

فرمت ارسال اصل مقالات

بررسی تاثیر فناوری زنجیره بلوک در مدل‌های کسب‌وکار داده محور

A survey of blockchain impact on data-driven business models

احسان آریانیان، استادیار پژوهشگاه ارتباطات و فناوری اطلاعات، ehsan_ariyanan@itrc.ac.ir

Ehsan Ariyanan, Assistant Professor, Research Institute for ICT, ehsan_ariyanan@itrc.ac.ir

فرزاد زرگری، دانشیار پژوهشگاه ارتباطات و فناوری اطلاعات

Farzad Zargari, Associate Professor, Research Institute for ICT, zargari@itrc.ac.ir

مرتضی سرگلزایی جوان، پژوهشگاه ارتباطات و فناوری اطلاعات

Morteza Javan, Research Institute for ICT, m.sargolzaei.javan@itrc.ac.ir

چکیده (فارسی)

یکی از زمینه‌هایی که زنجیره بلوک در آن بکارگرفته شده است شکل‌گیری انواع مختلف مدل‌های کسب و کارهای داده محور متناسب با سطح بکارگیری زنجیره بلوک است. سطح اول استفاده زنجیره بلوک در ایجاد پلت فرم‌های ذخیره‌سازی غیرمتمرکز است که در آنها پرداخت هزینه‌ها و اجرت‌ها در ازای تامین منابع ذخیره‌سازی بصورت توزیع شده با استفاده از فناوری زنجیره بلوک و رمزارزها صورت می‌گیرد. از شبکه SAFE به عنوان نمونه‌ای از این شبکه‌های ذخیره‌سازی داده غیرمتمرکز و توزیع شده می‌توان نام برد. نوع دیگری از مدل‌های کسب و کار داده محور در سطحی بالاتر از زنجیره بلوک جهت ثبت جریان نقل و انتقالات آثار دیجیتال در وب استفاده می‌کنند. به عنوان مثال SPOOL پروتکلی است که برای کنترل مالکیت معنوی در وب ارائه شده است و با ایجاد یک لایه جدید مالکیت در بالای اینترنت این عمل را انجام می‌دهد. از آنجا که SPOOL از زنجیره بلوک برای ثبت تاریخچه معاملات تغییر مالکیت استفاده می‌کند، بنابراین سوابق بصورت غیرقابل تغییر در زنجیره بلوک قرار دارد و توسط همه قابل مشاهده است. در سطح سوم مدل‌های کسب و کار داده محور نظیر Storj و BigchainDB قرار دارند که زنجیره بلوک هسته اصلی کارکرد آنها را به عنوان یک پایگاه داده توزیع شده تشکیل می‌دهد. هدف این دسته از پایگاه‌های داده این است که از تمامی مزایای اصلی زنجیره بلوک نظیر کنترل غیرمتمرکز، مقاوم بودن در مقابل حمله برای تغییر داده‌ها و قابلیت ایجاد و انتقال سرمایه بر روی شبکه بدون نظارت متمرکز استفاده شود. در این مقاله تحولاتی که با استفاده از زنجیره بلوک در سطوح مختلف در پایگاه‌های داده توزیع شده ایجاد شده، تشریح می‌گردند و نمونه‌های عملی از مدل‌های کسب و کارهای داده محور حاصل از آنها بررسی می‌شوند.

چکیده (انگلیسی)

One of the areas in which the block chain is used is the formation of different types of data-driven business models according to the level of block utilization. The first level is to use the block chain to create a decentralized storage platform in which fees and revenues are paid in return for the supply of distributed storage resources using block chain technology and ceipher currencies. The SAFE network can be named as an example of these decentralized and



distributed data storage networks. Another type of data-driven business model uses block chain in higher level to record the digital streams of digital transmissions. For example, SPOOL (Secure Public Online Ownership Ledger) is a protocol that is developed to control intellectual property on the Web and does so by creating a new layer of ownership on top of the Internet. Because SPOOL uses the block chain to record the history of ownership change transactions, so the records are immutable in the block chain and are visible to everyone. On the third level, data-centric business models such as Storj and BigchainDB are located where block chain is the core block of the distributed database. The purpose of this category of databases is to use all the major benefits of the block chain, such as decentralized control, attack-resistance, to change data, and the ability to create and transfer capital over a non-centralized network. In this paper, developments that have been created using block chains at different levels in distributed databases are described, and practical examples of data-driven business models are investigated.

واژگان کلیدی

زنجیره بلوک، مدل‌های کسب‌وکار داده محور، پایگاه‌های داده توزیع شده

مقدمه

اولین زنجیره بلوک توسط شخص (یا گروهی از افراد) که با عنوان ساتوشی ناکاماتو (Nakamoto, n.d.) شناخته شده اند در سال ۲۰۰۸ معرفی شد. زنجیره بلوک یک سال بعد توسط ناکاماتو به عنوان جزء اصلی از رمز ارز^۱ بیت کوین (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009) بکار برده شد، که آن را به عنوان دفتر عمومی^۲ برای ذخیره همه معاملات در شبکه استفاده میکرد. با استفاده از زنجیره بلوک، بیت کوین اولین ارز دیجیتال بود که برای حل مشکل خرج مجدد^۳ بدون نیاز به یک مرجع قابل اعتماد ارائه شد و الهام بخش بسیاری از کاربردهای دیگر گردید. یکی از کاربردهای زنجیره بلوک پایگاه‌های داده توزیع شده است.

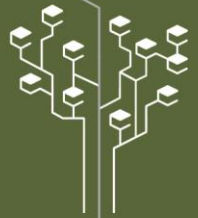
پایگاه‌های داده توزیع شده از پایگاه‌های داده ابری تا خود وب که بزرگترین پایگاه داده توزیع شده است کاربردهای گسترده ای یافته اند و هر روزه نیز بر دامنه کاربرد آنها افزوده میشود. این امر باعث آغاز پژوهش‌های متعدد جهت ارائه راهکارهای جدید جهت برطرف کردن کاستی‌های این پایگاه‌های داده گردیده است و تلاش میشود با برطرف کردن نقایص آنها بر دامنه کاربردهای آنها افزوده شود. زنجیره بلوک و رمز ارزها در برطرف کردن بسیاری از مشکلات پایگاه‌های داده توزیع شده بکار گرفته شده اند. برخی از مشکلات پایگاه‌های داده توزیع شده در ادامه شرح داده میشود.

در تلاش برای گسترش پایگاه‌های داده توزیع شده یکی از موضوعات مورد نظر استفاده از ظرفیت آزاد رایانه کاربران برای

^۱ Crypto Currency

^۲ Public Ledger

^۳ Double Spend



ذخیره اطلاعات کاربران دیگر است. یکی از چالش‌های موجود در این زمینه یافتن روشی برای پرداخت اجرت به کاربرانی است که ظرفیت دیسک خود را به اشتراک می‌گذارند و اصطلاحاً زارع^۴ نامیده میشوند. برخی از محققان این مشکل را با استفاده از انجام پرداختها بوسیله رمز ارزها حل کرده اند. آنها رمز ارزهایی را با استفاده از زنجیره بلوک ساخته و برای انجام پرداختها به زارعان از آنها استفاده مینمایند. چالش دیگر در این زمینه پیگیری مسیر نقل و انتقالات در پایگاه داده است. اطلاعات ذخیره شده اشیاء دیجیتال دارای مالکیت معنوی باشند. این امر بخصوص در پیگیری انتقال دارایی‌های دیجیتال در وب حائز اهمیت است. در این زمینه هم میتوان از زنجیره بلوک استفاده نمود. برخی از پژوهشگران ایده‌های متهورانه تری را ارائه نموده اند و سعی دارند با استفاده از زنجیره بلوک پایگاه داده‌ای را طراحی نمایند که دارای تمامی مزایای زنجیره بلوک نظیر کنترل غیر متمرکز، مقاوم بودن در مقابل حمله برای تغییر داده‌ها و قابلیت ایجاد و انتقال سرمایه بر روی شبکه بدون نظارت متمرکز باشد. هدف از این مقاله معرفی و بررسی پایگاه‌های داده‌ای است که برای برطرف کردن مشکلات پایگاه‌های داده موجود ارائه شده است و در این راه از زنجیره بلوک استفاده نموده اند. ترتیب ارائه باقی مطالب در این مقاله به شرح زیر است.

