

زنجیره بلوکی در فرماندهی و کنترل

مهدی دهقانی^{۱*}، جواد غریبی^۲

پذیرش مقاله: ۹۹/۰۶/۱۴

دریافت مقاله: ۹۹/۰۳/۲۹

چکیده

سامانه فرماندهی و کنترل شامل مجموعه‌ای از تجهیزات ارتباطی و رایانه‌ای است که به منظور تسهیل در تصمیم‌گیری و مدیریت صحنه نبرد استفاده می‌شود. در این سامانه، فرایند جمع‌آوری، پردازش و انتشار مداوم اطلاعات محیطی و برقراری و حفظ ارتباط بین اعضا، از اهمیت زیادی برخوردار است. این اطلاعات یک تصویر مناسب برای فرماندهی به منظور سازماندهی، هدایت، هماهنگی و کنترل نیروها فراهم می‌سازد. به خاطر حیاتی و حساس بودن این اطلاعات، انتقال سریع، صحیح و شفاف فرمان‌ها به سمت پایین زنجیره فرمان و برعکس، مستلزم برخورداری از یک زیرساخت امن و قابل اعتماد است. استفاده از فناوری‌های نوین مانند زنجیره بلوکی^۳ می‌تواند بسیاری از مخاطرات و چالش‌های امنیتی این سامانه را برطرف سازد. زنجیره بلوکی یک پایگاه داده غیرمتمرکز است که در یک محیط ناامن، با استفاده از رمزنگاری پیشرفته امنیت اطلاعات را تضمین می‌کند. در این مقاله ضمن بررسی این فناوری نوظهور، به بررسی نقش آن در تأمین امنیت و تسریع در انجام مأموریت‌های فرماندهی و کنترل پرداخته می‌شود. یافته‌های این تحقیق نشان می‌دهد، این فناوری با داشتن مزایایی از جمله سرعت عمل در شناسایی اهداف، امکان تعقیب هم‌زمان کلیه اهداف، پردازش، تلفیق و نمایش اطلاعات، تبادل سریع و خودکار اطلاعات، می‌تواند موجب کاهش خطای عملیاتی، قابلیت اطمینان بالا، واکنش سریع و کاهش تأخیر و وقفه در سامانه‌های فرماندهی و کنترل فراهم سازد.

واژگان کلیدی: زنجیره بلوکی، فرماندهی و کنترل، پایگاه داده، اقتصاد دیجیتال.

^۱. دکتری کامپیوتر و مدرس دانشگاه امام حسین (ع) drdeghani@ihu.ac.ir

^۲. دانشجوی دوره دوم دکترای دفاع سایبری، دانشگاه عالی دفاع ملی j.gharibi@sndu.ac.ir

^۳. Block Chain

مقدمه

فن‌آوری اطلاعات و ارتباطات و زیرمجموعه‌های اصلی آن نظیر سامانه‌های اطلاعاتی، رایانه‌ای و مخابراتی بخش مهمی از فرماندهی و کنترل را شامل می‌گردد یکی از بهترین تعریف‌هایی که می‌توان برای فرماندهی و کنترل به کاربرد، اعمال اختیار و هدایت از سوی یک فرمانده مشخص بر نیروهای مأمور برای تحقق مأموریت است. به عبارت دیگر کارکردهای مربوط به ترتیب بندی نیرو، تجهیزات، ارتباطات، تأسیسات و راه‌کارهای به کار گرفته شده توسط یک فرمانده در طرح‌ریزی، هدایت، هماهنگ‌سازی و کنترل نیروها و عملیات جهت تحقق کامل مأموریت (علمایی، ۱۳۸۴: ۱۷۲).

استفاده صحیح ما از تکنولوژی و شاید عدم اعتماد نهادها به یکدیگر باعث شده ما بتوانیم زیرساختی امن و مورد تأیید مانند زنجیره بلوکی به وجود آوریم که از کند شدن ما جلوگیری می‌کند و ما را نسبت به بانک‌ها، دولت‌ها، سازمان‌ها بی‌نیاز می‌کند. ما می‌توانیم تمام این عدم قطعیت‌ها را مهار کنیم و از آن برای همکاری و تبادلات هر چه بیشتر، سریع‌تر و آزادتر استفاده کنیم.

البته این بدان معنا نیست که تکنولوژی زنجیره بلوکی پاسخگوی تمام نیازهای ما است و راه حلی برای همه مشکلات ارائه می‌کند. شاید رسانه‌ها بگویند که زنجیره بلوکی می‌تواند قحطی در دنیا را ریشه‌کن کند، مشکل داروهای جعلی را برطرف کند و جنگل‌های بارانی ما را نجات دهد، ولی این تکنولوژی در دوران اولیه رشد خود است.

زنجیره بلوکی در موضوعات و صنایع گوناگون کاربردهای وسیعی دارد یکی از این موضوعات به‌کارگیری این فناوری در بخش نظامی است. سازمان ارتباطات و اطلاعات ناتو در حال ارزیابی پیشنهادی ارائه شده در چالش نوآوری (Innovation Challenge, 2016) است. این کار با هدف افزایش سرعت تحول و یافتن راه‌هایی برای حمایت از «NATO C4ISR» و توانایی‌های نیازهای سایبری صورت می‌گیرد. درخواست ناتو شامل بخشی با عنوان «کاربردهای نظامی زنجیره بلوکی»

است که شامل به کارگیری این فناوری در تدارکات نظامی، امور مالی و دیگر بخش‌هایی که آن کاربرد دارد، می‌شود.

ساده‌ترین تعریف برای زنجیره بلوکی، یک «فهرست دیجیتالی توزیع شده» است. زنجیره بلوکی یک پایگاه داده‌ی توزیع شده است که امکان انتقال اطلاعات از یک مکان به مکان دیگر را با امنیت بالا فراهم می‌کند. یکی از اصلی‌ترین ویژگی‌های این فناوری، قابلیت توزیع آن است؛ زیرا باعث می‌شود نسخه‌های متعددی از داده‌ها، درون چندین رایانه وجود داشته باشد. این رایانه‌ها یک شبکه هم‌تا به هم‌تا را شکل می‌دهند. به این معنی که هیچ پایگاه داده یا سرور مرکزی وجود نداشته و هر ماشین به عنوان گره‌ای از شبکه، ایفای نقش می‌کند.

مارک اندرسون، مؤسس شرکت خدمات رایانه‌ای «نت اسکایپ» درباره‌ی زنجیره بلوکی می‌گوید: «زنجیره بلوکی روشی برای کاربران اینترنتی است تا قطعه‌ای از دارایی‌های دیجیتالی یکتای خود را به دیگر کاربران انتقال بدهند. این انتقال تضمین شده، امن است و هیچ‌کس نمی‌تواند مشروعیت آن را به چالش بکشد.»^۱

زنجیره بلوکی هنوز نیازمند تجربیات و سعی و خطاهای بیشتری برای بلوغ است تا کاربردهای حقیقی آن در اقتصاد آشکار شود. ولی آنچه واضح است، کار و تلاش افراد زیادی برای توسعه و رشد این سیستم است. نهادهای مالی، شرکت‌های تکنولوژی و دانش بنیان و دانشگاه‌ها در حال کار روی این ایده جدید برای تحول نظام اقتصادی هستند.

عملیات اطلاعاتی

در حال حاضر، فناوری اطلاعات باعث توسعه مؤثر سلاح‌های هوشمند، کاهش تلفات نیروهای خودی و نفوذ و اختلال در سامانه‌های اطلاعاتی طرف مقابل شده است. کشورها و ارتش‌های مختلف با استفاده از فناوری اطلاعات، سامانه C4I و جنگ اطلاعات به فناوری‌ها و صنایع پیشرفته‌ای دست پیدا کرده‌اند (فرماندهی و کنترل ۱۳۸۴).

