

ارزیابی استحکام صورت عملیات گسسته رخداد در سیستم بلاکچین ارزهای دیجیتال

حسین شادی^{۱*}

یعقوب فرجامی^۲

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 می دانند 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 الکترونیکی 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 مهاجران 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 می کنند 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 باشد که نیاز اساسی ارزهای دیجیتال در یک زنجیره بلوکی سیستم توضیح شده می طلبد، در این پژوهش با دو الگوریتم (Nitti et.al) و (Ing-Rayet.al) که در زنجیره بلوکی سیستم های توضیح در ارزهای دیجیتال استفاده می شود در برابر حوادث و حملات احتمالی ارزیابی و مقایسه می شوند و نتایج آن با استناد از نتایج بدست آمده از دیگر پژوهش ها تایید می شود، 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، سیستم های توضیح، گسسته رخداد، ارزیابی استحکام

^۱ کارشناسی ارشد، مهندسی فناوری اطلاعات، دانشگاه قم، قم. ho3einshadi@gmail.com

^۲ دانشیار، مهندسی کامپیوتر، دانشگاه قم، قم. farjami@gmail.com

۱. پیشینه پژوهش ارزهای دیجیتال

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



شکل 1: الگوریتم‌های اجماع در سیستم‌های بلاک‌چین

۲. الگوریتم اجماع

بلاک‌چین‌ها در حقیقت 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 توزیع شده ساخته شده‌اند و این نودها برای انجام تراکنش‌هایی که در این شبکه روی می‌دهد، باهم همکاری می‌کنند؛ بنابراین ضرورت دارد که هر شبکه بلاک‌چین مکانیسمی داشته باشد که از طریق 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 بلاک‌چین اضافه شوند. به این سیستم غیرمتمرکز که

وضعیت صحیح بلاک چین را تعیین می کند، مکانیسم اجماع^۱ می گویند. مکانیسم های اجماع علاوه بر تضمین اجرای همه عملیات یک بلاک چین، می توانند روی ویژگی های مالی و امنیتی شبکه نیز تأثیر مستقیم بگذارند.

۳. انواع الگوریتم های اجماع در بلاک چین

بیشتر بلاک چین ها سه ویژگی اصلی دارند: «مقیاس پذیری» و «تمرکززدایی» و «امنیت». توسعه دهندگان هر بلاک چین به دنبال راهی هستند تا این سه ویژگی را از طریق کدهای برنامه نویسی در شبکه وارد کنند. ویتالیک بوترین، بنیان گذار اتریوم، این سه ویژگی را سه گانه بلاک چین^۲ نام گذاری کرده است؛ چون جمع کردن هم زمان هر سه آن ها در بلاک چین کار دشواری است. تلاش برای طراحی و پیاده سازی مدل حاکمیتی غیر متمرکز برای بلاک چین که تعادلی میان این سه ویژگی برقرار کند، مشکلی است که همچنان ادامه دارد؛ از این رو، هر بلاک چین مکانیسم اجماعی را برای خود انتخاب می کند که با اولویت های راهبردی اش بیشترین مطابقت را دارد. در ادامه مطلب، رایج ترین الگوریتم های اجماع را به اختصار معرفی خواهیم کرد.

۳-۱. اثبات کار

الگوریتم اجماع اثبات کار^۳ یا PoW مکانیسم اجماع غیر متمرکزی است که مشارکت کنندگان در شبکه را به حل معمایی ریاضی با استفاده از قدرت محاسباتی ملزم می کند تا از اقدامات مخرب و اسپم در سیستم جلوگیری کند. در این روش، همه ماینرها تلاش می کنند 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 می کند.

بیت کوین اولین ارز دیجیتالی است که از روش اجماع اثبات کار استفاده کرد. هر بلاک یک هیدر^۴ دارد که از هش حاوی اطلاعاتی از جمله عددی ۳۲ رقمی به نام نانس^۵ تشکیل شده است. هش خروجی تابعی یک طرفه است که ورودی آن را نمی توان از روی خروجی حدس زد. ماینرها باید هیدر بلاک بعدی را با استفاده از نانس های مختلف وارد تابع هش کنند تا زمانی که خروجی هش کمتر یا مساوی هش هدف را پیدا کنند که خود بلاک چین تعیین می کند. هر ماینری که هش مدنظر را پیدا کند، در واقع برنده حل همان معمای ریاضی است. اثبات کار امنیت بلاک چین را تأمین و آن را از دست کاری و حملات هکری و دوبار خرج کردن^۶ محافظت می کند؛ اما انتقادهایی هم به این روش وارد است که مهم ترین آن ها مصرف بسیار زیاد انرژی است. الگوریتم اثبات کار به قدرت محاسباتی بسیاری نیاز دارد که به مصرف انرژی فراوانی منجر می شود. گفتنی است علاوه بر بیت کوین، اتریوم نیز از این روش استفاده می کند؛ 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