بخش بعدی به پایگاه‌های داده‌های میپردازد که از زنجیره بلوک برای پرداخت هزینه‌ها به زارعان استفاده میکنند. در بخش سه پایگاه‌های داده‌ای که از زنجیره بلوک برای ذخیره جریان نقل و انتقال اطلاعات استفاده می‌کنند بررسی میشوند. نحوه استفاده از زنجیره بلوک برای ساخت پایگاه داده در بخش چهار شرح داده میشود و در نهایت مقاله در فصل پنج با جمع بندی مطالب گفته شده خاتمه می‌یابد.

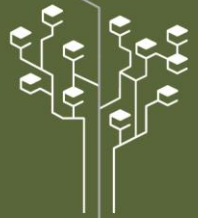
مفاهیم اولیه زنجیره بلوک و مروری بر ادبیات موضوع

در این بخش مفاهیم اولیه زنجیره بلوک را تا حدی که برای مطالعه باقی مطالب مقاله مورد نیاز است توضیح میدهم. برای آشنایی بیشتر با مفاهیم زنجیره بلوک میتوان به این منابع مراجعه نمود (Bruyn, 2017)، (Swan, 2015) و (Martinovic). زنجیره بلوک نوع جدیدی از پایگاه داده است و دلیل رایج شدن آن حل مسئله خرج مجدد بدون نیاز به فردی دیگر است و این امر افق تاره‌ای برای زمینه جدیدی از کاربردها ایجاد میکند. در این پایگاه داده، داده‌ها در بلوکی ذخیره می‌شوند که به نوبه خود به بلوک‌های دیگر در زنجیره‌ای که زنجیره بلوک را ایجاد می‌کند، مرتبط است. برای تامین امنیت بلوک از روشی به نام تایید بر اساس کار^۵ استفاده می‌شود. به طور خلاصه این بدان معنی است که چون کار بسیار زیاد (به عنوان مثال قدرت پردازشی زیاد) برای پیدا کردن یک بلوک مورد نیاز است در نتیجه تقریباً غیرممکن است که مدتی بعد از ثبت یک بلوک آن را در زنجیره بلوک تغییر داد. پیدا کردن یک بلوک توسط به اصطلاح معدنچیان^۶ انجام می‌شود که وقتی آنها بلوکی را پیدا می‌کنند، پرداخت کوچکی را در ازای تلاش خود دریافت میکنند. به بیان دقیقتر زنجیره بلوک یک پایگاه داده غیر متمرکز و توزیع شده است که برای نگهداری فهرست پیوسته‌ای از پرونده‌ها، به نام بلوک‌ها استفاده می‌شود. هر بلوک حاوی نشانه زمانی و یک پیوند به بلوک قبلی است. طراحی زنجیره بلوک به گونه‌ای است که به طور ذاتی نسبت به تغییر داده‌ها مقاوم است. در عمل زنجیره بلوک را می‌توان به عنوان یک دفتر باز و توزیع شده باشد که می‌تواند معاملات بین افراد را به نحوی کارا و غیرقابل تغییر ثبت کند.

^۴ Farmer

^۵ Proof of work (POW)

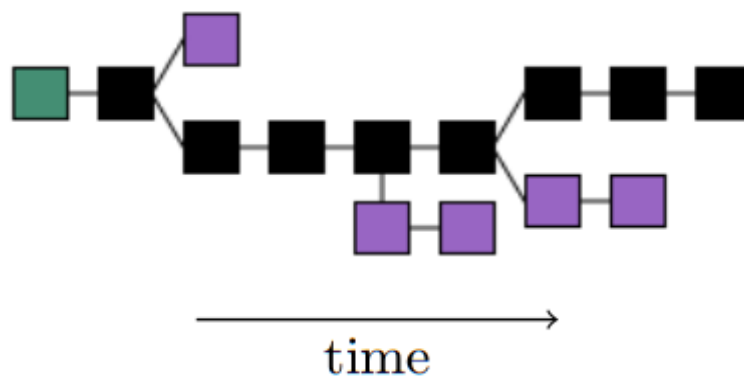
^۶ Minners



برای توضیح بهتر این مطلب رمز ارز بیت کوین را که بر مبنای زنجیره بلوک است را در نظر بگیرید. کیف پول این رمز ارز بر اساس زنجیره بلوک است و بنابراین نیازی به شخص ثالث برای ذخیره آن نیست. به جای اینکه تراکنش توسط یک شخص ثالث مثلاً یک بانک بررسی شود، توسط هر کسی که در سیستم شرکت می‌کند و هر کسی که در آینده به سیستم می‌پیوندد، "بررسی" خواهد شد. بنابراین نیاز به یک شخص ثالث متمرکز را برطرف می‌کند، این روش مزایای متعددی دارد مانند هزینه انتقال کمتر یا ناشناس ماندن پرداخت کننده، در حالی که پرداخت‌های در سطح بین‌المللی را تسهیل میکند و برگشت معامله در آن غیر ممکن است. همه اینها به همراه همان اطمینان دریافت پول خود وقتی که یک موسسه مالی دارایی شما را تضمین میکند.

از آنجا که زنجیره بلوک غیر متمرکز و توزیع شده است تمامی گره‌های فعلی و تمام گره‌های آینده می‌توانند بررسی کنند که آیا هر معامله بر اساس قوانین معینی انجام شده است. این باعث می‌شود که کسی نتواند در یک زمان پول را به دو شخص منتقل کند. این روش باعث از بین بردن نیاز به یک شخص ثالث که انحصار تمام اطلاعات را دارد و می‌تواند تصمیم‌هایی را که بررسی صحت آنها بسیار دشوار است را برطرف میکند. اما چگونه می‌توانید این اطمینان را به دست آورید که پول وعده داده شده خود را بدون اینکه هیچ شخص ثالثی آن را بررسی کند، به دست آورید؟ با یک مثال نشان می‌دهیم که ترتیب بلوک‌ها در زنجیره به طور قطعی، ترتیبی را که معاملات انجام شده‌اند را تعیین می‌کند. به این دلیل زنجیره بلوک نامگذاری شده است که اساساً یک زنجیره بی‌پایان از بلوک‌ها است. و ترتیب بلوک‌ها در این زنجیره ترتیب انجام معامله را مشخص میکند.

در تصویر ۱ مثالی از این زنجیره نشان داده شده است. رنگ‌های مختلف "انواع" بلوک را نشان می‌دهد. زنجیره از پایین به بالا رشد می‌کند. بلوک اول یک بلوک خاص است، زیرا تنها بلوک در کل زنجیره‌ای است که هیچ بلوک قبلی ندارد. به همین دلیل است که تنها یک بلوک با رنگ سبز در تصویر ۱ است. بلوک‌های سیاه بلوک‌های معمولی هستند. این‌ها بلوک‌هایی هستند که طولانی‌ترین زنجیره‌ای (و در نتیجه زنجیره اصلی) را تشکیل می‌دهند. بلوک‌های بنفش شکل "چنگال" را تشکیل می‌دهند. این شکل زمانی ایجاد میشود که دو بلوک همزمان یافت می‌شوند. برای یک لحظه کوتاه دو زنجیره‌ای با طول یکسان وجود دارند و تا زمانی که برای یکی از زنجیره‌ها بلوک جدید سریعتر از زنجیره دیگر پیدا نشود، مشخص نیست که کدام یک از آنها زنجیره اصلی است.





