فصلنامه
سیاست‌نامهٔ علم و فناوری
دورهٔ ۱۰ شمارهٔ ۳، پاییز ۱۳۹۹

بررسی کاربردی الگوریتم‌های اجماع استفاده‌شده در شبکه‌های بلاک‌چین

محمد شهبازی[۱]
سعید کاظم پوریان[۲]
محمدرضا تقوا[۳]

چکیده

فناوری بلاک‌چین، که با معرفی رمزارز بیت‌کوین در سال ۲۰۰۸ به اوج شکوفایی خود رسید، امروزه نوعی فناوری دگرگون‌کننده در فضای کسب‌وکار به‌شمار می‌رود. با استفاده از شبکه‌های بلاک‌چین می‌توان پایگاه‌های داده و دفاتر کل متمرکز را با دفاتر کل و پایگاه‌های دادهٔ امن و توزیع‌شده میان اعضای شبکه، که به‌عنوان صحه‌گذار شناخته می‌شوند، جایگزین نمود. مهم‌ترین بخش ساختار شبکهٔ بلاک‌چین، الگوریتم‌های اجماع به‌کاررفته در آن است که با استفاده از آن، شیوهٔ به‌توافق‌رسیدن اعضای شبکه دربارهٔ اضافه‌کردن بلوک اطلاعاتی به زنجیرهٔ اطلاعاتی بلوک‌ها تعیین می‌شود. به عبارت دیگر، الگوریتم‌های اجماع قوانین و پروتکل‌هایی را مشخص می‌کنند که مطابق آن اعضا دربارهٔ اینکه کدام بلوک به زنجیره اضافه شود و این کار را چه عضوی انجام دهد به‌توافق می‌رسند و از شکل‌گیری ساختارهای موازی و متناقض جلوگیری می‌کنند. الگوریتم‌های اجماعِ به‌کاررفته در بلاک‌چین به دو گروه تقسیم می‌شوند. گروه نخست، الگوریتم‌های اثبات‌محورند. در این الگوریتم‌ها، اعضای مشارکت‌کننده در شبکهٔ صحه‌گذاری باید نشان دهند که برای افزودن بلوک جدید شرایط و توان بهتری به‌نسبت سایرین دارند. گروه دوم الگوریتم‌های رأی‌محورند؛ در این الگوریتم‌ها، اعضای شبکه قبل از تصمیم نهایی، باید نتایج خود را درخصوصِ صحت تراکنش یا بلوک جدید با یکدیگر درمیان بگذارند. در این مقاله، الگوریتم‌های اجماعی بررسی می‌شوند که در بلاک‌چین کاربرد بیشتری دارند و ضمن بیان ویژگی‌های مهم آنها، از جهات گوناگون نیز با یکدیگر مقایسه می‌شوند.

واژگان کلیدی: الگوریتم‌های اجماع، بلاک‌چین، الگوریتم‌های اثبات‌محور، الگوریتم‌های رأی‌محور

تاریخ دریافت: ۱۳۹۹/۰۲/۰۴
تاریخ پذیرش: ۱۳۹۹/۰۳/۱۱

---

۱. دانشجوی دکتری مدیریت فناوری اطلاعات، دانشگاه علامه طباطبائی (نویسندهٔ مسئول)؛ M.shahbazi@gmail.com
نقش‌نامه: منبع‌یابی، مطالعه و مرور ادبیات، گردآوری داده‌ها، تحلیل، مقایسه و جمع‌بندی نتایج، روش‌شناسی پژوهش
۲. دانشجوی دکتری مدیریت فناوری اطلاعات، دانشگاه علامه طباطبائی
نقش‌نامه: معرفی منابع و نظارت بر روند پژوهش، کنترل تحلیل داده و نتیجه‌گیری، نگارش و بازخوانی
۳. دانشیار دانشگاه علامه طباطبائی
نقش‌نامه: نظارت بر روند کلی پژوهش، مشارکت در شکل‌دهی به بحث و بررسی نتایج، بازخوانی نسخهٔ نهایی

مقدمه

فناوری بلاک‌چین، که نخستین‌بار هابِر و استورنِتا (1991) آن را معرفی کردند، امروزه نوعی فناوری دگرگون‌کننده در فضای کسب‌وکار به‌شمار می‌رود (Attaran and Gunasekaran, 2019؛ Nguyen and im, 2018; Yang et al., 2019). این فناوری پس از اینکه ساتوشی ناکاموتو رمزارز بیت‌کوین را معرفی کرد (Nakamoto and Bitcoin, 2008) در ۲۰۰۸ به اوج شکوفایی رسید (Tschorsch and Scheuermann, 2016). علت این تحول شگرف را، که با معرفی بیت‌کوین همراه بود، می‌توان تغییر در اصل پایه در تراکنش‌های فضای کسب‌وکار دانست؛ یعنی ازبین‌بردن عاملیت واسطه‌ای معتمد و توزیع اطلاعات و تراکنش‌ها میان تمامی اعضای شرکت‌کننده. این ساختار، برای کل شبکه‌های بلاک‌چین مزایایی به همراه دارد؛ ازجمله دوام، شفافیت، اثبات‌پذیری و یکپارچگی فرایند (Abeyratne and Monfared, 2016). ازاین‌رو، کاربرد بلاک‌چین در کسب‌وکارهای گوناگون با سرعت درخور توجهی درحال گسترش است و حوزه‌های مالی، تدارکاتی، بهداشت و درمان و صنایع غذایی پیشتازان استفاده از این فناوری دگرگون‌کننده‌اند (Attaran and Gunasekaran, 2019; Wu et al., 2019). همچنین کاربردهای متنوعی در حوزه‌های پردازش ابری یا امن‌سازی بستر اینترنت اشیا برای بلاک‌چین درنظر گرفته شده است که کاربرد آن را گسترده‌تر می‌کند (پوریان و همکاران، ۱۳۹۹؛ Cohn et al., 2017).

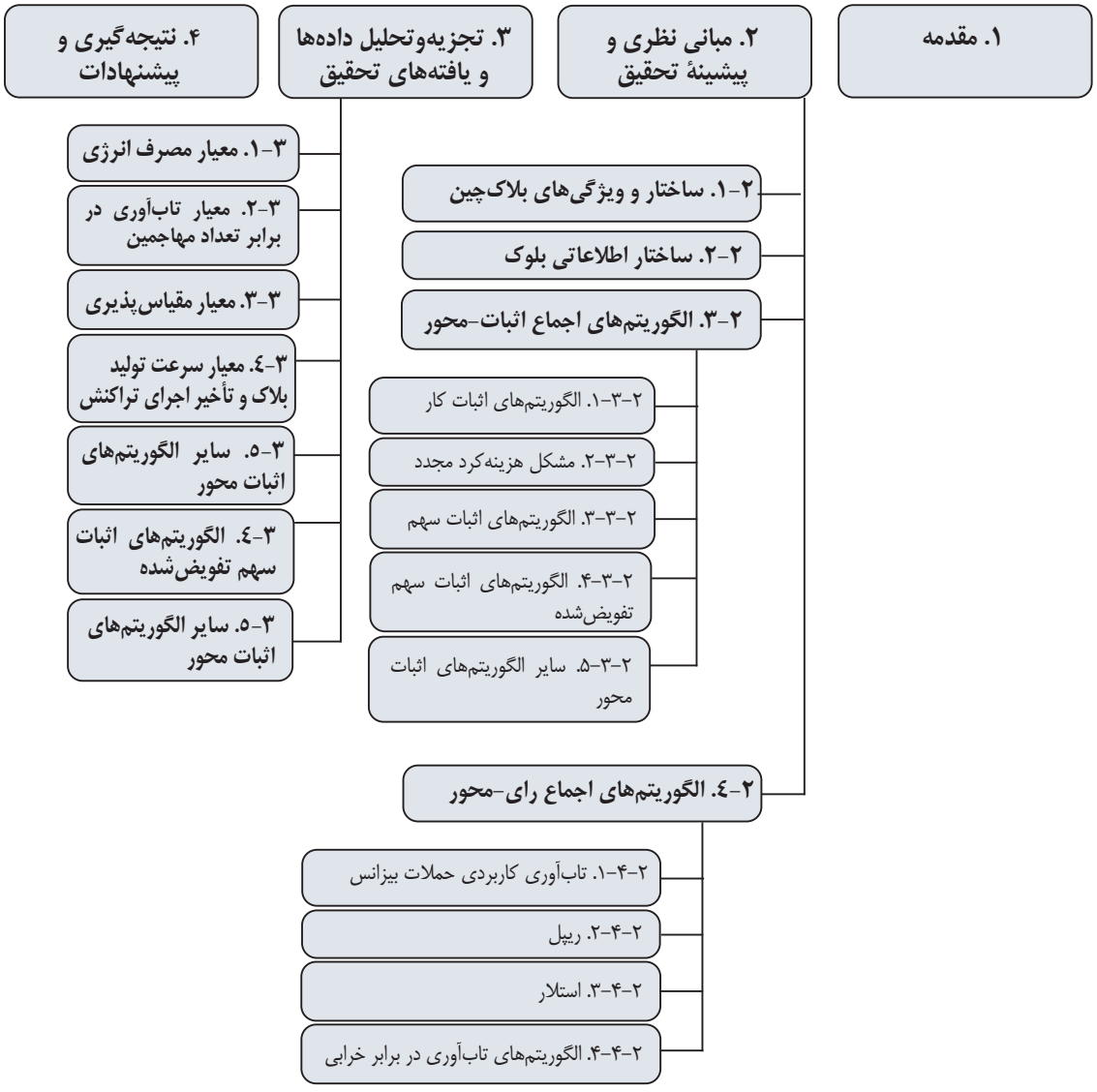
هنگامی که تراکنشی در شبکهٔ بلاک‌چین رخ می‌دهد، به علت نبود نهاد متمرکز واسط، اعضای شبکه اعتبار و صحت تراکنش‌ها را ارزیابی می‌کنند. به‌عبارتی، مهم‌ترین هدف و رسالت الگوریتم‌های اجماع فراهم‌کردن و مدیریت یکپارچگی شبکه در نبود عامل مرکزی و اعضای شبکه است و مهم‌ترین عامل در برقراری این یکپارچگی، ثبت‌کردن و انجام‌دادن تراکنش‌های معتبر در درون شبکه است. تراکنش معتبر نشان می‌دهد که فرستنده یا انجام‌دهنده وجه کافی برای تراکنش را داشته است (که از تراکنش‌های قبلی در بلوک‌های قدیمی‌تر استخراج می‌شود) و ارسال‌کننده اصالت تراکنش را با امضای دیجیتال خود تأیید کرده است (Robert, 2017). در این مرحله، برای نهایی‌شدن تراکنش و ارجاع‌پذیری آن، باید بلوک حاوی تراکنش به زنجیرهٔ اصلی اضافه شود و اعضا آن را شناسایی کنند. اعضای شبکه بلوک‌های تأییدشدهٔ خود را برای اضافه‌شدن به زنجیرهٔ اصلی به سراسر شبکه ارسال می‌کنند. اگر هریک از اعضا بلوک‌های مدنظر خود را برای درج‌شدن در زنجیرهٔ اصلی به سراسر شبکه ارسال کنند، احتمالاً بلوک‌های تکراری و متناقضی تشکیل می‌شود. برای جلوگیری از این مسئله، اعضا باید دربارهٔ اینکه کدام بلوک به زنجیره اضافه شود و همچنین، عضو اضافه‌کنندهٔ آن به‌توافق برسند. به این توافق و شیوهٔ حصول آن، الگوریتم اجماع[1] گفته می‌شود. با توجه به شیوهٔ فعالیت رمزارزهایی چون اِتریوم[2] (Ethereum, Online) و نکست‌کوین[3] (Popov, 2016; Nxt wiki, 2016)، که در آن اعضا به‌راحتی به شبکهٔ عمومی بلاک‌چین اضافه یا از آن حذف می‌شوند، اجماع با رأی‌گیری از همهٔ اعضا، مشابه آنچه در اجتماعات انسانی رخ می‌دهد، دشوار و گاهی غیرممکن است (Nguyen and Kim, 2018). در این حالت، عضو اضافه‌کنندهٔ بلوک باید اثبات کند که از سایر اعضای شبکه برای انجام‌دادن این کار شرایط بهتری دارد. ازاین‌رو، به این دسته از الگوریتم‌های اجماع الگوریتم‌های اثبات‌محور گفته می‌شود و معمولاً به عضو اضافه‌کننده نیز پاداش مشخصی اعطا می‌شود. الگوریتم‌های اثبات‌محور با توجه به آنچه مبنای اثبات قرار می‌گیرد به اقسام متعددی تفکیک می‌شوند. در صورتی که توان پردازش اعضا مبنای اثبات برتری آن‌ها قرار گیرد، الگوریتم اثبات کار (PoW)[4] نامیده می‌شود (Nakamoto and Bitcoin, 2008). درصورتی‌که میزان سرمایه و سهم مالی عضو مبنای اثبات برتری باشد، الگوریتم اثبات سهم (PoS)[5] نامیده می‌شود (Nguyen and Kim, 2018) که هدف آن غلبه بر مشکلات الگوریتم‌های اثبات کار است. در زمان نگارش این مقاله، الگوریتم‌های اثبات کار و اثبات سهم از مشهورترین و رایج‌ترین الگوریتم‌های اجماع‌اند. اما افزون‌بر این دو، الگوریتم‌های اثبات‌محور دیگری نظیر اثبات شانس (Milutinovic et al., 2016)، اثبات فعالیت (Bentov et al., 2014) و اثبات ظرفیت (Dziembowski et al., 2015) نیز استفاده می‌شوند که در بخش‌های بعدی تشریح و تبیین خواهند شد.

