

بلاکچین

توضیح بلاکچین: راهنمای نهایی برای درک چگونگی عملکرد بلاکچین

بلاکچین یک دفتر ثبت غیرمتمرکز هم‌تا به هم‌تای سریع، شفاف و امن است. نوع تکنولوژی بلاکچین سبب انقلابی در تکنولوژی‌های قدیمی خواهد شد و صنایع مختلف را تحت تاثیر قرار می‌دهد. اطلاعات ثبت شده بر روی بلاکچین بر روی بلاک‌هایی ثبت می‌شوند که به وسیله رمزنگاری به یکدیگر زنجیر شده‌اند و تشکیل یک زنجیره بلوکی را داده‌اند، این نوع از ثبت اطلاعات و داده‌ها می‌تواند، زمینه ذخیره اطلاعات به صورت شفاف، امن و غیرمتمرکز را فراهم کند و انقلابی در صنایع قدیمی به وجود آورد.

آخرین بروزرسانی ۱۲ آبان ۱۳۹۷

در این مقاله، شما به توضیحی ساده از بلاکچین دست خواهید یافت. به خوبی آگاهید که تلاش برای درک چگونگی عملکرد بلاکچین درست مثل تلاش برای درک علوم ماورای جهان است و بسیار گیج‌کننده است. به همین دلیل در این خودآموز بلاکچین، توضیح بلاکچین را از مفاهیم پایه‌ای آن شروع کرده و مزایای این فناوری و چگونگی کمک آن به شیوه‌ی اداره‌ی دنیا در آینده را بیان خواهیم کرد. از آنجایی که در این جا بلاکچین، به طور ساده و برای تازه‌کاران بیان شده است، بیاید پیش از شروع، موضوعی را روشن کنیم.

دو کلمه‌ی مهم دارای حرف "ب" در صنعت بلاکچین وجود دارد. کلمه‌ی اول (که آن را حدس زده‌اید) "بلاکچین" و کلمه‌ی دوم "بیت‌کوین" است. افراد تازه‌کار با تصور اینکه این دو، یک چیز هستند، موجب گمراهی خود می‌شوند؛ در حالی که آن‌ها یک چیز نیستند.

این دو بسیار به هم مرتبطند. به بیان ساده، بیت‌کوین یک ارز دیجیتال است. از طرف دیگر، بلاکچین آن فناوریست که توسط بیت‌کوین به کار برده شده و اجازه‌ی شکل‌گیری معاملات امن، عمومی و بی‌نام را می‌دهد.

بلاکچین را یک سیستم عامل (مثل ویندوز یا مک OS) و بیت‌کوین را یک نرم‌افزار که بر روی این سیستم عامل راه‌اندازی می‌شود، در نظر بگیرید.

بلاکچین چیست؟

این سوال، یکی از گیج‌کننده‌ترین سوال‌هاییست که در هنگام کشف ارزش‌های رمزنگاری شده، خود را در حال تلاش برای پاسخگویی به آن می‌یابیم. بنابراین توضیح بلاکچین بسیار ضروریست.

بلاکچین دفتر کلی دیجیتالی و غیر قابل دستکاری از معاملات اقتصادیست و می‌توان آن را به گونه‌ای تنظیم کرد که نه تنها معاملات اقتصادی، بلکه تقریباً هر چیزی که دارای ارزش است را نیز ثبت کند.

در اینجا توضیح بلاکچین به بیان ساده آمده است:

هدف اصلی بلاکچین فراهم آوردن امکان انجام معاملات هم‌تا به هم‌تای سریع، امن و روشن است. بلاکچین شبکه‌ای قابل‌اعتماد و غیرمتمرکز بوده که امکان انتقال ارزش‌های دیجیتال همچون ارز و داده را فراهم می‌کند.