تصویر ۱- مثالی از یک زنجیره بلوک (Bruyn, 2017)

سازنده زنجیره بلوک آن را با هدف حل یک مشکل خاص ارائه کرد: مشکل صرف هزینه دوگانه: "آنچه مورد نیاز است یک سیستم پرداخت الکترونیکی مبتنی بر رمزنگاری به جای اعتماد است، به نحوی که به دو طرف معامله اجازه می‌دهد تا بدون نیاز به یک شخص ثالث مورد اعتماد، به طور مستقیم با یکدیگر ارتباط برقرار کنند. معاملاتی که به صورت محاسباتی فروشندگان را از تقلب محافظت می‌کند و مکانیزم‌های سپرده معمول را می‌توان به راحتی برای محافظت از خریداران انجام داد. در این مقاله، ما راه حلی برای مشکل صرف هزینه دوگانه با استفاده از پرچسب زمانی توسط سرورهای توزیع شده نظیر به نظیر برای تولید اثبات محاسباتی ترتیب زمانی معاملات پیشنهاد می‌دهیم." ساتوشی ناکاموتو (Nakamoto, Bitcoin:)
(A Peer-to-Peer Electronic Cash System, 2009).

به عبارت دیگر: یک مشکل رو به رشد در دنیایی که رو به جهانی شدن می‌رود اعتماد است. مردم با افرادی که هرگز ملاقات نکرده‌اند، کسب و کار می‌کنند و احتمالاً هرگز حتی با آنها مواجه نخواهند شد. چگونه می‌توانید اطمینان حاصل کنید که شخص دیگری آنچه را به شما وعده داده است پرداخت خواهد کرد. و اگر او این کار را انجام ندهد، آیا کاری هست که شما می‌توانید در برابر آن انجام دهید؟ یا شما فقط همه محصولات تجاری خود را قمار کرده‌اید؟

همه انواع اقدامات مشابه (مانند Pay-pall) برای کمک به حل این نوع مشکلات بکار گرفته شده‌اند. اما آنها دارای ویژگی برگشت پرداخت هستند. زنجیره بلوک همه این مشکلات را حل می‌کند. از آنجا که پایگاه داده توزیع شده است، بسیار شفاف است: هر کس می‌تواند خودش، اگر همه قوانین مراعات شده باشند، صحت معاملات را بررسی کند. دیگر شخص ثالثی وجود ندارد که بتواند تصمیم بگیرد که یک معامله را برگشت بزند. یک بار که پرداخت انجام شود، دیگر انجام شده است. مزیت اضافه شده این است که بلوک‌ها به دلیل "تائید بر اساس کار" نمی‌توانند تغییر کنند.

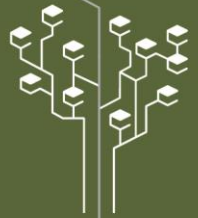
استفاده از زنجیره بلوک برای پرداخت هزینه‌ها در پایگاه‌های داده

شبکه‌های غیرمتمرکز یا نظیر به نظیر^۶ مفهوم جدیدی نیستند. از زمان انتشار Napster در تاریخ ۱ ژوئن ۱۹۹۹، این شبکه‌ها انقلابی در اشتراک گذاری فایل ایجاد کرده‌اند. این شبکه‌ها کاربران را از سراسر جهان به یکدیگر متصل می‌کنند و داده‌ها را مانند فیلم‌ها، کتاب‌ها و موسیقی به اشتراک می‌گذارند. در سال ۲۰۱۰ بیش از نیمی از ترافیک اینترنت به کاربردهای شبکه‌های نظیر به نظیر اختصاص یافت. اما استفاده از این فن آوری‌ها به اشتراک گذاری فایل محدود نمی‌شود. Freenet در مارس ۲۰۰۰ راه اندازی شد و به مردم اجازه داد تا وبسایت‌های غیرمتمرکز^۸ منتشر کنند. وبسایت‌های غیرمتمرکز در سرورهای مرکزی ذخیره نمی‌شوند بلکه در میان دستگاه‌های کاربران شبکه رمز شده توزیع می‌شوند. کمی بعد از آن پروتکل بیت تورنت توسط برام کوهن ایجاد شد. بیت تورنت^۹ به خصوص برای انتقال فایل‌های بزرگ در شبکه‌های نظیر به نظیر مناسب است و اجازه بارگیری همزمان از چند نظیر را فراهم می‌کند. گام بعدی که در توسعه اشتراک گذاری فایلها در شبکه می‌توان تصور شد یک شبکه داده کاملاً مستقل است. یک شبکه داده مستقل به این معنی است که قادر به مدیریت و بهینه‌سازی حجم کار، مسیریابی، بارگیری سیستم، احراز هویت، کنترل دسترسی و سایر کارهای شبکه و ذخیره

^۶ Peer to Peer (P2P)

^۸ Freesites

^۹ BitTorrent



سازی بدون دخالت انسان باشد.

شبکه ^{۱۰}SAFE (Nick Lambert, 2015) و (Irvine, 2018) تلاش میکند تا زیرساخت لازم برای یک شبکه کاملاً مستقل را فراهم آورد. بر خلاف اینترنت فعلی، زیرساخت SAFE توسط مجموعه‌ای از سرورهای فدرال، ماشین‌های مجازی، که دارای فضاهای ذخیره سازی یا گره‌های قابل شناسایی هستند تعریف نشده است. و بر خلاف بیت تورنت، به زیرساخت‌های اصلی وب برای تعیین محل و ردیابی فایل‌ها نیاز ندارد. هیچ گونه دخالت انسانی در شبکه SAFE وجود ندارد. شبکه خود در مورد هزینه‌ها، اجرت‌ها، نحوه محافظت از داده‌ها، ارتباطات و محاسبات را تصمیم می‌گیرد. SAFE یک شبکه نظیر به نظیر ایمن، مستقل، و داده محور را به عنوان یک جایگزین برای مدل کنونی وب مبتنی بر سرور پیشنهاد میکند. به جای قرار دادن فایلها در یک سرور مرکزی یا مرکز داده، فایل‌های افراد به قطعات تقسیم می‌شوند، رمزگذاری شده و در شبکه پخش می‌شوند. افراد کنترل کامل فایل‌های ایجاد شده خود را حفظ می‌کنند. این ساختار به حمله منع سرویس توزیع شده، نرم افزارهای مخرب و هک مقاوم می‌باشد و توسط شرکت‌ها و دولت کنترل نمی‌شود. به عنوان یک پلتفرم، چنین شبکه‌ای می‌تواند مدل‌های جدید کسب و کار ایجاد کند، همانطور که اینترنت در اواسط قرن گذشته چنین بود.

شبکه SAFE را می‌توان به عنوان یک لایه امن و رمزگذاری شده در نظر گرفت که در بالای اینترنت فعلی قرار می‌گیرد و این امکان را فراهم می‌آورد که ذخیره سازی خودمختار داده‌ها با جایگزینی سه لایه شبکه OSI (ارائه، جلسه و انتقال) انجام شود. شبکه SAF دو جزء اساسی دارد: انبارها ^{۱۱} و مشتریان ^{۱۲}. نرم افزار مشتری به کاربران اجازه می‌دهد تا به شبکه دسترسی داشته باشند، در حالی که انبارها قابلیت ذخیره سازی، مسیریابی و امنیت داده و نحوه به دست آوردن پول Safecoin را فراهم می‌کند. یک کامپیوتر می‌تواند بطور همان زمان جزء هر دو نوع گره باشد.