با توجه به کاربردهای گستردهٔ بلاچین در حوزهٔ تجارت و کسب‌وکار و با ورود شرکت‌های بزرگی چون آی بی ام و جی. پی. مورگان[6] در این حوزه (Cachin, 2016; QuorumChain Consensus, online) و بسترهای تجاری بلاک‌چینی که این شرکت‌ها فراهم کرده‌اند، شرایطی مهیا شده که در آن اعضا با ضوابط خاصی به شبکه وارد و احراز هویت می‌شوند. در این شبکه‌های خصوصی یا کنسرسیومی،[7] با توجه به ضوابط حاکم برای شناسایی اعضا و تعداد محدودتر اعضای تشکیل‌دهندهٔ شبکه به‌نسبت شبکه‌های عمومی بلاک‌چین، اجماع با رأی‌گیری از اعضا و به‌کارگیری سازوکار رأی‌گیری شکل می‌گیرد؛ ازاین‌رو، نوع دیگری از الگوریتم‌های اجماع، که به آن الگوریتم‌های

1. Consensus Algorithm
2. Ethereum
3. Nextcoin
4. Proof of Work
5. Proof of Stake
6. J.P. Morgan
7. Consortium

رأی‌محور گفته می‌شود، پیشنهاد شده است. در این الگوریتم‌ها، برای اضافه‌شدن بلوک به زنجیره باید دستِ‌کم به میزان T عضو شبکه با انجام‌دادن این کار موافق باشند و به آن رأی مثبت دهند؛ که مقدار T وابسته به اجرای الگوریتم و سیستم و بیش از ۵۰ درصد است. به‌منظورِ پیش‌گیری از تأثیر مخرب برخی اعضای شبکه در عملکرد کلی این دسته از الگوریتم‌ها، سازوکارهایی برای تاب‌آوری درمقابلِ خرابی یا حملات باید درنظر گرفته شود (Lamport, 2001; Castro and Liskov, 1999). شایان ذکر است الگوریتم‌های اثبات‌محور، علاوه‌بر شبکه‌های عمومی با تعداد اعضای زیاد، در شبکه‌های خصوصی و کنسرسیومی نیز استفاده شده و الگوریتم‌های رأی‌محور نیز در شبکه‌های عمومی به‌کار گرفته شده‌اند.

در این مقاله تلاش شده است که الگوریتم‌های اجماعِ استفاده‌شده در شبکه‌های بلاک‌چین بررسی شوند و ضمن بیانِ ویژگی‌های آن‌ها، از جنبه‌های گوناگون نیز این الگوریتم‌ها تحلیل و ارزیابی شوند. ساختار طرح مطالب در شکل ۱ نمایش داده شده است. پس از مقدمه، در بخش دوم، ادبیات حوزهٔ بلاک‌چین، شیوهٔ عملکرد آن و الگوریتم‌های اجماع موجود و پرکاربرد مرور و بازبینی می‌شوند. سپس در بخش سوم با معرفی معیارها و ملاک‌های ارزیابی، الگوریتم‌های معرفی‌شده از جنبه‌های گوناگون با یکدیگر مقایسه می‌شوند. درنهایت، در بخش چهارم با جمع‌بندی مطالب، پیشنهادهایی برای پژوهش‌های آتی بیان می‌شوند.



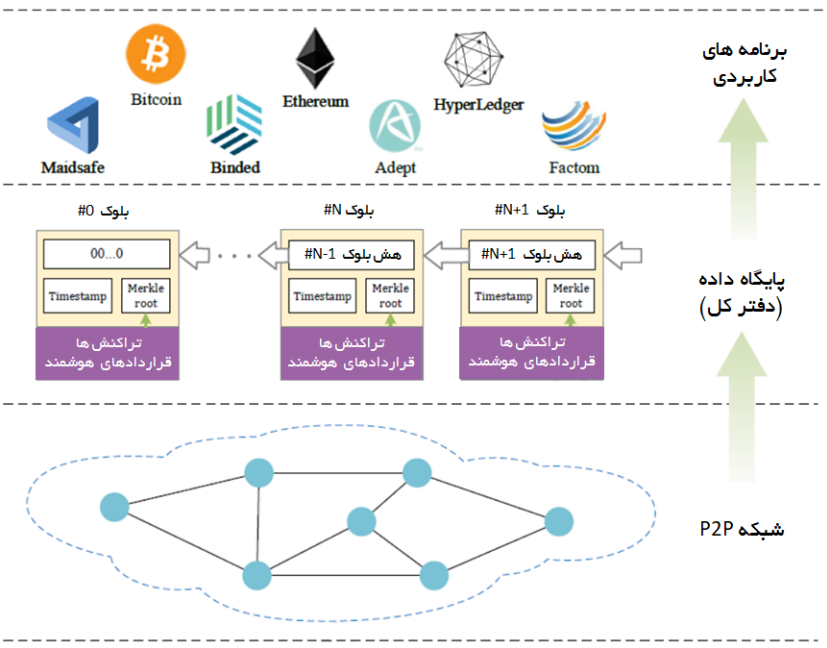
شکل ۱: ساختار مطالب بیان‌شده در این مقاله

۱. مبانی نظری و پیشینهٔ پژوهش

۱-۱. ساختار و ویژگی‌های بلاک‌چین

بلاک‌چین را می‌توان پایگاه داده‌ای درنظر گرفت که اطلاعات صرفاً به آن اضافه می‌شود و شبکه‌ای از اعضای همتابه‌همتا (P2P)[1] از آن نگه‌داری می‌کند. تاکنون پژوهشگران مدل‌ها و لایه‌های طراحی متعددی را برای ساختار بلاک‌چین معرفی کرده‌اند (Croman et al., 2016; Yu et al., 2018; Yu and He, 2019; Wu et al., 2019). اما در حالت ساده و کاربردی، می‌توان ساختاری مشابه شکل ۲ را در سه لایهٔ شبکهٔ همتابه‌همتا، پایگاه داده و برنامه‌های کاربردی برای آن درنظر گرفت (Feng et al., 2019). لایهٔ همتابه‌همتا باید مسئول برقراری ارتباط آزاد میان اعضای شبکه باشد؛ به‌گونه‌ای که موقعیت جغرافیایی آن‌ها متفاوت و متغیر بوده و تمامی اعضا در شبکه نقشی برابر داشته باشند. همچنین عضوی در جایگاه سرویس‌دهنده نباشد و اعضا هم مصرف‌کننده و هم تولیدکنندهٔ اطلاعات باشند. در این شبکه، همهٔ اعضا در فرایندهای مسیریابی شبکه، تأیید و اعتبارسنجی تراکنش‌ها، همگام‌سازی و ذخیرهٔ اطلاعات سهیم‌اند. ساختار مسطح شبکهٔ همتابه‌همتا مبنای ویژگی غیرمتمرکز بلاک‌چین و زیربنای این ساختار به‌شمار می‌رود.

لایهٔ دفتر کل یا پایگاه داده مسئولیت ثبت و ضبط تراکنش‌های اجراشده در شبکه را به‌عهده دارد. هر تراکنش شامل اطلاعات فرستنده (خریدار)، گیرنده (فروشنده)، پیام و امضای طرفین دخیل در آن است. از سوی دیگر، امکان دیگری در شبکه‌های بلاک‌چین فراهم شده که در آن تراکنش‌ها و تبادل پیام به‌شکلی کاملاً منعطف انجام می‌شود که به آن قرارداد هوشمند[2] گفته می‌شود. برای مثال، در شبکهٔ بیت‌کوین قطعه‌کدهای خاصی، پس از رمزنگاری موفق اطلاعات، خودکار اجرا می‌شوند یا در شبکهٔ اِتریوم زبان برنامه‌نویسی خاصی به نام سالیدیتی[3] برای اجرای توابع پیچیده حین برقراری شرایط خاص طراحی و استفاده می‌شود (ibid). اطلاعات مجموعه‌ای از تراکنش‌ها و قراردادهای هوشمند در ساختاری به نام بلوک ذخیره می‌شود و هر بلوک به بلوک قبلی خود اشاره دارد. بلوک شمارهٔ صفر بلوک جنسیس[4] نام دارد و به بلوک قبل ازخود اشاره‌ای ندارد. بنابراین، تمامی تراکنش‌های انجام‌شده در شبکه، در ساختاری اطلاعاتی که فقط قابلیت اضافه‌کردن دارد و حذف و اصلاح در آن امکان‌پذیر نیست قرار می‌گیرند و کل این ساختار، قابلیت ذخیره‌سازی به‌دست همهٔ اعضای شبکه را خواهد داشت. این ساختار اطلاعاتی در سراسر شبکهٔ همتابه‌همتا توزیع شده و اعضا با استفاده از سازوکار اجماع آن را همگام و هماهنگ، به‌روزرسانی می‌کنند. با توجه به این نکته که ساختار زنجیرهٔ بلوکی از طریق اجماع میان همهٔ اعضا به‌روزرسانی و توزیع می‌شود، یک یا چندین عضو مهاجم نمی‌توانند به‌راحتی آن را دستکاری و اصلاح کنند و اگر این اعضا نسخهٔ محلی خود را به‌روز کنند، نسخهٔ جدید و تغییرات آن را سایر اعضای شبکه معتبر نمی‌دانند.



شکل ۲: ساختار پایهٔ شبکهٔ بلاک‌چین

1. Peer to Peer
2. Smart Contract
3. Solidity
4. Gensis Block

با توجه به کاربرد گستردهٔ بلاک‌چین و ساختار آن، واسط‌های برنامه‌نویسی کاربردی (API)[1] بسیاری برای آن نوشته شده است که سایر کاربران را از رویارویی با زیرساخت آن بی‌نیاز و امکان مشارکت و استفاده از آن را برای عموم تسهیل می‌کند. مشاهدات نشان داده‌اند که تاکنون بیشترین کاربرد بلاک‌چین در حوزهٔ مالی بوده است (Feng et al., 2019؛ Attaran and Gunasekaran, 2019). علاوه‌برآن، زیرساخت‌هایی مانند هایپرلجر[2] قابلیت‌های بیشتری را از جمله موتور قراردادهای هوشمند، دفتر کل توزیع‌شده و واسط کاربری گرافیکی در اختیار عموم گذاشته است. به‌سبب این اقدامات و تغییرناپذیری و جامعیت این فناوری، علاوه‌بر حوزهٔ مالی، می‌توان به کاربردهای گسترده‌تر آن در سایر بخش‌ها اشاره کرد، کاربردهایی مانند فکتام[3] در حوزهٔ مدیریت اسناد دیجیتال، بیندد[4] در حوزهٔ مدیریت حقوق کپی‌رایت، میدسیف[5] در حوزهٔ توزیع اطلاعات و شبکهٔ ادپت[6] برای مدیریت اطلاعات در حوزهٔ اینترنت اشیا (Cohn et al., 2017؛ پوریان و همکاران، ۱۳۹۹)

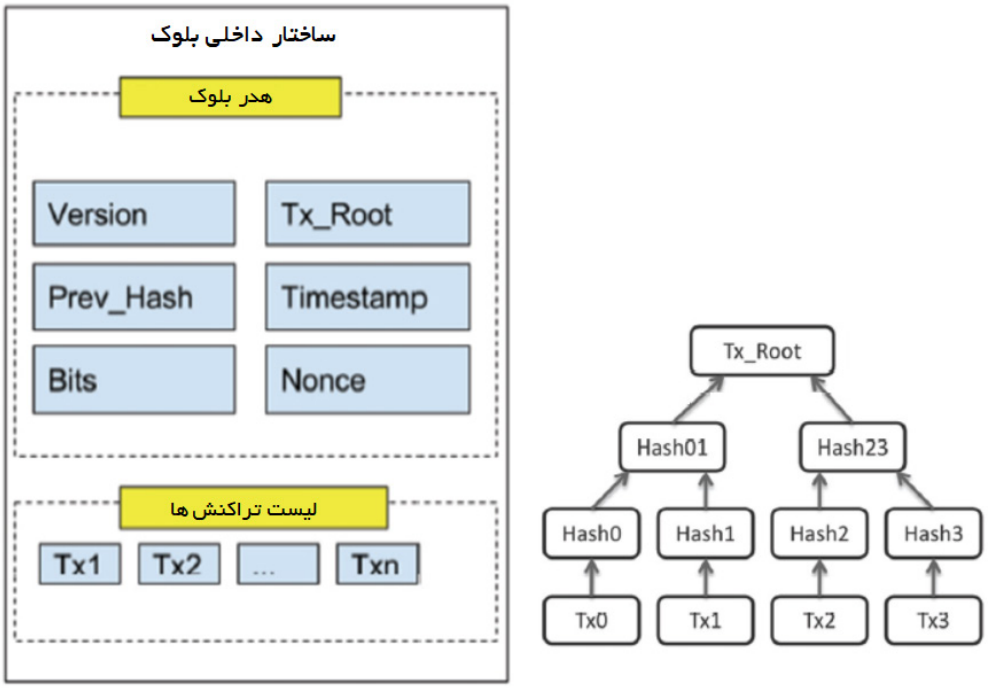
۱-۲. ساختار اطلاعاتی بلوک

ساختار عمومی بلوک‌ها در شبکهٔ بلاک‌چین بیت‌کوین در شکل ۳ نمایش داده شده است (Nguyen and Kim, 2018). اجزای تشکیل‌دهندهٔ بلوک در این مثال عبارت‌اند از:

۱. **مقدار هَش قبلی:**[7] به بلوک والد اشاره می‌کند؛ به‌گونه‌ای که همهٔ اطلاعات موجود در بلوک والد، در یک تابع هَش ۲۵۶ بیتی وارد می‌شود و مقدار حاصله در این فیلد قرار می‌گیرد؛

۲. **دورهٔ زمانی:**[8] زمانی است که بلوک شناسایی یا به‌اصطلاح استخراج شده است؛

۳. **ریشهٔ هَش تراکنش‌ها:**[9] این فیلد، که به آن ریشهٔ مِرکل[10] نیز گفته می‌شود، شامل هَش کلیهٔ تراکنش‌های موجود در بلوک است؛ به‌گونه‌ای که تراکنش‌ها دوبه‌دو هَش شده، مقادیر حاصل نیز مجدداً تا رسیدن به ریشه دوبه‌دو هَش می‌شوند. مقدار نهایی در این فیلد ذخیره می‌شود.



