مقایسه فرآیند اجماع در زنجیره‌بلوکهای معروف دنیا

Comparison of consensus protocols in famous blockchains

سیدجواد کاظمی‌تبار، استادیار دانشگاه صنعتی نوشیروانی بابل و مشاور شرکت داده‌کاوان هوشمند توسن،
Javad Kazemitabar, Babol Noshirvani University of Technology/Tosan Intelligent Data Miners
j.kazemitabar@nit.ac.ir

دکتر قربان خردمندیان، کارشناس ارشد، شرکت داده‌کاوان هوشمند توسن،
Ghorban Kheradmandian, Tosan Intelligent Data Miners
kheradmandian@tidm.ir

چکیده (فارسی)

کوتاه‌زمانی پس از آنکه مفهوم زنجیره‌بلوکی توسط ساتوشی ناکاموتو در قالب بیت‌کوین معرفی شد، برخی از افراد آینده نگر در حوزه فناوری پتانسیل‌های این مساله که زنجیره‌بلوکی را از بیت‌کوین جدا کنند دریافتند. این آغازی برای ایجاد زنجیره‌های بلوکی خصوصی بود. عنصر کلیدی همه این زنجیره‌های بلوکی فرآیندی به نام اجماع است. بلاک‌ها بوسیله فرایند اجماع راست آزمایی می‌شوند. فایده این کار این است که یکپارچگی داده حفظ می‌شود، هزینه نگهداری دفاتر پایین می‌آید و به علاوه داده‌ها قابل رهگیری هستند. زنجیره‌های بلوکی خصوصی با سازوکار اجماع متفاوتی برای اثبات انجام کار ساخته شده‌اند. در بسیاری از زنجیره‌های بلوکی اشتراک گذاری داده به شکل محدودتری انجام می‌شود تا سرعت پردازش بالا رود و در مقیاس‌های بزرگتری قابل استفاده باشد. در این مقاله به اختصار به مقایسه فرآیند اجماع در زنجیره‌های بلوکی بیت‌کوین، هایپرلجرفبریک، کوردا و استلار خواهیم پرداخت.

واژگان کلیدی: اجماع ، رمزارزها، زنجیره‌بلوکی ، بیت‌کوین، هایپرلجرفبریک، کوردا، استلار

چکیده (انگلیسی)

Shortly after Satoshi Nakamoto introduced blockchain thru inventing bitcoin people saw a potential in the concept of blockchain for general purposes. This initiated the invention of private blockchains. The core of all these blockchains is a process named consensus. In short, consensus is the mechanism for verifying blocks. Thru consensus, data integrity is protected, cost of saving records will decrease and records are traceable. Different blockchains have different consensus mechanisms. Some of them limit data sharing in expense for speeding up data processing in order to make them more scalable. In this paper, we briefly compare consensus algorithms used in bitcoin, Hyperledger-Fabric, Corda and Stellar.

مقدمه

ساختارهای مالی در حال حاضر ملغمه‌ای از سامانه‌های بسته هستند. هزینه تراکنشها بسیار بالا است [1] و سرعت انتقال نقدینگی بین مرزهای سیاسی و جغرافیایی کند است[2]. این مساله باعث ایجاد محدودیت‌هایی در خدمات مالی شده‌است و مشتریان فراوانی وجود دارند که خدمتی که بایسته آنهاست را دریافت نمی‌کنند [3]. برای حل این مشکلات نیازمند ساختار مالی هستیم که اجازه رشد و نوآوری ارگانیک (از نوعی که مثلا در رشد اینترنت دیده‌ایم) را بدهد. ولی در عین حال یکپارچگی تراکنشهای مالی را حفظ کند. به طور تاریخی حفظ یکپارچگی موانع فراوانی در سرراه ما می‌گذارد. ما به موسسات مالی اعتماد داریم و سعی می‌کنیم آنها را قانونمند کنیم. ولی این مساله به‌وضوح در تعارض با هدف ما یعنی رشد ارگانیک است. لازمه رشد کردن، وجود مشارکت‌کنندگان مبدع است که به امکانات محاسباتی و مالی متوسطی دسترسی دارند. ما به یک شبکه مالی جهانی نیاز داریم که به روی همه باز باشد تا سازمانهای نوظهور بتوانند به آن بپیوندند و دسترسی مالی برای جوامع مستضعف فراهم آورند. چالش بوجودآوردن چنین شبکه‌ای تضمین ثبت درست تراکنش‌هاست. چاره پیشنهادی یک سامانه غیر متمرکز است که در آن مشارکت‌کنندگان با کمک یکدیگر با توافق‌کردن روی اعتبار تراکنشهای همدیگر یکپارچگی آنها را تضمین می‌کنند. این توافقات برپایه سازوکاری به نام اجماع استوار است.

زنجیره‌بلوکی یک دفتر حساب گسترده برای ضبط تراکنشهاست که با تعداد زیادی گره بدون مرکزیت توسط یک پروتکل رمزنگاری گسترده مدیریت می‌شود. همه گرهها اطلاعاتی که قرار است به زنجیره‌بلوک ضمیمه شود را راست‌آزمایی می‌کنند. در واقع زنجیره‌بلوکها یا دفاترحساب گسترده سامانه‌هایی هستند که خدمات قابل اعتمادی را به گروهی از گره‌ها ارائه می‌دهند که به یکدیگر کاملا اعتماد ندارند. اگرچه زنجیره‌های بلوکی شامل رمزارزها نیز می‌شوند ولی زنجیره بلوکی بدون توکن یا نقدینگی نیز می‌تواند قابل تصور باشد. به طور کلی زنجیره بلوکی همانند یک شخص ثالث قابل اعتماد عمل می‌کند که می‌تواند یک حالت سیستم را ثبت کند، مبادلات را مدیریت نماید و یا یک موتور محاسبات امن باشد. بسیاری از زنجیره‌های بلوکی کارهای اختیاری همچون قراردادهای هوشمند را اجرا کنند که به یک زبان برنامه نویسی عمومی نوشته شده‌است. در یک زنجیره بلوک عمومی (بی مجوز) همچون بیت‌کوین یا اتریوم، هرکسی می‌تواند یک کاربر باشد یا به عنوان یک گره در نظر گرفته‌شود، و از تراکنش مدنظر خود را (در صورت پرداخت کارمزد تراکنش) در دفاتر حساب وارد نماید. یک زنجیره‌بلوکی با مجوز (مثلا زنجیره‌بلوکهای کنسرسیومی) ولی توسط کاربران تعیین شده‌ای اداره می‌شود. در زنجیره‌بلوکهای با مجوز اعضای یک کنسرسیوم یا سهامداران یک تجارت، ابزارهایی برای تشخیص گرههایی که مجاز به تغییر حالت فعلی سیستم هستند می‌باشند.

یک زنجیره‌بلوکی خصوصی نوعی از زنجیره‌بلوکی با مجوز است که توسط یک عضو خاص اداره می‌شود. زنجیره‌بلوکهای با مجوز به بسیاری از مشکلات شاخه محاسبات گسترده می‌پردازند. به عنوان مثال مساله سامانه‌های بیزانسی مقاوم به خطا یکی از این مسائل هستند. این زنجیره‌بلوکها می‌توانند از بسیاری از روشهایی که برای رسیدن به اجماع مانند تکرار حالت، پخش عمومی تراکنش‌ها و امثالهم بهره ببرند. این روشها مخصوصا در محیطهایی که گرهها به طور نهادینه غیر همزمان هستند، ارتباط شبکه غیرمطمئن است و گرهها ممکن است از کار بیفتند مفید می‌تواند باشد. گستره تکنولوژی بلاک‌چین پژوهشهای جدیدی را در پروتکلهای اجماع گسترده ایجاد کرده است.

