فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری

سال هفتم، شماره ۸۹، تابستان ۱۴۰۲، ص ۲۰۹۳-۲۰۶۷

Journal of New Research Approaches
in Management and Accounting

ISSN: 2588-4573
http://www.majournal.ir

ارزیابی استحکام صورت عملیات گسسته رخداد در سیستم بلاکچین ارزهای دیجیتال

حسین شادی [*1]
یعقوب فرجامی [2]

تاریخ دریافت: ۱۴۰۲/۰۵/۰۱ تاریخ چاپ: ۱۴۰۲/۰۶/۲۰

چکیده

ویژگی اصلی پول دیجیتالی ناشناسی فرآیند نقل و انتقال آن است عده ای این را مزیت پول دیجیتالی می‌دانند و معتقدند از این طریق، می توانند حریم خصوصی خود را از دید مراکز امنیتی و نیز جمع آوری اطلاعات شخصی از سوی موسسه های مالی و پرداختهای الکترونیک مانند ویزا حفظ کنند؛ اما در عوض برخی دولت ها با دست گذاشتن روی همین نکته استفاده از آن را در کشورشان ممنوع یا محدود کرده اند زیرا اعتقاد دارند از طریق این سیستم، پولهای کثیف رد و بدل میشود و امنیت اجتماعی و ملی کشورها به خطر می افتد. از این رو راه برای برخی از مهاجمان و سواستفاده کنندان در این سیستم هموار شده که نیاز اساسی برای حفظ امنیت برای جلوگیری از حملات کرد، به دلیل اینکه ماهیت آن به ارز کشور خاصی بستگی ندارد تا مادامی که دو طرف با پول دیجیتالی مبادله می‌کنند نیاز به تبدیل آن به ارزهای دیگر برای پرداخت و انتقال نیست این ایده در خود نوعی ابداع یک پول جهانی را دارد که به مرز خاصی محدود باشدکه نیاز اساسی ارزهای دیجیتال در یک زنجیره بلوکی سیستم توضیع شده می طلبد، دراین پژوهش با دو الگوریتم (Nitti et.al) و (Ing-Rayet.al) که در زنجیره بلوکی سیستم های توضیع در ارزهای دیجیتال استفاده می شود در برابر حوادث و حملات احتمالی ارزیابی و مقایسه می‌شوند و نتایج آن با استناد از نتایج بدست آمده از دیگر پژوهش‌ها تایید می‌شود، سپس با نتیجه بدست آمده سیستم اجماعی توصیه می شود که جامع تر بوده و عیوب کمتری نسبت به دیگر الگوریتم ها دارد.

واژگان کلیدی

ارزهای دیجیتال، سیستم‌های توضیع، گسسته رخداد، ارزیابی استحکام

[1] کارشناسی ارشد، مهندسی فناوری اطلاعات، دانشگاه قم، قم. ho3einshadi@gmail.com
[2] دانشیار، مهندسی کامپیوتر، دانشگاه قم، قم. farjami@gmail.com

۱. پیشینه پژوهش ارزهای دیجیتال

این الگوریتم‌ها هستند که فرایندهای اجماع در هریک از بلاک‌چین‌ها را از بلاک‌چین دیگر متفاوت می‌کنند. شبکه بلاک چین در فضایی واحد به میلیون‌ها نفر خدمات ارائه می‌دهد. باتوجه‌به اهمیت الگوریتم‌های اجماع در فهم نحوه کارکرد بلاک چین، در این مقاله انواع این الگوریتم‌ها را معرفی کرده‌ایم.

شکل 1: الگوریتم‌های اجماع در سیستم‌های بلاکچین

۲. الگوریتم اجماع

بلاک‌چین‌ها درحقیقت پایگاه‌های داده توزیع‌شده‌ای هستند که ذخیره و انتقال و تبادل اطلاعات را بدون نیاز به نهاد متصدی مرکزی انجام می‌دهند. بیشتر بلاک‌چین‌ها روی شبکه‌ای از نودهای مستقل توزیع‌شده ساخته شده‌اند و این نودها برای انجام تراکنش‌هایی که در این شبکه روی می‌دهد، باهم همکاری می‌کنند؛ بنابراین ضرورت دارد که هر شبکه بلاک چین مکانیسمی داشته باشد که ازطریق آن بتواند مطمئن شود که اطلاعات همه نودها باهم منطبق است و روی این موضوع با یکدیگر توافق دارند که کدام تراکنش‌ها صحیح هستند و باید به بلاک چین اضافه شوند. به این سیستم غیرمتمرکز که

وضعیت صحیح بلاک چین را تعیین می‌کند، مکانیسم اجماع[1] می‌گویند. مکانیسم‌های اجماع علاوه‌بر تضمین اجرای همه عملیات یک بلاک چین، می‌توانند روی ویژگی‌های مالی و امنیتی شبکه نیز تأثیر مستقیم بگذارند.

۳. انواع الگوریتم‌های اجماع در بلاک چین

بیشتر بلاک‌چین‌ها سه ویژگی اصلی دارند: «مقیاس‌پذیری» و «تمرکززدایی» و «امنیت». توسعه‌دهندگان هر بلاک چین به‌دنبال راهی هستند تا این سه ویژگی را ازطریق کدهای برنامه‌نویسی در شبکه وارد کنند. ویتالیک بوترین، بنیان‌گذار اتریوم، این سه ویژگی را سه‌گانه بلاک چین[2] نام‌گذاری کرده است؛ چون جمع‌کردن هم‌زمان هر سه آن‌ها در بلاک چین کار دشواری است. تلاش برای طراحی و پیاده‌سازی مدل حاکمیتی غیرمتمرکز برای بلاک چین که تعادلی میان این سه ویژگی برقرار کند، مشکلی است که همچنان ادامه دارد؛ ازاین‌رو، هر بلاک چین مکانیسم اجماعی را برای خود انتخاب می‌کند که با اولویت‌های راهبردی‌اش بیشترین مطابقت را دارد. درادامه مطلب، رایج‌ترین الگوریتم‌های اجماع را به‌اختصار معرفی خواهیم کرد.

۳-۱. اثبات کار

الگوریتم اجماع اثبات کار[3] یا PoW مکانیسم اجماع غیرمتمرکزی است که مشارکت‌کنندگان در شبکه را به حل معمایی ریاضی با استفاده از قدرت محاسباتی ملزم می‌کند تا از اقدامات مخرب و اسپم در سیستم جلوگیری کند. در این روش، همه ماینرها تلاش می‌کنند تا معمای ریاضی را حل کنند و کسی که موفق شود آن را حل کند، بلاک بعدی را ایجاد و در ازای آن پاداش دریافت می‌کند.

بیت کوین اولین ارز دیجیتالی است که از روش اجماع اثبات کار استفاده کرد. هر بلاک یک هِدِر[4] دارد که از هش حاوی اطلاعاتی ازجمله عددی ۳۲ رقمی به نام نانس[5]تشکیل شده است. هش خروجی تابعی یک‌طرفه است که ورودی آن را نمی‌توان از روی خروجی حدس زد. ماینرها باید هِدِر بلاک بعدی را با استفاده از نانس‌های مختلف وارد تابع هش کنند تا زمانی‌که خروجی هش کمتر یا مساوی هش هدف را پیدا کنند که خود بلاک چین تعیین می‌کند. هر ماینری که هش مدنظر را پیدا کند، درواقع برنده حل همان معمای ریاضی است. اثبات کار امنیت بلاک چین را تأمین و آن را از دست‌کاری و حملات هکری و دوبار خرج‌کردن[6] محافظت می‌کند؛ اما انتقادهایی هم به این روش وارد است که مهم‌ترین آن‌ها مصرف بسیار زیاد انرژی است. الگوریتم اثبات کار به قدرت محاسباتی بسیاری نیاز دارد که به مصرف انرژی فراوانی منجر می‌شود. گفتنی است علاوه‌بر بیت کوین، اتریوم نیز از این روش استفاده می‌کند؛ اما در حال انتقال به روش دیگری به نام اثبات سهام است که برای حل مشکلات اثبات کار طراحی شده است.

---

[1] Consensus Mechanism
[2] Blockchain Trilemma
[3] Proof of Work
[4] Header
[5] Nonce
[6] Double Spending

۳-۲. اثبات سهام

در مکانیسم اجماع اثبات سهام[۷] یاPoS ، مشارکت‌کنندگان به‌جای صرف قدرت محاسباتی و انرژی، باید مقداری از ارز دیجیتال همان بلاک چین را سهام‌گذاری [۸]کنند. در این روش، هرکسی که سهام بیشتری در شبکه داشته باشد، بخت بیشتری برای برنده‌شدن و دریافت پاداش دارد. ابتدا عده‌ای از سهام‌گذاران به‌صورت تصادفی انتخاب می‌شوند تا به‌عنوان نود فعالیت کنند. این نودها باید مقداری حداقلی از توکن‌های خود را سهام‌گذاری کرده باشند. سپس، تعدادی از نودها طی رأی‌گیری انتخاب می‌شوند تا به‌عنوان اعتبارسنج تراکنش‌های معتبر را تأیید و بلاک بعدی را ایجاد کنند.

الگوریتم اجماع اثبات سهام در بلاک‌چین‌های مختلف به شکل‌های متفاوتی پیاده‌سازی شده است؛ اما در همه آن‌ها اصل بر این است که افراد با سهام‌گذاری توکن‌های خود در شبکه مشارکت می‌کنند. مهم‌ترین مزیت اثبات سهام این است که به دستگاه‌های حرفه‌ای و انرژی زیاد نیازی ندارد و با کامپیوترهای عادی نیز می‌توان یک نود را در این شبکه‌ها اجرا کرد. بااین‌حال، برخی نیز انتقاد می‌کنند که روش اثبات سهام سیستم را از غیرمتمرکزبودن دور می‌کند. اتریوم ۲، بی‌ان‌بی چین(BNB) ، تزوس[۹]و بسیاری دیگر از بلاک‌چین‌ها از این روش استفاده می‌کنند.