شکل ۳: ساختار اطلاعاتی بلوک و فیلدهای تشکیل‌دهندهٔ آن در شبکهٔ بیت‌کوین

1. Application Programming Interface
2. Hyperledger
3. Factom
4. Binded
5. MaidSafe
6. ADEPT
7. Prev_Hash
8. Timestamp
9. Tx_Root
10. Merkle Root

۴. **نسخه:**[1] این فیلد نسخه‌ای از الگوریتم اجماعی را نشان می‌دهد که با آن بلوک تشکیل و تأیید می‌شود.

۵. **نانس:**[2] این فیلد، که در الگوریتم‌های اجماع اثبات کار استفاده می‌شود، مقداری است که اعضا از طریق محاسبه و آزمون‌وخطا برای حل‌کردن معمای محاسباتی به‌دست می‌آورند. توضیحات بیشتر در این‌باره در بخش تشریح الگوریتم‌های اثبات کار بیان شده است.

۶. **بیت:**[3] این فیلد نیز در الگوریتم اجماع اثبات کار استفاده می‌شود و میزان سختی معمای محاسباتی را مشخص می‌کند که در بخش مربوطه کامل‌تر توضیح داده خواهد شد.

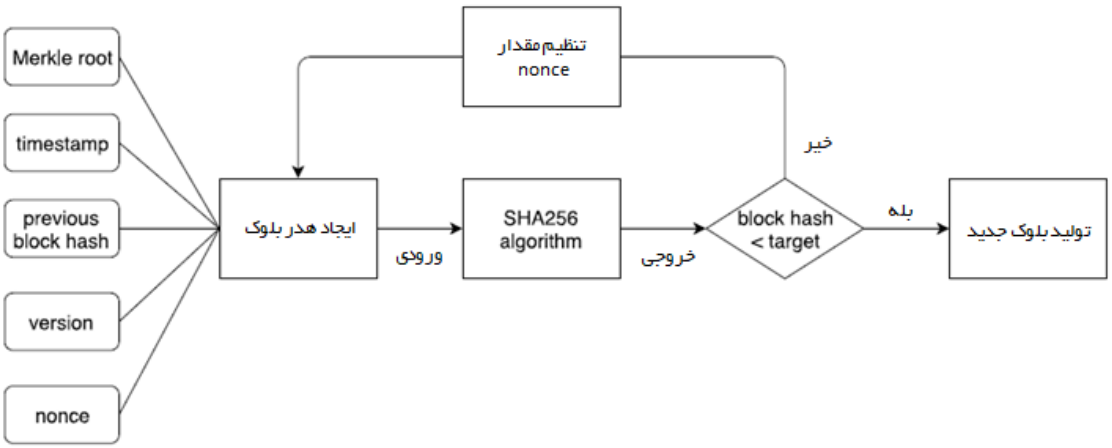
۱-۳. الگوریتم‌های اجماع اثبات‌محور

۱-۳-۱. الگوریتم‌های اثبات کار

در الگوریتم‌های اثبات کار، که از طریق رمزارزهای بیت‌کوین و اِتریوم معرفی شده‌اند و درحال حاضر کاربرد گسترده‌ای دارند، عضو خلق‌کنندهٔ بلوک در هر دور، از راه برگزاری رقابتی محاسباتی انتخاب می‌شود. این رقابت محاسباتی با حل‌کردن معمای محاسباتی رمزگذاری شده است و هر عضوی که زودتر از سایرین آن را حل کند صلاحیت لازم برای افزودن بلوک به زنجیره را خواهد داشت. به اعضایی که در این فعالیت شرکت می‌کنند استخراج‌کننده[4] یا کاوشگر گفته می‌شود و اگر کاوشگری بتواند با حل‌کردن این معما بلوک جدیدی را به زنجیره اضافه کند، مقدار مشخصی پاداش دریافت می‌کند. گردش کار الگوریتم‌های اثبات کار در شکل ۴ نشان داده شده است. کاوشگران باید مرتب مقدار نانس را با انجام‌دادن محاسبات پیچیدهٔ ریاضی تغییر دهند تا مقدار هَش جدید الزامات شبکه را، که در پارامتر target مشخص شده است، فراهم کنند (Zhang and Lee, 2019؛ Wu et al., 2019؛ Nguyen and Kim, 2018).

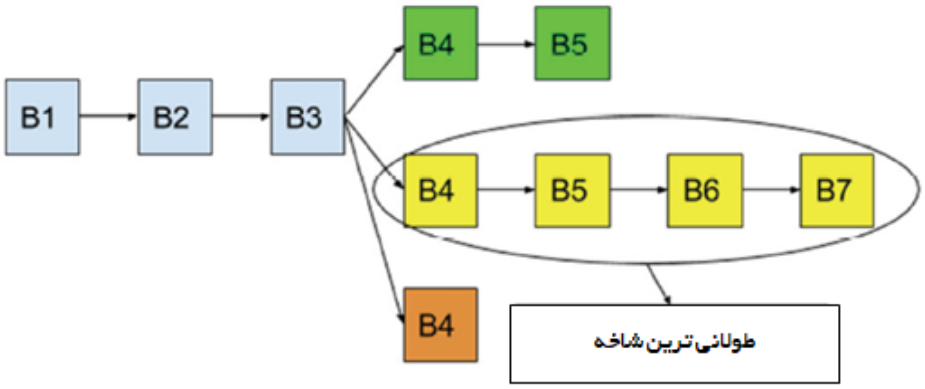
اگر کاوشگری بتواند به مقدار مناسبِ نانس دست یابد، بلوک مدنظر خود را به همراه مقدار نانس به‌دست‌آمدهٔ آن برای سایرین ارسال می‌کند تا آن‌ها را از حل‌شدن معمای محاسباتی مطلع سازد. زمانی که کاوشگران این پیام را دریافت کنند، محاسبات خود را روی بلوک مدنظر را متوقف می‌کنند و به اعتبارسنجی بلوک جدید و تراکنش‌های موجود در آن می‌پردازند. اگر اعتبار بلوک تأیید شود، آن را به نسخهٔ محلی بلاک‌چین خود اضافه می‌کنند و در غیر این صورت، روند محاسباتی حل‌کردن معما را ادامه می‌دهند.

انجام‌دادن محاسبات اثبات کار به توان پردازشی زیادی نیاز دارد و شرط اول‌شدن در رقابت نیز بیش‌ازپیش به نقش قدرت سخت‌افزاری در این الگوریتم و میزان مصرف انرژی در این‌خصوص وابسته است. با توجه به شیوهٔ تولید بلوک‌های جدید، هرقدر طول شاخهٔ بلوک‌های معتبر طولانی‌تر شود، مقدار انرژی و توان محاسباتی اعضای مهاجم برای تشکیل شاخه‌های جعلی نیز ازلحاظِ نمایی افزایش خواهد یافت. در نسخهٔ اصلی این الگوریتم، که ساتوشی ناکاموتو پیشنهاد کرده و در شبکهٔ بیت‌کوین معرفی شده است (Nakamoto and Bitcoin ,2008)، به‌ازای هر ۲۰۱۶ بلوک، مقدار سختی شبکه، که با پارامتر bit یا target تنظیم می‌شود، افزایش می‌یابد تا سرعت ایجاد بلوک به میزان ۱ بلوک در هر ۱۰ دقیقه برسد.



شکل ۴: گردش کار الگوریتم اثبات کار

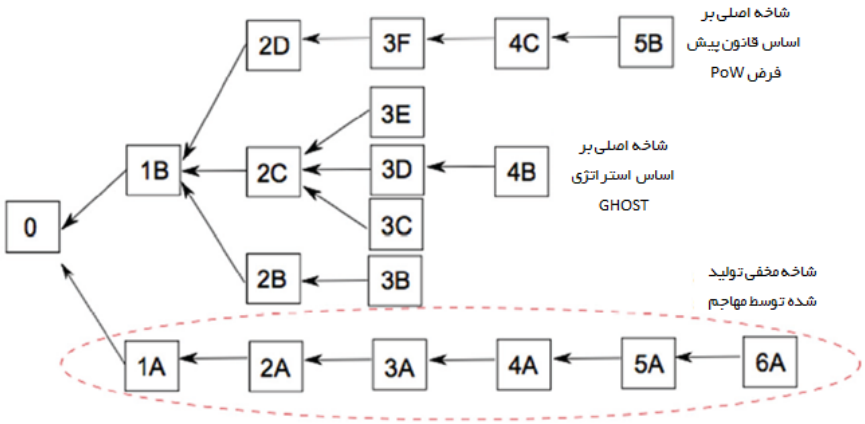
1. Version
2. Nonce
3. Bit
4. Miner



شکل ۵: شاخه‌سازی در بلاک‌چین

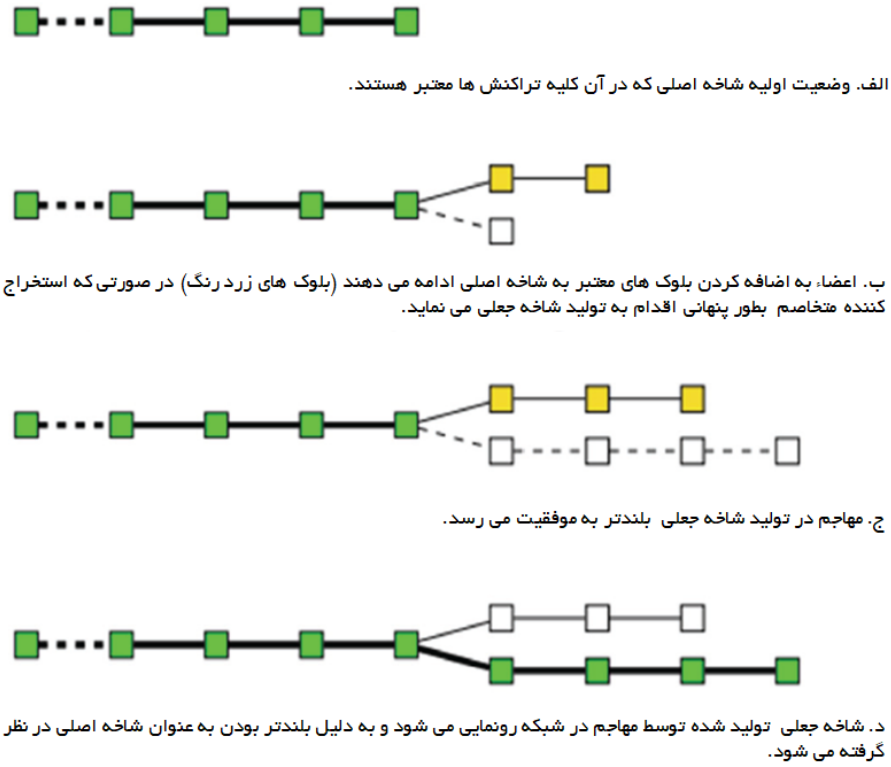
در مواردی، بیش از یک کاوشگر معمای محاسباتی را حل و اطلاعات آن را به شبکه ارسال می‌کنند. سایر اعضا با دریافت اولین بلوک معتبر آن را در زنجیرهٔ خود قرار می‌دهند و از بلوک‌های مشابه بعدی صرف‌نظر می‌کنند. براساس اینکه اعضا در ابتدا از کدام‌یک از کاوشگران تولیدکنندهٔ بلوک اطلاعات را دریافت کنند، شکل کلی زنجیره تغییر خواهد کرد. به این حالت، که در شکل ۵ نمایش داده شده، شاخه‌سازی[1] گفته می‌شود که در هرشاخه نیز بلوک‌های معتبری قرار گرفته‌اند.

براساس شکل ۵، پس از ایجاد بلوک B3، همزمان سه کاوشگر بلوک B4 را می‌یابند و به سایرین اطلاع‌رسانی می‌کنند. سایر کاوشگران با توجه به نوبت دریافت این پیام، زنجیرهٔ خود را تنظیم می‌کنند. برخی بلوکی را که کاوشگر اول (سبزرنگ) یافته را بلوک معتبر درنظر می‌گیرند و براین‌اساس، سایر بلوک‌ها را به زنجیره اضافه می‌کنند. به همین ترتیب، برخی از اعضا نیز بلوک‌های کاوشگران دوم و سوم (زرد و نارنجی) را به زنجیره اضافه می‌کنند و آن را مبنای خود برای اضافه‌کردن بلوک‌های بعدی قرار می‌دهند. بنابراین، تصویر کلی زنجیره بعد از بلوک B3 مانند شکل ۵ است و سه شاخهٔ مستقل و معتبر پدید آمده است. در نسخهٔ اولیه و پیشنهادی ناکاموتو، بزرگ‌ترین شاخه ملاک قرار می‌گیرد و سایر کاوشگران باید مطابق با آن اقدام کنند. پاداش نیز به کاوشگرانی اعطا می‌شود که بلوک‌هایشان را همهٔ اعضای شبکه تأیید کنند، نه اینکه صرفاً معمای محاسباتی را حل کنند (ibid). در روشی دیگر، که GHOST نام دارد (Sompolinsky and Zohar, 2013)، همهٔ شاخه‌هایی که به‌منزلهٔ شاخهٔ اصلی انتخاب نشده‌اند درنظر گرفته می‌شوند. آن‌گاه به‌جای شاخهٔ بلندتر، شاخه‌ای انتخاب می‌شود که بیشترین فعالیت اثبات کار روی آن انجام شده باشد. بدین‌معنا که از میان شاخه‌های هر گره، شاخه‌ای درنظر گرفته می‌شود که در آن تعداد بلوک‌های بیشتری وجود داشته باشد و این کار تا زمان رسیدن به یک شاخه ادامه می‌یابد. شکل ۶ مثالی از این وضعیت را نشان داده که در آن با استفاده از این روش، شاخهٔ جعلی که مهاجمان ساخته‌اند درنظر گرفته نمی‌شود؛ چراکه در شاخهٔ دیگر، تعداد بلوک‌های بیشتری وجود دارد و توان بیشتری برای ساختن آن صرف شده است.