ادبیات موضوع

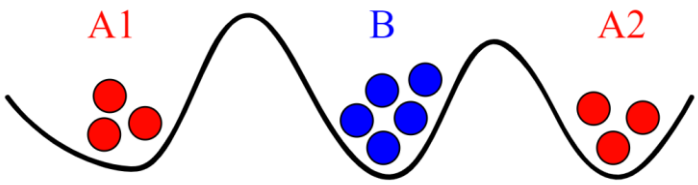
مفاهیم پایه

تاب‌آوری نسبت به خطا (Fault Tolerance)

تاب‌آوری نسبت به خطا خاصیتی است که موجب می‌شود یک سامانه بتواند با وجود خراب شدن یک یا چند تا از اجزایش کارش را ادامه دهد. یکی از راههای ایجاد تاب آوری نسبت به خرابی ایجاد افزونگی در سیستم است. به این ترتیب که برای انجام یک کار چند عنصر مختلف در سیستم نهادینه می‌شوند که هرکدام به تنهایی قابلیت انجام کار را دارند. این اجزا به صورت پشتیبان برای یکدیگر عمل می‌کنند. مثال این مساله قراردادن دو منبع تغذیه برای کامپیوتر یا وجود چند چرخ اضافه در کامیونهای هجده چرخ می‌باشد. در هر دو این مثالها در صورت خرابی یکی از اجزا بدون آنکه نیاز به تعویض عنصر خراب شده یا خاموش کردن دستگاه باشد، دستگاه مربوطه می‌تواند به کارش ادامه دهد.

تاب‌آوری بیزانسی نسبت به خطا (Byzantine fault tolerance)

یک خطای بیزانسی، خطایی است که در نظر شاهدان مختلف علائم مختلفی دارد[4]. یک خرابی بیزانسی به از دست‌رفتن سرویسی گفته می‌شود که ناشی از یک خطای بیزانسی است و در نتیجه نیاز به اجماع دارد [5]. تاب‌آوری بیزانسی به وابستگی یک سامانه کامپیوتری (خصوصا سامانه‌های غیر متمرکز) نسبت به خطاهایی گفته می‌شود که معلوم نیست آیا خطا در آنها رخ داده یا خیر. در یک خطای بیزانسی یک عنصر از سامانه همچون سرور به طور ناپیوسته‌ای هم خراب به نظر می‌آید و هم خوب.



تصویر۱ – شمای مساله دو ژنرال

برای دیگر اجزای سیستم دشوار است اعلام کنند که یک عنصر خراب شده یا خیر و آن را کنار بگذارند چرا که قبل از آن نیاز به اجماع بین اجزاست که کدام عناصر را خراب شده بینگارند. عنوان تاب‌آوری بیزانسی از روی مساله ژنرالهای بیزانسی گرفته شده است.

مساله دو ژنرال : فرض کنید دو ارتش مترصد حمله به یک شهر باشند. به دلیل کمبود نیرو، لازم است حمله به طور همزمان توسط این دو ارتش (A1 و A2) صورت گیرد. مشکل در این است که ما بین این دو ارتش یک ارتش متخاصم قرار دارد (B). اگر قاصدی از ارتش A1 به سمت ارتش A2 به منظور تعیین زمان حمله ارسال شود ممکن است توسط ارتش متخاصم B دستگیر شود. حتی اگرهم جان سالم به در ببرد باز لازم است به مبدا خود بازگردد و خبر موافقت ارتش دوم را به ارتش اول برساند. به دیگر سخن هر دو ارتش باید مطمئن باشند که زمان حمله نهایی شده است تا هیچ‌کدام تکی حمله نکند. مشکل دراین است که قاصد دوم نمی‌تواند اطمینان حاصل کند قاصدی که از سمت او به ارتش اول برمی‌گردد تا خبر توافق زمان حمله را برساند سالم به ارتش اول رسیده‌است یا خیر. در واقع برای فهمیدن اینکه یک قاصد سالم به مقصد رسیده، یک

قاصد دیگر نیاز است وبه این ترتیب بینهایت قاصد نیاز است تا مطلوب حاصل شود. یعنی این مساله جواب ندارد.

اعتماد در یک پروتکل زنجیره‌بلوکی

به طور خلاصه یک زنجیره‌بلوکی یا یک دفترحساب گسترده یک پروتکل غیرمتمرکز است. ولی ایجاد اعتماد و برقرارکردن امنیت در زنجیره بلوکی بدون چالش نخواهد بود. در واقع در این بخش نشان می‌دهیم که ایجاد فرآیند اجماع مشابه ساختن سامانه‌های مبتنی بر رمزنگاری است و نیاز به ابزارهای این رشته خواهد داشت. در حوزه پروتکل‌های زنجیره‌بلوکی می‌توان از تاریخچه رمزنگاری بهره فراوان برد. اصل کرشهوف بیان می‌دارد که یک سامانه رمزنگاری باید حتی در صورت دانستن همه ساز و کار آن امن باشد. فقط کلید است که مخفی می‌ماند. معنی این حرف این است که اگر امنیت سامانه‌ای که بخشهایی از آن باید مخفی بماند بالکل زیر سوال است.

در سالهای اخیر تعداد بی‌شماری ویژگی جدید در سامانه‌های با دفتر گسترده و زنجیره‌بلوک‌های نو پیشنهاد شده‌اند که عمدتا از فینتک‌ها سربرآورده‌اند. اکثر این روشها هیچ تعریف رسمی از فرضیات امنیت خود ندارند. به علاوه هیچ اجماع مورد توافقی در صنعت در مورد فرضیات واقع‌گرایانه برای کاربرد منظورشده آنها نیز وجود ندارد. به علاوه هیچ استانداردی برای راست‌آزمایی این پروتکل‌ها وجود ندارد. ادعاهای زیادی توسط کسانی که خود را خبره می‌خوانند یا استارت‌آپ‌ها، شرکت‌ها و مراکز پژوهشی در زمینه زنجیره‌بلوکی مطرح می‌شود. این مساله اگرچه هیجان‌انگیز است ولی باعث ایجاد سردرگمی در نظرعموم نسبت به زنجیره بلوکی خواهد شد. یک توافق عمومی در مورد فرضیات اعتماد، مدل‌های امنیت و روش‌های استدلال رسمی و اهداف یک پروتکل نیاز است. برنامه‌نویسان، سرمایه‌گذاران و استفاده‌کنندگان در صنعت باید برای ایجاد سامانه‌های قابل اعتماد به اصول و روشهای رمزنگاری و امنیت اتکا کنند. به دیگرسخن مباحثه آزاد، بازبینی‌های خبره و استاندارد جایگزین جو هیجانی شود.

زنجیره‌بلوکی و اجماع

یک زنجیره بلوکی یک پایگاه داده است که یک فهرست فزاینده از داده‌ها را در خود نگه‌می‌دارد. به علاوه این فهرست توسط واحدهایی کنترل می‌شود که نمی‌توانند به یکدیگر اعتماد کنند. رکوردها به صورت بسته‌ای یا بلوکی توسط پروتکل نامتمرکزی که بوسیله گرهها که موتور محرکه زنجیره بلوکی هستند به زنجیره‌بلوکی افزوده می‌شوند. هر بلوک شامل هش بلوک قبلی است که با این کار نمایش امن کل زنجیره را به نوعی در هر بلوک نهادینه می‌کند. ابزارهای حفظ یکپارچگی دیگری نیز اغلب در محیطهای بیزانسی یا کژرفتار استفاده می‌شوند. بعضی از این ابزارها شامل اثبات انجام کار بیت‌کوین (اینکه هش یک بلوک حتما چند صفر داشته‌باشد) و یا وجود چند امضا (آستانه امضا) برروی یک بلوک در زنجیره‌بلوک‌های بامجوزی همچون ریپل است. گرهها در شبکه بایکدیگر ارتباط برقرار می‌کنند و به طور همکارانه زنجیره را می‌سازند بدون آنکه نیاز به یک ارگان مرکزی داشته‌باشند.

