原网站：<https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6>

共识机制[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6&action=edit&section=0&summary=/*%20top%20*/%20)]

维基百科，自由的百科全书

[跳到导航](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#mw-head)[跳到搜索](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#p-search)

**共识机制**（consensus），常见于[区块链](https://zh.wikipedia.org/wiki/%E5%8C%BA%E5%9D%97%E9%93%BE" \o "区块链)领域，即达成共识的机制。

**目录**

* [1产生背景](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#%E4%BA%A7%E7%94%9F%E8%83%8C%E6%99%AF)
* [2常见的共识机制](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#%E5%B8%B8%E8%A6%8B%E7%9A%84%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6)
* [3参考](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#%E5%8F%82%E8%80%83)
* [4延伸阅读](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#%E5%BB%B6%E4%BC%B8%E9%96%B1%E8%AE%80)
* [5参阅](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#%E5%8F%83%E9%96%B1)

产生背景[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6&action=edit&section=1)]

由于[加密货币](https://zh.wikipedia.org/wiki/%E5%8A%A0%E5%AF%86%E8%B2%A8%E5%B9%A3" \o "加密货币)多数采用[去中心化](https://zh.wikipedia.org/wiki/%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96" \o "去中心化)的[区块链](https://zh.wikipedia.org/wiki/%E5%8C%BA%E5%9D%97%E9%93%BE" \o "区块链)设计，节点是各处分散且平行的，所以必须设计一套制度，来维护系统的运作顺序与公平性，统一区块链的版本，并[奖励](https://zh.wikipedia.org/wiki/%E7%8D%8E%E5%8B%B5" \o "奖励)提供资源维护区块链的使用者，以及惩罚恶意的危害者。这样的制度，必须依赖某种方式来证明，是由谁取得了一个区块链的打包权（或称记账权），并且可以获取打包这一个区块的奖励；又或者是谁意图进行危害，就会获得一定的惩罚，这就是共识机制。[[1]](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6" \l "cite_note-1)

常见的共识机制[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6&action=edit&section=2)]

* [工作量证明](https://zh.wikipedia.org/wiki/%E5%B7%A5%E4%BD%9C%E9%87%8F%E8%AD%89%E6%98%8E)（Proof-of-Work，PoW），典型案例：比特币网络
* [权益证明](https://zh.wikipedia.org/wiki/%E6%AC%8A%E7%9B%8A%E8%AD%89%E6%98%8E)（Proof-of-Stake，PoS，又译持有量证明），典型案例：以太坊
* 股份授权证明（Delegated-Proof-of-Stake，DPoS），典型案例：EOS
* 容量证明（Proof-of-space，PoSpace，又称 Proof-of-Capacity，PoC）典型案例：[Filecoin](https://zh.wikipedia.org/wiki/Filecoin" \o "Filecoin)
* Paxos
* RAFT
* PBFT
* LibraBFT（Byzantine fault-tolerance）：Libra上使用。

参考[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6&action=edit&section=3)]

* 1. [**^**](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6#cite_ref-1) [区块链简介与技术探讨](https://ictjournal.itri.org.tw/Content/Messagess/contents.aspx?&MmmID=654304432061644411&MSID=744257557510131250).

延伸阅读[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6&action=edit&section=4)]

* Herlihy, M.; Shavit, N. The topological structure of asynchronous computability. Journal of the ACM. 1999, **46** (6): 858. [doi:10.1145/331524.331529](https://dx.doi.org/10.1145%2F331524.331529). 已忽略未知参数|citeseerx= ([帮助](https://zh.wikipedia.org/wiki/Help:%E5%BC%95%E6%96%87%E6%A0%BC%E5%BC%8F1%E9%94%99%E8%AF%AF#parameter_ignored))
* Saks, M.; Zaharoglou, F. Wait-Free k-Set Agreement is Impossible: The Topology of Public Knowledge. [SIAM Journal on Computing](https://zh.wikipedia.org/w/index.php?title=SIAM_Journal_on_Computing&action=edit&redlink=1). 2000, **29** (5): 1449–1483. [doi:10.1137/S0097539796307698](https://dx.doi.org/10.1137%2FS0097539796307698).

参阅[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E8%AD%98%E6%A9%9F%E5%88%B6&action=edit&section=5)]

* [加密货币](https://zh.wikipedia.org/wiki/%E5%8A%A0%E5%AF%86%E8%B2%A8%E5%B9%A3)
* [区块链](https://zh.wikipedia.org/wiki/%E5%8C%BA%E5%9D%97%E9%93%BE)
* [加密电子货币列表](https://zh.wikipedia.org/wiki/%E5%8A%A0%E5%AF%86%E9%9B%BB%E5%AD%90%E8%B2%A8%E5%B9%A3%E5%88%97%E8%A1%A8)
* [共识动力学](https://zh.wikipedia.org/wiki/%E5%85%B1%E8%AD%98%E5%8B%95%E5%8A%9B%E5%AD%B8)
* [智能合约](https://zh.wikipedia.org/wiki/%E6%99%BA%E8%83%BD%E5%90%88%E7%BA%A6)