به نام خدا

گزارش مقالات

موضوع: بلاکچین

نام و نام خانوادگی: سید محمد حسین طباطبائی

نام استاد: سرکار خانم دکتر مریم لطفی

درس: سیستم های توزیع شده

فهرست مطالب

مقدمه

بلاکچین یک فناوری دفتر کل توزیع‌شده و غیرمتمرکز است که امکان ثبت تراکنش‌های دیجیتال را به‌صورت ایمن، شفاف و غیرقابل‌دستکاری فراهم می‌کند. برخلاف سیستم‌های متمرکز سنتی، بلاکچین نیاز به واسطه‌هایی مانند بانک‌ها یا مؤسسات مالی را از بین می‌برد و تراکنش‌های همتا به همتا را به‌طور مستقیم امکان‌پذیر می‌سازد.[1] این تغییر اساسی در پردازش تراکنش‌ها از طریق تکنیک‌های رمزنگاری، مکانیسم‌های اجماع و شبکه‌ای از گره‌های توزیع‌شده که به‌طور جمعی تراکنش‌ها را اعتبارسنجی و ثبت می‌کنند، تحقق می‌یابد.

مفهوم بلاکچین نخستین بار در وایت‌پیپر بیت‌کوین معرفی شد تا مشکل دوبار خرج کردن را در ارزهای دیجیتال حل کند و اطمینان حاصل شود که یک دارایی دیجیتال نمی‌تواند بیش از یک‌بار خرج شود، آن هم بدون نیاز به نظارت یک نهاد مورد اعتماد. [2] بلاکچین بیت‌کوین به‌عنوان یک دفتر کل غیرقابل‌تغییر عمل می‌کند، به این صورت که تراکنش‌ها در بلوک‌هایی گروه‌بندی شده، به‌صورت رمزنگاری‌شده به هم متصل شده و در یک شبکه غیرمتمرکز ذخیره می‌شوند. با گذر زمان، فناوری بلاکچین فراتر از بیت‌کوین تکامل یافت و به توسعه پلتفرم‌های پیشرفته‌تری مانند اتریوم منجر شد که قراردادهای هوشمند را معرفی کرد.[3]

بلاکچین دارای چند ویژگی کلیدی است :

- غیرمتمرکز بودن: به این معنا که هیچ نهاد واحدی کنترل کامل شبکه را در اختیار ندارد.
- تغییرناپذیری: به این معنا که داده‌های ثبت‌شده در آن را نمی‌توان به‌صورت بازگشتی تغییر داد.
- شفافیت: به این معنا که تراکنش‌ها به‌طور عمومی قابل‌تأیید هستند.
- امنیت: از طریق الگوریتم‌های رمزنگاری و پروتکل‌های اجماع تأمین می‌شود.[1]

این ویژگی‌ها بلاکچین را به ابزاری قدرتمند برای کاربردهایی فراتر از ارزهای دیجیتال تبدیل کرده‌اند، از جمله مدیریت زنجیره تأمین، احراز هویت دیجیتال، خدمات مالی و سیستم‌های حاکمیتی.[3]

با وجود مزایای فراوان، فناوری بلاکچین با چالش‌های مهمی، به‌ویژه در مقیاس‌پذیری و کارایی مواجه است. شبکه‌هایی مانند بیت‌کوین و اتریوم در مقایسه با سیستم‌های مالی سنتی مانند ویزا، که قادر به پردازش هزاران تراکنش در ثانیه است، با محدودیت توان عملیاتی روبه‌رو هستند.[2] علاوه بر این، با رشد بلاکچین، نیاز به ذخیره‌سازی و پردازش افزایش می‌یابد که می‌تواند منجر به تمرکزگرایی شود، چراکه تعداد کمتری از گره‌ها قادر به حفظ کل دفتر کل خواهند بود.[3] همچنین، آسیب‌پذیری‌های امنیتی مانند حملات ٪۵۱ (که در آن یک موجودیت واحد اکثریت کنترل شبکه را به دست می‌آورد) و استخراج خودخواهانه (که در آن ماینرها با تغییر استراتژی‌های استخراج، پاداش‌های بیشتری دریافت می‌کنند) می‌توانند یکپارچگی بلاکچین را به خطر بیندازند.[1]