باید توجه داشت که گرهها ممکن است از کار بیفتند، کژرفتاری کنند و برخلاف هدف عمومی عمل نمایند یا اینکه ارتباطات شبکه قطع شود. برای تحویل یک سرویس مداوم، گرهها باید یک پروتکل اجماع مقاوم به خطا را اجرا نمایند که تضمین کند همه آنها در مورد ترتیبی که رکوردها به زنجیره بلوکی افزوده می‌شوند توافق دارند.

از آنجایی که زنجیره بلوکی به صورت یک سامانه مورد اعتماد عمل می‌کند، باید قابل اتکا، تاب آور و امن باشد و ویژگی‌هایی همچون در دسترس بودن، اتکاپذیری، امنیت، محرمانگی، یکپارچگی و خیلی دیگر از خواص را داشته باشند. [6]. یک زنجیره بلوکی این مساله را با ساختن کپی‌های مشابه از داده و انجام عملیات روی تعداد زیادی گره تضمین می‌کند. همه گرهها می‌توانند اطلاعاتی که قرار است به زنجیره‌بلوک اضافه‌شود را اعتبارسنجی کنند. این ویژگی روحیه اعتمادپذیری را در گرهها تحریک می‌کند به گونه‌ای که زنجیره‌بلوک در مجموع درست عمل کند.

برای ارزیابی پروتکل زنجیره‌بلوک لازم است که فرضیات اعتماد یا مدل امنیت به طور روشن بیان شود. این فرضیات باید شامل همه عناصر سیستم از جمله شبکه، وجود ساعتهای سنکرون‌شدن، و رفتارها وکژرفتاری‌هایی که از گرهها انتظار می‌رود باشد. به عنوان مثال فرض اعتماد سیستمی با n گره مستقل می‌گوید که حداکثر تعداد گرههای از کار افتاده در شبکه (f) باید کمتر از k/n باشد تا سیستم درست عمل کند. به عبارت دیگر باید n-f گره درست در شبکه وجود داشته باشد.

کپی‌کردن ماشین-حالت. تحقیق رسمی در مورد توسعه الگوریتم‌هایی که از مشابه‌سازی برای تاب‌آوری سرورها استفاده می‌کردند به اثر لمپورت و همکاران [7,8] باز می‌گردد که در آن نویسندگاه توافق بیزانسی را معرفی کردند. همانطور که توسط اشنایدر [9] بیان‌شده‌است، عمل رسیدن به اجماع و نگهداشتن اجماع در میان گرههای غیر متمرکز، با دو عنصر قابل بیان است: ۱. یک ماشین حالت غیرتصادفی که منطق سرویسی که باید مشابه‌سازی شود را توضیح می‌دهد. ۲. یک پروتکل اجماع که تقاضاهای رسیده از گرهها را ترتیب اثر می‌دهد به گونه‌ای که هر گره یک رشته یکسان از تقاضاها را درون خود اجرا کند. در ادبیات موضوع، اجماع به طور سنتی به معنای به توافق رسیدن در مورد یک تقاضا است، درحالی که ارسال عمومی اتمیک [10] توافقی را درمورد یک رشته از تقاضاها تامین می‌کند(این مساله برای کپی‌کردن ماشین ـ حالت رخ می‌دهد). ولی از آنجاییکه ارتباط نزدیکی بین این‌دو وجود دارد (چرا که رشته‌ای از اجماع‌ها یک ارسال عمومی اتمیک را بوجود می‌آورد)، کلمه اجماع اغلب بیشتر برای ارسال اتمیک استفاده می‌شود مخصوصا در ادبیات زنجیره بلوک. ما هم در این مقاله از این نام‌گذاری استفاده می‌کنیم. به علاوه تراکنش و درخواست در این مقاله هر دو به معنی پیغامی است که در قالب ارسال عمومی اتمیک باید تحویل داده‌شود.

مدلهای غیرهمزمان و مدلهای نهایتا همزمان: در این مقاله ما پیشفرضی به نام ((درنهایت همزمان)) در نظر می‌گیریم که توسط دورک و همکاران معرفی شده‌است [11]. این فرض یک شبکه غیرهمزمان را مدل می‌کند که ممکن است رساندن پیغامها را به تاخیر بیندازد ولی درنهایت همه پیغامها را در یک بازه ثابت (ولی نامعین) به مقصد می‌رساند.

اجماع در زنجیره‌بلوک: اگرچه مقاله بیت‌کوین ساتوشی ناکاموتو [12] پارادایم تکرار ماشین-حالت [13] را صراحتا بیان نمی‌کند، ولی بیت‌کوین مفهوم اجماع برروی یک دفترحساب مشترک را براساس رای‌گیری میان گرهها پایه‌گذاری می‌کند: ((گرهها با قدت پردازنده مرکزی خود رای می‌دهند و پذیرش بلوک‌های معتبر را با توسعه‌دادن به این بلوکها و رد کردن بلوکهای غیرمعتبر را با استنکاف از کارکردن روی آنها بیان می‌دارند. هر قانون و مشوق مورد نیاز تحت این سازوکار اجماع قابل پیاده‌سازی است)) [12]. بعد از مقاله گری و همکاران [14]، معادل بودن کاری که پروتکل ناکاموتو انجام می‌دهد و مساله اجماع در محاسبات غیرمتمرکز به طور رسمی نشان‌داده‌شد. این نتیجه همزمان شد با این بینش که در فینتک‌ها پیدا شد، که بسترزنجیره‌بلوک یک سازوکار اجماع کلی را می‌تواند استفاده کند و بعد آن را با هر پروتکلی که سازگار با مدل اعتماد آن است پیاده‌سازی نماید [15]. در فهم امروزی، بستر زنجیره‌بلوک می‌تواند یک سازوکار دلخواه اجماع برگزیند و در عین حال اکثر وجوه خود همچون گسترده‌بودن، غیرقابل بازگشت‌بودن و شفاف بودن را نگهدارد. اجماع‌های موجود و سازوکارهای تکرار به همین دلیل مورد اقبال ویژه‌ای قرارگرفته‌اند چرا که می‌توان آنها را در زنجیره بلوک به‌کار برد.

پروتکل‌های بسیاری که مربوط به زنجیره بلوکی می‌شوند در بخشهای بعدی مرور خواهند شد.

اجماع مقاوم نسبت به خرابی

همچنان که قبلا گفته‌شد، نوعی از اجماع که به زنجیره‌بلوک مرتبط می‌شود با نام پخش اتمیک از آن یاد می‌شود. یک پخش اتمیک با دو رخداد غیر همزمان که ممکن است چند بار تکرار شوند مشخص می‌شود; پخش و تحویل. هر گره ممکن است یک پیغام (یا یک تراکنش) مانند ام را با اجرای پخش(ام) پخش نماید و پروتکل ام را بوسیله رخداد تحویل(ام) به اپلیکیشن محلی گره به عنوان خروجی تحویل می‌دهد. پخش اتمیک تضمین می‌کند که هر گره صحیح ترتیب یکسانی از پیغامها را بوسیله رخدادهای تحویل به عنوان خروجی تحویل دهد. به طور دقیقتر خواص زیر تضمین می‌شود [16,17]:

اعتبار: اگر یک گره درست مانند پی پیغامی مانند ام را پخش کند آنگاه پی در نهایت این پیغام به مقصد تحویل داده می‌شود.

توافق: اگر پیغام ام توسط یک گره صحیح تحویل مقصد داده شود، آنگاه پیغام ام توسط هر گره صحیح دیگری نیز تحویل داده خواهد شد.