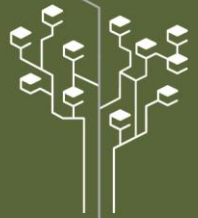
هسته SAFE Network از گره‌هایی به نام انبار تشکیل شده است. انبارها دارای برنامه‌هایی هستند که کاربران (زارعان) در رایانه‌هایشان اجرا می‌کنند و دستگاه‌ها را به یکدیگر متصل می‌کنند و با استفاده از پروتکل‌های موجود مانند TCP، UDP و μTP. انبارها اجازه می‌دهند تا کاربران شبکه داده‌ها را در دستگاه‌های آنها ذخیره کنند، در مقابل این کار به آنها رمز ارز Safecoin پرداخت می‌شود. انبارها همچنین مدیریت داده‌ها و مسیریابی آنها را در شبکه انجام داده و با تبادل پیام‌هایی صحت اتفاقات رخ داده در شبکه را تایید می‌کنند. نرم افزار انبار یک فایل اجرایی کوچک است که دستگاه کاربر را به شبکه SAFE متصل می‌کند. این برنامه داده‌ها را بر روی کامپیوتر کاربر ذخیره می‌کند و به این ترتیب ظرفیت ذخیره سازی در شبکه را فراهم می‌کند. نرم افزار انبار همچنین مسیرهای داده و داده‌های رمزگذاری شده را بر روی شبکه ذخیره می‌کند و با استفاده از پیام‌هایی که به طور کامل رمزگذاری شده اند ارتباطات را برقرار می‌سازد. انبارها به گروه‌های کوچکتری به نام "بخش" تقسیم می‌شوند که هر کدام مسئول مراقبت از اطلاعات ذخیره شده در محدوده مشخصی از آدرس‌ها هستند. اجرای یک برنامه انبار توسط یک کامپیوتر در شبکه SAFE زراعت نامیده می‌شود، زیرا انبارها از داده‌ها نگهداری میکنند تا در موقع نیاز استفاده شوند و برای این کار خود پول دریافت می‌کنند.

همانطور که نیازی به اجرای وب سرور برای استفاده از وب نیست، بنابراین لازم نیست که کاربران معمولی برنامه انبار را برای دسترسی به SAFE Network به اجرا بگذارند. کاربران معمولی از طریق برنامه مشتری با شبکه ارتباط برقرار می‌کنند. این برنامه نرم افزاری است که در حال حاضر با مرورگر Peruse همراه است که امکان اتصال امن به انبارها را به شبکه

^{۱۰} Secure Access For Everyone

^{۱۱} Vaults

^{۱۲} Clients



SAFE را تشکیل می‌دهند، فراهم می‌آورد ضمن آن که آدرس IP کاربر از شبکه پنهان میکند. هر کاربر (حتی اگر به سیستم وارد نشده باشد) قادر به درخواست داده‌ها از شبکه به صورت رایگان است. به عنوان مثال کاربران می‌توانند یک سایت را مرور کنند یا یک آهنگ یا فیلم را ارسال کنند و هیچ هزینه‌ای برای این کار نخواهند پرداخت. تنها زمانی که کاربر می‌خواهد اطلاعات را در شبکه ذخیره کند یک حساب کاربری با مقدار کمی Safecoin مورد نیاز است. SAFE نمونه‌ای از بکارگیری رمز ارز مبتنی بر زنجیره بلوک برای ایجاد یک سیستم مستقل و خودمختار در وب است. این پلتفرم میتواند الگویی برای کاربردهای دیگر که نیاز به پرداخت هزینه دارند و میخواهند بطور مستقل نیز عمل کنند در نظر گرفته شود.

استفاده از زنجیره بلوک برای ذخیره جریان نقل و انتقال اطلاعات

در بخش قبل در مورد بکارگیری زنجیره بلوک برای انجام پرداختها در یک سیستم خودمختار در وب صحبت شد و در این بخش در مورد سیستمی بحث میکنیم که با استفاده از زنجیره بلوک جریان نقل و انتقالات در وب را ثبت میکند تا بتواند مسئله حق مالکیت آثار دیجیتال را در وب حل کند. در اینترنت، سازندگان محتوای دیجیتال برای کار خود به طور عادلانه حق الزحمه دریافت نمی‌کنند. مصنوعات دیجیتال دارای ویژگی‌های منحصر به فرد تکرار بی پایان و هزینه‌های انتقال نزدیک به صفر هستند. این امر منجر به گسترش وسیع وب سایت‌ها توسط افرادی می‌شود که با کپی کردن آثار دیگران خود را دارای قابلیت‌هایی جلوه میدهند که فاقد آن هستند. اشکال این موضوع آن است که پدیدآورندگان به ندرت حقالزحمه کار خود را دریافت میکنند. ناشران از ترس از دست دادن درآمد خود، با ایجاد سیستم‌های مدیریت حقوق دیجیتالی^{۱۳} واکنش نشان داده‌اند. فن آوری مدیریت حقوق دیجیتالی واقعا موثر نیست، یکی از دلایل آن این است که صنعت موسیقی در عمل استفاده از آن را کنار گذاشته است. اما نیاز مبرم به یک راه حل قابل قبول برای مشکل مالکیت باقی مانده است، به خصوص به این خاطر که موارد جدیدتری از تولیدات دیجیتال نظیر آثار هنری دیجیتال، فیلم‌ها و حتی الگوهای چاپ سه بعدی به راحتی از طریق وب بصورت آنلاین در دسترس قرار میگیرند. ارائه یک راه حل قابل اجرا برای مدیریت مجوز در اینترنت میتواند منجر به انفجار بی سابقه‌ای از خلاقیت در اینترنت شود، زیرا هنرمندان و خالقان آثار هنری می‌توانند بدون ترس از سرقت از کار خود برای آنها مجوز صادر کنند یا آنها را به فروش برسانند.

طراحی مجدد اینترنت برای افزودن ویژگی در نظر گرفتن حق مالکیت، غیر عملی است. اما می‌توان آن را ارتقاء داد، به عنوان مثال با اضافه کردن یک زیرساخت که مسائل مربوط به حق مالکیت در نظر میگیرد بدون آنکه نیازی به ایجاد تغییرات اساسی در وب سایت‌های مختلف وب وجود داشته باشد.^{۱۴} SPOOL (Holtzman, 2015) یک پروتکل برای مستندسازی معاملات مربوط به مالکیت اموال دیجیتال است. SPOOL برای زدن برجسب‌های زمان و ثبت تاریخچه معاملات تغییر مالکیت استفاده می‌شود. این تاریخچه می‌تواند در صورت اختلاف بر سر مالکیت آثار دیجیتال به عنوان مدرک در دادگاه مورد استفاده قرار گیرد. SPOOL اقدامات مربوط به مالکیت و تغییر آن را با استفاده از برجسب زنی زمانی بر روی اعمال مربوط به تغییر مالکیت بر روی یک رجیستری که قابلیت اعتماد آن با استفاده از تکنولوژی موجود اثبات شده (زنجیره بلوک بیت کوین) تأمین می‌کند. زنجیره بلوک می‌تواند به عنوان یک پایگاه داده در نظر گرفته شود که هر کسی می‌تواند اطلاعات را به اضافه کند، اما هیچ کس نمی‌تواند آن را حذف کند و هیچ کس آن را "مالکیت" نمی‌کند. پروتکل بیت کوین به پردازش پرداختها تمرکز کرده است. البته در SPOOL، علاقه ما به پرداخت‌ها نیست، بلکه معاملات و تغییر مالکیت است.

