مدیریت زنجیره تامین و فناوری بلاکچین

تألیف: دکترمهدی اسلام پناه

سرشناسه	:	اسلامپناه، مهدی، ۱۳۶۳
عنوان و نام پدیدآور	:	مدیریت زنجیره تامین و فناوری بلاکچین/تالیف مهدی اسلامپناه ؛ ویراستار مسعود آزاد.
مشخصات نشر	:	تهران: منشور سمیر، ۱۳۹۹.
مشخصات ظاهری	:	۲۷۶ ص.
شابک	:	۹۷۸-۶۰۰-۴۶۷-۴۰۶-۵
وضعیت فهرست نویسی	:	فیپا
موضوع	:	تدارکات بازرگانی
موضوع	:	Business logistics
موضوع	:	بلاک‌چین (پایگاه‌های اطلاعاتی) -- جنبه‌های اقتصادی
موضوع	:	Blockchains (Databases) -- Economic aspects
رده بندی کنگره	:	HD۳۸/۵
رده بندی دیویی	:	۶۵۸/۵
شماره کتابشناسی ملی	:	۶۱۶۰۳۴۹

مدیریت زنجیره تامین و فناوری بلاکچین

تألیف: دکتر مهدی اسلام پناه

ویراستار: مسعود آزاد

ناشر: منشور سمیر

شمارگان: ۵۰۰ نسخه

نوبت چاپ: اول-۹۹

قیمت: ۸۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۴۶۷-۴۰۶-۵

حق چاپ: ۱۳۹۹، انتشارات منشور سمیر

www. manshoorsamir.ir

پیشگفتار

بلاکچین[1] فناوری جذابی‌ست که امروزه بر سر زبان‌ها افتاده و روز به روز تعداد کاربرانی که در معاملات مالی و سایر زمینه‌ها از آن استفاده می‌کنند بیشتر می‌شود.

اگر طی چند سال گذشته اخبار حوزه بانک، سرمایه گذاری و رمزارزها را دنبال کرده باشید ممکن است با بلاکچین آشنا باشید .فناوری که پایه و اساس بیت‌کوین است. مفهوم بلاکچین کمی پیچیده است و هنگام مطالعه درمورد آن احتمالا به تعریفی مانند: «بلاک‌چین یک دفتر کل توزیع شده، غیرمتمرکز و عمومی است.»

برخورده‌اید. خبر خوب این است که بلاکچین تعریفی ساده‌تر از این هم دارد و درک آن آنقدرها هم سخت نیست.

بلاکچین یک اختراع خلاقانه از سوی شخص یا گروهی ناشناس با نام مستعار ساتوشی ناکاموتو است. این مفهوم ابتدا در سال ۲۰۰۸ به منظور ایجاد یک دفتر کل برای رمزارز بیت‌کوین ایجاد شد و از آن زمان تا به امروز دچار تغییرات و پیشرفت‌های زیادی شده است.

بلاک‌ها در بلاکچین از بخش‌های مختلف اطلاعات تشکیل شده‌اند. این اطلاعات شامل ۳ بخش مختلف هستند:

۱- بلاک‌های اطلاعات مربوط به معاملات مثل تاریخ، ساعت و مبلغ آخرین خریدی که از آمازون داشتید را ذخیره می‌کنند. البته ما در اینجا آمازون را به عنوان مثال ذکر کردیم. این فروشگاه از بلاکچین استفاده نمی‌کند.

۲- در بخش دوم هویت کسانی که در معامله نقش داشتند در بلاک ذخیره می‌شود. برای مثال وقتی از آمازون خرید می‌کنید نام شما و نام شرکت آمازون به عنوان

---

1 - Blockchain

خریدار و فروشنده ثبت می‌شود. اما در بلاک‌چین نام و هویت واقعی شما مورد استفاده قرار نمی‌گیرد و خریدّ بوسیله یک امضای دیجیتال منحصر به فرد انجام می‌شود. این امضای دیجیتال در حقیقت مانند یک نام کاربری عمل می‌کند.

