禪

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

میدهد اطلاعات را با بالاترین استاندارد امنیتی ممکن از یک مکان به مکان دیگر انتقال دهید . زنجیره بلوکی یک فناوری متنباز بوده که هیچ کس مالک آن نیست، هیچ مدیریت مرکزی روی تایید اعتبار تراکنشها وجود نداشته و این خود فناوری است که همه چیز را تنظیم میکند . خودتنظیمی یکی از مهمترین نوآوریهای به کار گرفته شده در بلاکچین است . هر زمان اطلاعاتی در آن ذخیرهسازی میشود، امکان رونویسی یا تغییر اطلاعات وجود ندارد . در نتیجه همواره تاریخچهای از فعالیتها ثبت میشود . این پتانسیلها باعث شده سازمانهای فعال در حوزههای مختلف ترغیب شوند از زنجیره بلوکی در فعالیتهای خود استفاده کنند .»

مطلب پیشنهادی

Blockchain
زنجیره‌بلوکی:
فناوری آینده‌ساز

زنجیره بلوکی : فناوری آیندهساز

زنجیره بلوکی چیست، چگونه کار میکند و چرا جهان ما را متحول خواهد ساخت؟

بلاکچین چگونه کار میکند؟

از طریق بهکارگیری مکانیزم رمزگذاری، تراکنشها به شکل ماداماالعمر و عمومی ضبط میشوند . هر یک از تراکنشها مهر زمانی داشته، ترتیب خطی دارند و رشته کاراکترهای یکبار مصرف دادهای یا هشها را ایجاد میکنند . این هشهای 64 کاراکتری تولید شده با کدهای هش قبلی ترکیب شده و به این شکل یک بلاک جدید را ایجاد میکنند . بلاکی که با بلاک قبلتر از خود مرتبط است . در شرایط خاص بلاکهای دیجیتالی ساخته شده تنها زمانی که دو طرف موافقت خود را اعلام کنند تنها میتوانند بهروزرسانی شوند، در نتیجه امکان حذف یا ویرایش اطلاعات مجاور یکدیگر تقریبا غیرممکن است . همین موضوع باعث شده تا امکان دستکاری اطلاعات یا درج اطلاعات غیرمعتبر در این فناوری غیرممکن باشد . در مقطع فعلی سامانههای اداری و پشتیبانگیری مورد استفاده در بانکها در معرض تهدیدات مختلف سایبری همچون کلاهبرداری یا پولشویی قرار دارند . اما بلاکچین میتواند با اتکا بر قابلیتهای از پیشساخته شده ضبط تراکنشها و مهرزمانی برچسب خورده به تراکنشها جایگزین فرآیندهای پیچیده امروزی شده و ضمن حفاظت از اطلاعات بسیار محرمانه مانع بروز جرایم سایبری رایج شود . این حرف به معنای آن است که از بلاکچین میتوان در حوزههای بهداشتودرمان، مالی، صنعتی، بانکداری و حسابرسی استفاده کرد . درست پس از آنکه گارتنر در سال 2016 گزارشی تحلیلی در ارتباط با بلاکچین منتشر کرد، بهکارگیری بلاکچین در اولویت کاری رهبران صنعت قرار گرفت . به ویژه سازمانهایی که در زمینه خدمات مالی، انرژی و تولیدی به فعالیت اشتغال دارند . یکی از مهمترین فاکتورهایی که باعث محبوبیت بلاکچین شده در ارتباط با مکانیزم اعتبارسنجی پرداختهای انجام شده با بیتکوین است . عملکرد بسیار دقیق و بدون عیب بلاکچین در ارتباط با ارزهای دیجیتال همچون بیتکوین باعث شده که سازمانهای بزرگ پیشنهاد دهند کارکردهای این فناوری بسط پیدا کرده و در برنامههای کاربردی همچون شبکههای تحویل محتوا و سامانههای هوشمند تحت شبکه از آن استفاده کرد . رویکردی که مدیران بعضی از پیامرسانها به دنبال دستیابی به آن هستند .

BLOCK
CHAIN

بلاکچین چگونه میتواند در حوزه امنیت به کار گرفته شود؟

بلاکچین با پتانسیل بهبود یکپارچگی دادهها و شناسایی دقیقتر هویت دیجیتالی اجازه میدهد، دستگاههای اینترنت اشیا ایمنتر شده و به این شکل مانع بروز حملات DDoS میشود. در واقع، این پتانسیل بالای زنجیره بلوکی است که اجازه میدهد این فناوری حول محور سهگانه محرمانگی، یکپارچگی و قابلیت دسترسی (CIA) نقشی کلیدی بازی کرده و همچنین انعطافپذیری بیشتر، رمزنگاری قدرتمندتر و حسابرسی شفافتر را نیز ارائه کند . بیل بوقانان، استاد دانشکده محاسبات دانشگاه ادینبورگ نپر میگوید : «بلاکچین میتواند شکافهایی را که به واسطه پیادهسازی ضعیف مکانیزمهای امنیتی به وجود آمده و باعث شده در برخی موارد حس بیاعتمادی در ارتباط با یکسری فناوریها به وجود آید، پر کند . در سال جاری ما باید فرآیند رمزنگاری را به شکل پیشفرض روی همه دستگاهها قرار دهیم . در مقطع فعلی شما نمیتوانید اطمینان حاصل کنید زمانی که ایمیلی را برای فرد دیگری ارسال میکنید، شخص ثالثی آنرا مشاهده نکرده یا ویرایش نکرده باشد . در برخی موارد ما حتی نمیتوانیم هویت ارسالکننده ایمیل را تایید کنیم . اما از طریق بهکارگیری روشهایی که بلاکچین ارائه میکند، ما به شکل درستی قادر هستیم تراکنشهای خود را امضا کرده یا اصالت آنها را تایید کنیم .