^۱. coindesk.com/information/what-is-blockchain-technology

یکی از تبعات منفی جنگ اطلاعات، استفاده سازمان‌های تروریستی از آن است. این افراد با استفاده از فناوری اطلاعات و بدون به خطر انداختن خود می‌توانند از راه دور و در محیطی امن، عملیات خرابکارانه‌ای را بر علیه اهداف مورد نظر اطلاعاتی انجام دهند. به عنوان مثال، بجای ربودن یک هواپیما و به مخاطره انداختن خود، می‌توانند با نفوذ در سامانه‌های امنیتی و رایانه‌ای برج کنترل یک فرودگاه و ایجاد اختلال در آن، پرواز ده‌ها هواپیما را مختل نمایند. این حوزه نزاع نوظهور که مهاجمین می‌توانند از فضای اطلاعاتی استفاده نموده و بر عملیات نظامی استراتژیک و زیرساخت‌های ملی یک کشور اثر گذاشته و به تخریب آن‌ها بپردازند، به جنگ اطلاعات ماهیت استراتژیک داده است و امروز به یکی از مباحث مهم در حوزه دفاعی و غیر دفاعی دنیا تبدیل شده است (جوانمرد ۱۳۸۴).

آسیب‌شناسی سامانه‌ها و شبکه‌های اطلاعاتی C4I

سامانه‌ها (سیستم‌ها) و شبکه‌های اطلاعاتی در معرض چهار آسیب عمومی قرار دادند (دیزاستر رکاوری، ۲۰۰۲):

الف) دستیابی غیرمجاز به داده‌ها: با به دست آوردن داده‌های حساس (طبقه‌بندی شده یا طبقه‌بندی نشده) یا مرور یک فایل حساس که روی یک رایانه C4I ذخیره شده است، ممکن است دشمن بتواند اطلاعاتی را کسب نماید که مخل امنیت ملی است.

ب) تغییر نادرست داده‌ها: بدین وسیله دشمن می‌تواند یک طراح نظامی را فریب دهد یا مانع از اجرای یک طرح شود برای مثال، تغییر اطلاعات لجستیکی مشخصاً می‌تواند آرایش نیرو را به هم بریزد، یعنی اگر دسته‌های سربازان یا آذوقه و تدارکات را به مقصد نادرستی تغییر مسیر دهد یا نیازمندی‌های آن‌ها را حذف کند، در کارهایشان اختلال ایجاد کرده است.

ج) جعل هویت: دشمن با جای دادن مخفیانه خود به جای یک کاربر مجاز می‌تواند فرامین نادرست صادر کند، اطلاعات پایگاه داده‌ها را به نفع خود تغییر دهد یا احکام غیرمجازی برای فرماندهان صادر کند. برای مثال، دشمنی که به سیستم پردازش حقوق ارتش دست یافته، می‌تواند تأثیر عمیقی بر روی روحیه نظامیان بگذارد.

د) از کار انداختن سرویس یا حاشا کردن آن: با انکار یا ایجاد تأخیر در دستیابی به سرویس‌های الکترونیکی، دشمن می‌تواند طرح و اجرای عملیاتی را که زمان در آن یک عامل بحرانی و پراهمیت است، مختل کند. به‌عنوان مثال حمله‌ای که موجب غیر دسترس کردن سامانه اطلاعاتی وضعیت آب و هوا می‌شود. می‌تواند طرح یک عملیات نظامی را به تأخیر اندازد. همچنین حمله‌ای که موجب از کار افتادن سامانه موقعیت‌یاب جهانی خودی شود، در شناسایی موقعیت نیروها ایجاد اشکال می‌کند و موجب گمراهی آن‌ها می‌شود. به نظر بسیاری از کارشناسان، از کار انداختن سرویس جدیدترین نوع آسیب است، زیرا به آسانی انجام می‌گیرد و رفع آن، نیاز به پیچیدگی‌های تکنیکی نسبتاً کمی دارد. انواع حملاتی که سیستم‌های C4I با آن مواجه‌اند، بسیار گسترده‌تر و جدی‌تر از حملاتی است که سیستم‌های غیرنظامی و تجاری را تهدید می‌کند، زیرا حملاتی که به سیستم C4I می‌شود، قسمتی از حمله‌ای است که توسط یک دولت یا حکومت بیگانه برانگیخته شده و می‌تواند بر اساس منابعی باشد که به صورت مجاز و قانونی صرف حمله شده است، به‌علاوه مرتکبان، اغلب از جانب حکومت بیگانه‌ای حمایت می‌شوند و از برخی منفعت‌های قانونی بهره می‌برند.

زنجیره بلوکی چیست؟

تکنولوژی زنجیره بلوکی یک پایگاه داده غیرمتمرکز است که به صورت ایمن، بین چندین سازمان تقسیم‌شده است و هیچ فرد یا گروهی نمی‌تواند آن را به صورت انحصاری تحت کنترل داشته باشد و در آن، لیست دارایی‌ها و معاملات بر روی یک شبکه نظیر به نظیر (peer-to-peer) نگه‌داری می‌شود. در واقع یک دفتر ثبت اسناد عمومی است که در آن مشخص می‌شود هر شخص چه مقدار دارایی دارد و چه معاملاتی را تا به حال انجام داده است.

منظور از غیرمتمرکز بودن این پایگاه داده، این است که داده‌ها بر روی یک سرور مرکزی نگهداری نمی‌شوند. در این سیستم امنیت مبادلات توسط علم رمزنگاری کامپیوتری تأمین می‌شود و در طول زمان، تاریخچه معاملات در بلوک‌هایی از داده، قفل و نگه‌داری می‌شوند. بلوک‌هایی که به صورت رمزنگاری شده باهم مرتبط شده و ایمن می‌شوند. این سیستم یک نمونه غیرقابل تغییر و فراموشی

از تمام دارایی‌ها و مبادلات را بر روی شبکه خود به وجود می‌آورد. این نمونه بر روی تمامی رایانه‌هایی که از این شبکه استفاده می‌کنند تکرار می‌شود.

زنجیره بلوکی، یک App یا یک شرکت نیست. شاید شبیه‌ترین نمونه از این سیستم به لحاظ توضیح ویکی‌پدیا باشد. ما می‌توانیم همه‌چیز را روی ویکی‌پدیا ببینیم. مطالب روی آن همواره در حال به‌روزرسانی و تغییر هستند. ما می‌توانیم سابقه تغییرات مطالب را روی ویکی‌پدیا در گذر زمان مشاهده کنیم. ما حتی می‌توانیم ویکی‌های خودمان را روی ویکی‌پدیا ایجاد کنیم. همه این امکانات به خاطر این است که هسته ویکی‌پدیا یک زیرساخت داده است. یک زیرساخت داده متن‌باز که مطالب، عکس‌ها و تغییرات آن‌ها را در طول زمان نگهداری می‌کند.

زنجیره بلوکی یک زیرساخت آزاد است که می‌توانید روی آن دارایی‌های مختلف را نگه‌داری کنید. این زیرساخت تاریخچه حضانت این دارایی‌ها، مالک و مکان دارایی‌ها را نیز ذخیره می‌کند. این دارایی‌ها می‌تواند یک پول دیجیتال مانند بیت کوین یا دارایی‌های دیجیتال دیگر مانند عنوان مالک، آدرس IP او، یک قرارداد یا گواهی‌نامه، اشیاء حقیقی دنیای ما یا حتی اطلاعات تشخیص هویت باشد.

اطلاعات فنی زیاد دیگری در خصوص زنجیره بلوکی وجود دارد، ولی هسته آن این‌گونه کار می‌کند. دفتر اسناد رسمی عمومی که مبادلات را در بر روی یک شبکه نگه‌داری می‌کند و با تکرار این اسناد بر روی کامپیوترهای مختلف استفاده‌کننده از این شبکه امنیت داده‌ها را بالا می‌برد تا دست بردن در آن‌ها بشدت سخت شود.

به‌طور خلاصه زنجیره بلوکی را یک پایگاه داده به اشتراک گذاشته شده می‌نامیم. هر چیزی که به این پایگاه داده اضافه شود، یک رکورد جدید است. این پایگاه داده مشترک، در واقع انقلابی در فناوری است که به دنبال شکل‌گیری آینده ما است. برای روشن شدن مطلب، این فقط یک پایگاه داده نیست که در یک مکان مرکزی ذخیره شده باشد و توسط بسیاری از افراد به اشتراک گذاشته شده باشد، هزاران نسخه از این اطلاعات ثبت شده در کامپیوترهای سراسر جهان ذخیره می‌شود

در کامپیوترهای خانگی و سرورهای تجاری)، از این رو اصطلاح «غیرمتمرکز» به آن نسبت داده می‌شود.