۲-۳. اثبات سهام

در مکانیسم اجماع اثبات سهام^۷ یا PoS، مشارکت کنندگان به جای صرف قدرت محاسباتی و انرژی، باید مقداری از ارز دیجیتال همان بلاک چین را سهام گذاری^۸ کنند. در این روش، هر کسی که سهام بیشتری در شبکه داشته باشد، بخت بیشتری برای برنده شدن و دریافت پاداش دارد. ابتدا عده‌ای از سهام‌گذاران به صورت تصادفی انتخاب می‌شوند تا به عنوان نود فعالیت کنند. این نودها باید مقداری حداقلی از توکن‌های خود را سهام گذاری کرده باشند. سپس، تعدادی از نودها طی رأی گیری انتخاب می‌شوند تا به عنوان اعتبارسنج تراکنش‌های معتبر را تأیید و بلاک بعدی را ایجاد کنند.

الگوریتم اجماع اثبات سهام در بلاک چین‌های مختلف به شکل‌های متفاوتی پیاده‌سازی شده است؛ اما در همه آن‌ها اصل بر این است که افراد با سهام گذاری 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. با این حال، برخی نیز انتقاد می‌کنند که روش اثبات سهام سیستم را از غیرمتمرکز بودن دور می‌کند. اتریوم^۹، بی‌ان‌بی چین (BNB)^{۱۰}، تزوس^{۱۱} و بسیاری دیگر از بلاک چین‌ها از این روش استفاده می‌کنند.

۳-۳. اثبات سهام نمایندگی شده

اثبات سهام نمایندگی شده^{۱۱} یا DPoS یکی دیگر از انواع اثبات سهام است. در این مکانیسم نیز مشارکت کنندگان باید مقداری توکن در شبکه سهام گذاری کنند تا امکان مشارکت را داشته باشند. تفاوت اثبات سهام نمایندگی شده با اثبات سهام عادی این است که در روش نمایندگی شده، سهام‌گذاران حق رأی ناشی از توکن‌های خود را به افرادی می‌دهند که به آنان نماینده (Delegate) گفته می‌شود. سپس، این نمایندگان با رأی گیری اعتبارسنج‌ها را از میان سهام‌گذاران انتخاب می‌کنند. این اعتبارسنج‌ها تراکنش‌ها را تأیید و در ازای آن کارمزد تراکنش‌ها را به عنوان پاداش دریافت می‌کنند. قدرت رأی هر یک از مشارکت کنندگان متناسب با مقدار توکن‌هایی است که سهام گذاری کرده‌اند. به دلیل همین سیستم رأی گیری است که برخی از این الگوریتم به عنوان روش اجماع دموکراتیک یاد می‌کنند. روش اثبات سهام نمایندگی شده در مقایسه با الگوریتم‌های اثبات کار و اثبات سهام عادی سرعت بیشتری در پردازش و تأیید تراکنش‌ها دارد؛ چرا که برای این کار به تعداد کمتری اعتبارسنج نیازمند است. ایاس^{۱۱} یکی از بلاک چین‌های محبوبی است که از الگوریتم اجماع اثبات سهام نمایندگی شده استفاده می‌کند.

⁷ Proof of Stake

⁸ Staking

⁹ Tezos

¹⁰ Delegate Proof of Stake

¹¹ EOS

۳-۴. اثبات سهام اجاره شده

الگوریتم اجماع اثبات سهام اجاره شده^{۱۲} 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 اجاره شده 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 در نتیجه دریافت پاداش انتخاب شود؛ از این رو، دارندگان کوچک یک استخر تشکیل می‌دهند و توکن‌های خود را به یک نود می‌دهند تا مجموع توکن‌ها به میزان درخور توجهی 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 اجاره شده از برخی جهات شبیه اثبات سهام نمایندگی شده است؛ اما تفاوت این دو مکانیسم اجماع آن جاست که در روش اثبات سهام نمایندگی شده، توکن‌ها به نمایندگان واگذار می‌شوند و آنان اعتبارسنج‌ها را انتخاب می‌کنند؛ در حالی که در روش اثبات سهام اجاره شده توکن‌ها مستقیماً به اعتبارسنج‌ها اجاره داده می‌شوند. بلاک چین ویوز^{۱۳} از روش اثبات سهام اجاره شده استفاده می‌کند.

۳-۵. اثبات زمان سپری شده

الگوریتم اجماع اثبات زمان سپری شده^{۱۴} یا PoET اساساً در بلاک‌چین‌های خصوصی یا نیازمند مجوز به کار می‌رود؛ یعنی بلاک‌چین‌هایی که برای ورود به آن نیاز به مجوز و احراز هویت است. در این روش، هر یک از مشارکت‌کنندگان باید مدت زمان مشخصی را منتظر بمانند. طول این مدت زمان به صورت تصادفی تعیین می‌شود. هر کاربری که مدت زمان انتظارش سپری می‌شود، مجوز ورود به دفتر کل را دریافت و بلاکی جدید ایجاد می‌کند.