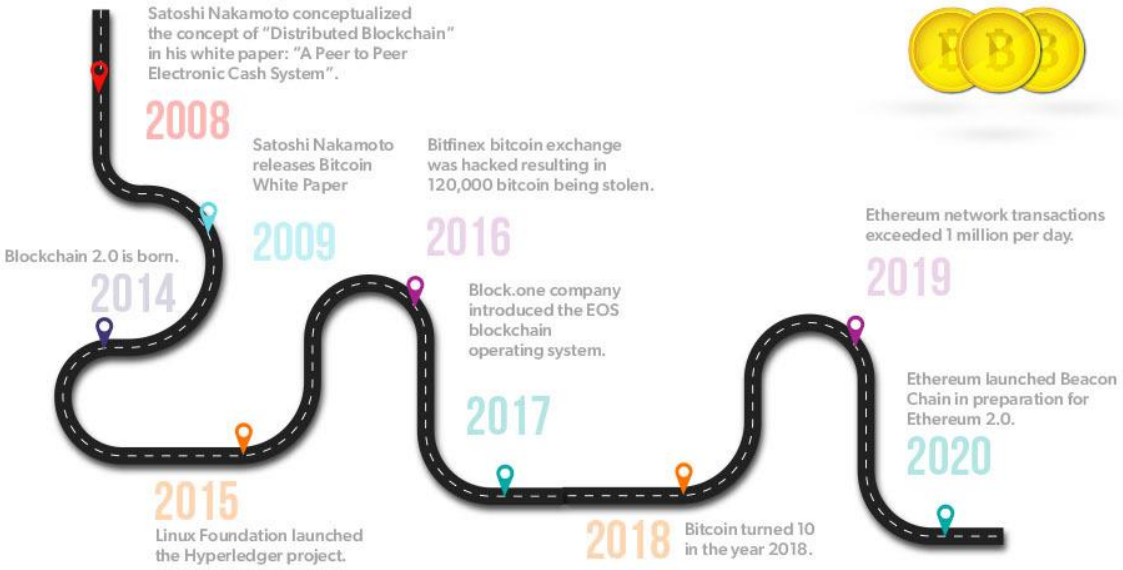
با گسترش پذیرش بلاکچین، تحقیقات و نوآوری‌ها بر حل این محدودیت‌ها متمرکز شده‌اند، از جمله الگوریتم‌های اجماع جدید، راهکارهای مقیاس‌پذیری لایه دوم و پروتکل‌های هم‌کنش‌پذیری. هدف اصلی، بهبود کارایی، امنیت و قابلیت استفاده بلاکچین در صنایع مختلف است.

تاریخچه پیدایش بلاکچین: از نیاز تا نوآوری

پیش از ظهور بلاکچین، سیستم‌های دیجیتال برای پرداخت‌های مالی و انتقال ارزش به شدت، به واسطه‌های متمرکز مانند بانک‌ها و پردازشگرهای پرداخت وابسته بودند. این مدل سنتی، اگرچه کارآمد به نظر می‌رسید، اما چالش‌های بزرگی را به همراه داشت:

- وابستگی به یک مرجع مرکزی: بانک‌ها و مؤسسات مالی به عنوان واسطه‌های اصلی عمل می‌کردند که باعث سرعت پایین پردازش، هزینه‌های بالا و نیاز به اعتماد به یک نهاد واحد می‌شد.
- ریسک تقلب و هک: اطلاعات مالی کاربران در پایگاه‌های داده متمرکز ذخیره می‌شدند که در برابر حملات سایبری و نقض داده‌ها آسیب‌پذیر بودند.
- مشکل دوبار خرج کردن: در سیستم‌های دیجیتال، یک کاربر می‌توانست بدون نظارت مناسب، یک واحد پولی را چندین بار خرج کند .راه‌حل این مشکل، نیاز به یک نهاد متمرکز برای تأیید تراکنش‌ها داشت.

در سال ۲۰۰۸، ساتوشی ناکاموتو مقاله‌ای منتشر کرد که راه‌حلی برای اعتماد در سیستم‌های مالی دیجیتال ارائه داد، شامل یک دفتر کل غیرمتمرکز و تغییرناپذیر برای ثبت تراکنش‌ها، استفاده از الگوریتم اثبات کار (PoW) برای تأیید تراکنش‌ها بدون واسطه و بهره‌گیری از رمزنگاری کلید عمومی برای افزایش امنیت. یک سال بعد، در ۲۰۰۹، اولین بلاک بیت‌کوین استخراج شد و این فناوری توانست مشکل دوبار خرج کردن را بدون نیاز به نهاد مرکزی حل کند.



شکل 1.1 – تاریخچه بلاکچین

معماری بلاکچین

هر تراکنش در بلاکچین یک واحد اطلاعاتی است که در بلاک‌های عمومی ذخیره می‌شود. این تراکنش‌ها غیرقابل تغییر هستند. امضای دیجیتال (ECDSA) امنیت تراکنش‌ها را تضمین می‌کند، به طوری که جعل امضا تقریباً غیرممکن است. برای اعتبارسنجی، ماینرها مقدار موجودی فرستنده را بررسی کرده و از دفتر کل برای جلوگیری از دوبار خرج کردن (Double Spending) استفاده می‌کنند.