۳-۳. اثبات سهام نمایندگی‌شده

اثبات سهام نمایندگی‌شده[۱۰] یا DPoS یکی دیگر از انواع اثبات سهام است. در این مکانیسم نیز مشارکت‌کنندگان باید مقداری توکن در شبکه سهام‌گذاری کنند تا امکان مشارکت را داشته باشند. تفاوت اثبات سهام نمایندگی‌شده با اثبات سهام عادی این است که در روش نمایندگی‌شده، سهام‌گذاران حق رأی ناشی از توکن‌های خود را به افرادی می‌دهند که به آنان نماینده (Delegate) گفته می‌شود. سپس، این نمایندگان با رأی‌گیری اعتبارسنج‌ها را از میان سهام‌گذاران انتخاب می‌کنند. این اعتبارسنج‌ها تراکنش‌ها را تأیید و در ازای آن کارمزد تراکنش‌ها را به‌عنوان پاداش دریافت می‌کنند. قدرت رأی هریک از مشارکت‌کنندگان متناسب با مقدار توکن‌هایی است که سهام‌گذاری کرده‌اند. به‌دلیل همین سیستم رأی‌گیری است که برخی از این الگوریتم به‌عنوان روش اجماع دموکراتیک یاد می‌کنند. روش اثبات سهام نمایندگی‌شده درمقایسه‌با الگوریتم‌های اثبات کار و اثبات سهام عادی سرعت بیشتری در پردازش و تأیید تراکنش‌ها دارد؛ چراکه برای این کار به تعداد کمتری اعتبارسنج نیازمند است. ایاس[۱۱] یکی از بلاک‌چین‌های محبوبی است که از الگوریتم اجماع اثبات سهام نمایندگی‌شده استفاده می‌کند.

---

[7] Proof of Stake
[8] Staking
[9] Tezos
[10] Delegate Proof of Stake
[11] EOS

۳-٤. اثبات سهام اجاره‌شده

الگوریتم اجماع اثبات سهام اجاره‌شده[12] یا LPoS روشی مشابه اثبات سهام کلاسیک است. یکی از مشکلات روش اثبات سهام این است که کاربرانی با دارایی توکنی اندک نمی‌توانند در سیستم مشارکت کنند. در اثبات سهام، سهام‌گذاران بزرگ بیشترین کنترل را روی شبکه و بیشترین بخت را برای بردن پاداش دارند. اثبات سهام اجاره‌شده تلاش کرده است که این مشکل را حل کند.

در این روش، دارندگان توکن شبکه می‌توانند توکن‌های خود را به نودهای شبکه اجاره دهند تا آنان هم بتوانند در شبکه سهام‌گذاری کنند و از آن سود ببرند. هر نودی که توکن‌های بیشتری برای سهام‌گذاری داشته باشد، احتمال بیشتری دارد که برای تولید بلاک بعدی و درنتیجه دریافت پاداش انتخاب شود؛ ازاین‌رو، دارندگان کوچک یک استخر تشکیل می‌دهند و توکن‌های خود را به یک نود می‌دهند تا مجموع توکن‌ها به میزان درخورتوجهی برسد. نودها نیز برای جذب توکن‌های بیشتر ممکن است درصد پاداش بیشتری بدهند. این روش بیشتر در بلاک‌چین‌هایی کاربرد دارد که برای اجرای نود و پردازش تراکنش‌ها نیازمند سخت‌افزار قدرتمندتری هستند.

مکانیسم اجماع اثبات سهام اجاره‌شده از برخی جهات شبیه اثبات سهام نمایندگی‌شده است؛ اما تفاوت این دو مکانیسم اجماع آن‌جاست که در روش اثبات سهام نمایندگی‌شده، توکن‌ها به نمایندگان واگذار می‌شوند و آنان اعتبارسنج‌ها را انتخاب می‌کنند؛ درحالی‌که در روش اثبات سهام اجاره‌شده توکن‌ها مستقیم به اعتبارسنج‌ها اجاره داده می‌شوند. بلاک چین ویوز[13] از روش اثبات سهام اجاره‌شده استفاده می‌کند.

۳-۵. اثبات زمان سپری‌شده

الگوریتم اجماع اثبات زمان سپری‌شده[14] یا PoET اساساً در بلاک‌چین‌های خصوصی یا نیازمند مجوز به‌کار می‌رود؛ یعنی بلاک‌چین‌هایی که برای ورود به آن نیاز به مجوز و احراز هویت است. در این روش، هریک از مشارکت‌کنندگان باید مدت‌زمان مشخصی را منتظر بمانند. طول این مدت‌زمان به‌صورت تصادفی تعیین می‌شود. هر کاربری که مدت‌زمان انتظارش سپری می‌شود، مجوز ورود به دفترکل را دریافت و بلاکی جدید ایجاد می‌کند.

ابتدا هریک از مشارکت‌کنندگان یک کد اعتماد را دانلود و یک جفت کلید دریافت می‌کنند. سپس با استفاده از آن کلیدها، کد اعتماد را به شبکه ارسال می‌کنند و درخواست دسترسی می‌دهند. هریک از مشارکت‌کنندگان مدت‌زمان انتظار تصادفی را از همان منبع کد می‌گیرند. وقتی مدت‌زمان انتظار سپری شود، کاربر مدنظر مجوز ایجاد بلاک را دریافت می‌کند. هایپرلجر ساوتوث[15] بلاک چینی ماژولار است که از روش اثبات زمان سپری‌شده استفاده می‌کند.

---

[12] Leased Proof of Stake
[13] Waves
[14] Proof of Elapsed Time
[15] Hyperledger Sawtooth

۳-۶. گراف‌های جهت‌دار غیرمدور

گراف‌های جهت‌دار غیرمدور[16] یا DAG درواقع نوعی ساختار داده است؛ اما می‌توان آن را روشی برای اجماع نیز در نظر گرفت. در بلاک چین، بلاک‌های حاوی اطلاعات تراکنش‌ها به‌صورت پشت‌سرهم به شبکه اضافه می‌شوند و توالی‌ای از داده‌ها را ایجاد می‌کنند. به‌همین‌دلیل، اگر دو ماینر هم‌زمان بلاک ایجاد کنند، برای لحظاتی شبکه به دو شاخه تقسیم می‌شود و نودها باید یکی از شاخه‌ها (بلندترین شاخه) را برای ادامه بلاک چین انتخاب کنند.

درDAG ، همه تراکنش‌ها بدون درنظرگرفتن ترتیب آن‌ها وارد دفترکل توزیع‌شده می‌شوند. همچنین، برخلاف بلاک چین که برنده رقابت استخراج تراکنش‌ها را به بلاک چین اضافه می‌کند، در DAG همه کاربران می‌توانند این کار را انجام دهند؛ درنتیجه، تصویر کامل‌تری از تراکنش‌های شبکه به‌دست می‌آید. یکی از مزایای DAG درمقابل بلاک چین این است که حجم کمتری را اشغال می‌کند؛ ازاین‌رو، هزینه تراکنش کاهش و سرعت شبکه افزایش می‌یابد. آیوتا[17] و هِدِرا هشگراف[18]دو شبکه‌ای هستند که از گراف‌های جهت‌دار غیرمدور استفاده می‌کنند.

۳-۷. اثبات فعالیت

مکانیسم اجماع اثبات فعالیت[19] یا PoA دو روش اثبات کار و اثبات سهام را با یکدیگر ترکیب می‌کند. در بیشتر نمونه‌های اثبات فعالیت، ماینرها برای استخراج بلاک جدید با یکدیگر رقابت می‌کنند و در ازای آن پاداش می‌گیرند. بلاک‌های ایجادشده ماینرها حاوی تراکنش‌ها نیستند؛ بلکه قالب‌هایی خالی هستند که فقط عنوان تراکنش و آدرس پاداش بلاک در آن قرار گرفته است. با استفاده از اطلاعاتی که در عنوان تراکنش قرار دارد، یک نود اعتبارسنج به‌صورت تصادفی انتخاب می‌شود تا بلاک را امضا و آن را برای دفترکل بلاک چین تأیید کند.

شایان ذکر است که فقط دارندگان توکن می‌توانند اعتبارسنج شوند. کارمزد تأمین امنیت شبکه میان استخراج‌کنندگان و اعتبارسنج‌هایی توزیع می‌شود که در پردازش و امضای آن بلاک مشارکت کرده‌اند. مکانیسم اجماع فعالیت احتمال حمله ۵۱درصد را کاهش می‌دهد؛ چون ساختار آن امکان شناسایی اعتبارسنج بلاک بعدی را غیرممکن کرده است. همچنین، رقابت میان ماینرها و اعتبارسنج‌ها باعث ایجاد تعادلی در شبکه شده است که انگیزه چنین حمله‌ای را خنثی می‌کند.

باوجوداین، انتقادهایی هم از این سیستم شده که مشابه همان انتقادهای مربوط به سیستم‌های سنتی اثبات کار و اثبات سهام است. در این روش، انرژی بسیار زیادی برای استخراج بلاک‌ها در فاز اثبات کار مصرف می‌شود. همچنین، در فاز اثبات سهام کسانی که توکن‌های بیشتری دارند، بختشان برای انتخاب‌شدن به‌عنوان امضاکننده بلاک بیشتر است؛ به‌همین‌دلیل، پاداش بیشتری هم دریافت می‌کنند. بلاک‌چین‌های دیکرد (Decred) و اسپرز[20] از الگوریتم اجماع اثبات فعالیت استفاده می‌کنند.

