مروری بر الگوریتم‌های اجماع در بلاکچین

جمیله بحری*[1] و حمیدرضا شایق بروجنی[2]

[1]کارشناسی ارشد، دانشگاه تربیت دبیر شهید رجایی، گروه مهندسی کامپیوتر، تهران، ایران
j.bahri@sru.ac.ir

[2]استادیار، دانشگاه تربیت دبیر شهید رجایی، گروه مهندسی کامپیوتر، تهران، ایران
h.shayegh@sru.ac.ir

چکیده

فناوری بلاکچین یک ساختار داده ذخیره‌سازی غیرمتمرکز، مبتنی بر زنجیره‌ای از بلاک‌های داده‌ای مرتبط به یکدیگر است. بلاکچین بدون نیاز به اعتماد به واسطه‌ها طی یک ساز و کار رقابتی یا رأی‌گیری، بلاک‌های جدید را در دفترکل ذخیره می‌کند. به‌دلیل ساختار زنجیره‌ای یا گراف بین هر بلاک با بلاک‌های قبلی خود، تغییر داده‌های بلاکچین غیرممکن است. معماری بلاکچین، اعتماد را در یک شبکهٔ نظیربه‌نظیر و بدون واسطه از طریق گره‌های داخل شبکه و طبق الگوریتم‌های مختلف اجماع ایجاد می‌کند. در این مقاله قصد داریم، سازوکار هر یک از الگوریتم‌های اجماع مبتنی بر اثبات، مبتنی بر رأی‌گیری و مبتنی بر گراف جهت‌دار بدون دور را شرح دهیم.

واژگان کلیدی: بلاکچین، اجماع، سامانه‌های غیرمتمرکز، ارز دیجیتال

۱- مقدمه

بلاکچین به‌عنوان یک سامانه غیرمتمرکز، که درواقع یک ساختار داده است که توسط گره‌هایی که به یکدیگر اعتماد ندارند، نگه‌داری می‌شود. بلاکچین به شکل چارچوبی برای پردازش داده‌ها عمل و تمامی حالات معاملات را نگه‌داری می‌کند و تمام گره‌ها در سیستم روی آن معامله و ترتیب معاملات در بلاکچین توافق دارند. نام‌گذاری بلاک‌چین به‌نحوی معرف شیوهٔ ذخیره داده‌های معاملات است که در آن هر بلاک از طریق یک اشاره‌گر به بلاک قبلی خود متصل است و مانع از تغییر بلاک و یا ایجاد بلاکی بین دو بلاک موجود می‌شود و بدین طریق اعتماد را در یک شبکهٔ نظیربه‌نظیر و بدون واسطه فراهم می‌کند، زیرا هر آنچه در دفترکل بلاکچین ذخیره شود، غیرقابل تغییر و برای همگان شفاف است؛ بنابراین پروتکل‌های مختلفی برای ایجاد اعتماد در سامانه‌های غیرمتمرکز از طریق اجماع پیشنهاد شده است که در ادامه این مقاله توضیح داده می‌شوند.

۱-۱- مفاهیم کلیدی

جهت درک بهتر مفاهیم فناوری بلاکچین، در ابتدا مفاهیم کلیدی از جمله دفترکل توزیع‌شده، اجماع، قرارداد هوشمند، رمزنگاری، اررزمز، دارایی دیجیتال، امضای دیجیتال، درهم‌سازی، مسألهٔ Mining و مسألهٔ Fork شرح داده می‌شود.

۱-۲- دفترکل توزیع شده

یک دفترکل، ساختمان داده‌ای شامل یک فهرست مرتب از معاملات است. برای مثال یک دفترکل ممکن است، معاملات پولی بین چندین بانک یا کالاهای مبادله‌شده بین بخش‌های مختلف را ثبت کند. در بلاکچین دفترکل روی تمام گره‌ها تکثیر می‌شود. علاوه‌براین معاملات در بلاک‌هایی دسته‌بندی و سپس باهم زنجیر می‌شوند. بنابراین یک دفترکل توزیع‌شده یک ساختمان دادهٔ تکثیر شده است و می‌توان به آن بلاک اضافه و تمام سوابق عملیات به‌روزرسانی را در آن ثبت کرد [۱].

۱-۳- اجماع

تکثیر و به‌روزرسانی بلاک‌ها در دفترکل باید با توافق همه شرکت‌کنندگان انجام شود. به‌عبارت دیگر چندین گره باید باهم به اجماع برسند تا یک بلاک به دفترکل اضافه شود. در بلاکچین گره‌ها به یکدیگر اعتماد ندارند به این معنی که

*نویسندهٔ مسؤول

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

بعضی از آن‌ها ممکن است رفتار خصمانه داشته باشند، بنابراین برای تأیید اعتبار بلاک جدید، گره‌ها باید به توافق برسند [۱].

۴-۱- قرارداد هوشمند

یک قرارداد هوشمند، به محاسبات اجراشده در زمان اجرای یک معامله گفته می‌شود. قرارداد می‌تواند به‌عنوان یک رویهٔ ذخیره‌شده بر مبنای معامله عمل کند. تمام بلاکچین‌ها دارای قراردادهای هوشمند هستند که منطق معاملات را پیاده‌سازی و سپس تمام قوانین قرارداد را مشابه یک قرارداد سنتی به‌طور خودکار اجرا می‌کنند. قراردادها می‌توانند به کد رایانه تبدیل و ذخیره شوند و تحت نظارت شبکه رایانه‌ی که بلاکچین را اداره می‌کنند، باشد. قراردادهای هوشمند در ابتدا فقط برای مبادلهٔ پول نظیربه‌نظیر طراحی شده بودند، اما پتانسیل انجام هرگونه مبادله روی اینترنت از طریق قراردادهای هوشمند وجود دارد [۲].

۵-۱- رمزنگاری

سامانه‌های بلاکچین از روش‌های رمزنگاری برای اطمینان از یکپارچگی دفاترکل استفاده می‌کنند. منظور از یک‌پارچگی، توانایی تشخیص دست‌کاری داده‌ها در بلاکچین است. بلاک‌ها تغییرناپذیر و از طریق یک زنجیره درهم‌ساز رمزنگاری‌شده، به یکدیگر متصل هستند. بلاک n+1 ام شامل درهم‌ساز بلاک n ام نیز هست، به این ترتیب هر تغییری در بلاک n ام تمام دنباله بلاک‌ها را غیر قابل قبول می‌کند [۳].

۶-۱- ارزرمز

موفقیت آمیزترین فناوری در بلاکچین ارزرمز است. ارزرمز درواقع یک ارز دیجیتال است که در دفاترکل حساب‌ها ثبت می‌شود و برای مبادله به‌صورت رمزشده استفاده می‌شود و تمامی عملیات آن مستقل از یک سازمان مرکزی است. در پی موفقیت بیت‌کوین به‌عنوان نخستین ارزرمز، چندین ارز رقابتی دیگر نیز ایجاد شد. بیش‌تر این ارزهای جایگزین مانند: اتریوم، لایت‌کوین، ریپل، استلار، مدل‌های داده‌ای مشابه بیت‌کوین دارند. ماهیت برنامه‌های ارز این است که تنها به یک دفترکل مشترک دسترسی دارند [۴].