ساختار بلاک

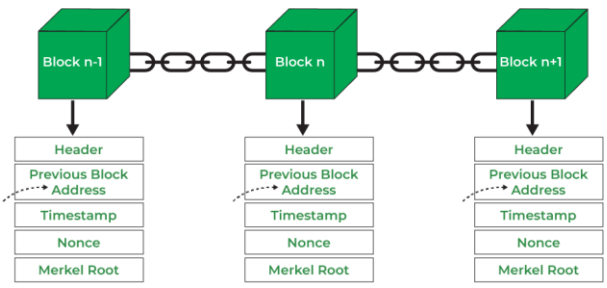
هر بلاک شامل یک هدر و یک بدنه است. هدر بلاک شامل متادیتاهایی مانند هش بلاک قبلی، ریشه درخت مرکل، زمان‌بندی و nonceاست. بدنه بلاک شامل تعداد تراکنش‌ها و جزئیات آن‌ها است. امنیت بلاکچین با استفاده از رمزنگاری نامتقارن و امضاهای دیجیتال تضمین می‌شود.

ویژگی‌های کلیدی بلاکچین

1. غیرمتمرکز بودن: تراکنش‌ها بدون نیاز به تأیید نهاد مرکزی انجام می‌شوند.
2. ماندگاری: تغییر یک تراکنش نیازمند تغییر تمام بلاک‌های بعدی است که تقریباً غیرممکن است.
3. ناشناس بودن: کاربران می‌توانند بدون افشای هویت خود از بلاکچین استفاده کنند.
4. قابلیت حسابرسی: تمام تراکنش‌ها در یک دفتر کل عمومی ثبت شده و قابل بررسی هستند.

انواع بلاکچین

1. عمومی: مانند بیت‌کوین و اتریوم که هر فردی می‌تواند در آن شرکت کند.
2. خصوصی: کنترل‌شده توسط یک سازمان خاص با دسترسی محدود.
3. کنسرسیوم: ترکیبی از بلاکچین عمومی و خصوصی، جایی که چندین سازمان مدیریت آن را برعهده دارند.



شکل 1.2 – ساختار هر بلاک در بلاکچین

مقایسه بلاکچین و سیستم‌های توزیع‌شده: تفاوت‌ها و شباهت‌ها

سیستم‌های توزیع‌شده و بلاکچین هر دو مبتنی بر مفاهیم عدم تمرکز و همکاری چندین گره برای انجام وظایف مشخص هستند. در سیستم‌های توزیع‌شده، هدف اصلی افزایش کارایی، مقیاس‌پذیری و تحمل خطاست، به‌طوری‌که چندین گره با همکاری یکدیگر، به‌عنوان یک سیستم یکپارچه عمل کنند. در مقابل، بلاکچین نوع خاصی از سیستم‌های توزیع‌شده است که تمرکز آن بر امنیت، شفافیت و تغییرناپذیری داده‌هاست. بلاکچین با استفاده از الگوریتم‌های اجماع، تضمین می‌کند که همه گره‌ها روی یک نسخه معتبر از داده‌ها توافق داشته باشند، در حالی که در سیستم‌های توزیع‌شده عمومی، ممکن است مدل‌های هماهنگی متفاوتی مانند اشتراک داده یا تقسیم وظایف وجود داشته باشد.

ویژگی	سیستم‌های توزیع‌شده	بلاکچین
تمرکززدایی	نسبی، بسته به معماری	کاملاً غیرمتمرکز (در حالت عمومی)
هدف اصلی	افزایش کارایی و قابلیت اطمینان	شفافیت، امنیت و تغییرناپذیری
مدیریت داده	معمولاً دارای کنترل مرکزی یا هماهنگی بین گره‌ها	داده‌ها تغییرناپذیر و توزیع‌شده بین گره‌ها
مکانیزم هماهنگی	مدل‌های مختلف مانند پیام‌رسانی، قفل توزیع‌شده	الگوریتم‌های اجماع مانندPoW ، PoS
تحمل خطا	وابسته به پروتکل‌های استفاده‌شدهRAFT ، Paxos	مقاوم در برابر حملات از طریق توزیع‌شدگی و اجماع
مثال‌ها	Google Cloud, Hadoop, Microservices	Bitcoin, Ethereum, Hyperledger

جدول 1.1 - تفاوت‌های کلیدی سیستم های توزیع شده و بلاکچین

با توجه به مقایسه انجام‌شده، می‌توان گفت که بلاکچین یک نوع خاص از سیستم‌های توزیع‌شده است که با هدف افزایش امنیت، شفافیت و تغییرناپذیری داده‌ها طراحی شده است. در حالی که سیستم‌های توزیع‌شده به دنبال بهینه‌سازی عملکرد، مقیاس‌پذیری و تحمل خطا هستند، بلاکچین تمرکز بیشتری بر حذف نیاز به اعتماد به یک نهاد مرکزی و ایجاد اجماع بین گره‌های مستقل دارد.

