# بلاکچین و رمزارزها

دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف

نام درس : کارگاه کامپیوتر


گردآورنده : معین آعلی

شماره دانشجویی : ۴۰۱۱۰۸۵۶۱


آبان ماه ۱۴۰۱

# فهرست عناوین

## جدول فهرست اشکال

# ۱. بلاکچین چیست ؟

### ۱/۱. تعریف بلاکچین :

بلاک چین نوع خاصی از پایگاه داده است که اطلاعات در آن ذخیره می‌شود. اما یک سری ویژگی‌های خاص، بلاک چین را از سایر پایگاه داده‌ها متمایز می‌کند. برای اضافه کردن داده جدید به بلاک چین یک سری قوانین وجود دارد. همچنین پس از اضافه شدن داده به بلاک چین و ذخیره آن، دیگر نمی‌توان آن را ویرایش یا حذف کرد.

### ۱/۲. ساختار بلاکچین :

داده‌ها در شبکه بلاک چین در ساختاری متشکل از بلوک ها وارد پایگاه داده می‌شوند. هر بلوک در ادامه بلوک قبلی ساخته می‌شود و شامل اطلاعاتی است که آن را به بلوک قبلی متصل می‌کند. با توجه به این‌که این بلوک‌ها به وسیله اطلاعاتی به همدیگر وصل هستند، بنابراین یک زنجیره تشکیل می‌دهند که در آن بلوک‌ها به ترتیب ساخت در کنار هم قرار می‌گیرند. به اولین بلوک شبکه که قبل از آن بلوک دیگری وجود ندارد بلوک پیدایش گفته می‌شود.

برای درک بهتر ساختار زنجیره بلوکی، فرض کنید دو ستون بر روی یک برگه رسم شده است. شما هر داده‌ای که می‌خواهید نگهداری کنید را در سطر اول از ستون اول قرار می‌دهید. داده درون این سلول، طی فرآیندی محاسباتی تبدیل به یک کلمه جدید با دو حرف می‌شود. این کلمه در ورودی بعدی مورد استفاده قرا می‌گیرد. در این حالت هر تغییری در سلول اول، منجر به تغییراتی در بلوک دوم و تا آخر زنجیره می‌شود. تصویر زیر مثالی از پایگاه داده‌ای است که اطلاعات در آن به صورت زنجیره‌ای به هم وصل شده‌اند.


۱.۲.شکل ۱

بنابراین آخرین شناسنامه بلوکی که در اینجا TH است ، حاصل تمام اطلاعات وارد شده در ردیف‌های قبلی است و هر تغییری در یکی از این داده‌ها منجر به تغییر همه داده‌ها خواهد شد. مثال ذکر شده در واقع توضیح ساده فرآیند هشینگ در بلاکچین است .

# ۲. کاربرد تابع هش در بلاکچین

### ۲/۱. مفهوم هش کردن :

هش کردن فرآیندی است که بلوک‌ها را در کنار هم نگه داشته و زنجیره بلوکی ایجاد می‌کند. در فرآیند هشینگ داده‌ها با هر اندازه‌ای وارد توابع ریاضی خاص می‌شوند تا خروجی که همان هش است را تولید کنند . طول این هش همواره ثابت است و ربطی به طول ورودی به تابع ندارد.

### ۲/۲. ویژگی های هش :

توابع هش مورد استفاده در بلاک چین‌ها به گونه‌ای هستند که احتمال پیدا کردن دو داده که دقیقا خروجی یکسانی داشته باشند، تقریبا صفر است. بنابراین همانند مثال بالا، هر اصلاح مختصری در داده‌های ورودی یکی از بلوک‌ها، منجر به تغییر در خروجی خواهد شد. به عنوان مثال SHA256 تابع هشی است که در بلاک چین بیت‌کوین مورد استفاده قرار می‌گیرد. تنها با تغییر دادن حرف اول یک عبارت طولانی در این تابع، خروجی کاملا متفاوتی ایجاد می‌شود.

این واقعیت که هیچ دو ورودی متفاوتی در تابع هش، منجر به خروجی یکسان نمی‌شود، برای تکنولوژی بلاک چین مهم و حیاتی است. این بدین معنی است که هر بلوک، با داشتن هش حاصل از بلوک قبلی به آن وصل می‌شود. بنابراین هر تلاشی برای ویرایش بلوک‌های قدیمی بلافاصله آشکار می‌شود. در ادامه و در بخش‌های مختلف، کاربردهای دیگر تابع هش در شبکه بلاک چین توضیح داده خواهد شد.

# ۳. نگاهی دقیق تر به ساختار بلاکچین

## ۳/۱. ساختار غیر متمرکز بلاکچین :

تا به حال ساختار بلاک چین به عنوان یک پایگاه داده بررسی شد و دیدیم که داده‌ها در این ساختار، زنجیروار به همدیگر متصل هستند. اگر به بلاک چین به عنوان پایگاه داده مستقل نگاه کنیم آنگاه فقط در برخی از اپلیکیشن‌های کاربردی استفاده خواهد شد. اما ما بلاک چین‌ها را به عنوان ابزاری برای هماهنگی افراد مختلف استفاده می‌کنیم.

در این حالت بلاک چین می‌تواند با استفاده از نظریه بازی و سایر فناوری ها ، به عنوان دفتر کل توزیع شده عمل کند که توسط هیچ کس کنترل نمی‌شود. این بدین معنا است که در این سیستم هیچ کس توانایی ویرایش داده‌ها را خارج از قوانین سیستم نخواهد داشت. بنابراین می‌توان اینطور در نظر گرفت که دفتر کل به طور همزمان متعلق به همه است و برای هر تغییری در آن باید اکثریت به توافق برسند. شاید با یک مثال ساده بتوان درک بهتری از غیرمتمرکز بودن بلاک چین داشت.

## ۳/۲. مثالی برای درک ساختار غیرمتمرکز بلاکچین :

فرض کنید در یک کلاس درس، دانش‌آموزان کلاس از همدیگر پول قرض می‌گیرند و هر وقت پول داشتند، آن را عودت می‌دهند. مبصر کلاس برای این‌که کسی بدهی خود را انکار نکند، گزارش تمام بدهی‌ها را در دفتر خود ثبت می‌کند. حال دانش‌آموزان می‌توانند با مراجعه به مبصر کلاس و مطالعه این دفتر از وضعیت بدهی‌ها و طلب‌های خود آگاه شوند. شرایطی را در نظر بگیرید که دفتر مبصر گم شده یا آتش گرفته باشد. در این حالت چه اتفاقی می‌افتد؟ احتمالا دانش‌آموزانی که بدهکار هستند این موضوع را انکار می‌کنند.

حتما تا به حال متوجه شده‌اید که ثبت اطلاعات در دفتری که احتمال دستکاری یا از بین بردن آن وجود دارد چقدر خطرناک است. برای این‌که این مشکل حل شود، راه حل پیشنهادی این است که تمام بده بستان‌ها در دفتر تمام بچه‌ها نوشته شود. در این حالت همه بچه‌ها یک نسخه از وضعیت کنونی را دارند. بنابراین در صورتی که یک دفتر گم شود دفترهای دیگر وجود دارند و مشکلی پیش نخواهد آمد. همچنین اگر کسی بخواهد دستکاری در دفتر انجام بدهد مورد قبول نخواهد شد مگر در حالتی که دفترِ بیش از نصف دانش‌آموزان کلاس را تغییر دهد. این مثال مشابه راه حلی است که بلاک چین برای حذف اعتماد بین افراد مختلف ارائه کرده است.

۳.۲.شکل۲

ویژگی مرکزگریزی بلاک چین، یک پتانسیل واقعی برای ایجاد محیط‌های غیرمتمرکز ایجاد می‌کند که در آن همه افراد باهم برابر هستند. در این حالت، بلاک چین قابل حذف نیست و نمی‌توان به صورت مخرب آن را کنترل کرد.