شکل ۶: روش انتخاب شاخهٔ اصلی بر اساس روش GHOST

1. Forking



الف. وضعیت اولیه شاخه اصلی که در آن کلیه تراکنش ها معتبر هستند.

ب. اعضاء به اضافه کردن بلوک های معتبر به شاخه اصلی ادامه می دهند (بلوک های زرد رنگ) در صورتی که استخراج کننده متخاصم بطور پنهانی اقدام به تولید شاخه جعلی می نماید.

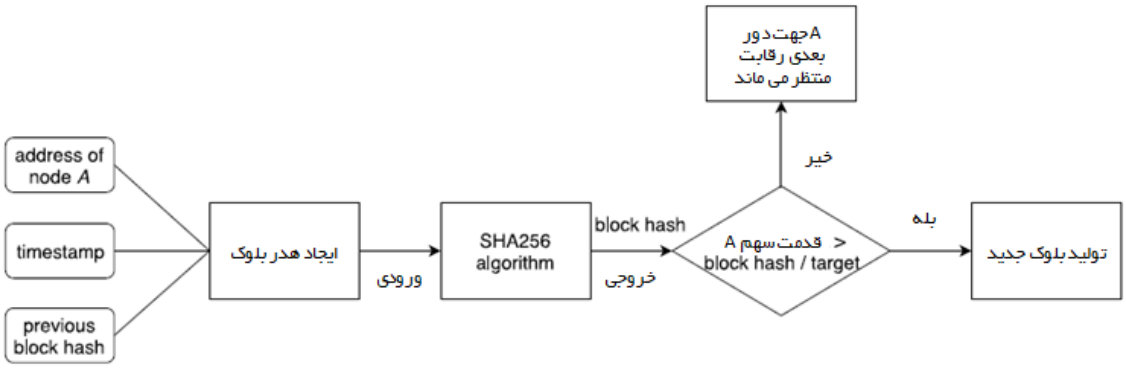
ج. مهاجم در تولید شاخه جعلی بلندتر به موفقیت می رسد.

د. شاخه جعلی تولید شده توسط مهاجم در شبکه رونمایی می شود و به دلیل بلندتر بودن به عنوان شاخه اصلی در نظر گرفته می شود.

شکل ۷: سناریوی رخداد حالت هزینه‌کرد مجدد از راه تولید شاخهٔ جعلی

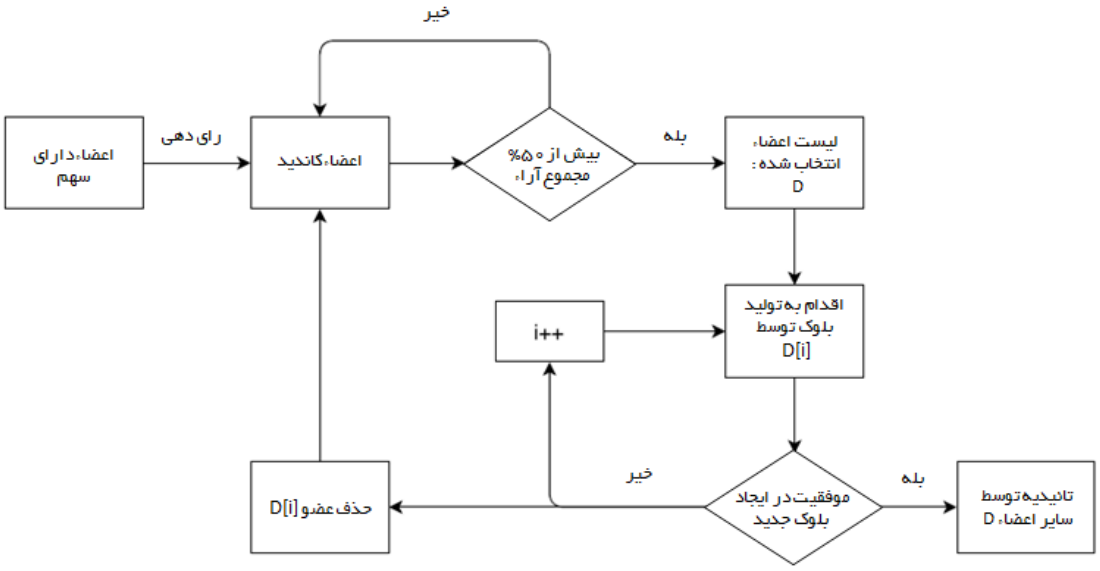
۱-۳-۲. مشکل هزینه‌کرد مجدد

از مشکلات رایجی که در الگوریتم‌های اجماع به‌کار رفته و در بلاک‌چین باید به آن توجه کرد هزینه‌کرد مجدد[1] است. این مشکل زمانی پدید می‌آید که در شبکهٔ رمزارز مبتنی‌بر بلاک‌چین یک رمزارز در دو تراکنش متفاوت استفاده می‌شود و به‌این‌ترتیب، از فروشندگانی که رمزارز مربوطه را دریافت کرده‌اند به‌نوعی کلاه‌برداری می‌شود. در شکل ۷ یکی از رایج‌ترین سناریوهای رخداد این حالت تشریح شده است که در آن مهاجم‌ها با صرف توان محاسباتی زیاد، ضمن ساختن شاخهٔ جعلی بلندتر در الگوریتم اثبات کار، تراکنش‌های معکوس مدنظر خود را در شاخهٔ جعلی قرار می‌دهند تا تراکنش اصلی و حقیقی انجام‌شده را بی‌اثر کنند. سپس مبلغ آزادشده را در تراکنش‌های بعدی به‌کار می‌برند. در شبکه‌هایی مانند بیت‌کوین، برای جلوگیری از بروز چنین حالتی، زمان تولید هر بلوک را از راه افزودن سختی شبکه بالا می‌برند تا احتمال موفقیت مهاجم در ساختن شاخهٔ جعلی بلندتر را به میزان زیادی کاهش دهند (Bradbury, 2013).



شکل ۸: گردش کار الگوریتم اثبات سهم

1. Double Spend Problem



شکل ۹: گردش کار الگوریتم اثبات سهم تفویض‌شده (DPoS)

۳-۳-۱. الگوریتم اثبات سهم

در این الگوریتم، شانس انتخاب اعضا برای ساختن بلوک جدید تا حدود زیادی به میزان سهم و پولی بستگی دارد که در شبکه به‌ازای وثیقه یا موجودی خود می‌پردازند. در شکل غالب الگوریتم‌های اثبات سهم، علاوه‌بر میزان سهم عضو، که ملاک اصلی است، قدرت محاسباتی محدودی نیز نیاز خواهد بود تا معادلهٔ مرتبط با الگوریتم هَش SHA256 (timestamp, previous hash…) < target * coin حل شود (Zhang and Lee, 2019). همان‌طور که در شکل ۸ نمایش داده شده، برخلافِ الگوریتم اثبات کار، در این الگوریتم چرخهٔ تکرارشوندهٔ یافتن نانس وجود ندارد و هرچه میزان سهم (که در اینجا با پارامتر coin نمایش داده شده است) بیشتر باشد، احتمال انتخاب به‌منزلهٔ عضو اضافه‌کنندهٔ بلوک بیشتر خواهد بود.

رمزارز پی.پی.کوین[1] نخستین‌بار از الگوریتم اثبات سهم در سطحی وسیع استفاده کرد. در رمزارز پی.پی.کوین علاوه‌بر میزان سهم، مدت در اختیار قراردادن سهم نیز مهم بود (King and Nadal, 2012) و با تعریف شاخص جدیدی به نام «قدمت سهم» تأثیر هر دو را در آن بررسی کرد. برای نمونه، اگر مقدار سهمی برابر با ۲۰۰ واحد به‌مدت ۱۵ روز در اختیار شبکه باشد، مقدار قدمت سهم برابر با ۳۰۰۰ خواهد بود و اگر این امتیاز برای ساختن بلوک جدید استفاده شود، قدمت سهم به مقدار صفر بازنشانی خواهد شد. علاوه‌بر رمزارز پی.پی. کوین، رمزارزهای دیگری نظیر نکست‌کوین و اروبوروس[2] نیز از الگوریتم اثبات سهم استفاده می‌کنند (Kiayias et al., 2017; Zhang and Lee, 2019) و شبکهٔ اِتریوم نیز به علت مزایای این رمزارز، یعنی داشتن سرعت بالا و مصرف انرژی کمتر، الگوریتم اثبات سهم را به‌جای اثبات کار در شبکهٔ خود به‌کار برده است. از مهم‌ترین مزایای این الگوریتم می‌توان به مصرف انرژی کمتر و داشتن سرعت بالاتر برای ساختن بلوک جدید و همچنین نیاز کمتر به تأمین سخت‌افزار قدرتمند اشاره کرد.

۳-۳-۴. الگوریتم اثبات سهم تفویض‌شده

در این الگوریتم، میزان سهم و فرایند رأی‌گیری با یکدیگر ترکیب می‌شوند و از اعضایی که سهام دارند برای انتخاب عضو اضافه‌کنندهٔ بلوک جدید رأی‌گیری می‌شود. در این صورت سهام‌داران ضمن رأی‌گیری، حق خود را برای ایجادکردن بلوک جدید به عضو انتخاب‌شده تفویض می‌کنند و بدین‌ترتیب توان محاسباتی از ایشان گرفته نخواهد شد (Larimer, 2014). گردش کار الگوریتم اثبات سهم تفویض‌شده (DPoS)[3] در شکل ۹ نمایش داده شده است. طبق این الگوریتم، که حالت پارلمانی دارد، اعضای دارای سهم پس از رأی‌گیری فهرستی از اعضا را برای ساخت بلوک جدید انتخاب می‌کنند که به آن‌ها «شاهد» گفته می‌شود. در این رأی‌گیری هرچه میزان سهم بیشتر باشد، قدرت رأی نیز بیشتر خواهد بود. سپس براساس میزان رأی کسب‌شده و از ابتدای فهرست شاهدان، عضو منتخب تراکنش‌ها و قراردادن آن در بلوک را اعتبارسنجی می‌کند. اگر نتواند این کار را با موفقیت انجام دهد، این حق از وی سلب شده، به عضو دیگر موجود در فهرست شاهدان اعطا می‌شود.

1. PPCoin
2. Ouroboros
3. Delegated Proof of Stake

در مقایسه با الگوریتم‌های اثبات سهم و اثبات کار، الگوریتم اثبات سهم تفویض‌شده سرعت بالاتر و هزینهٔ بسیار کمتری دارد (Zhang and Lee, 2019؛ Alsunaidi and Alhaidari, 2019) و ازاین‌رو، رمزارزهای مطرحی چون بیت‌شیرز[1] و ایی.اُ.اِس[2] از آن در شبکهٔ خود استفاده کرده‌اند (EOS. IO, 2018).

۱-۳-۵. سایر الگوریتم‌های اثبات‌محور

افزون‌بر الگوریتم‌های اثبات‌محور شرح داده‌شده، الگوریتم‌های مطرح دیگری نیز هستند که الگوریتم‌های اثبات کار و اثبات سهم را به روشی جدید ترکیب کرده یا معیار دیگری را برای اثبات کار برگزیده‌اند. برای نمونه، الگوریتم اثبات شانس (PoL)[3] از تولیدکنندهٔ اعداد تصادفی برای انتخاب عضو اضافه‌کنندهٔ بلوک استفاده می‌کند (Milutinovic et al., 2016). در این روش زمانی که دفتر کل میان همهٔ اعضا همگام شد، هر عضو بلوک محلی خود را تشکیل و به زنجیره اضافه می‌کند. سپس عددی تصادفی را در بازه [۱ و ۰] از طریق سخت‌افزار SGX[4] و در بستر TEE[5] تولید می‌کند و در سرآیند[6] بلوک قرار می‌دهد. این عدد، عدد شانس شناخته می‌شود و بلوکی درنهایت به زنجیره اضافه خواهد شد که عدد شانس بیشتری داشته باشد. در این حالت، عدالت به‌نحو مطلوبی رعایت می‌شود و به‌ندرت به حملهٔ هزینه‌کرد مجدد منجر می‌شود؛ چراکه مهاجم باید بسیار خوش‌شانس باشد تا در آن موفق شود.