هرچند بلاکچین مزایای مهمی مانند مقاومت در برابر دستکاری و تمرکززدایی دارد، اما هزینه‌های پردازشی بالاتر و محدودیت‌هایی در مقیاس‌پذیری نسبت به برخی سیستم‌های توزیع‌شده سنتی دارد. بنابراین، انتخاب بین این دو بستگی به نیازهای خاص یک سیستم دارد؛ اگر هدف، کارایی بالا و توزیع وظایف میان گره‌ها باشد، سیستم‌های توزیع‌شده گزینه مناسب‌تری هستند، اما اگر امنیت، شفافیت و تغییرناپذیری داده‌ها در اولویت باشد، بلاکچین انتخاب بهتری خواهد بود.[4]

انواع بلاکچین‌ها

بلاکچین‌ها به دو نوع بلاکچین‌های بدون مجوز و بلاکچین‌های مجوزدار تقسیم می‌شوند.

- بلاکچین‌های بدون مجوز(Permissionless)

این بلاکچین‌ها هیچ محدودیتی برای دسترسی نودها ایجاد نمی‌کنند. هر کسی می‌تواند داده‌ها را بخواند، بررسی کند و در فرآیند تایید تراکنش‌ها شرکت کند. از ویژگی‌های مهم این بلاکچین‌ها غیرمتمرکز بودن و شفافیت است .بیت‌کوین و اتریوم از جمله نمونه‌های این نوع بلاکچین هستند. با این حال، سرعت تراکنش‌ها در آن‌ها پایین‌تر از بلاکچین‌های مجوزدار است.[3]

- بلاکچین‌های مجوزدار(Permissioned)

در این بلاکچین‌ها، تنها گروهی خاص از شرکت‌کنندگان اجازه نوشتن داده‌ها را دارند. این نوع بلاکچین‌ها بیشتر برای کسب‌وکارها و سیستم‌های اجتماعی کاربرد دارند و بر اساس نیاز می‌توانند باز یا بسته باشند. در بلاکچین‌های مجوزدار باز، همه می‌توانند داده‌ها را بخوانند، اما در بلاکچین‌های مجوزدار بسته، داده‌ها تنها برای شرکت‌کنندگان خاص قابل مشاهده است.[3] این نوع بلاکچین‌ها به‌طور معمول در سیستم‌های هویتی یا گواهی‌نامه‌های علمی کاربرد دارند.

مزایا و محدودیت‌ها

ایده اولیه معرفی مفهوم بلاکچین برای از بین بردن تمرکزگرایی و افزودن شفافیت برای همگان جهت خواندن و به‌روزرسانی داده‌ها بوده است. بلاکچین‌های مجوزدار باز بیشتر به این اصل شفافیت پایبند هستند، اگرچه در نوشتن داده‌ها کمی متمرکزتر هستند و می‌توانند برای سیستم‌های هویتی، سیستم‌های گواهی‌نامه‌های علمی و موارد مشابه مفید باشند، جایی که هر کسی می‌تواند داده‌ها را بخواند اما تنها یک مجموعه خاص از شرکت‌کنندگان مجاز به نوشتن داده‌ها به بلاکچین هستند.

بلاکچین‌های مجوزدار بسته کاملاً متمرکز هستند و همچنین به هیچ کس شفاف نیستند، که این امر هسته مفهوم بلاکچین را تضعیف می‌کند. بنابراین، این بلاکچین‌ها می‌توانند با سیستم‌های دیتابیس توزیع‌شده با محدودیت‌های اعمال‌شده جایگزین شوند.