## ٤. مسئله فرماندهان بیزانسی در بلاکچین

### ٤/١. شرح مسئله :

مشکل اصلی در برابر ایجاد سیستم‌های غیرمتمرکز توضیح داده شده، چالشی است که با نام مسئله فرماندهان بیزانسی معروف است. این مساله در سال ۱۹۸۰ به این صورت مطرح شد که برای هماهنگی اقدامات در یک جمع، تک‌تک افراد باید با همدیگر ارتباط داشته باشند. مثال بارز این اتفاق زمانی است که فرماندهان جنگ، شهری را محاصره کرده‌اند و می‌خواهند در مورد حمله به آن تصمیم‌گیری کنند. تنها راه ارتباطی آن‌ها نیز استفاده از پیام‌رسان است .

در این حالت هر فرمانده به طور جداگانه باید تصمیم حمله یا عقب‌نشینی بگیرد. مساله حمله یا عقب‌نشینی در این حالت اهمیتی ندارد. آن چه مهم است توافق بر روی یک تصمیم مشترک است. اگر آن‌ها تصمیم به حمله بگیرند، در صورتی موفق خواهند بود که هم‌زمان این کار را انجام دهند. با وجود این‌که فرماندهان از طریق پیام‌رسان‌ها می‌توانند با هم هماهنگ شوند اما مشکلاتی در این بین به وجود می‌آید. به عنوان مثال پیام‌رسان می‌تواند پیام حمله فرمانده را با پیام عقب‌نشینی جایگزین کند.

### ٤/٢. نتیجه مسئله :

در این حالت هر فرمانده به طور جداگانه باید تصمیم حمله یا عقب‌نشینی بگیرد. مساله حمله یا عقب‌نشینی در این حالت اهمیتی ندارد. آن چه مهم است توافق بر روی یک تصمیم مشترک است. اگر آن‌ها تصمیم به حمله بگیرند، در صورتی موفق خواهند بود که هم‌زمان این کار را انجام دهند. با وجود این‌که فرماندهان از طریق پیام‌رسان‌ها می‌توانند با هم هماهنگ شوند اما مشکلاتی در این بین به وجود می‌آید. به عنوان مثال پیام‌رسان می‌تواند پیام حمله فرمانده را با پیام عقب‌نشینی جایگزین کند.

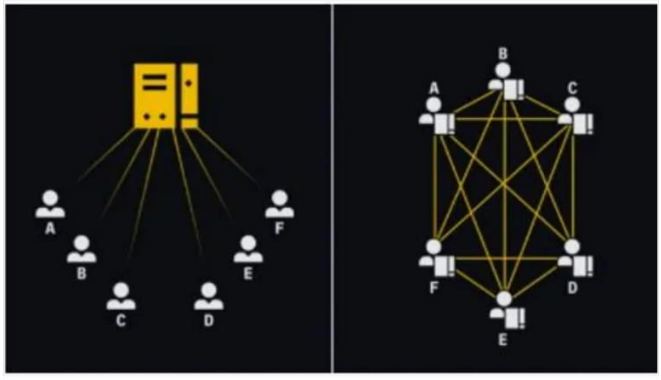
بنابراین، ما به یک استراتژی نیاز داریم که توسط آن به اجماع برسیم . در این حالت، رهگیری پیام‌ها یا حضور افراد غیرمطمئن، خللی در کار ایجاد نمی‌کند. پس، در صورتی که بخواهیم بدون این‌که کسی بر بلاک چین نظارت کند، اطلاعات صحیح به سایرین انتقال دهیم، حتما باید راهکاری بیندیشیم تا افراد بتوانند با یکدیگر ارتباط برقرار کنند.

برای غلبه بر مشکلات احتمالی که توسط یک یا چند کاربر می‌تواند به شبکه بلاک چین تحمیل شود، باید قوانین و مکانیزم‌ها طوری طراحی شوند که در برابر آن‌ها مقاوم باشند. اگر سیستمی این ویژگی را داشته باشد به آن سیستم «بیزانسی مقاوم در برابر خطا» گفته می‌شود. این ویژگی به وسیله الگوریتم‌های اجماع در شبکه بلاک چین ایجاد شده است که در ادامه به بررسی آن‌ها خواهیم پرداخت.

## ٥. شبکه همتا به همتا چیست ؟

### ٥/١. تعریف :

شبکه همتا به همتا لایه کاربران است که در آن افراد به طور مستقیم با یکدیگر ارتباط برقرار و اطلاعات رد و بدل می‌کنند. وقتی شما با دوست خود به طور مستقیم صحبت می‌کنید یک ارتباط همتا به همتا ایجاد می‌کنید. اما اگر با او تماس تلفنی داشته باشید، تماس شما توسط یک سرور بررسی و سپس به دوست شما اطلاع‌رسانی می‌شود. این ارتباط دیگر همتا به همتا نیست. در تصویر زیر می‌توانید تفاوت این دو حالت را مشاهده کنید.




۵.۱.شکل ۳ به ترتیب از چپ به راست: شبکه مرکزی و شبکه همتا به همتا

۵/۲. **مفهوم اصلی :**

در اصل ارتباط همتا به همتا در سیستم‌های متمرکز وجود ندارد و مختص شبکه‌های غیرمتمرکز است. در سیستم متمرکز معمولا تمام اطلاعات در سرور قرار دارد. بنابراین شما باید برای دسترسی به آن‌ها، درخواستی برای سرور بفرستید و در صورت تایید از سمت سرور، آن را دریافت کنید. در این حالت شما اگر تمام داده‌های سرور را دانلود و در سیستم خود نگهداری کنید، می‌توانید بدون نیاز به سرور به اطلاعات دسترسی داشته باشید.

در شبکه بلاک چین افراد دقیقا چنین کاری انجام می‌دهند و تمام داده‌های شبکه در کامپیوتر آن‌ها ذخیره می‌شود. بنابراین اگر کاربری از شبکه خارج شود، بقیه کاربران همچنان به داده‌ها دسترسی دارند و می‌توانند با همدیگر اطلاعات رد و بدل کنند. در زمان تشکیل یک بلوک جدید، داده آن در شبکه پخش می‌شود و افراد می‌توانند دفتر کل خود را به‌روز کنند.

## ۶. گره یا نود (NODE)

۶/۱. **تعریف گره :**

گره یا نود شبکه به شکل ساده، دستگاه‌ها یا ماشین‌هایمتصل به شبکه هستند که کپی اطلاعات بلاک چین را نگه‌داری می‌کنند. همچنین نودها وظیفه اشتراک اطلاعات با دیگر دستگاه‌ها را بر عهده دارند. به طور کلی، برای راه‌اندازی نود کافی است نرم‌افزار شبکه دانلود و نصب شود. بقیه مراحل توسط خود سیستم و نرم‌افزار انجام خواهد شد.

تعریف بالا تعریف خالصی از نود بود. در تعاریف دیگر به هرکسی که با شبکه در ارتباط است نیز نود یا گره گفته می‌شود. به عنوان مثال در رمزارزها، یک اپلیکیشن کیف پول در گوشی شما به عنوان یک نود در شبکه شناخته می‌شود.

## ۷. بلاکچین چطور کار میکند ؟

۷/۱. **طریقه کار :**

در قسمت‌های قبل گفته شد که بلاک چین زنجیره‌ای از بلوک‌ها است و هر بلوک لیستی از تراکنش‌های تایید شده را در خود ذخیره می‌کند. با توجه به این که سیستم بلاک چین توسط تعداد زیادی کامپیوترِ توزیع شده در سرتاسر دنیا کار می‌کند، بنابراین به عنوان یک دفتر کل توزیع شده می‌توان به آن نگاه کرد. این بدان معنی است که هر گره، یک کپی از داده‌های بلاک چین را در اختیار و با دیگر گره‌ها تعامل دارد تا همگام با آن‌ها باشد.