۳- در بخش آخر، بلاک اطلاعاتی را در خود ذخیره می‌کند تا بتوان آن را از سایر بلاک‌ها تشخیص داد. مانند من و شما که با نام‌هایمان از یکدیگر تشخیص داده می‌شویم. هر بلاک یک کد مخصوص به خود به نام هش[۲] دارد که آن را از دیگر بلاک‌ها متمایز می‌کند. بیایید فرض بگیریم هنگام خرید از یک فروشگاه آنلاین وقتی دکمه پرداخت را فشار دادید ناگهان متوجه شدید از آن کالا یک عدد دیگر هم نیاز دارید و دوباره خرید را تکرار می‌کنید. در اینجا با وجود اینکه جزییات مربوط به خرید جدید شما تقریبا با خرید اول یکی است اما هنوز می‌توانیم بلاک‌های هردو خرید را بوسیله کدهای منحصر به فردشان از هم تشخیص دهیم.

اولین بار استوارت هابر و اسکات استورنتا کار بر روی اولین مجموعه از بلاک‌های امن را در سال ۱۹۹۱ شروع کردند. آن‌ها می‌خواستند سیستمی را اجرایی کنند که در آن مولفه‌های زمانی قابلّ دستکاری و تغییر نباشند. آن‌ها در سال ۱۹۹۲ با استفاده از یک درخت درهم‌سازی طراحی این سیستم را بهبود دادند. به این صورت می‌شد چندین سند تایید شده در یک بلاک قرار بگیرند.

اما اولین بلاکچین توسط شخص یا گروهی به نام ساتوشی ناکاموتو در سال ۲۰۰۸ تعریف شد. ناکاموتو توانست با استفاده از یک متد مشابه به Hash cash طراحی بلاک‌ها را بهبود ببخشد. با اجرایی کردن این متد دیگر بدون نیاز به تاییدیه یک طرف قابل اعتماد می‌شد مولفه‌های زمانی در بلاک ثبت شوند. علاوه بر این سرعت افزوده

2 - Hash

شدن بلاک‌ها به زنجیره نیز افزایش پیدا کرد. این طراحی یک سال بعد توسط ناکاموتو به عنوان هسته تشکیل دهنده رمزارز بیت‌کوین به اجرا درآمد و کار خود را به عنوان یک دفتر کل برای ثبت تمامی معاملات شبکه شروع کرد.

استفاده از بلاکچین طی سال‌های پس از آن افزایش زیادی پیدا کرد و در سال ۲۰۱۴ حجم فایل بلاک‌چین بیت‌کوین، که در آن تمامی معاملات انجام شده ذخیره می‌شود، به ۲۰ گیگابایت رسید. در ژانویه ۲۰۱۵ حجم این فایل به ۳۰ و تا اوایل سال ۲۰۱۷ به ۱۰۰ گیگابایت رسید.

زمانی که اطلاعات در یک بلاک ذخیره شوند آن بلاک به زنجیره بلاک‌ها یا همان بلاکچین افزوده می‌شود. بلاکچین همانطور که از نامش پیداست از چندین بلاک که به صورت زنجیره‌ای به هم متصل هستند تشکیل شده است. اما پیش از آن که یک بلاک جدید به این زنجیره اضافه شود باید ۴ پیش شرط رعایت شود:

۱- یک معامله باید انجام شود. بیایید مثال خرید از آمازون را اینجا هم استفاده کنیم. پس از وارد کردن اطلاعات مختلف شما مبلغ را پرداخت و سفارش خود را ثبت می‌کنید.

۲- اکنون باید انتقال این مبلغ به تایید برسد و سفارش شما تایید شود. همانطور که در سایر منابع اطلاعاتی مثل بورس، ویکی‌پدیا یا کتابخانه محل یک نفر مسوول تایید و وارد کردن اطلاعات جدید است. اما در بلاک‌چین این کار بوسیله شبکه‌ای از کامپیوترها صورت می‌پذیرد. این شبکه‌ها در بیشتر اوقات از هزاران کامپیوتر متصل به هم در سرتاسر جهان تشکیل می‌شوند. مثلا شبکه بیت‌کوین تقریبا ۵ میلیون کامپیوتر دارد. وقتی خریدتان را از آمازون انجام می‌دهید این کامپیوترها به سرعت وارد عمل می‌شوند تا ببینند آیا این خرید همانطور که شما ادعا کردید انجام شده یا

خیر. آن‌ها جزییات خرید مثل ساعت و تاریخ، مبلغ و خریدار و فروشنده را چک و تایید می‌کنند.