توضیح ساده‌ی بلاکچین که برای تازه‌کاران مناسب است، در این جا آمده است:

1. بلاکچین را نوعی پایگاه داده‌ی دیجیتال؛ درست مثل یک صفحه اکسل در نظر بگیرید.
2. این پایگاه داده معمولاً در سطح شبکه‌ای گسترده که شامل کامپیوترهای بسیاریست (و با نام "نود" (node) شناخته می‌شود)، به اشتراک گذاشته شده و کاملاً عمومیست. به آن دلیل از کلمه‌ی "معمولا" استفاده می‌کنم که این شبکه از نظر فنی می‌تواند از هر تعداد نود تشکیل شود. هر چه تعداد نودها بیشتر باشد، شبکه امن‌تر است؛ اینکه می‌گوییم بهتر است تعداد زیادی نود در بلاکچین داشته باشیم نیز به همین دلیل است!
3. هر بار که شبکه پایگاه داده را به‌روزرسانی می‌کند، بلاکچین نیز به‌طور خودکار به‌روزرسانی شده و بر روی تمام کامپیوترهای شبکه داندلود می‌شود.
4. امنیت فناوری بلاکچین توسط تکنیک‌های رمزنگاری تامین می‌شود که امکان تغییر اطلاعات بر روی بلاکچین را برای هکرها تقریباً غیرممکن می‌سازد. تنها راه ایجاد تغییر این است که بیش از نیمی از نودهای بلاکچین را هک کنیم؛ دلیل این که چرا بهتر است نودها/کامپیوترهای بیشتری را در بلاکچین داشته باشیم نیز همین است.

توضیح ساده‌ی بلاکچین در اختیار شما قرار گرفت. بنابراین، از حالا به بعد وقتی کسی از شما پرسید "بلاکچین چیست؟"، شما دو پاسخ محکم دارید که می‌توانید از میان آن‌ها انتخاب کنید.

بلاکچین در مورد بیت‌کوین چگونه عمل می‌کند؟

بیت‌کوین اولین ارز رمزی بود که از فناوری بلاکچین استفاده کرد. این ارز توسط فرد یا گروهی که نام آن‌ها ساتوشی ناکاموتو (Satoshi Nakamoto) بود، اختراع شد.

تنها هدف بیت‌کوین این است که به عنوان نوعی منبع ارزش عمل کند. این ارز، امکان انجام معاملات هم‌تا به هم‌تا که احتیاج به واسطه ندارند، فراهم می‌کند.

توضیح بلاکچین بیت‌کوین برای درک عملکرد بلاکچین ضروریست. بلاکچین بیت‌کوین یک پایگاه داده است که فقط معاملات بیت‌کوین در آن ثبت شده‌اند. هیچ مکان مرکزی برای نگهداری این پایگاه داده وجود ندارد؛ در عوض، این پایگاه در سطح شبکه‌ای عظیم از کامپیوترها به اشتراک گذاشته می‌شود. بنابراین، اگر معاملات جدیدی بخواهند به پایگاه داده افزوده شوند، نودها باید تایید کنند که این معاملات واقعی و معتبرند.

نام این تایید گروهی نیز اجماع (Consensus) است که در طی فرآیند **استخراج** رخ می‌دهد.

نکته: استخراج فرآیندیست که در آن نودها داده‌های معاملاتی را بررسی و تایید کرده و برای کارشان پاداش دریافت می‌کنند. این فرآیند، هزینه‌های عملیاتی (مثل برق، حفظ و نگهداری و...) و سود کمی را نیز برای ارائه‌ی سرویس‌ها در بر می‌گیرد.

هنگامی که نودها تایید کنند که معامله واقعیست، معامله به یک "بلاک" افزوده شده (دلیل این که نام آن بلاکچین است نیز همین است) و در زیر بلاک قبلی معاملات در دفتر کل قرار می‌گیرد.

برای این که معامله معتبر باشد، کامپیوترها در شبکه باید تایید کنند که:

- در حساب کاربر، آن مقدار بیت‌کوین که کاربر قصد فرستادن آن را دارد، وجود داشته باشد.
- این مقدار قبلاً به فرد دیگری فرستاده نشده باشد.

برای مثال، بیایید فرض کنیم که تام (Tom) می‌خواهد 10 دلار بیت‌کوین را برای بن (Ben) بفرستد. تام تنها به ارزش پنج دلار در کیف پول خود بیت‌کوین دارد. از آن جایی که تام موجودی کافی برای فرستادن 10 دلار به بن را ندارد، این معامله معتبر نبوده و به دفتر کل افزوده نمی‌شود.

این به این معناست که هیچ‌کس نمی‌تواند یک مقدار پول را دوبار خرج کند! این موضوع ممکن است برای بانک‌های استاندارد و سیستم‌های پرداختی مشکل بزرگی به حساب بیاید، ولی در بیت‌کوین مشکل دوبار خرج کردن یک وجه به خوبی حل شده است.