۷/۲. **بخش اصلی :**

قسمت اصلی هر بلاک چینی فرآیند ماینینگ آن است که بر مبنای الگوریتم‌های هشینگ انجام می‌شود. در قسمت‌های قبل توضیح دادیم که هش، خروجی تابع ریاضی است. ورودی این تابع هر مقداری می‌تواند باشد اما خروجی آن یک مقدار منحصر به فرد با اندازه ثابت است. توابع هش، یک طرفه هستند و با داشتن خروجی نمی‌توان به ورودی آن‌ها دست پیدا کرد. یک طرفه بودن هش، باعث امنیت شبکه بلاک چین می‌شود. حال که با الگوریتم‌های مختلف شبکه بلاک چین آشنا شدیم بهتر است با بررسی دو مثال از سیستم‌های مالی سنتی و سیستم بلاک چین نحوه کار بلاک چین را توضیح دهیم.

۷.۲.شکل ۴

### ۷/۳. مثالی برای نحوه کار سیستم مالی سنتی :

فرض کنید علی می‌خواهد به حساب دوستش رضا ۵۰۰ هزار تومان پول واریز کند و هر دو آن‌ها در یک بانک حساب دارند. در این حالت، ابتدا علی درخواست انتقال خود را به بانک می‌دهد. بانک حساب علی را بررسی می‌کند تا موجودی مد نظر را برای انتقال داشته باشد. پس از آن تراکنش انجام می‌شود و ۵۰۰ هزار تومان از حساب علی کم و به حساب رضا اضافه می‌شود. در نهایت پایگاه داده بانک، با اطلاعات جدید به‌روز می‌شود.

باتوجه به این‌که بلاک چین نوعی پایگاه داده است، تراکنش‌ها در آن تقریبا طی فرآیند مشابهی با مثال بالا انجام می‌شوند. تفاوت اساسی در این است که در بلاک چین یک واحد به‌خصوص، مسوولیت بررسی حساب‌ها و به‌روزرسانی پایگاه داده را در اختیار ندارد. در عوض تمامی گره‌ها این مسوولیت را بر عهده دارند.

### ۷/٤. مثالی برای نحوه کار سیستم بلاکچین :

حال فرض کنید علی می‌خواهد ۲ بیت‌کوین برای رضا بفرستد و کل دارایی ارز دیجیتال او همین مقدار است. برای این منظور پیام انتقال از طرق ایجاد تراکنش در کیف پول، به شبکه و گره‌های آن فرستاده می‌شود. گره‌ها با مشاهده این پیام و بررسی دفتر کل توزیع شده، صحت اطلاعات را بررسی می‌کنند. اگر گره‌ها به اجماع رسیدند که علی این دو بیت‌کوین را دارد، تراکنش انجام و به بلوک اضافه می‌شود. برای بررسی دارایی‌ها، باید هویت علی در شبکه معلوم باشد که این کار از طریق «کلید خصوصی» انجام می‌شود.

اطلاعات موجود در هر بلوک شامل هش بلوک قبلی و تراکنش‌های تایید شده است. برای ایجاد رقابت بین ماینرها عبارتی به نام نانس(Nonce) بر اساس سختی شبکه به اطلاعات اضافه می‌شود. نانس به معنی «عددی که تنها یکبار به کار می‌رود» است. این عبارت توسط شبکه تعریف شده است و ماینرها به دنبال یافتن آن هستند. از آن‌جایی که تغییرات کوچک در ورودی، خروجی هشینگ را عوض می‌کند، از این‌رو، ماینرها نانس‌های مختلفی به ورودی اضافه و امتحان می‌کنند تا در نهایت خروجی هش مناسب را پیدا کنند.

این خروجی شامل تعدادی صفر بر اساس نانس استفاده شده است. پس از این‌که ماینری هش را حل کرد. نانس نهایی را به کل شبکه می‌فرستد. دیگر گره‌ها با قرار دان نانس در اطلاعات بلوک و اجرای تابع هش، صحت این ادعا را بررسی می‌کنند. در صورت تایید بلوک به زنجیره اضافه می‌شود.

در نهایت وقتی بلوک ایجاد شد اطلاعات آن در کل شبکه توزیع می‌شود تا دفتر کل برای تمامی گره‌ها به‌روز شود. اگر علی پس از انتقال ۲ بیت‌کوین خود به رضا، بار دیگر بخواهد ۲ بیت‌کوین به حسین بفرستد، نودها با بررسی دفتر کل به این نتیجه می‌رسند که علی این مقدار ارز را ندارد. بنابراین تراکنش انجام نمی‌شود. این مساله با نام خرج مضاعف (Double Spending) مطرح است که بلاک چین از آن جلوگیری می‌کند.

## ۸. مالکیت در فضای بلاکچین چطوری تامین میشود ؟

### ۸/۱. رمزنگاری در بلاکچین :

مفاهیمی مانند نام کاربری و رمز عبور که در سیستم‌های معمولی متداول است، کاربردی در شبکه بلاک چین ندارد. برای اثبات مالکیت در این فضا از رمزنگاری کلید عمومی (Public Key Cryptography) یا رمزنگاری نامتقارن (asymmetric cryptography) استفاده می‌شود. این نوع رمزنگاری از دو کلید عمومی و خصوصی بهره می‌گیرد. همین ویژگی باعث امنیت بالای این روش و گسترش استفاده از آن در سیستم‌های کامپیوتری و شبکه‌های بلاک چینی شده است.

### ۸/۲. وظیفه ی کاربران :

کاربران برای این‌که قابلیت دریافت رمزارز از دیگران را داشته باشند، باید کلید خصوصی خود را ایجاد کنند. کلید خصوصی یک عدد تصادفی بسیار طولانی است که حدس زدن آن حتی با صرف صدها سال برای کسی ممکن نیست. البته اگر کلید خصوصی در اختیار کس دیگری قرار بگیرد، او می‌تواند با وارد کردن رمز، ادعای مالکیت و مبالغ موجود را خرج کند. بنابراین هر کس باید کلید خصوصی خود را مخفی نگه دارد.
در پاراگراف قبل گفته شد که کلید خصوصی نباید به کس دیگری داده شود. حال سوالی که پیش می‌آید این است که طرف مقابل چگونه برای ما ارز انتقال می‌دهد. جواب این سوال در کلید عمومی نهفته است. کلید عمومی می‌تواند در اختیار دیگران قرار بگیرد. در واقع کلید عمومی به نوعی شماره حساب شما تلقی می‌شود. تبدیل کلید عمومی به کلید خصوصی تقریبا غیرممکن است بنابراین این روش امنیت بسیار بالایی برای کاربران ایجاد می‌کند .


۸.۲.شکل ۵

## ۹. امنیت در فضای بلاکچین چطوری تامین میشود ؟

بلاک چین‌ها به وسیله مکانیزم‌های متعددی که شامل تکنیک‌های پیشرفته رمزنگاری و مدل‌های رفتاری-تصمیم‌گیری ریاضی، امنیت خود را تامین می‌کنند. در بسیاری از کاربردهای بلاک چین مساله تغییرناپذیری و امنیت بسیار حیاتی است. در این بخش نحوه تامین این دو ویژگی مهم بحث می‌شود.

### ۹/۱. اجماع و تغییرناپذیری :

ویژگی اجماع به توانایی گره‌های یک شبکه برای رسیدن به اجماع، جهت ثبت تراکنش‌ها و ساخت بلوک گفته می‌شود. در مقابل، ویژگی تغییرناپذیری به معنی جلوگیری از کپی شدن معاملاتی است که قبلا در سیستم ثبت شده‌اند. این دو ویژگی در کنار هم باعث ایجاد امنیت در بلاک چین می‌شوند.

الگوریتم‌های اجماع به ما اطمینان می‌دهند که قوانین شبکه در حال اجرا است و همه اعضای شبکه در مورد وضعیت فعلی شبکه توافق دارند. در حالی که تغییرناپذیری، یکپارچگی داده‌ها و سوابق تراکنش‌های انجام شده را پس از تایید اعتبار هر بلوک تضمین می‌کند.