یکپارچگی:هیچ گره صحیحی بیشتر از یک بار پیغام را تحویل نمی‌دهد. به علاوه اگر یک گره صحیح پیغام ام را تحویل دهد و فرستنده این پیغام (مثلا گره پی) صحیح باشد، آنگاه ام توسط پی قبلا پخش عمومی شده بوده است.

ترتیب کلی:برای پیغامهای امیک و امدو، فرض کنید پی و کیو دو گره صحیح باشند که پیغامهای امیک و امدو را تحویل می‌دهند. آنگاه پی امیک را زودتر از امدو تحویل می‌دهد اگر و تنها اگر کیو امیک را قبل از امدو تحویل دهد.

مهمترین و برجسته‌ترین راه برای پیاده‌سازی پخش اتمیک (یا همان اجماع) در سیستمهای غیرمتمرکز که مستعد خرابی‌های کمتر از نصف تعداد گرهها هستند خانواده‌ای از پروتکل‌ها هستند که امروزه آنها را پاکسوس [18,19] و وی‌اس‌آر [20,21] می‌نامیم. این پروتکل‌ها در دهها سیستم مهم ابری پیاده‌سازی شده‌اند [22].

پروتکل‌های زاب که در نگهبان باغ‌وحش (zoo keeper) به‌کار می‌رود یک عضو برجسته از این خانواده است که اصالتا از شرکت یاهو بیرون آمده است. این پروتکل به صورت متن‌باز موجود است [23, 24, 25] (https://zookeeper.apache.org) و در بسیاری از سیستم‌ها استفاده می‌شود. یک عضو جدید این خانواده رافت است [26] که با هدف ساده‌تر کردن فهم و پیاده‌سازی پاکسوس درست شده‌است و در دهها ابزار متن‌باز استفاده می‌شود (مثلا نگاه کنید به https://github.com/coreos/etcd)

اجماع بیزانسی

اخیرا پروتکل‌های اجماعی که بتوانند گرههای بیزانسی را تحمل کنند توسعه یافته‌اند که در آنها گرهها ممکن است توسط یک مهاجم گمراه شوند و در مقابل هدف مشترک که همان رسیدن به توافق است بدخیمانه رفتار کنند. در مدل نهایتا همزمان که در این مقاله در نظر گرفته‌شده است برجسته‌ترین پروتکل همانا پی‌بی‌اف‌تی است[27]. این پروتکل به نوعی گسترش‌یافته خانواده پاکسوس یا وی‌اس‌آر است [28, 29, 30]. در سیستمی با n گره، پی‌بی‌اف‌تی، حداکثر $f < n/3$ گره بیزانسی را تحمل می‌کند که بهینه است. تحقیقات بسیاری جنبه‌هایی از آن را تحلیل‌کرده و بهبوددادند و در پروتوتایپها آن را مقاوم

نموده‌اند.

تعداد سامانه‌های واقعی که پی‌بی‌اف‌تی یا یکی از انشعابات آن را پیاده‌سازی نموده‌اند بسیار کمتر از آنهایی است که پاکسوس یا وی‌اس‌آر را پیاده‌سازی نموده‌اند. در واقع تا پیش از سال ۲۰۱۵ که زنجیره‌بلوک‌های بامجوز زیادشدند [31]، تنها پروژه مبتنی بر پی‌بی‌اف‌تی اسمارت بود (https://github.com/bft-smart/library). بسانی و همکاران [32,33] از دانشگاه لیسبون، در حدود سال ۲۰۱۰ پروژه اسمارت را استارت زدند. دیدگاه غالب این است که اسمارت پیشرفته‌ترین و آزموده‌شده‌ترین پیاده‌سازی پروتکل اجماع بی‌اف‌تی درحال‌حاضر است. آزمایشها نشان‌داده که می‌تواند به نرخ ۸۰هزار تراکنش در ثانیه برروی شبکه لن برسد [33] و سربار تاخیر آن در وان کم باشد [34]

همچون پاکسوس و وی‌اس‌آر، اجماع بیزانسی پیاده‌سازی‌شده توسط پی‌بی‌اف‌تی و اسمارت شبکه‌ای نهایتان همزمان می‌طلبد. بدون این فرض، فقط پروتکل‌های تصادفی برای اجماع بیزانسی قابل تصور هستند. مثل انواعی که مبتنی بر رمزنگاری غیرمتمرکز هستند [35] همچون سیناترا [36] یا هانی‌بجر [37]

روش تحقیق

مشهورترین سازوکار اجماع گسترده همان اثبات انجام کار است که توسط بیت‌کوین [12] معرفی شده‌است. بیت‌کوین یک روش دومنظوره برای اجماع به‌کار می‌گیرد. اول اینکه یک انگیزه مادی برای کاربران منطقی فراهم می‌آورد که درست رفتار کنند. دوم اینکه تراکنشها را بوسیله الگوریتم اثبات انجام کار (Proof of work) حل‌وفصل می‌کند. الگوریتم اثبات‌انجام کار به گونه‌ای طراحی شده که از سیستم در مقابل کاربران کژرفتاری که البته اکثریت توان محاسباتی را ندارند محافظت می‌کند. بیت‌کوین به طور خارق‌العاده‌ای گرایش به اجماع گسترده را به تصویرکشیده‌است[3]. با این وجود اثبات انجام کار محدودیت‌هایی دارد. اول اینکه منابع را به هدر می‌دهد. طبق یک تخمین که در سال ۲۰۱۴ منتشر شد، بیت‌کوین احتمالا به اندازه کل کشور ایرلند توان الکتریکی مصرف می‌کند[38]. دوم اینکه تراکنش‌های امن در بیت‌کوین ممکن است چندین دقیقه برای حل‌وفصل شدن تاخیر داشته‌باشند[39]. و نهایتا اینکه برخلاف پروتکل‌های سنتی رمزنگاری، اثبات انجام کار امنیت مجانبی را تضمین نمی‌کند. مثلا اگر حمله‌کننده‌هایی داشته‌باشیم که غیرعقلایی فکر کنند یا کسانی باشند که ذاتا دنبال خرابکاری هستند یک برتری نسبی در توان محاسباتی کافی‌است تا امنیت سامانه را با تغییر رکوردهای پیشین بهم بزنند; حادثه‌ای که از آن به حمله ۵۱ ٪ یاد می‌شود. یک اتفاق بدتر البته این است که کاربری که کمتر از ۵۰ درصد قدرت محاسباتی را در اختیار دارد می‌تواند سیستم را به بازی بگیرد تا پاداش غیر متناسب برای کسانی که به او می‌پیوندند بدهد [40] و به تدریج از این طریق قدرت محاسباتی اکثریت را بدست آورد. بیت‌کوین به عنوان رمزارزی با بیشترین پشتوانه محاسباتی به نوعی از یک مصونیت نسبت به حمله ۵۱ درصد برخوردار است. این حمله از سامانه‌های رمزارز کوچکتر ولی قربانی گرفته‌است [41,42] که نشان از مشکل موجود در همه سامانه‌های مبتنی بر اثبات انجام کار که بر بستر زنجیره‌بلوک بیت‌کوین نیستند می‌باشد.