یک مثال ساده برای این که بلاکچین را بهتر توضیح دهیم

بیایید نحوه‌ی ذخیره‌سازی و به‌اشتراک‌گذاری داده در سیستم‌های استاندارد (غیر بلاکچین) را با نحوه‌ی ذخیره‌سازی و به‌اشتراک‌گذاری آن در یک سیستم بلاکچین مقایسه کنیم.

نحوه‌ی عملکرد دفتر کل‌های سنتی (غیر بلاکچین) بسیار شبیه به روشی است که شما از طریق آن یک فایل word را با دوستان خود به اشتراک می‌گذارید:

1. زمانی که شما در حال ویرایش فایل خود هستید، دسترسی دوستان به آن قطع شده و نمی‌تواند هیچ تغییری اعمال کند.
2. زمانی که اعمال تغییراتتان به پایان برسد، آن را برای دوست خود می‌فرستید تا آن را بیشتر ویرایش کند.
3. حالا که دوست شما در حال ویرایش فایل است، دسترسی شما به آن قطع شده و نمی‌توانید هیچ تغییری اعمال کنید؛ این حالت تا زمانی که اعمال تغییرات دوستان تمام شده و فایل را مجدداً برای شما بفرستد، ادامه خواهد یافت.

با این حال، در یک سیستم بلاکچین، تمامی کاربران می‌توانند در عین اینکه تغییرات اعمال می‌شوند، شاهد آن‌ها باشند.

به جای این که داده برای یک شرکت یا فرد در یک زمان (به علت ریسک از دست دادن آن) قفل شود، در محیطی امن و مشترک قابل دسترسی خواهد بود. برای مثال، اگر داده بر روی یک کامپیوتر ذخیره شده و این کامپیوتر هک یا خاموش شود، جدیدترین نسخه‌ی داده از دست خواهد رفت.

و حالا برای توضیح بلاکچین: داده، همراه با بلاکچین، بر روی تمام کامپیوترها/نودهایی که آن را راه‌اندازی می‌کنند، ذخیره می‌شود. این به این معناست که اگر یکی از کامپیوترها/نودها هک یا خراب شود، داده در معرض هیچ ریسکی نخواهد بود.

همانطور که می‌بینید، فناوری بلاکچین تنها به ارزشهای رمزنگاری شده سود نمی‌رساند، بلکه باعث سود و منفعت صنایع مختلف بسیاری نیز می‌شود. میزان حساب‌ها و داده‌های مشتری که قانونی و امن بوده و به این شکل استفاده می‌شوند را تصور کنید.

این مورد تنها یکی از مزایای فراوان فناوری بلاکچین است! حالا بیایید به چند مزیت دیگر از آن نگاهی بیندازیم.

مزایای کلیدی بلاکچین

غیرمتمرکز

غیرمتمرکز بودن از اصلی‌ترین و مهم‌ترین مزایای فناوری بلاکچین است. این مزیت سال‌ها مفهومی مطلوب بوده است، اما در اصل فناوری بلاکچین بود که آن را امکان‌پذیر ساخت.

هیچ سرور مرکزی برای ذخیره‌ی داده‌های بلاکچین لازم نیست؛ این به این معناست که بلاکچین متمرکز نیست. چیزی که باعث می‌شود بلاکچین این قدر قوی باشد نیز همین است. به جای این که اطلاعات در یک جا ذخیره شود، بر روی بلاکچین ذخیره شده و نیروی آن را نیز کامپیوترها/نودهای مختلف تامین می‌کنند. این یعنی هیچ واسطه‌ای نیست که بتوان به آن اعتماد کرد و کارمزد پرداخت.

مستحکم و پایدار

زمانی که معامله تایید شود، بر روی دفتر کل ذخیره شده و با استفاده از رمزنویسی از آن محافظت می‌شود. این معامله را نمی‌توان بدون اتفاق آراء (موافقت گروه) حذف کرد، و این چیز است که باعث می‌شود بلاکچین مستحکم و پایدار باشد.

اعتماد و شفافیت

اعتماد در توضیح دنیای پیچیده‌ی بلاکچین بخشی ضروریست. از آن جایی که بلاکچین پایگاه داده‌ی مشترک‌یست، همه می‌توانند جزئیات معاملات را در آن ببینند. این جزئیات شامل منبع اولیه، تاریخ، زمان و مقصد معامله می‌شوند.