---

[16] Directed Acyclic Graphs
[17] IOTA
[18] Hedera Hashgraph
[19] Proof of Activity
[20] Espers

۳-۸. اثبات اهمیت

اثبات اهمیت[۲۱] یا PoI شاخه‌ای از اثبات سهام است که تلاش می‌کند رویکرد جامع‌تری به تعیین ارزش مشارکت نودها در شبکه داشته باشد. مکانیسم‌های اثبات سهام رایج برای تعیین حقوق حاکمیتی نودها فقط میزان سرمایه آنان را در نظر می‌گیرند؛ اما مکانیسم‌های اثبات اهمیت عوامل دیگری را هم در ارزیابی خود از نودها دخالت می‌دهند.

معیارهای مدنظر در اثبات اهمیت در بلاک‌چین‌های مختلف متفاوت است. بسیاری از این بلاک‌چین‌ها ویژگی‌های خود را از الگوریتم‌های اجماع به‌کاررفته در خوشه‌سازی شبکه‌ای[۲۲] و رتبه‌بندی صفحات[۲۳] گرفته‌اند. رایج‌ترین این معیارها عبارت‌اند از: تعداد تراکنش‌هایی که هر نود در بازه زمانی مشخصی در آن‌ها مشارکت کرده است و میزان ارتباطی که نودها ازطریق خوشه‌های فعالیت با یکدیگر برقرار کرده‌اند.

در مکانیسم اثبات اهمیت، دارندگانِ بیشترین توکن‌ها قدرت مطلق در شبکه نیستند؛ ازاین‌رو، ریسک تمرکز قدرت و ثروت در این روش اندک است. همچنین، اگر فورک جدیدی ایجاد شود، مشارکت‌کنندگان باید منابع بیشتری را به‌کار گیرند تا فعالیتشان را به فورک‌های جدید هم گسترش دهند و بتوانند امتیازشان را حفظ کنند. این باعث می‌شود که مشارکت‌کنندگان انگیزه چندانی برای ایجاد فورک‌های بی‌مورد نداشته باشند. بلاک‌چین‌های نیو اکونومی موومِنت[۲۴] یا نِم[۲۵] از مکانیسم اجماع اثبات اهمیت استفاده می‌کند.

۳-۹. اثبات ظرفیت / فضا

الگوریتم اجماع اثبات ظرفیت[۲۶] یا اثبات فضا[۲۷] که به‌اختصار PoC یا PoSpace نامیده می‌شود، از فضای قابل‌استفاده در هارد ماینرها برای تعیین حق استخراج و تأیید تراکنش بهره می‌برد. در این روش، پیش از آنکه فعالیت استخراج شروع شود، فهرستی از راهکارهای استخراج رمزنگاری‌شده در هارد دستگاه ماینر ذخیره می‌شود. هرچه فضای موجود در هارد بیشتر باشد، راهکارهای بیشتری در آن ذخیره‌شدنی است. پس هرچه ظرفیت ذخیره‌سازی ماینر بیشتر باشد، احتمال بیشتری دارد که مقدار هش بلاک جدید در هارد آن ماینر پیدا شود و او برنده پاداش استخراج باشد.

هدف از طراحی روش اجماع اثبات ظرفیت رفع مشکل مصرف زیاد انرژی در مکانیسم‌های اثبات کار و نابرابری در توزیع پاداش‌ها در مکانیسم‌های اثبات سهام است. اثبات ظرفیت شباهت‌های زیادی با روش اجماع ذخیره[۲۸] در بلاک چین فایل کوین (Filecoin) دارد. مکانیسم اجماع اثبات ظرفیت در بلاک‌چین‌هایی مثل پرما کوین[۲۹] و برست کوین (Burstcoin)و اسپیس مینت (SpaceMint) به‌کار رفته است.

---

[21] Proof of Importance
[22] Network Clustering
[23] Page Ranking
[24] New Economy Movement
[25] NEM
[26] Proof of Capacity
[27] Proof of Space
[28] Proof of Storage
[29] Permacoin

۳-۱۰.اثبات سوختن

در روش اثبات سوختن[30] یاPoB ، ماینرها باید توکن‌های خود را برای همیشه از بین ببرند یا به‌اصطلاح بسوزانند تا در ازای آن حق استخراج بلاک‌های جدید و تأیید تراکنش‌ها را به‌دست بیاورند. هرچه ماینرها توکن‌های بیشتری بسوزانند، بخت بیشتری برای انتخاب‌شدن به‌عنوان اعتبارسنج بلاک بعدی خواهند داشت.

بدین‌ترتیب، ماینرها به‌جای استفاده از منابع محاسباتی و سخت‌افزارهای قدرتمند استخراج، با سوزاندن توکن‌هایشان وفاداری خود را به شبکه نشان می‌دهند. روش اثبات سوختن از این طریق انرژی بسیار کمتری درمقایسه‌با سیستم‌های اثبات کار مصرف می‌کند. پروتکل‌های کانترپارتی (Counterparty) و اسلیم کوین (Slimcoin) و فکتوم (Factom) از مکانیسم اجماع اثبات سوختن استفاده می‌کنند.

۳-۱۱.اثبات وزن

اثبات وزن[31] یکی از مدل‌های ارتقاء یافته اثبات سهام است که می‌کوشد مشکل توزیع ناعادلانه پاداش را در اثبات سهام حل کند. در روش اثبات سهام، دارندگانِ سهام بیشتر بخت بیشتری برای انتخاب‌شدن به‌عنوان اعتبارسنج و درنتیجه دریافت پاداش دارند.

الگوریتم اثبات وزن علاوه‌بر میزان سهام مشارکت‌کنندگان، عوامل دیگری را نیز در نظر می‌گیرد. برای مثال، فایل کوین حجم دادهIPFS مشارکت‌کنندگان را هم محاسبه می‌کند. این کار مشابه همان روشی است که در الگوریتم‌های اثبات فضازمان[32] و اثبات تکثیر[33] به‌کار می‌رود.

۳-۱۲.اثبات ذخیره و اثبات تکثیر و اثبات فضازمان

الگوریتم اجماع اثبات ذخیره[34]یا همان PoStorage به‌جای سهام‌گذاری، مبتنی‌بر داده طراحی شده است. این پروتکل به‌دلیل نوع عملکردش اساساً در شبکه‌هایی استفاده می‌شود که کار اصلی‌شان ذخیره‌سازی غیرمتمرکز داده است. در مکانیسم اثبات ذخیره، هر نود که ذخیره داده بیشتری به شبکه اختصاص داده باشد، برای استخراج بلاک جدید انتخاب می‌شود. از این نظر این پروتکل به اثبات سهام شباهت دارد؛ اما تفاوتش این است که در اثبات ذخیره به‌جای درنظرگرفتن توکن‌های سهام‌گذاری‌شده، مقدار ذخیره داده هر نود مبنا قرار می‌گیرد. در اثبات ذخیره، برای رسیدن به اجماع باید ثابت شود که هر مشارکت‌کننده همان مقدار ذخیره داده‌ای را که ادعا می‌کند، برای شبکه فراهم کرده است. پاداش مشارکت نیز بر همین اساس توزیع می‌شود.

---

[30] Proof of Burn
[31] Proof of Weight
[32] Proof Spacetime
[33] Proof of Replication
[34] Proof of Storage

فایل کوین[۳۵]، یکی از تأمین‌کنندگان ذخیره‌سازی داده مبتنی‌بر بلاک چین، از دو نوع مکانیسم اجماع اثبات ذخیره استفاده می‌کند: یکی اثبات تکثیر[۳۶] یا PoRep و دیگری اثبات فضازمان یا ProSpacetime در اثبات تکثیر، نودهای مشارکت‌کننده در شبکه می‌توانند ازطریق مکانیسم اجماع تأیید کنند که مقدار مشخصی داده در فضای ذخیره فیزیکی که منحصراً برای همان اختصاص داده شده، تکثیر شده است.

همچنین، شبکه فایل کوین با استفاده از مکانیسم اثبات فضازمان به‌صورت تصادفی ماینرهایی را انتخاب می‌کند که داده‌ها باید ازطریق آن‌ها خوانده و سپس تأیید و در یک گواه اثبات فضازمان فشرده‌سازی شود. سپس، ماینرها باید گواه متناظری فراهم کنند مبنی‌بر اینکه داده‌های مدنظر در دوره زمانی مشخصی به‌صورت مداوم در حافظه فیزیکی بوده است. از این طریق مشخص می‌شود که آیا نود مدنظر وظایفش را در هر بازه زمانی معین انجام داده است یا خیر.

پس اثبات تکثیر برای این استفاده می‌شود که ثابت کنیم یک ماینر نسخه منحصربه‌فردی از یک داده را در همان لحظه‌ای ذخیره کرده که مُهر شده است. از کاربرد دیگر اثبات فضازمان این است که نودها را به‌صورت تصادفی بررسی می‌کند تا مطمئن شود که فضای ذخیره داده مدنظر را به‌صورت مستمر تأمین کرده‌اند. علاوه‌بر فایل کوین، استورج (Storj) نیز از مکانیسم اجماع اثبات ذخیره استفاده می‌کند.

اثبات اعتبار

روش اثبات اعتبار[۳۷] یا PoA برای تأیید تراکنش‌ها و تولید بلاک‌های جدید از مدلی مبتنی‌بر شهرت[۳۸] استفاده می‌کند. در بلاک‌چین‌های اثبات اعتبار، معمولاً اعتبارسنج‌ها را دیگر مشارکت‌کنندگان شبکه به‌عنوان مدیران سیستم انتخاب می‌کنند. ازاین‌رو، اعتبارسنج‌ها معمولاً سرمایه‌گذاران نهادی یا شرکای راهبردی حاضر در اکوسیستم آن بلاک چین هستند که منافعشان در موفقیت بلندمدت شبکه است و با افشای هویت خود برای مسئولیت‌پذیری مشکلی ندارند.