^{۱۳} Digital right management (DRM)

^{۱۴} Secure Public Online Ownership Ledger



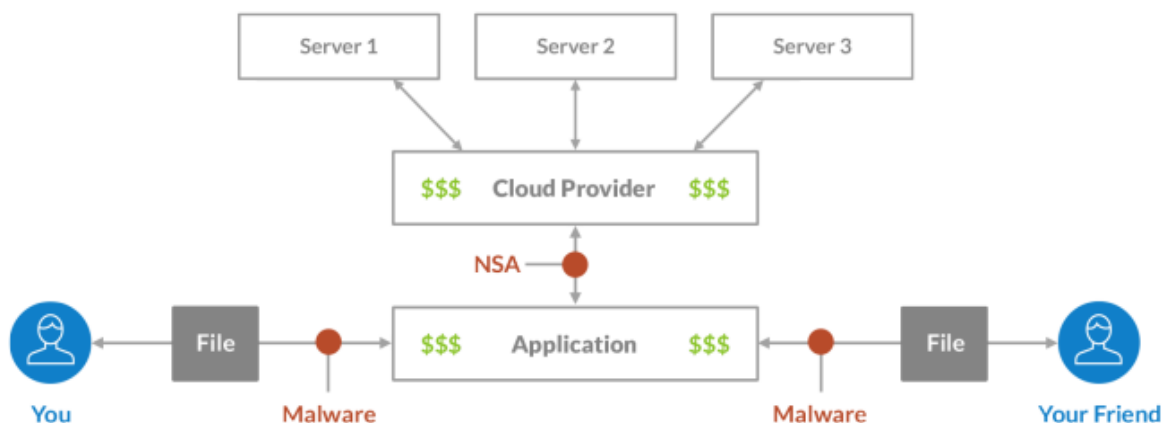
از آنجا که SPOOL از زنجیره بلوک برای ثبت تاریخچه معاملات تغییر مالکیت استفاده می‌کند، بنابراین مالک اثر نیاز ندارد برای حفظ سوابق مالکیت به SPOOL تکیه کند. حتی اگر SPOOL به طور کامل از بین برود تمام کاربران امتیازات کپی رایت و مجوز خود را حفظ خواهند کرد، زیرا سوابق غیر قابل تغییر در زنجیره بلوکی است که توسط همه کس قابل مشاهده است. اگر این چنین نبود، مردم پول خود را در بیت کوین قرار نمیدادند که ارزش جهانی بیش از یک میلیارد دلار آمریکا است.

استفاده از زنجیره بلوک برای ساخت پایگاه داده

همانگونه که قبلاً گفته شد برخی از پژوهشگران ایده های متهورانه تری در استفاده از زنجیره بلوک برای ساخت پایگاه داده ارائه نموده اند و سعی دارند با استفاده از زنجیره بلوک پایگاه داده ای را طراحی نمایند که دارای تمامی مزایای زنجیره بلوک نظیر کنترل غیر متمرکز، مقاوم بودن در مقابل حمله برای تغییر داده ها و قابلیت ایجاد و انتقال سرمایه بر روی شبکه بدون نظارت متمرکز باشد. در این بخش دو پایگاه داده Metadisk و BigchainDB که با این هدف ارائه شده اند بررسی میشوند.

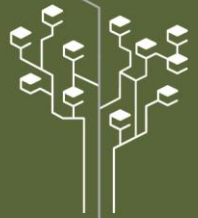
پایگاه داده Metadisk

هنگامی که داده ها در ابر ذخیره می شوند، داده ها بوسیله پروتکل TCP / IP از کامپیوتر مشتری به سرور میزبان در یک مرکز داده انتقال یابند. این سرور سپس آنها را به سرورهای دیگر کپی می کند و به منظور انطباق با قوانین افزونگی استاندارد از آن سه نسخه میسازد (تصویر ۲).



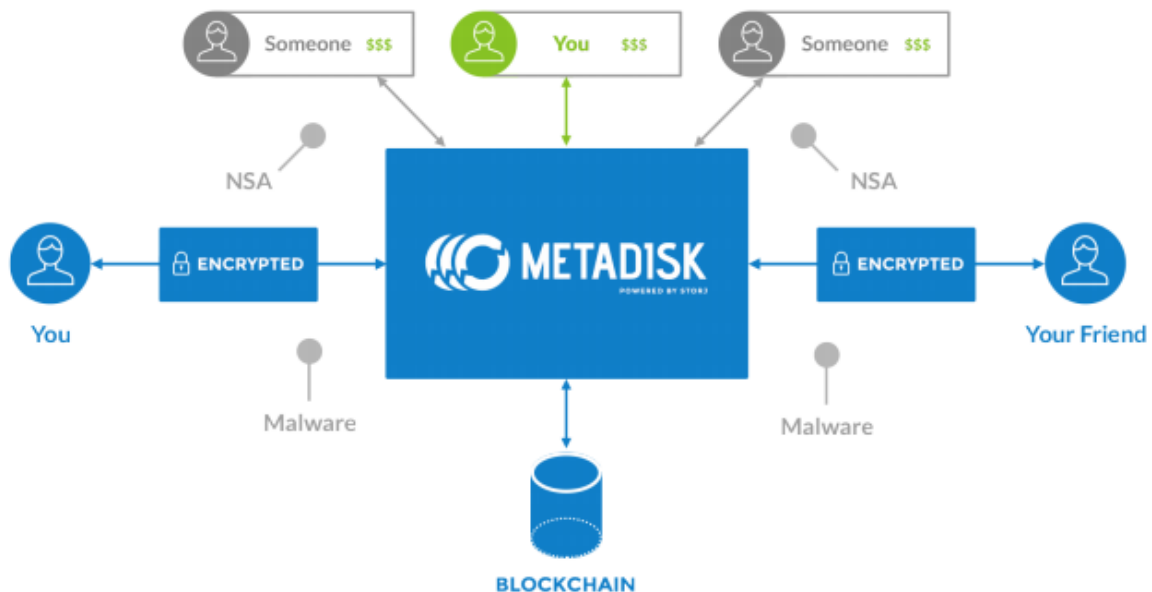
تصویر ۲-مدل استاندارد ذخیره سازی در cloud (Shawn Wilkinson, 2014)

مدل فعلی ذخیره سازی ابری که از طریق مؤسسات معتمد که اطلاعات خصوصی به آنها سپرده شده است ارائه میشود بطور



ذاتی از جنبه های مختلف امن نیست. دزدان اطلاعات، جاسوسها و سانسورچی ها می توانند داده های ذخیره شده بر روی سرور میزبان را از طرق سیاسی یا تاکتیک های قانونی و با تکنیکهای فن آوری، کپی نموده یا نابود کنند. در حال حاضر مشخص است که حفظ حریم شخصی و امنیت اطلاعات سازمانی تنها زمانی می تواند به دست آید که ذخیره سازهای داده بتوانند در مقابل حملات انجام شده از هر سه طریق محافظت شوند. یکی از نقاط ضعف امنیتی ذاتی در مدل ذخیره سازی ابری فعلی انواع مکانیسم های پرداخت است که در حال حاضر بصورت گسترده در موسسات ارائه خدمات ذخیره سازی ابری استفاده می شوند. این مکانیسم ها نه حریم خصوصی را حفظ میکنند و نه از نظر اطلاعاتی امن هستند زیرا در بیشتر تکنیک های پرداخت آنلاین که اطلاعات مربوط به پرداخت کننده و پرداخت کننده را ذخیره میکنند امکان نشت این اطلاعات وجود دارد. در واقع به یک مدل ذخیره سازی ابر نیاز داریم که بر پایه اعتماد بین مشتری و میزبان نیست. تمام داده های شخصی مشتری، از جمله نام فایل، تاریخ و سایر فراداده ها، باید قبل از هرگونه انتقال از رایانه مشتری به ابر رمزگذاری شوند. نتوان هیچ نقطه مرکزی خرابی با استفاده از بردارهای حمله سیاسی یا قانونی در سیستم ایجاد کرد. تمام پرداخت های مشوق برای هر دو ارائه دهندگان منابع و مصرف کنندگان اتوماتیک و از طریق یک رمز ارز انجام خواهد شد.

این اصول با استفاده از ترکیبی از تکنولوژی های موجود مانند Bitcoin (Bittorrent sync, 2014) ، Sync رمزنگاری کلید عمومی و توابع هش رمزنگاری قابل پیاده سازی هستند. Metadisk (Shawn Wilkinson, 2014) با هدف ادغام آسان با پروژه های منبع باز موجود با هدف توسعه یک شبکه ذخیره سازی غیرمتمرکز ارائه شده است (تصویر ۳).