مقرون به صرفه

از آن جایی که بلاکچین شبکه‌ی هم‌تا به هم‌تا قابل اعتمادیست، نیاز به واسطه‌ی مرکزی را از بین می‌برد. این مورد، یکی از فواید مهم برای کسب و کارهاست؛ زیرا تمام هزینه‌های لازم برای پرداخت به واسطه را از بین می‌برد.

عملیات‌های سریع‌تر

بیایید از مثالی واقعی استفاده کنیم:

فرض کنید که می‌خواهید به فردی در یک کشور دیگر مبلغی بپردازید. بدون کمک فناوری بلاکچین، معمولاً باید کارمزدهای بالا (به بانک‌ها) پرداخت کنید و بین 3 تا 10 روز نیز طول می‌کشد تا معامله روند خود را طی کرده و کامل شود.

با استفاده از بلاکچین می‌توان این کار را فوراً و با هزینه‌ی بسیار کمتری انجام داد.

در دسترس بودن

بلاکچین یک شبکه‌ی هم‌تا به هم‌تا غیرمتمرکز بوده و هیچ نقطه ضعف مرکزی در آن وجود ندارد. حتی اگر کامپیوتر خراب شده یا از شبکه خارج شود، باز هم کامپیوترهای دیگری وجود دارند که گردش و جریان شبکه را حفظ کنند. به همین علت، این مورد مزیت بسیار بزرگیست.

برای توضیح بلاکچین به صورت واضح‌تر، سرور یک بیمارستان را فرض کنید: این سرور در بر دارنده‌ی داده‌های مهمی بوده که باید تمام وقت قابل دسترسی باشند. اگر کامپیوتری که از آخرین نسخه‌ی داده نگه‌داری می‌کند خراب شود، داده قابل دسترسی نخواهد بود. بسیار بد خواهد بود اگر این اتفاق در یک موقعیت اضطراری رخ دهد!

اگر بیمارستان از بلاکچین استفاده می‌کرد، خراب شدن کامپیوتر اهمیتی نداشت. در یک بلاکچین، آخرین نسخه‌ی داده در سراسر شبکه به اشتراک گذاشته شده و بنابراین، همیشه در دسترس خواهد بود.

ساده‌سازی معاملات تجاری

بیشتر کسب و کارها از سیستم‌های مختلف استفاده می‌کنند؛ بنابراین، برای آن‌ها سخت است که پایگاه داده‌ای را با کسب و کاری دیگر به اشتراک بگذارند. از آن جایی که بلاکچین می‌تواند به عنوان پایگاه داده‌ای مشترک برای هر دو تجارت عمل کند تا آن‌ها به کار خود ادامه دهند، به اشتراک گذاشتن داده در سیستم بلاکچین برای آن‌ها بسیار ساده‌تر است.

بلاکچین در صنایع واقعی

برای این که به شما کمک کنیم تا مزایای دیگری که نقش بلاکچین در کسب و کارها را درک کنید، در این جا مثال‌هایی از صنایعی آورده‌ایم که در حال حاضر از فناوری بلاکچین استفاده می‌کنند. این مورد، قطعاً توضیح بلاکچین را ارائه خواهد کرد:

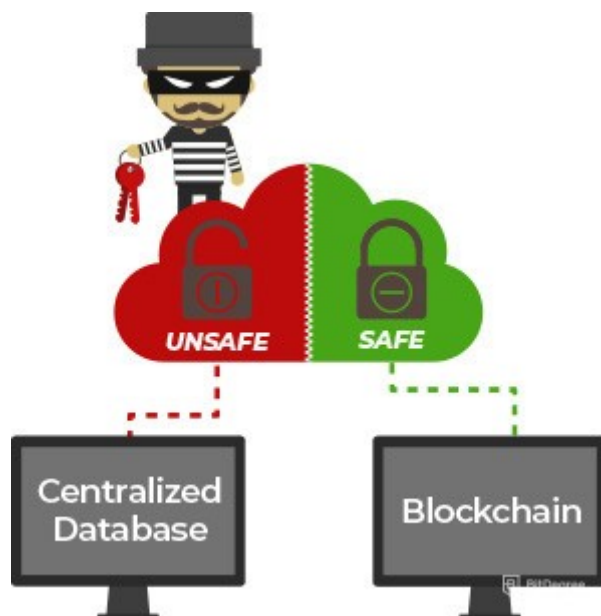
هویت

تهدیدات امنیت مجازی در صنعت مدیریت هویت مشکل بسیار بزرگی به حساب می‌آیند. در دنیای کنونی، هویت ما توسط شرکت‌های بزرگ کنترل می‌شود. این شرکت ممکن است شرکت نت‌فلیکس، فیس‌بوک، اینستاگرام یا حتی شرکتی که در آن کار می‌کنید، باشد.