۷-۱- دارایی دیجیتال

دارایی دیجیتال یک داده است که در دنیای واقعی دارای ارزش است و اغلب توسط نهادهایی صادر می‌شود و برای انتقال ارزش‌ها به‌کار می‌رود [۳]. بلاکچین تنها یک رسانه برای ثبت موجودیت و مبادلات دارایی‌های دیجیتال است. ارزرمز نیز یک نمونه دارایی دیجیتال است.

۸-۱- امضای دیجیتال

امضای دیجیتال از رمزهای نامتقارن، که هر کاربر دارای دو کلید خصوصی و عمومی برای رمزنگاری است، استفاده می‌کند. این کلیدها با یک رابطه ریاضی به یکدیگر مربوط می‌شوند. کلید عمومی برای دریافت پیام از طرف دیگر کاربران، به اشتراک گذاشته و کلید خصوصی به‌صورت مخفی نزد هر کاربر نگه‌داری می‌شود. در امضای دیجیتال، تابع درهم‌ساز پیام، توسط کلید خصوصی، رمز و در سمت گیرنده با کلید عمومی فرستنده رمزگشایی و با تابع درهم‌ساز پیام مقایسه و هویت فرستنده و یک‌پارچگی پیام تأیید می‌شود [۳].

۹-۱- درهم‌سازی

درهم‌سازی به‌ازای دریافت ورودی دلخواهی، با اعمال برخی الگوریتم‌های ریاضی به آن، یک خروجی با طول ثابت تولید می‌کند که درهم‌ساز نام دارد. این ورودی می‌تواند تعدادی بیت، نویسه، یک فیلم، یک رمان کامل، برگه تاریخچه حساب بانکی، و حتی کل اینترنت باشد. نکته مهم این است که، ورودی می‌تواند بزرگ باشد، ولی پس از اعمال محاسباتی بر روی آن، خروجی با تعداد بیت ثابت به‌عنوان مثال ۱۲۸ یا ۲۵۶ یا ۵۱۲ تولید می‌کند. از توابع درهم‌سازی برای تأیید دست‌کاری‌نشدن فایل‌ها و حفظ یک‌پارچگی آن‌ها استفاده می‌شود [۳].

نحوه محاسبهٔ تابع درهم‌سازی در بلاکچین: نخستین درهم‌سازی برای بلاک نخست (Genesis) محاسبه می‌شود، برای بلاک جدید که بعدها تولید می‌شود، درهم‌سازی بلاک قبلی و تراکنش جدید به‌عنوان ورودی تابع درهم‌سازی استفاده می‌شود. بدین ترتیب زنجیره‌ای از بلاک‌ها شکل می‌گیرد. این روش درهم‌سازی تضمین‌کنندهٔ این است که در هیچ تراکنشی، امکان دست‌کاری وجود ندارد؛ زیرا درصورت تغییر بخشی از تراکنش، درهم‌سازی بلاک جدید و همهٔ زیربلاک‌ها تغییر می‌کند. تشخیص دست‌کاری‌شدن در بلاکچین آسان است؛ زیرا فقط نیاز به تأیید ۲۵۶ بیت دارد [۳].

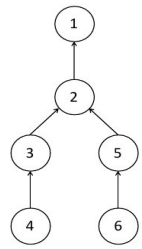
[DOR: 20.1001.1.24763047.1398.8.1.3.9]

۱۰-۱- مسأله Mining

الگوریتم Mining در شبکه بلاکچین برای تأیید و محاسبه تابع درهم‌سازی بلاک جدید استفاده می‌شود. Mining مستلزم عملیات سنگین و پر هزینهٔ محاسبهٔ تابع درهم‌سازی است و درنهایت ماینری که سریع‌تر تابع درهم‌ساز هدف را به‌دست آورد آن را به شبکه اعلام و پاداشی را از شبکه دریافت می‌کند. ماینرها از سخت‌افزارهایی با طراحی خاص استفاده می‌کنند تا به‌صورت کارآمد بتوانند عملیات را انجام دهند [۱].

۱۱-۱- Fork

وضعیتی را که سر بلاک جدید از سر اجداد بلاک جاری نباشد، یک fork می‌نامیم. اگر دو بلاک مختلف ایجاد شود که یک والد مشابه را نشان دهد، همان‌طور که در شکل (۱) نشان داده شده، یک fork اتفاق می‌افتد و زنجیره را نامعتبر می‌کند [۵].



(شکل-۱): fork در بلاکچین [۵]

۲- دسته‌بندی انواع بلاکچین

با درک چگونگی کارکرد بلاکچین سازمان‌ها شروع به استفاده از آن برای اهداف گوناگون کردند. بلاکچین را می‌توان در دسته‌بندی‌های زیر مورد بررسی قرار داد [۱]:

- بلاکچین عمومی
- بلاکچین خصوصی
- بلاکچین کنسرسیوم

۱-۲- بلاکچین عمومی

در بلاکچین عمومی به جای استفاده از یک سرور مرکزی، امنیت توسط تابع درهم‌سازی، برقرار می‌شود. هر گره، می‌تواند به‌عنوان ماینر، این معاملات را جمع‌آوری و منتشر کند؛ زیرا گره مشخصی برای تأیید تراکنش‌ها مورد اعتماد نیست؛ بلکه تمام کاربران یک الگوریتم رمزنگاری را اجرا و تراکنش را تأیید می‌کنند. یک بلاکچین عمومی، برای تمام گره‌ها قابل دسترس است و همه می‌توانند با آن ارتباط برقرارکنند؛ هر بلاکچین فقط شامل معاملات معتبر است و هر گره می‌تواند به فرآیند اجماع کمک کند. فرآیند اجماع تعیین می‌کند که چه بلاک‌هایی به زنجیره اضافه شوند و وضعیت فعلی بلاکچین چیست. مثال‌هایی از بلاکچین عمومی: Bitcoin، Ethereum، Monero، Litecoin است [۱].

۲-۲- بلاکچین خصوصی

بلاکچین‌های خصوصی با استفاده از فناوری بلاکچین و ایجاد گروه‌های خصوصی به‌صورت داخلی معاملات را تأیید می‌کنند. مالک بلاکچین دارای بالاترین مجوز برای تغییر اطلاعات است و سایر گره‌ها دسترسی محدود برای خواندن دارند. مثال‌هایی از بلاکچین خصوصی: MONAX، Multichain، AlphaPoint، Hyperledger است [۶].

۳-۲- بلاکچین کنسرسیوم

بلاکچین کنسرسیوم یک دفترکل توزیع‌شده است که در آن فرآیند اجماع توسط یک مجموعهٔ ازپیش‌تعیین‌شده از گره‌ها کنترل می‌شود. کنسرسیوم بیشتر در بانک‌ها و مؤسسات مالی استفاده می‌شود و فرآیند اجماع توسط گره‌های از پیش‌تعیین‌شده انجام می‌شود؛ برای مثال، ممکن است، یک کنسرسیوم متشکل از پانزده مؤسسه مالی (گره) باشد، ده گره باید هر بلاک را امضا کند تا بلاک معتبر باشد. حق خواندن بلاکچین، ممکن است عمومی یا محدود به برخی از شرکت‌کنندگان باشد. کنسرسیوم سریع‌تر از بلاکچین عمومی است و حریم خصوصی تراکنش را نیز حفظ می‌کند [۱]. مثال‌هایی از بلاکچین کنسرسیوم: R3 (بانک‌ها)، EWF (انرژی)، B3i (بیمه) است.