۳- حالا که معامله ما تایید شد باید اطلاعات مربوط به آن در یک بلاک ذخیره شود. مبلغ خرید، امضای دیجیتال شما (خریدار) و امضای دیجیتال آمازون (فروشنده) همه در یک بلاک ثبت می‌شوند.

۴- در مرحله آخر این بلاک باید هش یا همان کد منحصر به فرد خود را دریافت کند. این کد تنها زمانی که تمامی معاملات ذخیره شد در بلاک به تایید رسیده باشند اعطا می‌شود. علاوه بر این کد مخصوص آخرین بلاکی که به زنجیره اضافه شده است هم به بلاک داده می‌شود، پس از این بلاک ما می‌تواند به زنجیره اضافه شود.

هدف از ایجاد بلاکچین جلوگیری از ویرایش اطلاعات معاملات و همچنین امکان ثبت و پخش اطلاعات دیجیتال بوده است. بدون آشنایی با طرز کار این پروسه درک کردن آن کمی سخت است. بنابراین بهتر است به گذشته برویم و ببینیم اولین نمونه از بلاکچین چطور کار می‌کرد. همانطور که پیشتر هم گفتیم بلاکچین ابتدا در سال ۱۹۹۱ ایجاد شد امّا تقریبا دو دهه طول کشید تا در سال ۲۰۰۹ برای اولین بار عملیاتی شود.

پروتکل بیت‌کوین نیز بر اساس بلاکچین ساخته شده است. خالق این رمزارز ساتوشی ناکاموتو آن را به عنوان یک سیستم مالی دیجیتال توصیف کرد که کاملا همتا به همتا میان خریدار و فروشنده است و هیچ عضو سومی در آن دخیل نیست. بنابر گزارش دانشگاه کمبریج در سال ۲۰۱۷ در سرتاسر جهان نزدیک به ۶ میلیون نفر دارای بیت‌کوین هستند. حالا فرض می‌گیریم یکی از این ۶ میلیون نفر می‌خواهد با

بیت‌کوین‌هایش تنقلات خریداری کند. در اینجا است که بلاکچین اهمیت پیدا می‌کند.

وقتی صحبت از پول‌های چاپی به میان می‌آید دستگاه‌های مثل بانک مرکزی و دولت وظیفه نظارت بر نحوه استفاده از آن‌ها را بر عهده دارند. اما بیت‌کوین توسط هیچ فرد یا دستگاهی کنترل نمی‌شود. در عوض این شبکه‌های کامپیوتری هستند که معاملات را تایید می‌کنند. وقتی فردی یک کالا را با استفاده از بیت‌کوین خریدار می‌کند این کامپیوترها برای تایید این معامله شروع به کار می‌کنند. برای تایید این معامله کاربران برنامه‌ای را روی سیستم خود نصب کرده و سپی می‌کنند یک معادله پیچیده ریاضی به نام هش را حل کنند.

وقتی یک کامپیوتر معادله را حل کرد الگوریتم‌هایی که برای حل معادله از آن‌ها استفاده کرده، معاملات بلاک را هم تایید می‌کنند. معامله انجام شده سپس در بلاک ذخیره و بلاک به زنجیره سایر بلاک‌ها افزوده می‌شود. در این مرحله دیگر هیچکس قادر به ویرایش اطلاعات مربوط به این معاملات نیست. در بیت‌کوین و سایر رمزارزها کامپیوترهایی که با موفقیت این معادلات را حل و بلاک‌ها را تایید کنند برای این کار پاداش دریافت می‌کنند.