الگوریتم‌های اثبات سوزاندن (PoB)[7] و اثبات ظرفیت (PoC)[8] از دیگر مواردی هستند که از ایدهٔ متفاوتی استفاده می‌کنند. در الگوریتم‌های اثبات سوزاندن، کاوشگران باید مبالغ یا سکه‌های دیجیتالی خود را به آدرس مشخصی برای سوزانده‌شدن ارسال کنند؛ به این معنا که مبلغ سوخت‌شده بازگشت‌پذیر نخواهد بود و در بازه زمانی مشخص، هر کاوشگری که بیشترین مبلغ را بسوزاند حق امتیاز تشکیل بلوک جدید را خواهد داشت (P4Titan, 2014). در الگوریتم اثبات ظرفیت کاوشگران، به‌جای ارتقای توان پردازشی، باید روی ظرفیت ذخیره‌سازی خود سرمایه‌گذاری کنند که اقتصادی‌تر است. این الگوریتم در خلال اجرای خود، حجم بسیار زیادی از داده‌ها را با نام پلات[9] تولید و در فضای ذخیره‌سازی کاوشگر ذخیره می‌کند. هرقدر تعداد گره‌های پلات‌ها بیشتر باشد، کاوشگر شانس بیشتری برای انتخاب‌کردن خواهد داشت (Dziembowski et al., 2015).

الگوریتم اثبات اهمیت (PoI)[10] نیز، که رمزارز ان.ای.ام[11] از آن استفاده می‌کند، از تعریف مفهوم «اهمیت» برای اعطای حق اضافه‌کردن بلوک جدید بهره می‌برد. مفهوم اهمیت به میزان سرمایه‌ای که در اختیار عضو قرار دارد و همچنین به تعداد تراکنش‌هایی که انجام داده وابسته است. نوآوری به‌کاررفته در این الگوریتم، استفاده از نظریهٔ گراف برای محاسبهٔ شاخص اجماع است. این‌گونه که گراف متناظر تراکنش‌های انجام‌شده ترسیم می‌شود و براساس یال‌های ورودی و خروجی و معیار امتیازدهی خاص خود مهم‌ترین گره (عضو) را شناسایی و حق اضافه‌کردن بلوک جدید را به او واگذار می‌کند (Nem Technical Reference).

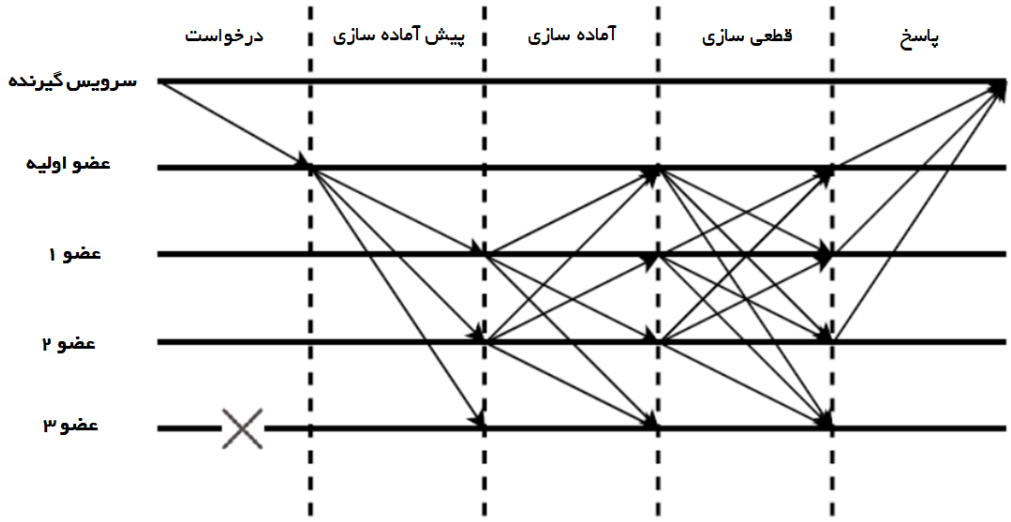
از سایر مدل‌های ترکیبی ثبات کار و اثبات سهم می‌توان به الگوریتم اثبات فعالیت (PoA)[12] اشاره کرد. در این الگوریتم، نخست بلوکی خالی از تراکنش براساس الگوریتم اثبات کار با مقدار مناسب نانس تولید می‌شود. سپس به تعداد N عضو، به‌شکلی تصادفی و بر مبنای مقدار سهم، از میان اعضا انتخاب می‌شوند و فقط عضو آخر حق اضافه‌کردن بلوک به زنجیره را خواهد داشت (Bentov et al., 2014).

۱-۴. الگوریتم‌های اجماع رأی‌محور

در الگوریتم‌های رأی‌محور، اعضای شرکت‌کننده در فرایند اجماع باید قبل از شروع فرایند احراز هویت شوند. همچنین تراکنش به‌شکل جمعی و مشارکتی تأیید می‌شود و امتیازات فردی هر نود (توان پردازش یا میزان سرمایهٔ در اختیار) در این میان تأثیری نخواهد داشت. این مشارکت، با تبادل پیام میان اعضا در سراسر شبکه شکل می‌گیرد. با توجه به احتمال خرابی یا خراب‌کاری احتمالی برخی از اعضا، متاثر از ادبیات سیستم‌های توزیع‌شده، تاب‌آوری در مقابل خطا در الگوریتم‌های رأی‌محور نیز درنظر گرفته می‌شود. ازاین‌رو، این دسته از الگوریتم‌ها در دو دسته به شرح ذیل قرار می‌گیرند:

۱. **تاب‌آور درمقابلِ حملات بیزانس (BFT):**[13] درمقابلِ تهاجم اعضای متخاصم و همچنین خرابی احتمالی اعضا مقاومت دارد و با درصد مشخصی از اعضای سالم شبکه پایدار خواهد بود. حملات بیزانس (Lamport et al., 1982) به وضعیتی اشاره دارد که در آن تعداد n فرمانده ارتش قصد دارند به یک شهر حمله کنند. این فرماندهان از یکدیگر دورند فقط از طریق تبادل پیام با پیک امکان هماهنگی با یکدیگر را دارند. هر فرمانده امکان حمله یا عقب‌نشینی دارد و درصورتی که بخشی از فرماندهان حمله

1. BitShares
2. EOS
3. Proof of Luck
4. Intel Software Guard Extensions
5. Trusted Execution Environment
6. Header
7. Proof of Burn
8. Proof of Capacity or Proof of Space
9. Plot
10. Proof of Importance
11. NEM
12. Proof of Activity
13. Byzantine Fault Tolerance



شکل ۱۰: فرایند پروتکل PBFT

کنند و بخشی دیگر حمله را آغاز نکنند قطعاً شکست می‌خورند و نابود می‌شوند. در این وضعیت، تبادل درست و به‌موقع پیام برای هماهنگی بسیار مهم است و باید به روشی باشد که دستکاری عمدی محتوای پیام را تا حد مقبولی خنثی کند؛

۲- تاب‌آور درمقابلِ خرابی (CFT):[1] فقط درمقابلِ خرابی و از مدار خارج‌شدن درصد مشخصی از اعضا قابلیت تاب‌آوری دارد (Alsunaidi and Alhaidari, 2019 Nguyen and Kim, 2018).

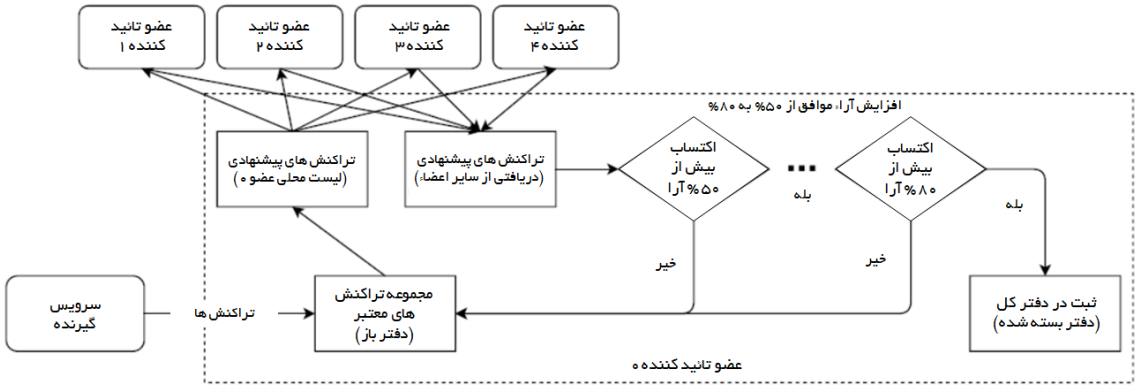
۱-۴-۱. تاب‌آوری کاربردی حملات بیزانس

از مهم‌ترین مباحث در حوزهٔ الگوریتم‌های رأی‌گرا، پروتکل تاب‌آوری کاربردی حملات بیزانس (PBFT)[2] است که در حوزهٔ سیستم‌های توزیع‌شده و غیرهمزمان کاربرد فراوان دارد (Castro and Liskov, 1999؛ Wu et al., 2019). این پروتکل دربردارندهٔ پنج مرحله شامل درخواست، پیش‌آماده‌سازی، آماده‌سازی، قطعی‌سازی و پاسخ است (Zhang and Lee, 2019). همان‌طور که در شکل ۱۰ نمایش داده شده است، عضو اولیه پیامی را که سرویس‌گیرنده ارسال کرده به سه عضو دیگر ارسال می‌کند. در این مثال، که عضو شمارهٔ ۳ از دسترس خارج است، پیام ارسال‌شده برای رسیدن به اجماع، پنج مرحلهٔ گفته‌شده را طی می‌کند و در پایان، پاسخ نهایی به سرویس‌گیرنده ارسال می‌شود و فرایند به‌اجماع‌رسانی به پایان می‌رسد.

چارچوب بلاک‌چین مشهور هایپرلجر فابریک، که شرکت آی.بی.ام تهیه کرده است، از پروتکل تاب‌آوری کاربردی حملات بیزانس استفاده می‌کند که الگوریتم استفاده‌شدهٔ آن شامل دو نوع عضو است: عضو نگه‌دارندهٔ دفتر کل و عضو تأییدکننده. سرویس‌گیرنده در آغاز درخواست خود را به یکی از اعضای تأییدکننده ارسال می‌کند، عضو تأییدکننده تراکنش را بررسی می‌کند و همزمان آن را برای سایر اعضا، که شامل عضو نگه‌دارندهٔ دفتر کل هم می‌شود، ارسال می‌کند. زمانی که تعداد تراکنش‌ها به تعداد معینی رسید و پس از مدت زمانی مشخص، عضو نگه‌دارندهٔ دفتر تراکنش‌های دریافتی را براساسِ زمان تهیه‌کردن آن‌ها مرتب و در بلوک ثبت می‌کند، سه مرحلهٔ پیش‌آماده‌سازی، آماده‌سازی و قطعی‌سازی طی می‌شود. در مرحلهٔ پیش‌آماده‌سازی، عضو نگه‌دارنده دفتر بلوکِ مدنظر خود را برای سایر اعضا ارسال می‌کند. اعضای تأییدکننده، پس از دریافت، آن را در نسخهٔ محلی خود ذخیره می‌کنند. سپس، به‌منظور اطمینان از اصالت بلاکِ دریافت‌شده، درخلال مراحل آماده‌سازی و قطعی‌سازی، آن را در اختیار سایر اعضا نیز قرار می‌دهند. در مرحلهٔ آماده‌سازی، درصورتی که عضو منتشرکننده از بیش از دوسوم اعضا بلوکی مشابه با نسخهٔ محلی خود دریافت کند، مرحلهٔ قطعی‌سازی را مشابه با مرحلهٔ قبلی انجام می‌دهد. با این کار، همهٔ اعضا از اعتبار تراکنش‌ها و بلاک ذخیره‌شدهٔ خود اطمینان حاصل می‌کنند و آن را در نسخهٔ محلی زنجیرهٔ خود قرار می‌دهند (Nguyen and Kim, 2018).

دو زیرساخت مشهور بلاک‌چین دیگر آر.تری کوردا[3] و سیمبیونت[4] هستند که با ایجادکردن تغییراتی، پروتکل تاب‌آوری کاربردی حملات بیزانس را مبنای الگوریتم اجماع خود قرار می‌دهند (ibid). در هر دو سیستم، از الگوریتمی به نام BFT-SMaRt (Bessani et al., 2014) که بسیار استفاده شده است

1. Crash Fault Tolerance
2. Practical Byzantine Fault Tolerance
3. R3 Corda
4. Symbiont



شکل ۱۱: الگوریتم به‌کاررفته در سیستم ریپل

شبیه تاب‌آوری کاربردی حملات بیزانس است، اما نام‌گذاری گام‌های آن متفاوت است (پیشنهاد، ثبت، تأیید درمقابل پیش‌آماده‌سازی، آماده‌سازی و قطعی‌سازی). علاوه‌براین، برای ثبت‌کردن اتفاقاتِ رخ‌داده در هر ماشین سازوکارهایی وجود دارد که درصورت نقص عملکرد و راه‌اندازی مجدد ماشین، بتوان همان روند را ادامه داد. همچنین تندرمینت[1] الگوریتم مطرح دیگری در این حوزه است که با اصلاحاتی در تاب‌آوری کاربردی حملات بیزانس، فرایند به‌اجماع‌رسانی را طی دو مرحله انجام می‌دهد و در هر مرحله گام‌های پیشنهاد، پیش‌رأی و پیش‌ثبت طی می‌شود و بلوک‌ها برحسب موقعیت مسدود (قفل) می‌شوند (Wu et al., 2019). درنهایت و در شرایطی که بلوک مدنظر رأی پیش‌ثبت از حداقل دوسوم اعضا را به‌دست آورد، صلاحیت ثبت در دفتر کل را نیز به‌دست می‌آورد.