### ۹/۲. نقش رمزنگاری در امنیت بلاکچین :

بلاک چین‌ها برای تامین امنیت داده‌های خود به طور گسترده از رمزنگاری استفاده می‌کنند. در این زمینه توابع هش رمزنگاری از اهمیت بالایی برخوردار هستند. هش کردن فرآیندی است که در آن یک تابع هش، ورودی را با اندازه دلخواه دریافت می‌کند و خروجی هش را با با یک طول ثابت برمی‌گرداند. در فرآیند هشینگ با کوچکترین تغییر در ورودی، خروجی تغییر می‌کند. اما اگر ورودی ثابت باشد هر چند بار هم تابع اجرا شود خروجی یکی خواهد بود.

در فضای بلاک چین خروجی توابع (هش) به عنوان شناساگرهای منحصربه‌فرد در بلوک داده‌ها استفاده می‌شوند. هش هر بلوک، با استفاده از هش بلوک قبل ایجاد شده است. همین موضوع باعث ایجاد زنجیره بلوک می‌شود. بنابراین، هش هر بلوک به هش بلوک قبلی و داده‌های ذخیره شده در بلوک بستگی دارد. شناساگرهای هش نقش مهمی در حفظ امنیت و تغییرناپذیری بلاک چین ایفا می‌کنند.

### ۹/۳. اقتصاد رمزنگاری :

اقتصاد رمزنگاری، مطالعه اقتصاد در پروتکل‌های بلاک چین و بررسی خروجی حاصل از طراحی آن بر مبنای رفتار کاربران شبکه است. منظور از امنیت اقتصاد در فضای رمزنگاری این است که بلاک چین انگیزه‌های اقتصادی بیشتری برای عمل صادقانه نسبت به رفتارهای مخرب برای گره‌ها ایجاد می‌کند. الگوریتم اجماع اثبات کار بیت‌کوین بهترین مثال در این حوزه است. کاربری که صادقانه عمل می‌کند از شبکه بیت‌کوین پاداش می‌گیرد. اما اگر این کاربر رفتار مخرب داشته باشد، توان محاسباتی و برق مصرفی او انگار هدر رفته است.

همین امر می‌تواند امنیت بلاک چین را در برابر حمله‌های احتمالی که هدف آن کنترل اجماع شبکه است، تامین کند. فضای رقابتی شدید که در بیت‌کوین وجود دارد به گونه‌ای است که به ندرت کسی یا گروهی اقدام به انجام حمله ۵۱ درصد می‌کند. این درحالی است که هزینه تامین ابزارهای لازم برای در اختیار داشتن توان اجماع ۵۱ درصدی نیز بسیار زیاد است. بنابراین انجام این کار در کل، صرفه اقتصادی نخواهد داشت.

۹.۳.شکل ۶

## ۱۰. مقیاس پذیری در بلاکچین چیست ؟

**۱۰/۱.تعریف مقیاس پذیری :**

مقیاس پذیری بلاک چین، به توانایی شبکه در پاسخ به افزایش تقاضا در سیستم اشاره دارد. اگرچه بلاک چین ویژگی‌های مثبتی مانند غیرمتمرکز بودن و تغییرناپذیری را دارد اما این ویژگی‌ها در ازای پرداخت هزینه به دست آمده است. کاهش مقیاس‌پذیری یکی از این هزینه‌ها است. پایگاه داده‌های متمرکز برخلاف بلاک چین، توانایی انجام تراکنش‌ها را با سرعتی به مراتب بالاتر دارند. دلیل این امر عدم نیاز این سیستم‌ها به تایید تراکنش‌ها توسط هزاران نفر در سرتاسر دنیا است.

اگرچه راه‌حل‌های متفاوت زیادی برای حل این مشکل ارائه و اجرا شده‌اند اما در حال حاضر راه‌حل کارای نهایی، برای هیچ‌کس مشخص نیست. به نظر می‌رسد که راه‌حل‌های مختلف باید مورد آزمایش قرار بگیرند تا این‌که ساده‌ترین راه‌حل برای حل مشکل مقیاس‌پذیری به دست آید.

**۱۰/۲.یک سوال اساسی :**

یک سوال اساسی در مورد مقیاس‌پذیری وجود دارد که دیدگاه‌ها را به دو دسته تقسیم می‌کند. یک دسته معتقدند برای افزایش مقیاس‌پذیری شبکه، باید عملکرد خود بلاک چین را افزایش دهیم که به آن مقیاس پذیری درون زنجیره ای(on-chain scaling) گفته می‌شود. دسته دیگر معتقدند که باید اجازه دهیم تراکنش‌ها بدون درگیری با بلاک چین اصلی انجام شوند و از این طریق مقیاس‌پذیری را افزایش دهیم. به این روش مقیاس پذیری برون زنجیره ای(off-chain scaling) گفته می‌شود.

هر یک از این روش‌ها مزایای خودشان را دارند. راه‌حل‌های مقیاس‌پذیری درون زنجیره‌ای می‌تواند شامل کاهش اندازه تراکنش‌ها یا بهینه‌سازی نحوه ذخیره آن‌ها در بلوک باشد. از طرف دیگر راه‌حل‌های خارج از زنجیره شامل دسته‌بندی معاملات خارج از شبکه اصلی و اضافه کردن آن‌ها به شبکه با تاخیر زمانی است. برخی از روش‌های معروف مقیاس‌پذیری استفاده از سایدچین(Sidechain) و کانال های پرداخت( Payment Channels) است .

**۱۰/۳.مزایای مقیاس پذیری :**

دلیل ایجاد بلاک چین، جایگزینی سیستم‌های متمرکز است. بلاک چین برای رقابت با این سیستم‌ها حداقل باید به اندازه آن‌ها مقیاس‌پذیر باشد. البته در عمل، برای جذب توسعه‌دهندگان و عموم مردم برای استفاده از این پلتفرم‌ها، بلاک چین مجبور است مقیاس‌پذیری بالاتری از سیستم‌های معمول ارائه کند. بنابراین نیاز است که بلاک چین سریع‌تر، ارزانتر و راحت‌تر از سیستم‌های سنتی باشد.

به عنوان مثال شبکه اجتماعی را در نظر بگیرید که در بلاک چین راه‌اندازی شده است. اگر این شبکه تنها توانایی انتقال ۱۰ پیام در دقیقه را داشته باشد و میلیون‌ها کاربر در سرتاسر جهان بخواهند از این بستر استفاده کنند، پیام شما ممکن است بعد از چند روز به دست مخاطب برسد. در عمل استفاده از این سیستم هیچ مبنا و منطقی ندارد.

## ۱۱. مزایا و معایب بلاکچین

بلاک چین برای حل مشکلات موجود در زمینه‌های مختلف مانند امور مالی و ذخیره‌سازی فایل به کار گرفته می‌شود. شبکه توزیع شده، نقاط قوت زیادی در مقابل مدل سنتی Client-Server دارد اما معایبی نیز در آن دیده می‌شود. در ادامه این دو وجهه از بلاک چین را مورد بحث و بررسی قرار می‌دهیم.

**۱۱/۱.مزایای بلاکچین :**

یکی از مزایای اولیه استفاده از بلاک چین – همانطور که در سفیدنامه بیت‌کوین آمده است – انجام تراکنش‌ها بدون حضور واسطه است. این قضیه در بلاک چین‌های نسل اول مانند بیت‌کوین و لایت‌کوین برای انتقال پول به وجود آمده است. در بلاک چین‌های جدید علاوه بر آن، امکان انتقال بدون واسطه هر نوع داده دیگر نیز فراهم است. حذف واسطه به معنی کاهش احتمال دستکاری و حذف داده و همچنین کاهش هزینه انتقال داده است.

دومین مزیت استفاده از بلاک چین، عدم نیاز به دریافت اجازه از شخص یا سازمان است. هر شخص با وصل بودن به اینترنت و داشتن نرم‌افزار مورد نظر شبکه می‌تواند به راحتی وارد شبکه شود و از امکانات آن استفاده کند. بنابراین، در این فضا هیچ کس نمی‌تواند به دیگری اعمال نظر کند و همه در برابر قوانین شبکه یکسان هستند.

