实现了绝对终结性。任何在预投票或预提交中得到2/3以上票数的区块都可实现即时终结。这一过程持续进行下去，直到达1/3或以上的验证人不再做出积极反应，在这种情况下网络会暂时中断，由此可见，Tendermint对一致性的青睐要超过了可用性。在对Tendermint应用PoS削减规则时，该协议也实现了经济终结性。ThunderellaThunderella的快速路径提供了绝对终结性。任何获得公证的最大交易序列都可以被视为经过确认的输出。如果大于3/4的快捷路径委员会成员诚实且在线，申请人也是诚实的，那么有效交易可即时确认。然而，快速路径确认不同于整体的终结性，它是一种理想条件下的终结性。交易一旦被记录在基础区块链上，就会完全确认，这既可以架设在链上，也可以基于BFT算法。Thunderella在快速路径失败的情况下会推到基础区块链，由此可见，它优先考虑可用性。Algorand只要攻击者控制该协议的货币价值不足总价值的1/3，Algorand就可以保证分叉的概率可以忽略不计，从而允许协议以强同步方式运行，使得每个区块达成最终协议。在弱同步中，Algorand可能会分叉，但要使用拜占庭协议BA\*来协商选择哪个分叉。这样一来，当协议恢复到强同步时，Algorand中的交易会最终确定。Algorand优先考虑一致性而非可用性，在不能接受候选区块时，宁愿选择生成空区块。Ouroboros GenesisGenesis可以根据其区块链的选择规则，实现概率上的终结。这个规则为对于短程最多k个区块，其中k是安全参数，遵循最长链；对于长程超过k个区块用充分性规则plenitude rule，意味着在当前链分叉后即时查看时间段，并选择更高密度的链。Casper FFGCasper FFG旨在为基于区块链的系统提供绝对/经济上的终结性，在委员会按股权加权获得了2/3以上绝对多数，即可签署区块。Casper FFG使用这种构建方式，即使攻击者控制了底层区块链的提案机制，出现冲突的检查点也不可能最终完成。但是，由于FFG提供了安全性，而提案机制提供了活跃度，因此对手可以拖延共识来阻止Casper最终完成未来的检查点。FFG优先考虑一致性，因为它不允许在未获超过2/3的验证者同意的情况下完成检查点。FFG还允许通过削减机制实现经济上的终结。

Casper TFGCasper TFG通过具有不同容错阈值的验证者，实现绝对终结。也就是说，其协议是异步安全的拜占庭容错，允许验证者具有不同的容错阈值。