۱-۴-۲. ریپل

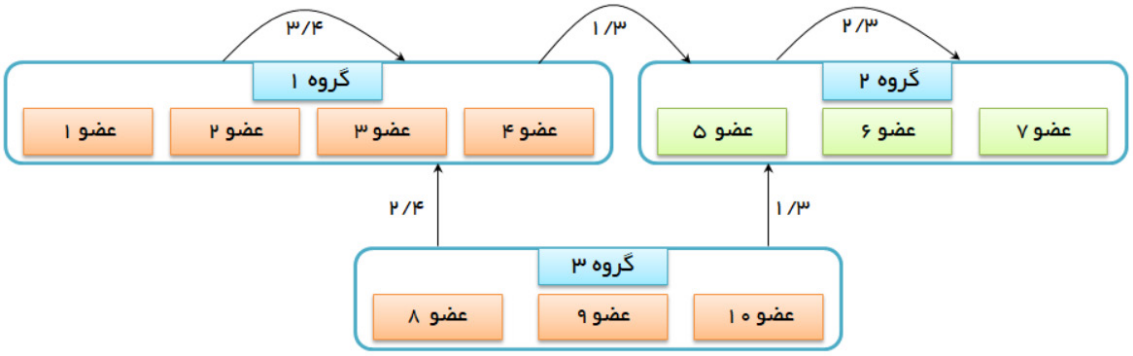
در الگوریتم پروتکل اجماع ریپل[2] یا RPCA،[3] که به‌شکل پروتکل پرداخت متن‌باز طراحی شده است، تراکنش‌ها را اعضای سرویس‌گیرنده آغاز می‌کنند و اطلاعات آن را اعضای دنبال‌کننده یا تأییدکننده در سراسر شبکه انتشار می‌دهند. فرایند اجماع در ریپل را اعضای تأییدکننده پیش می‌برند که هریک فهرستی از اعضای قابل‌اعتماد را، که به آن UNL[4] گفته می‌شود، در اختیار دارند (Wu et al., 2019؛ Schwartz et al., 2014؛ Zhang and Lee, 2019). اعضای مندرج در UNL می‌توانند به تراکنش‌هایی که خود تأیید می‌کنند رأی دهند. همان‌گونه که در شکل ۱۱ نشان داده شده، هر عضو تأییدکننده فهرستی از تراکنش‌هایی را که خود تأیید کرده به‌منزلهٔ پیشنهاد به سایر اعضای تأییدکننده ارسال می‌کند. هنگامی که عضوی تأییدکننده پیشنهادی را از عضو همتای خود در UNL دریافت می‌کند، تراکنش‌های موجود در پیشنهاد را بررسی می‌کند و چنان‌که تراکنش مذکور در فهرست تراکنش‌هایی که خود تأیید کرده وجود داشته باشد، یک رأی مثبت به آن اعطا می‌کند. زمانی که تراکنشی موفق به کسب بیش از ۵۰ درصد آرا شد، وارد دور بعدی می‌شود. در دور دوم، معیار غربالگری سخت‌تر می‌شود و تراکنش‌هایی که بیش از ۸۰ درصد آرای اعضا را به خود اختصاص دهند در دفتر توزیع‌شده درج خواهند شد. دفتر توزیع‌شده در ساختار ریپل، به دو شکل نگه‌داری می‌شود: ۱) آخرین دفتر بسته‌شده که دربردارندهٔ تراکنش‌هایی است که بیش از ۸۰ درصد آرا را کسب کرده‌اند؛ ۲) دفتر باز که شامل تراکنش‌هایی است که هنوز به حدنصاب لازم برای درج‌شدن در دفتر کل نرسیده‌اند (Zhang and Lee, 2019).

از قوانین شبکهٔ ریپل دربارهٔ فهرست UNL آن است که مجموعهٔ UNLهای هر دو عضو تأییدکنندهٔ دلخواه باید دست‌کم به‌میزان ۲۵ درصد با یکدیگر اشتراک داشته باشند. درواقع در ریپل با تنظیم فهرست UNL زیرشبکهٔ امنی برای اِعمال تاب‌آوری حملهٔ بیزانس ساخته است (Wu et al., 2019). برخی از محققان، کنترل بیش از حد آزمایشگاه مرکزی ریپل در امنیت شبکهٔ آن را به رعایت‌نکردن حالت نامتمرکز شبکه تعبیر کرده‌اند (Armknecht et al., 2015).

۱-۴-۳. استلار

پروتکل اجماع استلار[5] یا SCP[6] را می‌توان گونه‌ای از سامانهٔ ریپل برشمرد که در آن همانند نقشی که UNL در ریپل ایفا می‌کند، از گروهی به نام «برش سهمیه»[7] استفاده می‌شود (Mazieres, 2015). در این حالت، اعضای تصدیق‌کننده‌ای

1. Tendermint
2. Ripple
3. Ripple Protocol Consensus Algorithm
4. Unique Node List
5. Stellar
6. Stellar Consensus Protocol
7. Quorum Slice



شکل ۱۲: نمونه‌ای از ساختار برش سهمیه در استلار

که در برش سهمیه مشخص شده‌اند با یکدیگر ارتباط برقرار و اجماع می‌کنند. هر عضو تأییدکننده می‌تواند عضو یک یا چند برش سهمیه باشد. درصورتی که تراکنشی را عضو تصدیق‌کننده تأیید کند، عضو مذکور باید از همهٔ اعضای موجود در برش سهمیهٔ خود برای تأییدکردن تراکنش استعلام بگیرد و اگر اعتبار تراکنش را همهٔ اعضای برش سهمیه تأیید کنند، تراکنش مربوطه معتبر تلقی خواهد شد. مفهوم برش سهمیه، که برگرفته از نظریهٔ مجموعه‌هاست، درواقع نوعی اجرای حالتی به نام رأی‌گیری کنفدراسیونی[1] است که در آن اعضای رأی‌دهنده کمتر است و الزامات تاب‌آوری حملهٔ بیزانسی نیز به‌نحو مطلوبی لحاظ شده است (ibid). شکل ۱۲ نمونه‌ای از ساختار برش سهمیه در SCP را نمایش می‌دهد که مطابق آن، اعضا در سه گروه به‌صورت سلسله‌مراتبی تقسیم‌بندی شده‌اند. در این حالت، برش سهمیهٔ عضو ۱ شامل سه عضو از گروه شمارهٔ ۱ و یک عضو از میان اعضای گروه شماره ۲ است. بدین‌ترتیب، گروه اعضای ۱، ۲، ۳، ۵ و ۱، ۲، ۴، ۶ نمونه‌هایی از برش سهمیه‌های موجود ممکن برای عضو ۱ هستند. همچنین گروه‌های ۱ و ۲ در بالای سلسله‌مراتب قرار می‌گیرند و هر تراکنشی را باید ابتدا این دو گروه تأیید کنند. می‌توان گروه ۱ را بانک و گروه ۲ را ارائه‌دهندهٔ خدمات اعتبارسنجی فرض کرد. گروه ۳ نیز زیرمجموعه‌ای از کاربرانی است که از خدمات پرداخت استفاده می‌کنند. برای نمونه، اگر عضو ۱۰ بخواهد تراکنشی را ثبت کند، باید دو عضو از گروه ۱ و یک عضو از گروه ۲ آن را تأیید کنند.

استلار با این هدف طراحی شد که اولین مکانیسم اجماعِ اطمینان‌پذیری باشد که همزمان چهار ویژگی عدم‌تمرکز، زمانِ تأخیر کم در تأیید تراکنش‌ها، اعتماد انعطاف‌پذیر و امنیت تنظیم‌شونده را داشته باشد. امنیت تنظیم‌شونده بدان معناست که در SCP امنیت عملکرد بر پایهٔ امضای دیجیتال و الگوریتم‌های هَش استوار است که در محیط اجرایی و براساسِ میزان حملات و شرایط کاری می‌توان قدرت محاسباتی لازم برای نفوذ را تا حد بسیار زیادی افزایش داد (Wu et al., 2019).

۱-۴-۴. الگوریتم‌های تاب‌آور در مقابل خرابی (CFT)

از معروف‌ترین الگوریتم‌های این دسته می‌توان به الگوریتم‌های Chain (ibid)، Raft (Nguyen and Kim, 2018) و Paxos (Lamport, 2001) اشاره کرد. الگوریتم Raft در شرایطی که حداقل [n/2 + 1] عضو از اعضای شبکه درست عمل نکنند، عملکرد شبکه همچنان پایدار خواهد بود. در این الگوریتم اعضا به سه دستهٔ دنبال‌کننده، کاندید و رهبر تقسیم می‌شوند که این اعضا با ردوبدل کردن پیام RequestVote برای انتخاب رهبر و AppendEntries برای انتقال درخواست به سایر اعضا با یکدیگر ارتباط دارند؛ به‌گونه‌ای که در یک سری زمانی مشخص، اعضای دنبال‌کننده به اعضای کاندید تبدیل می‌شوند و براساس رأی‌گیری، عضو رهبر تا زمان مشخصی انتخاب می‌شود. پس از این دوره، عضو رهبر دوباره به عضو دنبال‌کننده تبدیل می‌شود و فرایند انتخاب از سر گرفته خواهد شد. فرایند اجماع نیز به این ترتیب خواهد بود که سرویس‌گیرندگان تراکنش‌های خود را برای رهبر ارسال می‌کنند و رهبر نیز آن‌ها را در فهرست ورودی خود ثبت می‌کند. سپس رهبر از راه پیام AppendEntries هریک از تراکنش‌های ثبت‌شده در فهرست ورودی خود (t) را به همراه شمارهٔ ردیف تراکنش قبل از آن (i_{t-1}) برای یکایک اعضای دنبال‌کننده ارسال می‌کند. هنگامی که عضو دنبال‌کننده پیام AppendEntries را دریافت کرد، اگر آخرین تراکنش ثبت‌شدهٔ وی i_{t-1} باشد، t را در فهرست ورودی خود ثبت می‌کند؛ در غیر این صورت، باید آخرین تراکنش ثبت‌شدهٔ خود را، که با رهبر همگام شده است، پیدا کند. سپس تراکنش‌های بعدی آن را در فهرست محلی خود حذف کرده، فهرست را دوباره با رهبر همگام کند. این فرایند تا همگام‌شدن فهرست همهٔ اعضای دنبال‌کننده با فهرست عضوِ رهبر ادامه می‌یابد. هنگامی‌که رهبر از همگام‌بودن تمامی فهرست‌ها اطمینان حاصل کرد، یک شمارهٔ ردیف از فهرست را انتخاب می‌کند و تمامی تراکنش‌های قبل از آن را، به‌منزلهٔ تراکنش‌های نهایی، در بلوک جدیدی ثبت

1. Federated Voting

جدول ۱: تعداد تراکنش در ثانیه برای برخی از رمزارزهای مشهور تا ۲۰۱۸ (Bach et al., 2018)

نام رمزارز	الگوریتم اجماع	تعداد تراکنش در ثانیه (TPS)
بیت‌کوین	PoW	۷
اِتریوم	PoW	۱۵
ریپل	Ripple	۱۵۰۰
بیت‌کوین کش	PoW	۶۰
کاردانو	PoS	۷
استلار	Stellar	۱۰۰۰
ان.ای.او	PBFT	۱۰۰۰۰
لایت‌کوین	PoW	۵۶
ای.او.اس	DPoS	درحد میلیون تراکنش
ان.ای.ام	PoI	۴۰۰۰

و به زنجیره اضافه می‌کند و آن را برای اطلاع سایرین درخلالِ شبکه انتشار می‌دهد.

۲. تجزیه‌وتحلیل داده‌ها و یافته‌های پژوهش

در این بخش، الگوریتم‌های اجماع معرفی‌شده در بخش قبل از منظر کارایی بررسی و مقایسه می‌شوند. معیارهای درنظر گرفته‌شده در این بخش عبارت‌اند از: بهره‌وری و مصرف انرژی، تاب‌آوری در مقابل تعداد مهاجم‌ها، مقیاس‌پذیری، سرعت تولید بلوک، تأخیر اجرای تراکنش، نیاز به سخت‌افزار پیشرفته، درجهٔ عدم‌تمرکز و سربار شبکه. خلاصهٔ نتایج این بررسی در جدول ۲ بیان شده است.

با توجه به تنوع و تعداد حالت‌های اجرای الگوریتم‌های اجماع، برای ارائهٔ تصویری واضح‌تر از مقایسهٔ عملکرد الگوریتم‌های اجماع در معیارهای گوناگون، در اینجا شکل استاندارد الگوریتم‌های PoS، PoW و DPoS از خانوادهٔ الگوریتم‌های اثبات‌محور و حالت استاندارد الگوریتم‌های PBFT، ریپل و استلار از خانواده رأی‌محور بررسی و مقایسه می‌شوند. بدیهی است هرگونه تغییر در حالت استاندارد و معمول الگوریتم‌های فوق، نیازمند تحلیل و بررسی ویژه است و ممکن است با نتایج ارائه‌شده در این بخش سازگاری نداشته باشد.

۲-۱. مصرف انرژی

در میان الگوریتم‌های اجماع، خانوادهٔ PoW بیشترین توان محاسباتی را نیاز دارد؛ چراکه الگوریتم، برای یافتن مقدار مناسب نانس، محاسبات پیچیدهٔ مربوط به هَش‌کردن اطلاعات و مقایسه آن را پیوسته تکرار می‌کند. الگوریتم‌های PoS و DPoS، به علت جایگزین‌کردن محاسبه با میزان وثیقه، توان محاسباتی و مصرف انرژی را به‌شدت محدود می‌کنند (Zhang and Lee, 2019؛ Alsunaidi and Alhaidari, 2019). شایان ذکر است الگوریتم PoS با توجه به محاسبات هَش مصرف انرژی بیشتری در مقایسه با الگوریتم DPoS دارد. الگوریتم‌های خانواده رأی‌محور نیز، با توجه به ماهیت عملکردشان که براساس ارتباط‌سازی در شبکه و تبادل پیام است، مصرف انرژی بسیار محدودی دارند.