زنجیره بلوکی چگونه کار می‌کند؟

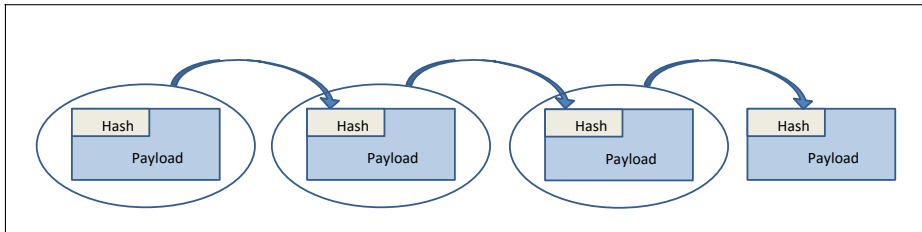
تابع هش^۱ یک تابع یک طرفه است که ورودی با اندازه‌های مختلف را می‌گیرد و آن را به خروجی به یک اندازه ثابت تبدیل می‌کند و در هش‌های مبتنی بر رمزنگاری امکان رسیدن به ورودی از خروجی این تابع بسیار سخت یا تقریباً غیرممکن است. مثل sha1 و MD5 و sha2

► $MD5("abc") = 900150983cd24fb0d6963f7d28e17f72$

در اینجا خروجی ۱۲۸ بیت است که به صورت هگز نمایش داده شده است.

اگر مقدار یک هش به عنوان ورودی یک تابع هش دیگر استفاده شود، یک هش جدید بدست می‌آید که اگر این فرایند تکرار شود و نتایج ترکیب شود در دنباله‌ای از هش‌ها یک **hashchain** بدست می‌آید.

هش در هر زنجیره بلوکی با یک تابع ریاضی خاص به دست می‌آید که توسعه دهندگان آن را مشخص می‌کنند. کوچک‌ترین تغییر در اطلاعات یک بلوک، هش آن را به طور کلی تغییر می‌دهد. مثلاً اگر یک کاراکتر به اطلاعات اسم شهرهای ایران اضافه شود، هش بلوک تغییر می‌کند و در نتیجه بلوک‌های بعدی هم غیر معتبر خواهند شد؛ به همین دلیل این فناوری زنجیره بلوکی یا زنجیره بلوک‌ها نام دارد.



شکل ۱: زنجیره بلوکی هش

^۱ . HASH FUNCTIONS

هر تراکنش یک کد هش^۱ ۶۴ کاراکنتری تولید می‌کند. این کد با کد هش قبلی ترکیب می‌شود تا یک بلوک جدید ایجاد کند. آجای ویج^۲ معاون مدیر و رئیس بخش خدمات مالی شرکت اینفوسیس^۳ می‌گوید: «هر بلوک با استفاده از بلوک‌های جدید، یک ترتیب خطی، زمانی و رشته کاراکترهای یک‌بار مصرف، تولید می‌شود. به همین دلیل دستکاری و ایجاد اطلاعات نادرست و غیرقابل ردیابی، تقریباً غیرممکن است.» در حال حاضر سامانه‌های اداری و بانک‌ها در معرض جرائم سایبری قرار دارند؛ اما زنجیره بلوکی می‌تواند جلوی همه‌ی آن‌ها را بگیرد. زنجیره بلوکی می‌تواند با استفاده از جایگزین کردن پردازش‌های موجود پیچیده، تمام تراکنش‌های انجام شده را ضبط و نگهداری کند. دیو ریسیزین^۴ مدیر بخش فناوری و راهبردهای شرکت انگلیسی هدلانندن^۵ گفت: «زنجیره بلوکی، پایگاه داده‌هایی است که محیط امن یکپارچه‌هایی را در محیط‌های ناامن ایجاد می‌کند. به این معنا که تمام اطلاعات معاملات انجام شده در هر صنعتی را ذخیره می‌کند. می‌توان از این فناوری در زمینه‌های مالی، حسابرسی، پزشکی و صنعتی نیز استفاده کرد.»

✓ ایجاد هویت دیجیتال

طبق راهنمای ما «فناوری زنجیره بلوکی چگونه کار می‌کند»، ایجاد **identity** یا هویت در فن‌آوری زنجیره بلوکی از طریق استفاده از کلیدها، رمزنگاری انجام می‌شود. ترکیب کلیدهای عمومی و خصوصی باعث ایجاد یک هویت دیجیتالی قوی که مالکیت را تأیید می‌کند، می‌شود. یک کلید عمومی، شما را در بین افراد مختلف شناسایی می‌کند (مانند یک آدرس ایمیل). کلید خصوصی چگونگی تمایل شما برای انجام تراکنش است. اصول رمزنگاری یک مهم در انقلاب زنجیره بلوکی است.

1. Hash

2. Ajay Vij

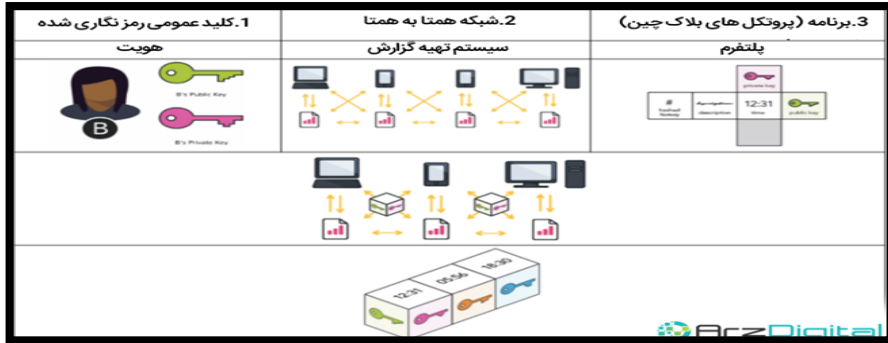
3. Infosys

4. Dave Hryciszyn

5. HeadLondon



شکل ۲: شکل گیری امضای دیجیتال



شکل ۳: بلاک چین ها از ۳ تکنولوژی مختلف ایجاد شده اند

✓ اثبات غیرقابل تغییر بودن داده‌ها

یکی از ویژگی‌های اصلی پایگاه داده زنجیره بلوکی، داشتن تاریخچه در خودش است. به همین دلیل آن‌ها اغلب نامرئی نامیده می‌شوند؛ به عبارت دیگر، برای تغییر داده‌های ورودی در پایگاه داده زنجیره بلوکی، روند بسیار سختی (تقریباً غیرممکن) وجود دارد، زیرا نیاز به تغییر تمام اطلاعات بعد از آن گره (که قرار است تغییر داده شود) است. به این ترتیب، این یک سیستم تهیه گزارش بسیار بهتر و قوی‌تر از یک پایگاه داده معمولی است. زنجیره بلوکی‌ها از یک تکنولوژی جدید ساخته نشده‌اند. آن‌ها از ترکیب سه تکنولوژی جداگانه و منحصر به فرد ایجاد شده‌اند.

کاربردهای زنجیره بلوکی

زنجیره بلوکی به اینترنت یک هویت قطعی می‌دهد، زنجیره بلوکی یک فناوری جدید و پروتکلی اینترنتی است که در تراکنش‌های مالی آنلاین به کار گرفته می‌شود، اما می‌توان موارد استفاده‌ی دیگری نیز برای آن پیدا کرد. ریچارد مولدز^۱ مدیر ارشد شرکت امنیت الکترونیکی تیلز^۱ گفت: «زنجیره بلوکی می‌تواند اعتماد مردم به اینترنت را افزایش دهد؛ به عنوان مثال می‌تواند علاوه بر

^۱. Richard Moulds

متصل کردن اشیا به یکدیگر و اینترنت، رابطی برای تراکنش‌های مالی بین مردم و اشیا مختلف نیز باشد.» در حالی که عده‌ی زیادی فکر می‌کنند، تنها کاربرد زنجیره بلوکی، استفاده در بیت کوین است.