ابتدا هر یک 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. هر یک از مشارکت‌کنندگان مدت زمان انتظار تصادفی را از همان منع کد می‌گیرند. وقتی مدت زمان انتظار سپری شود، کاربر مدنظر مجوز ایجاد بلاک را دریافت می‌کند. هایپرلجر ساوتووث^{۱۵} بلاک‌چینی ماژولار است که از روش اثبات زمان سپری شده 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^{۱۶} یا DAG در واقع نوعی ساختار داده است؛ اما می‌توان آن را روشی برای اجماع نیز در نظر گرفت. در بلاک چین، بلاک‌های حاوی اطلاعات تراکنش‌ها به صورت پشت سرهم به شبکه اضافه می‌شوند و توالی‌ای از داده‌ها را ایجاد می‌کنند. به همین دلیل، 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. در DAG، همه تراکنش‌ها بدون در نظر گرفتن ترتیب آن‌ها وارد دفترکل توزیع شده 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؛ در نتیجه، تصویر کامل‌تری از تراکنش‌های شبکه به دست می‌آید. یکی از مزایای DAG در مقابل بلاک چین این است که حجم کمتری را اشغال می‌کند؛ از این رو، هزینه تراکنش کاهش و سرعت شبکه افزایش می‌یابد. آیوتا^{۱۷} و هِدِرا هشگراف^{۱۸} دو شبکه‌ای هستند که از گراف‌های جهت‌دار غیرمدور استفاده می‌کنند.

۳-۷. اثبات فعالیت

مکانیسم اجماع اثبات فعالیت^{۱۹} 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 به صورت 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 استخراج کنندگان و اعتبارسنج‌هایی توزیع می‌شود که در پردازش و امضای آن بلاک مشارکت کرده‌اند. مکانیسم اجماع فعالیت احتمال حمله ۵۱ درصد 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. با وجود این، 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 انتخاب شدن به عنوان امضاکننده بلاک بیشتر است؛ به همین دلیل، پاداش بیشتری هم دریافت می‌کنند. بلاک چین‌های دیگر (Decred) و اسپرز^{۲۰} 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 به کاررفته 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 از طریق خوشه‌های فعالیت با یکدیگر برقرار کرده‌اند.

در مکانیسم اثبات اهمیت، دارندگان بیشترین توکن‌ها قدرت مطلق در شبکه نیستند؛ از این رو، ریسک تمرکز قدرت و ثروت در این روش اندک است. همچنین، اگر فورک جدیدی ایجاد شود، مشارکت کنندگان باید منابع بیشتری را به کار گیرند تا فعالیتشان را به فورک‌های جدید هم گسترش دهند و بتوانند امتیازشان را حفظ کنند. این باعث می‌شود که مشارکت کنندگان انگیزه چندانی برای ایجاد فورک‌های بی‌مورد نداشته باشند. بلاک‌چین‌های نیو اکونومی موومننت^{۲۴} یا NEM^{۲۵} از مکانیسم اجماع اثبات اهمیت استفاده می‌کند.

۳-۹. اثبات ظرفیت / فضا

الگوریتم اجماع اثبات ظرفیت^{۲۶} یا اثبات فض^{۲۷} که به اختصار PoC یا PoSpace نامیده می‌شود، از فضای قابل استفاده 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 رمزنگاری شده 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 بلاک‌چین فایل کوین (Filecoin) دارد. مکانیسم اجماع اثبات ظرفیت در بلاک‌چین‌هایی مثل پرما کوین^{۲۹} و برست کوین (Burstcoin) و اسپیس مینت (SpaceMint) به کار 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^{۳۰} یا PoB، ماینرها باید توکن‌های خود را برای همیشه از بین ببرند یا به اصطلاح بسوزانند تا در ازای آن حق استخراج بلاک‌های جدید و تأیید تراکنش‌ها را به دست بیاورند. هرچه ماینرها توکن‌های بیشتری بسوزانند، بخت بیشتری برای انتخاب شدن به عنوان اعتبارسنج بلاک بعدی خواهند داشت. بدین ترتیب، ماینرها به جای 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 در مقایسه با سیستم‌های اثبات کار مصرف می‌کند. پروتکل‌های کانترپارتنری (Counterparty) و اسلیم کوین (Slimcoin) و فکتوم (Factom) از مکانیسم اجماع اثبات سوختن استفاده می‌کنند.

۳-۱۱. اثبات وزن

اثبات وزن^{۳۱} یکی از مدل‌های ارتقاء یافته اثبات سهام است که می‌کوشد مشکل توزیع ناعادلانه پاداش را در اثبات سهام حل کند. در روش اثبات سهام، دارندگان سهام بیشتر بخت بیشتری برای انتخاب شدن به عنوان اعتبارسنج و در نتیجه دریافت پاداش دارند.

الگوریتم اثبات وزن علاوه بر میزان سهام مشارکت‌کنندگان، عوامل دیگری را نیز در نظر می‌گیرد. برای مثال، فایل کوین حجم داده IPFS مشارکت‌کنندگان را هم محاسبه می‌کند. این کار مشابه همان روشی است که در الگوریتم‌های اثبات فضا زمان^{۳۲} و اثبات تکثیر^{۳۳} به کار می‌رود.

۳-۱۲. اثبات ذخیره و اثبات تکثیر و اثبات فضا زمان

الگوریتم اجماع اثبات ذخیره^{۳۴} یا همان PoStorage به جای سهام‌گذاری، مبتنی بر داده طراحی شده است. این پروتکل به دلیل 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 به جای در نظر گرفتن توکن‌های سهام‌گذاری شده، مقدار ذخیره داده هر نود مبنای 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 تأمین کنندگان ذخیره‌سازی داده مبتنی بر بلاک چین، از دو نوع مکانیسم اجماع اثبات ذخیره استفاده می‌کند: یکی اثبات تکثیر^{۳۶} یا PoRep و دیگری اثبات فضا زمان یا ProSpacetime در اثبات تکثیر، نودهای مشارکت کننده در شبکه می‌توانند از طریق مکانیسم اجماع تأیید کنند که مقدار مشخصی داده در فضای ذخیره فیزیکی که منحصرأ برای همان اختصاص داده شده، تکثیر شده است.

همچنین، شبکه فایل کوین با استفاده از مکانیسم اثبات فضا زمان به صورت تصادفی ماینرهای را انتخاب می‌کند که داده‌ها باید از طریق آن‌ها خوانده و سپس تأیید و در یک گواه اثبات فضا زمان فشرده‌سازی شود. سپس، ماینرها باید گواه متناظری فراهم کنند مبنی بر اینکه داده‌های مدنظر در دوره زمانی مشخصی به صورت 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 منحصر به فردی از یک داده را در همان لحظه‌ای ذخیره کرده که مَهر شده است. از کاربرد دیگر اثبات فضا زمان این است که نودها را به صورت تصادفی بررسی می‌کند تا مطمئن شود که فضای ذخیره داده مدنظر را به صورت مستمر تأمین کرده‌اند. علاوه بر 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 مبتنی بر شهرت^{۳۸} استفاده می‌کند. در بلاک چین‌های اثبات اعتبار، معمولاً اعتبارسنج‌ها را دیگر مشارکت کنندگان شبکه به عنوان مدیران سیستم انتخاب می‌کنند. از این رو، اعتبارسنج‌ها معمولاً سرمایه‌گذاران نهادی یا شرکای راهبردی حاضر در اکوسیستم آن بلاک چین هستند که منافعتشان در موفقیت بلندمدت شبکه است و با افشای هویت خود برای مسئولیت‌پذیری مشکلی ندارند.

در بلاک چین‌های اثبات سهام، نودهای اعتبارسنج برای تضمین رفتار مسئولانه باید سرمایه مالی خود را به میان بیاورند؛ اما در بلاک چین‌های اثبات اعتبار، آنان از سرمایه اجتماعی خود که همان شهرت است، برای تضمین عملکردشان هزینه می‌کنند. با وجود این، بسیاری از این بلاک چین‌ها اعتبارسنج‌ها را ملزم می‌کنند که علاوه بر اعتبارشان، سرمایه مالی سنگینی را نیز در شبکه سرمایه‌گذاری کنند. با این کار کسانی که اشتیاق کافی برای اعتبارسنج شدن 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 بلاک چین‌های اثبات اعتبار را دارای ماهیت متمرکز یا نیمه‌متمرکز قلمداد کنند. بیشتر بلاک چین‌های اثبات اعتبار تعداد اعتبارسنج‌ها را محدود می‌کنند تا مقیاس‌پذیری شبکه

³⁵ Filecoin

³⁶ Proof of Replication

³⁷ Proof of Authority

³⁸ Reputation

افزایش یابد. در نتیجه، 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 پیش از 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 کاربران 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. در نهایت، 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؛ به همین دلیل، 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 از طریق آن لحظه وقوع هر رویدادی روی بلاک چین اثبات پذیر 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 از طریق تابع هش ساده SHA-256 رمزگذاری می‌کند و ساعت مخصوص خود را دارد.

هر بار که اعتبارسنج‌های سولانا با یکدیگر ارتباط برقرار می‌کنند، یک گواه رمزنگاری شده از ترتیب و زمان هر پیام در دفترکل شبکه ذخیره می‌شود. بدین ترتیب، 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 غیرمتمرکز بودن شبکه کاسته شود، البته این اقدام باعث کاهش امنیت سیستم می‌شود و برای افزایش راندمان بهتر است براساس نوع اجماع والگویه درست پیاده‌سازی انجام دهیم که این اقدام به صرفه‌تر است زیرا بعضی از ارزش‌های دیجیتال نیاز به نوع پیاده‌سازی متمرکز، غیر متمرکز بودن یا نیمه متمرکز بودن برای توضیح 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 الگوریتم‌های اجماع از فرمول (۱) استفاده می‌کنیم که در آن X_T تعداد حملات موفق هست و O_K درصد موفقیت حملات در الگوریتم اجماع می‌باشد.

$$O_k = \frac{(\max X_T)}{\sum_1^K x} \quad (1)$$

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

$$T_{ij} = \alpha R_{ij} + \beta I_{ij} + \gamma O_{ij}^{dir} + \delta O_{ij}^{ind} \quad (2)$$

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

جدول ۱: آسیب پذیری الگوریتم‌های اجماع در برابر حملات

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

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

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

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

جدول ۲: معیارهای مقایسه الگوریتم اجماع

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

۴. الگوریتم‌های رمزنگاری

۴-۱. الگوریتم SHA-256

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

الگوریتم‌های هش ایمن در گروه توابع هشینگ کریپتوگرافیک (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.

۴-۲. الگوریتم sCrypt

الگوریتم اسکرپیت^{۴۷} یک الگوریتم هش است که در بلاک‌چین‌های با ساز و کار اثبات کار خاصی استفاده می‌شود و با تولید اعداد تصادفی و غیر تکراری فرایند استخراج بلاک را برای کاربران مخرب دشوار می‌کند و باعث افزایش چندین برابری امنیت شبکه‌های ارز دیجیتال می‌شود.

به عبارت ساده‌تر اسکرپیت رشته‌های الفبایی منحصر به فرد و غیر تکراری 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 اسکرپیت به این منظور طراحی شده تا شکستن رمز عبورهایی که با این الگوریتم هش شده را برای سخت افزارهای مخصوص مانند ASIC ها دشوارتر کند. 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 به راحتی 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 Artfortz توسعه یافت. اولین پروژه بلاک‌چینی بود که از الگوریتم استخراج sCrypt به عنوان یک الگوریتم هش استفاده می‌کرد.

⁴⁷ sCrypt

۳-۴. الگوریتم Ethash

الگوریتم استخراج Ethash اولین بار توسط بنیانگذار و خالق اتریوم یعنی ویتالیک بوتورین^{۴۸} در سال ۲۰۱۳ تا ۲۰۱۴ ساخته شد؛ بنابراین از این الگوریتم برای ارزهای دیجیتال 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 ASIC را مجبور به مخفی کردن و کاهش قدرت هش دستگاه‌های خود کرد.

ویتالیک بوتورین 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 ASIC برای 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)

۴-۴. الگوریتم X11

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 Script فقط یک تابع هش تنها نیست، بلکه از ۱۱ تابع هش متفاوت ساخته شده است.

۵-۴. 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 متن‌با^{۵۱}ز و پروتکل لایه‌ای کاربردی است.

⁴⁸ Vitalik Buterin

⁴⁹ Bitmain

⁵⁰ CryptoNight

الگوریتم استخراج کریپتونايت هم به گونه ای طراحی شده که در مقابل ASIC مقاوم است. ویژگی اصلی این الگوریتم هاش بسیار سریع آن است و امکان مقیاس پذیری خوبی را فراهم می کند.

هدف اصلی از ایجاد این الگوریتم استخراج، پر کردن شکاف بین ماینرهای است که فقط به پردازنده CPU دسترسی دارند و توانایی تهیه سخت افزارهایی نظیر کارت های گرافیک و ASIC 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: الگوریتم های رمزنگاری استفاده شده در بلاکچین

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

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

از جایی که بررسی عملکرد روش‌های کنترل اعتماد و شهرت در ارتباطات ضروری است، در این قسمت با معرفی شاخص‌های عددی، شیوه‌هایی با مقایسه نتیجه‌های کمی حاصل از شبیه‌سازی 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 گره‌های 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 جدول‌های ۱ و ۲ مقایسه و ویژگی‌های عمده شهودی ارائه شد و الگوریتم‌ها در جدول ۴ نکاتی به دست می‌آید که به وسیله آن می‌توان ضعف‌ها و برتری‌های الگوریتم‌ها را نسبت به یکدیگر مقایسه کرد و برای ارائه مدل بهتر مد نظر داشت.

جدول ۴: معیار ارزیابی مدل‌ها در برابر حوادث گسسته رخداد

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

[23]	ذهنی	×	×	×	×	×	×	×	ارائه خدمت	✓	×	×	×	✓	نرخ موفقیت
	عینی								بد، بازخورد منفی	×				✓	
[37]		×	✓	✓	×	×	×	×	ارائه خدمت راس خودخواه، تبانی	×	×	×	×	×	توان عملیاتی شبکه و از دست دادن بسته، پیشنهادهای تقلبی کشف شده، منفی اشتباه و مثبت اشتباه در حضور حملات بدگویی و خوب گویی
[19]		✓	✓	✓	×	×	×	×	---	×	×	✓	×	×	همگرایی، دقت و انعطاف پذیری الگوریتم در رسیدن به ذاتی، اعتماد مقایسه با روش های Eighen Trust و Peer Trust
[24]		×	✓	✓	×	×	×	×	---	×	×	×	×	×	همگرایی و دقت الگوریتم در رسیدن به اعتماد ذاتی

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

در مقاله ۳۳ دو الگوریتم جهت ارزیابی ارائه شده است که بر اساس آن الگوریتم های مورد استفاده در ارزشهای دیجیتال احراز هویت می شوند 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 دیجیتال 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 \emptyset
 1: authorized $\leftarrow 0$
 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 $\text{getBalance}(PK_{SC_i}) \geq \varphi r$ then
 5: authorized $\leftarrow \text{True}$
 6: end if
 7: end if
 8: end if
 9: if authorized then
 10: return Token
 11: else
 12: return \emptyset
 13: end

Algorithm 2 Feedback Mechanism

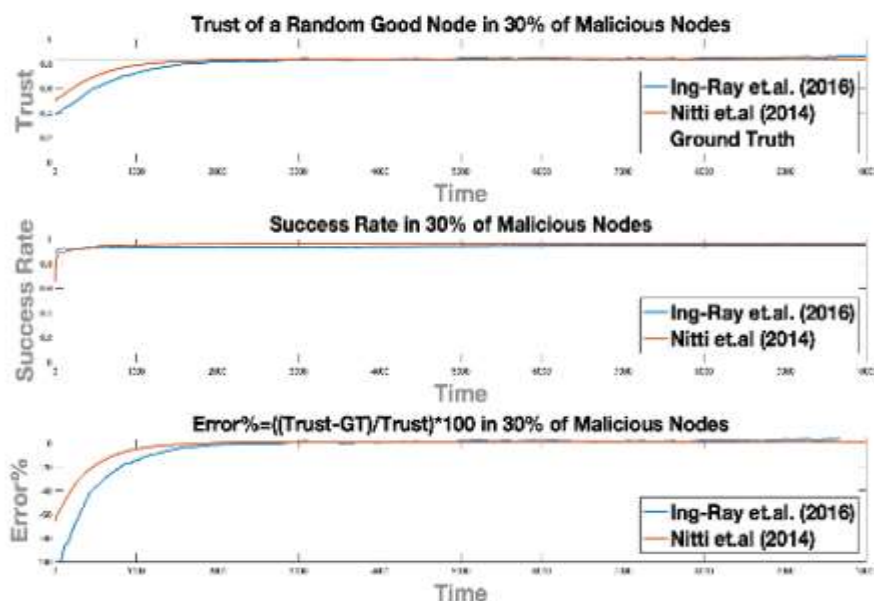
Input: $P_{(r,c)}, TX_F$
 Output: True or False
 1: last_update $\leftarrow \text{getUpdateTimestamp}(\text{Data})$
 2: access_timestamp $\leftarrow \text{getAccessTimestamp}(\text{Data})$
 3: evidence $\leftarrow \text{checkSig}(\text{Data})$
 4: result $\leftarrow \text{False}$
 5: if $H(\neg \text{Token} \mid _R)$ exist then
 6: return result
 7: end if
 8: if $(\text{access_timestamp} - \text{last_update}) < U_r$ then
 9: if $F_{(SP_j,r)} = \text{positive}$ and evidence = True then
 10: $\epsilon_t \leftarrow \epsilon_{\text{pos}}$
 11: result $\leftarrow \text{True}$
 12: end if
 13: else
 14: if $F_{SP_j,r} = \text{negative}$ and evidence = True
 15: $\epsilon_t \leftarrow \text{neg}$
 16: eut $\leftarrow \text{True}$
 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: reCalculate $T_{SP_j}^{SC_i}, A_{SC_i}, R_{SC_i}$
 25: sendCryptoTo (SP_j)

الگوریتم های زیادی جهت محاسبه ترکیب وزن دار اعتماد وجود دارند که نظر کلیه رئوسی که با معتمد تراکنش داشته اند بررسی می کنند. در حالی که در مدل میانگین، نظر تعدادی از دوستان که بیشترین شباهت به معتمد را دارند، به صورت وزن دار با یکدیگر ترکیب می شوند. با توجه به نتایج شبیه سازی، جمع آوری نظرات کلیه پیشنهاددهندگان تا زمانی که رئوس مخرب ۳۰ درصد یا کمتر باشد بهتر حساب می کنند؛ در حالی که با بالا رفتن درصد رئوس مخرب، اهمیت پایش نظراتی که با یکدیگر ترکیب می شوند بیشتر می شود؛ لذا الگوریتم میانگین ریاضی با وجود نیمی از رئوس مخرب بعد از ۴۹۳۱ ثابت زمانی به اعتماد ذاتی می رسد.

جدول 5 bn: پارامترهای شبیه سازی

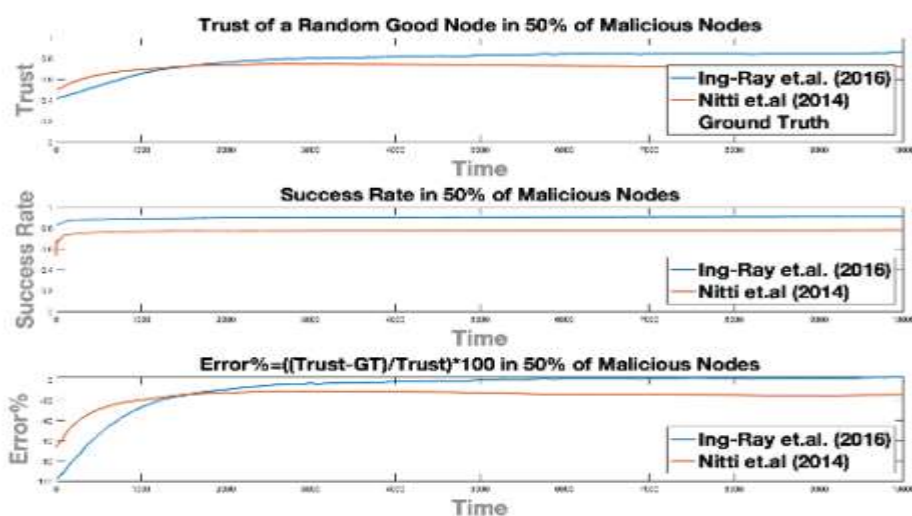
پارامتر	مقدار
تعداد کاربران	۴۰
الگوریتم دوستی کاربران	باراباسی-آلبرت
تعداد اشیا	۲۰۰
تقسیم بندی مکانی	۱۶*۱۶
الگوریتم حرکت	SWIM
نوع حمله	خوب گویی و بدگویی
درصد رئوس مخرب	۳۰٪ و ۵۰٪
زمان نهایی	۱۰,۰۰۰
تکرار مونت کارلو	۵۰

شکل ۲ نتایج مقایسه عملکرد سرعت و دقت رسیدن به اعتماد و شهرت کلی یک همسایگی خوب تصادفی، نرخ موفقیت و درصد خطا در حضور 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.



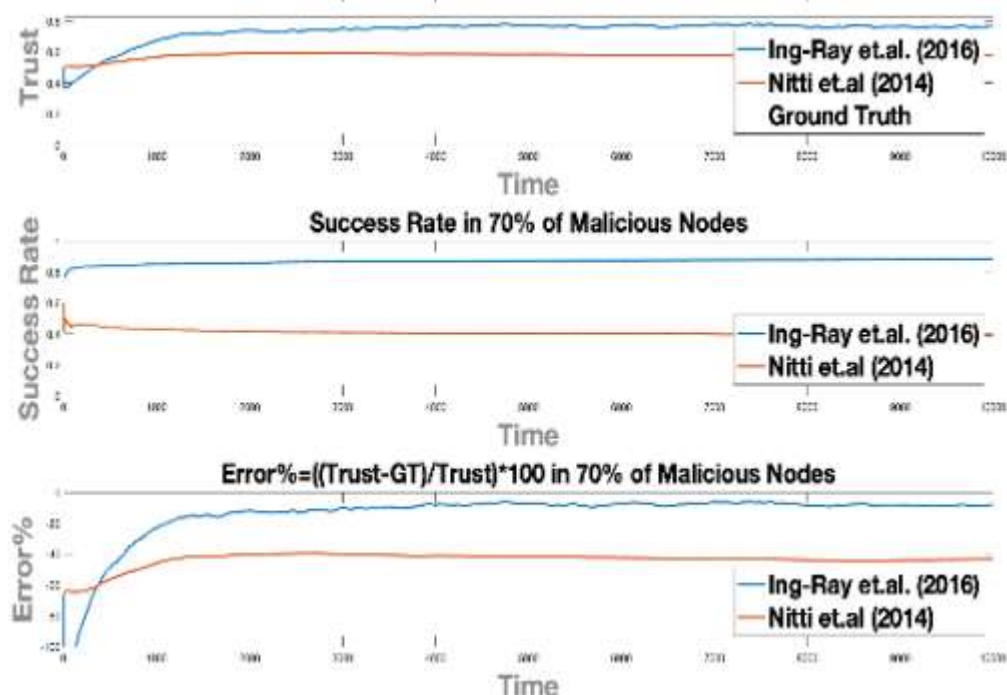
شکل 2: مقایسه دو مدل در حضور ۳۰ رأس مخرب