با وجود اینکه معاملات به صورت عمومی در دسترس قرار دارند اما اطلاعات کاربران به طور کامل عمومی نیست. برای انجام یک معامله از طریق بیت‌کوین خریدار و فروشنده باید از برنامه‌ای به نام کیف پول بلاک‌چین یا والت[3] استفاده کنند. هر کیف پول بلاک‌چین دارای دو کلید منحصر به فرد و رمزنگاری شده است: کلید عمومی و کلید خصوصی. کلید عمومی در واقع مانند شماره حساب بانکی شماست که با

3- Wallet

استفاده از آن رمزارز واریز و برداشت می‌شود و اگر مثلا کالایی را به کسی می‌فروشید باید این کلید را به او بدهید تا او مبلغ را برایتان ارسال کند. این کلید همچنین در دفتر کل بلاک‌چین به عنوان امضای دیجیتال هر کاربر ثبت می‌شود.

اما برای آن که بتوانید از این کلید، بیت‌کوین برداشت کنید به کلید خصوصی نیاز دارید. کلید خصوصی در واقع نسخه طولانی‌تر کلید عمومی کاربر است که با استفاده از الگوریتم‌های پیچیده ریاضی ساخته می‌شود. به دلیل پیچیدگی این الگوریتم‌ها غیرممکن است که بتوانید این پروسه را برعکس کرده و با داشتن کلید عمومی یک کاربر کلید خصوصی او را هم بدست بیاورید. از همین رو بلاکچین را یک شبکه محرمانه و امن به شمار می‌آورند.

بلاکچین در آستانه سی سالگی خود بالاخره در حال گسترش و رشد است. این امر بیشتر به لطف بیت‌کوین و رمزارزها حاصل شده است. فناوری بلاکچین در آینده نزدیک احتمالا با سرعت بیشتری فراگیر خواهد شد و می‌تواند کسب و کارها و دولت‌ها را مسوولیت پذیرتر، کارآمدتر و مطمئن‌تر کند.

به طور خلاصه، فناوری بلاک‌چین را از منظر تجاری، قانونی و فنی می‌توان به عنوان یک راهکار بسیار خوب در نظر گرفت. بلاک‌چین می‌تواند به کسب و کارها در خصوص اجرای آسانتر اقدامات روزانه خود در شبکه همتا به همتا کمک کند. از لحاظ قانونی نیز تمام واسطه‌ها از دفترکل بلاک‌چین کنار گذاشته می‌شوند و تمام ارتباطات فقط بین طرفین تراکنش ایجاد می‌شود. از نظر فنی نیز کنترل،-امنیت و حریم خصوصی اطلاعات داخل سیستم را تضمین می‌کند.

فناوری بلاک‌چین به سازمان‌ها و شرکت‌ها ویژگی‌هایی از جمله امکانات زیر ارائه می‌دهد:

- امکان انجام سریعتر تراکنش‌ها با اعتماد کامل
- کاهش هزینه برای کسب و کارها یا فرآیندهای بین سازمانی و حذف واسطه‌ها، ناکارآمدی‌ها و تقلیدهای
- معرفی تعامل دیجیتالی مدرن
- ارائه فرصت برای کنترل فرآیندهای تجاری و تراکنش‌ها بدون وجود کنترل مرکزی
- حذف تقلب، حملات سایبری یا سایر جرایم الکترونیکی

بلاک‌چین با مکانیزم‌های شفاف خود و حداکثر شفاف‌سازی ممکن، سرانجام نحوه انجام تراکنش افراد و جوامع را متحول خواهد کرد. جای تعجبی وجود ندارد که بسیاری از پروژه‌ها از بلاک‌چین استفاده می‌کنند. برای مثال، TenX کاربران را در خرج کردن ارزهای دیجیتال کمک می‌کند، EOS.IO کاربردهایی برای برنامه‌های غیرمتمرکز ارائه می‌دهد، آگر[4] با تحلیل‌های بازار به پیش بینی رویدادهای آینده می‌پردازد.

آینده بلاک‌چین روشن به نظر می‌رسد. بلاک‌چین در حوزه‌هایی نظیر جذب سرمایه، معاملات سهام، اقتصاد و به بسیاری از جنبه‌های سلامت و سایر صنایع به کار گرفته می‌شود.

4 - Augur