تصویر ۳-مدل ذخیره سازی در Metadisk (Shawn Wilkinson, 2014)

چنین شبکه ای باید به صورت تدریجی و با نرم افزارهای ماژولار با قابلیت عملکرد متقابل و قابل جایگزینی که از طیف وسیعی



از سخت افزارها، از جمله مدل ارائه دهنده سخت افزاری به عنوان یک سرویس که در ذخیره سازی ابری موجود است، پشتیبانی می کنند. Metadisk می تواند از یک مدل انگیزشی مشابه آنچه که توسط بیت کوین استفاده می شود استفاده کند. از آنجا که معدنچیان بیت کوین پاداش های بلوک برای کمک به منابع قدرت هش کردن رمزنگاری را به شبکه می دهند، Metadisk می تواند از رمزنگاری خود به عنوان وسیله ای برای پرداخت و مبادله فضای ذخیره سازی و پهنای باند استفاده کند. این مدل نیروی قدرتمند لازم برای رشد و بهره وری شبکه ها را در حالی که عدم تمرکز حفظ می گردد را فراهم می کند.

Metadisk به عنوان رابط کاربر غیر فنی و همچنین پلت فرم توسعه شبکه Storj (Wilkinson, 2014) خدمت می کند. کاربران با استفاده از رابط وب متادیسک یا واسط برنامه کاربردی^{۱۵} می توانند فایل های خود را از شبکه ایمن آپلود و دانلود کنند. فایل ها در طول فرآیند آپلود با استفاده از کلید خصوصی ارائه شده توسط کاربر رمزگذاری می شوند. اگر کاربر قبلاً از Metadisk استفاده نکرده باشد، رابط وب ممکن است برای کمک به کاربر یک کلید خصوصی به او ارائه دهد. Metadisk با شبکه ارتباط برقرار می کند تا منابع ذخیره سازی موجود را پیدا کند و سپس پرونده را به حداقل سه مکان جداگانه منتقل می کند تا افزونگی سه برابر (x3) را به عنوان استاندارد صنعت برای ذخیره سازی ابر در نظر بگیرد. کاربر یا برنامه می تواند افزونگی بیشتر را با هزینه اضافی فراهم کند. ما یک روش ثبت کارآمد بوسیله زنجیره بلوک ارائه داده ایم، بنابراین وقتی یک کاربر یک فایل را آپلود می کند، یک رکورد از متادیتای فایل آپلود شده در زنجیره بلوک ساخته می شود. بعد از اینکه فایل رمزنگاری شد، هش^{۱۶} SHA-256 آن را پیدا می کنیم که هم به عنوان یک شناسه ی منحصر به فرد فایل و همچنین روشی برای تشخیص دستکاری فایل عمل می کند. اگر هر گونه تغییر پس از آپلود، در فایل رخ دهد هش آن متفاوت خواهد شد. ما از این واقعیت در پلتفرم پایه Storj استفاده می کنیم (Storj - decentralized cloud storage, 2014)، بنابراین شبکه می تواند فایل ها را مستقیماً بدون دسترسی به آنها بررسی کند. یک مشتری همچنین می تواند با استفاده از هش فایل از اینکه فایل دریافت شده معتبر است اطمینان حاصل کند. هش فایل در یک blockchain همراه با مکان ذخیره سازی سه کپی فایل مورد استفاده برای تولید هش، ذخیره می شوند. تمام ابر داده های که در بلوکچین وارد شده اند می توانند با استفاده از رمزنگاری کلید عمومی در مقابل خواندن غیر مجاز و همچنین کپی کردن محافظت شوند. از آنجا که تمام داده ها و ابر داده های ورودی به شبکه رمزگذاری شده اند و ما می توانیم داده ها را از طریق هش کردن بررسی کنیم، اشخاص مخرب نمی توانند به جاسوسی، تقلب یا تغییر داده ها دست بزنند.

پایگاه داده BigchainDB

پایگاههای داده توزیع شده دارای ویژگیهایی به شرح زیر هستند:

- راندمان بالا در عملیات پایگاه داده که با افزایش نودها افزایش می یابد
- ظرفیت بالا که با افزایش نودها افزایش می یابد
- تاخیر کم
- قابلیت بالا در کار با کوئری ها
- قابلیت بالا در دادن انواع مجوزها به کاربران

^{۱۵} Application program interface (API)

^{۱۶} Hash



در حالیکه ویژگی‌های اصلی زنجیره بلوک عمدتاً عبارتند از:

- کنترل غیر متمرکز
- مقاوم بودن در مقابل حمله برای تغییر داده‌ها
- قابلیت ایجاد و انتقال سرمایه بر روی شبکه بدون نظارت متمرکز

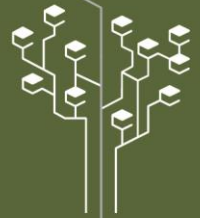
هدف (Trent McConaghy, 2016) BigchainDB ایجاد پایگاه داده مبتنی بر زنجیره بلوک است که این پایگاه داده از تمامی مزایای فوق بهره‌مند شود. یکی از مشکلات بکارگیری زنجیره بلوک در پایگاه داده راندمان پایین زنجیره بلوک در انجام تراکنشها است. به عنوان مثال بیت کوین بطور میانگین در هر ثانیه یک انتقال انجام میدهد و در هر ۱۰ دقیقه یک بلوک را پردازش میکند. در حالیکه Visa در هر ثانیه بطور متوسط ۲۰۰۰ انتقال و در حالت پیک ۱۰۰۰۰ انتقال را انجام می‌دهد. مشکل دیگر در این زمینه تاخیر زیاد است. با توجه به ۱۰ ثانیه زمان پردازش یک بلوک در بیت کوین برای رسیدن به امنیت کافی لازم است برای تأیید یک بلوک یک ساعت صبر کنیم در حالیکه Visa در یک ثانیه انتقال را تأیید میکند. لازم به ذکر است که بسیاری از کاربردهای مالی به تاخیرهای زیر ۳۰ تا ۱۰۰ میلی ثانیه نیاز دارند.

ظرفیت و پهنای باند شبکه مورد دیگری است که میتواند مانعی در جهت استفاده زنجیره بلوک در پایگاههای داده گردد. حجم زنجیره بلوک بیت کوین در حدود ۱۰۰ گیگا بایت است و در سال به میزان چندین گیگا بایت افزایش میابد. در صورتی که راندمان آن در حد Visa (۲۰۰۰ انتقال در ثانیه) باشد پایگاه داده در هر روز حدوداً ۴ گیگابایت افزایش میابد که در سال حدود یک ونیم پتابایت (یکمیلیون و پانصد هزار گیگا بایت) میشود. اگر راندمان ۱۵۰۰۰۰ انتقال در ثانیه باشد پایگاه داده در هر سال ۲۱۴ پتابایت بزرگتر میشود. اگر راندمان ۱ میلیون انتقال در ثانیه باشد پهنای باند مورد نیاز برای ذخیره آن، هر گره ای در شبکه را از کار می‌اندازد.

یکی دیگر از خصایص مهم پایگاه داده‌های توزیع شده الگوریتم اجماع است. در الگوریتم اجماع گره‌های مسئول تکثیر یک داده از یک الگوریتم اجماع برای توافق برای کپی داده استفاده میکنند. مسئله اجماع بطور خلاصه مسئله توافق بین چند فرایند محاسباتی بر روی یک موضوع است با این فرض که بعضی از آنها میتوانند دارای خطا باشند و آنها تنها با پیامهای دو طرفه میتوانند ارتباط برقرار کنند. الگوریتم اجماع توسط تمامی فرایندهایی که دارای خطا نیستند اجرا میشود. الگوریتم اجماع به نوع خطایی که برای فرایندها در نظر گرفته میشود بستگی دارد. انواع خطا در فرایندهای اجماع میتوانند در نظر گرفته شوند که مشهورترین آنها به شرح زیر هستند:

- خطای Benign یا fail-stop در این حالت فرایند دارای خطا پاسخ به پیام نمیدهد (به علت از کار افتادن هارد دیسک یا داغ شدن cpu)
- خطای Byzantine در این حالت فرایند دارای خطا میتواند انواع خطاها را داشته باشد مثلاً دروغ بگوید، بصورت گروهی تبانی، وانمود کند از کار افتاده است یا مشارکت کند.