خطر سرقت هویت مردم توسط سارقان مجازی - یا همان هکران - همیشه وجود دارد. تمام این شرکت‌ها از سرورهای متمرکز استفاده می‌کنند. برای مثال، نت‌فلیکس نقطه‌ی مرکزی سرور نت‌فلیکس است؛ اگر نت‌فلیکس هک شود، تمام داده‌هایی که برای مشتریان خود نگه می‌دارد، در معرض ریسک قرار خواهند گرفت. همین اواخر بود که داده‌های شرکت اکوی‌فکس (Equifax) هک شد.

حقایق جالب

اکوی‌فکس یکی از بزرگ‌ترین آژانس‌های گزارش اعتباریست، که از اطلاعات شخصی بیش از 800 میلیون مشتری نگه‌داری می‌کند. این رقم به این معناست که داده‌ی بیش از 145 میلیون کاربر دزدیده شده است.



بنابراین، چگونه می‌توان با استفاده از بلاکچین جلوی هک شدن داده‌ها را گرفت؟

خب، داده‌های شما در حال حاضر در یک پایگاه متمرکز (مثل اکویی‌فکس) نگهداری می‌شوند. هک کردن پایگاه متمرکز بسیار ساده‌تر است؛ زیرا از "یک" سرور اصلی استفاده می‌کند. در این صورت، تمام آنچه هکرها لازم است انجام دهند این است که این سرور اصلی را هک کنند. در یک بلاکچین، هیچ سرور اصلی وجود ندارد؛ یعنی هیچ نقطه‌ی مرکزی وجود ندارد که هکر به آن حمله کند!

بانکداری و پرداخت

"بلاکچین همان کاری را با بانکداری می‌کند که اینترنت با رسانه‌ها کرد."

میزان اهمیت بلاکچین برای صنعت مالی همین قدر است. با استفاده از بلاکچین می‌توان سرویس‌های مالی را برای افرادی که هم اکنون به آن‌ها دسترسی ندارند، فراهم کرد. تعداد این افراد بیش از دو میلیارد نفر است!

بیا بید مجدداً از بیت‌کوین به عنوان مثال استفاده کنیم؛ به لطف بیت‌کوین، هر فردی که به اینترنت دسترسی داشته باشد، اکنون می‌تواند پرداخت دیجیتال انجام دهد. آینده همین است! بنابراین، در این جا مزیت دیگری از بلاکچین توضیح داده شده و به لیست اضافه شده است.

بلاکچین، علاوه بر کمک به آن‌هایی که دارای سرویس‌های مالی نیستند، به خود بانک‌ها نیز کمک می‌کند. شرکت اکسنچر (Accenture) برآورد کرده است که بانک‌های سرمایه‌گذاری بزرگ می‌توانند به لطف بلاکچین در هر سال بیش از 10 میلیارد دلار ذخیره کنند؛ زیرا معاملات بسیار ارزان‌تر و سریع‌تر هستند.

تامین انرژی

در گذشته، مردم می‌توانستند تنها از یک راه - منبع متمرکز - انرژی دریافت کنند.

با این حال، اکنون ما می‌توانیم از دستگاه‌های خود یا از سیستم‌های شبکه‌ای با نام "ریزشبکه (Microgrid)" انرژی تجدیدپذیر دریافت کنیم. ریزشبکه‌ها این امکان را به افرادی که دارای پنل‌های خورشیدی هستند، می‌دهند که انرژی باقی‌مانده‌ی خود را، بدون هیچ واسطه‌ای، به افراد دیگر و خرده‌فروشان انرژی بفروشند. بنابراین، بیاید مزیت دیگری از بلاکچین را توضیح دهیم.