یکی از مهمترین نقاط قوت شبکه‌های بلاک چین این است که از مقاومت بالایی در برابر سانسور یا حذف شبکه به وسیله افراد یا سازمان‌ها برخوردارند. در سیستم‌های متمرکز برای انجام خراب‌کاری تنها کافی است سرور شبکه مورد حمله قرار گیرد. اما در شبکه همتا به همتای بلاک چین، هر گره به عنوان یک سرور عمل می‌کند. لذا حذف آن راحت نیست.

بلاک چینی مانند بلاک چین بیت‌کوین بیش از ۱۰ هزار گره قابل مشاهده در جهان دارد. برای یک عامل مخرب با منابع مالی قوی هم از کار انداختن این شبکه تقریبا غیرممکن است. این درحالی است که تعداد زیادی گره پنهان نیز در شبکه وجود دارد که قابل مشاهده نیستند. بنابراین، با در نظر گرفتن آن‌ها، امکان حمله به این شبکه و از بین بردن آن تقریبا صفر است.

مزایای ذکر شده در اکثر شبکه‌های بلاک چینی وجود دارد. اما هر بلاک چین به طور خاص می‌تواند مزایای دیگری نیز داشته باشد. برای اطلاع از مزایای هر پروژه مطالعه سفیدنامه پروژه و سایت‌های مربوطه توصیه می‌شود. برای اطلاع از ماهیت و مزایای مهمترین ارزهای دیجیتال می‌توانید به مطالب زیر مراجعه کنید :

- **بیت کوین چیست؟ — از مفاهیم اولیه تا استخراج و پس انداز | به زبان ساده**
- **اتریوم چیست؟ | کامل ترین راهنمای رایگان — به زبان ساده**
- **کاردانو چیست؟ — به زبان ساده**
- **ارز دیجیتال تتر چیست؟ — همه چیز درباره استیبل کوین تتر(Tether)**
- **ارز دیجیتال ترون چیست؟ — آنچه برای شروع باید بدانید | به زبان ساده**

۱۱.۱.شکل ۷

**۱۱/۲.معایب بلاکچین :**

بلاک چین‌ها برای دستیابی به مزایای گفته شده، برخی از مزایای سیستم‌های قبلی را از دست داده‌اند. یکی از مهم‌ترین مسائلی که اکثر بلاک چین‌ها با آن روبه‌رو هستند، مساله مقیاس‌پذیری است. از آن‌جایی که همه گره‌ها در شبکه باید همگام باشند، اطلاعات نمی‌توانند خیلی سریع به بلاک چین اضافه شوند. بنابراین در این سیستم‌ها به منظور حفظ ویژگی غیرمتمرکز بودن شبکه، از قابلیت مقیاس‌پذیری آن صرف نظر شده است.

این مشکل در زمان‌های اوج استفاده از شبکه، بیشتر برای کاربران قابل لمس است. بلوک‌ها در بلاک چین‌ها نمی‌توانند اطلاعات زیادی را در خود نگه‌دارند و فورا به زنجیره اضافه نمی‌شوند. برای مثال در بیت‌کوین زمان ساخت هر بلوک به طور متوسط ده دقیقه است. بنابراین اگر تعداد تراکنش‌ها بیش از حد مجاز هر بلوک باشد، بقیه تراکنش‌ها باید منتظر بلوک بعدی باشند. حجم هر بلوک بیت‌کوین در حدود ۱ مگابایت ذکر می‌شود.

ارتقای سیستم‌های بلاک چین یکی دیگر از مشکلات موجود است. اگر شما نرم‌افزاری را برای خودتان برنامه‌نویسی می‌کنید، به دلخواه خود می‌توانید هر ویژگی که دوست داشتید به آن اضافه کنید. اما در محیطی که پتانسیل حضور میلیون‌ها کاربر را دارد، اعمال تغییرات به شدت سخت است. البته شما می‌توانید برخی از پارامترهای نرم‌افرار گره خود را تغییر دهید اما این کار باعث دور افتادن شما از شبکه اصلی خواهد شد. در حالتی که نرم افزار بهبود یافته با سایر گره‌ها ناسازگار باشد، آن‌ها از برقراری ارتباط با شما امتناع خواهند کرد.

تنها راه اعمال تغییرات در شبکه جلب نظر اکثریت اکوسیستم شبکه است. بنابراین در شبکه‌های بزرگ ممکن است ماه‌ها یا سال‌ها بحث‌های فشرده‌ای در انجمن‌های بلاک چین برای اعمال تغییرات صورت بگیرد. در صورتی که شخص یا گروهی بخواهد تغییراتی خارج از توافق انجام بدهد، می‌تواند هاردفورک(Hard Fork) یا سافت فورک(Soft Fork) ایجاد کند .

## ۱۲. فورک چیست ؟

**۱۲/۱.تعریف :**

فورک (Fork) به فرآیندی گفته می‌شود که در آن یک نرم‌افزار که از قبل موجود است، کپی و اصلاح می‌شود. بنابراین هم برنامه اصلی پابرجاست و هم نسخه اصلاح شده آن وجود دارد. اما پس از این مرحله، دو نرم‌افزار مسیرهای مختلفی را طی می‌کنند. این اتفاق مثل دوراهی، پس از طی مسیر در یک جاده است و برای ادامه مسیر باید یکی از این دو راهی‌ها انتخاب شوند.

در پروژه‌های برنامه‌نویسی متن باز (open source) این اتفاق زیاد می‌افتد. قبل از ایجاد رمزارزها نیز این اتفاق بارها در سایر پروژه‌های متن باز اتفاق افتاده است. در شبکه‌های بلاک چین اتفاق جدید، وجود دو نوع فورک به نام هاردفورک و سافت فورک است که در ادامه هر یک را توضیح خواهیم داد.

**۱۲/۲.هارد فورک :**

هارد فورک‌ها به‌روزرسانی نرم‌افزاری به شمار می‌آیند که با نسخه قدیم سازگار نیستند. به طور معمول، هاردفورک زمانی اتفاق می‌افتد که برخی از گره‌های شبکه بخواهند قوانین جدیدی به شبکه اضافه کنند و این قوانین مغایر با قوانین شبکه اصلی باشند. در این حالت، گره‌های جدید تنها با نودهایی که از نسخه جدید نرم‌افزار استفاده می‌کنند، در ارتباط هستند. بنابراین بلاک چین به دو شبکه جدا از هم تقسیم می‌شود که یکی با قوانین گذشته و دیگری با قوانین جدید فعالیت می‌کند.

هر دو شبکه در این حالت بلوک‌های معاملات خود را تولید می‌کنند اما دیگر در یک شبکه فعالیت نمی‌کنند. همه گره‌ها تا نقطه انجام فورک، بلاک چین یکسانی دارند و سابقه تراکنش آن‌ها را در اختیار دارند اما پس از آن، بلوک‌ها و تراکنش‌های متفاوتی خواهند داشت. به دلیل وجود سابقه مشترک، اگر شما سکه‌های بلاک چین را در اختیار داشتید با انجام هاردفورک در هر دو شبکه این تعداد سکه را خواهید داشت.

این قضیه با نام ایردراپ هاردفورک نیز شناخته می‌شود. شما سکه‌های خود را می‌توانید در شبکه قدیمی به فروش برسانید و تراکنش آن در بلوک‌های بعد از هاردفورک آن ثبت می‌شود. اما تعداد سکه‌های شما در شبکه جدید تغییر نمی‌کند. با فرض این‌که رمزنگاری در هاردفورک تغییر نکرده باشد، کلید خصوص شما در هاردفورک جدید همچنان سکه‌های قدیمی را در خود دارد.