سازوکار	کنترل‌غیرمتمرکز	تاخیر کم	امنیت انعطاف‌پذیر	امنیت مجانبی
اثبات انجام کار	√			
اثبات سهام	√	شاید		شاید
توافق بیزانسی		√	√	√
Tendermint	√	√		√
استلار	√	√	√	√

یک راه‌حل جایگزین برای اثبات انجام کار، روش "اثبات سهام" (proof of stake) است [43]. در این روش اجماع به طرفینی وابسته است که گرویی گذاشته‌باشند. همانند اثبات انجام کار، پاداشها طوری طراحی شده‌اند که شرکت‌کننده عاقل از پروتکل پیروی نماید. به علاوه برخی طراحی‌ها [44, 45] کژرفتاری را تنبیه می‌کنند. گواه سهام، راه را برای حمله‌ای با نام "چیزی برای از دست دادن نداشتن" هموار می‌کند. در این حمله کاربرانی که قبلا گرویی گذاشته‌اند و آن را خرج کرده‌اند می‌توانند به اصطلاح، تاریخ را به زمانی که هنوز پول داشته‌اند برگردانند. برای مقابله با چنین حمله‌ای، سامانه‌ها به طور کارآمد اثبات انجام کار را با گواه برسهام ترکیب می‌کنند. به این صورت که میزان کار لازم را نسبت به گرویی لازم کاهش می‌دهند یا بازگرداندن گرویی را تا زمانی که فرایند اجماع یک نقطه بازرسی غیرقابل بازگشت ایجاد کند به تعویق می‌اندازند.

یک راه دیگر برای اجماع توافق بیزانسی است [7,8]. بهترین نوع این اجماع پی بی اف تی است [27]. توافق بیزانسی اجماعی را تضمین می‌کند که در مقابل رفتار (هرچند غیر معقول) درصدی از کاربران مصون است. این رهیافت دو خاصیت جذاب دارد. اول اینکه اجماع سریع و کاراست. دوم اینکه اعتماد کاملا از مالکیت منابع مجزاست. این مساله کمک می‌کند که مثلا یک ارگان غیرانتفاعی کوچک بتواند ارگانهای قدرتمندی همچون بانکها را صادق نگه‌دارد. نکته پیچیده این روش اینجاست که همه طرفین درگیر باید روی فهرست مشخصی از مشارکت‌کنندگان توافق کنند. به علاوه حمله‌کنندگان باید از اینکه بتوانند چندبار عضو شوند یا از آستانه شکست سیستم گذر کنند منع گردند. به فرآیند آخر حمله سیبیل گفته می‌شود [46]. بی‌اف‌تی-کاپ [47] پذیرای مشارکت‌کنندگان ناشناس است ولی با این‌حال سازوکار متمرکزی دارد که نسبت به حمله سیبیل مصون است.

درحالت کلی، عضویت در توافق بیزانسی توسط یک نهاد مرکزی انجام می‌شود یا با یک مذاکره بسته. یک رهیافت که توسط ریپل (Ripple) پیاده‌سازی شده این است که یک عضویت اولیه تصویب گردد که مشارکت‌کنندگان بتوانند برای خودشان ویرایش کنند با این امید که تغییراتی که افراد ایجاد می‌کنند یا بی‌نتیجه است یا توسط اقلیتی از اعضا انجام بشود. متاسفانه به دلیل آنکه فهرستهای غیرهمگرا تامین امنیت را نقض می‌کنند [48] کاربران در عمل متمایل به ویرایش فهرست نیستند و مقدار زیادی توان برروی نگهداری فهرست اولیه متمرکز می‌شود. رهیافت دیگر که توسط رمزارز تندرمینت پی‌گرفته شده‌است [49]، این است که پایه عضویت را گواه سهام بگذاریم. ولی با این کار بازهم امنیت را به مالکیت منابع گره می‌زنیم.

سامانه توافق بیزانسی آزاد

همانند توافق‌های بیزانسی معمولی، توافق بیزانسی آزاد نیز معضل حالتهای تکراری را در یک تراکنش یا در یک درخت مرجع صدور گواهی پوشش می‌دهد. با توافق برروی این مساله که چه تغییراتی را اعمال کنیم، گرهها از حالتهای متناقض و غیرقابل حل و فصل جلوگیری می‌کنند. هر بروزرسانی توسط یک فضای خالی که از طریق آن وابستگی‌های بروزرسانی‌های بینابینی مشخص می‌شود تعیین می‌گردد. به عنوان مثال فضای خالی می‌توان مکانهای پشت‌سرهم شماره‌گذاری‌شده که در یک فهرست متوالی آورده شده‌است. سامانه توافق بیزانسی آزاد از پروتکل اجماعی استفاده می‌کند که تضمین می‌کند گرهها برروی محتویات یک فضای خالی توافق دارند. هر گره وی می‌تواند به طور امن بروزرسانی اکس را در فضای خالی آی اجرا کند وقتی که بروزرسانی را روی همه گرههایی که آی به آنها وابسته‌است اجرا کرده باشد. به علاوه وی بر این باور است که همه کارکردهای گرهها نهایتا برروی بروزرسانی اکس در فضای خالی آین توافق خواهند کرد. در این لحظه به اصطلاح می‌گوییم گره وی بروزرسانی اکس را برای فضای خالی آی خارجی کرده است. دنیای خارج نسبت به مقادیر خارجی‌شده ممکن است به شکل غیر قابل بازگشتی عکس‌العمل نشان دهد به گونه‌ای که یک گره نتواند بعدا نظرش را تغییر بدهد. چالشی برای این سامانه این است که مشارکت‌کنندگان کژرفتار می‌توانند به دفعات زیادی به هم بپیوندند و از نظرتعداد گرههای صادق را پشت‌سر بگذارند. در نتیجه حدنصابهای سنتی مبتنی بر اکثریت در این سیستم کار نخواهند کرد. درعوض این سامانه حدنصابها را به صورت غیر متمرکز تعیین می‌کند به گونه‌ای که هر گره، آنچه که ما فضای‌خالی حدنصاب را بر می‌گزینند.

یافته‌ها و نتایج

تانگاروا (Tangaroa)

پیش از آنکه پروتکل‌های موجود در زنجیره‌بلوکهای عملی را مورد بررسی قرار دهیم، برخی خطاهای معمول را توضیح می‌دهیم. پروتکل تانگاروا [50] یک شاخه از رفت[51] است که برای پروتکلهای بیزانسی مقاوم به خطا طراحی شده است. این پروتکل در خلال یک پروژه درسی یکی از کلاسهای دانشگاه در زمینه سامانه‌های غیر متمرکز توسعه یافت. اگرچه این پروتکل هیچگاه مورد داوری همتا قرارنگرفت ولی به عنوان یک پروتکل اجماع بیزانسی مقاوم به خطا در زنجیره‌بلوکهای بدون مجوز بسیار مشهور شد.

مشکل زنده‌ماندن:اگر شبکه همزمان باشد، آنگاه لازم است پروتکل زنده بماند و به طور پیوسته پیغام بگذارد. ولی از آنجایی‌که هر گره می‌تواند خودش را به عنوان رهبر نامزد کند، ممکن است یک گره بدخیم در این راه پیشرو شود و بعد از انتخاب به عنوان رهبر از انجام هرکاری دریغ ورزد. یعنی زنده‌بودن شبکه زیرسوال می‌رود.

مشکل ایمنی:رهبر گروه باید اطمینان حاصل نماید که همه گرههای درست، پیغامهای یکسان را با ترتیب یکسان تحویل می‌دهند. این کار پیچیده است زیرا رهبر ممکن است موفق به گرفتن موافقت از باقی گرهها نشود یا حتی از روی عمد چنین کند .

چه خطاهایی توسط پروتکل تحمل می‌شود؟	خرابی گره خاص	معمولی $t < n/2$ گره خراب شوند	گره خاص بدخیم شود	معمولی $f < n/3$ گره بدخیم شود
Hyperledger Fabric/Kafka	.	✓	.	–
Hyperledger Fabric/PBFT	.	✓	.	✓
Tendermint	.	✓	.	✓
Symbiont/BFT-SMaRt	.	✓	.	✓
R3 Corda/Raft	.	✓	.	–
R3 Corda/BFT-SMaRt	.	✓	.	✓
Iroha/Sumeragi (BChain)	.	✓	.	✓
Kadena/ScalableBFT	?	?	?	?
Chain/Federated Consensus	–	(✓)	–	–
Quorum/QuorumChain	–	(✓)	–	–
Quorum/Raft	.	✓	.	–
MultiChain +	.	✓	.	–
Sawtooth Lake/PoET	⊕	✓	⊕	–
Ripple	⊗	(✓)	⊗	–
Stellar/SCP	?	?	?	?
IOTA Tangle	?	?	?	?

خلاصه خواص تاب‌آوری پروتکلهای اجماع. نشان‌گذاری: علامت تیک یعنی پروتکل نسبت به خطا مقاوم است و خط تیره یعنی نیست. نقطه بیان می‌کند که گره ویژه وجود ندارد در این پروتکل. علامت سوال نشانگر خواصی است که به دلیل عدم وجود اطلاعات کافی قابل ارزیابی نیستند. علامت تیک با پرانتز نشان‌دهنده خراب‌شدن دیگر گرهها (غیر از گره ویژه) است. علامت جمع یعنی چندزنجیره تصمیمات غیر نهایی دارد. اگزور یعنی پی او ای تی فرض می‌کند سخت‌افزار مورد اعتماد فقط از یک وندور در دسترس است. ضرب دایره‌دار هم مربوط به عملگرهای ریپل است.

زنجیره‌بلوک‌های بامجوز

	تعداد کل گره‌ها	تعدادگره‌های مجاز برای خراب شدن	تعدادگره‌های مجاز برای بدخیم شدن
ایمنی	n	$t < n/2$	–
زنده‌بودن	n	$t < n/2$	–

تاب‌آوری هایپرلجر فابریک نسخه یک

	تعداد کل گره‌ها	تعدادگره‌های مجاز برای خراب شدن	تعدادگره‌های مجاز برای بدخیم شدن
ایمنی	n	$t < n/2$	$f < n/3$
زنده‌بودن	n	$t < n/2$	$f < n/3$

تاب‌آوری هایپرلجر فابریک نسخه 0.6

	تعداد کل گره‌ها	تعدادگره‌های مجاز برای خراب شدن	تعدادگره‌های مجاز برای بدخیم شدن
ایمنی	n	$t < n/3$	$f < n/3$
زنده‌بودن	n	$t < n/3$	$f < n/3$

تاب‌آوری Tendermint

	تعداد کل گره‌ها	تعدادگره‌های مجاز برای خراب شدن	تعدادگره‌های مجاز برای بدخیم شدن
ایمنی	n	$t < n/3$	$f < n/3$
زنده‌بودن	n	$t < n/3$	$f < n/3$

تاب‌آوری BFT-SMaRt

	تعداد کل گره‌ها	تعدادگره‌های مجاز برای خراب شدن	تعدادگره‌های مجاز برای بدخیم شدن
ایمنی	n	$t < n/2$	-
زنده‌بودن	n	$t < n/2$	-

تاب‌آوری Corda (مبتنی بر Raft)

	تعداد کل گره‌ها	تعدادگره‌های مجاز برای خراب شدن	تعدادگره‌های مجاز برای بدخیم شدن
ایمنی	n	$t < n/3$	$f < n/3$
زنده‌بودن	n	$t < n/3$	$f < n/3$

تاب‌آوری Corda (مبتنی بر BFT-SMaRt)

	تعداد کل گره‌ها	تعدادگره‌های مجاز برای خراب شدن	تعدادگره‌های مجاز برای بدخیم شدن
ایمنی	n	$t < n/3$	$f < n/3$
زنده‌بودن	n	$t < n/3$	$f < n/3$

تاب‌آوری Iroha (BChain)

زنجیره‌بلوک‌های بدون مجوز

هایپرلجر ساتوث لیک (Hyperledger Sawtooth Lake)

پلتفرم هایپرلجر ساتوث یک دفترحساب گسترده برای قراردادهای هوشمند همه‌منظوره است که دارای دو مود بامجوز و بدون مجوز می‌باشد. این پلتفرم پروتکل اجماعی به نام اثبات گذرزمان ارائه می‌دهد که ابتدائا توسط اینتل معرفی شد. این پروتکل اجماع براین پایه بنانهاده شده است که اثبات انجام کار یک زمان انتظار اجباری تصادفی را برای انتخاب گره رهبر تحمیل می‌نماید. به‌طورخاص وقتی پاداش استخراج در بیت‌کوین را کنار بگذاریم، اجماع ناکاموتو به همه گرهها اجازه می‌دهد که در یک تجربه احتمالاتی شرکت کنند که در آن هر گره برای مدتی تصادفی مجبوراست انتظار بکشد.

در روش اثبات گذرزمان، مدت زمان انتظار تصادفی توسط یک ماژول سخت‌افزاری بنام اس‌جی‌اکس (SGX) که در بسیاری از پردازنده‌های اینتل یافت می‌شود تولید می‌گردد. هر گره آنکلیو (enclave) درون اس‌جی‌اکس را برای تولید تاخیر تصادفی صدا می‌زند و متناسب با آن منتظر می‌ماند و بعد خود را به عنوان رهبر گروه اعلام می‌کند و زنجیره بلوکی را ادامه می‌دهد. با فرض آنکه سخت‌افزار قابل دستکاری نیست، می‌توان فرض کرد عملکرد این روش همانند اثبات انجام کار عمل خواهد کرد.

ریپل و استلار (Ripple & Stellar)

ریپل و استلار دو شبکه مبادله جهانی با رمزارزهای نهادینه خود هستند. برخلاف بیت‌کوین، استخراج ارز در آنها وجود ندارد. الگوریتم اجماع در ریپل و فرزند آن الگوریتم اجماع استلار تفاوتی بنیادی با مفروضات امنیت در پروتکل‌های اجماع دارند (یعنی در مورد فرض تعدادگرههای خراب کمتر از ثلث کل گرهها). بدین‌ترتیب که مفروضات امنیتی خود را انعطاف‌پذیر می‌گیرند [52,48]. این یعنی هر گره خودش اعلام می‌کند که به چه گرههای دیگری اعتماد دارد به‌جای آنکه فرض عمومی در مورد اینکه پروتکل چه تبانی‌هایی را تحمل خواهد کرد را بپذیرد. هر گره فهرستی از گرههایی که برای مجاب کردن خود لازم دارد در نظر می‌گیرد (در ریپل به آن فهرست گرههای یکتا و در استلار به آن حدنصاب برش می‌گویند). ریپل و استلار هرکدام یک دفترحساب غیرمتمرکز تحت مدیریت پروتکل نگاه می‌دارند که مبادلات شبکه را ثبت می‌کند.

در ریپل فرآیند توسعه دادن دفترحساب مشترک غیر متمرکز توسط گرههای اعتبارسنجی کننده کنترل می‌شود. این گرهها متناوبا شروع به ایجاد یک سرفصل جدید در دفترحساب می‌کنند (هرچند ثانیه) و به طور گردشی و نوبتی در مورد محتوای آن رای می‌دهند. هر گره سرفصل پیشنهاد شده را در صورتی که به ترتیب نوبتها ۵۰٪ الی ۸۰٪ تغییرات تطبیق داشته‌باشند می‌پذیرد. طبق شهادت مستندات خود ریپل، درست بودن چهارپنجم همه گرههای اعتبارسنجی کننده برای درست کارکردن