پیش از فناوری بلاکچین، مردم تنها می‌توانستند انرژی باقی‌مانده خود را به دلالان بفروشند (واسطه‌ها). قیمت‌های آن‌ها برای فروش انرژی بسیار پایین بود؛ دلالان آن انرژی را مجدداً به افراد دیگر می‌فروختند و بسیار سود می‌کردند.

از آن جایی که بلاکچین نیاز به واسطه را از بین می‌برد، افراد می‌توانند بر سر یک قیمت که برای هر دو طرف عادلانه است، توافق کرده و هزینه‌ی پیشین که توسط دلالان دریافت می‌شد، کاهش دهند.

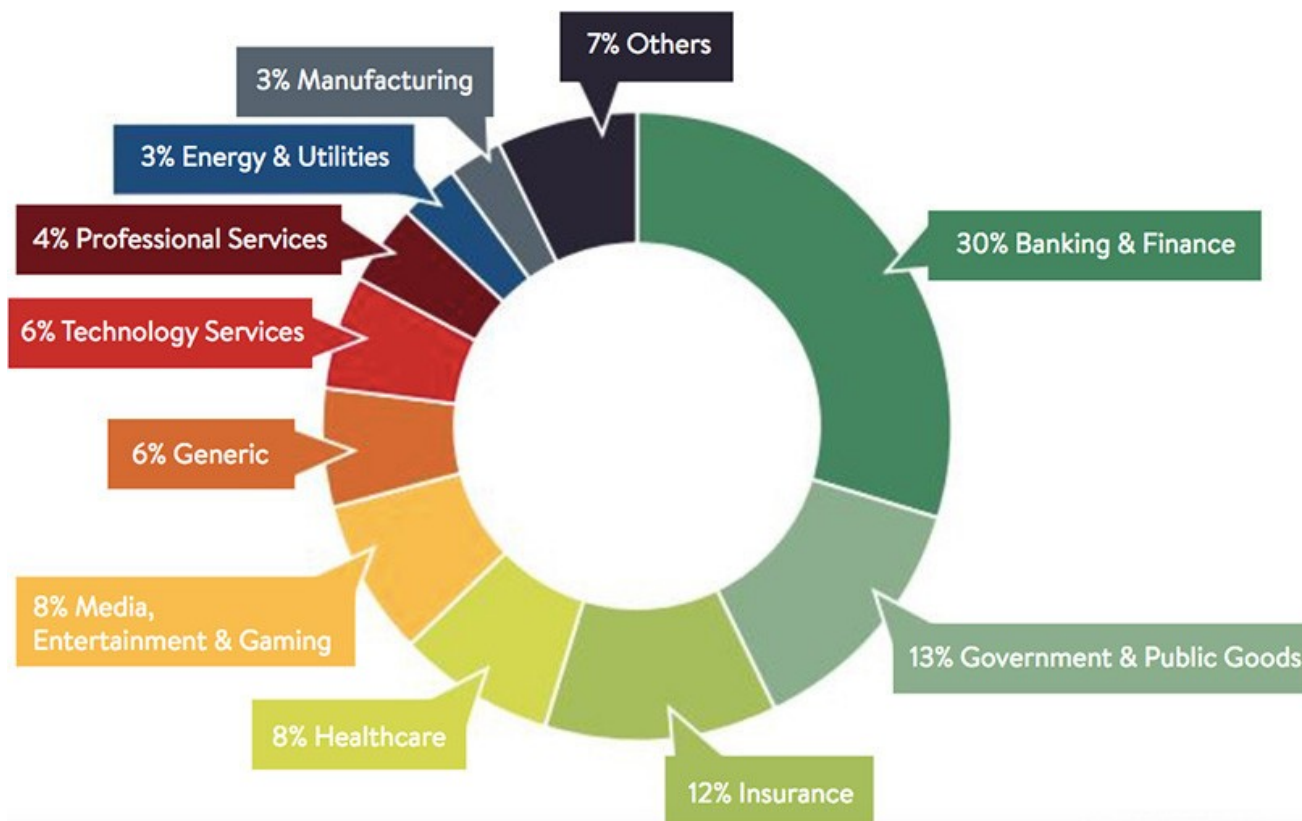
بلاکچین نحوه‌ی عملکرد بسیاری از صنایع فعلی دیگر را نیز تغییر خواهد داد

مثال‌های بالا تنها بخش کوچکی از آنچه از طریق بلاکچین ممکن است را تشکیل می‌دهند. بلاکچین برای صنایعی بسیار بیشتر از آنچه در بالا آمده است، به کار گرفته می‌شود.