**۱۲/۳.مثالی از هاردفورک :**

در سال ۲۰۱۷ شبکه بیت‌کوین به وسیله هاردفورک به دو شبکه بلاک چین بیت‌کوین و بیت‌کوین کش تقسیم شد. این فورک پس از مدت‌ها بحث و گفتگو روی موضوع بهترین رویکرد برای مقیاس‌پذیری انجام شد. طرفداران بیت‌کوین کش می‌خواستند اندازه بلوک‌ها را افزایش دهند تا تعداد زیادی تراکنش در آن‌ها ثبت شود اما طرفداران بیت‌کوین با این تغییر مخالف بودند.

افزایش اندازه بلوک‌ها نیازمند اصلاح قوانین است. بنابراین گره‌ها فقط بلوک‌های با اندازه کمتر از ۱ مگابایت را قبول می‌کنند. اگر شما بلوکی با اندازه ۲ مگابایت تولید کنید که حتی تراکنش‌های معتبر داخل آن ذخیره شده باشد، سایر گره‌ها آن را قبول نخواهند کرد. تنها، گره‌هایی که قوانین جدید را قبول کرده و نرم افزار خود را به روز کرده‌اند، می‌توانند بلوک‌های با اندازه بیش از ۱ مگابایت را قبول کنند.

**۱۲/٤. سافت فورک :**

سافت فورک، به‌روزرسانی نرم‌افزاری سازگار با نسخه قدیمی است. به این معنی که در این حالت گره‌های ارتقا یافته همچنان می‌توانند با سایر گره‌ها در ارتباط باشند. معمولا در سافت فورک قانون جدیدی به شبکه اضافه می‌شود که تناقضی با قوانین گذشته ندارد.

به عنوان مثال کاهش اندازه بلوک‌ها به وسیله سافت فورک قابل اجرا است. چراکه هیچ محدودیتی برای حداقل اندازه یک بلوک در شبکه قرار داده نشده است. بنابراین در این حالت شما همچنان به شبکه وصل هستید و تنها برخی از داده‌هایی که آن‌ها برای شما ارسال می‌کنند را فیلتر می‌کنید.

**۱۲/٥. مثالی از سافت فورک :**

سافت فورکِ سگویت یک نمونه خوب برای سافت فورک است که پس از ایجاد بیت‌کوین کش در شبکه بیت‌کوین به وقوع پیوست. به‌روزرسانی انجام شده در سگویت مربوط به ساختار بلوک‌ها و معاملات بود. این به‌روزرسانی به طرز هوشمندانه‌ای انجام شد. به گونه‌ای که گره‌های قدیمی همچنان توان ایجاد بلوک‌ها و تایید تراکنش‌ها را داشته باشند.

نودهای قدیمی تراکنش‌ها و اطلاعات را از سایرین دریافت می‌کنند اما ممکن است بسیاری از این پیام‌ها نامفهوم باشد. تنها در حالتی توانایی درک فیلدهای جدید برای گره‌ها ایجاد خواهد شد که از نرم‌افزار جدید استفاده کنند. این نرم‌افزار امکان تجزیه و تحلیل داده‌های جدید را دارد.

## ۱۳. اجماع در بلاکچین

**۱۳/۱.تعریف :**

قبل از این در مورد گره‌های شبکه و ارتباط آن‌ها باهم و این‌که هر کدام یک کپی از اطلاعات شبکه را دارند صحبت کرده‌ایم اما هنوز در مورد نحوه اضافه شدن بلوک به شبکه چیزی نگفته‌ایم. در بلاک چین هیچ شخص یا نهادی مسوولیت تقسیم وظایف بین کاربران را بر عهده ندارد. با توجه به این‌که همه گره‌ها از قدرت یکسانی برخوردار هستند، تصمیم‌گیری در مورد این‌که چه کسی بلوک را به زنجیره اضافه کند به مکانیزم عادلانه‌ای نیاز دارد.

**۱۳/۲.طراحی :**

این سیستم باید به گونه‌ای طراحی شده باشد که امکان تقلب کردن از کاربران را سلب کند اما به خاطر درست‌کاری به آن‌ها پاداش بدهد. در این حالت رفتار کاربران به گونه‌ای خواهد بود که بتوانند بیشترین سود را کسب کنند. چون در شبکه نیاز به اجازه گرفتن از هیچ کس نیست، امکان ساخت بلوک باید برای همه وجود داشته باشد. پروتکل‌ها اغلب با الزام کاربر به قرار دادن بخشی از سرمایه خود در ریسک، این پروسه را تضمین می‌کنند. با انجام این کار کاربران می‌توانند در پروسه ساخت بلوک شرکت کنند و در صورت ایجاد یک بلوک معتبر از شبکه پاداش بگیرند.

به هر حال، اگر کاربر یا کاربرانی بخواهند تقلب کنند سایر گره‌ها از آن مطلع خواهند شد. در نتیجه مصرف برق و توان محاسباتی آن‌ها هدر خواهد رفت. مکانیزم ارائه شده را الگوریتم های اجماع(Consensus Algorithms) می‌نامند. الگوریتم اجماع این امکان را برای کاربران فراهم می‌کند که بر روی بلوک جدید اجماع کنند. الگوریتم‌های اجماع مختلفی در بلاک چین مورد استفاده قرار می‌گیرند. دو مورد از پرکاربردترین این الگوریتم‌ها در ادامه بررسی می‌شوند.

## ۱٤. ماینینگ :

### ۱٤/۱.تعریف :

ماینینگ (Mining) با اختلاف پرکاربردترین الگوریتم اجماع در بلاک چین‌ها است. در ماینینگ از الگوریتم اجماع اثبات کار(Proof of Work) استفاده می‌شود. در این شکل از اجماع، کاربران قدرت پردازشی خود را برای حل معمایی خرج می‌کنند که توسط پروتکل ارائه شده است.

### ۱٤/۲.یک مشکل :

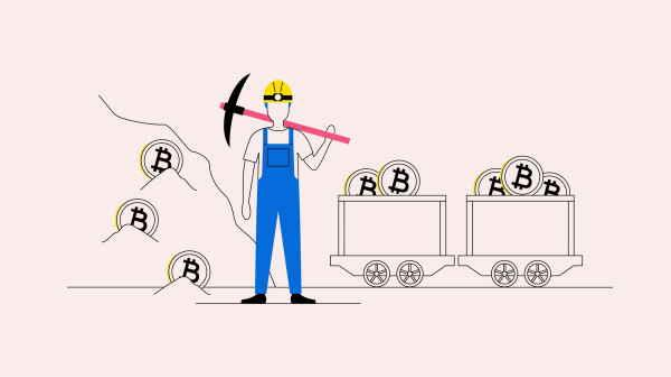
این معما کاربران را ملزم به هش معاملات و سایر اطلاعات موجود در بلوک می‌کند. اطلاعات هر بلوک شامل تراکنش‌ها و هش شبکه قبلی است. بنابراین اطلاعات برای همه یکسان است. در این حالت، اگر فرآیند هشینگ انجام شود تمام ماینرها به خروجی یکسان خواهند رسید و رقابت عملا بی‌معنی خواهد بود.

### ۱٤/۳.حل یک مشکل :

برای حل این مشکل، بلاک چین بر حسب سختی شبکه، به داده‌های ورودی عبارت دیگری به نام نانس اضافه می‌کند و هش تابع در واقع با استفاده از آن انجام می‌شود. این نانس تعداد زیادی صفر در ابتدای هش خروجی ایجاد می‌کند که ماینرها برای دستیابی به هش درست باید نانس را پیدا کنند. برای این منظور ، تابع هش را با یک نانس فرضی اجرا می‌کنند. این کار تا زمانی ادامه پیدا می‌کند که به هش تعیین شده توسط سختی شبکه برسند.

بدیهی است که هش کردن مکرر داده‌ها از نظر محاسباتی هزینه زیادی دارد. در بلاک چین‌های با الگوریتم اجماع اثبات کار، سهمی که کاربران ارائه می‌کنند، پول سرمایه‌گذاری شده در دستگاه‌های استخراج ارز دیجیتال و برق مورد استفاده برای آن‌ها است. زمانی که یک ماینر بلوک جدیدی ایجاد و برای شبکه ارسال می‌کند، کاربران دیگر از آن به عنوان ورودی در تابع هش بهره می‌گیرند.