۴-۲- مقایسه انواع بلاکچین

تمایز بین بلاکچین عمومی، کنسرسیوم و خصوصی مهم است. بلاکچین خصوصی در مقایسه با بلاکچین عمومی مزیت‌هایی دارد؛ در بلاکچین خصوصی مالک بلاکچین می تواند قوانین بلاکچین را تغییر دهد و سطح بالاتری از حریم خصوصی را ارائه دهد؛ همچنین معاملات بلاکچین خصوصی، ارزان‌تر هستند؛ زیرا فقط به چندین گره که قدرت پردازش بسیار بالا دارند، اعتماد می‌کنند؛ ولی در بلاکچین عمومی هزینه‌های معامله گران‌تر است. در جدول (۱) نیز قابلیت‌های مختلف در انواع بلاکچین بررسی شده است.

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

(جدول-۱): مقایسه انواع بلاکچین

قابلیت / انواع	عمومی	خصوصی و کنسرسیوم
دسترسی	مجوز خواندن و نوشتن	مجوز خواندن یا نوشتن
سرعت	آهسته	سریع
امنیت	پروتکل‌های اجماع اثبات‌کار و اثبات‌سهام	شرکت کنندگان از پیش تعیین شده
هویت	ناشناس و نام مستعار	هویت مشخص

۳- الگوریتم‌های اجماع در بلاکچین

الگوریتم‌های اجماع در بلاکچین را می‌توان در سه دستهٔ کلی به‌صورت زیر دسته‌بندی کرد:

- الگوریتم‌های مبتنی بر اثبات
- الگوریتم‌های مبتنی بر رأی‌گیری
- الگوریتم‌های مبتنی بر گراف جهت‌دار بدون دور

در ادامه الگوریتم‌های موجود در هر دسته‌بندی، توضیح داده می‌شود.

۴- الگوریتم‌های اجماع مبتنی بر اثبات در بلاکچین

در الگوریتم‌های مبتنی بر اثبات در میان تمام گره‌های شبکه، یک گره اثبات می‌کند که بلاک جدید زنجیره صحیح است و پاداش دریافت می‌کند و به‌طورمعمول در بلاکچین‌های عمومی کاربرد دارد که گره‌های شبکه، اعتبارسنجی نمی‌شوند و ایجاد اعتماد از طریق حل پازل‌های رمزنگاری توسط گره‌ها صورت می‌گیرد.

۴-۱- POW (Proof Of Work)

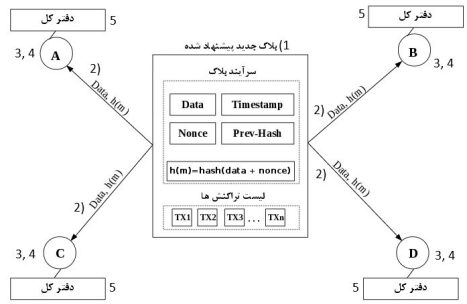
در این روش، تمام گره‌های شبکه، بلاک‌های خود را جهت تأیید در شبکه ارسال می‌کنند و سپس تمام ماینرهای شبکه برای حل پازل ریاضی و اضافه‌کردن بلاک جدید با هم رقابت می‌کنند و هنگامی که یک ماینر راه حل مناسب را پیدا کرد، در همان زمان آن را به کل شبکه اعلام می‌کند، و یک پاداش توسط پروتکل رمزنگاری دریافت می‌کند. اثبات‌کار مستلزم محاسبات رایانه‌ای سنگین و زمان‌بری به نام Mining است، که با انجام آن تراکنش جدید (به‌اصطلاح بلاک) در دفترکل توزیع‌شده‌ای به نام بلاکچین اضافه می‌شود [۷]. ماینرها یک پازل ریاضی را که به‌عنوان مسأله اثبات‌کار شناخته می‌شود، حل می‌کنند. نخستین ماینری که بتواند مسأله را حل کند، پاداش می‌گیرد و تراکنش تأییدشدهٔ آن در بلاکچین ذخیره می‌شود. عملیات Mining دو هدف دارد:

- اجتناب از پرداخت‌های دوگانه
- تأیید درست‌بودن معاملات درون هر بلاک

الگوریتم کلی اجماع اثبات‌کار در بلاکچین به‌صورت زیر است:

در ابتدا، یک nonce که یک مقدار شانزده رقمی تصادفی است، تولید و به دادهٔ اصلی بلاک، اضافه و سپس درهم‌سازی داده و nonce اضافه‌شده محاسبه می‌شود. فرض می‌کنیم، شبکه فقط پیام‌هایی را که درهم‌سازی آن‌ها با تعداد معینی صفر، آغاز می‌شود، به اشتراک می‌گذارد و هرچه سرعت تولید بلاک در شبکه افزایش یابد؛ به‌طور خودکار سختی کار (تعداد صفرهای) نیز افزایش می‌یابد، در حال حاضر پیام‌های شبکه بیت‌کوین با هفتاد؛ صفر آغاز می‌شوند و این تعداد در بازه‌های زمانی افزایش می‌یابد. اگر شرایط تابع درهم‌ساز برقرار باشد، پیام و درهم‌ساز پیام در شبکه ارسال و درغیر این‌صورت، یک nonce دیگر تولید و دوباره تابع درهم‌سازی پیام محاسبه می‌شود تا نتیجه دلخواه حاصل شود. این عمل بسیار وقت‌گیر و حجم محاسبات آن زیاد است. چنانچه گیرنده، پیامی دریافت کند که درهم‌سازی آن با مقدار مورد نیاز صفر شروع نشده باشد، از آن صرف‌نظر می‌کند؛ اما اگر درهم‌ساز پیام دریافتی شامل تعداد مورد نیاز صفر بود، دریافت‌کننده پیام بایستی nonce صحیح را حدس بزند و به پیام دریافت‌شده اضافه و دوباره درهم‌ساز آن را محاسبه کند و سپس با دادهٔ درهم‌ساز دریافتی، مطابقت دهد که آیا برابر هستند یا خیر؟

اگر پیام دچارتغییر شده باشد، طبق خواص تابع درهم‌ساز، درهم‌سازی آن نیز تغییر خواهد کرد. این در اصل فرآیندی است که در پشت اثبات‌کار قرار دارد. محاسبهٔ تابع درهم‌سازی، یک رشتهٔ بسیار آسان است، اما فرآیند پیداکردن nonce مناسب برای تابع درهم‌سازی هدف، یعنی حل پازل رمزنگاری بسیار دشوار و وقت گیر است؛ بنابراین، در پروتکل اثبات‌کار ماینرها پازل‌های رمزنگاری را حل می‌کنند تا بلاک جدید را تأیید و به بلاکچین اضافه کنند. زمانی‌که، ماینر پازل را حل می‌کند، nonce صحیح آن بلاک را به تمامی گره‌های شبکه ارسال می‌کند و تمامی گره‌ها پس از بررسی nonce و تایید بلاک، برای اضافه‌شدن آن بلاک به زنجیره، به توافق می‌رسند [۸]. تمامی این مراحل در شکل (۲) نشان داده شده است.



(شکل-۲): فرآیند اجماع در POW [۸]

مرحله نخست) تولید بلاک جدید و محاسبهٔ تابع درهم‌سازی آن

مرحله دوم) ارسال دادهٔ بلاک و تابع درهم‌ساز به تمام گره‌های شبکه

مرحله سوم) انجام عملیات mining به‌طور هم‌زمان توسط تمام گره‌ها، جهت تأیید بلاک

مرحله چهارم) نخستین ماینری که پازل محاسباتی را حل کند، nonce صحیح را به دیگر گره‌های شبکه ارسال می‌کند.