این فناوری در سال گذشته با مبلغ ۱ میلیارد دلار، بیشترین سرمایه‌گذاری روی یک فناوری نوظهور را به خود اختصاص داده است. زنجیره بلوکی طراحی شد تا جلوی کلاهبرداری در معاملات گرفته شود. این فناوری یک پایگاه داده‌ی توزیع شده است که هر کسی می‌تواند در آن اعتبار معاملات را بررسی کند. (فناوری زنجیره بلوکی تقریباً مانند امضای دیجیتال عمل می‌کند. گرت استیفنز^۲ رئیس بخش توسعه طرح‌ها در شرکت انگلیسی جمع‌آوری اطلاعات جی.بی. جی^۳ گفت: زنجیره بلوکی یک سیستم عامل توزیع شده است که امکان انتقال اطلاعات از یک مکان به مکان دیگر را با امنیت بالا فراهم می‌کند). زنجیره بلوکی یک فناوری متن‌باز است و کسی صاحب آن نیست، این فناوری یک مجری مرکزی برای تأیید تراکنش‌های انجام شده ندارد و به صورت خودکار شبکه را تنظیم می‌کند. استیفنز می‌گوید: «در حقیقت نکته اصلی فناوری زنجیره بلوکی، قدرت بسیار بالای تنظیم خودکار آن است.»

الف) زنجیره بلوکی در اقتصاد دیجیتال:

از این پایگاه داده می‌توان برای ثبت اطلاعات مختلفی استفاده کرد؛ به عنوان مثال اولیه بسیاری از آن برای ارسال و دریافت پول استفاده می‌کنند، همان‌طور که در حال حاضر رایج‌ترین کاربرد آن است.

هنگامی که دو نفر بخواهند برای یکدیگر پول انتقال بدهند، یک رکورد جدید ایجاد می‌شود که جزئیات آن تراکنش را مشخص می‌کند. این رکورد به صدها نفر از رایانه‌های دیگر که دارای یک کپی از رکورد هستند، ارسال می‌شود. این کامپیوترها تأیید می‌کنند که این معامله مجاز است و در نهایت آن‌ها قبل از تأیید رکورد، موافقت یا مخالفت می‌کنند که همه‌چیز در مورد معامله، مشروع

1. Thales e-Security

2. Gareth Stephens

3. GBG

است. این کار باید با همه رونوشت‌های اطلاعات مطابقت داشته باشد. به نظر می‌رسد که چند صد نفر در کنار این دو، ناظر این هستند که نفر اول پول را به نفر دوم می‌دهد و همه آن‌ها موافقت کردند که نفر دوم واقعاً پولش را به دست آورده و دیگر جنبه‌های معامله، مانند اینکه مقدار آن هم درست است را چک می‌کنند.

چگونه این عملیات با یک بانک متفاوت است؟

نبوغ این پایگاه داده این است که نیازی به هیچ بانک یا شرکت مرکزی ندارد و شما مجبور نیستید به هیچ موسسه مالی اعتماد کنید. نیازی به هیچ واسطه‌هایی نیست.

اگر بخواهیم بیشتر توضیح دهیم، این پایگاه داده متعلق به هیچ فرد یا سازمانی نیست. این اطلاعات متعلق به همه افرادی است که یک کپی از آن اطلاعات را دارند؛ اما این بدان معنا نیست که هر یک از افرادی که دارای کپی هستند، کنترل دارند.

علاوه بر این، ما این پایگاه داده را «تغییرناپذیر» می‌نامیم یا به‌طور عام آن را غیرقابل برگشت می‌دانیم. هر داده‌ای که ساخته شده است تا زمانی که اینترنت هست، به‌طور دائم وجود خواهد داشت. حال اگر نفر دوم بخواهد پول نفر اول را پس بدهد، این یک داده‌ی جدید است.

به خاطر تصمیمات مربوط به طراحی فناوری، دست بردن در داده‌های این پایگاه داده غیرممکن است. اگر شخصی که یک یا چند نسخه از این اطلاعات را در رایانه‌های خود داشته باشد و سعی کند به‌طور غیرقانونی آن را تغییر دهد، آن تغییرات توسط بسیاری از رایانه‌های دیگر در روند تأیید این تغییرات، رد می‌شود و داده‌ها باهم تطابق نخواهند داشت. اگر بانک وجود نداشته باشد، پس پول در کجا ذخیره می‌شود؟

یکی از بخش‌های چالش برانگیز این است که زمانی که ما در مورد پول دیجیتال، مانند بیت کوین^۱ صحبت می‌کنیم، هیچ مخزنی از سکه وجود ندارد. این مورد در پایگاه داده به عنوان پول شناخته می‌شود. زنجیره بلوکی عدم قطعیت را کاهش می‌دهد و سیستم‌های اقتصادی را متحول می‌کند، عدم قطعیت یک مشکل بزرگ در اقتصاد است. معمولاً ۳ فرم مختلف از عدم قطعیت در

^۱. Bitcoin

تراکش‌ها و مبادلات روزانه ما وجود دارد که با آن روبرو می‌شویم و زنجیره بلوکی می‌تواند نقشی در برطرف کردن آن‌ها داشته باشد.

۱) عدم قطعیت در خصوص شخصی که با آن معامله می‌کنیم.

۲) شفاف نبودن معامله‌ای که انجام می‌دهیم.

۳) نبودن چاره در زمانی که اشتباهی در معامله رخ می‌دهد.

تکنولوژی زنجیره بلوکی به ما این امکان را می‌دهد تا یک سامانه جهانی و آزاد ایجاد کنیم و بر روی آن گواهی‌های هر شخص حقیقی یا حقوقی از هر منبعی را نگهداری کنیم.

این قابلیت به ما این امکان را می‌دهد یک سیستم تصدیق هویت دستی (پرتابل) تحت کنترل کاربران ایجاد کنیم. این بدان معناست که شما می‌توانید اطلاعات مختلف هویتی خود را به صورت انتخابی نمایان سازید که این کار منجر به تسهیل تجارت و معامله می‌شود. برای مثال اینکه شناسنامه ارائه شده توسط دولت به شما مشخص می‌کند که سن شما بالای ۲۱ سال است. با نمایش این گواهی‌های تصدیق شده به شیوه رمزنگاری دیجیتال و اعتمادسازی نسبت به صحت این اطلاعات در دنیای واقعی و مجازی، ما می‌توانیم انواع مختلف تجارت را به شیوه‌ای جدید دنبال کنیم.

دومین معضل مورد بحث، وجود شفافیت در معاملات و ارتباطات است با کمک تکنولوژی زنجیره بلوکی ما می‌توانیم یک واقعیت را بین نهادهایی که به هم اعتماد کامل ندارند به اشتراک بگذاریم. تمام گره‌های روی شبکه زنجیره بلوکی نیاز ندارند که یکدیگر را بشناسند و به هم اعتماد داشته باشند، زیرا هرکدام از آن‌ها این قابلیت را دارد که زنجیره بلوکی را مانیتور و تأیید کند. برای درک بهتر این قضیه دوباره به شیوه کارکرد ویکی‌پدیا فکر کنید، سایتی که در واقع یک زیرساخت پایگاه داده اشتراک یافته بین کاربران است که خوانندگان و نویسندگان زیادی در آن واحد روی آن فعالیت می‌کنند تا یک واقعیت یکتا را روی آن به وجود بیاورند و ثبت کنند.

ما می‌توانیم این کار را در زنجیره بلوکی هم انجام دهیم. ما می‌توانیم یک پایگاه داده غیرمتمرکز بسط یافته ایجاد کنیم که تمام مزایای یک سیستم با سرور مرکزی را داشته باشد و در عین حال

شامل یک نهاد مرکزی برای کنترل آن نباشد. این برای مصرف کنندگان به معنای سطح‌های جدیدی از شفافیت است. همان‌طور که اشیاء فیزیکی دنیای واقعی ما نقل و مکان می‌شوند، ما می‌توانیم یک گواهی دیجیتال یا یک جز (توکن) الکترونیک را روی زنجیره بلوکی جابجا کنیم.

ب) آینده دموکراسی

در MiVote.org.au از این فناوری مشترک برای رأی‌گیری استفاده شده است. در واقع، بیت کوین (که نشان دهنده ارز هستند) را با نشانه‌هایی از خودمان که نماینده‌ی آرا است، جایگزین کرده‌اند. به جای هزینه کردن بیت کوین، شما رأی می‌دهید. همان مزایایی که ما با سکه‌های دیجیتال می‌بینیم، برای این آرا وجود دارد: اعتبار و مشروعیت آن‌ها توسط رایانه‌های بسیاری از مردم تأیید شده است و داده‌های رأی‌گیری هرگز نمی‌تواند مورد سوءاستفاده قرار گیرد. این آرا با همان نتیجه، برای همیشه وجود دارد.