در بلاک‌چین‌های اثبات سهام، نودهای اعتبارسنج برای تضمین رفتار مسئولانه باید سرمایه مالی خود را به‌میان بیاورند؛ اما در بلاک‌چین‌های اثبات اعتبار، آنان از سرمایه اجتماعی خود که همان شهرت است، برای تضمین عملکردشان هزینه می‌کنند. باوجوداین، بسیاری از این بلاک چین‌ها اعتبارسنج‌ها را ملزم می‌کنند که علاوه‌بر اعتبارشان، سرمایه مالی سنگینی را نیز در شبکه سرمایه‌گذاری کنند. با این کار کسانی که اشتیاق کافی برای اعتبارسنج‌شدن ندارند یا انگیزه‌های مشکوک دارند، از گردونه حذف می‌شوند؛ اما نودهای درست‌کاری که برای فعالیت بلندمدت آمادگی دارند، مشوق‌های مالی دریافت می‌کنند.

این روش انتخاب اعتبارسنج باعث شده است که خیلی‌ها بلاک‌چین‌های اثبات اعتبار را دارای ماهیت متمرکز یا نیمه‌متمرکز قلمداد کنند. بیشتر بلاک‌چین‌های اثبات اعتبار تعداد اعتبارسنج‌ها را محدود می‌کنند تا مقیاس‌پذیری شبکه

---

[35] Filecoin
[36] Proof of Replication
[37] Proof of Authority
[38] Reputation

افزایش یابد. درنتیجه، این نوع بلاک چین‌ها عموماً امکان سازگاری با سیستم‌های غیرمتمرکز و بدون نیاز به مجوز را ندارند؛ اما انتخاب مناسبی برای بلاک‌چین‌های خصوصی و نیازمند مجوز هستند. وی چین[۳۹] و تومو چین[۴۰] جزو پروژه‌هایی هستند که از مکانیسم اثبات اعتبار استفاده می‌کنند.

۳-۱۳.اثبات مشارکت

الگوریتم اجماع اثبات مشارکت[۴۱] یا PoCo با الگوریتم‌هایی تخصصی مشارکت همه نودهای فعال در شبکه را در دوره اجماع بررسی می‌کند. سپس، حق ایجاد بلاک بعدی را به نود یا نودهایی می‌دهد که بیشترین مشارکت را کرده‌اند. در این روش، به هر اقدام اجرایی آستانه اعتماد مشخصی تخصیص داده می‌شود. این آستانه سطح حداقلی اعتمادی را تعیین می‌کند که برای محاسبات مربوط به همان اقدام لازم است. کاربرانی که می‌خواهند محاسبه‌ای درون‌زنجیره‌ای را انجام دهند، باید پیش‌از آن سپرده امنیتی ایجاد کنند. سطح مشارکت هر کاربر تابعی از سابقه و میزان سپرده او و نتیجه محاسباتش برای هر اقدام است.

در هر دوره اجماع، نتایج محاسبات مرتبط را گروهی از کاربرانِ دارای صلاحیت پیشنهاد می‌کنند. سپس، یکی از این کاربران که سطح اعتمادش با آستانه لازم برای آن محاسبه مطابقت دارد، می‌تواند نتیجه را پیشنهاد دهد. در مرحله بعد، کارمزد تراکنش‌ها به نودهایی پرداخت می‌شود که نتیجه معتبر را محاسبه کرده‌اند. سپرده کاربرانی که نتیجه محاسباتشان نادرست بوده است، نیز به آن نودها پرداخت می‌شود. درنهایت، اعتبار همه کاربرانی که در این فرایند مشارکت کرده‌اند، براساس عملکردشان بررسی و دوباره تنظیم می‌شود.

تقریباً در همه موارد، چندین کاربر موفق می‌شوند نتیجه را دقیق محاسبه کنند؛ به‌همین‌دلیل، امتیاز اعتماد کلی براساس مجموع سطح اعتماد این کاربران محاسبه و پاداش اجماع در میان آنان تقسیم می‌شود. استفاده از الگوریتم اجماع اثبات مشارکت چندان گسترده نیست. در میان پروژه‌های معدودی که این الگوریتم را پیاده‌سازی کرده‌اند، می‌توان به آی‌اکسک[۴۲] اشاره کرد. آیکون نتورک[۴۳] نسخه‌ای اصلاح‌شده از اثبات مشارکت را دارد که اثبات مشارکت نمایندگی‌شده[۴۴] یا DPoC نامیده می‌شود. در این روش، کاربران امتیاز اعتبارسنجی خود را به نودهای منتخب واگذار می‌کنند تا آنان کار اعتبارسنجی را انجام دهند.

۳-۱۴.اثبات تاریخ

پروتکل اثبات تاریخ[۴۵] یا PoH حافظه تاریخی داخلی دارد که ازطریق آن لحظه وقوع هر رویدادی روی بلاک چین اثبات‌پذیر است .سولانا [۴۶]یکی از بلاک‌چین‌هایی است که از اثبات تاریخ استفاده می‌کند. در بلاک‌چین‌های دیگر،

---

[39] VeChain
[40] TomoChain
[41] Proof of Contribution
[42] iExec
[43] ICON Network
[44] Delegated Proof of Contribution
[45] Proof of History

اعتبارسنج‌ها باید درباره زمان وقوع تراکنش به اجماع برسند؛ اما در سولانا هر اعتبارسنج گذر زمان را ازطریق تابع هش ساده SHA-256 رمزگذاری می‌کند و ساعت مخصوص خود را دارد.

هربار که اعتبارسنج‌های سولانا با یکدیگر ارتباط برقرار می‌کنند، یک گواه رمزنگاری‌شده از ترتیب و زمان هر پیام در دفترکل شبکه ذخیره می‌شود. بدین‌ترتیب، شبکه دیگر به ساعت نیازی ندارد و همه تأخیرهای احتمالی در شبکه را با زمان خودش برطرف می‌کند. این کار باعث می‌شود که انتقال و جمع‌آوری داده‌های تراکنش‌ها با کارایی بیشتری انجام شود و دیگر به رعایت ترتیب بلاک‌ها برای تأیید آن‌ها احتیاجی نباشد. استفاده از الگوریتم اجماع اثبات تاریخ به سولانا امکان داده است که تأیید تراکنش‌ها را با سرعت بسیار زیادی انجام دهد، بدون اینکه چیزی از امنیت و غیرمتمرکزبودن شبکه کاسته شود، البته این اقدام باعث کاهش امنیت سیستم می‌شود و برای افزایش راندمان بهتر است براساس نوع اجماع والگویه درست پیاده سازی انجام دهیم که این اقدام به صرفه‌تر است زیرا بعضی از ارزهای دیجیتال نیاز به نوع پیاده سازی متمرکز، غیر متمرکز بودن یا نیمه متمرکز بودن برای توضیع منابع خود دارند، در جدول شماره ۱ می‌توان الگوریتم اجماع و نوع حمله آسیب پذیر بودن را مشاهده کرد، برای حساب کردن درصد آسیب پذیری الگوریتم های اجماع از فرمول (۱) استفاده می‌کنیم که در آن X_T تعداد حملات موفق هست و O_K درصد موفقیت حملات در الگوریتم اجماع می باشد.

$$O_k = \frac{(\max X_T)}{\sum_1^K x} \qquad (۱)$$

در حساب مجموع برآیند تاثیرات غیر مستقیم یک حمله به دیگر الگوریتم های اجماع که تعهد تاثیر بر الگوریتم اعتماد وشهرت می‌باشد برای تاثیر مستقیم dir و تاثیر غیرمستقیم برچسب ind و برای تاثیرجز به جز از ایندکس ij استفاده می‌کنیم که نسبت آسیب پذیری الگوریتم به نوع حمله بدست آید.

$$T_{ij} = \alpha R_{ij} + \beta I_{ij} + \gamma O_{ij}^{dir} + \delta O_{ij}^{ind} \qquad (۲)$$

$$\alpha + \beta + \gamma + \delta = 1$$

جدول ۱: آسیب پذیری الگوریتم‌های اجماع در برابر حملات

حمله / اجماع	اثبات سهام	اثبات وزن	اثبات سوختن	اثبات ظرفیت	اثبات اهمیت	اثبات فعالیت	اثبات زمان	اثبات کار
خاموش- روشن	-	-	*	-	*	-	*	–
حمله تبانی	*	*	*	–	*	*	*	*
حمله فرصت طلبانه	*	-	*	*	*	*	*	–
حمله سیبیل	*	-	*	*	-	*	*	*
حمله تله شهرت	*	*	*	-	*	*	-	–

[46] Solana

حمله نوسان	-	-	*	*	-	*	-	–
حمله تکثیر	-	*	-	-	-	-	*	–
حمله انکار سرویس	*	-	-	*	-	*	-	–
درصد آسیب پذیری	۸/۵	۸/۵	۸/۶	۸/۴	۸/۴	۸/۶	۸/۵	۸/۲

با توجه به فرمول (۱) ما بررسی کلی از رفتار مهاجمان می توانیم بدست آوریم که مهم‌ترین هدف تلاش برای جعل در سرویس مربوطه می‌باشد،

با توجه به مقالات [۳۴] بهترین الگوریتم اجماع pow یا اثبات کار می‌باشد که دررمزارز مهمی مانند ارز بیت کوین استفاده می‌شود اگر چه برای افزایش امنیت بیشتر الگوریتم های ترکیبی حائز اهمیت تر هستن و این باعث افزایش حجم و زمان انجام تراکنش می‌شود بنابراین بهتر است برای درک بهتر مزایا ومعایب در جدول ۲ آورده شده است وارسی و نقطه عطف ویژگی هر سیستم اجماع را بدانیم.