مرحله پنجم) گره‌ها پس از بررسی nonce صحیح، برای اضافه‌شدن بلاک به توافق می‌رسند و بلاک جدید به بلاکچین اضافه می‌شود [۸].

افراد و سازمان‌هایی که از ASIC سریع‌تر و قدرتمندتری برخوردار باشند، به‌طورمعمول شانس بیش‌تری برای Mining نسبت به دیگران دارند.

نقاط قوت اثبات‌کار:

- تضمین امنیت و یکپارچگی بلاکچین به‌طور مؤثر
- پدیده fork در اثبات‌کار بسیار نادر است.
- برنامه‌ریزی و حمله به شبکه Pow بسیار گران است.

نقاط ضعف اثبات‌کار:

- نیاز به محاسبات رایانه‌ای سنگینی به نام mining دارد.
- افزودن بلاک جدید به زنجیره بلاکچین زمان‌بر است و حداقل ده دقیقه طول می‌کشد.
- نیاز به منابع بیشتر جهت انجام محاسبات

POS(Proof Of Stack) -۴-۲

در این روش، ابتدا استخرهای محاسباتی برای تأیید بلاک و افزودن بلاک به زنجیره به‌وجود می‌آید. گره‌های شبکه می‌توانند بدون هیچ اولویتی به این استخرها ملحق شوند؛ و اعتبارسنجی بلاک را انجام دهند. اعتبارسنج‌ها که در این سامانه Forgers نامیده می‌شوند، باید برخی از سکه‌های خود را به‌عنوان سهام قرار دهند و هرچه میزان سهام اعتبارسنج بیشتر باشد، در شبکه مورد اعتمادتر است. هدف اثبات‌سهام، همانند اثبات‌کار است؛ اما روند اعتبارسنجی معاملات و رسیدن به توافق، متفاوت است. هنگامی که یک بلاک جدید بخواهد به زنجیره اضافه شود، همانند روش اثبات‌کار اعتبارسنج‌ها سعی در حل پازل ریاضی دارند، با این تفاوت که اعتبارسنج‌ها به صورت مشارکتی nonce صحیح را حدس می‌زنند و به پیام دریافت‌شده اضافه و سپس درهم‌سازی آنها را محاسبه می‌کنند و با دادهٔ درهم‌سازی شده، مطابقت می‌دهند که آیا برابر هست یا خیر؟

چنانچه اعتبار بلاک جدید توسط ۲/۳ اعتبارسنج‌ها تأیید شود، بلاک به زنجیره بلاکچین اضافه می‌شود، و اعتبارسنج‌ها با توجه به میزان سهام خود، پاداش دریافت خواهند کرد. همچنین اگر اعتبارسنج‌ها قصد تقلب داشته باشند و بلاک غیرمعتبری را تأیید کنند، جریمه می‌شوند و سهام خود را از دست می‌دهند. در این روش به‌دلیل وجود استخرهای محاسباتی، بسیاری از محاسبات تکراری انجام نمی‌شود و حجم محاسبات برای تأیید بلاک جدید کاهش می‌یابد [۹].

نقاط قوت اثبات‌سهام:

- ارزهای Pos می‌توانند چندین هزار برابر مؤثرتر باشند؛
- افزودن بلاک جدید به زنجیره بلاکچین، سریع‌تر است و حدود سه دقیقه طول می‌کشد؛
- نیاز به منابع کمتری جهت انجام محاسبات در مقایسه با Pow دارد؛

نقاط ضعف اثبات‌سهام:

- پدیده fork در اثبات سهام بیشتر اتفاق می‌افتد؛
- برنامه‌ریزی و حمله به شبکه Pos ارزان است.

Proof Of Elapsed Time -۴-۳

این روش از یک محیط اجرای قابل اعتماد به نام TEE و یک دستگاه خاصی به نام XGS استفاده می‌کند و مشابه الگوریتم اجماع اثبات‌کار است؛ اما نیاز به حل پازل رمزنگاری و عملیات محاسباتی سنگین ندارد؛ بلکه در آن تمام گره‌ها با اجرای یک تابع تصادفی، مدت زمان انتظار مختلفی را دریافت کرده‌اند، و گره‌ای با کوتاه‌ترین زمان، نقش اصلی را در فرآیند اجماع ایفا و بلاک بعدی را تعیین می‌کند. با توجه به هزینهٔ کم این مدل، تمامی گره‌ها می‌توانند به‌راحتی در فرآیند اجماع شرکت کنند، این مدل غیرمتمرکز، مناسب بلاکچین‌های خصوصی است [۱۰].

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

Proof Of Luck -۴-۴

این روش نیز از یک محیط اجرای قابل اعتماد به نام TEE و یک دستگاه خاصی به نام XGS استفاده می‌کند. برای اجرای این روش پس از همگام‌شدن وضعیت تمام ماینرها، هر ماینر یک بلاک جدید ایجاد و به انتهای زنجیرهٔ موجود نزد خود، اضافه می‌کند؛ سپس یک عدد تصادفی مابین صفر و یک به هر بلاک ایجادشده، تخصیص می‌یابد. این عدد تصادفی تعیین‌کنندهٔ میزان شانس آن بلاک است؛ همچنین تمام گره‌ها بر روی زنجیره‌ای با بیشترین شانس، به‌عنوان زنجیرهٔ اصلی توافق دارند. وقوع حملهٔ پرداخت دوگانه، در این روش بسیار سخت است، زیرا مهاجم باید شانس زیادی داشته باشد، تا بتواند عملیاتش را موفقیت‌آمیز اجرا کند [۱۱].

Multichain -۴-۵

یک نوع الگوریتم اجماع است، که از نظر عملیات mining و مدیریت fork بسیار شبیه pow است. اگرچه multichain مانند روش pow گره‌هایی را برای افزودن و تأیید بلاک انتخاب نمی‌کند، اما از یک زمان‌بندی نوبت گردشی برای انتخاب گره، جهت افزودن بلاک به زنجیره استفاده می‌کند. در هر مرحله، تمام گره‌ها بایستی برای یک مدت کوتاه منتظر بمانند و سپس صحت بلاک اضافه‌شده به زنجیره را بررسی کنند. اگر بین p*N بلاکی که اخیراً اضافه شده است، هیچ بلاکی توسط گره فرضی A ایجاد نشده باشد؛ سپس گره A می‌تواند بلاک پیشنهادی خود را ابتدا به زنجیرهٔ خود اضافه و بعد آن را به دیگر ماینرها ارسال کند. همچنین فاکتور p که مابین صفر تا یک است، معرف تنوع گره‌ها برای عملیات mining است [۱۲].

Proof Of Burn -۴-۶

ایده این روش اجماع این است که، ماینرها باید سکه‌های خود را به یک نشانی مجازی جهت سوزاندن، ارسال کنند. به این معنی که، آن سکه‌ها توسط گره دیگری قابل استفاده نیست. درواقع ماینر کسی است که، بیشترین مقدار سکه را در طول یک دوره، برای mine یک بلاک جدید سوزانده باشد. ماینرها از طریق سوزاندن سکه‌های خود در این روش، اثبات می‌کنند که مورد اعتماد هستند و توافق صحیحی را انجام می‌دهند [۱۳].