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 یکی 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 شبیه‌سازی را در می‌توان مشاهده کرد. با توجه به مرجع [۳۴] اعتماد همگانی رأس خوب استوکاستیک ۸۳٪ جهت مقایسه دو مدل بررسی زمان رسیدن به ۸۳٪ در نظر گرفته شده است؛ جدول ۴ نشان

می دهد که الگوریتم [۳۳] با درصد مجاورت ویرانگر پایین تر زودتر به ۸۳/۰ همگرا می شود؛ در حالی که با بالا رفتن درصد رثوس ویرانگر تا پایان زمان شبیه سازی همگرا نمی شود؛ 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 نتیجه گیری است، عملکرد بهتر در جداول به صورت خانه های حاشیه دار نمایش داده شده اند.

جدول ۶: مقایسه نتایج کمی حاصل از شبیه سازی در مقالات m.nitti, ing-ray et.al

زمان رسیدن به اعتماد ذاتی			
درصد رثوس 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)			

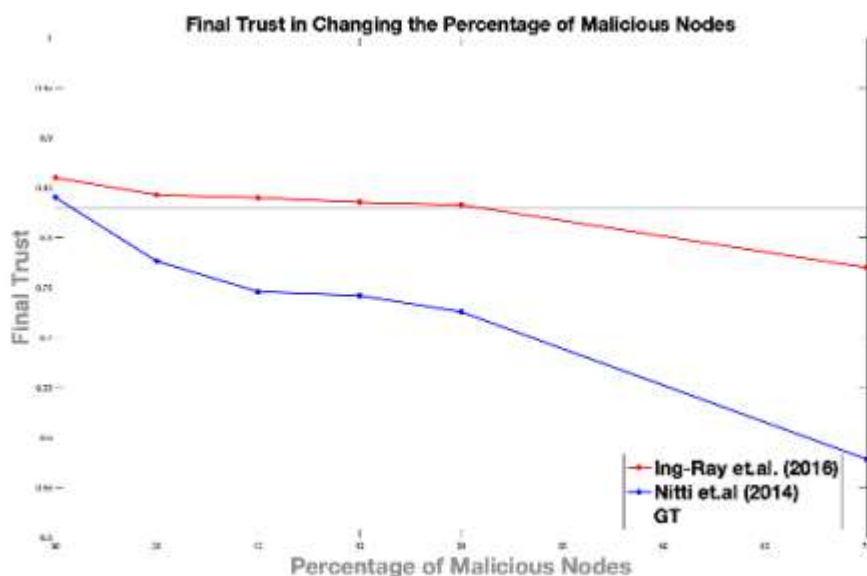
در فرآیند مقایسه زمان شبیه سازی به دو حالت گذرا و ناگذر تقسیم می شوند به این ترتیب که از ابتدا تا رسیدن به اعتماد ذاتی، زمان گذرا و پس از آن زمان پایدار الگوریتم در نظر گرفته می شود و مقایسه حسابی این دو روش در زمان پایداری در جدول ۶ نشان داده شده است. هدف از این مقایسه بررسی پایداری الگوریتم بعد از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

جدول نشانگر زمانی که درصد گره هلی مخرب ۳۰ باشد الگوریتم وزندار خطای کمتری دارد، در حالی که با افزایش درصد حملات به ثبات نمی رسند و بنابراین اعدادی برای مقایسه وجود نخواهد داشت. با در نظر گرفتن جداول ۴ و ۵ و ۶ ویژگی های دو مدل و نتایج عددی حاصل از شبیه سازی های ارائه شده در جدول ۶ نکاتی بدست می آید که به کمک آن می توان ضعف ها و برتری های الگوریتم ها 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 رثوس مخرب به ۵۰٪، برای مدل [۲۳]، ۳۰٪ است.

جدول ۷: مقدار نهایی اعتماد با تغییر درصد رئوس مخرب

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



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

۶. 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.
- [۴] Jøsang, A., Ismail, R., and Boyd, C., A survey of trust and reputation systems for online service provision. Decision support systems 43, 2007: p. ۶۱۸-۶۴۴.

- [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.
- [۶] 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.
- [۱۴] 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
- [۱۶] 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.
- [۲۴] 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.
- [۲۵] 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.
- [۲۶] 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
- ۳۴ 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.
- [۳۴] Ebrahimi, Tedin, Mohammad Hossam, Sayadghiqi, & 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