جدول ۲: معیارهای مقایسه الگوریتم اجماع

معایب	مزایا
مصرف انرژی زیاد سیستم بلاکچین	انحصارزدایی
ناشناس بودن افراد در این شبکه به منظور استفاده از پولشویی	اختیار داشتن در تغییر محتوای ارز دیجیتال
مقیاس پذیری و محدودیت در پشتیبانی تراکنش‌ها	قدرت پردازش بالا در سیستم بلاکچین
پر هزینه بودن تغییر اطلاعات در شبکه بلاکچین	قدرت ذخیره‌سازی سیستم بلاکچین
عدم امکان بازگرداندن یک تراکنش	کارایی اطلاعاتی
عدم امکان بازیابی کلید خصوصی در شبکه بلاکچین	دسترسی آسان و یکسان به اطلاعات
	عدم امکان نقض حریم خصوصی در سیستم بلاکچین
	امکان فروش ثانویه و تشکیل بازارثانویه
	ایجاد تنوع و به تبع کاهش ریسک سرمایه‌گذاری در بازارهای مالی
	افزایش رقابت و به تبع کاهش هزینه‌های تراکنش
	توزیع سرورها و به تبع امنیت باالی شبکه در تراکنش‌ها
	در دسترس بودن همیشگی شبکه
	شفافیت اطلاعاتی
	بی معنی کردن تحریم‌های مالی
	مقبولیت عام پول دیجیتالی
	صرفه‌جویی در مصرف کاغذ

٤. الگوریتم‌های رمزنگاری

٤-١. الگوریتمSHA-256

اولین الگوریتم استخراج ارزهای دیجیتال به زمان پیدایش بیت‌کوین بر می‌گردد. زمانی که بیت‌کوین به عنوان رمز ارز برتر و رهبر ارزهای دیجیتال به دنیا معرفی شد مردم با اولین الگوریتم استخراج هم آشنا شدند. این الگوریتم استخراج که SHA-256نام دارد یک تابع هش قدرتمند است که برای استخراج رمز ارزهایی همچون بیت‌کوین، بیت‌کوین کش، آکوین و برخی ارزهای دیجیتال دیگر مورد استفاده قرار می‌گیرد.

الگوریتم‌های هش ایمن در گروه توابع هشینگ کریپتوگرافیگ (رمزنگاری) قرار می‌گیرند و در این میان، SHA-256 یکی از الگوریتم‌های پرطرفدار است که توسط آژانس امنیت ملی توسعه یافته و توسط موسسه ملی فناوری در سال ۲۰۰۱ منتشر شد و در سال ۲۰۰۲ به استاندارد فدرال برای پردازش اطلاعات تبدیل شد، الگوریتم SHA-256 رایج‌ترین تابع هش در جهان است که از امنیت بالایی برخوردار است و قابلیت بازیابی CPU را فراهم می‌کند، این قابلیت با GPU و ASIC سریعتر همراه است.

٤-٢. الگوریتم sCrypt

الگوریتم اسکریپت[47] یک الگوریتم هش است که در بلاک‌چین‌های با ساز و کار اثبات کار خاصی استفاده می‌شود و با تولید اعداد تصادفی و غیرتکراری فرایند استخراج بلاک را برای کاربران مخرب دشوار می‌کند و باعث افزایش چندین برابری امنیت شبکه‌های ارز دیجیتال می‌شود.

به عبارت ساده‌تر اسکریپت رشته‌های الفبایی منحصر به‌فرد و غیرتکراری را ایجاد می‌کند که هدف از استفاده از این رشته‌های الفبایی این است که داده‌های کلیدی الگوریتم را استتار کرد تا فرایند شکستن هش‌ها برای افراد مخرب پیچیده‌تر و سخت‌تر شود.

از طرفی دیگر الگوریتم اسکریپت به این منظور طراحی شده تا شکستن رمز عبورهایی که با این الگوریتم هش‌شده را برای سخت افزارهای مخصوص مانندASIC ها دشوارتر کند Scrypt .در مقایسه با توابع مشابه، این کار را با استفاده از حجم زیادتری از حافظه انجام می‌دهد که همین امر هم باعث شده تا هکرها به‌راحتی نتوانند به اهداف خودشان دست پیدا کنند.

این الگوریتم اولین بار در سال ۲۰۱۱ با راه‌اندازی پروژه Tenebrix (TBX) توسط یک برنامه‌نویس ناشناس ملقب به Artfortzتوسعه یافت Tenebrix .اولین پروژه بلاک‌چینی بود که از الگوریتم استخراج Scrypt به عنوان یک الگوریتم هش استفاده می‌کرد.

[47] sCrypt

٤-٣. الگوریتم Ethash

الگوریتم استخراج Ethash اولین بار توسط بنیانگذار و خالق اتریوم یعنی ویتالیک بوترین[۴۸] در سال ۲۰۱۳ تا ۲۰۱۴ ساخته شد؛ بنابراین از این الگوریتم برای ارزهای دیجیتالی همچون اتریوم و ارزهای هم رده اتریوم استفاده می‌شود.

این الگوریتم با این هدف طراحی شده که با استفاده از تکنیک‌های محاسباتی بسیار پیشرفته باعث افزایش سطح امنیت شبکه می‌شود. الگوریتم استخراج Ethash شکل ارتقا یافته الگوریتم قبلی اتریوم یعنی Dagger-Hashimoto است و جایگزین آن شده است.

هدف اصلی و اولیه از ساخت این الگوریتم استخراج، تمرکز بر محافظت از ماینرهای ASIC بود؛ اما با گذشت زمان و با افزایش محبوبیت اتریوم که ارز دیجیتال اصلی Ethash است، علاقه توسعه‌دهندگان ماینرهای ASIC را به تولید ماینرهای سازگار با این الگوریتم افزایش داد؛ سرانجام در سال ۲۰۱۸ بیت‌مین[۴۹]، شرکت مطرح سازنده ماینرهای ارز دیجیتال، اولین ماینرهای ASIC را برای Ethash به بازار معرفی کرد.

اما بعد از این اتفاق، تیم توسعه‌دهنده پروژه اتریوم به شدت با تسلط ASIC بر شبکه مخالفت کرد. این نظرات ماینرهای ASICرا مجبور به مخفی کردن و کاهش قدرت هش دستگاه‌های خود کرد.

ویتالیک بوترین هدف اصلی خود از ایجاد این الگوریتم را اینطور عنوان کرده که همه بتوانند با کامپیوترهای معمولی اتریوم استخراج کنند و تنها به دستگاه‌های ASIC نیاز نداشته باشند. این در حالی است که همچنان از دستگاه‌های ASICبرای استخراج اتریوم و سایر ارزها بر اساس این الگوریتم استفاده می‌شود.

ارزهایی که قابلیت استخراج با این الگوریتم را دارند عبارتند از:

Ethereum (ETH)
Ethereum Classic (ETC)
Expanse (EXP)

٤-٤. الگوریتمX11

یکی از ایمن‌ترین و قدرتمندترین الگوریتم‌های استخراج ارزهای دیجیتال الگوریتم استخراج X11 است که از رشته‌ای از توابع هش مختلف برای ایجاد بیشترین امنیت در استخراج ارزهای دیجیتال استفاده می‌کند. این الگوریتم استخراج برخلاف SHA-256 (الگوریتم استخراج بیت‌کوین) یا الگوریتم Scrypt فقط یک تابع هش تنها نیست، بلکه از ۱۱ تابع هش متفاوت ساخته شده است.

٤-٥. الگوریتم CryptoNight

از دیگر الگوریتم‌هایی که بر پایه ساز و کار اثبات کار طراحی شده الگوریتم استخراج کریپتونایت[۵۰] است. این الگوریتم استخراج یک فناوری متن با[۵۱]ز و پروتکل لایه‌ای کاربردی است.

---

[48] Vitalik Buterin
[49] Bitmain
[50] CryptoNight

الگوریتم استخراج کریپتونایت هم به گونه ای طراحی شده که در مقابل ASIC مقاوم است. ویژگی اصلی این الگوریتم هش بسیار سریع آن است و امکان مقیاس‌پذیری خوبی را فراهم می‌کند.

هدف اصلی از ایجاد این الگوریتم استخراج، پر کردن شکاف بین ماینرهایی است که فقط به پردازنده CPU دسترسی دارند و توانایی تهیه سخت افزارهایی نظیر کارت‌های گرافیک وASIC ها را ندارند. این اقدام برای ایجاد عدالت در ماینینگ برای کاربران بهتر بوده و غیر متمرکز سازی بیشتری به دنبال خواهد داشت.

جدول ۳: الگوریتم‌های رمزنگاری استفاده شده در بلاکچین

الگوریتم CryptoNigh	الگوریتم Ethash	الگوریتم SHA-256	الگوریتم Scrypt	الگوریتم X11
onero (XMR)	Ethereum (ETH)	BitcoinCash (BCH)	Litecoin (LTC)	Dash (DASH)
Bytecoin (BCN)	Ethereum Classic (ETC)	Bitcoin (BTC)	Dogecoin (DOGE)	CannabisCoin (CANN)
Boolberry (BBR)	Expanse (EXP)	21Coin (21)	Novacoin (NVC)	StartCoin (START)
Dashcoin (DSH)		Peercoin (PPC)	WorldCoin (WDC)	MonetaryUnit (MUE)
DigitalNote (XDN)		Namecoin (NMC)	Latium (LAT)	Karmacoin (Karma)
DarkNetCoin (DNC)		Unobtanium (UNO)	FeatherCoin (FRC)	XCurrency (XC)
FantomCoin (FCN)		Betacoin (BET)	Bitmark (BTM)	
Pebblecoin (XPB)		Bytecoin (BTE)	TagCoin (TAG)	
Quazarcoin (QCN)		Joulecoin (XJO)	Ekrona (KRN)	
		Devcoin (DVC)	MidasCoin (MID)	
		Ixcoin (IXC)	DigitalCoin (DGC)	
		Terracoin (TRC)	Elacoin (ELC)	
		Battlecoin (BCX)	Anoncoin (ANC)	
		Takeicoin (TAK)	PandaCoins (PND)	
		PetroDollar (P$)	GoldCoin (GLD)	

[51] open-source

۵. استخراج شاخص‌ها و ارائه روش‌های عددی با هدف مقایسه الگوریتم‌های اعتماد با تکیه بر ارزیابی استحکام