ج) آینده موسیقی با زنجیره بلوکی

چقدر خوب می‌شود اگر هنگام باز کردن یک برنامه مانند اسپاتیفای^۱ به جای اینکه اسپاتیفای هزینه هنری را از شما بگیرد تا حق امتیاز را به هنرمند پرداخت کند، به‌طور مستقیم به هنرمند پرداخت کنید. به عنوان مثال، هنگامی که شما در ثانیه ۳۵ ام یک آهنگ هستید، یک یا دو سنت به‌طور مستقیم از حساب مالی شما به هنرمند پرداخت شود. مقدار آهنگی که شما گوش کرده‌اید و آنچه شما پرداخت کرده‌اید، توسط بسیاری از رایانه‌های دیگر تأیید شده است و در پایگاه داده‌ها ثبت شده است *Ujo music* و *Voise* از این تکنولوژی استفاده می‌کنند.

د) آینده ذخیره‌سازی فایل

به جای اینکه فایل‌های خود را در سرورهای *Dropbox* یا *Onedrive* ذخیره کنید، تصور کنید که فایل شما بتواند به قطعات کوچک تقسیم شده و در هزاران یا میلیون‌ها کامپیوتر در سراسر جهان ذخیره شود. اینکه چه بخشی از فایل‌ها مال شما است و هر بخش در کجا ذخیره شده است،

1. Spotify

قابل تغییر نیست. فقط شما کلید مشاهده قطعات به عنوان یک فایل کامل را دارید و هیچ سازمانی اطلاعات شما را ندارد.

ه) آینده انرژی

تصور کنید یک کشور پر از خانه‌های مجهز به باتری‌های تسلا^۱ قابل شارژ^۱ که برق منزل را تأمین می‌کند است که به جای جدا بودن از شبکه، آن‌ها به شبکه وصل هستند؛ اما آن‌ها به تولیدکننده انرژی، پولی پرداخت نمی‌کنند. در واقع، در این آینده هیچ نیازی به این تولیدکننده‌های انرژی‌های سنتی وجود ندارد. در عوض، خانه‌ها به‌طور خودکار انرژی تولید و ذخیره می‌کنند و بر اساس آنکه کدام همسایه‌ها نیاز به برق اضافی دارند و کدام خانه‌ها بیش از حد انرژی در باتری‌های خود دارند، برق را با خود تبادل می‌کنند. به خاطر وجود زنجیره بلوکی این کار دیگر تخیلی نیست. از استرالیا تا نیویورک همه از این نوع مدل استفاده می‌کنند. شایان ذکر است با توجه به کاربردهای مختلف ذکر شده‌ی فوق، حضور زنجیره بلوکی در دنیای فناوری امروز به اینجا ختم نمی‌شود و به گونه‌ای همین خدمات موجب تغییر اساسی در صنایع شده است که لازم دانستیم بدان‌ها نیز بپردازیم:

پنج صنعتی که با روی کار آمدن زنجیره بلوکی زیر و رو می‌شوند

کاربردهای زنجیره بلوکی از نظر عموم به بیت‌کوین یا همان ارز دیجیتال محدود می‌شود. حال آن که این فناوری نوظهور قابلیت‌های چشم‌گیرتری دارد. تکنولوژی زنجیره بلوکی توانایی منحصر به فردی برای ایجاد یک تغییر و تحول اساسی در جهان دارد. در واقع، زنجیره بلوکی یک پایگاه داده‌ی باز برای تعاملات مالی است و امکانات بی‌شمار آن می‌تواند در حین کارآمدی، ایمنی و سرعت را هم فراهم کند. در ادامه به معرفی ۵ صنعتی خواهیم پرداخت که با ورود زنجیره بلوکی متحول خواهند شد:

^۱. Tesla Powerwall

۱. شبکه‌های انرژی

زنجیره بلوکی برای این معضل هم راه‌حلی دارد. در حال حاضر، در بخش بروکلین و مناطق مجاور آن، شبکه‌های هوشمندی در حال آزمایش است؛ به این ترتیب شهروندان این مناطق که از پنل‌های خورشیدی استفاده می‌کنند، می‌توانند با کمک زنجیره بلوکی، انرژی را طی قراردادهای هوشمند خرید و فروش کنند.

تمام این تراکنش‌های مالی توسط زنجیره بلوکی تأیید و ایمن می‌شود و نیاز به هیچ شرکت نیروگاهی واسطه‌ای در این میان وجود ندارد؛ بنابراین قیمت‌ها کاهش پیدا می‌کند و از طرفی دیگر بازدهی زیاد می‌شود.

۲. بنگاه‌های معاملات املاک

هر کسی که قصد خرید یا فروش ملکی را داشته باشد، گذر او به بنگاه‌های املاک می‌افتد. در حالی که زنجیره بلوکی این پتانسیل را دارد که معاملات مربوط به ملک را به صورت آنلاین و امن ارائه دهد. به این ترتیب، فروشندگان می‌توانند عملیات انتقال سند را انجام دهند و خریداران هم از طریق ارز رمزگذاری شده اقدام به پرداخت پول کنند. از طرفی زنجیره بلوکی می‌تواند در خصوص ارسال سوابق مالکیت به سازمان‌های دولتی هم مؤثر باشد.

۳. بخش درمانی

زنجیره بلوکی می‌تواند پایگاه داده‌ای از تمامی اطلاعات مربوط به سلامت ما مانند نسخه‌های پزشکی، عکس‌های رادیولوژی، ویزیت‌های اورژانسی و اطلاعات بیمه‌ای تهیه کند. تقریباً وضعیت سلامت هر شخص در طول زندگی‌اش با تغییراتی همراه است. با زنجیره بلوکی می‌توان شرایطی را تصور کرد که اطلاعات سلامتی فرد از بدو تولد تا پایان عمر او ثبت شود.

از طرفی، این سیستم می‌تواند زندگی شما را نجات دهد؛ زیرا پزشکان اورژانس مجاز هستند تا به اطلاعاتی نظیر آلرژی‌ها، نوع گروه خون و حتی اطلاعات ژنتیکی شما دسترسی داشته باشند تا در شرایطی که قادر به توضیح نیستید، تصمیمات آگاهانه‌تری بگیرند. این سیستم می‌تواند در بهبود وضعیت سلامت در کشورهای در حال توسعه که به پایگاه داده‌های دیجیتالی دسترسی ندارند،

انقلاب ایجاد کند. در اوایل سال جاری، پنج گروه مراقبت‌های بهداشتی اقدام به اجرای آزمایشی این برنامه کرده‌اند.

۴. حمل و نقل

زنجیره بلوکی پتانسیل‌هایی در خصوص فعال کردن اینترنت اشیا در شهرهای هوشمند دارد. علائم خیابانی، چراغ‌های راهنمایی، اتومبیل‌ها و دیگر اشیای متحرک و ساکن می‌توانند به سنسورهایی مجهز شوند تا داده‌های مربوط را جمع‌آوری و ارسال کنند. به این ترتیب، اتوبوس‌ها، ترامواها، وسایل نقلیه‌ی اورژانسی و دیگر خودروها می‌توانند سریع‌ترین مسیر را پیدا کرده و از ایجاد ترافیک اجتناب شود. نتیجه نهایی چه خواهد شد؟ شلوغی کم‌تر، رفت و آمد سریع‌تر و کاهش انتشار کربن؛ از طرفی، زنجیره بلوکی می‌تواند به رانندگان کمک کند تا محل مناسب برای پارک اتومبیل خود را پیدا کنند و گزارش‌های مربوط به تصادفات یا ایرادات اتومبیل را گزارش دهند.

۵. آموزش

هم‌زمان که دوره‌های آموزشی آنلاین^۱ در جهان رشد پیدا کرده و فراگیر شده است، نیاز به سیستمی وجود دارد که بتواند سوابق تحصیلی دانش‌آموختگان این دوره‌ها را ثبت کند. زنجیره بلوکی می‌تواند امکانی را به وجود آورد که افراد، مدرک معتبر خود را دریافت کنند و امکان جعل این مدارک وجود نداشته باشد. به این ترتیب، تمام این گواهینامه‌های پایان دوره می‌توانند توسط زنجیره بلوکی ذخیره شوند و به راحتی به کارفرمایان و سایر موسسات دانشگاهی ارسال شوند. این قابلیت به تقویت و اعتبار سازمان‌های آموزشی غیرانتفاعی کمک می‌کند و به کارفرمایان اطمینان می‌دهد که افراد مناسب را برای استخدام انتخاب می‌کنند.