شکل 1.3 – تفاوت بلاکچین های مجوزدار و بدون مجوز

الگوریتم‌های اجماع در بلاکچین

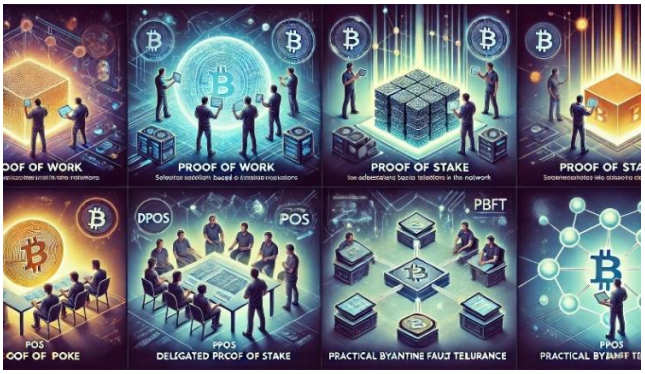
در بلاکچین، حل مشکل اجماع بین نودهای غیرقابل‌اعتماد، تبدیل‌شده‌ای از مشکل ژنرال‌های بیزانسی است. در این مشکل، گروهی از ژنرال‌ها که بخشی از ارتش بیزانسی را فرماندهی می‌کنند، برای حمله به یک شهر نیاز به هماهنگی دارند. اگر تنها بخشی از آنها حمله کنند، حمله شکست خواهد خورد. ژنرال‌ها باید با یکدیگر ارتباط برقرار کنند تا تصمیمی مشترک در مورد حمله یا عدم حمله بگیرند، در حالی که ممکن است تعدادی خائن در بین آنها وجود داشته باشد که اطلاعات مختلفی به دیگران ارسال کنند. این مشکل در دنیای بلاکچین مشابه است، جایی که نودها نیازی به اعتماد به یکدیگر ندارند و باید به شکلی مطمئن به اجماع برسند.[2]

الگوریتم‌های اجماع مکانیسم‌هایی هستند که در آن‌ها نودهای شبکه بلاکچین برای تأیید اعتبار و اصالت تراکنش‌ها یا بلاک‌ها به توافق می‌رسند. چون دفتر کل تراکنش‌های بلاکچین متمرکز نیست، اجماع باید به‌گونه‌ای تضمین شود که بلاک جدید تنها نسخه معتبر باشد و از حمله‌های دشمنانه جلوگیری شود. این الگوریتم‌ها دو هدف دارند: اول تأیید بلاک که تنها نسخه درست آن در سیستم پذیرفته شود و دوم جلوگیری از منحرف کردن زنجیره توسط حملات. [2]

برای حل این مشکل، الگوریتم‌های مختلفی پیشنهاد شده‌اند که به‌طور کلی به روش‌هایی برای واگذاری و پاداش‌دهی به تأیید تراکنش‌ها یا بلاک‌ها تمرکز دارند. برخی از این الگوریتم‌ها شامل اثبات کار(Proof of Work) ، اثبات سهام(Proof of Stake) ، اثبات اهمیت(Proof of Importance) ، گراف جهت‌دار غیرمدور (DAG) و عملکرد بهینه تحمل خطای بیزانسی هستند. هر کدام از این الگوریتم‌ها به شیوه‌های مختلفی سعی در حل مشکل اجماع دارند.[3]

الگوریتم اجماع اثبات کار(Proof of Work - PoW)

الگوریتم اثبات کار (PoW) مکانیزمی است که در آن ماینرها برای ایجاد بلاک جدید، یک معمای رمزنگاری پیچیده را حل می‌کنند. این فرایند نیازمند محاسبات سنگین است، اما تأیید آن برای سایر نودها آسان بوده و امنیت شبکه را تضمین می‌کند. ماینرها پس از یافتن مقدار nonce مناسب، بلاک را به شبکه ارسال کرده و در صورت تأیید، پاداش بلاک و کارمزد تراکنش‌ها را دریافت می‌کنند. میزان سختی استخراج با Difficulty Adjustment تنظیم شده تا میانگین زمان تولید بلاک ثابت بماند. از چالش‌های PoWمی‌توان به مصرف بالای انرژی، تمرکزگرایی استخراج و خطر حمله ٪۵۱ اشاره کرد. برای کاهش این مشکلات، روش‌هایی مانند اثبات سوزاندن (PoB) و به‌کارگیری محاسبات PoW در مسائل علمی پیشنهاد شده‌اند.[3][2][1]



شکل1.4 – انواع الگوریتم های اجماع در بلاکچین

الگوریتم اثبات سهام(Proof of Stake - PoS)