از جایی که بررسی عملکرد روش های کنترل اعتماد و شهرت در ارتباطات ضروری است، در این قسمت با معرفی شاخص های عددی، شیوه‌هایی با مقایسه نتیجه های کمی حاصل از شبیه سازی در مقالات. برای رسیدن به این هدف دو الگوریتم [۲۳] (Nitti et.al) و [۱۹] (Ing-Rayet.al) جدول ۴ ارائه شده است. از آنجایی که از ابتدا تا رسیدن به اعتماد ذاتی، زمان گذرا و پس از آن زمان پایدار الگوریتم در نظر گرفته می‌شود، در فرآیند مقایسه زمان شبیه‌سازی به دو حالت گذرا و ناگذر تقسیم می‌شوند و مقایسه حسابی این دو روش در زمان پایداری در جدول ۵ نشان داده شده است. هدف از این مقایسه بررسی پایداری الگوریتم بعد از رسیدن به اعتماد کلی می‌باشد هنگامی که درصد گره‌های مخرب ۳۰ باشد، الگوریتم وزن دار خطای کمتری دارد. در حالی که گره های مخرب با افزایش درصد حملات به ثبات نمی‌رسند، پس اعدادی برای مقایسه وجود نخواهد داشت که این موضوع به خوبی در شکل ۵ نشان داده شده است. با بررسی جدول های ۱ و ۲ مقایسه و ویژگی‌های عمده شهودی ارائه شد و الگوریتم‌ها در جدول ۴ نکاتی به دست می آید که به وسیله آن می‌توان ضعف‌ها و برتری‌های الگوریتم‌ها را نسبت به یکدیگر مقایسه کرد و برای ارائه مدل بهتر مد نظر داشت.

جدول ٤: معیار ارزیابی مدل ها در برابر حوادث گسسته رخداد

روش‌های ارزیابی الگوریتم بلاکچین	محدودیت‌های عناصر				تنبیه	مقاومت در برابر حملات							منابع
	قدرت محاسبات	انرژی	حافظه	آگاهی از موضوع		سایرین	حمله Sybil	حمله رفتار متناقض	حمله روشن- خاموش	حمله خدمت فرصت طلبانه	حمله خوب گویی	حمله بدگویی	حمله خودبزرگ نمایی	
نرخ موفقیت	✓	×	×	×	✓	ارائه خدمت بد، بازخورد منفی	×	×	×	×	×	×	×	[21]
سرعت و دقت رسیدن به سطح اعتماد ذاتی	×	×	×	×	×	---	×	×	×	×	✓	✓	×	[17]
سرعت و دقت رسیدن به اعتماد ذاتی بین گروهی و داخل گروهی	×	×	✓	×	×	---	×	×	×	×	✓	✓	×	[22]
کیفیت پیشنهادها، سطح اعتماد در حضور حملات	✓	✓	×	✓	✓	---	×	×	✓	✓	×	✓	×	[18]
تهدیدات امنیتی برنامه های موبایل	×	×	×	×	---	×	×	×	×	×	×	×	×	[49]

نرخ موفقیت	✓ ✓	×	×	×		✓ ×	ارائه خدمت بد، بازخورد منفی	×	×	×	×	×	×	ذهنی عینی [23]
توان عملیاتی شبکه و از دست‌دادن بسته، پیشنهادهای تقلبی کشف شده، منفی اشتباه و مثبت اشتباه در حضور حملات بدگویی و خوب‌گویی	×	×	×	×		×	راس خودخواه، تبانی	×	×	×	×	✓	✓	×	[37]
همگرایی، دقت و انعطاف‌پذیری الگوریتم در رسیدن به ذاتی، اعتماد مقایسه با روش‌های Eighen Trust وPeer Trust	×	×	✓	×		×	---	×	×	×	×	✓	✓	✓	[19]
همگرایی و دقت الگوریتم در رسیدن به اعتماد ذاتی	×	×	×	×		×	---	×	×	×	×	✓	✓	×	[24]

همگرایی و دقت الگوریتم در رسیدن به اعتماد ذاتی، مقایسه با روشهای [17] و[22]	✓	×	✓	✓	✓	بازخورد غلط، تبانی	×	×	×	×	×	×	[25]
سرعت و دقت همگرایی الگوریتم در رسیدن به اعتماد ذاتی برای رئوس خوب و بد، زمان انتظار و درصد سرویس های استفاده شده نامطلوب نسبت به زمان	×	×	×	✓	---	حمله عدم همکاری و حمله گزارش جعلی	×	×	×	×	✓	✓	[20]
سرعت و دقت همگرایی الگوریتم در رسیدن به اعتماد ذاتی، نرخ موفقیت	×	✓	×	✓	---	---	×	×	✓	✓	✓	✓	[58]

در مقاله ۳۳ دو الگوریتم جهت ارزیابی ارائه شده است که بر اساس آن الگوریتم های مورد استفاده در ارزهای دیجیتال احراز هویت می‌شوند که در الگوریتم شماره یک بر اساس شرایط و کلید مورد نیاز و در الگوریتم دوم بر اساس توابع و فرآیند اجرایی جهت احراز هویت می باشد.

که در حسن انجام شبیه به الگوریتم metrust, Eighen Trust در مقاله ۳۴ می باشد که شرایط استراتژی والگوریتم اجماع بسته به آن الگوریتم توزیع دهنده آن ارز دیجتال هم تغییر می کند.

Algorithm 1 Access Request Validation
Input: $P_{r,c}, TX_R, T_{SC_i}^{SP_j}, R_{SC_i}$, and A_i
Output: Token or ∅
1: authorized ← 0
2: if $A_p \subset A_i$ and $\tau \subset \tau_p$ then
3: if $T_{SP_j} \geq T_{SC}^{\min}$ and $R_{SC_i} \geq R_{SC}^{\min}$ then
4: if getBalance $(PK_{SC_i}) \geq \varphi r$ then
5: authorized ← True
6: end if
7: end if
8: end if
9: if authorized then
10: return Token
11: else
12: return ∅
13: end

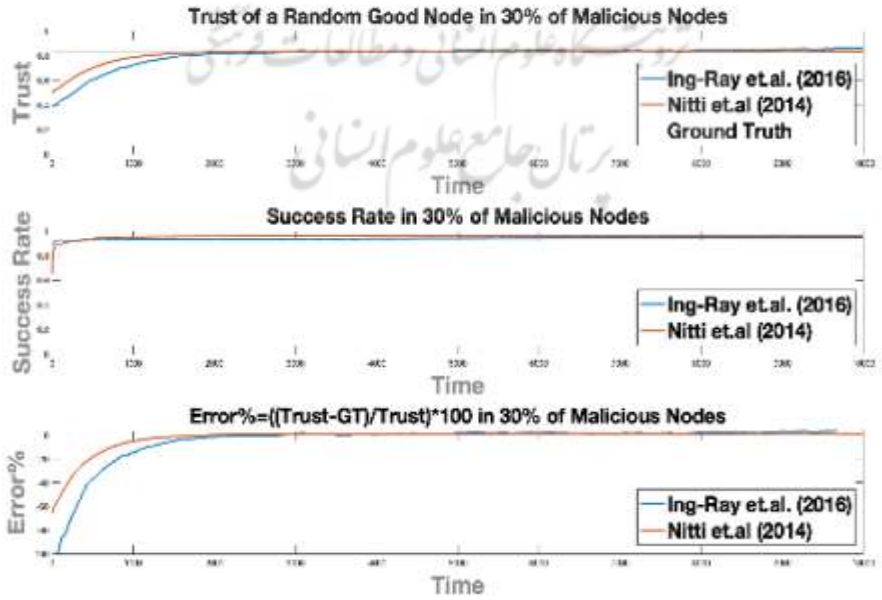
Algorithm 2 Feedback Mechanism
Input: $P_{(r,c)}, TX_F$
Output: True or False
1: last_update ← getUpdateTimestamp (Data)
2: access_timestamp ← getAccessTimestamp (Data)
3: evidence ← checkSig (Data)
4: result ← False
5: if H(┤ Token ├ _R) exist then
6: return result
7: end if
8: if (access_timestamp - last_update)<U_r then
9: if F_(SP_j,r)= positive and evidence = True then
10: () $\varepsilon_t \leftarrow \varepsilon_{\text{"pos "}}$
11: result ← True
12: end if
13: else
14: if$F_{SP_j,r}$ = negative and evidence = True
15: $\varepsilon_t \leftarrow$ neg
16: eut ← True
17: end if
18: end if
19: if result = True then
20: reCalculate $T_{SP_j}^{SC_i}, A_{SP_j}, R_{SP_j}$
21: sendCryptoTo (SC_i)
22: else
23: $\delta_t \leftarrow \delta_{\text{neg}}$
24: reaculate $T_{SP_j}^{SC_i}, A_{SC_i}, R_{SC_i}$
25: sendCryptoTo (SP_j)

الگوریتم های زیادی جهت محاسبه ترکیب وزن داراعتماد وجود دارند که نظر کلیه رئوسی که با معتمد تراکنش داشته‌اند بررسی می کنند. در حالی که در مدل میانگین، نظر تعدادی از دوستان که بیشترین شباهت به معتمد را دارند، به صورت وزن‌دار با یکدیگر ترکیب می‌شوند. با توجه به نتایج شبیه‌سازی، جمع‌آوری نظرات کلیه پیشنهاددهندگان تا زمانی که رئوس مخرب ۳۰ درصد یا کمتر باشد بهتر حساب می‌کنند؛ در حالی که با بالا رفتن درصد رئوس مخرب، اهمیت پایش نظراتی که با یکدیگر ترکیب می‌شوند بیشتر می شود؛ لذا الگوریتم میانگین ریاضی با وجود نیمی از رئوس مخرب بعد از ۴۹۳۱ ثابت زمانی به اعتماد ذاتی می‌رسد.