Proof Of Space -۴-۷

ایده این روش از pow و pos گرفته نشده است. در این الگوریتم اجماع، ماینرها پول خود را بر روی تجهیزات ذخیره‌سازی، که بسیار ارزان‌تر از دستگاه‌های محاسباتی pow است، سرمایه‌گذاری می‌کنند. در طی اجرای الگوریتم اجماع، به روش space، چندین مجموعه داده‌ای بزرگ به نام قطعه تولید، و بر روی دیسک سخت هر گره، ذخیره می‌شود. درواقع، هرچه میزان ظرفیت دیسک سخت بیشتر باشد، ماینرها قطعات بیش‌تری را ذخیره کرده‌اند و احتمال mine کردن بلاک جدید، و به‌دست‌آوردن پاداش بیشتر می‌شود [۱۴].

Activity Of Proof -۴-۸

در این روش ابتدا یک بلاک خالی ساخته می‌شود و تمام ماینرها nonce مناسب را برای این بلاک خالی پیدا می‌کنند. ماینری که nonce مناسب را پیدا کند، مشابه روش pow آن را به سایر ماینرها منتقل می‌کند تا صحت آن را تأیید کنند. درصورتی‌که N-1 ماینر، بلاک خالی را امضا کنند به معنای اثبات بلاک است و تمام امضاها در شبکه منتقل می‌شود. در این روش ایجادکنندهٔ بلاک و تمام ماینرها پاداش یکسانی می‌گیرند. علاوه‌بر جلوگیری از حملهٔ پرداخت دوگانه، در این روش ماینرها برای جمع‌آوری پاداش از شبکه، فعال هستند و براساس فعالیتی که دارند، پاداش دریافت می‌کنند و درنهایت، یکی از آخرین گره‌ها معاملات را به بلاک اضافه می‌کند. این روش ترکیبی از pow و pos است، که علاوه‌بر حل مسئلهٔ حملات پرداخت دوگانه، از افزایش کارمزد تراکنش‌ها توسط ماینرها نیز جلوگیری می‌کند. زیرا افزایش کارمزد موجب غیر قابل استفاده‌شدن بلاکچین برای کاربران می‌شود. همچنین توزیع پاداش به‌طور عادلانه‌تری نسبت به pow صورت می‌گیرد و تمام ماینرها به نسبت فعالیت، پاداش دریافت می‌کنند درحالی‌که در pow فقط ماینری که پازل را حل کند، پاداش دریافت می‌کند و سایر ماینرها که نقش حفظ و نگه‌داری دفاترکل و اعتبارسنجی بلاک جدید را دارند، پاداشی دریافت نمی‌کنند [۱۵].

Proof Of Authority -۴-۹

اثبات هویت یک سازوکار اجماع در بلاکچین است که به‌طوراساسی به یک گره یا تعداد مشخصی از گره‌ها، با یک کلید خصوصی خاص، حق ایجاد تمام بلاک‌ها در بلاکچین را می‌دهد که این امر باعث ایجاد تمرکز می‌شود. این روش به‌علت مصرف انرژی کم و سرعت زیاد، به‌طورمعمول در بلاکچین‌های خصوصی مورد استفاده قرار می‌گیرد [۱۶].

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

Proof Of Weight -۴-۱۰

ایده‌ی کلی این روش مبتنی بر اثبات سهام است که در آن احتمال کشف بلاک بعدی از طریق تعداد نشانه‌هایی که در شبکه داشته باشیم، تعیین می‌شود. Proof of Weight یک میزان وزن نسبی با استفاده از Proof of Reputation و Proof of Space محاسبه می‌کند، که احتمال کشف بلاک بعدی را مشخص می‌کند. این روش مصرف انرژی پایین و مقیاس‌پذیری مناسبی دارد [۱۷].

Proof Of Reputation -۴-۱۱

مدل اجماع تأیید اعتبار، با توجه به اعتبار شرکت‌کنندگان امنیت شبکه را حفظ می‌کند. شرکت‌کننده بایستی اعتبار مهم و کافی در شبکه داشته باشد، تا احتمال تقلب آن کاهش پیدا کند، زیرا درصورت وقوع تقلب، با عواقب مالی و اعتباری قابل توجهی روبه‌رو می‌شود. شرکت‌کننده‌ای که اعتبار آن اثبات شود و از مرحلهٔ اعتبارسنجی عبور کند، به‌عنوان گرهٔ معتبر می‌تواند در شبکه رأی دهد. در این مرحله مانند Proof Of Authority عمل می‌کند و می‌تواند بلاک‌ها را امضا و اعتبارسنجی کند. این روش امنیت بالایی دارد و تنها در شبکه‌های بلاکچین خصوصی استفاده می‌شود [۱۸].

۵- الگوریتم‌های اجماع مبتنی بر رأی‌گیری در بلاکچین

الگوریتم‌های مبتنی بر رأی‌گیری، یک گره برای اضافه‌کردن بلاک جدید، با دیگر گره‌ها ارتباط برقرار می‌کند و به‌طورمعمول در بلاکچین‌های خصوصی، که هویت گره‌ها مشخص است کاربرد دارد و ایجاد اعتماد وابسته به میزان اعتبار سایر گره‌های معتمد شبکه است.

D-POS(Delegate Proof Of Stack) -۵-۱

در این روش هر گره، می‌تواند در انتخابات تولید بلاک شرکت کند و با دریافت توکن‌هایی، یک بلاک را از طریق سامانهٔ رأی‌گیری تأیید کند. در کل N نماینده، بلاک‌ها را امضا می‌کنند و به تراکنش‌هایی که در شبکه ایجاد می‌شود، رأی می‌دهند. این رأی‌گیری غیرمتمرکز، در طراحی DPOS موجب دموکراتیک‌بودن این روش نسبت به روش‌های دیگر می‌شود. علاوه‌براین، هر بلاکی که امضا می‌شود، باید تأیید کند که بلاک قبلی آن، توسط یک گره قابل اعتماد امضا شده باشد. DPOS منتظر تعداد معینی از گره‌های غیر قابل اعتماد برای تأیید تراکنش نمی‌ماند، و این کاهش زمان انتظار موجب افزایش سرعت معاملات می‌شود، به‌طوری‌که می‌توان میلیون‌ها تراکنش در ثانیه را انجام داد.

هر یک از اعضای شبکه، توانایی ایجاد اعتماد و نامزدشدن را دارد و اعتماد لزوماً متعلق به اعضایی نیست که منابع بیشتری را در اختیار دارند، و هر یک از اعضا می‌تواند نماینده مجاز اکثریت کاربران باشد. نقش نمایندگان در این سامانه تولید و توزیع بلاک است. تولید بلاک شامل جمع‌آوری معاملات نظیر به نظیر و امضای آنها با کلید خصوصی نماینده است [۱۹].

درواقع DPOS یک لایهٔ دموکراسی برای ازبین‌بردن تأثیرات منفی سامانه‌های متمرکز ایجاد می‌کند [۶].

نقاط قوت DPOS:

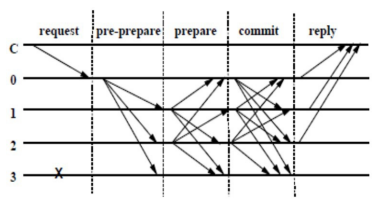
- Fork اتفاق نمی‌افتد، زیرا به جای رقابت برای پیداکردن بلاک‌ها، اعضا ملزم به همکاری هستند.
- DPOS به‌طورمعمول دارای مشارکت صددرصدی برای ساخت بلاک است.
- معاملات به‌طورمعمول در عرض ۱/۵ ثانیه از زمان پخش با اطمینان ۹۹/۹ درصد تأیید می‌شوند.

