



## پروتکل اجماع: همبستگی و توافق در شبکه‌های توزیع شده

## فهرست

|   |   |
|---|---|
| 3 | تعریف کلی از پروتکل اجماع.....                      |
| 3 | اهمیت پروتکل اجماع در بلاک چین.....                 |
| 4 | نحوه استفاده از پروتکل اجماع با یک مثال ساده.....   |
| 4 | مزایای استفاده از پروتکل اجماع در شبکه بلاکچین..... |
| 5 | نتیجه گیری  |

یکی از مهم‌ترین ویژگی‌های شبکه‌های بلاکچین و سایر دفاتر توزیع شده؛ غیر متمرکز بودن است. در واقع غیر متمرکز بودن این شبکه‌ها بدین معناست که تمامی اطلاعات روی سرور اصلی ذخیره و پردازش نشده و بر روی چندین رایانه گوناگون ذخیره می‌شود. به سرورهایی که مسئول نگهداری و حفظ داده‌ها هستند نود یا گره گفته می‌شود. از طرفی اصلی‌ترین دلیل استفاده از دفاتر کل توزیع شده مثل بلاکچین، بالا بردن سطح امنیت و اطمینان از عدم نابودی و خرابی دیتاها است. در واقع اگر اطلاعاتی که بر روی یکی از گره‌ها قرار دارند به دلایل مختلف خراب شوند یا از بین روند، بی‌شمار گره دیگر وجود دارد که اطلاعات را در خود ذخیره کرده‌اند.

اما در زمان استفاده از بلاکچین یا انواع دیگر دفاتر کل توزیع شده، یک موضوع بسیار حیاتی وجود دارد آن هم این است که داده‌ها دائماً به روز رسانی می‌شوند، این به روز رسانی باید بر روی تمام گره‌ها یا سرورها انجام شود که برای انجام این کار از مکانیزم یا الگوریتمی به نام پروتکل اجماع استفاده می‌کنند.

## تعریف کلی از پروتکل اجماع

الگوریتم اجماع به یک قرارداد یا سازوکار مشخصی اطلاق می‌شود که در فناوری بلاکچین و شبکه‌های مبتنی بر آن استفاده می‌شود. هدف اصلی الگوریتم اجماع، به دست آوردن یک توافق مشترک بین اعضای شبکه در مورد صحت و اعتبار تراکنش‌ها و ترتیب آن‌ها است.

در شبکه‌های بلاکچین، اعضای شبکه (معمولاً نودها) با همکاری و تعامل با یکدیگر، توافقی بر سر اعتبار یک تراکنش یا بلاک را برقرار می‌کنند. بدون وجود پروتکل اجماع، امکان تغییر و تزریق تراکنش‌های نادرست وجود دارد و اعتماد به صحت و اعتبار شبکه بلاکچین کاهش می‌یابد.

## اهمیت پروتکل اجماع در بلاک چین

اهمیت الگوریتم اجماع در بلاکچین این است که به شبکه اعتماد و امنیت می‌بخشد و موجب می‌شود تا تراکنش‌ها با صحت و قطعیت بالا در شبکه ثبت شوند. هر الگوریتم اجماعی ویژگی‌ها و مزایا و معایب خاص خود را دارد و بسته به نوع استفاده و محیط بکارگیری، انتخاب می‌شود.

مهم‌ترین پروتکل‌های اجماع در بلاکچین عبارتند از:

1. Proof of Work (PoW): این پروتکل توسط بیت کوین و بسیاری از سایر ارزهای دیجیتال استفاده می‌شود. در این پروتکل، ماینرها باید مسئله‌ای پیچیده را حل کنند تا بتوانند بلاک جدید را تولید و اعتبار تراکنش‌ها را تایید کنند.
2. Proof of Stake (PoS): در این پروتکل، نودها بر اساس میزان سرمایه‌ای که در شبکه قرار دارند، اجازه تولید بلاک و تایید تراکنش‌ها را دارند. این پروتکل از منابع کم‌تری نسبت به PoW استفاده می‌کند.
3. Delegated Proof of Stake (DPoS): در این پروتکل، حامیان انتخاب می‌شوند تا به نمایندگی از تمام نودهای شبکه، عملیات تولید بلاک و اجماع را انجام دهند. این پروتکل در برخی شبکه‌های بلاکچینی مانند EOS استفاده می‌شود.

## نحوه استفاده از پروتکل اجماع با یک مثال ساده

برای مثال در یک شرکت اگر کارمندان بر سر یک موضوع نظرهای متفاوتی داشته باشند، در نهایت مدیر شرکت تصمیم نهایی را می‌گیرد. در بلاک چین با کمک الگوریتم اجماع، به توافق رسیدن بین نودها از طریق یک سیستم رای گیری صورت می‌گیرد. به این صورت که اگر یک کاربر تراکنشی را به شبکه ارسال کند. اطلاعات ارسال شده توسط گره‌ها بررسی می‌شود. اگر با توجه به اطلاعات قبلی، تراکنش فرستاده شده صحت داشته باشد، گره یک تاییدیه مبنی بر صحت آن به شبکه ارسال می‌کند. مجموعه‌ای از تراکنش‌ها یک بلاک را تشکیل می‌دهند. در نهایت اگر بیش از نیمی از نودها، اضافه شدن بلاک مورد نظر را به بلاک چین تایید کند، نودها بلاک جدید را به سیستم خود اضافه می‌کنند و در آخر تراکنش‌ها موفق و نهایی می‌شوند.