جدول 5 bn: پارامترهای شبیه سازی

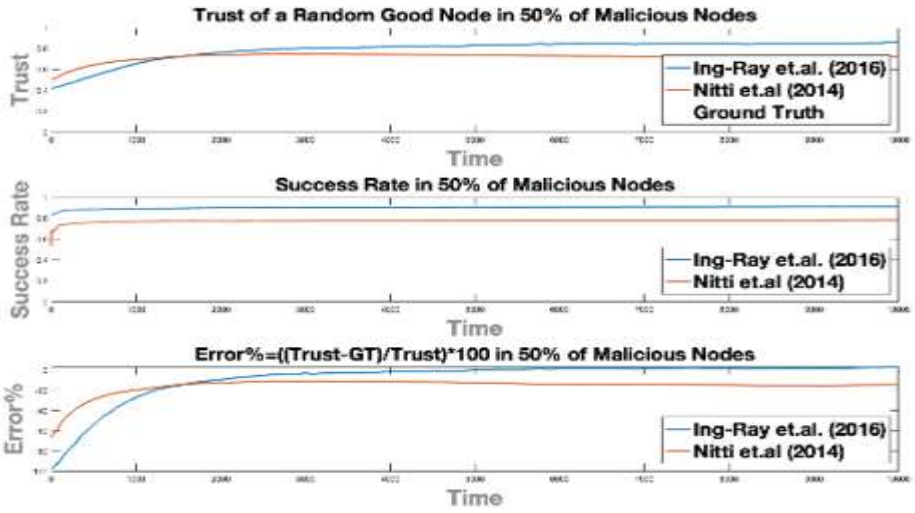
پارامتر	مقدار
تعداد کاربران	۴۰
الگوریتم دوستی کاربران	باراباسی-آلبرت
تعداد اشیا	۲۰۰
تقسیم‌بندی مکانی	۱۶*۱۶
الگوریتم حرکت	SWIM
نوع حمله	خوب‌گویی و بدگویی
درصد رئوس مخرب	٪۳۰ و ٪۵۰
زمان نهایی	۱۰،۰۰۰
تکرار مونت کارلو	۵۰

شکل ۲ نتایج مقایسه عملکرد سرعت و دقت رسیدن به اعتماد و شهرت کلی یک همسایگی خوب تصادفی، نرخ موفقیت و درصد خطا درحضور ٪۳۰ رئوس مخرب در شکل ۲ نشان داده شده است. الگوریتم [۳۳] در حضور ٪۳۰ رئوس مخرب، عملکرد بهتری دارد؛ به طوری که سرعت و دقت رسیدن به اعتماد ذاتی بهتر، نرخ موفقیت بیشتر و خطای الگوریتم هم کمتر است و این موضوع به خوبی در شکل ۲ قابل مشاهده است.



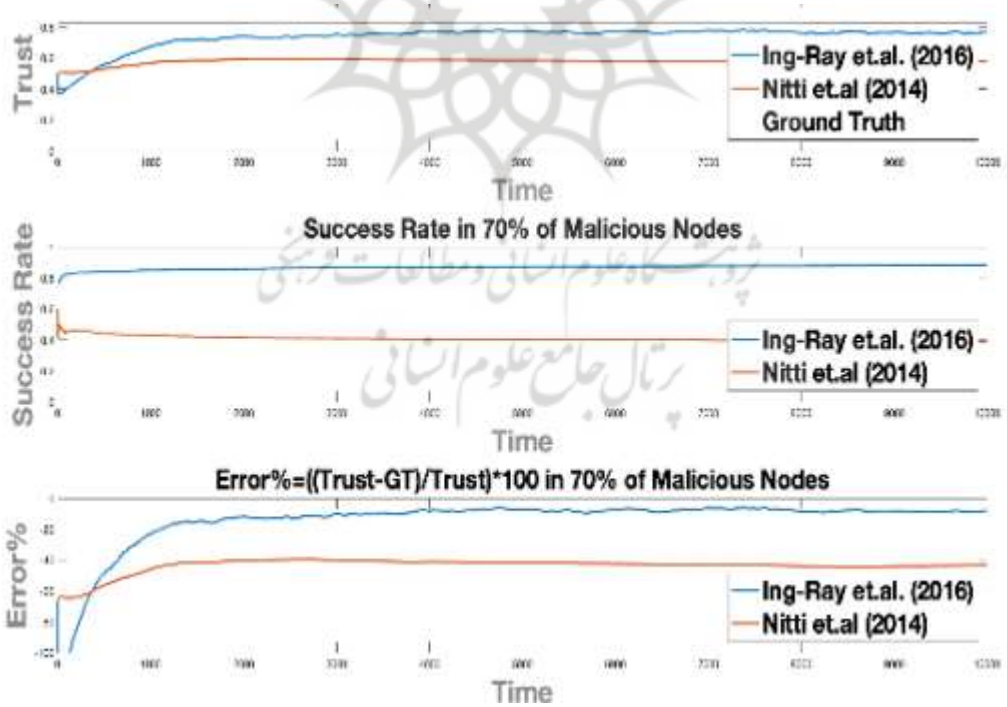
شکل 2: مقایسه دو مدل در حضور ۳۰ رأس مخرب

شکل ۳ نیز همین شبیه‌سازی‌ها را با حضور ۵۰٪ رئوس مخرب نشان می‌دهد اما تفاوتش در این است که نتایج شبیه‌سازی نشان می‌دهد الگوریتم [۱۹]، در حضور ۵۰٪ از رئوس مخرب عملکرد بهتری دارد.



شکل 3: مقایسه دو مدل در حضور ۵۰ رأس مخرب

در شکل ۴ درصد رئوس مخرب ۷۰٪ است. نتایج اکی از آن است که هر دو مدل تاب‌آوری خود را در برابر حملات نودهای مخرب از دست داده و به اعتماد ذاتی نمی‌رسند، درحالی که باز الگوریتم [۱۹] بهتر عمل می‌کند.



شکل 4: مقایسه دو مدل در حضور ۷۰ رأس مخرب

جدول ۴ از زمان آغاز تا پایان شبیه سازی را در می‌توان مشاهده کرد. با توجه به مرجع [۳۴] اعتماد همگانی رأس خوب استوکاستیک ۸۳/۰ جهت مقایسه دو مدل بررسی زمان رسیدن به ۸۳/۰ در نظر گرفته شده است؛ جدول ۴ نشان

می‌دهد که الگوریتم [۳۳] با درصد مجاورت ویرانگر پایین‌تر زودتر به ۸۳/۰ همگرا می‌شود؛ در حالی که با بالارفتن درصد رئوس ویرانگر تا پایان زمان شبیه‌سازی همگرا نمی‌شود؛ هم چنین نتایج شکل ۴ به خوبی نشان دهنده ی کاهش عملکرد هر دو الگوریتم با افزایش حملات است، با وجود این که با افزایش حملات الگوریتم [۱۳] از [۱۱] عملکرد بهتری دارد و مقایسه مقادیر نهایی در هر دو مدل با هدف سهولت در مقایسه گواه این نتیجه‌گیری است، عملکرد بهتر در جداول به صورت خانه‌های حاشیه‌دار نمایش داده شده‌اند.

جدول ٦: مقایسه نتایج کمی حاصل از شبیه سازی در مقالات m.nitti, ing-ray et.al

زمان رسیدن به اعتماد ذاتی			
درصد رئوس مخرب	٪۳۰	٪۵۰	٪۷۰
Ing-Ray et.al.	۲۸۳۱	۴۹۳۱	—
M. Nitti	۱۹۳۵	—	—
خطای میانگین مربعات اعتماد			
Ing-Ray et.al.	۰/۰۸۶۷	۰/۱۰۳۶	۰/۱۱۷۸
M. Nitti	۰/۰۵۴۹	۰/۱۱۳۹	۰/۲۵۲۴
مقدار نهایی اعتماد، (t=10000)			

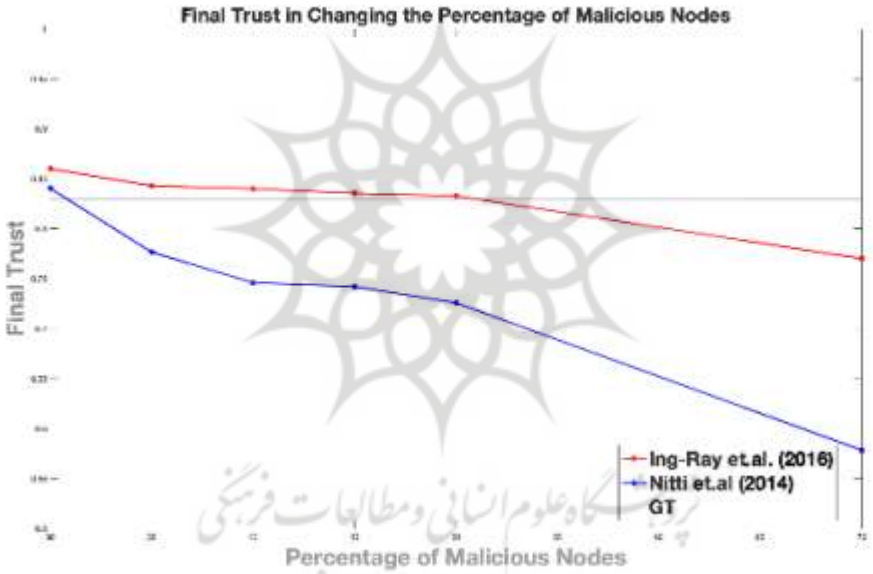
در فرآیند مقایسه زمان شبیه‌سازی به دو حالت گذرا و ناگذر تقسیم می‌شوند به این ترتیب که از ابتدا تا رسیدن به اعتماد ذاتی، زمان گذرا و پس از آن زمان پایدار الگوریتم در نظر گرفته می‌شود و مقایسه حسابی این دو روش در زمان پایداری در جدول ۶ نشان داده شده است. هدف از این مقایسه بررسی پایداری الگوریتم بعد از رسیدن به اعتماد کلی می‌باشد.