شناخته شده ترین الگوریتم اجماع مقاوم در برابر خطا الگوریتم Paxos و مشتقات آن است. این الگوریتم و مشتقات آن توسط سازمانهایی نظیر گوگل، IBM، مایکروسافت و بسیاری از سازمانهای معتبر دیگر استفاده میشوند. این الگوریتم مقاوم بودن در برابر خطای Benign را فراهم می‌آورد. اما این الگوریتم اجماع نقایصی هم دارد. به عنوان مثال بوسیله یک کاربر ادمین کنترل میشود، قابل دستکاری شدن است، قابل استفاده توسط افراد با منافع متفاوت نیست، برای

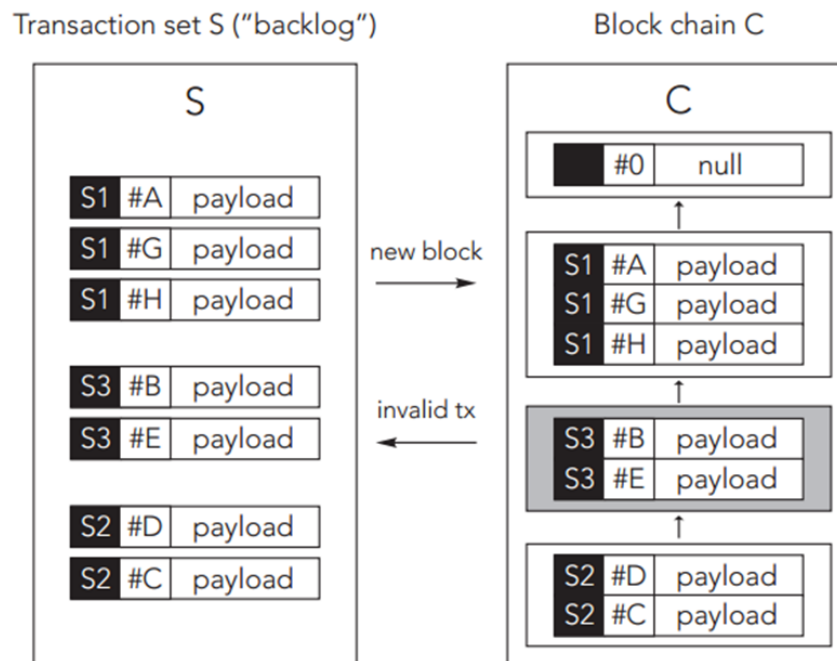


جلوگیری از حمله Sybil طراحی نشده است و بصورت همگانی در دسترس عموم قرار نگرفته است. در صورتی که بخواهیم پایگاه داده توزیع شده مبتنی بر زنجیره بلوک را ایجاد نماییم الگوریتم اجماع ارائه شده برای آن لازم است که ویژگیهای مقاوم بودن در مقابل خطاهای Bening, Beyzentine, Sybil و را داشته باشد.

در BigchainDB از پایگاههای داده توزیع شده استفاده شده است و سعی شده ویژگی های زیر که بر اساس زنجیره بلوک هستند به پایگاه داده توزیع شده اضافه شوند: کنترل غیر متمرکز، جاودانگی داده ها و ابلیت ایجاد و انتقال سرمایه

معماری پایگاه داده توزیع شده BigchainDB

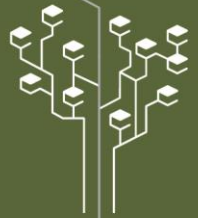
در این پایگاه داده API داده شده به کلاینتها به نحوی است که تصور میکنند تنها یک پایگاه داده زنجیره بلوک وجود دارد. اما در عمل دو پایگاه داده توزیع شده S(Transaction Set) و C(Block chain) وجود دارند که الگوریتم مبتنی بر Paxos خود را برای حفظ تطابق بین درایوها اجرا میکنند (تصویر ۴). دو پایگاه داده S و C از طریق الگوریتم اجماع زنجیره داده^{۱۷} با یکدیگر مرتبط هستند. BCA بر روی هر گره ثبت شده اجرا میشود. گره های ثبت نشده میتوانند به پایگاه داده زنجیره بلوک متصل شوند و بر اساس مجوزی که دارند میتوانند بخوانند، سرمایه ایجاد کنند، سرمایه منتقل کنند یا کارهای دیگر انجام دهند.



تصویر ۴- معماری پایگاه داده توزیع شده BigchainDB (Trent McConaghy, 2016)

پایگاه داده S حاوی مجموعه مرتب نشده ای از دستورهای انتقال است. وقتی یک دستور انتقال میرسد باید بوسیله گره

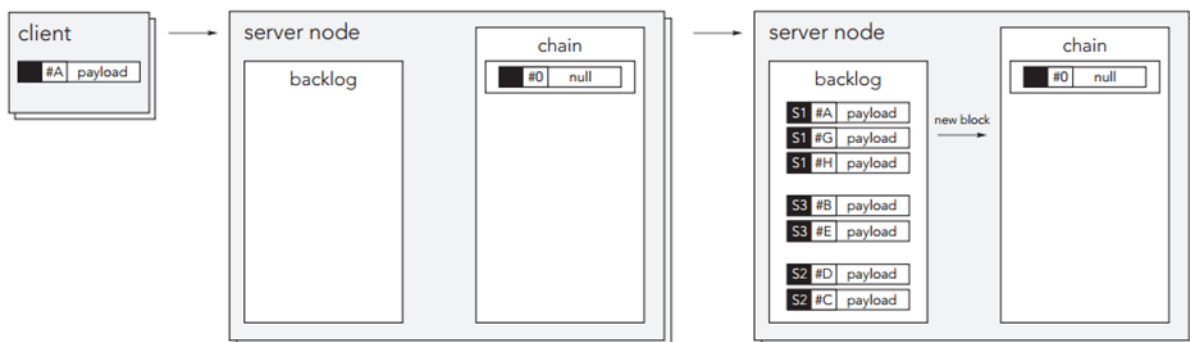
^{۱۷} BCA (BigchainDB Consensus Algorithm)



دریافت کننده تصدیق شود تا در S ذخیره شود. اگر N گره ثبت شده وجود داشته باشد مجموعه $S_k = \{t_{(k,1)}, t_{(k,2)}, \dots\}$ گره K مجموعه S_k را به شکل یک لیست مرتب در می‌آورد، یک بلوک از دستورات انتقال می‌سازد و بلوک را در پایگاه داده C قرار می‌دهد.