کل شبکه لازم است. به‌علاوه، واضح است که حداقل هم‌پوشانی بین مجموعه‌های مجاب‌کننده (یعنی فهرستهای یکتا) از همه زوجهای گرههای اعتبارسنجی کننده لازم است چرا که در غیراینصورت، دفترحساب دودسته‌خواهد شد (Fork). ریپل بیان می‌کند که هم‌پوشانی باید حداقل یک‌پنجم اندازه فهرست حساب باشد [48]. تنها داوری همتای پروتکل ریپل با این نظر مخالف است[53]. درحال حاضر ریپل یک فهرست پیشفرض و توصیه‌شده از گرههای اعتبارسنجی‌کننده فراهم می‌آورد که توسط خود ریپل و برخی اشخاص ثالث عملیاتی می‌شوند. با استفاده از یک فایل پیکربندی پنج گره اعتبارسنج متعلق به ریپل وجود دارند که به یکدیگر اعتماد دارند ولی به هیچ گره دیگری اعتماد ندارند. این طور به نظر می‌آید که این فهرست توسط اکثر گرههای اعتبارسنج در سیستم پذیرفته شده است. در نتیجه اعتماد اصلا آن طور که تبلیغ می‌شود غیرمتمرکز نیست. معمولا فرآیند اجماع برای ایجاد یک سرفصل جدید در دفترحساب کمتر از یک چهارم ثانیه به طور متوسط طول می‌کشد. ریپل نرخ ارسالی حدود ۱۰۰۰ تراکنش در ثانیه ادعا نموده است [54]. در مقایسه با نرخهای ۱۰۰۰۰ تراکنش درثانیه در پلتفورمهای مقاوم نسبت به خطای بیزانسی که صرفا با گرههای اعتبار سنجی بین ۴ الی ۱۰ گره کار می‌کنند [34]، نرخ ریپل خیلی پایین می‌نماید.

استلار: از آنجاییکه استلار از ریپل انشعاب پیدا کرد از ایده‌های مشابهی استفاده می‌کند. به علاوه اینکه از یک پروتکل بانام توافق بیزانسی آزادشده نیز بهره می‌برد. فقط گرههای اعتبارسنی کننده در فرآیند رسیدن به اجماع شرکت می‌کنند.

هر گره اعتبارسنجی کننده مجموعه مجاب‌کننده خودش را اعلام می‌کند (برش حدنصاب) که باید به اندازه کافی با مجموعه‌های مجاب‌کننده دیگرگرهها هم‌پوشانی داشته‌باشد تا از تشکیل انشعاب (دودستگی) جلوگیری شود. هر گره یک رای یا یک تراکنش جدید در دفترحساب را درصورتی می‌پذیرد که آستانه‌ای از گرهها در مجموعه مجاب‌کننده آن را بپذیرند. مثالهایی در مستندات ریپل وجود دارند که نشان می‌دهند هر گروه ممکن است به طور سلسله مراتبی به چند زیرگروه تقسیم شود و هر زیرگروه آستانه خاص خود را خواهد داشت. ولی آستانه بالاترین سطح از زیرگروهها دارای آستانه‌ای برابر ۲/۳ خواهد بود.

آیوتا (IOTA)

آیوتا را با نام رمزارز بدون زنجیره‌بلوک می‌شناسند که درآن یک گراف جهت‌دار بدون‌چرخش جایگزین زنجیره بلوکی شده‌است. تراکنش‌ها در یک شبکه همتا به همتا مانند بیت‌کوین پخش می‌شوند. هر تراکنش تعدادی توکن را از مالکیت یک نفر به مالکیت یک نفر دیگر در می‌آورد و باید به امضای فرستنده برسند. به علاوه تراکنش شامل حل یک معمای اثبات انجام کار می‌باشد که دو یا بیشتر تراکنش را به همراه هش آنها در خود دارد. این عملیات یک گراف جهت‌دار بدون چرخش را تولید می‌کند که هر یال از یک تراکنش تایید شده به سمت تراکنش جدید خواهد بود. وزن این یال متناسب با سختی معمایی است که در اثبات انجام کار مربوط به این ترکنش حل شده است.

یک گره به چند طریق می‌تواند تقلب کند: ۱) با صدور تراکنش نامعتبر (دوبار خرج کردن) ۲) با شامل نمودن تراکنشهای قبلی غیر معتبر ۳) با انتخاب نکردن تصادفی تراکنشها برای تایید شدن. ولی دیگر گرهها به طور شهودی تراکنشهای از نوع ۱) و ۲) را تایید نمی‌کنند (به اصطلاح چنین تراکنشی یتیم خواهد شد). در یک گراف چگال، این طور انتظار می‌رود که اکثر تراکنشهای پیرتر از یک سن خاص توسط اکثریت تراکنشهای جدید تایید اعتبار می‌شوند.

ادعای مستندات آیوتا این است که پایداری آیوتا در حد دیگر زنجیره‌بلوکهای بدون مجوز است. ولی این ادعا توسط ارگان

مستقل دیگری تایید نشده است.

جمع بندی

در این مقاله برخی از پروتکل‌های معروف مبتنی بر زنجیره‌بلوک را به طور خلاصه مورد تحلیل قراردادیم. بحث کردیم که توسعه فرآیندهای اجماع شبیه تولید رمزهای جدید است و توسعه‌دهندگان زنجیره‌های بلوکی باید به تجربه رمزنگاری در این زمینه مراجعه کنند که در آن امنیت سامانه مورد داوری همتا قرار می‌گیرد. در غیر این صورت اعتماد کردن و سپردن مسائل مالی به این تکنولوژی نوین خطرناک خواهد بود. نیاز به بحث‌های آزاد، نظرخواهی‌های خبره، اعتبارسنجی و استانداردسازی در این زمینه می‌باشد. مرور پروتکل‌های اجماع و ویژگی‌های آنها به این مساله کمک می‌کند. وقتی به تعداد کافی از این پروتکل‌ها به طور عمومی قابل استفاده شدند و به طور گسترده مورد استفاده قرار گرفتند مقایسه کارایی آنها براساس تاب‌آوری آنها نسبت به حمله‌های واقعی جالب خواهد بود.

منابع

[1] Claire Provost. 2013. Why do Africans pay the most to send money home? (January 2013). http://www.theguardian.com/global-development/2013/jan/30/africans-pay-most-send-money
[2] Rachel Banning-Lover. 2015. Boatfuls of cash: how do you get money into fragile states? (February 2015). http://www.theguardian.com/global-development-professionals-network/2015/feb/19/boatfuls- of-cash-how-do-you-get-money-into-fragile-states
[3] Cynthia Dwork and Moni Naor. 1992. Pricing via Processing or Combatting Junk Mail. In Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. 139–147.
[4] Driscoll, K.; Hall, B.; Paulitsch, M.; Zumsteg, P.; Sivencrona, H. (2004). "The Real Byzantine Generals": 6.D.4–61-11
[5] Driscoll, Kevin; Hall, Brendan; Sivencrona, Håkan; Zumsteg, Phil (2003). "Byzantine Fault Tolerance, from Theory to Reality". 2788: 235–248.
[6] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 1(1):11–33, 2004.
[7] L. Lamport, R. Shostak, and M. Pease. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3):382–401, July 1982.
[8] M. Pease, R. Shostak, and L. Lamport. Reaching agreement in the presence of faults. Journal of the ACM, 27(2):228–234, Apr. 1980.
[9] F. B. Schneider. Implementing fault-tolerant services using the state machine approach: A tutorial. ACM Computing Surveys, 22(4):299–319, Dec. 1990.
[10] V. Hadzilacos and S. Toueg. Fault-tolerant broadcasts and related problems. In S. J.