نقاط ضعف DPOS:

- مقیاس‌پذیری کم‌تری نسبت به اثبات کار و اثبات سهام دارد.
- آسیب‌پذیری بیش‌تر است و حمله به آن راحت‌تر انجام می‌شود.

P-BFT -۵-۲

در روش practical byzantine fault tolerance یک گره رهبر، و تعدادی گره تأییدکننده وجود دارد. گره‌های تأییدکننده، مراحلی را برای اضافه‌شدن بلاک به زنجیره دنبال می‌کنند. این مراحل در شکل (۳) که شامل پنج حالت است، نمایش داده شده است.



(شکل-۳): گام‌های PBFT [۲۰]

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

۱. Request: کلاینت درخواست را به گره سرور اصلی ارسال می‌کند، گره اصلی به درخواست یک timestamp اختصاص می‌دهد.
۲. Pre-prepare: گره سرور اصلی، پیام درخواستی را ثبت و شماره ترتیبی به آن اختصاص می‌دهد؛ سپس گره اصلی یک پیام Pre-prepare به تمام گره‌های دیگر آن سرور ارسال می‌کند. گره‌های دیگر نیز در ابتدا تعیین می‌کنند که آیا درخواست را قبول می‌کنند یا نه.
۳. Prepare: اگر یک گره سرور تصمیم بگیرد که درخواست را قبول کند، یک پیام Prepare را به تمام گره‌های سرور ارسال می‌کند و از دیگر گره‌ها نیز پیام Prepare را دریافت می‌کند. بعد از جمع‌آوری پیام‌ها اگر اکثریت گره‌ها (2f+1) درخواست را پذیرفته باشند، آن درخواست وارد حالت commit می‌شود.
۴. Commit: هر گره در حالت commit یک پیام commit به همهٔ گره‌های دیگر در سرور ارسال می‌کند. هم‌زمان اگر گره سرور، (2f+1) پیام commit دریافت کند، به این باور می‌رسد که بیش‌تر گره‌ها برای پذیرش درخواست به اجماع رسیده‌اند؛ سپس گره دستورالعمل پیام درخواستی را اجرا می‌کند.
۵. Reply: گره‌های سرور به کلاینت پاسخ را ارسال می‌کنند. اگر گره‌های کلاینت به‌دلیل تأخیرهای شبکه پاسخ را دریافت نکنند، درخواست دوباره به گره‌های سرور ارسال می‌شود. اگر درخواست در حال اجرا باشد، لازم است گره‌های سرور تنها پاسخ پیام را دوباره ارسال کنند [۲۰].

DBFT -۵-۳

در الگوریتم delegated byzantine fault tolerance تمام گره‌های شبکه، گروهی از گره‌ها را به‌عنوان نماینده انتخاب می‌کنند. کار این نمایندگان، تصویب قوانین است، اگر نماینده‌ای وظایف خود را به‌درستی انجام ندهد، نماینده دیگری جایگزین می‌شود. همچنین، یک سخنران به‌طور تصادفی از بین نمایندگان، انتخاب می‌شود. سخنران مسئول ساخت بلاک جدید معاملات و همچنین محاسبهٔ درهم‌سازی و تأیید بلاک است؛ سپس بلاک ایجادشده توسط سخنران به نمایندگان شبکه، جهت تأیید معاملات ارسال می‌شود. معاملات می‌تواند به معنای هر نوع دادهٔ قابل ثبت در بلاکچین، از جمله: دعوت‌نامه‌ها، قراردادهای هوشمند و ... باشد.

نماینده‌ها، نتایج بررسی بلاک را در شبکه به اشتراک می‌گذارند و نتایج را مقایسه می‌کنند تا همگی به یک نتیجه یکسان برسند. در حالت ایده‌آل چنانچه نمایندگان صادق باشند، برای رسیدن به توافق، بایستی بیش از ۶۶,۶۶ درصد از نماینده‌ها بلاک را تأیید کنند، تا بلاک به بلاکچین اضافه شود. درصورتی‌که کمتر از ۱/۳ گره‌ها متقلب باشند، DBFT تضمین می‌کند که توافق انجام‌شده، صحیح است. برای درک چگونگی سازوکار اجماع DBFT سه سناریوی مختلف را شرح می‌دهیم.

سناریوی نخست) سخنران متقلب: همیشه این احتمال وجود دارد که سخنران متقلب باشد یا به‌درستی عمل نکند. در این صورت، سخنران یک بلاک مخرب را به دو نفر از سه نماینده ارسال می‌کند. هر نماینده با دراختیارداشتن معاملات قبلی، می‌تواند اعتبار بلاک را بررسی کند. در مقایسه‌ای بین نمایندگان، تعیین می‌شود که بلاک نادرستی از سخنران دریافت شده و بلاک تأیید نمی‌شود؛ زیرا بیش از پنجاه درصد نمایندگان آن را نادرست می‌دانند. بنابراین سخنران دوباره انتخاب می‌شود.

سناریوی دوم) نماینده متقلب: همیشه این احتمال وجود دارد که نماینده متقلب باشد یا به‌درستی عمل نکند. در این صورت، تمام نمایندگان یک بلاک معتبر از سخنران دریافت کرده‌اند؛ اما نماینده متقلب ناعادلانه بلاک را نامعتبر اعلام می‌کند و سپس در مقایسه‌ای که بین نمایندگان انجام می‌شود، تعیین می‌شود که نماینده ناعادلانه عمل کرده است و چون بیش از پنجاه درصد نمایندگان بلاک را معتبر می‌دانند، بنابراین توافق حاصل می‌شود.

سناریوی سوم) سخنران و نماینده متقلب: همیشه این احتمال وجود دارد که سخنران و نماینده متقلب باشد یا به‌درستی عمل نکنند. در این صورت، تمام نمایندگان بلاک‌های مختلفی را از سخنران دریافت کرده‌اند و نماینده متقلب ناعادلانه بلاک را اعتبارسنجی می‌کند، درحالی‌که دیگر نماینده‌ها اعتبارسنجی درستی را اعلام می‌کنند و سپس در مقایسه‌ای که بین نمایندگان انجام می‌شود، تعیین می‌شود که نماینده ناعادلانه عمل کرده است و یا بلاک نامعتبری را از سخنران دریافت کرده است. درنهایت چون بیش از پنجاه درصد نمایندگان بلاک را نامعتبر می‌دانند، بنابراین توافق حاصل و نماینده و سخن‌گوی متقلب جایگزین می‌شوند [۲۱].

Stellar Consensus -۵-۴

پروتکل اجماع Stellar یا SCP یک پروتکل اجماع غیرمتمرکز است که در آن گره‌های داخل شبکه نیاز به اعتماد کامل به شبکه ندارند، بلکه باید توانایی انتخاب

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

گره‌هایی را داشته باشند که به آن‌ها اعتماد دارند. این گروه از گره‌هایی که به یکدیگر اعتماد دارند، به‌عنوان quorum slice نامیده می‌شوند و رسیدن به یک توافق را شکل می‌دهند. کنترل غیرمتمرکز، تأخیر کم، امنیت بالا و اعتماد انعطاف‌پذیر از ویژگی‌های این پروتکل است [۲۲].