۲-۲. تاب‌آوری درمقابلِ مهاجم‌ها

در الگوریتم‌های PoS، PoW و DPoS با توجه به ساختار و طراحی الگوریتم‌های داخلی، مهاجم‌ها باید مقادیر شایان‌توجهی از توان محاسباتی یا وثیقه‌ها را برای فراهم‌کردن کارکرد نادرست شبکه، که همان تشکیل زنجیرهٔ اشتباه به‌جای زنجیرهٔ معتبر است، صرف کنند. برای نمونه، در رمزارز بیت‌کوین، مهاجم باید حداقل به میزان ۵۰ درصد از توان محاسباتی شبکه را در اختیار داشته باشد تا با تشکیل زنجیرهٔ دلخواه حالت مصرف مجدد رمزارز را ارائه کند. ازاین‌رو، در بیشتر اجراهای الگوریتم PoW، درصورتی که مهاجم‌ها بیش از ۵۰ درصد توان محاسباتی شبکه را در اختیار داشته باشند، شبکه در حالت ناپایدار قرار خواهد گرفت. مشابه PoS، PoW و DPoS نیز باید از دراختیار مهاجمان قرارگرفتن بیش از ۵۰ درصد مجموع وثیقه‌های شبکه پیشگیری کنند. در PBFT، اگر تعداد اعضای شبکه را $3f + 1$ درنظر بگیریم، تعداد عضوهای سالم باید بیش از $2f + 1$ باشد تا شبکه عملکرد صحیح از خود نشان دهد. به عبارت دیگر، تعداد مهاجمان شبکه، اگر حداکثر به f عضو برسد، هنوز شبکه تاب‌آوری دارد و پایدار خواهد بود. ازاین‌رو، میزان تاب‌آوری PBFT برابر با ۳۳ درصد خواهد بود (Castro and Liskov, 1999). در این‌باره،

جدول ۲: مقایسهٔ گونه‌های اصلی الگوریتم‌های اجماع براساس عوامل شناخته‌شده در ادبیات موضوع

معیار ارزیابی	الگوریتم‌های اجماع اثبات‌محور			الگوریتم‌های اجماع رأی‌محور		
	PoW	PoS	DPoS	PBFT	ریپل	استلار
مصرف انرژی	بسیار زیاد	کم	بسیار کم	بسیار کم	بسیار کم	بسیار کم
تاب‌آوری درمقابلِ تعداد مهاجم‌ها	٪۵۰	٪۵۰	٪۵۰	٪۳۳	٪۲۰	با توجه به نوع اجرا
مقیاس‌پذیری	بسیار زیاد	بسیار زیاد	بسیار زیاد	بسیار کم	کم	کم
سرعت تشکیل بلاک	پایین	بالا	بسیار بالا	بالا	بالا	بالا
تأخیر اجرای تراکنش	بالا	پایین	بسیار پایین	پایین	پایین	پایین
نیاز به سخت‌افزار پیشرفته	بله	خیر	خیر	خیر	خیر	خیر
میزان عدم‌تمرکز	بسیار بالا	بسیار بالا	بالا	بسیار کم	بسیار کم	کم
سربار شبکه	کم	کم	کم	بسیار زیاد	زیاد	زیاد

تاب‌آوری الگوریتم ریپل برابر با ۲۰ درصد است (Schwartz et al., 2014). بنابراین، تاب‌آوری شبکهٔ ریپل در مواجهه با حملهٔ بیزانس به میزان ۲۰ درصد از کل اعضای شبکه خواهد بود و تا این مقدار، شبکه کارکرد صحیح خود را حفظ خواهد کرد. در الگوریتم استلار میزان تاب‌آوری به چینش و ترکیب اعضا در برش‌های سهمیه وابسته است. بنابراین، مقدار مشخص و پیش‌فرضی را نمی‌توان برای آن تعیین کرد (Wu et al., 2019).

۲-۳. مقیاس‌پذیری

از مهم‌ترین معیارها برای استفادهٔ عملی و گسترده از بلاک‌چین معیار مقیاس‌پذیری است (ibid). الگوریتم‌های PoW، PoS و DPoS عملاً مقیاس‌پذیری مناسبی نشان داده‌اند؛ چراکه شبکه‌هایی نظیر بیت‌کوین، بیت‌شیرز، پیرکوین[1] و اِتریوم با تعداد اعضای بسیار زیاد درحالِ فعالیت و گسترش‌اند. اگرچه TPS الگوریتم‌های فوق زیاد نیست، راهکارهایی برای افزایش مقیاس‌پذیری آن‌ها پیشنهاد شده است. برای مثال، بیت‌کوین شبکهٔ رعدآسا[2] را برای پرداخت‌های غیرزنجیره‌ای معرفی کرده است تا سرعت و مقیاس‌پذیری را به‌نحو مطلوبی افزایش دهد (Poon and Dryja, 2016). اِتریوم نیز فناوری شاردینگ[3] و پلاسما را در سطوح لایه‌های ۱ و ۲ مطرح کرده است تا سرعت و مقیاس‌پذیری شبکه را افزایش دهد (Poon and Buterin, 2017). به‌نسبت خانوادهٔ اثبات‌محور، الگوریتم‌های رأی‌محور مقیاس‌پذیری کمتری دارند؛ چراکه این الگوریتم‌ها بیشتر در شبکه‌های خصوصی یا کنسرسیومی با اعضای محدودتر استفاده می‌شوند و حجم تبادل پیام در آن‌ها در مقیاس‌پذیری تأثیر می‌گذارد (Alsunaidi and Alhaidari, 2019; Vukolic, 2015).

۲-۴. سرعت تولید بلوک و تأخیر در اجرای تراکنش

سرعت اجرای تراکنش از مدت زمان لازم برای تأیید تراکنش‌ها در شبکهٔ اعضا متأثر است. سرعت تولید بلوک نیز از سرعت تأیید تراکنش‌ها و مدت زمان لازم برای انتخاب عضو مجاز ایجادکنندهٔ بلوک متأثر است (Alsunaidi and Alhaidari, 2019). در میان الگوریتم‌های اجماع، PoW نیازمند بیشترین توان محاسباتی است و در نمونهٔ بیت‌کوین توان پردازش تراکنش‌ها در ثانیه (TPS) بین ۳ تا ۷ است که این مسئله برنامه‌های کاربردی این حوزه را به‌شدت محدود می‌کند. در شبکهٔ ریپل، چرخه‌های به‌اجماع‌رسانی به‌سرعت اتفاق می‌افتد و ازاین‌رو، برای کاربرد در معاملات روزمره بسیار مناسب است (Zhang and Lee, 2019). در پژوهش‌های ارائه‌شده (Alsunaidi and Alhaidari, 2019) مشخص شده است که شبکه‌های بلاک‌چین خصوصی به‌نسبت سایر انواع شبکه‌ها TPS بهتری دارند. در جدول ۱ تعداد تراکنش در ثانیه برای برخی از رمزارزهای مشهور تا ۲۰۱۸ ارائه شده است.

۲-۵. نیاز به سخت‌افزار پیشرفته

با توجه به وجود رابطهٔ مستقیم میان توان محاسباتی و نیاز به سخت‌افزار پیشرفتهٔ اعضای کاوشگر، خانوادهٔ الگوریتم‌های PoW به تأمین سخت‌افزار قدرتمند نیاز بیشتری دارند؛ چراکه در این الگوریتم عضوی برندهٔ رقابت خواهد شد که معمای محاسباتی را زودتر از سایرین حل کند که این موضوع با سخت‌افزار تخصیص‌یافته به این کار ارتباط مستقیم دارد (Zhang and Lee, 2019)؛ درحالی‌که در سایر الگوریتم‌ها این الزام وجود ندارد و سخت‌افزار برتر لزوماً مزیت به‌شمار نمی‌رود.

1. Peercoin
2. Lightening Network
3. Sharding Technology

۲-۶. میزان عدم‌تمرکز

سیستم‌های بلاک‌چین امروزی ازنظرِ میزان تمرکز به سه گروه تقسیم می‌شوند. در شبکه‌های بلاک‌چین عمومی، تمامی اعضا می‌توانند در فرایند اجماع شرکت کنند و به دفتر کل توزیع‌شده دسترسی داشته باشند. الگوریتم‌های PoS، PoW و DPoS کاربرد گسترده‌ای در این نوع شبکه‌ها دارند. نوع دوم و سوم، شبکه‌های خصوصی و کنسرسیومی‌اند که در آن‌ها فقط اعضای خاصی و با کسب احراز هویت مجوز شرکت در شبکه و فرایند اجماع را به‌دست می‌آورند. ازآنجاکه هویت اعضا در PBFT، ریپل و استلار برای سایرین مشخص است، بنابراین این الگوریتم‌ها برای بلاک‌چین‌های خصوصی یا کنسرسیومی مناسب‌اند. اگرچه شبکه‌های خصوصی و کنسرسیومی به اندازهٔ شبکه‌های عمومی حالت عدم‌تمرکز را ندارند، به علت سازگاری و بازدهی بیشتر در فرایند اجماع، در کاربردهای تجاری و پزشکی بیشتر به آن‌ها توجه می‌شود (ibid).

۲-۷. تولید سربار شبکه

در الگوریتم‌های رأی‌محور، در هر چرخهٔ کاریِ به‌اجماع‌رسانی، حجم پیام‌های زیادی میان اعضای شبکه مبادله می‌شود که این امر موجب تولید سربار در شبکه می‌شود (ibid). بنابراین، در صورتی که ظرفیت و سرعت شبکهٔ ارتباطی میان اعضا عملکرد مناسبی نداشته باشد، این خانواده از الگوریتم‌ها دچار اشکال خواهند شد. در میان الگوریتم‌های رأی‌محوری که ازنظرِ میزان تبادل پیام در شبکه با هم مقایسه شده‌اند الگوریتم PBFT بالاترین میزان سربار را دارد؛ زیرا اطلاعات تقریباً میان همهٔ اعضای شبکه ردوبدل می‌شود. اما در الگوریتم ریپل و استلار، این تبادل به محدودهٔ فهرست‌های UNL یا برش سهمیه محدود می‌شود و درنتیجه سربار کمتری دارند.

نتیجه‌گیری

در این پژوهش، الگوریتم‌های اجماع استفاده‌شده در شبکه‌های بلاک‌چین، که در جدول ۳ شرح داده شده‌اند، کاملاً مورد بررسی قرار گرفته‌اند. الگوریتم‌های مذکور را می‌توان در دو گروه اثبات‌محور و رأی‌محور طبقه‌بندی کرد که در طبقهٔ نخست صلاحیت عضو سنجشگر با برگزاری رقابتی درون‌شبکه‌ای مشخص می‌شود و در طبقهٔ دوم، سنجش صلاحیت از راه سازوکار رأی‌گیری حاصل می‌گردد. مهم‌ترین الگوریتم‌های اثبات‌محور، الگوریتم‌های اثبات کار (PoW)، اثبات سهم (PoS) و اثبات سهم تفویض‌شده (DPoS) هستند که با توجه به ویژگی‌های خود کاربرد گسترده‌ای دارند. در خانوادهٔ الگوریتم‌های رأی‌محور نیز الگوریتم‌های تجاری ریپل، استلار و همچنین الگوریتم‌های تاب‌آوری کاربردی حملات بیزانس (PBFT) و تاب‌آور در مقابلِ خرابی (CFT) مهم‌ترین الگوریتم‌های موجود در ادبیات موضوع‌اند.

سپس برای مقایسه و ارزیابی الگوریتم‌های بررسی‌شده، معیارهای مهم و پرکاربرد از ادبیات موضوع شناسایی و استخراج شدند. به‌این‌ترتیب، هفت معیار مصرف انرژی، تاب‌آوری در مقابلِ تعداد مهاجم‌ها، مقیاس‌پذیری، سرعت تولید بلاک، تأخیر در اجرای تراکنش، نیاز به سخت‌افزار پیشرفته، میزان عدم‌تمرکز و سربار شبکه برای هر الگوریتم بررسی شدند و جدولی مقایسه‌ای (جدول ۲) در این‌خصوص تنظیم شد.