الگوریتم اثبات سهام (PoS) یک مکانیزم اجماع است که در آن والیدیتورها با استیک کردن دارایی خود، شانس ایجاد و تأیید بلاک‌ها را به دست می‌آورند. برخلاف اثبات کار(PoW) ، این روش نیازی به محاسبات سنگین و مصرف بالای انرژی ندارد، بلکه بر اساس میزان استیک کاربران، والیدیتورها را انتخاب می‌کند. این ویژگی باعث افزایش کارایی و کاهش مصرف انرژی می‌شود، اما ممکن است منجر به تمرکز ثروت و قدرت در دست نودهای بزرگ‌تر شود. یکی از چالش‌هایPoS ، مشکل "هیچ چیزی در خطر نیست " (Nothing-at-Stake)است که پروتکل‌هایی مانند Casper اتریوم با اعمال مجازات برای رفتارهای مخرب تلاش در حل آن دارند. بلاکچین‌هایی مانند Blackcoin، Peercoin و Nxt از این الگوریتم استفاده می‌کنند و اتریوم نیز در حال انتقال به PoS برای بهبود امنیت و کارایی شبکه است.[3][2][1]

الگوریتم اثبات سهام واگذاری(Delegated Proof of Stake - DPoS)

الگوریتم اثبات سهام واگذاری‌شده (DPoS) که توسط دانیل لاریمر توسعه یافت، نسخه‌ای اصلاح‌شده از PoS است که در آن نودها از طریق رأی‌گیری، وظیفه اعتبارسنجی تراکنش‌ها را به شاهدان (witnesses) واگذار می‌کنند. این روش با کاهش تعداد تولیدکنندگان بلاک، منجر به سرعت بالاتر پردازش تراکنش‌ها و مقیاس‌پذیری بیشتر نسبت به PoW و PoS می‌شود. با این حال، خطر تمرکزگرایی در آن وجود دارد، زیرا نودهای با سهم بیشتر می‌توانند به‌راحتی به عنوان تولیدکننده بلاک انتخاب شوند. در صورت رفتار مخرب، سهامداران می‌توانند شاهدان را برکنار کنند. از مزایای این الگوریتم مصرف کمتر منابع محاسباتی و امکان جایگزینی سریع نودهای نامعتبر است، اما انتقادات زیادی به تمرکزگرایی آن وارد شده است. بلاکچین‌هایEOS ، BitShares، Steemit و Liskاز این الگوریتم استفاده می‌کنند.[3][2][1]

الگوریتم تحمل خطای بیزانسی عملی(Practical Byzantine Fault Tolerance - pBFT)

الگوریتم تحمل خطای بیزانسی عملی (pBFT) که توسط میگل کسترو و باربارا لیسکوف معرفی شد، یک مکانیزم اجماع مقاوم در برابر نودهای مخرب است که در بلاکچین‌های مجوزدار مانند Hyperledger Fabric و Zilliqa استفاده می‌شود. در این الگوریتم، یک نود رهبر وظیفه پردازش درخواست‌ها را بر عهده دارد و سایر نودها به عنوان پشتیبان عمل می‌کنند. اجماع از طریق رای‌گیری چندمرحله‌ای انجام می‌شود و برای تأیید هر بلاک، بیش از دو سوم نودها باید موافق باشند. pBFT در محیط‌های غیرهمزمان عملکرد سریعی دارد، مصرف انرژی کمتری نسبت به PoW دارد و برای بلاکچین‌های خصوصی و مجوزدار مناسب است. از دیگر کاربردهای این الگوریتم می‌توان به Stellar و (Antshares) DBFT اشاره کرد.[3][2][1]

کاربردهای بلاکچین

بلاکچین به‌عنوان یک فناوری می‌تواند در حوزه‌های مختلفی از جمله سلامت، رای‌گیری، مدیریت هویت، حاکمیت، زنجیره تأمین و منابع انرژی استفاده شود. این تکنولوژی نه تنها در زمینه پول الکترونیکی مانند بیت‌کوین موفق بوده است، بلکه پیش‌بینی می‌شود که تأثیرات آن در آینده بر دنیای دیجیتال مشابه اینترنت باشد. بلاکچین به دلیل ویژگی‌های غیرقابل تغییر و توزیع‌شده‌اش، قادر به ارائه راه‌حل‌های نوین در زمینه‌های مختلف است و به همین دلیل پژوهش‌های گسترده‌ای در حال انجام است تا کاربردهای بیشتری از آن کشف شود.[2]

خدمات مالی و بانکداری

بلاکچین به‌طور گسترده در صنعت مالی مورد استفاده قرار گرفته و امکان انجام پرداخت‌های بین‌المللی سریع‌تر و ارزان‌تر، تجارت سهام، مدیریت وام‌دهی و حسابرسی را فراهم کرده است. به گفته‌ی مجمع جهانی اقتصاد، انتظار می‌رود تا سال ۲۰۲۵ حدود ۱۰٪ از تولید ناخالص داخلی جهانی بر بستر بلاکچین ذخیره شود.