بسیاری از صنایع اثرات مثبت زنجیره بلوکی را احساس خواهند کرد. برخی از آن‌ها سریع‌تر به این درک می‌رسند و بعضی دیگر به تدریج متوجه اهمیت آن خواهند شد. فرصت‌های پیش روی آینده بی‌شمار هستند. با این حال، سخت‌ترین بخش مربوط به زنجیره بلوکی تبیین آن برای عموم

1. MOOCS

و استفاده از قابلیت آن در استخدام استعداد‌های برتر در شرکت‌ها است. هر چند که این مورد هم با گذر زمان حل خواهد شد (رضادوست و رضانی شمامی، ۱۳۹۷).

فرماندهی و کنترل در فناوری‌های نظامی

در عصر اطلاعات، حمله به سامانه‌های اطلاعاتی امری گریز ناپذیر است و به همین دلیل دفاع در برابر حملات اطلاعاتی اهمیت قابل ملاحظه‌ای پیدا می‌کند. منظور از دفاع در C4I ممانعت از حملات اطلاعاتی، بی‌اثر کردن آن‌ها و کنترل خسارات بر جای مانده ناشی از آن‌ها است. البته باید توجه داشت که دفاع کامل در مقابل حملات اطلاعاتی، امری ایده آل و غیر واقع‌گراانه است و یک شبکه کاملاً امن وجود ندارد. لیکن می‌توان در این زمینه تدابیری اتخاذ کرد که نتایج قابل قبولی در پی داشته باشد. نکته مهم این است که در مقابل حملات اطلاعاتی که نیروهای متعارف نظامی برای مقابله با آن کارآمدی ندارد.

زنجیره بلوکی در فناوری‌های نظامی و فرماندهی و کنترل

سازمان‌های دارپا¹ و ناتو² به‌طور مشترک، درخواست تولید برنامه‌ای نظامی با استفاده از فناوری زنجیره بلوکی را ارائه داده‌اند.

دارپا می‌خواهد برای ایجاد یک سامانه‌ی پیام‌رسان امن از قدرت فناوری زنجیره بلوکی استفاده کند. طرح اولیه‌ی این پیام‌رسان «بستر پیام‌رسان امن³» نام گرفته و بخشی از برنامه‌ی «تحقیقات نوآوری کسب‌وکار کوچک⁴» به حساب می‌آید. هدف این پروژه ایجاد پیام‌رسانی برای انتقال پیام از طریق یک پروتکل امن غیرمتمرکز، در سراسر کانال‌های امن چندگانه است. این پیام‌رسان شامل پروتکل حمل‌ونقل، رمزگذاری پیام از طریق روش‌های مختلف و اجرای نسخه‌ی سفارشی‌سازی شده از زنجیره بلوکی است و از آن برای شکستن پیام و بازسازی آن استفاده می‌کند. دارپا توضیح

1. Defense Advanced Research Projects Agency

2. North Atlantic Treaty Organization

3. Secure Messaging Platform

4. Small Business Innovation Research

می‌دهد که طرح بستر پیام‌رسان امن، اجازهی آزمایش روی اکوسیستم شبکه‌ی وزارت دفاع را به دست آورده است.

در بخشی از متن طرح مذکور آمده است: «با انجام این کار، بخش‌های مهمی از زیرساخت دفاتر وزارت دفاع می‌توانند اسناد را در یک شبکه‌ی غیرمتمرکز بدون آن‌که شناسایی شده و مورد هجوم هکرها قرار گیرند، ارسال و دریافت کنند. این موضوع خطر حمله را نسبت به روش مکاتبه‌ی پیامکی سنتی رایج کاهش داده و تأخیرهای به وجود آمده را از بین خواهد برد.»

وزارت دفاع قصد دارند در یک فرآیند سه مرحله‌ای به هدف ذکر شده دست پیدا کند. این موضوع شامل یک سامانه‌ی پیام‌رسان امن با معماری غیرمتمرکز و زنجیره بلوکی می‌شود. این پیام‌رسان می‌تواند پیغام‌ها را به‌صورت زنده مدیریت کرده به جلو و عقب هدایت کند یا در صورت لزوم وجود آن‌ها را انکار کرده و از بین ببرد. زیرساخت‌های غیرمتمرکز در برابر حملات سایبری انعطاف‌پذیر هستند. همچنین افراد به‌راحتی می‌توانند از آن استفاده کنند.

مرحله اول: هدف این مرحله، ایجاد یک پیام‌رسان غیرمتمرکز ویژه با استفاده از چارچوب‌های به کار رفته در زنجیره بلوکی است.

مرحله دوم: در این مرحله ویژگی‌های یک نمونه اولیه مانند، توسعه، ارزیابی و آزمایش می‌شوند.

مرحله سوم: در این مرحله تمرکز روی پیاده‌سازی یک نسخه‌ی کامل و بستری برای صنایع و تجارت گذاشته خواهد شد.

با توجه به توضیحات مرحله‌ی اول و پیاده‌سازی با استفاده از زنجیره بلوکی، می‌توان به پروژه‌ی هایپرلجر¹ بنیاد لینوکس اشاره کرد. این پروژه در ماه دسامبر سال گذشته شروع شد تا یک سامانه توزیع شده با استانداردهای منبع باز بر پایه‌ی زنجیره بلوکی، برای استفاده در صنایع مختلف ایجاد شود. پروژه‌ی هایپرلجر توسط شرکت‌هایی مانند آی. بی. ام، ایتل و اکسنچر² آمریکا و چندین بانک و موسسه‌ی دیگر حمایت می‌شود.

1. Hyperledger Project

2. Accenture

در حالی که دارپا ادعا می‌کند از پروژه‌ی هایپرلجر استفاده نمی‌کند؛ اما بخشی از متن طرح اولیه این پیام‌رسان، نشان می‌دهد که دارپا به‌شدت به استفاده از این طرح تشویق شده است. شهبازی افزود: «فناوری زنجیره بلوکی قابلیت اعتماد بالاتری نسبت به سامانه‌های قدیمی دارد؛ زیرا می‌تواند به‌جای نگهداری معاملات و پیام‌ها در یک محیط مرکزی آن را به‌صورت توزیع شده در خود نگه دارد. این عمل، کار هکرها را سخت‌تر و شناسایی آن‌ها را ساده‌تر می‌کند.» امین‌گان‌سیرر^۱، استاد علوم رایانه دانشگاه کرنل^۲ آمریکا، گفت: «پروتکل زنجیره بلوکی، کلاس جدیدی از پروتکل‌ها است که به علت توزیع شده بودن، در برابر حملات انعطاف بالایی از خود نشان می‌دهد. بسیار جالب است که دولتمردان به تمام مباحث زمینه‌ی سامانه‌های رایانه‌ای علاقه‌مند شده و توجه نشان می‌دهند.»

از طرفی سازمان ارتباطات و اطلاعات ناتو در حال ارزیابی پیشنهادی ارائه شده در چالش نوآوری^۳ است. این کار با هدف افزایش سرعت تحول و یافتن راه‌هایی برای حمایت از «NATO C4ISR» و توانایی‌های نیازهای سایبری صورت می‌گیرد. درخواست ناتو شامل بخشی با عنوان «کاربردهای نظامی زنجیره بلوکی است که شامل به‌کارگیری این فناوری در تدارکات نظامی، امور مالی و دیگر بخش‌هایی که آن کاربرد دارد، می‌شود.» (رامک، مهرباب و محمدحسن شاهرضا، ۱۳۹۳).

یکی دیگر از این درخواست‌ها به استفاده‌ی زنجیره بلوکی در فناوری اینترنت اشیا مربوط می‌شود.

زنجیره بلوکی در فرماندهی و کنترل:

• سیستم‌های فرماندهی و کنترل C4I:

به امکانات، تجهیزات، ارتباطات، رویه‌ها و پرسنل مورد نیاز فرمانده جهت برنامه‌ریزی، هدایت و کنترل کارهای نیروهای منسوب به او مطابق با مأموریت منسوب شده، سیستم فرماندهی و کنترل گفته می‌شود.