جدول ۳: الگوریتم‌های اجماع بررسی‌شده در این پژوهش

خانوادهٔ الگوریتم	عنوان الگوریتم	منابع بررسی‌شده
الگوریتم‌های اجماع اثبات‌محور	الگوریتم اثبات کار (PoW)	(Nakamoto and Bitcoin, 2008) (Sompolinsky and Zohar, 2013) (Bradbury, 2013)
	الگوریتم اثبات شانس (PoL)	(Milutinovic et al., 2016)
	الگوریتم‌های اثبات سوزاندن (PoB)	(P4Titan, 2014)
	اثبات ظرفیت (PoC)	(Dziembowski et al., 2015)
	الگوریتم اثبات اهمیت (PoI)	(Nem Technical Reference)
	الگوریتم اثبات فعالیت (PoA)	(Bentov et al., 2014)
	الگوریتم اثبات سهم (PoS)	(Zhang and Lee, 2019) (King and Nadal, 2012) (Kiayias et al., 2017)
	الگوریتم اثبات سهم تفویض‌شده (DPoS)	(Larimer, 2014) (Alsunaidi and Alhaidari, 2019)

خانوادهٔ الگوریتم	عنوان الگوریتم	منابع بررسی‌شده
الگوریتم‌های اجماع رأی‌محور	تاب‌آوری کاربردی حملات بیزانس(PBFT)	(Castro and Liskov, 1999) (Wu et al., 2019) (Zhang and Lee, 2019) (Nguyen and Kim, 2018)
	الگوریتم‌های تاب‌آور درمقابلِ خرابی (CFT)	(Nguyen and Kim, 2018) (Lamport, 2001)
	ریپل	(Schwartz et al., 2014) (Zhang and Lee, 2019) (Wu et al., 2019) (Armknecht et al., 2015)
	استلار	(Mazieres, 2015) (Wu et al., 2019)

با توجه به مطالعات انجام‌شده، الگوریتم‌های اثبات کار از خانوادهٔ الگوریتم‌های اثبات‌محور تاکنون بیشترین و گسترده‌ترین کاربرد را در شبکه‌های بلاک‌چین داشته‌اند و ویژگی غیرمتمرکز و توزیع‌شدگی شبکه‌های بلاک‌چین را به‌خوبی نشان داده‌اند. این امر به علت ویژگی‌های این الگوریتم در پذیرش نامحدود اعضا و تا حدودی تأثیرناپذیری کلی آن از تعداد اعضای شبکه حاصل شده است. از سوی دیگر، با گسترده‌ترشدن شبکه‌های مبتنی بر الگوریتم‌های اثبات کار، چالش‌های مهمی ازجمله میزان مصرف انرژی و مخاطرات امنیتی پدید آمده‌اند. مخاطرات امنیتی، که عمدتاً ناشی از تشکیل شاخهٔ جعلی و فراهم‌کردن شرایط حملهٔ هزینه‌کرد مجدد است، از راه طولانی‌ترکردن زمان اجرای تراکنش‌ها تاحدودی بهبود یافته است. اما درعوض موجب افت شدید سرعت تولید بلاک و تأخیر زیاد در اجرای تراکنش‌ها شده است. به همین علت، به الگوریتم‌های اثبات سهم (PoS) و اثبات سهم تفویض‌شده (DPoS) توجه شده است و شبکه‌های بزرگ به‌تدریج درپیِ جایگزین‌کردن PoW با الگوریتم‌های مذکورند. البته به این معنا نیست که الگوریتم‌های PoS و DPoS بدون چالش‌اند، بلکه مخاطرات امنیتی، به‌ویژه در حوزهٔ مقدار سهم و تعیین برنده و عامل تأییدکنندهٔ تراکنش‌ها، مبحث مهمی است که نیاز به بررسی و کار پژوهشی ویژه‌ای دارد.

خانوادهٔ الگوریتم‌های رأی‌محور کاملاً مناسب شبکه‌های خصوصی و کنسرسیومی است که در آن اعضا پس از فرایند احراز هویت قوی می‌توانند در شبکه فعالیت کنند. با توجه به نظام پارلمانی موجود در جوامع انسانی، این الگوریتم‌ها نیز براساس تعداد آرایی که هر کاندیدا کسب کرده، تراکنش‌ها یا اعضای صلاحیت‌دار را انتخاب می‌کنند. در این الگوریتم‌ها، تبادل پیام میان اعضا برای هماهنگی و اجرای سازوکار رأی‌دهی نقشی اساسی دارد. ازنظرِ مصرف انرژی، این الگوریتم‌ها بسیار بهینه‌اند، اما شدیداً از ناحیهٔ افت کارایی شبکه، به علت بالارفتن حجم ارسال و دریافت پیام، تهدید می‌شوند. ازاین‌رو، ایجاد حالت بهینه در تبادلات و ارتباطات مبنای شکل‌گیری پروتکل‌های ریپل و استلار بوده است. چالش جدی دیگری که در این حوزه مطرح است، امکان جهت‌دارشدن آرا و ایجاد حالت لابی‌گری در عملکرد شبکه است که ممکن است اعضایی که ارتباطات و نفوذ گسترده‌ای دارند منافع اعضای ضعیف‌تر را پایمال و قدرت شبکه را به‌سمت منافع خود هدایت کنند؛ به‌ویژه اینکه به علت سازوکار احراز هویت و سایر فرایندهای کنترلی، حالت غیرمتمرکز و توزیع‌شدگی شبکه، در مقایسه با شبکه‌های عمومی و الگوریتم‌های اثبات‌محور، کمتر رعایت می‌شود. هرچند این موضوع ابعاد پیچیده‌ای دارد، به‌نظر می‌رسد که با افزایش تعداد اعضای فعال در شبکه، احتمال رخداد آن کمتر یا دست‌کم تعدیل شود. بنابراین، انجام‌دادن کاری پژوهشی به‌منظورِ معرفی الگوریتم‌هایی که با کمترین تبادلات پیام بتوانند اجماع ایجاد کنند، راهگشاست و هدف آرمانی الگوریتم رأی‌محور بهینه را محقق می‌سازد.

منابع

پوریان، سعید کاظم، شهبازی، محمد و تقوا، محمدرضا (۱۳۹۹). «امن‌سازی رایانش مرزی از طریق زنجیرهٔ بلوکی». سیاست‌نامهٔ علم و فناوری، دورهٔ ۱۰، شمارهٔ ۱، ص ۱۷-۳۸.

Abeyratne, S. A. and Monfared, R. P. (2016). "Blockchain ready manufacturing supply chain using distributed ledger". *International Journal of Research in Engineering and Technology*, 5(9), pp. 1-10.

Alsunaidi S., J. and Alhaidari, F. A., (2019). "A

Survey of Consensus Algorithms for Blockchain Technology". In 2019 International Conference on Computer and Information Sciences (ICCIS), pp. 1-6. IEEE. https://ieeexplore.ieee.org/xpl/conhome/8710212/proceeding.

Armknecht, F., Karame, G. O., Mandal, A., Youssef, F. and Zenner, E. (2015). "Ripple: Overview and outlook". In International Conference on Trust and Trustworthy Computing, pp. 163–180. Springer, Cham.

Attaran, M. and Gunasekaran, A. (2019). *Applications of Blockchain Technology in Business: Challenges and Opportunities*. Springer Nature.

Bach, L.M., Mihaljevic, B. and Zagar, M. (2018). "Comparative analysis of blockchain consensus algorithms". In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1545-1550. IEEE.

Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M. (2014). "Proof of activity: Extending bitcoin's proof of work via proof of stake". *ACM SIGMETRICS Performance Evaluation Review*, 42(3), pp. 34-37.

Bessani, A., Sousa, J. and Alchieri, E. E. (2014). "State machine replication for the masses with BFT-SMART". In 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 355-362. IEEE. https://www.computer.org/csdl/proceedings/dsn/2014/12OmNBBhN9G.

Bradbury, D. (2013). "The problem with Bitcoin". *Computer Fraud and Security*, 2013(11), pp. 5–8.

Cachin, C. (2016), "Architecture of the hyperledger blockchain fabric". In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 310(4).

Castro, M. and Liskov, B. (1999). "Practical Byzantine fault tolerance". In *OSDI*, 99(1999), pp. 173–186.

Cohn, J. M., Finn, P. G., Nair, S. P., Panikkar, S. B. and Pureswaran, V. S. (2017). "Autonomous decentralized peer-to-peer telemetry". *U.S. Patent Application* No. 15/138,619.

Croman, K., Decker, C., Eyal, I., Gencer, A. E. and Juels E. A. A. (2016). "On scaling decentralized blockchains". *ICFCDStra*, Christ Church, Barbados, pp. 106–125.

Dziembowski, S., Faust, S., Kolmogorov, V. and Pietrzak, K. (2015). "Proofs of space". In Advances in Cryptology conference, pp. 585-605. Springer, Berlin, Heidelberg.

EOS. IO. (2018). EOS.IO Technical White Paper v2. from https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md, 2018.

Ethereum [Online]. Available: https://www.ethereum.org.

Feng, Q., He, D., Zeadally, S., Khan, M. K. and Kumar, N. (2019). "A survey on privacy protection in blockchain system". *Journal of Network and Computer Applications*, 126, pp. 45-58.

Haber, S. and Stornetta, W. S. (1991). "How to time-stamp a digital document". *Journal of Cryptology*, 3(2), pp. 99-111.

Kiayias, A., Russell, A., David, B. and Oliynykov, R. (2017). "Ouroboros: A provably secure proof-of-stake blockchain protocol". In Annual International Cryptology Conference, *Springer*, Cham, pp. 357–388.

King, S. and Nadal, S. (2012). "PpCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". *Self-published paper*, August, 19, p. 1.

Lamport, L., Shostak, R. and Pease, M. (1982). "The Byzantine Generals Problem ACM Transactions on Programming Languages and Systems". *ACM Transactions on Programming Languages and Systems*, 4(3), pp. 382-401.

Lamport, L. (2001). "Paxos made simple". *ACM Sigact News*, 32(4), pp. 18-25.

Larimer, D. (2014). "Delegated proof-of-stake (dpos)". *Bitshare whitepaper*. https://steemit.com/bitshares/@testz/bitshares-history-delegated-proof-of-stake-dpos

Mazieres, D. (2015). "The Stellar consensus protocol: A federated model for internet-level consensus". *Stellar Development Foundation*, Page 32.

Milutinovic, M., He, W., Wu, H. and Kanwa, M.

(2016). “Proof of luck: An efficient blockchain consensus protocol”. In Proceedings of the 1st Workshop on System Software for Trusted Execution (pp. 1-6).

Nakamoto, S. and Bitcoin, A (2008). “A peer-to-peer electronic cash system”. *Bitcoin* –URL ftom https://bitcon. Org/bitcoin.pdf.

Nem technical reference. Available: https://nem:io/wp-content/themes/nem/files/NEM techRef: pdf.

Nguyen, G. T. and Kim, K. (2018). “A Survey about Consensus Algorithms Used in Blockchain”. *Journal of Information Process Systems*, 14(1), pp.101-128.

Nxt wiki, (2016). Whitepaper: Nxt, [Online]. from https://nxtwiki.org/wiki/Whitepaper:Nxt.

P4Titan (2014). Slimcoin: a peer-to-peer crypto-currency with proof-of-burn [Online]. from http://www.doc.ic.ac.uk/~ids/realdotdot/crypto_papers_etc_worth_reading/proof_of_burn/slimcoin_whitepaper.pdf.

Poon, J. and Dryja, T. (2016). “The bitcoin lightning network: Scalable off-chain instant payments”. https://lightning.network/lightning-network-paper.pdf

Poon, J. and Buterin, V. (2017). “Plasma: Scalable autonomous smart contracts”. *White Paper*, pp.1-47.

Popov, S. (2016). “A probabilistic analysis of the Nxt forging algorithm”. *Ledger*, 1, pp. 69-83.

QuorumChain Consensus [Online]. Available: https://github.com/jpmorganchase/quorum/wiki/QuorumChain-Consensus.

Robert, E. (2017). *Digital signatures*, [Online]. from http://cs.stanford.edu/people/eroberts/courses/soco/projects/public-key-cryptography/dig_sig.html.

Schwartz, D., Youngs, N. and Britto, A. (2014). “The ripple protocol consensus algorithm, [Online]. From https://ripple.com/files/ripple_consensus_whitepaper.pdf.

Sompolinsky, Y. and Zohar, Z. (2013). “Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains”. *IACR Cryptol*. ePrint Arch., 2013, p. 881.

Tschorsch, F. and Scheuermann, B. (2016). “Bitcoin and beyond: a technical survey on decentralized digital currencies”. *IEEE Communications Surveys and Tutorials*, 18(3), pp. 2084–2123.

Yang, R., Yu, F. R., Si, P., Yang, Z. and Zhang, Y. (2019). “Integrated blockchain and edge computing Systems: A Survey, Some Research Issues and Challenges”. *IEEE Communications Surveys and Tutorials*, 21(2), pp. 1508–1532.

Yu, F. R., Liu, J., He, Y., Si, P. and Zhang, Y. (2018). “Virtualization for distributed ledger technology (vDLT)”. *IEEE Access*, 6, pp. 25019–25028.

Yu, F. R. He, Y (2019). “A service-oriented blockchain system with virtualization”. *Transactions on blockchain technology and Applications*, 1(1), pp. 1–10.

Vukolic, M. (2015). “The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication”. In International Workshop on Open Problems in Network Security, pp. 112-125, Springer, Cham.

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M. and Rong, C. (2019). “A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond”. *IEEE Internet of Things Journal*, 6(5), pp. 8114-8154.

Zhang, S. and Lee, J. H. (2019). Analysis of the main consensus protocols of blockchain, *ICT Express*, 6(2), pp. 93-97.

An Applied Investigation of Consensus Algorithms Used in Blockchain Networks

Mohammad Shahbazi[1]
Saeed Kazem Pourian[2]
Mohammad Reza Taghva[3]

Abstract

Today, Blockchain technology is seen as a revolutionary technology in the business environment, and the peak of its prosperity was the introduction of Bitcoin in 2008. Blockchain networks allow centralized databases and general ledgers to be replaced, protected, and distributed databases to network members recognized as network verifiers. The most important part of the Blockchain network structure is the consensus algorithm, which determines how a new block between all nodes in the verifying network is agreed to be appended. In other words, consensus algorithms decide rules and protocols that define which block and by which member to connect to the main chain, and prevent parallel and conflicting structures. Consensus algorithms can be divided into two principal classes. The first category is proof-based consensus algorithms, which allow the nodes that enter the verifying network to demonstrate that they are more eligible and better than the others to do the new block that is to be added. The second group is consensus algorithms focused on voting, allowing nodes in the network to share their results from checking a transaction or a new block before making the final decision. In this paper, we discuss consensus algorithms that have been researched and are currently being applied in some well-known Blockchain applications, while discussing and comparing key features in various aspects.

Keywords: Consensus algorithms, Blockchain, Proof-based Algorithms, Vote-based Algorithms

---

1. Ph.D Student of Allameh Tabataba'i Uniersity; m.shahbazi@gmail.com

2. Ph.D Student of Allameh Tabataba'i University

3. Associate Professor of Allameh Tabataba'i University