آن‌ها فقط با یک بار اجرای تابع هش مطمئن می‌شوند که بلوک ایجاد شده تحت قوانین بلاک چین، معتبر است یا نه. اگر بلوک معتبر نبود، ماینر پاداشی دریافت نمی‌کند و هزینه صرف شده برای استخراج هدر می‌رود. بیت‌کوین اولین شبکه بود که از این الگوریتم استفاده کرد اما بعدا شبکه‌های دیگری نیز آن را به کار گرفتند. دستگاه‌های مختلفی مانند کارت گرافیک و ای‌سیک برای استخراج بیت کوین استفاده می‌شود.



۱۴.۳.شکل ۸

**۱۴/۴.معایب الگوریتم اجماع اثبات کار :**

در کنار مزایایی که برای الگوریتم اجماع اثبات کار ذکر شد معایبی نیز می‌توان بر آن متصور بود. نقاط ضعف این الگوریتم، منجر به ایجاد و استفاده از الگوریتم‌های اجماع جدید شده است.

- **مصرف انرژی :** فرآیند ماینینگ با مصرف انرژی بالا همراه است که خود منجر به مشکلات محیط زیستی می‌شود.
- **افزایش هزینه‌های ورود به شبکه در طی زمان :** با افزایش تعداد ماینرهای در شبکه، پروتکل‌ها سختی معمای ماینینگ را افزایش می‌دهند. اشخاص برای این‌که بتوانند در رقابت برای ماینینگ باقی بمانند باید تجهیزات قوی‌تری تامین کنند. این ممکن است برای ماینرها هزینه‌های زیادی ایجاد کند.
- **حمله ۵۱ درصد :** اگرچه ماینینگ یک فرآیند غیرمتمرکز است اما احتمال این‌که یک ماینر بتواند اکثریت توان هشینگ را به دست آورد، هنوز از بین نرفته است. اگر چنین اتفاقی بیفتد، آن‌ها می‌توانند معاملات را تغییر داده و امنیت بلاک چین را از بین ببرند.

## ۱۵. الگوریتم اجماع اثبات سهام

**۱۵/۱.تعریف :**

در الگوریتم PoW بلاک چین برای اطمینان از عملکرد مناسب شما هزینه‌های محاسباتی تحمیل می‌کند. اگر نتوانید به طور صحیح بلوک‌ها را استخراج کنید سرمایه‌گذاری شما بی‌ثمر خواهد بود. الگوریتم اجماع اثبات سهام(Proof of Stake) هزینه خارج از شبکه به سهامداران تحمیل نمی‌کند. به جای ماینرها ما اعتبارسنج ها(Validators) را داریم که بلوک‌ها را می‌سازند (forge) یا به عبارت دیگر پیشنهاد می‌دهند.

اعتبارسنج‌ها می‌توانند با کامپیوترهای معمولی خود بلوک‌های جدید را تولید کنند اما آن‌ها باید بخش از دارایی خود را برای گرفتن این امتیاز در معرض خطر قرار دهند. استیکینگ با مبلغ از پیش تعیین شده‌ای از ارز دیجیتال اصلی هر بلاک چین و با توجه به قوانین هر پروتکل انجام می‌شود. به عنوان مثل برای استیکینگ در شبکه کاردانو باید مقداری ADA (ارز دیجیتال اصلی شبکه)، استیک کنید.

پیاده‌سازی‌های مختلف این الگوریتم تفاوت‌هایی با هم دارند اما با استیک کردن ارزهای دیجیتال توسط اشخاص، پروتکل به صورت تصادفی از میان افراد یکی را برای ساختن و ارائه بلوک جدید انتخاب می‌کند. اگر این کار به درستی انجام شود به اعتبارسنج‌ها پاداش داده می‌شود. گزینه‌ای دیگر برای ساخت بلوک‌ها، تایید آن توسط چندین نفر است که در این صورت پاداش به نسبت سهام هر شخص بین آن‌ها تقسیم می‌شود. بلاک چین‌های متعددی از این الگوریتم استفاده می‌کنند. ارز دیجیتال اتریوم نیز به دنبال تغییر الگوریتم خود از Pow به PoS است.

۱۵.۱.شکل ۹

### ۱۵/۲.مزایای الگوریتم اجماع اثبات سهام :

الگوریتم‌های اجماع اثبات سهام به منظور پوشش معایب الگوریتم اجماع اثبات کار ارائه شدند. مزایای این الگوریتم‌ها را می‌توان در سه مورد زیر خلاصه کرد.

- **طرفدار محیط زیست :** در این الگوریتم نیازی به انجام فرآیند هشینگ با دستگاه‌های محاسباتی پیشرفته وجود ندارد. بنابراین مصرف برق آن بسیار کمتر از الگوریتم PoW است. هر چه مصرف برق کمتر باشد، دی‌اکسید کربن کمتری تولید می‌شود و این به معنی حفاظت از محیط زیست است.
- **تراکنش‌های سریع :** از آن‌جایی که در این الگوریتم نیازی به صرف نیروی محاسباتی برای حل معماهای تعیین شده نیست، ادعا می‌شود که این الگوریتم‌ها می‌توانند سرعت انجام تراکنش‌ها را افزایش دهند.
- **پاداش استیکینگ :** در این روش پاداش مستقیم به دارندگان توکن شبکه داده می‌شود. در PoW پاداش به ماینرها داده می‌شد که آن‌ها ممکن است توکن شبکه را نداشته باشند. در کنار این، برخی از الگوریتم‌های اجماع اثبات سهام به کاربران امکان درآمدزایی با استیک کردن سرمایه را می‌دهند.

### ۱۵/۳.معایب الگوریتم اجماع اثبات سهام :

الگوریتم اجماع اثبات سهام برخی از مشکلات الگوریتم PoW را حل کرد. اما همچنان با یک سری نقاط ضعف روبه‌رو است. به طور کلی این معایب را می‌توان در سه مورد زیر خلاصه کرد.

- **نسبت به Pow کمتر آزمایش شده‌اند :** پروتکل‌های PoS هنور در مقیاس بزرگ آزمایش نشده‌اند. ممکن است برخی از مشکلات آن در فرآیند اجرا و رمزنگاری هنوز کشف نشده باشد.
- **حاکمیت ثروتمندان :** اکوسیستم ایجاد شده توسط این الگوریتم به گونه‌ای است که ثروتمندان در آن ثروت بیشتری کسب می‌کنند. این مساله از آنجایی نشات می‌گیرد که هرچه اعتبارسنج مبلغ بیشتری استیک کند، پاداش بیشتتری دریافت خواهد کرد.
- **متمرکز شدن سیستم :** الگوریتم اجماع اثبات سهام برای بالابردن سرعت تراکنش‌ها، سیستم نسبتا متمرکزتری را ایجاد کرده است. مشکلاتی چون حمله ۵۱ درصد در این روش همچنان پابرجاست.

## ۱۶. بلاکچین عمومی و خصوصی

بیت‌کوین پایه ایجاد صنعت بلاک چین را بنا گذاشت و پس از آن صنعت بلاک چین با پیشرفت‌های گسترده‌ای همراه شد. همزمان با این‌که بیت‌کوین در حال تثبیت خود به عنوان دارایی مالی بود، دیگر مبتکران پتانسیل‌های تکنولوژی زیرساخت بیت‌کوین را در سایر زمینه‌ها بررسی می‌کردند. همین مساله منجر به کشف موارد جدید استفاده بلاک چین خارج از امور مالی شد.

بیت‌کوین یک بلاک چین عمومی است. به این معنا که هرکسی که به اینترنت وصل باشد و نرم‌افزار مخصوص آن را نصب کند، می‌تواند تمامی معاملات درون شبکه را مشاهده کند. با توجه به این‌که برای حضور در شبکه بیت‌کوین نیاز به هیچ کار دیگری نیست، این بستر را به عنوان محیطی تعریف می‌کنند که برای حضور در آن نیازی به اجازه گرفتن از کسی نیست.