Ripple Consensus -۵-۵

این روش با استفاده از زیرشبکه‌های قابل اعتماد مشترک، اجماع را در شبکه بلاکچین انجام می‌دهد و یک الگوریتم اجماع با تأخیر کم است. در این روش الگوریتم اجماع هر چند ثانیه توسط گره‌ها اعمال می‌شود تا درستی و توافق شبکه را حفظ کند. در هر دوره اجماع، هر سرور تمام معاملات معتبر را که قبل از شروع اجماع دیده می‌شود، در فهرستی به نام candidate sct قرار می‌دهد و سپس تمام سرورها candidate set خود را در UNL با یکدیگر ادغام می‌کنند و در مورد صحت تمام معاملات رأی می‌دهند. معاملاتی که بیشتر از حداقل درصد آرا "بله" دریافت کنند به دور بعد منتقل و در غیر این‌صورت حذف می‌شوند و یا در candidate set فرآیند اجماع بعدی قرار می‌گیرند. هر سرور بر درستی هر معامله در یک یا چند دور رأی می‌دهد و تمام معاملاتی که در دور آخر حداقل هشتاد درصد رأی بله کسب کرده باشند، در دفترکل عمومی نوشته می‌شوند و دفترکل بسته می‌شود [۲۳].

۶- الگوریتم‌های اجماع مبتنی بر گراف جهت‌دار بدون دور

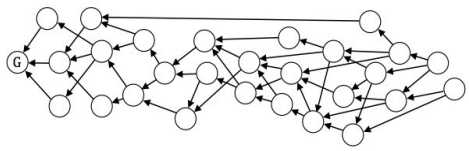
به‌طوراساسی سامانه‌های بلاکچین دارای ساختار خطی هستند و بلاک‌ها به‌صورت ترتیبی و پشت سرهم در بلاکچین ذخیره می‌شوند. این بلاکچین را آهسته می‌کند و بلاک‌ها نمی‌توانند به‌صورت موازی اضافه شوند؛ اما در گراف جهت‌دار بدون دور، بلاک‌ها یا تراکنش‌ها می‌توانند به‌صورت موازی به زنجیره اضافه شوند و هر بلاک یا تراکنش، تعدادی از بلاک‌های قبل از خود را تأیید می‌کند و این مقیاس‌پذیری بیشتری به گراف جهت‌دار بدون دور، می‌دهد [۲۴].

Tangle -۶-۱

روش tangle با هدف حل مسائل مربوط به مقیاس‌پذیری، در سامانه‌های iot ایجاد شده است. Tangle به جای استفاده از معماری زنجیره‌های بلوکی، از dag جهت ذخیره‌سازی بلاک‌ها استفاده می‌کند. هرگره دارای یک وزن است، که متناسب با تلاش آن گره از طرف صادرکننده تراکنش تعیین می‌شود و استراتژی انتخاب تراکنش به‌صورت تصادفی از میان گره‌هایی است که وزن بالاتری دارند؛ همچنین برای انجام یک تراکنش، دو تراکنش قبل اعتبارسنجی می‌شود. درصورت بروز مسائلی همچون هزینه دوگانه و حملات، تمام تاریخچه تراکنش‌های قبلی مورد بررسی قرار می‌گیرد [۲۵].

Byteball -۶-۲

روش Byteball با استفاده از DAG ترتیب جزئی بین معاملات را ایجاد و با استفاده از الگوریتم main chain(MC) زنجیره اصلی را در DAG تعیین می‌کند. که درصورت بروز پرداخت دوگانه، تراکنشی که زودتر در زنجیره اصلی قرار گرفته باشد، معتبر است و بقیه نامعتبر می‌شوند. هر تراکنش به یک یا چند گره قبل از خود متصل است و تابع درهم‌ساز آن را امضا می‌کند. اتصال بین تراکنش‌ها مطابق شکل (۴)، به‌صورت DAG و از تراکنش فرزند به پدر است. هر تراکنش فرزند، تمام تراکنش‌های پدر را تا ریشه تأیید می‌کند [۲۶].



(شکل-۴): واحدهای ذخیره‌سازی متصل در گراف جهت‌دار بدون دور [۲۶]

Hashgraph -۶-۳

ساختمان دادهٔ hashgraph توافق توزیع‌شده‌ای را فراهم می‌کند که، به تعدادی از گره‌ها امکان ایجاد ترتیب در ایجاد تراکنش‌ها را می‌دهد. هر گره می‌تواند یک تراکنش جدید ایجاد کند و آن را درون یک بلاک قرار دهد و در کل شبکه پخش کند. به این ترتیب این سامانه اعتماد را به‌صورت تصادفی از طریق اشتراک با گره‌های دیگر ایجاد می‌کند درحالی‌که گره‌ها مورد اعتماد یکدیگر نیستند. در این روش برخلاف زنجیره‌های بلوکی که درصورت وقوع دو تراکنش هم‌زمان، تنها یک تراکنش را حفظ و دیگری را حذف می‌کنند، تمام تراکنش‌ها مورد بررسی قرار می‌گیرد. بنابراین، در hashgraph بلاکی حذف نمی‌شود و تمام شاخه‌ها

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

همچنان برای همیشه وجود دارند. این الگوریتم ساده، سریع، کارآمد، زمان‌بندی‌شده و مقاوم در برابر Dos است [۲۷].

۷- مقایسه، جمع‌بندی و نتیجه‌گیری

در این مقاله عملکرد الگوریتم‌های اجماع در بلاکچین شرح داده شد که با بررسی آن‌ها متوجه می‌شویم که هیچ یک از سازوکارهای اجماع کامل نیستند و هر کدام به‌منظور خاصی به‌کار می‌روند.

هدف اصلی الگوریتم‌های مبتنی بر اثبات، این است که در میان همه گره‌هایی موجود در شبکه یک گره به‌طور کارآمد اثبات می‌کند که بلاک جدید زنجیره، صحیح است و پاداشی را از شبکه دریافت می‌کند. و به‌طورمعمول در بلاک‌چین‌های عمومی کاربرد دارد که گره‌های شبکه اعتبارسنجی نمی‌شوند و ایجاد اعتماد از طریق حل پازل‌های رمزنگاری توسط گره‌ها صورت می‌گیرد. فرآیند اثبات به‌دلیل محاسبات زیاد بسیار زمانبر و آهسته است. جدول (۲) مقایسه دو روش اصلی pow و pos که مبتنی بر اثبات است را نشان می‌دهد.

(جدول-۲): مقایسه pow و pos [۹]

معیار	POW	POS
بهروری انرژی	خیر	بله
سخت‌افزار مدرن	خیلی مهم	لازم نیست
چندشاخه‌شدن	یافتن همزمان nonce مناسب توسط دو گره	بسیار دشوار
حملهٔ پرداخت دوگانه	بله	سخت
سرعت ایجاد بلاک	آهسته	سریع

در الگوریتم‌های مبتنی بر رأی‌گیری، گره‌های داخل شبکه شناخته شده هستند و به‌طورمعمول در بلاک‌چین‌های خصوصی، که هویت گره‌ها مشخص است، کاربرد دارد. این تفاوت اصلی، در مقایسه با الگوریتم‌های مبتنی بر اثبات است که گره‌ها اغلب به صورت آزاد و بدون تأیید و هویت‌سنجی به شبکه اضافه می‌شوند. در الگوریتم‌های توافق، مبتنی بر رأی‌گیری علاوه‌بر نگه‌داری دفاترکل، تمام گره‌ها معاملات یا بلاک‌ها را بررسی می‌کنند و قبل از تصمیم‌گیری برای اضافه‌کردن بلاک جدید به زنجیره با دیگر گره‌ها ارتباط برقرار می‌کنند. جدول (۳) مقایسه کلی بین الگوریتم‌های اجماع مبتنی بر اثبات و الگوریتم‌های اجماع مبتنی بر رأی‌گیری را نشان می‌دهد.