مدیریت زنجیره تأمین و لجستیک

شفافیت و تغییرناپذیری بلاکچین باعث شده است که بسیاری از شرکت‌ها از این فناوری برای رهگیری کالاها و جلوگیری از تقلب استفاده کنند. ترکیب بلاکچین با فناوری‌هایی مانند RFID و GPS می‌تواند داده‌های دقیق از مسیر انتقال کالاها را در اختیار تولیدکنندگان، تأمین‌کنندگان و مشتریان قرار دهد.

رأی‌گیری الکترونیکی

بلاکچین با ایجاد یک دفتر کل تغییرناپذیر و شفاف، می‌تواند امنیت و اعتماد در انتخابات را افزایش دهد. در ایالات متحده، ایالت ویرجینیای غربی از بلاکچین برای رأی‌گیری الکترونیکی در انتخابات میان‌دوره‌ای ۲۰۱۸ استفاده کرد، هرچند این سیستم هنوز نیاز به بهبود دارد.

بهداشت و درمان

بلاکچین می‌تواند یک سیستم امن و شفاف برای مدیریت سوابق پزشکی ایجاد کند. به‌عنوان مثال، سیستم MedChain مبتنی بر Hyperledger Fabric به بیماران امکان می‌دهد کنترل کاملی بر داده‌های پزشکی خود داشته باشند و آن را با پزشکان منتخب به اشتراک بگذارند.

قراردادهای هوشمند

قراردادهای هوشمند از جمله مهم‌ترین نوآوری‌های بلاکچین هستند که امکان اجرای خودکار توافقات را بدون نیاز به واسطه‌ها فراهم می‌کنند .این قراردادها بر روی بلاکچین‌هایی مانند اتریوم، زلیکا و EOS پیاده‌سازی می‌شوند و می‌توانند در حوزه‌هایی مانند بیمه، املاک، تجارت و خدمات حقوقی مورد استفاده قرار گیرند.[3][2][1]

چالش‌ها و مشکلات بلاکچین

فناوری بلاکچین علی‌رغم پتانسیل بالای خود، هنوز با چالش‌های متعددی روبرو است که مانع از پذیرش گسترده آن شده‌اند. این چالش‌ها را می‌توان به دسته‌های فنی، اقتصادی، نظارتی و امنیتی تقسیم کرد. در ادامه، مهم‌ترین مشکلات بلاکچین مورد بررسی قرار می‌گیرد.

مقیاس‌پذیری (Scalability) 📈

یکی از بزرگ‌ترین مشکلات بلاکچین، محدودیت در مقیاس‌پذیری است. به‌عنوان مثال، بیت‌کوین می‌تواند بین ۳ تا ۷ تراکنش در ثانیه پردازش کند، در حالی که اتریوم حدود ۱۵ تراکنش در ثانیه را پردازش می‌کند. این میزان در مقایسه با سیستم‌هایی مانند ویزا که توان پردازش ۲۴,۰۰۰ تراکنش در ثانیه را دارد، بسیار کم است. تلاش‌هایی مانند افزایش اندازه بلاک (Bitcoin Cash) ، استفاده از شاردینگ (Sharding)، و توسعه‌ی لایه دوم (مانند شبکه‌ی لایتنینگ) برای حل این مشکل پیشنهاد شده‌اند.

مصرف بالای انرژی (Energy Consumption) 🔋

مکانیزم‌های اجماع مانند اثبات کار (PoW) که در بیت‌کوین و بسیاری از ارزهای دیجیتال استفاده می‌شوند، نیاز به توان محاسباتی بسیار بالایی دارند. مصرف برق شبکه بیت‌کوین در برخی موارد با مصرف برق یک کشور کوچک برابری می‌کند. این موضوع باعث نگرانی‌های زیست‌محیطی شده و برخی کشورها مانند چین، استخراج ارزهای دیجیتال را ممنوع کرده‌اند. روش‌های جایگزینی مانند اثبات سهام (PoS) و اثبات اعتبار (Proof of Authority - PoA) برای کاهش مصرف انرژی پیشنهاد شده‌اند.

امنیت و حملات شبکه (Security and Network Attacks) 🔐

علی‌رغم امنیت بالای بلاکچین، هنوز تهدیداتی مانند حمله ۵۱٪ وجود دارند که طی آن، اگر گروهی از ماینرها بیش از ۵۰٪ قدرت پردازشی شبکه را در اختیار داشته باشند، می‌توانند تراکنش‌ها را تغییر دهند. سایر حملات شامل استخراج خودخواهانه، حملات دوبار خرج کردن و حملات سایبری به کیف پول‌ها و قراردادهای هوشمند هستند.