1. Emin Gun Sirer

2. Cornell University

3. Innovation Challenge 2016

نقش سیستم فرماندهی و کنترل «ترسیم تصویری کلی برای فرمانده» و نقش فرمانده نیز گرفتن تصمیماتی به شدت فعل و انفعالی، در یک سیستم است.

در فرماندهی و کنترل سه مسئولیت اساسی وجود دارد:

۱. فراهم کردن اطلاعات لازم برای توسعه و بهبود مفاهیم فرمان برای فرماندهان
۲. انتقال صحیح، وفادارانه، صادقانه و شفاف مفاهیم فرمان‌ها به سمت پایین زنجیره‌های فرمان
۳. انتقال سریع و شفاف شکست‌های کشف شده یا قریب الوقوع از مفاهیم فرمان به سمت بالای زنجیره‌های فرمان

وظایف فرماندهی و کنترل از طریق ترتیبات نیرو، تجهیزات، ارتباطات، تسهیلات و فرایندهایی انجام می‌شود که توسط فرمانده در طرح‌ریزی، هدایت، هماهنگی، کنترل نیروها و عملیات‌ها در اجرای مأموریت به‌کارگیری می‌شود.

• نقش زنجیره بلوکی در فرماندهی و کنترل:

برای رسیدن به اهداف فرماندهی و کنترل و حفظ امنیت لازم در این فرایند، نیاز به یک پایگاه داده‌ی مشترک و در عین حال امن و قدرتمند می‌باشد که در آن واحد بتواند با حفظ داده‌های ثبت شده در فایل‌های تعریف شده و تعیین حدود اشتراک‌گذاری برای کاربران و رعایت امنیت در سلسله مراتب، اهداف سیستم‌های کنترل فرماندهی را پیاده کند. برای توصیف کامل نقش زنجیره بلوکی در ادامه به تشریح سامانه‌ی C4I می‌پردازیم. عبارت C4I معرف کلمات فرماندهی، کنترل، ارتباطات، رایانه و اطلاعات است.

فرماندهی و کنترل، بخش تصمیم‌گیری و مدیریت نظامی سامانه C4I است و فناوری‌های رایانه و ارتباطات بخش فناوری و اطلاعات، محور و پایه همه فرایندها و اقدامات در این سامانه است.

• سه رکن اصلی و تشکیل دهنده C4I عبارت‌اند از:

۱. تعامل بین سامانه‌ها
۲. امنیت سامانه‌های اطلاعاتی
۳. فرایندهای اداری و فرهنگ سازمانی

• موارد و ویژگی‌های مرتبط با امنیت اطلاعات و ارتباطات سامانه‌های فرماندهی و کنترل تحت پوشش زنجیره بلوکی:

در بیان ارتباط محتوایی امنیت اطلاعات با سایر موارد، نکاتی که نگرش به بحث امنیت سامانه‌های فرماندهی و کنترل را ضروری کرده و بر آن تأثیرگذار می‌باشند و در حقیقت و از ویژگی‌های بلاک چین و C4I می‌باشند برحسب مؤلفه عمده فهرست کرده و به تشریح برخی از آن‌ها در ذیل اشاره می‌شود:

۱. تطبیق‌پذیری (سازگاری)

۲. احراز هویت: اطمینان از اینکه هویت اصلی شخص همان است که ادعا می‌کند معمولاً این عمل بر اساس دانسته‌های شخصی (مثل کلمه عبور)، آنچه که متعلق به اوست (مثل یک کارت فایل خواندن توسط رایانه) یا آن چه هست (مثل اثرانگشت) انجام می‌گیرد. با بلاک چین به خوبی می‌توانیم امنیت ایجاد کنیم با ایجاد رمزگذاری‌های که در توضیحات بالک چین آورده شده.

۳. قابلیت تهیه (استطاعت) یا جامعیت داده‌ها: اطمینان از اینکه اطلاعات و داده‌ها به یک روش مشخص و مجاز تغییر، تعویض و یا تصحیح می‌شوند. به عنوان مثال جلوگیری از دخالت دشمن در تعویض، ترتیب واحدهای عملیات رزمی و تغییر شکل وقایع میدان جنگ به نفع خود. در استفاده از بلاک چین جامعیت داده‌ها حفظ می‌شود.

۴. میزان دسترسی یا در دسترس بودن سیستم: اطمینان از اینکه کاربران مجاز دارای دسترسی مدارم و به هنگام به اطلاعات و منابع هستند، به عنوان مثال ممکن است دشمن در شبکه ایجاد ترافیک جعلی و ساختگی کند و عملیات و ترافیک حقیقی را به تأخیر بیندازد؛ و با خصوصیتی که این مقاله برای بلاک چین آورده شده اگر سامانه C4I ما تحت پروتکل‌های این فن‌آوری قرار گیرد امکان ایجاد ترافیک جعلی و ساختگی از بین خواهد رفت.

۵. قابلیت اتصال یا صدور مجوز دستیابی: اعطای اجازه به کاربر برای انجام عمل یا یک مجموعه عملیات خاص با استفاده از پروتکل‌های بلاک چین قابل دسترسی است.

۶. ارتباط دو جانبه (همبستگی)

۷. توسعه‌پذیری

۸. انعطاف‌پذیری

۹. اطلاع‌رسانی: امنیت مفهومی بالاتر از حفاظت اطلاعات در برابر افشا شدن دارد. در حوزه C4I اطلاعات طبقه‌بندی شده بسیاری وجود دارد نظیر وضعیت آب‌وهوا، داده‌های کارکنان، حقوقی و لجستیک و سایر داده‌های مربوط به جنگ‌افزارها می‌باشد که در صورت افشای بعضی از آن‌ها امنیت ملی به خطر می‌افتد نیازمند یک سری سرویس‌های حفاظتی و امنیتی است که بعضی از آن‌ها از جمله احراز هویت که بلاک چین ضامن حفظ امنیت داده‌ها می‌باشد.

۱۰.

کپارچگی

۱۱.

عامل‌پذیری داخلی

۱۲.

عامل‌پذیری خارجی

۱۳.

عمیر پذیری، انکارناپذیری، استفاده از امضای دیجیتال، جامعیت پیغام و هویت ایجاد کننده آن را حفظ می‌کند و آن‌ها را در برابر تلاش برای از کار انداختن تکنیک‌های احراز هویت حفظ می‌کند یک امضای دیجیتال یک بلوک داده است که به آن‌ها پیام اضافه می‌شود. هر تغییری در پیام اعمال شود امضاء مورد تأیید قرار نمی‌گیرد که مفصلاً در کاربرد بلاک چین تشریح شد.

۱۴.

ابلیت اطمینان پیکربندی سیستم: اطمینان از اینکه سیستم یا شبکه تنها توسط افراد مجاز و به صورت سازگار با خط‌مشی‌های امنیتی اساسی سیستم تغییر می‌یابد، نیازمندی دیگر که در ارتباط با همه موارد فوق‌الذکر وجود دارد، قابلیت جوابگویی است.

۱۵.

ابلیت برنامه‌ریزی مجدد

۱۶.

قابلیت دوام و بقا

• چالش‌های عمده در انتقال اطلاعات به مناطق دور در سیستم فرماندهی و کنترل پیشرفته و امنیت آن‌ها

مهم‌ترین چالش در بهره‌برداری مؤثر از قابلیت‌های سامانه فرماندهی و کنترل امنیت سیستم‌های C4I متصل به شبکه‌های ارتباطی در برابر حملات اطلاعاتی است با توجه به این حقیقت که این سیستم‌ها و شبکه‌هایی که به آن متصل می‌شوند، مستقل از زیرساخت ملی اطلاعاتی نیستند. مسئله امنیت سیستم‌های C4I در برابر حملات به‌طور قابل ملاحظه‌ای پیچیده می‌شود. در واقع به علت اتصال در سیستم‌های نظامی و ملی، مرز بین این دو کاملاً نامشخص و مبهم است؛ و فن‌آوری بلاک چین راه‌کار بسیار توانمندی برای حل مشکلات ارائه می‌دهد.

نقش بلاک چین در افزایش امنیت سیستم‌های C4I

به موازات افزایش تعداد دستگاه‌هایی که به یک سیستم C4I متصل می‌شوند کاربران آن نیز افزایش پیدا می‌کند. ویژگی کلیدی جامعه شبکه‌ای توانایی کنار هم قرار گرفتن سریع سیستم‌ها با استفاده مهندسی شبیه‌سازی فناوری داخلی است، یعنی یک مهاجم می‌تواند پس از ناکام ماندن تهاجمش، به سرعت خود را برای تهاجمی دیگر آماده کند. در این جامعه شبکه‌ای، نقش بلاک چین برای جلوگیری از چنین حملاتی در سیستم‌های C4I در حالت‌های مختلف و حجم بسیار بالا انتقال

- داده‌ها در شبکه به خوبی خودش را نشان می‌دهد و با تلفیق این تکنولوژی با سیستم‌های C4I می‌توانیم از ویژگی‌های زیر به خوبی بهره‌برداری کنیم.
۱. کشف اتوماتیک اهداف با نظارت اپراتور
 ۲. تبادل سریع و اتوماتیک اهداف کشف شده
 ۳. قابلیت دریافت هم‌زمان اطلاعات از کلیه منابع
 ۴. شناسایی اتوماتیک و سرعت عمل در امر شناسایی
 ۵. امکان تعقیب هم‌زمان کلیه اهداف به‌طور اتوماتیک
 ۶. پردازش، تلفیق و نمایش کلیه اطلاعات
 ۷. امکان نظارت فرماندهان بر وضعیت تحرکات منطقه نبرد و کل کشور در زمان
 ۸. انجام کلیه محاسبات رهگیری و درگیری
 ۹. محاسبه و پیشنهاد مناسب‌ترین پایگاه جهت پرواز هواپیمای آلت
 ۱۰. پیشنهاد مناسب‌ترین جنگ افراز زمین به هوا

نتیجه‌گیری

زنجیره بلوکی با ایجاد فضایی برای توزیع (نه کپی کردن) اطلاعات دیجیتال، نوع جدیدی از اینترنت را به وجود آورده است. در ابتدا برای ارز دیجیتال بیت‌کوین مورد استفاده قرار گرفت اما کم‌کم برای فن‌آوری‌های دیگری نیز مورد استفاده قرار گرفت.

زنجیره بلوکی می‌تواند ارزش‌های دیجیتال دیگری نیز ایجاد کند. درست مانند اینترنت (یا ماشین)، شما برای استفاده از آن لازم نیست بدانید زنجیره بلوکی چگونه کار می‌کند. با این وجود داشتن دانش پایه‌ای از این تکنولوژی جدید می‌تواند به شما نشان دهد که چرا این تکنولوژی انقلابی در این صنعت به وجود آورد.

فن‌آوری زنجیره بلوکی مانند اینترنت، دارای یک استحکام داخلی است. با ذخیره بلوک‌های اطلاعاتی که در سراسر شبکه‌ی آن یکسان هستند، زنجیره بلوکی نمی‌تواند توسط نهاد یا واحد کنترل خاصی اداره شود و هیچ نقطه‌ی شکستی ندارد.

زنجیره بلوکی در دوران شروع خود خیلی زود در حال پیشرفت است. اکثر پروژه‌های بزرگ زنجیره بلوکی هنوز منتشر نشده است. پیش‌بینی می‌شود که فناوری‌های مبتنی بر مفهوم زنجیره بلوکی یک بخش خوب از اینترنت را که شما در ۱۰ تا ۱۵ سال آینده استفاده می‌کنید، پایه‌گذاری می‌کنند؛ اما مانند اینترنت امروز، درک کردن این‌که چگونه اینترنت فعال‌شده با زنجیره بلوکی کار می‌کند، سخت‌تر می‌شود.

هر روز مهارت‌ها تخصصی‌تر می‌شوند و این فضا نیاز به شناخت راه‌های گسترده‌ی مهارت‌ها و ایجاد امنیت در فضاها و ذخیره‌سازی اطلاعاتی حوزه‌های هرکدام از این مهارت‌ها می‌باشد که طراحی سیستم‌هایی کاربردی و دقیق برای بهبود این مشکلات نیازمند شناخت دقیق سازوکار سیستم‌های اجتماعی اقتصادی، دولت‌ها و رابطه آن‌ها با تکنولوژی است که فضای نظامی و فرماندهی و کنترل نیز این‌ها از این تکنولوژی عظیم مستثنی نیستند. لازم به ذکر است به نوعی جایگاه زنجیره بلوکی در سامانه‌های فرماندهی و کنترل کاربردی‌تر می‌باشد زیرا در انسجام اجرایی و ضرورت سامانه‌های فرماندهی و کنترل که در ذیل مراحل آن آورده شده است الزام زنجیره بلوکی مشهود است.

۱. جمع‌آوری اطلاعات از منابع دوردست با سرعت زیاد
۲. ادغام داده‌های جمع‌آوری شده از حساسه‌های نامتجانس در محل‌ها و زمان‌های مختلف
۳. قابلیت جمع‌بندی و تحلیل بهتر اطلاعات جمع‌آوری شده در زمان واقعی
۴. دقت بالاتر و بهتر یا کاهش خطای عملیاتی
۵. قابلیت اطمینان بیشتر
۶. کاهش نظام‌مند عدم قطعیت و ابهام در تصمیم‌گیری فرماندهی
۷. عکس‌العمل سریع‌تر یا کاهش تأخیر و وقفه
۸. جمع‌آوری اطلاعات از منابع دوردست با سرعت زیاد
۹. ادغام داده‌های جمع‌آوری شده از حساسه‌های نامتجانس در محل‌ها و زمان‌های مختلف
- ۱۰.
۱۱. ابلت جمع‌بندی و تحلیل بهتر اطلاعات جمع‌آوری شده در زمان واقعی
- قت بالاتر و بهتر یا کاهش خطای عملیاتی

ق

.۱۲

ابلیت اطمینان بیشتر

ک

.۱۳

اهش نظام‌مند عدم قطعیت و ابهام در تصمیم‌گیری فرماندهی

ع

.۱۴

کس‌العمل سریع‌تر یا کاهش تأخیر و وقفه

فهرست منابع:

الف - منابع فارسی

- رضا دوست، نیما، مؤگان، رضانی شمامی (۱۳۹۷)، بررسی بلاک چین و کاربرد آن در حوزه‌های مختلف، دومین کنفرانس ملی دانش و فناوری علوم مهندسی ایران، تهران، موسسه برگزار کننده همایش‌های توسعه محور دانش و فناوری سام ایرانیان.
- رامک، مهرباب، شاهرضا، محمدحسن (۱۳۹۳)، نقش فضای سایبری در صحنه فرماندهی و کنترل جنگ‌های آینده، هشتمین کنفرانس ملی فرماندهی و کنترل ایران، تهران، دانشگاه هوایی شهید ستاری.
- مروی نام، محمدرضا، بخشنده، محمد و ممی زاده، الیاس (۱۳۹۳)، تهدیدات آینده و رهیافت‌های نوین فرماندهی و کنترل، هشتمین کنفرانس ملی فرماندهی و کنترل ایران (C4I)، تهران، دانشگاه هوایی شهید ستاری

- اریکسون، اندرس (۱۹۹۹)، امنیت ملی و بین‌المللی در جامعه شبکه‌ای: نیازی برای تجدید بنای نوآوری نظامی.
- جوانمرد، مهدی (۱۳۸۴)، فناوری اطلاعات و ارتباطات در فرماندهی و کنترل، تهران: فصلنامه مهندسی اسوه، سال اول، شماره ۱.

ب - منابع انگلیسی

- Small Business Innovation Research Program (SBIR). Institute of Education Sciences. Retrieved 2018-02-15.
- Department of Defence-The C3I HandBook-1st edition
- kismet, "MIT Artificial Intelligence Laboratory, Humanoid Robotics Group.

پ - منابع اینترنتی

- موسسه‌ی اطلاع‌رسانی سایبربان <https://www.cyberbannews.com>
- انجمن علمی فرماندهی کنترل ایران <http://www.ic4i.ir/links>
- پایگاه اطلاع‌رسانی پدافند سایبری ایران www.papsa.ir
- انجمن میلیتاری بزرگ‌ترین مرجع مباحث نظامی در ایران <http://www.military.ir>
- فصلنامه‌ی علمی، خبری، تحلیلی پژوهشکده‌ی پارسا شریف www.Samamagazine.com
- دانشگاه دفاع ملی <http://sndu.ac.ir>
- coindesk.com/information/what-is-blockchain-technology