همچنین هریک از روش‌های اجماع، با توجه به کارکرد در دسته‌بندی مشخصی از بلاکچین‌ها مورد استفاده قرار می‌گیرد. جدول (۴) کاربرد تمام الگوریتم‌های تشریح شده در این مقاله را در پیاده‌سازی‌های مختلف بلاکچین نمایش می‌دهد.

(جدول-۳): مقایسه الگوریتم‌های مبتنی بر اثبات و رأی‌گیری [۹]

معیار	الگوریتم‌های مبتنی بر اثبات	الگوریتم‌های مبتنی بر رای گیری
اساس ایجاد توافق	اثبات کافی گره‌های دنبال‌کننده	تصمیم‌گیری با اکثریت گره‌ها
اضافه‌شدن گره به صورت آزادانه	خیر	بله
تعداد گره اجرایی	نامحدود	محدود
غیرمتمرکزسازی	اغلب زیاد	کم
اعتماد	بیشتر قابل اعتماد	کمتر قابل اعتماد
مدیریت هویت گره	خیر	بله
تهدیدات امنیتی	جدی‌تر	کمتر جدی
پاداش	بله	اغلب ندارد

(جدول-۴): انواع الگوریتم اجماع و کارکرد آن‌ها در بلاکچین

الگوریتم اجماع	کاربرد
POW	Bitcoin
POS	Ethereum
Proof Of Elapsed Time	HyperLedger Sawtooth
Proof Of Luck	-
Multichain	-
Proof Of Burn	Slimcoin
Proof Of Space	Burstcoin
Proof Of Activity	Decred
Proof Of Authority	POA.Network,
Proof Of Weight	Algorand
Proof of Reputation	GoChain
D-POS	EOS
PBFT	Hyperledger
DBFT	NEO
Stellar	Stellar
Ripple	Ripple
Tangle	IOTA
Byteball	-
Hashgraph	Hedera

۸- مراجع

[1] J.Wiley, Sons, "Blockchain For Dummies", "IBM Limited Edition", "United States", 2017.

[2] [Online], available: https://blockchainhub.net/blockchain-intro.

[3] D. Drescher, "Blockchain Basics: A Non-Technical Introduction in 25 Steps", Vol.1, Germany, 2017.

[DOR: 20.1001.1.24763047.1398.8.1.3.9]

[4] J. Bambara and R. Allen, "Blockchain: A Practical Guide to DevelopingBusiness, Law, and Technology Solutions",Vol.1, 2018.

[5] F. Morath, "Implementing a Distributed Reliable Database", Computer Engineering and Networks Laboratory ETH Zürich, 2018.

[6] D. Mingxiao, M. Xiaofeng, Z.Zhe, W. Xiangwei, and C. Qijun, "A Review on Consensus Algorithm of Blockchain", *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2017.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008.

[8] V.Gramoli, "From blockchain consensus back to Byzantine consensus", 2017.

[9] G. Truong Nguyen and K.Kim, "A Survey about Consensus Algorithms Used in Blockchain", *Journal of information processing system JIPS*, 2018.

[10] Intel, "Sawtooth v1.0.1," 2017 [Online]. Available: https://sawtooth.hyperledger.org/docs/co-rc/releases/latest/introduction.html.

[11] M. Milutinovic, W. He, H. Wu, and M. Kanwa, "Proof of luck: an efficient Blockchain consensus protocol, " in *Proceedings of the 1st Workshop on System Software for Trusted Execution*, New York, NY, 2016.

[12] Multichain [Online]. Available: https://github.com/MultiChain/multichain.

[13] P. Titan, "Slimcoin: a peer-to-peer crypto-currency with proof-of-burn," 2014.

[14] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Advances in Cryptology*, Heidelberg: Springer, pp. 585-605, 2015.

[15] Z. Liu, S. Tang, S. S. M. Chow, Z. Liu, and Y. Long, "Forking-free hybrid consensus with generalized proofof-activity," 2017 [Online]. Available: https://eprint.iacr.org/2017/367.pdf.

[16] P. technologies, "Proof of authority chains", [Online], available: "https://github.com/parity-tech/parity/wiki/Proof-of-Authority-Chains", 2017.

[17] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine Agreements for Cryptocurrencies. Cryptology", ePrint Archive, Report 2017/454, 2017.

[18] Gochain, "Proof of Reputation", [Online], available: "https://medium.com/gochain/proof-of-reputation-e37432420712".

[19] D. Larimer, "Delegated Proof-of-Stake (DPOS), [Online], Available: "https://bitshares.org/technology/delegatedproof-of-stake-consensus/" ,2014.

[20] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", in *Symposium on Operating Systems Design and Implementation*, pp. 173-186, 1999.

[21] K.Leussink, "Operates on the principle of Byzantine Fault tolerance to verify blocks", by using an election followed by a validation process [Online], available: https://cryptographics.info/cryptographics/blockchain/consensus-mechanisms/delegated-byzantine-fault-tolerance-dbft.

[22] D. Mazi´eres, "The Stellar consensus protocol: A federated model for internet-level consensus" .https://www.stellar.org/papers/stellar-consensus-protocol.pdf, November 2015.

[23] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm", https://ripple.com/consensus-whitepaper/, September 2014.

[24] G.Danezis, D.Hrycyszyn."Blockmania: from Block DAGs to Consensus." arXiv preprint arXiv:1809.01620, 2018.

[25] S. Popov, The Tangle, http://iotato-ken.com/IOTA_Whitepaper.pdf, 2016.

[26] A. Churyumov, "Byteball: A decentralized system for storage and transfer of value," 2016. [Online]. Available: https://byteball.org/Byteball.pdf

[27] Baird, Leemon et al., "Hedera: A Governing Council and Public Hashgraph Network", https://s3.amazonaws.com/hedera-hashgraph/hh-whitepaper-v1.0-180313.pdf, Mar. 2018.

حمیدرضا شایق بروجنی استادیار گروه مهندسی نرم‌افزار در دانشگاه تربیت دبیر شهید رجایی است. وی مدرک کارشناسی ارشد و دکترای خود را در رشته مهندسی نرم‌افزار از دانشگاه تربیت مدرس اخذ کرده است. زمینه‌های پژوهشی ایشان هوش‌مصنوعی، یادگیری ماشین و سامانه‌های توزیع‌شده است. از وی تاکنون مقالات متعددی در نشریه‌ها و کنفرانس‌های داخلی و خارجی به چاپ رسیده است.

جمیله بحری دانشجوی کارشناسی ارشد مهندسی نرم‌افزار در دانشگاه تربیت دبیر شهید رجایی است. وی مدرک کارشناسی خود را در رشته مهندسی نرم‌افزار از دانشگاه فنی و حرفه‌ای دکتر شریعتی در سال ۱۳۹۴ اخذ کرده است. زمینه‌های علاقه‌مندی او فناوری بلاک‌چین، الگوریتم‌های اجماع و قراردادهای هوشمند است.