مشکلات حریم خصوصی (Privacy Concerns) 🔒

با اینکه بلاکچین داده‌ها را به‌صورت رمزنگاری‌شده ذخیره می‌کند، اما همچنان مشکلاتی در زمینه‌ی حریم خصوصی وجود دارد. در بلاکچین‌های عمومی، همه کاربران می‌توانند تاریخچه‌ی تراکنش‌ها را مشاهده کنند، که می‌تواند منجر به شناسایی هویت کاربران شود. برخی راهکارها مانند استفاده از تراکنش‌های محرمانه (Confidential Transactions) و شبکه‌های خصوصی بلاکچین برای رفع این مشکل پیشنهاد شده‌اند.

نتیجه‌گیری

فناوری بلاکچین به‌عنوان یکی از مهم‌ترین نوآوری‌های قرن ۲۱، توانسته است تحولی عمیق در شیوه ذخیره، پردازش و تبادل اطلاعات ایجاد کند. این فناوری با ارائه یک دفتر کل توزیع‌شده و غیرمتمرکز، نیاز به واسطه‌های سنتی را کاهش داده و اعتماد را از طریق رمزنگاری و مکانیسم‌های اجماع جایگزین کرده است. در ابتدا، بلاکچین به‌عنوان زیربنای ارزهای دیجیتال مانند بیت‌کوین مطرح شد، اما به مرور زمان، کاربردهای آن در حوزه‌های مختلف از جمله خدمات مالی، مدیریت زنجیره تأمین، قراردادهای هوشمند، رأی‌گیری الکترونیکی، احراز هویت دیجیتال و صنعت سلامت گسترش یافت.

یکی از ویژگی‌های کلیدی بلاکچین، تغییرناپذیری و شفافیت داده‌ها است که امکان تقلب و دستکاری اطلاعات را به‌شدت کاهش می‌دهد. این فناوری همچنین می‌تواند با افزایش امنیت و کاهش هزینه‌های پردازشی، سرعت و کارایی تراکنش‌ها را بهبود بخشد. بااین‌حال، بلاکچین هنوز با چالش‌های متعددی روبه‌روست که مانع از پذیرش گسترده آن در سطح جهانی شده است.

یکی از مهم‌ترین موانع، مقیاس‌پذیری پایین شبکه‌های بلاکچینی است. در حالی که سیستم‌های مالی سنتی مانند ویزا قادر به پردازش هزاران تراکنش در ثانیه هستند، بلاکچین‌هایی مانند بیت‌کوین و اتریوم همچنان از محدودیت‌های سرعت و کارمزدهای بالا رنج می‌برند. علاوه بر این، مکانیسم‌های اجماع مبتنی بر اثبات کار (PoW) مصرف انرژی بالایی دارند که باعث ایجاد نگرانی‌های زیست‌محیطی شده است. از طرفی دیگر، تهدیدات امنیتی مانند حمله ٪۵۱، ضعف‌های قراردادهای هوشمند و مشکلات مربوط به حریم خصوصی همچنان به‌عنوان چالش‌های جدی مطرح هستند.

برای غلبه بر این موانع، نوآوری‌هایی در حال توسعه هستند که می‌توانند کارایی، امنیت و مقیاس‌پذیری بلاکچین را بهبود بخشند. راهکارهایی مانند شاردینگ(Sharding) ، شبکه‌های لایه دوم (مانند لایتنینگ)، استفاده از الگوریتم‌های اجماع کارآمدتر مانند اثبات سهام(PoS) ، تراکنش‌های محرمانه و بلاکچین‌های ترکیبی (کنسرسیوم و خصوصی) از جمله تلاش‌هایی هستند که می‌توانند زمینه را برای پذیرش گسترده‌تر این فناوری فراهم کنند.

در نهایت، بلاکچین پتانسیل آن را دارد که در آینده به یک زیرساخت کلیدی در اقتصاد دیجیتال، مدیریت داده‌ها و سیستم‌های غیرمتمرکز تبدیل شود. با پیشرفت‌های مداوم در زمینه الگوریتم‌های اجماع، بهینه‌سازی مصرف انرژی و افزایش سرعت پردازش، بلاکچین می‌تواند نه‌تنها محدودیت‌های فعلی خود را کاهش دهد، بلکه به‌عنوان یک فناوری بنیادین برای تحول در تعاملات دیجیتالی، امنیت اطلاعات و مدیریت اعتماد در سراسر جهان مورد استفاده قرار گیرد.

منابع

1. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges
2. A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities
3. A Survey on Blockchain Technology Concepts, Applications, and Issues
4. chatgpt.com
5. CFTE
6. wikipedia.org
7. perplexity.ai

با سپاس از توجه و زمانی که صرف بررسی این گزارش نمودید

پایان