## مزایای استفاده از پروتکل اجماع در شبکه بلاکچین

استفاده از الگوریتم اجماع در شبکه بلاکچین، که به عنوان یک مکانیزم اساسی برای حل مسئله هماهنگی و توافق در شبکه بلاکچین استفاده می‌شود، مزایای بسیاری دارد. در زیر تعدادی از مزایای استفاده از الگوریتم اجماع در شبکه بلاکچین آورده شده است:

### امنیت

الگوریتم اجماع به عنوان یک مکانیزم اصلی برای تضمین امنیت شبکه بلاکچین عمل می‌کند. با استفاده از این الگوریتم، تمامی شرکت کنندگان در شبکه بلاکچین برای رسیدن به توافق در مورد وضعیت بلاک‌ها و تراکنش‌ها همکاری می‌کنند. این توافق باعث ایجاد یک مجموعه بلاک‌های متفق بین تمامی شرکت کنندگان می‌شود و هر تغییر غیرمجاز در یک بلاک نیاز به تغییر تمامی بلاک‌های بعدی دارد. این ویژگی امنیت بالایی را در برابر تغییرات تاریخچه شبکه بلاکچین فراهم می‌کند.

### توافق

پروتکل اجماع به شرکت کنندگان در شبکه بلاکچین کمک می‌کند تا در مورد تراکنش‌ها و وضعیت بلاک‌ها توافق برسانند. که بدین معناست همه اعضای شبکه به یک توافق مشترک درباره حالت فعلی بلاکچین می‌رسند. این ویژگی توافق در شبکه بلاکچین امکان انجام تراکنش‌ها میان اعضا را فراهم می‌کند و از وجود متناقضات در سیستم جلوگیری می‌کند.

### ضمانت اعتبار

الگوریتم اجماع در شبکه بلاکچین به طور کلی برای تضمین اعتبار تراکنش‌ها و بلاک‌ها استفاده می‌شود. با استفاده از الگوریتم اجماع، تمامی شرکت کنندگان قادر خواهند بود تغییراتی که به بلاک‌ها یا تراکنش‌ها اعمال می‌شود را تایید یا رد کنند. این ویژگی به شرکت کنندگان اعتماد بیشتری به سیستم بلاکچین می‌دهد.

### انحصار داده

با استفاده از پروتکل اجماع، همه شرکت کنندگان در شبکه بلاکچین به یک توافق درباره وضعیت داده‌ها می‌رسند. این به بدین معناست که تمامی شرکت کنندگان اطلاعاتی که در شبکه ذخیره می‌شوند را مشاهده می‌کنند و هیچ شخصیت یا سازمانی قادر به ایجاد تغییرات غیر مجاز در داده‌ها نیست. این مزیت، انحصار داده‌ها را در برابر دستکاری و سرقت اطلاعات تضمین می‌کند.

## غیرتمرکزی

الگوریتم اجماع در شبکه بلاکچین برای تصمیم‌گیری همگانی بین شرکت کنندگان استفاده می‌شود. این به معنای این است که تصمیم‌گیری در شبکه بر اساس یک رویکرد غیرمرکزی صورت می‌گیرد و هیچ سازمان مرکزی یا نهادی قدرت کنترل بر سیستم را ندارد. این ویژگی غیرمرکزی باعث افزایش اعتماد به سیستم بلاکچین و جلوگیری از احتمال تعطیلی یا کنترل شبکه توسط یک شخص یا سازمان خاص می‌شود.

به طور کلی، استفاده از الگوریتم اجماع در شبکه بلاکچین منجر به ایجاد امنیت، توافق، ضمانت اعتبار، انحصار داده و غیرتمرکزی می‌شود. این مزایا باعث افزایش کارایی و اعتماد به شبکه بلاکچین می‌شود و در نتیجه منجر به کاربردهای گسترده‌تر و موثرتری می‌شود.

## نتیجه‌گیری

اجماع فرآیندی است که طی آن گروهی از نودها (تصمیم‌گیرندگان) در یک شبکه تعیین می‌کنند که کدام تراکنش‌ها در یک شبکه بلاکچین معتبر هستند و کدام یک از آن‌ها احتمال معتبر نیستند. به بیانی دیگر پروتکل اجماع شیوه برای دستیابی به توافق هستند. مجموعه قوانینی که از قبل در یک بلاکچین تعریف شده و طبق الگوریتم‌های اجماع، تایید می‌شود، از شبکه در مقابل رفتارهای مخرب و حملات هکرها مراقبت می‌کند.



راهاکو، مرجع تخصصی مجازی سازی ایران

# مجله راهاکو

RAHA MAG

آدرس: تهران، خیابان سپهد قرنی، خیابان دهقانی، پلاک 12  
کدپستی 1583616414      تلفن: 02154521      [www.rahaco.net](http://www.rahaco.net)