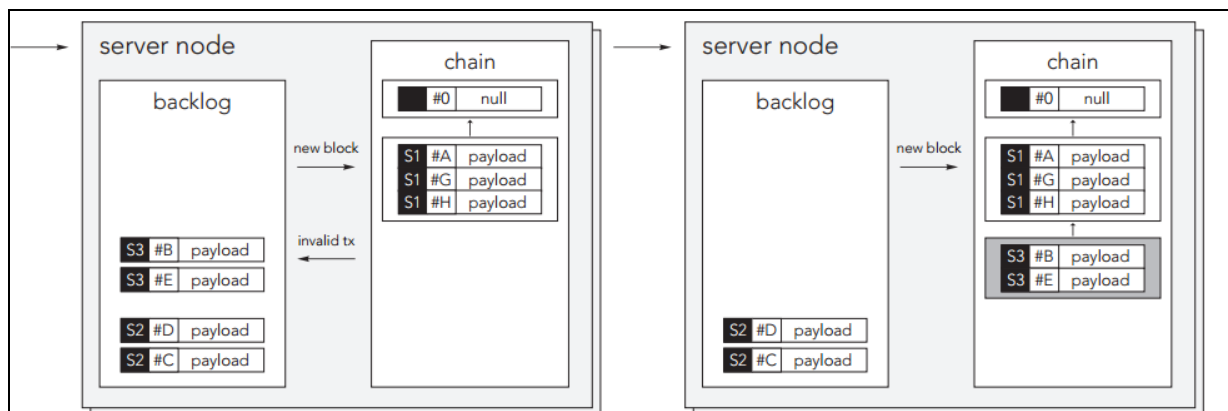
پایگاه داده C یک لیست مرتب شده از بلوکها است به نحوی که هر بلوک به یک بلوک بالاتر خود و محتوایش ارجاع دارد (یک زنجیره بلوک). هر گره ثبت شده میتواند رای دهد که یک بلوک معتبر است یا نه. اگر گره ثبت شده در یک بلوک هیچ دستور انتقال غیر معتبری پیدا نکند آن بلوک را معتبر اعلام میکند و در غیر اینصورت آن را غیر معتبر اعلام میکند. هر بلوک در آغاز در وضعیت تصمیم گیری نشده است و به محض اینکه اکثریتی از تصمیمات معتبر یا نامعتبر برای آن بلوک حاصل شد بلوک از وضعیت تصمیم گیری نشده به وضعیت تصمیم گیری شده معتبر یا نامعتبر می‌رود و تصمیم گیری در مورد بلوک خاتمه میابد. هر بلوک در زنجیره بلوک دارای شماره، برچسب زمانی، دستورات انتقال و اطلاعات رای گیری است.

عملکرد BigchainDB در تصویر ۵ توصیف شده است. هرکارت در این تصویر یک ماشین فیزیکی است. کلاینتها با سرورهای پایگاه داده زنجیره بلوک (گره های رای دهنده) ارتباط برقرار میکنند. کلاینت دستور انتقال با شماره $A\#$ و محتوای مشخص را به یکی از سرورها میفرستد و این سرور یا خودش دستور را تأیید میکند یا برای سروری دیگر میفرستد. هر سرور از مجموعه ای از دستورات انتقال یک بلوک می‌سازد.



تصویر ۵- نمایش عملکرد BigchainDB (Trent McConaghy, 2016)

گره $S1$ بلوک ساخته شده اش را به پایگاه داده C میفرستد. سپس تصمیم گیری بر روی معتبر بودن بلوکها در C آغاز میشود. تصمیم گیری بر روی یک بلوک در C زمانی شروع میشود که در مورد تمامی بلوکهای بالاتر از آن تصمیم گیری انجام شده باشد. در تصویر ۶ بلوک مربوط به $S1$ معتبر و بلوک مربوط به $S3$ نامعتبر است. در یک بلوک نامعتبر میتوانند دستورات انتقال معتبری هم باشند. بنابراین بلوک نامعتبر به $S3$ بازگرداننده میشود و یک شانس دیگر برای تصحیح و ارسال آن داده میشود.



تصویر ۶- نمایش چگونگی تصمیم‌گیری BigchainDB در مورد بلوکهای ورودی (Trent McConaghy, 2016)

الگوریتم اجماع در BigchainDB

دو الگوریتم اجماعی متداول در زنجیره بلوک عبارتند از تایید بر اساس کار (Proof of work (POW) و تایید بر اساس سهام (Proof of stake (POS). اما هر دو این الگوریتمها از نظر مقیاس پذیری با مشکل مواجه هستند. به همین دلیل در BigchainDB از الگوریتم اجماع فدراسیون (Federation) استفاده شده است. ویژگیهای الگوریتم اجماع فدراسیون به شرح زیر هستند:

- هر عضو فدراسیون رای مساوی با بقیه دارد.
- معمولاً دو سوم ارا برای رسیدن به تایید نیاز است.
- در هنگام رای دادن عضو باید هویت خود را آشکار کند.

تصمیم‌گیری در مورد لغو عضویت بر اساس تاریخچه رای‌های عضو در مطابقت با رای اکثریت دارد.

بنابراین علیرغم آنکه دو مکانیزم قبلی از نظر مقیاس‌پذیری با مشکل روبرو هستند ولی الگوریتم اجماع فدراسیون مقیاس‌پذیر بوده و میتواند نرخ بالای درخواستها را نیز بخوبی پاسخگو باشد و مدیریت نماید.

جمع‌بندی و نتیجه‌گیری

در این مقاله موارد مختلف بکارگیری زنجیره بلوک در پایگاههای داده توزیع شده بررسی شده اند. به عنوان مثال در SAFE از رمزآزایی مبتنی بر زنجیره بلوک برای پرداخت هزینه‌ها بین کاربران استفاده شده است و بدینوسیله پایگاه داده‌ای مستقل و بدون نیاز به ناظر انسانی ارائه شده است. درجایی دیگر (SPOOL) از زنجیره بلوک برای ذخیره جریان نقل و انتقال اطلاعات مربوط به حق مالکیت دارایی‌های دیجیتال استفاده شده است و بدین وسیله تلاش شده که راه کاری برای حفظ مالکیت معنوی دارایی‌های دیجیتال پخش شده در وب فراهم گردد. موارد دیگری نیز وجود دارند که هدف آنها برآورده نمودن امکانات بیشتری با استفاده از زنجیره بلوک بوده است و بنابراین به میزان بیشتری از این تکنیک استفاده نموده اند. برای مثال در Storj با بکارگیری زنجیره بلوک هم مشخصات کاربران و هم اطلاعات آنها محفوظ نگاه داشته میشود. یا در



BigchainDB تلاش گردیده است که ویژگی‌های خاص زنجیره بلوک نظیر کنترل غیر متمرکز، مقاوم بودن در مقابل حمله برای تغییر داده‌ها و قابلیت ایجاد و انتقال سرمایه بر روی شبکه بدون نظارت متمرکز را به پایگاه‌های داده توزیع شده اضافه نمایند. بنابراین بکارگیری تکنیک زنجیره بلوک در پایگاه‌های داده توزیع شده توانسته است هم زمینه‌های استفاده از آنها را افزایش داده و هم قابلیت‌های جدیدی را به آنها بیفزاید.

منابع

- [1] *Bittorrent sync*. (2014). Retrieved from <http://www.bittorrent.com/sync>.
- [2] Bruyn, A. S. (2017). *Blockchain, an introduction*.
- [3] Holtzman, D. M. (2015). *Towards An Ownership Layer for the Internet*. Retrieved from <http://trent.st/blog/2015/6/25/new-paper-towards-an-ownership-layer-for-the-internet.html>
- [4] Irvine, D. (2018). *A SAFE Network Primer*.
- [5] Martinovic, P. I. (n.d.). *Blockchains: Design Principles, Applications, and Case Studies*.
- [6] Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- [7] Nakamoto, S. (n.d.). *The creator(s) of bitcoin*. Retrieved from https://en.wikipedia.org/wiki/Satoshi_Nakamoto
- [8] Nick Lambert, Q. M. (2015). *Safecoin: The Decentralised Network Token*.
- [9] Shawn Wilkinson, J. L. (2014). *Metadisk: Blockchain-Based Decentralized File Storage Application*.
- [10] *Storj - decentralized cloud storage*. (2014). Retrieved from <http://storj.io/>
- [11] Swan, M. (2015). *Blockchain, Blueprint for a New Economy*.
- [12] Trent McConaghy, R. M. (2016). *BigchainDB: A Scalable Blockchain Database*.
- [13] Wilkinson, S. (2014). *Storj: A Peer-to-Peer Cloud Storage Network*.