در مقابلِ بلاک چین‌های عمومی، یک سری بلاک چین‌های دیگر وجود دارند که «بلاک چین‌های خصوصی (Private Blockchains) نامیده می‌شوند. این سیستم‌ها قوانینی دارند که طبق آن‌ها معین می‌شود چه کسانی می‌توانند با بلاک چین تعامل داشته باشند و تراکنش‌ها را مشاهده کنند. بنابراین برای شرکت در فضای این بلاک چین‌ها باید طبق قوانین، اجازه ورود بگیرید.

ممکن است در ابتدای امر ایجاد بلاک چین‌های خصوصی زائد به نظر برسد. اما این بلاک چین‌ها کاربردهای زیادی به‌خصوص در بخش‌های سازمانی دارند. مدیران یک سازمان خصوصی حتما می‌خواهند اطلاعات شرکت به بیرون درز نکند. این امر با استفاده از بلاک چین‌های عمومی ممکن نیست و حتما باید از بلاک چین خصوصی برای طراحی استفاده شود. برای کسب اطلاعات بیشتر در مورد انواع بلاک چین مطالعه مقاله زیر پیشنهاد می‌شود.

۱۶.۱.شکل ۱۰

## ۱۷. کاربرد های بلاکچین

بلاک چین کاربردهای بسیار زیادی دارد. تقریبا در هر بستری که نیاز به ثبت و انتقال داده یا پیام وجود دارد می‌توان از بلاک چین استفاده کرد. در این بخش به برخی از کاربردهای مهم بلاک چین پرداخته می‌شود.

### ۱۷/۱. کاربرد بلاکچین در چرخه زنجیره تامین :

زنجیره تامین کارا، هسته اصلی بسیاری از شرکت‌های موفق است که هدف آن مدیریت توزیع کالا و خدمات از تولیدکننده به مصرف‌کننده است. هماهنگی ذینفعان متعدد یک صنعت خاص، با استفاده از روش‌های سنتی بسیار سخت است.

تکنولوژی بلاک چین می‌تواند سطوح پیشرفته‌تری از شفافیت را در بسیاری از صنایع ایجاد کند. اکوسیستم زنجیره تامین که قابلیت تعامل داشته باشد و حول یک پایگاه داده تغییرناپذیر بچرخد، چیزی است که بسیاری از صنایع برای قوی‌تر و قابل اعتمادتر شدن به آن نیاز دارند. بلاک چین دقیقا این نیاز را برطرف می‌کند.

### ۱۷/۲. بازی های کامپیوتری :

صنعت بازی‌های رایانه‌ای یکی از صنایع بزرگ حوزه سرگرمی در دنیا است که می‌تواند از بلاک چین بهره زیادی ببرد. در بیشتر بازی‌های رایانه‌ای، افراد مجبورند که قوانین توسعه‌دهندگان بازی را اجرا و از بستر مشخص شده توسط آن‌ها استفاده کنند. امکان توسعه و تغییر نیز در بسیاری از آن‌ها برای کاربران وجود ندارد. بلاک چین می‌تواند در زمینه تمرکززدایی از مالکیت، مدیریت و نگهداری بازی‌ها مفید باشد.

با استفاده از رویکردهای مبتنی بر بلاک چین، بازی‌ها در دراز مدت می‌توانند پایدار بمانند. اقلام درون بازی‌ها که به عنوان مجموعه‌های رمزنگاری صادر می‌شوند، می‌توانند ارزش واقعی پیدا کنند و در دنیای واقعی خرید و فروش شوند. امروزه بازی‌های بر بستر بلاک چین وجود دارند که از NFT استفاده می‌کنند. کاربران می‌توانند اقلامی که در این بازی درست کرده‌اند را به دیگران بفروشند.

### ۱۷/۳. سیستم بهداشت و درمان :

ذخیره‌سازی امن داده‌های پزشکی برای هر سیستم بهداشت و درمانی ضروری و مهم است. متکی بودن سیستم درمان به سرورهای متمرکز، آن را در موقعیت خطرناکی قرار می‌دهد. شفافیت و امنیت، تکنولوژی بلاک چین را به بهترین پلتفرم برای ذخیره داده‌های پزشکی تبدیل می‌کند.

بیماران با داشتن اطلاعات درمانی خود به صورت رمزنگاری شده در بلاک چین، می‌توانند هم‌زمان با این‌که حریم خوصی خود را حفظ می‌کنند، اطلاعات پزشکی خود را با هر موسسه درمانی به اشتراک بگذارند. اگر تمامی اعضای سیستم بهداشت و درمان کنونی دنیا در یک سیستم جهانی و امن حضور داشته باشند در اینصورت، جریان اطلاعات بین آن‌ها سریع‌تر گسترش خواهد یافت. این کار با استفاده از بلاک چین قابل انجام است و منجر به بهبود عملکرد سیستم درمان در دنیا خواهد شد.

### ۱۷/٤. انجام پرداخت های بین المللی :

انتقال پول در سطح بین‌المللی با بانکداری سنتی دردسرساز است. به دلیل وجود شبکه پیچیده‌ای از واسطه‌ها، استفاده از سیستم بانکی سنتی هزینه‌بر است و به کندی انجام می‌پذیرد. ارزهای دیجیتال و بلاک چین این واسطه‌ها را از بین می‌برند و انتقال سریع و ارزانی را در سرتاسر جهان تامین می‌کنند. بسیاری از پروژه‌های بلاک چینی از این فناوری برای ایجاد بستری در جهت انجام تراکنش‌های ارزان و تقریبا فوری بهره می‌گیرند. اگرچه گاهی اوقات برخی از ویژگی‌های اصلی بلاک چین مثل غیرمتمرکز بودن در آن‌ها نادیده گرفته می‌شود.

**۱۷/۵.ایجاد شناسنامه دیجیتال :**

مدیریت ایمن هویت افراد و موجودیت‌ها در اینترنت نیازمند یک راه‌حل سریع است. مقادیر بسیار زیادی از داده‌های شخصی ما بر روی سرورهای متمرکز ذخیره می‌شوند. این اطلاعات بدون توجه به رضایت ما توسط الگوریتم‌های هوش مصنوعی تجزیه و تحلیل می‌شود.

فناوری بلاک چین به کاربران اجازه می‌دهد تا مالکیت داده‌های خود را در اختیار داشته باشند. در این شبکه‌ها افراد می‌توانند هر اطلاعاتی که خودشان می‌خواهند با بقیه به اشتراک بگذارند و بقیه داده‌ها همچنان خصوصی بماند. این اتفاق معجزه رمزنگاری است که می‌تواند بدون آسیب رساندن به حریم خصوصی افراد، تجربه‌ای روان برای آن‌ها در فضای آنلاین ایجاد کند. با گسترش روزافزون استفاده از شبکه‌های اجتماعی، اهمیت این موضوع بیشتر از همیشه شده است.

## ۱۸. نتیجه گیری

بلاک چین یک فناوری نوین به شمار می‌آید که هدف آن ذخیره‌سازی و انتقال هر نوع داده به صورت غیرمتمرکز است. در این سیستم گره‌ها وظیفه تایید و ثبت تراکنش‌ها را دارند. این گره‌ها در سرتاسر دنیا توزیع شده‌اند و برای انجام درست وظایف خود، از الگوریتم‌های اجماع استفاده می‌کنند. امنیت شبکه بلاک چین حاصل استفاده از ایده‌های مبتکرانه در حوزه رمزنگاری و اقتصاد است. در این مقاله علاوه بر بررسی تمام جنبه‌های فنی و عملی بلاک چین کاربردهای بلاک چین در حوزه‌های مختلف شرح داده شده است.

## منابع :


- https://blog.faradars.org
- https://wallex.ir
- https://blog.nobitex.ir
- https://fa.wikipedia.org