جدول نشانگر زمانی که درصد گره‌هلی مخرب ۳۰ باشد الگوریتم وزندار خطای کمتری دارد، در حالی که با افزایش درصد حملات به ثبات نمی‌رسند و بنابراین اعدادی برای مقایسه وجود نخواهد داشت. با در نظر گرفتن جداول ۴ و ۵ و ۶ ویژگی‌های دو مدل و نتایج عددی حاصل از شبیه‌سازی‌های ارائه شده در جدول ۶ نکاتی بدست می‌آید که به کمک آن می‌توان ضعف‌ها و برتری‌های الگوریتم‌ها را نسبت به یکدیگر مقایسه کرد و برای ارائه مدل بهتر در نظر گرفت.

در صورتی که استحکام الگوریتم اعتماد در برابر حملات رسیدن مقدار نهایی اعتماد به اعتماد ذاتی تعریف شود، استحکام الگوریتم [۱۹] تا رسیدن رئوس مخرب به ۵۰٪، برای مدل [۲۳]، ۳۰٪ است.

جدول ۷: مقدار نهایی اعتماد با تغییر درصد رئوس مخرب

مقدار نهایی اعتماد، (t=10000)		
M. Nitti	Ing-Ray et.al.	درصد رئوس مخرب
۰/۸۴۰۴	۰/۸۶	٪۳۰
۰/۷۷۶۵	۰/۸۴۲۹	٪۳۵
۰/۷۴۶۰	۰/۸۴۰۰	٪۴۰
۰/۷۴۲۰	۰/۸۳۵۴	٪۴۵
۰/۷۲۵۸	۰/۸۳۲۸	٪۵۰
۰/۵۷۸۴	۰/۷۷	٪۷۰



شکل 5: نمودار مقدار نهایی اعتماد نسبت به درصد رئوس مخرب

٦. منابع

[۱]*directions.* Journal of Network and Computer Applications, 2019. 137: p. 93-111.

[۲] Agate, V., et al., *A Simulation Software for the Evaluation of Vulnerabilities in Reputation Management Systems.* ACM Transactions on Computer Systems, 2021. 37(1-4): p. 1-30.

[۳]Wang, D., Muller, T., Liu, Y., and Zhang, J., *Towards robust and effective trust management for security: A survey. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications.* IEEE Access, 2014: p. pp. 511-518.

[٤]Jøsang, A., Ismail, R., and Boyd, C., *A survey of trust and reputation systems for online service provision.* Decision support systems 43, 2007: p.٦١٨-٦٤٤ .

[۵]Ureña, R., et al., *A review on trust propagation and opinion dynamics in social networks and group decision making frameworks.* Information Sciences, 2019. 478: p. 461-475.
[٦]Yahiatene, Y., et al., *A blockchain-based framework to secure vehicular social networks.* Transactions on Emerging Telecommunications Technologies, 2019. 30.(۸)
[۷]Akerlof, G.A., *The Market for" Lemons": Quality Uncertainty and the Market Mechanism.* 84Q. J. ECON 488, 1970: p. 489-490.
[۸]Houser, D. and J. Wooders, *Reputation in Auctions: Theory, and Evidence from eBay.* Journal of Economics and Management Strategy, 2006. 15(2): p. 353-369.
[۹]Truong, N., et al., *A blockchain-based trust system for decentralised applications: When trustless needs trust.* Future Generation Computer Systems, 2021. 124: p. 68-79.
[۱۰] Ramya, G., et al., *A Review on Various Applications of Reputation Based Trust Management.* International Journal of Interactive Mobile Technologies (iJIM), 2021. 15.(۱۰)
[۱۱] Wang, F. and Z. Wei, *A Statistical Trust for Detecting Malicious Nodes in IoT Sensor Networks.* IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021. E104.A(8): p. 1084-1087.
[۱۲] Szaller, Á., P. Egri, and B. Kádár, *Trust-based resource sharing mechanism in distributed manufacturing.* International Journal of Computer Integrated Manufacturing, 2019. 33(1): p. 1-21.
[۱۳] Wang, Y., Cai, Z., Yin, G., Gao, Y., and Pan, Q., *A trust measurement in social networks based on game theory. In International Conference on Computational Social Networks.* Springer, 2015: p. pp. 236-247.
[۱٤] Bidgoly, A.J., *Robustness verification of soft security systems.* Journal of Information Security and Applications, 2020. 55.
[۱۵] G. D. Putra, V. Dedeoglu, S.S. Kanhere, R. Jurdak, " Toward Blockchain-Based Trust and Reputation Management for Trustworthy 6G Networks", IEEE Network Magazine, Volume36, Issue:4, 2022
[۱٦] Mayer, R.C., Davis, J.H., and Schoorman, F.D., *An integrative model of organizational trust.* Academy of management review 20, 1995: p. 709-734.
[۱۷] Y. Xiao, L. Zhu, and X. Li, "A Review on Trust and Reputation Management Systems in e-commerce and P2P Network", 2nd International Conference on E-Commerce and Internet Technology (ECIT), pp.58-62, 2021.
[۱۸] Schneider, J., Kortuem, G., Jager, J., Fickas, S., and Segall, Z., *Disseminating trust information in wearable communities.* Personal Technologies 4, 2000: p. 245-248.
[۱۹] Mui, L., Mohtashemi, M., and Ang, C., *A probabilistic rating framework for pervasive computing environments.* In Proceedings of the MIT Student Oxygen Workshop (SOW'2001), 2001.
[۲۰] Josang, A., and Ismail, R., *The beta reputation system.* In Proceedings of the 15th bled electronic commerce conference, 2002. 5: p. pp. 2502-2511.
[۲۱] Aringhieri, R., and Bonomi, D., *A simulation model for trust and reputation system evaluation in a P2P network.* In Computational Intelligence, Theory and Applications. (Springer), 2006: p. pp. 169-180.
[۲۲] Hoffman, K., Zage, D., and Nita-Rotaru, C., *survey of attack and defense techniques for reputation systems.* ACM Computing Surveys (CSUR), 2009: p. 42, 1-31.

[۲۳] Yan, S. and L. Yuhong, *Security of Online Reputation Systems: The evolution of attacks and defenses.* IEEE Signal Processing Magazine, 2012. 29 :(۲)p. 87-97.

[۲٤] Sun, Y.L., Han, Z., Yu, W., and Liu, K.R., *Attacks on trust evaluation in distributed networks.* In 2006 40th Annual Conference on Information Sciences and Systems. (IEEE), 2006: p. pp. 1461-1466.

[۲٥] H. Wu, D. Gao, Sh. Li, W. Su, H. Zhang, " Towards an efficient DHT-based identifier-to-locator separation approach", 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), pp.3-7, 2010.

[۲٦] Weng, J., *An Entropy-Based Approach to Protecting Rating Systems from Unfair Testimonies.* IEICE Transactions on Information and Systems, 2006. E89-D(9): p. 2502-2511.

[۲۷] Mui, L., Mohtashemi, M., Ang, C., Szolovits, P., and Halberstadt, A., *Ratings in distributed systems: A bayesian approach. In Proceedings of the Workshop on Information Technologies and Systems.* WITS, 2001: p. pp. 1-7.

[۲۸] Bidgoly, A.J. and B.T. Ladani, *Modelling and Quantitative Verification of Reputation Systems Against Malicious Attackers.* The Computer Journal, 2015. 58(10): p. 2567-2582.

[۲۹] V. Thirunavukkarasu, A. S. Kumar, D. C. J. Josephine, T. P. Arasu," Selection of Optimistic Nodes for Reputation Based Routing in Wireless Networks", 7th International Conference on Smart Structures and Systems (ICSSS), pp.1-3, 2020

[۳۰] Jøsang, A., *Robustness of trust and reputation systems: Does it matter?* In IFIP International Conference on Trust Management. (Springer), 2012: p. pp. 253-262.

[۳۱] Yan Lindsay, S., et al., *Information theoretic framework of trust modeling and evaluation for ad hoc networks.* IEEE Journal on Selected Areas in Communications, 2006. 24(2): p. 305-317.

[۳۲] Aldini, A., *Formal approach to design and automatic verification of cooperation-based networks.* IARIA Int J Adv Internet Technol 6, 2013: p. 2.

[۳۳] Ignjatovic, A. (2021). Trust-based blockchain authorization for iot. *IEEE Transactions on Network and Service Management*, *18*(2), 1646-1658

۳٤ Cheng, C. L., Xu, X. L., & Gao, B. Z. (2012). METrust: A mutual evaluation-based trust model for P2P networks. *International Journal of Automation and computing*, *9*(1), 63-71.

[۳٤] Ebrahimi, Tedin, Mohammad Hossam, Sayadhaghiqi, & Mohammad. (2021). Trust Algorithms in Internet of Things: Review, Analysis and Presentation of Evaluation Criteria.

Evaluating the robustness of discrete event operations in the blockchain system of digital currencies

Hossein Shadi[*1]
Yaqub Farjami [2]

Abstract

The main feature of anonymous digital money is the transfer process, which they call the advantage of digital money and believe that in this way, you can protect your privacy from security centers and also collect personal information from institutions. Maintain financial and electronic payments such as Visa. But instead, some governments have banned or restricted its use in their country by focusing on this point because they believe that through this system, dirty money is exchanged and social and national security is endangered. Direct payment without intermediaries is another advantage of digital money. While because its nature is not the desire of another country, as long as two parties exchange with digital money, there is no need to convert it into other currencies for payment and transfer. to be The boundary of the feature is limited. In this research, with two algorithms (Nitti et.al) and (Rayet.al-Ing) which are used in the block chain of distribution systems in digital currencies, they are evaluated and compared against the possible events and probability, and the results are based on the results It is confirmed from other researches.

Key words*:* Digital currencies, distribution systems, event detection, robustness evaluation

1. Graduate(master's degree, Information Technology Engineering, University of Qom,Qom) ho3einshadi@gmail.com
2. Associate Professor, Computer Engineering, University of Qom, Qom) farjami@gmail.com