Mullender, editor, Distributed Systems (2nd Ed.). ACM Press & Addison-Wesley, New York, 1993. Expanded version appears as Technical Report TR94-1425, Department of Computer Science, Cornell University, Ithaca NY, 1994.
[11] C. Dwork, N. Lynch, and L. Stockmeyer. Consensus in the presence of partial synchrony. Journal of the ACM, 35(2):288–323, 1988.
[12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Whitepaper, 2009. http:// bitcoin.org/bitcoin.pdf.
[13] F. B. Schneider. Implementing fault-tolerant services using the state machine approach: A tutorial. ACM Computing Surveys, 22(4):299–319, Dec. 1990.
[14] J. A. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In Advances in Cryptology: Eurocrypt 2015, volume 9057 of Lecture Notes in Computer Science, pages 281–310. Springer, 2015.
[15] T. Swanson. Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems. Report, available online, Apr. 2015. URL: http://www.ofnumbers.com/ wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
[16] C. Cachin, R. Guerraoui, and L. Rodrigues. Introduction to Reliable and Secure Distributed Pro- gramming (Second Edition). Springer, 2011.
[17] P. Hunt, M. Konar, F. P. Junqueira, and B. Reed. ZooKeeper: Wait-free coordination for internetscale systems. In Proc. USENIX Annual Technical Conference, 2010.
[18] L. Lamport. The part-time parliament. ACM Transactions on Computer Systems, 16(2):133–169, May 1998.
[19] L. Lamport. Paxos made simple. SIGACT News, 32(4):51–58, 2001
[20] B. Lampson. The ABCD's of Paxos. In Proc. 20th ACM Symposium on Principles of Distributed Computing (PODC), 2001.
[21] B. Liskov. From viewstamped replication to Byzantine fault tolerance. In B. Charron-Bost, F. Pedone, and A. Schiper, editors, Replication: Theory and Practice, volume 5959 of Lecture Notes in Computer Science, pages 121–149. Springer, 2010.
[22] T. D. Chandra, R. Griesemer, and J. Redstone. Paxos made live: An engineering perspective. In Proc. 26th ACM Symposium on Principles of Distributed Computing (PODC), pages 398–407, 2007.
[23] P. Hunt, M. Konar, F. P. Junqueira, and B. Reed. ZooKeeper: Wait-free coordination for internetscale systems. In Proc. USENIX Annual Technical Conference, 2010.
[24] F. Junqueira, B. Reed, and M. Serafini. Zab: High-performance broadcast for primary-backup systems. In Proc. 41st International Conference on Dependable Systems and Networks, 2011.
[25] R. van Renesse, N. Schiper, and F. B. Schneider. Vive la diff´erence: Paxos vs. viewstamped replication vs. zab. IEEE Transactions on Dependable and Secure Computing, 12(4):472–484, 2015.
[26] D. Ongaro and J. K. Ousterhout. In search of an understandable consensus algorithm. In Proc. USENIX Annual Technical Conference, pages 305–319, 2014.
[27] M. Castro and B. Liskov. Practical Byzantine fault tolerance and proactive recovery. ACM Trans- actions on Computer Systems, 20(4):398–461, Nov. 2002.
[28] B. Lampson. The ABCD's of Paxos. In Proc. 20th ACM Symposium on Principles of

Distributed Computing (PODC), 2001.
[29] B. Liskov. From viewstamped replication to Byzantine fault tolerance. In B. Charron-Bost, F. Pedone, and A. Schiper, editors, Replication: Theory and Practice, volume 5959 of Lecture Notes in Computer Science, pages 121–149. Springer, 2010
[30] C. Cachin. Yet another visit to Paxos. Research Report RZ 3754, IBM Research, Nov. 2009.
[31] T. Swanson. Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems. Report, available online, Apr. 2015. URL: http://www.ofnumbers.com/ wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.
[32] A. Bessani and J. Sousa. From Byzantine consensus to BFT state machine replication: A latencyoptimal transformation. In Proc. 9th European Dependable Computing Conference, pages 37–48, 2012.
[33] A. N. Bessani, J. Sousa, and E. A. P. Alchieri. State machine replication for the masses with BFT-SMaRt. In Proc. 44th International Conference on Dependable Systems and Networks, pages 355–362, 2014.
[34] J. Sousa and A. Bessani. Separating the WHEAT from the chaff: An empirical design for georeplicated state machines. In Proc. 34th Symposium on Reliable Distributed Systems (SRDS), pages 146–155, 2015.
[35] C. Cachin, K. Kursawe, and V. Shoup. Random oracles in Constantinople: Practical asynchronous Byzantine agreement using cryptography. Journal of Cryptology, 18(3):219–246, 2005.
[36] C. Cachin and J. A. Poritz. Secure intrusion-tolerant replication on the Internet. In Proc. Inter- national Conference on Dependable Systems and Networks (DSN-DCCS), pages 167–176, June 2002.
[37] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song. The honey badger of BFT protocols. In Proc. ACM Conference on Computer and Communications Security (CCS), 2016.
[38] Karl J. O'Dwyer and David Malone. 2014. Bitcoin Mining and its Energy Footprint. In Irish Signals and Systems Conference. Limerick, Ireland, 280–285.

[39] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. 2012. Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on Computer and communications security. 906–917.
[40] Ittay Eyal and Emin G¨un Sirer. 2013. Majority is not Enough: Bitcoin Mining is Vulnerable. (November 2013). http://arxiv.org/abs/1311.0243.
[41] crazyearner. 2013. TERRACOIN ATTACK OVER 1.2TH ATTACK CONFIRMD [sic]. (July 2013). https://bitcointalk.org/index.php?topic=261986.0.
[42] Danny Bradbury. 2013. Feathercoin hit by massive attack. (June 2013). http://www.coindesk.com/feathercoin-hit-by-massive-attack/.
[43] Sunny King and Scott Nadal. 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. (August 2012). http://peercoin.net/assets/paper/peercoin-paper.pdf.
[44] Vitalik Buterin. 2014. Slasher: A Punitive Proof-of-Stake Algorithm. (January 2014). https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/
[45] Kourosh Davarpanah, Dan Kaufman, and Ophelie Pubellier. 2015. NeuCoin: the First

Secure, Cost-efficient and Decentralized Cryptocurrency. (March 2015).
[46] John R. Douceur. 2002. The Sybil Attack. In Revised Papers from the First International Workshop on Peer-to-Peer Systems. 251–260.
[47] Eduardo A. Alchieri, Alysson Neves Bessani, Joni Silva Fraga, and Fab´ıola Greve. 2008. Byzantine Consensus with Unknown Participants. In Proceedings of the 12th International Conference on Principles of Distributed Systems. 22–40.
[48] David Schwartz, Noah Youngs, and Arthur Britto. 2014. The Ripple Protocol Consensus Algorithm. (2014). https://ripple.com/files/ripple_consensus_whitepaper.pdf.
[49] Jae Kwon. 2014. Tendermint: Consensus without Mining. (2014). http://tendermint.com/docs/tendermint.pdf.
[50] C. Copeland and H. Zhong. Tangaroa: A Byzantine fault tolerant raft. Class project in Distributed Systems, Stanford University, http://www.scs.stanford.edu/14au-cs244b/labs/ projects/copeland_zhong.pdf, Dec. 2014.
[51] D. Ongaro and J. K. Ousterhout. In search of an understandable consensus algorithm. In Proc. USENIX Annual Technical Conference, pages 305–319, 2014.
[52] D. Mazi`eres. The Stellar consensus protocol: A federated model for Internet-level consensus. Stellar, available online, https://www.stellar.org/papers/stellar-consensusprotocol. pdf, 2016.
[53] F. Armknecht, G. O. Karame, A.Mandal, F. Youssef, and E. Zenner. Ripple: Overview and outlook. In M. Conti, M. Schunter, and I. G. Askoxylakis, editors, Proc. Trust and Trustworthy Computing (TRUST), volume 9229 of Lecture Notes in Computer Science, pages 163–180. Springer, 2015.
[54] W. Anderson. Ripple consensus ledger can sustain 1000 transactions per second. Ripple Dev Blog, https://ripple.com/dev-blog/ripple-consensus-ledger-cansustain- 1000-transactions-per-second/, 2017.
[55] Blockchain Consensus Protocols in the Wild, Christian Cachin Marko Vukoli´c, 31st International Symposium on Distributed Computing (DISC 2017). Article No. 1; pp. 1–16