در این جا صنایعی دیگر که در حال حاضر از بلاکچین استفاده کرده تا عملکرد خود را بهبود بخشند، آمده است:

- امنیت مجازی
- آموزش
- بازاریابی و تبلیغات
- مدیریت زنجیره تامین
- سیستم‌های دولتی
- اشتراک ویدیو و موسیقی
- تجارت الکترونیک
- رای‌گیری

با وجود این مقدار مزیت در استفاده از بلاکچین، احتمالات واقعا بی‌انتهاستند! بلاکچین به همه‌ی ما چیزی را می‌دهد که به دنبال آن هستیم.



SOURCE: University of Cambridge Judge Business School

نتیجه‌گیری

بیاید مرور کنیم که در این راهنمای توضیح بلاکچین چه چیزهایی یاد گرفتیم؛ و بعضی از مهم‌ترین مشخصه‌های بلاکچین را برجسته کرده تا آن‌ها را به یاد داشته باشیم:

بلاکچین چیست؟

- یک شبکه‌ی هم‌تا به هم‌تا که لزوم اعتماد به واسطه‌ها را از بین می‌برد.
- معاملات روند خود را سریع‌تر طی کرده و از سیستم‌های رایج (غیر بلاکچین) ارزان‌تر هستند.
- یک پایگاه داده‌ی عمومی بوده و تمام معاملات در شبکه قابل دیدن هستند؛ و این مسئله باعث جلوگیری از حمله‌های سایبری می‌شود
- تنها در صورت موافقت بیش از نیمی از شبکه می‌توان پایگاه داده را تغییر داد؛ این مورد باعث امنیت بسیار بیشتر آن می‌شود.
- توسط یک شرکت کنترل نشده و حتی یک نقطه ضعف هم ندارد.
- بلاکچین را می‌توان در صنایع مختلف استفاده کرد و استفاده آن فقط برای ارزهای دیجیتالی نیست.

بلاکچین چگونه کار می‌کند؟

- به عنوان یک پایگاه داده‌ی بزرگ که در سر تا سر شبکه‌ای از نودها (کامپیوترها) به اشتراک گذاشته شده است، کار می‌کند

- نودهای شبکه در کنار یکدیگر کار می‌کنند تا معاملات را تایید کرده و با ارز بلاکچین پاداش دریافت کنند؛ این روند با نام استخراج شناخته می‌شود
- زمانی که معامله توسط شبکه تایید شود، در یک بلاک قرار می‌گیرد
- بلاک‌های معاملات جدید به ترتیب در زیر بلاک‌های معاملات قبلی قرار می‌گیرند
- تمام معاملات بر روی یک پایگاه داده‌ی توزیعی (دفتر کل) ذخیره می‌شوند
- برای یک هکر بسیار سخت است که معاملات را تغییر دهد؛ زیرا برای این کار نیاز دارد تا بر روی بیش از نیمی از کامپیوترهای شبکه کنترل داشته باشد

این موضوع چگونه باعث سود صنایع بزرگ می‌شود؟

- هزینه لازم برای واسطه‌ها را از میان برمی‌دارد
- پرداخت و داده بسیار سریع‌تر پردازش می‌شوند
- مدیریت پایگاه داده بین کسب و کارها بسیار آسان‌تر است
- محافظت/امنیت داده تا حد زیادی ارتقاء می‌یابد

حرف آخر

واضح است که فناوری بلاکچین روش عملکرد کسب و کارها را تغییر خواهد داد، اما این تنها چیزی نیست که بلاکچین آن را تغییر می‌دهد. بلاکچین زندگی میلیون‌ها نفر را با دادن این امکان به آن‌ها که بتوانند پول ذخیره کرده و یا برای یکدیگر بفرستند، تغییر خواهد داد. به لطف بلاکچین، دنیا می‌تواند به جای بهتری تبدیل شود.

بلاکچین

بلاک چین

الگوریتم اجماع

ارز رمزنگاری شده

ارز رمز

ارز دیجیتال

اتریوم

Blockchain

Bitcoin



بیت‌کوین

[ارسال نظر](#)