در حالی که امروزه اخبار مرتبط با بلاکچین بیشتر حول محور ارزهای دیجیتالی قرار دارد، اما واقعیت این است که پیادهسازی راهکارهای مبتنی بر بلاکچین باعث میشوند ما به شکل قابل اعتمادتری از سرویسهای دیجیتالی رایج استفاده کنیم . بزرگترین کاربرد بلاکچین در ارتباط با بخش عمومی است که اجازه میدهد زیرساختهای شهری متمرکز بر شهروندمحور بودن را ایجاد کنیم . این سیاست راهبردی به شهروندان اجازه میدهد هویت خاص خود را داشته باشند و برای هر تراکنشی که انجام میدهند از هویت واقعی خود استفاده کنند . ما میتوانیم از این فناوری در ارتباط با سرویسهای عمومی همچون پرداختهای همراه با مزایا، قراردادهای هوشمند و اظهارنامههای مالیاتی امضا شدهای که به شکل دقیق هویت هر شهروند را مشخص میکنند، استفاده کنیم .» اما پرسشی که اکنون مطرح میشود این است که زنجیره بلوکی در دنیای واقعی در چه حوزههایی از دنیای امنیت میتواند مورد استفاده قرار گیرد؟

1. Blockchain Data Integrity

Blockchain Data Integrity (BDI) Watson IoT Big Blue.

2. Filament Blocklet

.GE’s Predix

.3

Obsidian

iMessage

.4

Public Key Infrastructure (PKI)

2013

(Keyless Signature Infrastructure

3000

PKI

CertCoin

PKI

REMME

SSL

Pomcor

PKI

5. یک DNS ایمنتر

باتنت میرای نشان داد، نفوذگران چگونه میتوانند به سادهترین شکل زیرساختهای اینترنت را در معرض تهدید قرار دهند . باتنت فوق با خاموش کردن سامانه نام دامنه (DNS) موفق شد دسترسی به سایتهای بسیار مهمی را غیرممکن کند . در این حمله کاربران برای چند ساعت موفق نشدند به توییتر، نتفلیکس، پیپال و دیگر سرویسهای بزرگ دسترسی داشته باشند . اما رویکردی که بلاکچین ارائه میکند به این صورت است که اعلام میدارد موجودیتهای DNS در فضای ابری ذخیرهسازی شوند. Nebulis پروژه جدید است که به دنبال بررسی مفهوم DNS توزیع شدهای است که هیچگاه از کار نخواهند افتاد و درخواستهای دسترسی به آنها هیچگاه ناکام نخواهد ماند . Nebulis از زنجیره بلوکی اتریوم و فناوری IPFS (سرنام Interplanetary Filesystem) که یک جایگزین توزیع شده برای HTTPS است برای ثبت و حل مشکلات مربوط به فضای نام دامنه استفاده میکند . بوکانان در این ارتباط میگوید : «در هسته اینترنت، شاهد حضور سرویسهای حیاتی از قبیل DNS هستیم که به هکرها اجازه میدهد انواع مختلفی از عملیات خرابکارانه را روی سرویسها اعمال کرده و برای سازمانها مشکلات جدی را به وجود آورند . اما یک زیرساخت DNS قابل اعتماد که از مکانیزمهای زنجیره بلوکی استفاده میکند، اجازه میدهد به شکل قابل اعتمادتری از زیرساختهای مرکزی اینترنت استفاده کنیم ».

6. کاهش حملات منع سرویس توزیع شده

استارتآپ Gladius که در زمینه زنجیره بلوکی به فعالیت اشتغال دارد، اعلام داشته که یک سامانه دفتر غیرمتمرکز را طراحی کرده که از سازمانها در برابر حملات منع سرویس توزیع شده زمانی که شدت این حملات به 100 گیگابیت بر ثانیه میرسد، محافظت کند . شرکت میگوید: «راهحلهای غیرمتمرکز میتوانند از سازمانها در برابر این مدل حملات محافظت کرده و شما را به سرویسهای ایمنی متصل کنند که ضمن ارائه حفاظت بهتر، سرعت دسترسی به محتوا را نیز افزایش دهند.» این شرکت میگوید: «شبکه طراحی شده از سوی این استارتآپ قادر است در نقش یک شبکه تحویل محتوا سرعت دسترسی به اینترنت و محتوا را افزایش دهد.»

نویسنده :
حمیدرضا_تائبی
منبع :
blockchaincan
csoonline
techradar
دسته بندی:
امنیت
پرونده ویژه

تاریخ انتشار :
13:00 - 07/06/1397

برچسب:
زنجیره بلوکی - فناوری زنجیره بلوکی - فناوری پلاک چین - بلاک چین

نشانی
□□□□: https://www.shabakeh-mag.com/security/13049/%D8%B2%D9%86%D8%AC%DB%8C%D8%B1%D9%87-%D8%A8%D9%84%D9%88%DA%A9%DB%8C-%DA%A9%D9%84%DB%8C%D8%AF-%DA%AF%D9%85%D8%B4%D8%AF%D9%87-%D8%AF%D9%86%DB%8C%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA