
بسم الله
الرحمن
الرحيم

کسب و کار بلاکچین

استفاده از نسل بعدی فناوری اینترنت؛ از حرف تا عمل

ویلیام موگایار
پیش‌گفتار: ویتالیک بوترین
ترجمه: پیمان رحمانی
مقدمه: محمدرضا سوهانیان

هاب
راه‌پرداخت

سرشناسه: موگایار، ویلـیام. Mougayar، William. /عنوان و نام پدیدآور: کسب و کار بلاکچین: استفاده از نسل بعدی فناوری اینترنت؛ از حرف تا عمل/ویلـیام موگایار؛ مترجم: پیمان رحمانی؛ ویراستار: یلدا شایسته‌فر. /مشخصات نشر: تهران: رضا قربانی، ۱۳۹۷ /مشخصات ظاهری: ۲۳۲ ص. تصویر. جدول. نمودار/شابک: ۸-۱۳۱۹-۰۰-۶۲۲-۹۷۸ /وضعیت فهرست نویسی: فیپا/یادداشت: عنوان اصلی: Promise, Practice, and Application of the Next Internet Technology C2016 : The Business Blockchain / یادداشـــت: کتابنامه. /عنوان دیگر: استفاده از نســـل بعدی فناوری اینترنت؛ از حرف تا عمل. /موضوع: اینترنت-- نوآوری /موضوع: Internet--Technological innovation /موضـــوع: انتقال اینترنتی وجوه /موضوع: Elecronic funds transfers /شناســـه افزوده: رحمانی، پیمان، ۱۳۶۳ -، مترجم/شناسه افزوده: قربانی، رضا، ۱۳۶۳ -، مترجم/شناسه افزوده: سوهانیان، محمدرضا، ۱۳۵۵ -، مقدمه نویس / رده‌بندی کنگره: ۱۳۹۷ ۹ز۸م/HG ۱۷۱۰ /رده‌بندی دیویی: ۳۳۲/۱۷۸ /شـــماره کتاب‌شناســـی ملی: ۵۳۶۴۲۷۴

کسب و کار بلاکچین

استفاده از نسل بعدی فناوری اینترنت؛ از حرف تا عمل

ویلیام موگایار
پیش‌گفتار: ویتالیک بوترین
ترجمه: پیمان رحمانی
مقدمه: محمدرضا سوهانیان

هاب
راه‌پرداخت

کسب و کار بلاکچین: استفاده از نسل بعدی فناوری اینترنت؛ از حرف تا عمل / ناشر: رضا قربانی / مؤلف: ویلیام موگایار / مترجمان: پیمان رحمانی / ویراستار: یلدا شایسته‌فر / صفحه‌آرا: ایمان شاه‌سمندی / مدیر تولید: رسول قربانی / نوبت چاپ: اول - ۱۳۹۷ / شمارگان: ۱۰۰۰ نسخه / شابک ۸-۱۳۱۹-۰۰-۶۲۲-۹۷۸ / لیتوگرافی، چاپ و صحافی: هنراشکان / تمام حقوق این اثر محفوظ و متعلق به شبکه راه پرداخت است / نشانی انتشارات: تهران، جنت‌آباد جنوبی، پایین‌تر از میدان چهارباغ، نبش کوچه نوبختی، پلاک ۱، طبقه ۳، واحد ۴ / تلفن: ۰۹۱۰۶۹۴۹۳۰۲ / دورنگار: ۸۹۷۸۴۹۰۲ / پست الکترونیک: mediamanager.ir@gmail.com / پایگاه اینترنتی: Way2Pay.ir

فهرست

معرفی هوشمند اول بهشتی (هاب)

مجموعه هوشمند اول بهشتی (هاب) از بخش‌های متنوعی تشکیل شده است که همگی با هدف حمایت از توسعه پایدار کسب‌وکارهای نوپا و سخت‌توسعه کنار یکدیگر جمع شده‌اند. هسته اصلی شرکت هاب با همکاری استراتژیک دانشگاه شهید بهشتی و شرکت ارتباطات سیار ایران (همراه اول) شکل گرفته تا محلی باشد برای همبستگی بیشتر دانش و تجر به دانشگاه و صنعت.

بستر فراهم‌شده از این همکاری استراتژیک به هاب کمک کرده است تا در مقیاس پذیری تیم‌های نوپا و افزایش درآمد آنها با تکیه بر روش‌های خلاقانه‌ای که زندگی ایرانیان را تسهیل می‌کند، حضور موفقی داشته باشد. در این راستا شـــتاب‌دهنده Early stage هاب نیز به‌عنوان اولین شتاب‌دهنده مراحل اولیه رشد استارت‌آپ‌ها در ایران، در کنار سایر بخش‌های هاب شکل گرفت تا در مسیر بهبود اکوسیستم استارت‌آپی کشور همراهی باشد در توسعه پایدار کسب‌وکارهای نوآورانه کشور.

با تاکید بر اینکه بلا کچین پاسخی برای همه چالش‌ها و ســـوالات نیست (همه می‌دانیم که این

جواب فقط یک عدد است: ۴۲!*)، هاب با هدف ترویج بهره‌گیری از این فناوری و کمک به شناخت بهتر فرصت‌های ایجاد کسب‌وکارهای مبتنی بر آن که می‌تواند دنیا را متحول سازد، تصمیم به حمایت از انتشار نسخه ترجمه فارسی کتاب حاضر گرفت.

امید است که ترجمه و نشر این کتاب قدمی باشد جهت شناخت فرصت مناسب در به‌کارگیری فناوری مناسب به شکلی مناسب در توسعه پایدار زیرساخت‌ها و کسب‌وکارها در ایران عزیزمان.

*برگرفته از کتاب معروف The Hitchhiker>s Guide to the Galaxy نوشته Douglas Adams

یادداشت حامی

اثر بلاکچین در تحول کسب‌وکارها شاید سال‌ها به درازا بکشد؛ منتها نکته مهم این است که سفر مدتی است که آغاز شده! با توجه به اهمیت این سفر همه ما باید واقعیت‌هایی درباره بلاکچین یا زنجیره بلوک بدانیم.

پیش از هر چیز لازم است بدانیم که وقتی درباره بلاکچین صحبت می‌کنیم، صرفا درباره یک فناوری معمولی حرف نمی‌زنیم. بلاکچین یک فناوری بنیادی است؛ چیزی که احتمالا در سال‌های آینده ساختارهای مالی و اقتصادی و حتی اجتماعی و سیاسی را تغییر می‌دهد. اساسا قراردادها، تراکنش‌ها و ذخیره‌سازی این تراکنش‌ها سیستم‌های سیاسی، حقوقی و اقتصادی جوامع را تعریف می‌کنند. اینکه ما مالک چه چیزهایی هستیم، مجاز به انجام چه کارهایی هستیم و نیستیم، اجازه ورود به چه مکان‌هایی را داریم یا نداریم و با چه کسانی مجاز به تعامل هستیم و بسیاری از آن چیزهایی که هویت ما را در جامعه تعریف می‌کنند، مبتنی بر قراردادها، تراکنش‌ها و البته شیوه‌های ذخیره‌سازی و

دسترسی به آنها هستند. این سه، از دارایی‌های ما محافظت می‌کنند و مرزهای سازمان‌ها را مشخص می‌کنند، اما متاسفانه بوروکراسی حاکم بر سازمان‌ها نه‌تنها در ایران؛ بلکه در جهان نیز هنوز نتوانسته با تحول دیجیتال کنار بیاید.

درست است که همه ما شنیده‌ایم که بلاکچین انقلابی در کسب‌وکارها به پا می‌کند؛ منتها باید توجه داشته باشیم مدت‌زمان رسیدن به این تحول بسیار بیشتر از آن چیزی است که بسیاری ادعای آن را دارند. بلاکچین یک فناوری بنیادی است و شاید شبیه‌ترین مثال تاریخی برای درک بلاکچین، فناوری TCP/IP است که پایه و اساس توسعه اینترنت است. پیش از ورود این فناوری ارائه‌دهندگان سرویسهای تلکام و تولیدکنندگان تجهیزات، میلیاردها دلار هزینه صرف روش‌هایی کرده بودند که فناوری TCP/IP با ورودش به کلی آن را دگرگون کرد. در ابتدا بخش‌های سنتی نسبت به این فناوری بدبین بودند. تعداد اندکی فکر می‌کردند که ارتباطات ویدئویی، صوتی، پیام‌رسان و انتقال داده می‌توانند روی معماری جدید برقرار شوند یا اینکه این سیستم می‌تواند حفظ و بزرگ شود. به‌مرور روش‌های ارتباطی سنتی جایش را به فناوری جدید داد و سازمان‌ها هم افزایش کارایی ناشی از کاربرد آن را درک کردند، استفاده از سرویس‌های اینترنتی مرسوم شد، اتصال به شبکه جهانی ارزان‌تر و سریع‌تر شد و شرکت‌ها با کمک اینترنت برنامه‌های نوین و متحول‌کننده ساختند که مدل‌های کسب‌وکار را به‌صورت بنیادین تغییر داد. می‌دانید این قصه چند سال طول کشید؟ ۳۰ سال! ۳۰ سال طول کشید تا TCP/IP تمامی فازها را طی کند و به اقتصاد شکل جدیدی بدهد. امروز دیگر بنیان‌های اقتصاد دگرگون شده‌اند و مقیاس فیزیکی و دارایی‌های منحصر به‌فرد دیگر مزایای شکست‌ناپذیری به حساب نمی‌آیند.

TCP/IP ارزش اقتصادی جدیدی را با کاهش چشم‌گیر هزینه‌های ارتباطات ایجاد کرد و حالا بلاکچین که در ابتدا به‌عنوان بخشی از پروژه بیت‌کوین معرفی شد، می‌تواند به‌شدت هزینه‌های انجام تراکنش را کاهش دهد و این پتانسیل را دارد که به سیستم ثبت تمامی تراکنش‌ها تبدیل شود. اگر این اتفاق رخ دهد، اقتصاد بار دیگر تحولی چشم‌گیر را تجربه خواهد کرد و منابع جدید مبتنی بر بلاکچین ظهور می‌کنند.

مانند فناوری TCP/IP که وب و اینترنت روی آن ساخته شد، پیچیدگی‌های فناوری بلاکچین و دامنه تاثیرگذاری آن باعث می‌شود بلوغ این فناوری هم زمانبر باشد. تجربه نشان می‌دهد برای اینکه یک

نوآوری بنیادی مانند بلاکچین بتواند انقلابی به پا کند، باید موانع متعدد فنی، حاکمیتی، سازمانی و حتی اجتماعی از میان بروند. عجله کردن در زمینه نوآوری بلاکچین و حرکت بدون آینده‌نگری اشتباه است. آنچه از تجربه به دست آمده، این است که دو بعد روی نحوه تکامل فناوری بنیادی و کاربرد آن در کسب‌وکار تاثیر می‌گذارد؛ تازگی و پیچیدگی. تازگی یعنی میزان جدید بودن یک برنامه برای مردم؛ هرچه تازگی بیشتر باشد، تلاش بیشتری لازم است که مردم بدانند این برنامه دقیقا چه مساله‌ای را حل می‌کند. پیچیدگی هم تعداد و تنوع گروه‌هایی است که باید با یکدیگر کار کنند تا توسط فناوری ایجاد ارزش صورت بگیرد. مثلا یک شبکه اجتماعی با یک عضو ارزشی ندارد! یک شبکه اجتماعی زمانی ارزش دارد که اکثر ارتباطات ما در آن ثبت شده باشد. از این روست که به نظر می‌رسد تحول واقعی در استفاده از بلاکچین در دولت و سازمان‌ها در سال‌های دور رخ خواهد داد. این ادعا به این دلیل است که بلاکچین یک فناوری توفنده و اخلال‌گر نیست که به یک مدل کسب‌وکار سنتی حمله کند و راه‌حلی ارزان را جایگزین روش‌های قدیمی کند. بلاکچین این پتانسیل را دارد که بنیان سیستم‌های اجتماعی و اقتصادی را از نو خلق کند، اما شاید ده‌ها سال طول بکشد که بلاکچین بتواند جایگزین نظم موجود شود؛ چراکه فرایند به‌کارگیری بلاکچین تدریجی خواهد بود. بلاکچین ناگهانی تغییر ایجاد نمی‌کند، این مسیر سال‌ها طول می‌کشد؛ منتها برای موفقیت در این زمینه باید از هم‌اکنون برنامه‌ریزی را آغاز کرد!

محمدرضا سوهانیان
مدیرعامل شرکت هاب

درباره کتاب

کتاب کسب‌وکار بلاکچین قلمرو جدیدی را در افزایش درک ما از بلاکچین باز می‌کند و این امکان را می‌دهد تا با عناصری که پیش از این در هیچ کتاب دیگری مورد اشاره قرار نگرفته‌اند، آشنا شویم. کسب‌وکار بلاکچین کمک خواهد کرد تا بسیاری از تصورات ذهنی در این حوزه به واقعیت تبدیل شوند. بر اساس پیش‌بینی ویلیام موگایار، در آینده حداقل شاهد هزاران و شاید میلیون‌ها بلاکچین خواهیم بود که نه‌تنها امکان تبادل ارزش بدون اصطکاک را فراهم می‌سازند، بلکه جریان ارزش جدیدی را نیز شکل خواهند داد و به بازتعریف نقش‌ها، روابط، اعتماد، قدرت و حاکمیت خواهند انجامید. در این کتاب، موگایار دو ادعای راهبردی دیگر را نیز مطرح می‌کند. طبق اولین ادعای وی، بلاکچین دارای ویژگی‌های چندوجهی است. به بیان دیگر، استفاده از بلاکچین، اثری چندگانه دارد. طبق ادعای دوم، اینکه بلاکچین می‌تواند چه مشکلاتی را حل کند، پرسش مناسبی نیست، زیرا دید ما نسبت به توانایی‌های بالقوه بلاکچین را محدود خواهد کرد. در عوض، باید به فرصت‌های جدید در این حوزه فکر کنیم و این امکان را به بلاکچین بدهیم تا بتواند مشکلات فراتر از مرزهای ذهنی،

قانونی و سازمانی را حل کند. ویلیام موگایار که تجربه‌ای ۳۴ساله در صنعت فناوری دارد و در این مدت به‌عنوان مدیر اجرایی، تحلیلگر، مشاور، کارآفرین، منتور استارت‌آپ، نویسنده، وبلاگ‌نویس، معلم، رهبر فکری و سرمایه‌گذار مشغول به کار بوده است، آینده‌ای را تصور می‌کند که تحت تاثیر تغییرات اساسی ناشی از فناوری بلاکچین است که فاکتور مهمی در افزایش سرعت تحولات در حوزه فناوری به‌شمار می‌رود. درست به همان شیوه‌ای که اینترنت توانست امکانات جدیدی را در اختیار ما قرار بدهد که در سال‌های اول ظهور و پیدایش‌اش قابل تصور نبود، بلاکچین نیز مدل‌های کسب‌وکار و ایده‌های جدیدی را شکل خواهد داد که هنوز نمی‌توانیم تصوری از آنها داشته باشیم.

پیش‌گفتار

این دهه زمان مناسبی برای توسعه فناوری‌های غیر متمرکز به‌شمار می‌رود. اگر چه رمزنگارها، ریاضی‌دانان و کدنویس‌ها، تلاش زیادی به خرج داده‌اند تا پروتکل‌های پیشرفته‌تری را به منظور افزایش بیشتر حریم شخصی و اصالت سیستم‌های مختلف (از پول نقد الکترونیکی گرفته تا رای‌گیری برای انتقال فایل) ایجاد کنند، اما پیشرفت کار آنها طی بیش از ۳۰ سال بسیار کند بوده است. نوآوری بلاکچین و به بیان عام‌تر، نوآوری اجماع اقتصادی عمومی ایجادشده توسط ساتوشی ناکاموتو در سال ۲۰۰۹، گام امیدبخشی بود که جهش عظیم دیگری را در حرکت رو به جلوی صنعت کامپیوتر ایجاد کرد.

بحران مالی عظیم سال ۲۰۰۸ باعث شد تا به اعتماد به بخش مالی جریان اصلی، یعنی شرکت‌ها و دولت‌هایی که معمولا بر آنها نظارت دارند، خدشه زیادی وارد شود. این اتفاق بسیاری را بر آن داشت تا به‌دنبال شیوه‌های جایگزین دیگری بگردند. در ادامه، افشاگری‌های ادوارد اسنودن در سال ۲۰۱۳، در مورد ورود دولت به حریم خصوصی شهروندان، انگیزه بیشتری را به کسانی داد که به‌دنبال

راه‌حل‌هایی برای این وضعیت می‌گشتند. اگرچه هنوز فناوری‌های بلاکچین به راهکار جریان اصلی تبدیل نشده‌اند، اما عنصر غیر متمرکزسازی می‌تواند به پذیرش فزاینده آنها کمک کند.

کاربرد بلاکچین، از تلفن‌های اپل تا واتس‌اپ را در بر می‌گیرد. یکی از عناصر مهم در این فناوری، رمزگذاری نام دارد که بر اساس آن، شرکت نویسنده نرم‌افزار و سازمان مدیریت‌کننده سرورها نیز نمی‌توانند رمز آن را بشکنند. از نظر کسانی که شرکت‌ها را به دولت ترجیح می‌دهند، اقتصاد اشتراکی نسخه ۱/۰ نتوانسته به بسیاری از وعده‌هایی که داده است، جامه عمل بپوشاند. تنها کاری که غول‌هایی همانند او بر انجام داده‌اند، جایگزین کردن خودشان با واسطه‌های دیگر بوده است. توجه داشته باشید که لزوما عملکرد این غول‌ها همیشه بهتر از واسطه‌های قبلی نیست.

بلاکچین و فناوری‌های مرتبط با آن که من نام کریپتوی نسخه ۲/۰ را بر آنها می‌گذارم، راهکار جذابی را ارائه می‌کنند. در اینجا، به جای دلخوش بودن به رفتار صادقانه گروه‌هایی که در تعامل با آنها هستیم، سیستم‌های فناورانه‌ای خلق می‌شوند که ویژگی‌های مطلوبی را در داخل سیستم ایجاد می‌کنند، به نحوی که با وجود فعالیت بازیگران ناصادق، سیستم همچنان بتواند با اطمینان به کارش ادامه بدهد.

همه تراکنش‌های تحت کریپتوی نسخه ۲/۰ دارای دنباله‌های قابل ممیزی اثبات‌ها یا سندهای رمزنگاری‌اند. شبکه‌های فرد به فرد غیر متمرکز، تکیه ما به یک سرویس‌دهنده منفرد را کاهش خواهند داد. رمزنگاری کلید عمومی، امکان شکل‌گیری هویت‌های قابل حمل و کنترل‌شده توسط کاربر را فراهم می‌سازد. انواع پیشرفته‌تر قابلیت‌های ریاضی از قبیل امضاهای حلقه‌ای، رمزگذاری هومومورفیک و اثبات‌های دانش صفر (دانایی صفر)، به تضمین حریم شخصی کمک می‌کنند و این امکان را به کاربران می‌دهند تا بتوانند داده‌های مربوط به خودشان را مورد استفاده قرار بدهند؛ به گونه‌ای که بتوان ویژگی‌های خاصی از آنها را مورد راستی‌آزمایی قرار داد و حتی بدون افشای جزئیات حریم شخصی، آنها را محاسبه کرد.

با این حال، عجیب‌ترین نکته از نظر استفاده‌کنندگان قدیمی این فناوری، به پذیرش سازمانی سریع آن طی دو سال گذشته بر می‌گردد. در فاصله زمانی ۲۰۱۱ تا ۲۰۱۳، صحنه بلاکچین و به عبارت روشن‌تر، صحنه بیت‌کوین، به میدانی برای تحولات متنوع و ایده‌آل‌گرا و ابزاری برای جنگ قدرت تبدیل شده است. با این حال، اکنون که در سال ۲۰۱۶ قرار داریم، مشارکت با آی‌بی‌ام یا مایکروسافت،

گزارش تحقیقاتی بانک انگلستان و اعلامیه‌های کنسرسیوم بانکداری، مهیج‌ترین بیانیه‌هایی هستند که به رشد اعضای فضای کریپتو کمک خواهند کرد.

چه اتفاقی افتاد؟ به نظر من برخی آنارشیست‌های کریپتو، انعطاف‌پذیری و پیشرفت تکنولوژیکی بانک‌ها و حتی شرکت‌های بزرگ آرمانگرا را دست‌کم گرفتند. بیشتر اوقات فراموش می‌کنیم که عنصر اصلی شرکت‌ها را مردم تشکیل می‌دهند و ارزش‌ها و نگرانی‌های افراد داخل شرکت‌ها غالبا همانند افراد عادی است. ممکن است چنین تصور شود که آنچه نشریه اکونومیست «ماشین اعتماد» می‌نامد، جایگزین کاملی برای لنگر اعتماد متمرکز، هم در تامین مالی و هم در حوزه‌های دیگر که متکی به نظارت بر قانون‌گذاری و تایید اعتبار جهان حقیقی هستند، به‌شمار می‌رود، اما واقعیت خیلی پیچیده‌تر از این حرف‌هاست. در حقیقت، سازمان‌ها کاملا به هم اعتماد ندارند و نگرانی سازمان‌های متمرکز واقع در یک صنعت در مورد متمرکزسازی در صنایع دیگر، همانند مردم عادی است. شرکت‌های انرژی که کارشان تولید و فروش برق است، درست به همان اندازه که از فروش در بازار متمرکز خوشحال می‌شوند، به فروش در بازار غیر متمرکز نیز علاقه‌مند هستند و حتی در برخی موارد، بازار غیر متمرکز را ترجیح خواهند داد.

علاوه بر این، اگرچه در حال حاضر با صنایع غیر متمرکز زیادی مواجه هستیم، اما غیر متمرکز بودن آنها به حدی است که توسط افراد خارج از این صنایع احساس نمی‌شود و از کارایی بالایی نیز برخوردار نیستند. در این نوع غیر متمرکزسازی، شرکت‌ها باید زیرساخت خودشان را که مبتنی بر مدیریت کاربران، تراکنش‌ها و داده‌هاست، حفظ کنند و بتوانند آن را در هنگام تعامل با سایر شرکت‌ها، تغییر بدهند. اگرچه یکپارچگی حول یک رهبر بازار منفرد، کارایی این صنایع را بالا خواهد برد، اما رقبای رهبر فوق‌الذکر و قانون‌گذاران ضد تراست علاقه‌ای به آن ندارند و این ما را به بن‌بست می‌رساند. با ظهور و پیدایش بانک‌های اطلاعاتی غیر متمرکزی که بتوانند با کمک فناوری، منافع اثر شبکه‌ای انحصار یکجانبه را نصیب کاربران کنند، همه افراد امکان الحاق و سود بردن از این وضعیت را بدون شکل‌گیری انحصار یکجانبه که تاثیرات منفی‌ای را به همراه خواهد داشت، پیدا خواهند کرد.

به دلایلی که در بالا ذکر شد، علاقه به زنجیره‌های بلوک کنسرسیومی در بخش مالی، کاربرد بلاکچین در صنعت زنجیره تامین و سیستم‌های تشخیص هویت مبتنی بر بلاکچین روزبه‌روز افزایش می‌یابد. استفاده از بانک‌های اطلاعاتی غیر متمرکز این امکان را به افراد خواهد داد تا بدون اینکه زیر

بار کنترل یک پلتفرم بروند و احیانا به‌واسطه انحصارطلبی‌اش مورد سوءاستفاده قرار بگیرند، از منافع حضور در آن پلتفرم برخوردار شوند.

پس از آنکه ساتوشی ناکاموتو در ژانویه ۲۰۰۹ بیت‌کوین را راه‌اندازی کرد، طی همان چهار سال اول حضورش توجه بسیاری را به سمت خود جلب کرد. ویژگی‌های پرداخت بیت‌کوین و نقش آن به‌عنوان یک ذخیره ارزش جایگزین، جالب توجه بود. در سال ۲۰۱۳، نگاه فعالان این حوزه به اپلیکیشن‌های بلاکچین نسخه ۲/۰ جلب شد. زیربنای اپلیکیشن‌های بلاکچین نسخه ۲ را نیز فناوری مورد استفاده در امنیت و غیر متمرکزسازی بیت‌کوین تشکیل می‌داد و گستره وسیعی از ثبت‌نام دامنه تا قراردادهای مالی، تامین مالی جمعی و حتی بازی‌ها را در بر می‌گرفت. دانش هسته و پشت صحنه پلتفرم من یعنی اتریوم این بود که می‌توانستیم یک زبان برنامه‌نویسی تورینگ کامل را که در داخل پروتکل لایه پایه تعبیه شده بود، به‌صورت کاملا انتزاعی مورد استفاده قرار دهیم تا توسعه‌دهندگان بتوانند اپلیکیشن‌های مختلف با هر هدف یا منطق کسب‌وکار را تولید کنند و در عین حال از ویژگی‌های هسته بلاکچین نیز سود ببرند. تقریبا در همان زمان، سیستم‌هایی از قبیل سیستم فایل بین سیاره‌ای (IPFS) پلتفرم ذخیره‌سازی غیر متمرکز پا به عرصه گذاشتند و ابزارهای قدرتمند جدیدی در اختیار رمزنگارها قرار گرفتند تا بتوانند با استفاده از آنها در کنار فناوری بلاکچین، حریم شخصی و به‌طور خاص zk-SNARK ها (اثبات دانایی صفر، کوتاه و غیرتعاملی دانش) را افزایش بدهند. ترکیب رایانش مبتنی بر بلاکچین تورینگ کامل و شبکه‌های غیربلاکچینی غیر متمرکز با استفاده از فناوری‌های رمزنگاری مشابه و همچنین یکپارچه‌سازی بلاکچین با رمزنگاری پیشرفته، به چیزی منتهی شد که من نام آن را «کریپتوی نسخه ۲/۰» می‌گذارم. اگرچه ممکن است این عنوان، ابهام‌آمیز باشد، اما به نظر من بهترین اسمی است که می‌توان روی آن گذاشت.

کریپتوی نسخه ۳/۰ چیست؟ کریپتوی نسخه ۳/۰، تا حدودی، ادامه‌دهنده روندهای موجود در کریپتوی نسخه ۲/۰ و به‌طور خاص، پروتکل‌های عمومی مربوط به حریم شخصی و انتزاع محاسباتی است، اما علاوه بر آن به فاکتور مهمی به نام مقیاس‌پذیری نیز توجه دارد. در حال حاضر، همه پروتکل‌های بلاکچینی موجود از این ویژگی برخوردارند که هر رایانه موجود در شبکه باید هر تراکنش را پردازش کند. این ویژگی، به افزایش امنیت و تحمل بیشتر در برابر خطا منتهی خواهد شد، اما در عین حال، توان پردازشی شبکه را به توان پردازشی گره‌های موجود در آن محدود می‌سازد.

هدف کریپتوی نسخه ۰/۳، حداقل تا جایی که من می‌دانم، فائق آمدن بر این محدودیت و افزایش مقیاس استفاده از ارزهای رمزنگاری‌شده به سطح مورد نیاز برای پذیرش جریان اصلی است. خوانندگانی که اطلاعات فنی خوبی دارند، حتما در این رابطه با ایده‌هایی همانند «شبکه‌های صاعقه»، «کانال‌های حالت» و «شاردینگ» (بخش‌بندی) برخورد کرده‌اند.

سوال دیگری که در این رابطه مطرح است، به پذیرش بر می‌گردد. اتفاق دیگری که کریپتوی نسخه ۰/۲، علاوه بر مورد کاربرد ساده‌اش در حوزه ارزهای رمزنگاری‌شده، در سال ۲۰۱۵ با آن مواجه شد این بود که اگرچه افراد زیادی در مورد آن صحبت می‌کردند و توسعه‌دهندگان، پلتفرم‌های پایه زیادی را توسعه داده بودند، اما شاهد کاربرد قابل توجهی برای آن نبودیم. در سال ۲۰۱۶، شاهد توسعه اثبات‌های مفهوم هم از جانب بازیگران سازمانی و هم از جانب استارت‌آپ‌ها بودیم. البته همانند همه حوزه‌های دیگر، در اینجا نیز اکثریت آنها به موفقیتی دست نیافتند و محو شدند. اگر کارآفرین باشید، حتما می‌دانید که معمولا ۹۰ درصد کسب‌وکارهای جدید به سرانجام نمی‌رسند. اما ۱۰ درصدی که موفق می‌شوند، احتمالا خواهند توانست میلیون‌ها نفر را به سمت خود جلب کنند و نکته جالب توجه در حوزه بلاکچین نیز به همین موضوع بر می‌گردد.

کتاب ویلیام و ورود شما به فرایند اصلاح کسب‌وکار بلاکچین می‌تواند به درک هرچه بیشترتان از فناوری بلاکچین کمک کند.

ویتالیک بوترین
مخترع اتریوم و دانشمند ارشد بنیاد اتریوم
دوم آوریل ۲۰۱۶

پیش‌گفتار نویسنده کتاب

در بسیاری از مواقع شانس در خانه من را نمی‌زد، اما یکی از فرصت‌های خوب زندگی من به اولین آشنایی‌ام با ویتالیک بوترین، مخترع اتریوم بر می‌گردد که در همان شهری که من زندگی می‌کردم، یعنی تورنتو اتفاق افتاد.

در یکی از عصرهای سرد روزهای اول ژانویه ۲۰۱۴، یک ساعت قبل از شروع یکی از جلسات هفتگی بیت‌کوین تورنتو که توسط آنتونی دی یوریو ترتیب داده شده بود، ویتالیک از پله‌های مرکز Bitcoin Decentral که در ساختمان باریک قدیمی‌ای در خیابان اسپادینا قرار داشت، پایین می‌رفت. در آنجا برای اولین‌بار با او صحبت کردم و تلاش کردم تا آنچه را که او «فراتر از بیت‌کوین» می‌نامد، بفهمم. آشنایی من با بیت‌کوین به شـــش ماه قبل از این ملاقات بر می‌گشت و فناوری اتریوم چیز جدیدی برای من بود.

کمی بعد از شروع بحث من و ویتالیک، افراد مختلف اتاق را پر کردند و جلسه شروع شد. همهمه خاصی در میان مردم پیچیده بود، زیرا ویتالیک مقاله سفیدی را در مورد یک پلتفرم بلاکچینی جدید

منتشـــر کرده بود که ظاهرا بهتر از بیت‌کوین عمل می‌کرد و می‌توانست گام بزرگ دیگری در حوزه بلاکچین باشد.

کنجکاوی و شیفتگی بالا مرا بر آن داشت تا ویتالیک را با پرسش‌هایی در مورد اتریوم و معماری‌اش ســـوال‌پیچ کنم. من تحت تاثیر اختراع او قرار گرفته بـــودم، اما آنچه بیـــش از چیزهای دیگر برایم سوال‌برانگیز بود به نحوه استقرار و گسترش آن بر می‌گشـــت. ویتالیک به همه سوالات من جواب نداد، اما کاملا می‌شد عزم راسخ و خوش‌بینی بیش از حدش در مورد آینده بهتر بلاکچین را در گفتار و رفتار او مشاهده کرد (اگرچه از نظر خیلی‌ها در آن زمان، این خوش‌بینی بالا، ساده‌انگارانه به نظر می‌رسید). احساس کردم که همه ویژگی‌های بلاکچین در اتریوم و بیت‌کوین خلاصه نمی‌شوند. شناخت ویژگی‌های بلاکچین، به بررسی عمیق‌تری نیاز دارد. بلاکچین امکان نقش‌آفرینی در جامعه، حاکمیت، کسب‌وکار و باورهای قدیم و جدید را نیز خواهد داشت. یک عنصر انسانی در این فناوری وجود داشت که راهکارهای منصفانه‌تری را برای دنیای عاری از عدالت و پر از پیچیدگی پیشنهاد می‌کرد. دو هفته بعد با ویتالیک ملاقات کردم و با هر زوری بود او را مجبور کردم تا معماری نحوه کار اتریوم در چارچوب استقرار را برایم شرح دهد. بعد از توضیحاتش، نسخه ابتدایی دست‌نویس‌شده‌ام را کشیدم و به او نشان دادم. چند ثانیه‌ای به آن نگاه کرد، به هم ریخت، نرم‌افزار گرافیکی Inkscape را در رایانه شخصی‌اش باز کرد و دیوانه‌وار شروع به ترسیم اولین نسخه یک فریمورک (چارچوب) معماری مبتنی بر بلاکچین زد که اتریوم را در بر می‌گیرد. نقشه معماری ویتالیک چندین بار تغییر کرد و نهایتا در یکی از پست‌های وبلاگش با عنوان «On Silos» قرار داده شد.

از چند ماه پس از آن تا به امروز، من و ویتالیک چیزهای زیادی از هم آموختیم. او خیلی چیزها را در مورد بلاکچین به من یاد داد و من توصیه‌هایی را در مورد موضوعات مربوط به کسب‌وکار و رشد اتریوم در اختیارش گذاشتم. هرگز نمی‌توانم رویای واقعی ویتالیک در مورد بلاکچین را درک کنم، اما در مورد یک چیز اطمینان دارم؛ ویتالیک یک تاجر زرنگ است که از فناوری‌های طراز اول دیگر الهام می‌گیرد و بنیاد اتریوم و فناوری هسته آن همیشه به رهبری او نیاز دارند.

من ۵۰ پست وبلاگی در مورد بیت‌کوین، بلاکچین و اتریوم نوشـــته‌ام و با مخترعان، نوآوران، پیش‌قراولان، رهبران، کارآفرینان، استارت‌آپ‌ها، مدیران اجرایی سازمان‌ها و متخصصان پیشرو در فناوری بلاکچین و پیاده‌سازی آن ملاقات کرده‌ام.

بخش اعظم این کتاب بر اساس یافته‌های من که حاصل ۳۴ سال تجربه در بخش فناوری است به رشته تحریر درآمد. اولین مرحله از این سفر به ۱۴ سال حضور سازنده در شرکت هیولت‌ـپاکارد (HP) برمی‌گردد. علاوه بر آن، ۱۰ سال به‌عنوان یک مشاور مستقل، نویسنده و اینفلوئنسر در فضای اینترنت مشغول به فعالیت بودم (۱۹۹۵ تا ۲۰۰۵). در سال ۱۹۹۶، یکی از اولین کتاب‌های کسب‌وکارم در رابطه با استراتژی کسب‌وکار اینترنتی را با عنوان «گشایش بازارهای دیجیتال» منتشر کردم. نوشتن این کتاب بهانه‌ای شد تا به تجزیه‌وتحلیل کامل میزان اهمیت وب در کسب‌وکار بپردازم و با شرکت‌های بزرگ و کوچکی که در حال پیاده‌سازی آن بودند، کار کنم. در سال ۲۰۰۵، توانستم به‌عنوان تحلیلگر حرفه‌ای گروه تحقیقاتی آبردین مشغول به کار شوم. کار بعدی‌ام، سه سال حضور در شرکت Cognizant Technology Solutions که به معنای واقعی یک سازمان بدون مرز بود و معاملات ارزی بین‌المللی در مرکز آن انجام می‌گرفت. از سال ۲۰۰۸، به مدت پنج سال به دنیای استارت‌آپ‌ها قدم گذاشتم و دو استارت‌آپ نسبتا موفق (Eqentia و Engagio) را پایه‌ریزی کردم. چیزهایی که از شکست خواهید آموخت، بیش از درس‌هایی است که موفقیت‌ها می‌توانند به شما یاد بدهند.

شور و اشتیاق من به فناوری فرد به فرد (P2P) مبتنی بر بلاک‌چین، اتفاقی نبود. در سال ۲۰۰۱، سایت PeerIntelligence.com را راه انداختم که شرح وقایع اولین موج فناوری‌های P2P را بر عهده داشت. در این مدت، کار اصلی و عمده P2P، به اشتراک‌گذاری فایل محدود می‌شد و من از همان اوایل به قدرت این فناوری جدید اعتقاد داشتم. متاسفانه اولین تلاش‌ها در P2P، بعد از دعاوی حقوقی علیه سرویس موسیقی دیجیتال Napster در نطفه خفه شدند، اما پروتکل BitTorrent آن برای استفاده‌های بعدی حفظ شد.

همه این تجربیات در شکل‌گیری افکارم در مورد بلاکچین تاثیر داشتند و عصاره آنها را در این کتاب مشاهده می‌کنید.

در سال ۲۰۱۳، زمانی که با بیت‌کوین و بلاکچین آشنا شدم، رویاهای اولیه مردم در سال ۱۹۹۵ در مورد نقش تحول‌آفرین اینترنت به ذهنم خطور کرد و به یاد روزهای اولیه ظهور و پیدایش P2P در سال ۲۰۰۱ افتادم. خوشبختانه P2P توانست در سال ۲۰۰۹ که مقارن با تولد بلاکچین بیت‌کوین است، به ایده‌های نظری مربوط به خودش جامه عمل بپوشاند.

در اولین آشنایی‌ام با بلاکچین به یاد حرف‌های اندی گرو در کتاب سال ۱۹۹۶ خودش با عنوان

«تنها بی‌پروایان پایدارند» افتادم؛ «این کسب‌وکار آرامش ندارد. پر از باد و توفان است. اما اگر ۱۰ برابر نیروی خودتان را به خرج بدهید، امکان تغییر نیروی این توفان را پیدا خواهید کرد». البته اندی در مورد اینترنت حرف می‌زد؛ نیرو یی توفانی که می‌تواند هر کسب‌وکاری را با تغییرات اساسی مواجه سازد. امروزه، بلاکچین همان نیروی توفانی ۱۰ برابر است که دارد بسیاری از کسب‌وکارها را تغییر می‌دهد و تازه در اول راه است. اعتراف می‌کنم که برای درک بسیاری از جنبه‌های بلاکچین سختی‌های زیادی را پشت سر گذاشتم. بسیاری از نظریه‌پردازان باهوش آن، افرادی بودند که دید فنی داشتند و کانون توجه اصلی آنها به پیامدهای تجاری آن معطوف نبود. در نتیجه، درک جامع و فراگیر بلاکچین برای من با فراز و نشیب‌هایی همراه بود. اتفاقا همین سختی راه به انگیزه‌ای برای نوشتن این کتاب تبدیل شد. بنابراین تصمیم گرفتم به گونه‌ای این کتاب را بنویسم تا خواننده با ترس و وحشت کمتری بتواند فناوری بلاکچین و شاخه‌های مختلف آن را درک کند.

بلاکچین بخشی از تاریخ اینترنت است. از نظر اهمیت به وب جهان‌شمول می‌رسد و می‌تواند به تحقق بیشتر برخی از ایده‌های اولیه اینترنت، یعنی غیر متمرکز تر بودن، بازتر بودن، امن‌تر بودن، خصوصی‌تر بودن، عادلانه‌تر بودن و دسترس‌پذیرتر بودن کمک کند. راستش را بخواهید، بسیاری از اپلیکیشن‌های بلاکچین، تنها جایگزینی برای اپلیکیشن‌های وب موروثی به حساب می‌آیند که نمی‌توانند توابع اعتماد متمرکز خودشان را کنار بگذارند.

صرف‌نظر از اینکه چه پیش خواهد آمد، داستان بلاک‌چین پس از اینکه شما خواندن این کتاب را هم به پایان برسانید به طور مستمر نوشته خواهد شد، همان‌طور که داستان وب پس از ابداع اولیه به طور مستمر نوشته شده است. اما چیزی که آینده بلاکچین را حتی جالب‌تر می‌کند این است که شما بخشی از آن هستید.

امیدوارم کتاب «کسب‌وکار بلاکچین» که با همه وجود آن را نوشته‌ام، به کارتان بیاید.

ویلیام موگایار
شهر تورنتوی استان انتاریو
wmougaray@gmail.com
مارس ۲۰۱۶

مقدمه

اگر تاکنون تحت تاثیر بلاکچین قرار نگرفته‌اید، قول می‌دهم که به‌زودی مبهوت آن خواهید شد.

بعد از آغاز اینترنت، این اولین فناوری‌ای است که به رویای انسان‌ها جامه عمل می‌پوشاند و با وجود اینکه در ابتدا دامنه کاربرد کمی داشت، به‌سرعت در حال گسترش است.

به دنیای جدید بلاکچین خوش آمدید.

در هسته بلاکچین فناوری‌ای وجود دارد که کارش ثبت دائمی تراکنش‌ها با شرایط زیر است: تراکنش‌ها به‌صورت متوالی به‌روزرسانی می‌شوند؛ هیچ کسی نمی‌تواند تراکنش‌ها را حذف کند؛ و یک دنباله تاریخی بی‌نهایت از تراکنش‌ها وجود دارد. این توصیف عملکردی که ظاهرا ساده به نظر می‌رسد، پیامدهای عظیمی را به همراه خواهد داشت. تعریف بالا موجب می‌شود تا شیوه‌های قدیمی ایجاد تراکنش‌ها، ذخیره‌سازی داده و انتقال دارایی‌ها را مورد بازنگری قرار بدهیم. البته این تازه شروع کار است.

بلاکچین بیش از آنکه یک انقلاب باشد، حرکت آرامی است که به‌تدریج به یک سونامی تبدیل

می‌شود و هر چیزی را که در مسیر پیشرفتش مشکل ایجاد کند، از پیش رو بر می‌دارد. به بیان ساده، اگر وب را اولین لایه اینترنت در نظر بگیریم که در سال ۱۹۹۰ شکل گرفت، بلاکچین را می‌توان به‌عنوان دومین لایه مهم در بالای اینترنت به شمار آورد. کانون توجه اصلی این لایه عمدتا به اعتماد مربوط می‌شود و به همین دلیل نام آن را لایه اعتماد می‌گذاریم.

بلاکچین سرعت تغییر شیوه حاکمیت، روش زندگی، مدل‌های شرکتی سنتی، جامعه و نهادهای بین‌المللی را بالا می‌برد. البته نفوذ بلاکچین با مقاومت‌هایی مواجه خواهد شد، زیرا تغییری که ایجاد می‌کند، بسیار شدید است.

بلاکچین، ایده‌های قدیمی را که برای دهه‌ها و شـــاید قرن‌ها فکر ما را درگیر خود کرده بودند، به مبارزه می‌طلبد. بلاکچین شیوه حاکمیت و روش‌های متمرکز اجرای تراکنش‌ها را به چالش می‌کشد. به‌عنوان مثال، اگر یک بلاکچین بتواند بررسی خودکار و غیرقابل انکاری را انجام بدهد، آنگاه دیگر چه نیازی به پرداخت پول در یک حساب امانی جهت تنظیم بیمه سند مالکیت است؟

بلاکچین، ایجاد اعتماد را که پیش از این در دست نهادهای مرکزی (مثل بانک‌ها، سیاست‌گذاران، موسسات تسویه‌حساب بین‌بانکی، دولت‌ها و شرکت‌های بزرگ) بود، تسهیل خواهد کرد و امکان گریز از این نقاط مرکزی قدیمی را فراهم خواهد ســـاخت. به‌عنوان مثال، چه می‌شـــود اگر بتوانیم تایید اعتبار طرف معامله را به جای کمک گرفتن از یک موسسه تسویه‌حساب بین‌بانکی، روی یک بلاکچین انجام بدهیم؟

بگذارید مثال مشابهی بزنم. در قرن شانزدهم، انجمن‌های صنفی قرون وسطی، انتشار اطلاعات در مورد نحوه نسخه‌برداری از برخی صنایع دستی را کنترل کردند و بدین وسیله آنها را در انحصار خود درآوردند. سانسور اطلاعات در اکثر کشورهای اروپایی از طریق تبانی با کلیسای کاتولیک و دولت‌ها اتفاق می‌افتاد و چاپ و نشر اطلاعات به کسب مجوز نیاز داشت. این نوع کنترل مرکزی و انحصار یکجانبه زیاد طول نکشید و بعد از رشد سریع و انفجاری حوزه چاپ، جریان آزاد اطلاعات تحقق پیدا کرد، امروزه فکر کردن به اینکه نشر دانش یک فعالیت غیرقانونی است حتی قابل تصور هم نیست. می‌توانیم نگهدارنده‌های سنتی اعتماد مرکزی را به‌عنوان انجمن‌های صنفی در نظر بگیریم و این سوال را مطرح کنیم که اگر فناوری بلاکچین بتواند نگهداری اعتماد را به نحو بهتری انجام بدهد، دیگر چه نیازی به ادامه کار آنها خواهد بود.

درست همان‌طور که نهادهای قرون وسطایی مجبور شدند از کنترل حوزه چاپ دست بکشند، محدود شدن عنصر اعتماد به برخی نهادهای موجود نیز توسط بلاک‌چین از میان خواهد رفت.

اگر بلاک‌چین را فقط به‌عنوان یک دفترکل توزیع‌شده در نظر بگیریم، به اشتباه افتاده‌ایم، زیرا دفترکل توزیع‌شده، تنها یکی از ابعاد بی‌شمار بلاک‌چین را نشان می‌دهد. درست مانند اینکه اینترنت را تنها به‌عنوان یک شبکه و پلتفرم انتشار در نظر گرفته باشیم. این ویژگی‌ها و شرایط لازم هستند، اما کافی نیستند. به همین دلیل است که بلاک‌چین را نمی‌توان صرفا در مجموعه‌ای از قابلیت‌های مهم آن خلاصه کرد.

طرفداران بلاک‌چین اعتقاد دارند که اعتماد باید رایگان باشد و نیروی مرکزی نباید آن را از طریق وضع مالیات یا شیوه‌های دیگر (مانند کارمزد، حق دسترسی یا مجوز) محدود کند. آنها بر این باورند که اعتماد می‌تواند و باید به بخشی از روابط فردبه‌فرد تبدیل شود و فناوری بلاک‌چین به سهولت اعمال آن کمک خواهد کرد. اعتماد را می‌توان کدگذاری کرد و درست یا غلط بودن آن را با شیوه قطعی ریاضی مورد محاسبه قرار داد که از طریق رمزگذاری قدرتمند حفاظت می‌شود. اساسا اثبات‌های رمزنگاری جای اعتماد را می‌گیرند و اعتماد با کمک شبکه‌ای از رایانه‌های معتمد (گره‌های درستکار) حفظ می‌شود که به امنیت آن کمک خواهند کرد (برخلاف موجودیت‌های منفردی که موجب بوروکراسی اضافی یا غیرضروری می‌شوند).

اگر بلاک‌چین به روش جدیدی برای پیاده‌سازی تراکنش‌های قابل اعتماد بدون نیاز به واسطه‌های معتمد تبدیل شود، آنگاه می‌توانیم بدون نیاز به واسطه به اعتماد برسیم. در آن صورت، سیاست‌گذارانی که قوانین مربوط به نهادهای معتمد از قبیل بانک‌ها را وضع کرده‌اند، با یک معضل بزرگ مواجه می‌شوند. چگونه می‌توانید برای چیزی که در حال بر باد رفتن است قانون وضع کنید؟ آنها باید قوانین قدیمی خودشان را به‌روز کنند.

اعتماد کنترل‌شده از طریق واسطه با مشکلاتی مواجه بود، اما بلاک‌چین می‌تواند اعتماد بدون اصطکاک را به ارمغان بیاورد. بسیار خوب. سوال مهم دیگر این است که اگر اعتماد مجانی باشد، چه اتفاقی خواهد افتاد؟ طبیعتا این نوع اعتماد با کمترین مقاومت مواجه می‌شود و به‌تدریج شاهد غیرمتمرکز شدن آن در لبه‌های شبکه خواهیم بود.

علاوه بر این، بلاک‌چین‌ها می‌توانند به تبادل دارایی‌ها و ارزش کمک کنند و سرعت انتقال ارزش

همه دارایی‌ها را بدون نیاز به واسطه‌های غیرضروری بالا ببرند.

بلاکچین، نقش زیرساخت بک‌اند (بخش پشتی) را ایفا می‌کند و می‌توانیم آن را به رایانه‌های بدون توقف تشبیه کنیم. بعد از راه‌اندازی، رایانه‌های مزبور، به‌دلیل انعطاف‌پذیری فوق‌العاده بالایشان هرگز از کار نخواهند افتاد. برخلاف سیستم‌های بانکی و سرویس‌های مبتنی بر ابر، هیچ نقطه شکست منفردی در بلاکچین وجود ندارد و با از کار افتادن برخی گره‌ها بلاکچین همچنان به محاسبات خود ادامه خواهد داد.

اینترنت توانست جایگزین برخی واسطه‌ها شود. بلاکچین نیز به‌زودی جای واسطه‌های دیگر را خواهد گرفت و در عین حال واسطه‌های جدیدی را خلق خواهد کرد. واسطه‌های کنونی باید کاملا بر این نکته اشراف داشته باشند که رقابت شدیدی برای غیرمتمرکزسازی همه چیز درگرفته و ممکن است این روند روی نقش آنها تاثیر بگذارد.

افراد زیادی هر روز به تجزیه‌وتحلیل، موشکافی و پیش‌بینی آینده بلاکچین مشغول‌اند؛ چراکه متخصصان فناوری، کارآفرینان و سازمان‌های بزرگ، هنوز در مورد ویتامین بودن یا سم بودن بلاکچین ابهام دارند.

اگرچه امروزه نوشته‌های زیادی به قابلیت‌ها و توانایی‌های بلاکچین اشاره می‌کنند، اما ممکن است قابلیت‌هایی در آینده وجود داشته باشد که اکنون از آنها غافلیم. بیشتر صحبت ما در اینجا معطوف به توانایی‌هایی است که می‌توان از بلاکچین انتظار داشت. درست همانند اینترنت، وب و بانک‌های اطلاعاتی، بلاکچین نیز اصطلاحات فنی جدیدی دارد.

از اواسط دهه ۱۹۵۰ به بعد که فناوری اطلاعات تکامل پیدا کرد، با اصطلاحات فنی جدیدی آشنا شدیم؛ کامپیوترهای بزرگ، بانک‌های اطلاعاتی، شبکه‌ها، سرویس‌دهنده‌ها، نرم‌افزار، سیستم‌های عامل و زبان‌های برنامه‌نویسی. از اوایل دهه ۱۹۹۰، واژگان جدیدی بر سر زبان‌ها افتادند؛ مرورگری، وب‌سایت، جاوا، بلاگ‌نویسی، URL، HTTP، SMTP، TCP/IP‌ها و HTML. امروزه نیز با ظهور و پیدایش بلاکچین، با مفاهیم جدیدی مواجه هستیم؛ الگوریتم‌های اجماع، قراردادهای هوشمند، دفترکل‌های توزیع‌شده، اوراکل‌ها، کیف پول‌های دیجیتال و بلوک‌های تراکنش.

در این کتاب، به‌صورت گام‌به‌گام، شما را با اصطلاحات این فناوری، تعریف بلاکچین، حوزه نفوذ و پیامدهای تغییراتی که به‌واسطه آن ایجاد می‌شوند آشنا خواهم کرد.

امروزه جست‌وجوی ما در گوگل عمدتا به اطلاعات و محصولات خلاصه می‌شود، اما در آینده می‌توان از طریق گوگل، اعتبار رکوردها، هویت‌ها، اصالت، حقوق، کار انجام‌شده، اسناد مالکیت، قراردادها و فرایندهای مربوط به دارایی‌های ارزشمند دیگر را تایید کرد. به‌زودی همه چیز می‌تواند گواهی مالکیت دیجیتال دریافت کند. درست همان‌طور که نمی‌توان هیچ پول دیجیتالی را دو بار خرج کرد (با تشکر از ساتوشی ناکاموتو به خاطر اختراعش)، امکان کپی مضاعف یا جعل گواهینامه‌های رسمی موجود در بلاکچین نیز وجود نخواهد داشت. بلاکچین توانست به ما کمک کند تا برای این بخش فراموش‌شده از انقلاب اطلاعاتی، راهکار ارائه دهیم.

هنوز یادم نرفته است که وقتی برای اولین بار در سال ۱۹۹۴ شرکت پست فدکس اعلام کرد که می‌توانید بسته ارسالی را از طریق وب ردیابی کنید، چه هیجانی داشتم. اگرچه امروزه این نوع خدمات زیاد به چشم نمی‌آیند، اما سرویس فدکس نقطه عطفی در اوایل روزهای وب به‌شمار می‌رفت. پیغام اساسی آن اتفاق این بود که سرویسی که پیش از این به بخش خصوصی محدود می‌شد، به‌صورت مجانی در دسترس همه افرادی که به اینترنت دسترسی داشتند، قرار می‌گرفت. برخی از این خدمات به شرح زیر بودند: بانکداری برخط، ثبت مالیات، خرید محصولات، خرید و فروش سهام و بررسی سفارش‌ها. درست همان‌طور که امکان دسترسی به سرویس‌های جست‌وجوی بانک‌های اطلاعاتی عمومی را داریم، می‌توانیم سرویس‌هایی را نیز برای بررسی زنجیره‌های بلوکی و تایید صحت اطلاعات در اختیار داشته باشیم. همه ما علاوه بر دسترسی به اطلاعات، خواهان دسترسی به حقیقت نیز هستیم و انتظار داریم تغییر رکوردهای مختلف با حداکثر شفافیت اتفاق بیفتد. بلاکچین ادعا می‌کند که می‌تواند این نوع شفافیت را در اختیار ما قرار دهد.

در حقیقت این سوال قدیمی که «آیا این در بانک اطلاعاتی قرار دارد؟» جای خود را به «آیا این روی بلاکچین قرار دارد؟» خواهد داد.

آیا بلاکچین پیچیده‌تر از وب است: قطعا.

اکنون برای سفر به عمق بلاکچین با من همراه شوید.

فصل یک

بلاکچین چیست؟

«اگر نتوانید آن را بدون توضیح درک کنید، پس با توضیح دادن نیز آن را درک نمی کنید.»
هاروکی موراکامی

به دقت توجه کنید. این فصل احتمالا مهم‌ترین فصل این کتاب است، زیرا در نظر دارد یک توضیح پایه‌ای از بلاکچین ارائه دهد. در این فصل یک نمای کلی از پتانسیل های بلاکچین به شما ارائه می‌شود. درک بلاکچین کمی سخت است. شما قبل از اینکه با پتانسیل های آن آشنا شوید، باید بتوانید پیام آن را درک کنید. بلاکچین علاوه بر ظرفیت‌های فنی و تکنولوژیکی، زمینه‌های فلسفی، فرهنگی و ایدئولوژیکی نیز دارد که باید درک شوند.

بلاکچین محصولی نیست که شما همین طوری روشن کرده و استفاده کنید، شما باید یک توسعه‌دهنده نرم‌افزار باشید تا بتوانید از آن استفاده کنید. بلاکچین سایر محصولاتی را که شما از آنها استفاده می کنید، تهیه می کند، اگرچه شما ممکن است ندانید که یک بلاکچین در پشت آنها وجود دارد، همان‌طور که از پیچیدگی های چیزی که هم‌اکنون در وب مشاهده می کنید باخبر نیستید. وقتی

خودتان و بدون تلاش به درک بلاکچین شروع به تصور امکانات و احتمالات آن می کنید، شما در مرحله‌ای دیگر از بلوغ خود برای بهره‌برداری از آن خواهید بود.

به اعتقاد من انتقال دانش مربوط به درک بلاکچین بسیار راحت‌تر از این است که بدانیم بلاکچین مناسب چه جاهایی هست. مانند یادگیری رانندگی است. من می توانم به شما یاد بدهم چطور یک ماشین را برانید، اما نمی توانم پیش‌بینی کنم که شما آن را کجا می برید. فقط خودتان از تجارت‌ها یا موقعیت‌های خاص خبر دارید و پس از اینکه درک کردید بلاکچین چه کارهایی می تواند بکند، این فقط شما هستید که می توانید بفهمید بلاکچین مناسب چه جایی است. البته ما اول به آزمایش‌ها و ارزیابی‌ها خواهیم پرداخت تا ایده‌هایی از این مفهوم به شما بدهیم.

مشاهده مقاله ساتوشی

هنگامی که تیم برنرز لی، اولین صفحه وب را در سال ۱۹۹۰ ایجاد کرد، نوشت: «وقتی ما اطلاعات را در وب به یکدیگر پیوند می دهیم، خودمان را قادر میسازیم حقایق را کشف کنیم، ایده‌ها را ایجاد کنیم، چیزها را بخریم و بفروشیم و با سرعت و مقیاسی که در دنیای آنالوگ قابل تصور نبود، روابط جدید ایجاد کنیم.»

در این بیانیه کوتاه، برنرز لی، جست‌وجو، انتشار، تجارت الکترونیک، پست الکترونیکی و رسانه‌های اجتماعی را یکجا و با یک بیانیه پیش‌بینی کرده است. معادل بیت‌کوین با آن نوع پیش‌بینی که کسی چیزی خارق‌العاده ایجاد کرده است را می توان در مقاله سال ۲۰۰۸ ساتوشی ناکاموتو با نام «بیت‌کوین؛ یک سیستم پول الکترونیک فرد به فرد» یافت که اساس ریشه ابداع ارز رمزنگاری شده مبتنی بر بلاکچین مدرن به حساب می آید.

خلاصه مقاله پایه بیت‌کوین و اصول اولیه آن توضیح داده شده است:

- یک نسخه کاملا فرد به فرد از پول نقد الکترونیکی اجازه می دهد که پرداخت آنلاین بدون استفاده از یک موسسه مالی و به‌طور مستقیم از یک طرف به طرف دیگر انجام گیرد.
- برای جلوگیری از خرج مضاعف به یک شخص ثالث مورد اعتماد نیازی نیست.
- ما با استفاده از یک شبکه فرد به فرد راه‌حلی برای مشکل خرج مضاعف ایجاد کردیم.

شبکه تراکنش‌ها را با استفاده از فرآیند هشینگ و در درون زنجیره‌های پیوسته مبتنی بر هش اثبات کار

تایید می‌کند، و سابقه‌ای برای آن ایجاد می‌کند که نمی‌توان آن را بدون انجام مجدد اثبات کار تغییر داد.

طولانی‌ترین زنجیره نه‌تنها به‌عنوان اثبات دنباله‌ای از وقایع مشاهده‌شده عمل می‌کند؛ بلکه به‌عنوان اثباتی که از بزرگ‌ترین مخزن نیروی CPU آمده است نیز عمل می‌کند. تا زمانی که اکثریت قدرت و نیروی CPU توسط گره‌هایی کنترل می‌شود که در حمله به شبکه شرکت ندارند، آنها طولانی‌ترین زنجیره را ایجاد کرده و از مهاجمان پیشی می‌گیرند.

شبکه خودش به ساختار حداقلی نیاز دارد. پیام‌ها بر اساس بهترین تلاش پخش می‌شوند و گره‌ها می‌توانند از طریق شبکه به‌طور اتفاقی بیرون بروند و دوباره به شبکه متصل شوند و طولانی‌ترین زنجیره اثبات کار را به‌عنوان مدرکی از آنچه در نبود آنها رخ داده، قبول کنند.

اگر شما یک خواننده غیرفنی هستید و روی قسمت‌های پررنگ‌تر تمرکز می‌کنید، حتما تاکنون توانسته‌اید چیزهایی را درک کنید. لطفا نکات بالا را دوباره بخوانید تا زمانی که منطق ترتیب ناکاموتو در ذهن شما بنشیند. شما باید باور کنید و بپذیرید که معتبر ساختن تراکنش‌های فرد به فرد فقط وقتی میسر هستند که به شبکه اجازه داده شود یک وظیفه اعتمادی را بدون دخالت مرکز یا دستی انجام دهد.

با تفسیر مقاله ناکاموتو باید به این نکات توجه کنیم:

- معامله‌های الکترونیکی فرد به فرد و اثر متقابل
- عدم دخالت نهادهای مالی؛
- اثبات رمزنگاری به جای اعتماد مرکزی؛
- اعتماد به شبکه به جای اعتماد به نهاد مرکزی

مشخص است که بلاکچین تکنولوژی است که پشت بیت‌کوین قرار دارد و باعث تحقق بیت‌کوین شده است. حال که خلاصه مقاله ساتوشی هنوز در ذهن شماست، بیایید سه تعریف متفاوت ولی تکمیلی از بلاکچین را ارائه دهیم؛ تعاریف فنی، کسب و کاری و قانونی.

از نظر فنی بلاکچین یک پایگاه داده back-end (عقبه) است که یک دفترکل توزیع‌شده را که می‌تواند آزادانه بازبینی شود، حفظ و نگهداری می‌کند. از لحاظ کسب و کاری، بلاکچین یک شبکه تبادل برای معاملات، ارزش‌ها و دارایی‌های در حال حرکت بین کامپیوترها؛ آن هم بدون کمک یک واسطه است. از نظر قانونی، بلاکچین معاملات را معتبر می‌کند و جایگزین نهادهایی شده است که قبلا مورد اعتماد بودند.

فنی	پایگاه‌داده back-end (عقبه) که یک دفترکل توزیع‌شده را آزادانه حفظ و نگهداری می‌کند.
کسب‌وکاری	شبکه تبادل برای انتقال ارزش بین همتایان
قانونی	مکانیسم تایید یک معامله که به واسطه‌ای نیاز ندارد.

وب، همه چیز از نو

گذشته، قطب‌نمای دقیق آینده نیست، اما درک اینکه از کجا آمده‌ایم، به ما کمک می‌کند که دید واضح و روشن و نیز زمینه بهتری برای جایی که می‌رویم به دست آوریم. بلاکچین فقط بخشی از ادامه تاریخ فناوری اینترنت است که توسط وب نشان داده می‌شود و همان‌طور که به سفر خود ادامه می‌دهد، به دنیا، تجارت، جامعه و دولت ما رخنه کرده و از چندین چرخه و مرحله می‌گذرد که فقط از آینه جلویی قابل رویت هستند.

اگرچه اینترنت برای اولین بار در سال ۱۹۸۳ افتتاح شد، اما این شبکه جهانی وب بود که لحظات تکاملی را در اختیار ما گذاشت؛ زیرا اطلاعات و خدمات مبتنی بر اطلاعات را به‌صورت آشکار و بلافاصله برای هر کسی که روی زمین و به وب متصل است، قابل دسترس می‌کرد. همان‌طور که در حال حاضر میلیاردها نفر از مردم در سراسر جهان به وب متصل هستند، میلیون‌ها نفر و سپس میلیاردها نفر به بلاکچین‌ها متصل خواهند شد. ممکن است سرعت استفاده از بلاکچین از رشد کاربران وب‌سایت‌های اینترنتی بیشتر شود که جای تعجبی هم ندارد.

تا اواسط سال ۲۰۱۶، ۴۷ درصد از ۷/۴ میلیارد نفر جمعیت دنیا دارای ارتباط اینترنتی بودند. در سال ۱۹۹۵ این تعداد کمتر از یک درصد بود. افزایش این تعداد به یک میلیارد کاربر اینترنتی تا سال ۲۰۰۵ به طول انجامید. در مقابل استفاده از تلفن همراه رشد سریع‌تری داشت و در سال ۲۰۰۲ تعداد کاربران تلفن همراه از تعداد کاربران تلفن‌های ثابت گذشت و در سال ۲۰۱۳ از تعداد جمعیت جهان نیز فراتر رفت. برای وب‌سایت‌ها نیز می‌توان گفت که تعداد کل آنها در سال ۲۰۱۶ حدود یک میلیارد بود. احتمالا بلاکچین‌ها به چندین نوع تقسیم خواهند شد و به‌راحتی برای راه‌اندازی وب‌سایت‌ها در وردپرس (Wordpress) یا Squarespace قابل تنظیم خواهند بود.

افزایش استفاده از بلاکچین مزیت‌هایی برای خط سیر وب نیز دارد؛ زیرا نقطه شروع آن را در

چهار بخش تقویت می‌کند؛ کاربران وب، کاربران تلفن همراه، صاحبان وب‌سایت‌ها و هر چیز دیگری که از اتصال آنها سود می‌برد و به یک چیز هوشمند تبدیل می‌شود. در واقع استفاده از بلاکچین در این چهار دسته قرار خواهد گرفت و در عوض به‌دنبال کاربران جدید خواهد بود.

یک بلاکچین یا چندین بلاکچین؟

هیچ پارادایم یا نمونه قبلی‌ای از بلاکچین وجود ندارد. بلاکچین نسخه جدید TCP/IP، یا پروتکل شبکه اینترنت نیست. بلاکچین همچنین یک نوع اینترنت جدید نیست. در سال ۲۰۱۵، برخی از طرفداران بلاکچین بیت‌کوین از وجود چندین بلاکچین اظهار تاسف کردند. بلاکچین از طریق یک لنز تک‌بعدی (بیشینه‌گرای بیت‌کوین) دیده می‌شد و نگرشی که نسبت به آن وجود داشت، شبیه به اینترنت بود. بله، خیلی خوب است که تنها یک اینترنت وجود دارد، وگرنه هرگز اینقدر گسترش نمی‌یافت. اما بلاکچین یک ساختار متفاوت است و بیشتر شبیه به یک محصول جدید است که در بالای اینترنت قرار دارد، درست همان‌طور که صفحات جهانی وب از طریق استانداردهای تکنولوژی‌شان در بالای اینترنت قرار دارند.

بلاکچین بخشی از پایگاه داده، پلتفرم توسعه و توانمندساز شبکه است، بنابراین ما به نمونه‌های بسیاری از آن و نیز تغییرات زیادی از آن نیاز داریم. بلاکچین پوششی است که در بالای اینترنت قرار گرفته و انواع مختلفی از پیاده‌سازی را انجام می‌دهد. بلاکچین را می‌توان به‌عنوان یک لایه اعتماد، یک واسطه تبادل، یک لوله امن، مجموعه‌ای از قابلیت‌های غیر متمرکز و حتی بیشتر از اینها دید.

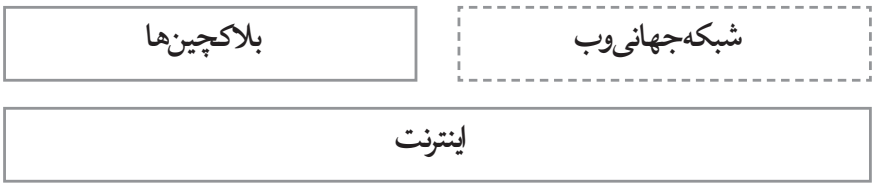
البته از لحاظ چگونگی پذیرش تکنولوژی، باید بدانید که شباهت‌های زیادی بین سال‌های اولیه به‌وجودآمدن وب و تکامل بلاکچین وجود دارد.

فراموش نکنید پس از اینکه مشخص شد صفحات وب می‌تواند در تجارت هم به کار گرفته شود، حدودا سه سال طول کشید تا اکثر شرکت‌ها توانستند به‌طور کامل توانایی‌های وب را درک کنند (تقریبا ۱۹۹۷-۱۹۹۴) و از زمان اختراع اینترنت در سال ۱۹۸۳ حدود هفت سال طول کشید تا صفحات وب به وجود آمدند. شکی نیست که بلاکچین پدیده نیمه‌مرموز و نیمه‌پیچیده بین سال‌های ۲۰۱۸-۲۰۱۵ است، همان‌طور که سه سال طول کشید (۲۰۱۲-۲۰۰۹) تا عموم مردم با بیت‌کوین آشنا شدند.

معرفی کاربردهای بلاکچین

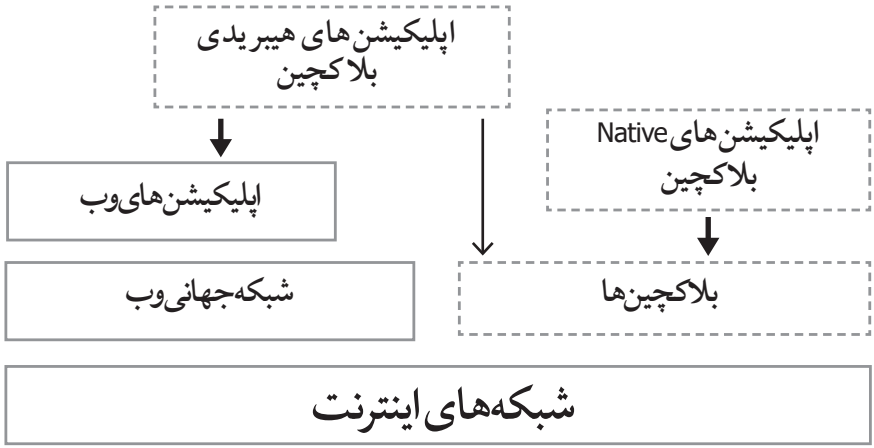
وب بدون اینترنت نمی‌تواند وجود داشته باشد. بلاکچین نیز نمی‌تواند بدون اینترنت وجود داشته باشد. وب باعث مفیدتر شدن اینترنت شد، زیرا مردم علاقه بیشتری به استفاده از اطلاعات نشان می‌دادند تا اتصال کامپیوترها به یکدیگر. بلاکچین نیز به اینترنت نیاز دارد، اما می‌تواند وب را کنار بگذارد و نسخه جدیدی به ما بدهد که غیر متمرکزتر و شاید عادلانه‌تر باشد. این یکی از بزرگ‌ترین وعده‌های فناوری بلاکچین است.

بلاکچین نیز همانند وب به اینترنت نیاز دارد



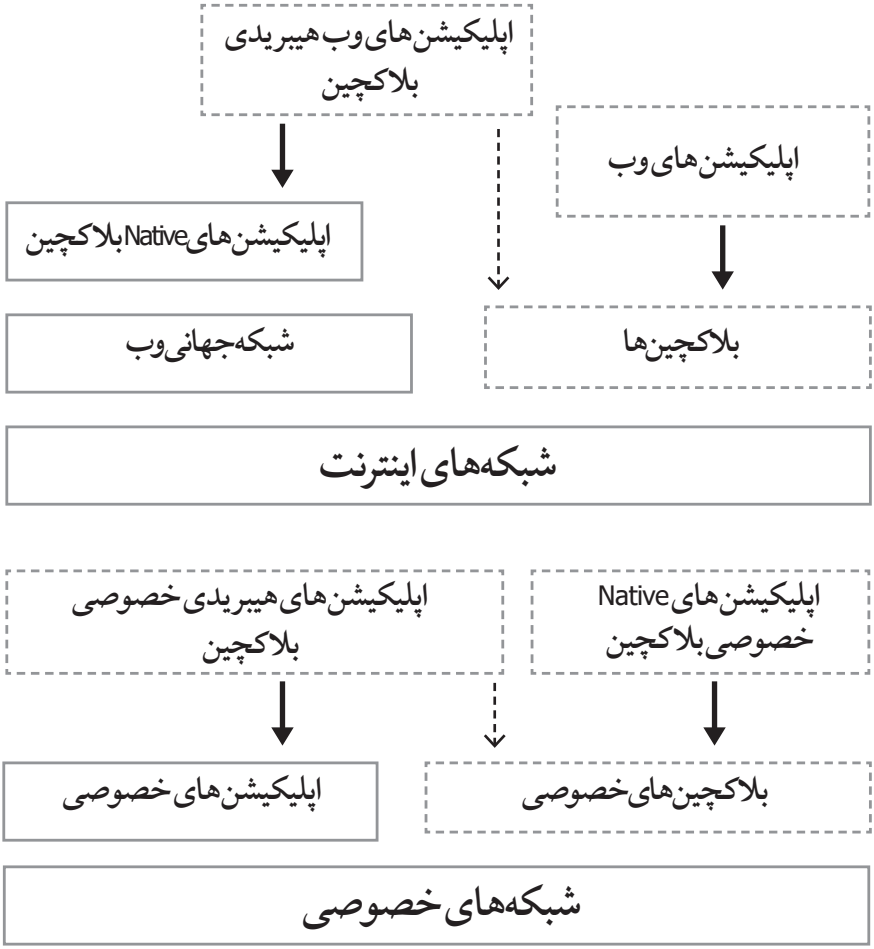
بیش از یک راه برای ساخت اپلیکیشن مبتنی بر بلاکچین وجود دارد، شما می‌توانید اپلیکیشن‌ها را به طور ساده روی یک بلاکچین بسازید، یا اینکه آنها را در اپلیکیشن‌های وب موجود ترکیب کنید که ما آن را یک چاشنی می‌نامیم: «اپلیکیشن‌های بلاکچین ترکیبی» (hybrid blockchain applications)

چاشنی‌ها و انواع برنامه‌های بلاکچین



از آنجایی که اینترنت شامل یک نسخه عمومی و چندین نسخه خصوصی است، بلاکچین‌ها نیز همین مسیر را دنبال می‌کنند. بنابراین، ما بلاکچین‌های عمومی و خصوصی خواهیم داشت. بعضی از آنها به‌صورت ساده به یک بلاکچین دیگر متصل می‌شوند، در حالی که بقیه ممکن است به‌طور ترکیبی پیکربندی شده باشند و بخشی از یک وب‌سایت یا برنامه خصوصی باشند.

چهار نوع مختلف از برنامه‌های بلاکچین



روایت‌پردازی بلاکچین بسیار قوی است

نشانه تاثیر قوی یک تکنولوژی یا روند، این است که آیا روایت قوی‌ای دارد یا خیر. چه تفاوتی بین یک داستان و روایت وجود دارد؟ یک داستان معمولا هماهنگ و شناخته‌شده است و یک روایت داستان‌های فردی بیشتری را برای هر کسی که با آن روبه‌رو می‌شود، ایجاد می‌کند.

جان هگل این تفاوت را به خوبی توضیح می‌دهد:

داستان‌ها تودار و کامل‌اند؛ آنها دارای یک آغاز، یک وسط و یک پایان هستند. از سوی دیگر، روایت‌ها دارای پایان باز هستند – نتیجه حل نشده باقی می‌ماند و تعیین نمی‌شود. دوم اینکه، داستان‌ها در مورد من، یا همان قصه‌گو، یا دیگران هستند؛ آنها در مورد شما نیستند.

در مقابل، در روایت‌ها بسته به انتخاب شما و اقداماتی که شما انجام می‌دهید، نتیجه تعیین می‌شود.

اینترنت روایت قوی‌ای داشت. اگر از افراد مختلفی درباره نحوه استفاده‌شان از اینترنت یا آنچه به آنها مربوط می‌شود، بپرسید، بدون شک می‌توانید پاسخ‌های مختلفی را بشنوید، زیرا هر فرد بسته به استفاده‌هایی که از اینترنت دارد، اینترنت را به خود اختصاص می‌دهد.

بلاکچین یک روایت قوی دارد، زیرا تخیل ما را به کار می‌اندازد. به گفته هگل، مواردی که در ادامه به آنها اشاره می‌شود، مزایای خاصی هستند که روایت‌ها ارائه می‌دهند:

- **تقسیم‌بندی:** به شما کمک می‌کند که از جمعیت جدا شوید.
- **قدرت نفوذ:** افراد خارج از شرکت شما را بسیج می‌کند.
- **نوآوری توزیع‌شده:** نوآوری را در جهت‌های غیر منتظره‌ای گسترش می‌دهد.
- **جذابیت:** با فرصت‌ها و چالش‌هایی که ترتیب داده‌اید، مردم را جذب می‌کند.
- **روابط:** روابط پایدار را با دیگران به وجود می‌آورد که تحت نفوذ روایت شما قرار دارد.

جان هگل مشخص می‌کند که «این مهم مربوط به اتصال و بسیج دیگران از مرزهای ... است». نقطه‌ها را با بلاکچین عوض کنید؛ آنگاه شما یک روایت بلاکچین قوی و بلندمدت خواهید داشت.

یک اَبَرتکنولوژی

بلاکچین یک ابرتکنولوژی است؛ زیرا تکنولوژی‌های دیگر را تحت تاثیر قرار می‌دهد و خودش

از چندین تکنولوژی تشکیل شده است. بلاکچین پوششی از کامپیوترها و شبکه‌هایی است که در بالای اینترنت ساخته شده‌اند. وقتی شما لایه‌های معماری یک بلاکچین را بررسی می‌کنید، متوجه خواهید شد که از چندین قسمت تشکیل شده است؛ پایگاه‌داده، نرم‌افزار کاربردی، تعدادی کامپیوتر که به یکدیگر متصل شده‌اند، مشتریانی برای دسترسی به آن، محیط نرم‌افزاری برای توسعه آن، ابزاری برای نظارت بر آن و قطعات دیگر (که در فصل ۶ بررسی خواهند شد).

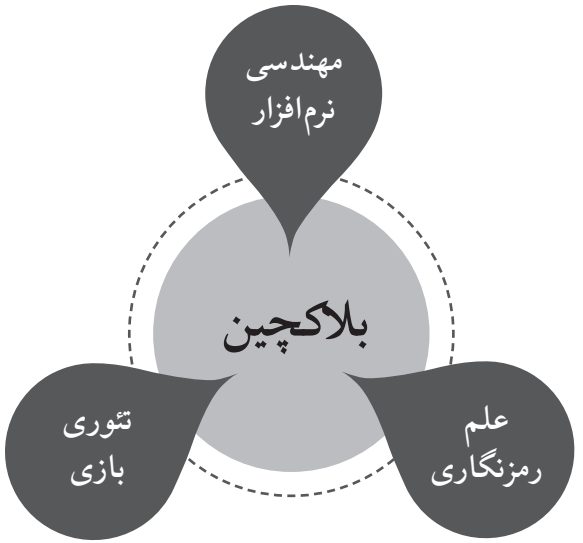
بلاکچین فقط یک تکنولوژی جدید نیست؛ بلکه نوعی تکنولوژی است که سایر تکنولوژی‌های نرم‌افزاری موجود را به چالش می‌کشد، زیرا بلاکچین این پتانسیل و قابلیت را دارد که جایگزین روش‌های موجود شده یا آنها را کامل کند. در اصل، بلاکچین یک تکنولوژی است که سایر تکنولوژی‌ها را تغییر می‌دهد.

آخرین باری که شاهد چنین فناوری عالی‌ای بودم، به زمان ورود وب بر می‌گردد. وب نیز نحوه نوشتن برنامه‌های نرم‌افزاری را تغییر داد و تکنولوژی‌های نرم‌افزاری جدیدی را با خود به همراه آورد که تکنولوژی‌های نرم‌افزاری قدیمی را به چالش می‌کشیدند و جایگزین آنها می‌شدند. در سال ۱۹۹۳، زبان نشانه‌گذاری HTML باعث تغییر حالت انتشار در وب شد. در سال ۱۹۹۵، جاوا زبان برنامه‌نویسی تحت وب را تغییر داد. چند سال قبل از آن TCP/IP (پروتکل شبکه کامپیوتری) فرآیند شبکه‌سازی را در سراسر جهان تغییر داد.

از نقطه نظر یک برنامه‌نویس، یکی از بزرگ‌ترین نمونه‌ها و پارادایم‌های تغییر که بلاکچین ادعا کرده است، به چالش کشیدن عملکرد و انحصاری بودن پایگاه‌داده‌های سنتی به آن شکلی است که ما آنها را می‌شناسیم. بنابراین ما باید عمیقا درک کنیم که چطور بلاکچین ما را مجاب می‌کند درباره سازه‌های پایگاه‌های داده موجود مجددا فکر کنیم.

نرم‌افزار، رمزنگاری و نظریه بازی

روش دیگر برای درک بلاکچین مشاهده هیجان‌ها و غوغاهای ایجادشده در سه رشته مختلف است: ۱) نظریه بازی، ۲) علم رمزنگاری، ۳) مهندسی نرم‌افزار. این سه رشته از زمان‌های قدیم به‌طور مجزا وجود داشته‌اند، اما برای اولین‌بار به‌طور هماهنگ با یکدیگر ترکیب شده و در داخل فناوری بلاکچین متبلور شده‌اند.



نظریه بازی «با اســتفاده از مدل‌های ریاضی به تحلیل روش‌های همکاری یا رقابت موجودات منطقی و هوشمند می‌پردازد.»

و از آنجایی که بلاکچین بیت‌کوین که توسط ساتوشــی ناکاموتو ابداع شده بود، مجبور به حل معمای نظریه بازی شناخته‌شده‌ای به نام مساله ژنرال بیزانس بود، پس نظریه بازی به بلاکچین مربوط می‌شود. برای حل این مساله باید هر تلاشی را که از سوی ژنرال‌های غیراخلاقی صورت می‌گیرد، تســکین و تخفیف داد، در غیر این صورت آنها به تعدادی خائن تبدیل می‌شوند که برای رسیدن به پیروزی حملات خود را هماهنگ می‌کنند.

این کار با اجرای یک فرآیند برای تایید کار انجام شــده و ایجاد محدودیت زمانی مورد نیاز برای مشاهده پیام‌های غیرقابل اعتماد انجام می‌گیرد، تا بتوان از اعتبار آنها اطمینان حاصل کرد. پیاده‌سازی «تحمل خطای بیزانتی» بسیار مهم است، زیرا با این فرض آغاز می‌شود که شما نمی‌توانید به هیچ کسی اعتماد کنید، اما با این حال اطمینان خاطر می‌دهد که معاملات بر اساس اعتمادی که به شبکه در طول این نقل‌وانتقال و در حین نجات از حملات احتمالی، وجود داشــت به سلامت به مقصد رسیده است.

دلایل بنیادینی برای استفاده از این روش رسیدن به امنیت در معاملات نهایی وجود دارد زیرا وجود و نقش واسطه‌های مورد اعتماد فعلی را که اختیار سنتی اعتباردهی به معاملات را بر عهده دارند، زیر سوال می‌برد. این امر باعث می‌شود ما به این پرسش فکر کنیم: چرا به یک قدرت مرکزی نیاز داریم تا مطمئن شویم وقتی تراکنش‌ها از طریق اینترنت و از فردی به فرد دیگری انتقال پیدا می‌کند به همان اعتماد دست می‌یابیم؟

علم رمزنگاری در جاهای مختلف برای ارائه امنیت برای شبکه بلاکچین مورد استفاده قرار می‌گیرد و سه مفهوم کلی دارد؛ هش کردن، کلیدها و امضاهای دیجیتال. یک هش اثر انگشت خاص و منحصربه‌فردی است که تایید می‌کند بخش خاصی از اطلاعات دستکاری نشده است، آن هم بدون اینکه نیازی به بررسی آن داشته باشد. کلیدها حداقل در دو ترکیب استفاده می‌شوند: کلیدهای عمومی و کلیدهای خصوصی. به‌عنوان مثال، دری را در نظر بگیرید که برای باز شدن به دو کلید نیاز دارد. در این حالت، کلید عمومی توسط فرستنده برای کدگذاری و رمزنگاری اطلاعات استفاده می‌شود و فقط صاحب کلید خصوصی می‌تواند آن را رمزگشایی کند. شما هرگز کلید خصوصی خود را به کسی نشان نمی‌دهید. یک امضای دیجیتال یک محاسبه ریاضی است که برای اثبات اصل بودن و معتبر بودن یک سند یا پیام (دیجیتالی) مورد استفاده قرار می‌گیرد.

رمزگذاری مبتنی بر هژمونی عمومی/خصوصی است. شما می‌توانید آدرس خانه خودتان را به‌صورت عمومی منتشر کنید، اما این کار هیچ اطلاعاتی درباره شکل داخلی خانه شما ارائه نمی‌دهد. شما برای ورود به خانه خصوصی خودتان به یک کلید خصوصی نیاز دارید و از آنجایی که ادعا کرده‌اید آن آدرس از آن شماست، هیچ کس دیگری حق ندارد ادعای آدرسی مشابه با آدرس شما داشته باشد. اگرچه مفهوم رمزنگاری مدت‌هاست که وجود دارد، اما مهندسان نرم‌افزار در تلاش هستند آن را با نوآوری نظریه بازی ترکیب کنند تا بتوانند روی هم رفته ساختمان بلاکچین که عدم قطعیت ظاهری را با اطمینان ریاضی قریب‌الوقوع کاهش می‌دهد.

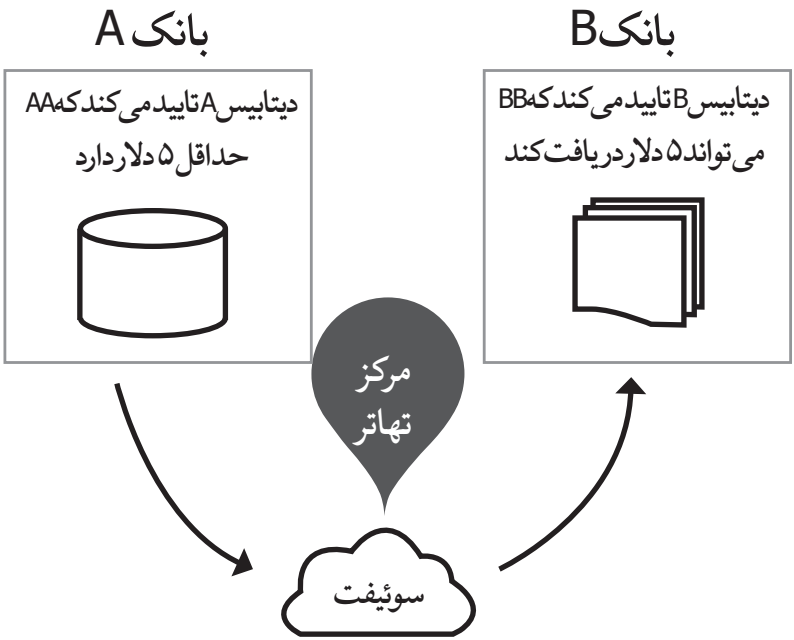
پایگاه داده در برابر دفترکل

ما معاملاتی داریم که می‌توانند بدون کمک یک شخص ثالث مورد تایید قرار بگیرند. حال، شما فکر می‌کنید که پس پایگاه داده چه می‌شود؟ ما همیشه تصور می‌کردیم که پایگاه داده‌ها مخازن مورد

اعتمادی برای نگهداری دارایی ها هستند.

در مورد بلاکچین می توان گفت که دفترکل یک سابقه غیرقابل انکار است که رجیستری معاملاتی که توسط شبکه بلاکچین اعتبارسنجی شده‌اند را نگه می دارد.

حال بیایید تاثیر این وضعیت را مورد بررسی قرار دهیم؛ پایگاه داده در مقابل دفترکل (بلاکچین).



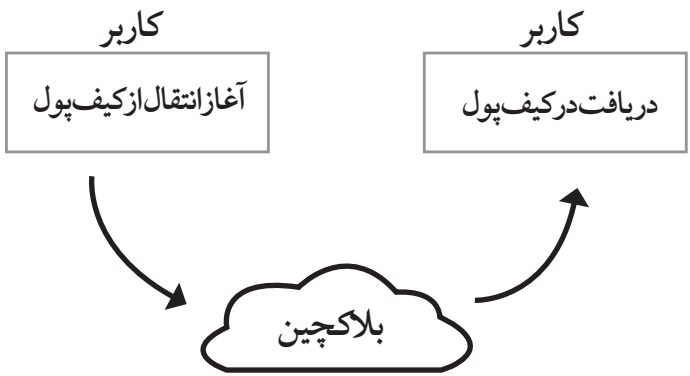
وقتی یک حساب بانکی باز می کنید، شما واقعا اختیار حساب خود را به بانک واگذار کرده‌اید. در واقع، آنها توهم دسترسی و فعالیت شفاف با آن حساب را به شما نشان داده‌اند. هر زمان که بخواهید پول را جابه‌جا کنید، به کسی پرداخت داشته باشید، یا سپرده‌ای داشته باشید، بانک به شما دسترسی صریح می دهد، زیرا شما به آنها اعتماد ضمنی داده‌اید. اما این «دسترسی» نیز توهم دیگری است. این دسترسی در واقع دسترسی به سابقه پایگاه داده است که می گوید شما چنین مقدار پولی دارید. باز هم، آنها با ارائه این توهم که شما صاحب آن پول هستید، فریب‌تان می دهند. اما آنها مسئولیت بالاتری را در اختیار دارند، زیرا آنها پایگاه داده‌ای را دارند که به آن مطلب اشاره دارد که می گوید شما

پول دارید و شما فرض می‌کنید که پول خودتان را در اختیار دارید.

بانکداری پیچیده است، اما من سعی کردم تصویر فوق را ساده‌تر کنم تا بتوانم بر این موضوع تاکید داشته باشم که یک بانک مشخص برای اعطا یا رد دسترسی به پولی که در اختیار دارند، دارای سلسله مراتب کنترلی است. همین مفهوم را می‌توان برای هر دارایی دیجیتالی (سهام، اوراق قرضه، اوراق بهادار) که یک موسسه مالی ممکن است از طرف شما نگه داشته باشد، به کار برد.

ورود به بلاکچین

در ابتدایی‌ترین حالت، همین سناریو ممکن است بدون پیچیدگی‌های بالا نیز رخ دهد. یک کاربر می‌تواند از طریق کیف پول منحصر به‌فرد، پول را به دیگری بفرستد و شبکه بلاکچین تصدیق این کار را بر عهده دارد و حدوداً در ۱۰ دقیقه کار اعتبارسنجی و انتقال را با یا بدون تبادل رمزنگاری در وسط این کار، انجام می‌دهد.



یعنی جادوی بلاکچین در همین شکل ساده آن است. به همین دلیل است که من به هر کسی که قرار است در پیاده‌سازی و اجرای بلاکچین درگیر شود، پیشنهاد می‌دهم اجرا و اعمال این نوع از معاملات را با کیف پول خودش تجربه کند و این کیف پول را، یا با دانلود کردن یکی از نسخه‌های موجود، یا با ثبت نام در یک صرافی محلی بیت‌کوین که در هر جایی که زندگی می‌کنید وجود دارد، می‌تواند به دست بیاورد. پس از اینکه این کار را انجام دادید، متوجه معنای واقعی «بدون واسطه» خواهید شد و شروع خواهید کرد به پرسیدن این سوال که چرا ما هنوز از واسطه‌های فعلی استفاده می‌کنیم.

نگاه به گذشته برای اینکه بتوانیم نگاهی به آینده داشته باشیم

بلاکچین در کجای سیر تکاملی تکنولوژی قرار می‌گیرد؟

در سال ۲۰۰۳، «نیکلاس. جی. کار» مقاله‌ای را در مجله «هاروارد بیزنس ریویو» با عنوان «IT چه اهمیتی دارد» ارائه داد که محافل فناوری اطلاعات را تکان داد و ارتباط استراتژیک آنها را زیر سوال برد. او نوشت:

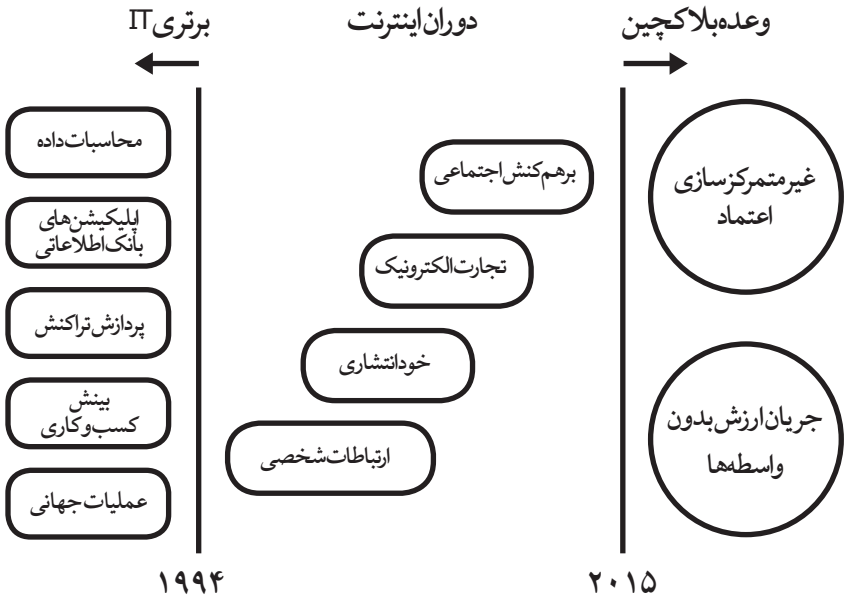
«آنچه منابع واقعا اســتراتژیک را ایجاد می‌کند و آنچه ظرفیت مزیت رقابتــی پایدار را به وجود می‌آورد، حضور در همه جا نیست؛ بلکه کمیاب بودن است. شما فقط بر بالای کارهایی که رقبایتان نمی‌توانند انجام دهند می‌ایستید. در حال حاضر، توابع و عملکردهای اصلی ذخیره‌سازی داده‌های IT، پردازش داده‌ها و انتقال داده‌ها برای همه قابل دسترس شده‌اند.

اگرچه «کار» (Carr) تا دو سال پس از این مقاله مناظره‌های شدیدی داشت، اما مقاله‌اش همچنان در مرکز توجه بود و با ظهور وب به‌عنوان یک پلتفرم محاسباتی قدرتمند همزمان شده بود. وب مدیران فناوری اطلاعات را غافلگیر و شگفت‌زده کرد و بسیاری از آنها را تا سه سال در بی‌نظمی و سردرگمی قرار داد، مخصوصا اینکه بسیاری از آنها بیشتر بر روی مساله رسیدن سال ۲۰۰۰ متمرکز بودند. در واقع، با ورود وب، IT تنزل پیدا کرد، چون وب مزیت رقابتی قابل توجهی را برای آنهایی که زود بر آن تسلط پیدا کرده بودند، به همراه آورد.

همان‌طور که در نمودار زیر نشان داده می‌شود، پایان برتری IT با ظهور دوران اینترنت همراه شده و در ادامه با وعده‌های بلاکچین تداوم یافته است.

توصیف دوره‌های تکنولوژی

راه دیگر برای پی بردن به سیر تکاملی تکنولوژی، ترسیم مراحل مختلف تکامل وب و مشاهده این موضوع است که بلاکچین هنوز یکی از این مراحل است که بر معاملات دارایی‌های مبتنی بر اعتماد و فرد به فرد متمرکز شده است. بیایید انقلاب کوچک کلیدی‌ای را که اینترنت از سال ۱۹۹۴ برای ما به ارمغان آورده است، به خاطر بیاوریم؛ ارتباطات شخصی، خودانتشاری، تجارت الکترونیک و وب اجتماعی. در نهایت هر یک از این مراحل با سازوکارهایی که در آن اختلال ایجاد کرده‌اند، توضیح داده می‌شود؛ دفتر پست، رسانه‌های چاپی، زنجیره‌های تامین/فروشگاه‌های فیزیکی و دنیای واقعی.



موضوع جالب این است که اپلیکیشن‌های مبتنی بر بلاکچین می‌توانند جایگزین هر نوع اپلیکیشن تحت وب شوند. اگرچه ما فکر می‌کنیم که وب انتشار اطلاعات، ارتباطات و تجارت الکترونیک را برای ما به ارمغان آورده است، اما این توابع با ظهور نسخه جدیدی که مبتنی بر پروتکل‌های فرد به فرد هستند و توسط فناوری‌های بلاکچین محکم شده‌اند، مورد تهدید قرار گرفته‌اند.

مرحله	هدف	اختلال	نتیجه
ارتباطات	دسترسی به هر کسی در دنیا	دفتر پست	ارتباطات شخصی
انتشار	پخش ایده‌ها	رسانه‌های چاپی	خودانتشاری
تجارت	معاملات	زنجیره تامین و فروشگاه‌های فیزیکی	تجارت الکترونیک
تعاملات اجتماعی	ارتباط با دوستان	دنیای واقعی	وب اجتماعی
دادوستد دارایی	مدیریت چیزهایی که برای شماست	نگهبان‌های موجود	خدمات مبتنی بر اعتماد

باز کردن بلاکچین

حال بیایید لایه‌های مختلف و بسیار بلاکچین را آشکار کنیم! اگر یک نکته برای کندوکاو وجود داشته باشد، تاکید بر این موضوع است که بلاکچین یک آیتم، یک مورد، روند، یا ویژگی نیست. بلاکچین بخش‌های بسیاری است که در کنار هم قرار گرفته‌اند، برخی از آنها با یکدیگر و برخی دیگر به‌طور مستقل کار می‌کنند.

وقتی در سال ۱۹۹۵ اینترنت تجاری‌سازی شد، ما اغلب آن را یک پدیده چندمنظوره توصیف کردیم. در کتاب قبلی‌ام، «افتتاح بازارهای دیجیتال»، که در سال ۱۹۹۷ چاپ شد، من اینترنت را «دارای پنج هویت» قلمداد کردم و اضافه کردم که هر فرد باید با ایجاد استراتژی‌های مختلف از هر کدام از این هویت‌ها استفاده کند. وب نیز به‌طور همزمان یک شبکه، یک پلتفرم توسعه، یک پلتفرم معامله، یک واسطه و یک بازار بود (ما در آن زمان جنبه شبکه اجتماعی آن را ندیدیم و این ویژگی بعدها نمایان شد).

بلاکچین این عملکردهای متعدد را بیشتر بسط می‌دهد و به‌طور همزمان ۱۰ ویژگی زیر را به نمایش می‌گذارد:

- ارز رمزنگاری شده؛
- زیرساخت محاسبات؛
- پلتفرم معامله؛
- بانک اطلاعاتی غیرمتمرکز؛
- دفترکل حسابداری توزیع‌شده؛
- پلتفرم توسعه؛
- نرم‌افزار منبع‌باز؛
- بازار خدمات مالی؛
- شبکه فرد به فرد؛
- لایه خدمات اعتمادی.

در اولین گام برای اینکه درک پایه ای از بلاک‌چین به دست بیاوریم، بیایید هر یک از موارد فوق را بررسی کنیم.

۱. ارز رمزنگاری شده دیجیتالی

عملکرد پول دیجیتالی احتمالا یکی از قابل رویت‌ترین عناصر در بلاکچین است، مخصوصا اگر بلاکچین عمومی باشد، مثل بیت‌کوین (BTC) یا اتریوم (ETH). ارز رمزنگاری شده معمولا یک پروکسی اقتصادی برای داشتن یک عملیات پایدار و ایمن در بلاکچین است و گاهی اوقات در قالب یک توکن ارائه می‌شود می‌شود.

یکی از مسائل چالش‌برانگیز ارز رمزنگاری شده به نوسانات قیمت آن مربوط می‌شود که برای دور نگه داشتن اغلب مشتریان از این بازار کافی است. در یک مقاله که در سال ۲۰۱۴ منتشر شد، «رابرت سامز» به نقل از «نیک زابو»، روشی برای ثابت نگه داشتن قیمت ارز رمزنگاری شده ارائه داد: «نوسان قیمت بیت‌کوین ناشی از تنوع گمانه‌زنی‌ها در مورد آن است که به‌دلیل شک‌وتردید از آینده انجام میشود. کارآمدترین و سیال‌ترین مکانیسم‌ها نیز به کاهش این شک‌وتردید کمکی نکرده‌اند.» همان‌طور که ارز رمزنگاری شده درک و پذیرش بیشتری را به دست می‌آورد، آینده آن از ثبات بیشتری برخوردار می‌شود و در نتیجه یک منحنی تدریجا پایدار و مناسب را ایجاد می‌کند.

ارز رمزنگاری شـــده می‌تواند یک نقش تولیدی هم داشـــته باشـــد چرا که برای جبران تلاش ماینرهایی که با موفقیت تراکنش‌ها را معتبر می‌سازند، جوایزی در نظر می‌گیرد. همچنین هنگام پرداخت کارمزدهای اندک برای اجرای قراردادهای هوشمند (نظیر اتریوم) و یا به عنوان کارمزد تراکنش‌های انجام‌شده (مثل ریپل و بیت‌کوین)، ارز رمزنگاری شده می‌تواند نقش مصرفی داشته باشد. این هزینه‌ها و انگیزه‌های اقتصادی ایجاد شده‌اند تا از سوءاستفاده از بلاکچین جلوگیری شود. در حالت استفاده پیشـــرفته‌تر، می‌توان از آن به‌عنوان واحد ارزش داخلی نیز استفاده کرد، مثل سازمان‌های توزیع‌شده مستقل (DOAs) که این موضوع در فصول ۵ و ۷ کتاب مورد بررسی قرار خواهد گرفت.

خارج از محدوده کاری بلاک‌چین ارز رمزنگاری شـــده شبیه ســـایر ارزهاست. می‌توان در معاملات دادوستد شـــود و می‌توان از آن برای خرید و فروش کالاها و خدمات استفاده کرد. ارز رمزنگاری شده در داخل شبکه‌های بلاکچین بسیار مفید و کارآمد است، اما هر وقت به دنیای واقعی پول (ارز) سنتی (که ارز یا پول فیات نیز نامیده می‌شود) ورود کند در آن اصطکاک و سایش به وجود می‌آید.

۲.غیرمتمرکز کردن محاسبات زیرساخت

بلاکچین را می‌توان به‌عنوان یک روش طراحی نرم‌افزار نیز دید که تعدادی از کامپیوترها را به یکدیگر متصل می‌کند و معمولا از یک فرایند اجماع مشابه برای آزادسازی، ثبت و ضبط اطلاعاتی که دارند استفاده می‌کنند و تمام تعاملات و روابط آنها توسط رمزنگاری اعتبارسنجی می‌شود.

از منظر فیزیکی، سرورهای کامپیوتری شبکه‌شـــده همان چیزی است که به بلاکچین‌ها قدرت می‌دهد، اما توسعه‌دهندگان باید این سرورها را اجرا و تنظیم کنند و این بخشی از جادوی بلاکچین است. بر خلاف وب که در آن یک درخواســـت HTTP (پروتکل انتقال ابرمتنی) به سرور فرستاده می‌شود، در اپلیکیشن‌های بلاکچین، شبکه به بلاکچین درخواست می‌دهد.

۳. پلتفرم تراکنش و معامله

یک شبکه بلاکچین می‌تواند انواع مختلفی از تراکنش‌های مربوط به پول دیجیتال یا دارایی‌هایی را که دیجیتالی شده‌اند تایید کند. هر بار که یک توافق حاصل شود، معامله روی «بلوکی» که فضای ذخیره‌سازی دارد ثبت می‌شود. بلاکچین به پیگیری یک بلاکچین دیگر می‌پردازد و بنابراین این پلتفرم قادر به نگه داشتن تراکنش‌های کوچک و بزرگ است.

اگر ما بلاکچین را با دیگر شبکه‌های پردازش معاملاتی یکســـان فرض کنیم، چیزی که به ذهن می‌آید، توان عملیاتی پردازش آن است که از طریق معیار اندازه‌گیری «تراکنش در هر ثانیه» (TPS) محاسبه می‌شود. به‌عنوان مثال در سال ۲۰۱۵، «ویزا» به‌طور متوسط ۲۰۰۰ TPS را در «ویزانت» پردازش می‌کرد که حداکثر نرخ پردازش ۴۰۰۰ TPS و حداکثر ظرفیت ۵۶۰۰۰ TPS بود. طی سال ۲۰۱۵، پی‌پال کلا ۴/۹ میلیارد پرداخت را پردازش کرد که معادل ۱۵۵ TPS بود. در سال ۲۰۱۶، توان پردازش بلاکچین بیت‌کوین بسیار پایین‌تر از این اعداد بود و در حدود ۷-۵ TPS را پردازش می‌کرد، اما به‌دلیل پیشرفت در تکنولوژی سایدچین (sidechain) و افزایش مورد انتظار در اندازه بلوک‌های بیت‌کوین چشم‌انداز بسیار بزرگ‌تری برای بیت‌کوین انتظار می‌رود. برخی از بلاکچین‌های دیگر سریع‌تر از بیت‌کوین هستند.

به‌عنوان مثال، اتریوم با ۱۰ TPS در سال ۲۰۱۵ کار خود را آغاز کرد و تا ۱۰۰-۵۰ TPS در سال ۲۰۱۷ رسید و درصدد است تا ســـال ۲۰۱۹ به ۱۰۰۰۰۰-۵۰۰۰۰ TPS برسد. بلاکچین‌های

خصوصی سریع‌تر هستند؛ زیرا آنها نیازهای امنیتی کمتری دارند و ما TPS ۱۰۰۰۰-۱۰۰۰ در سال ۲۰۱۶ را می‌بینیم که در سال ۲۰۱۷ تا TPS ۱۵۰۰۰-۲۰۰۰ بالا می‌رود و پس از سال ۲۰۱۹ به‌طور بالقوه به یک سقف نامحدودی می‌رسد. در نهایت، خروجی بلاکچین با تکنولوژی بانک اطلاعاتی دسته بندی‌شده پیوند می‌یابد و محدودیت‌های تراکنشی را پوشش دهد و به توسعه مثبت منجر شود.

٤. بانک اطلاعاتی غیرمتمرکز

بلاکچین پارادایم پردازش بانک اطلاعاتی / معامله را مختل می‌کند. در سال ۲۰۱۴، من به‌شدت تایید کردم که بلاکچین یک پایگاه داده جدید است و به توسعه‌دهندگان هشدار دادم که برای بازنویسی همه چیز آماده شوند.

بلاکچین مانند مکانی است که در آن شما هر گونه اطلاعات را به‌طور نیمه عمومی در یک جعبه خطی (بلوک) ذخیره می‌کنید. هر کسی می‌تواند تایید کند که شما این اطلاعات را قرار داده‌اید، زیرا جعبه امضای شما را روی خود دارد، اما فقط شما (یا یک برنامه) می‌توانید آنچه را درون جعبه قرار می‌دهید، ببینید، زیرا فقط شما کلیدهای خصوصی آن داده‌ها را در اختیار دارید که بسیار ایمن است.

بنابراین بلاکچین تقریبا همانند یک پایگاه داده رفتار می‌کند، به‌جز اینکه بخشی از اطلاعاتی که ذخیره می‌شود و «سرتیتر» (header) آن عمومی است. مسلما، بلاکچین‌ها بانک‌های اطلاعاتی خیلی کارآمدی نیستند، اما اشکالی ندارد. آنها نمی‌خواهند جایگزین بانک‌های اطلاعاتی بزرگ شوند، بلکه این کار توسعه‌دهندگان نرم‌افزاری است که بفهمند چطور باید برنامه‌های خود را بازنویسی کنند تا بتوانند از قابلیت‌های تراکنشی و معاملاتی بلاکچین استفاده کنند.

٥. دفترکل حسابداری توزیع‌شده و به اشتراک گذاشته‌شده

بلاکچین همچنین یک دفترکل یا سرفصل دارایی توزیع‌شده، عمومی و دارای برچسب زمانی است که تمام معاملات و تراکنش‌های انجام‌شده یا پردازش‌شده در شبکه را در خود نگه می‌دارد و به کاربر کامپیوتر اجازه می‌دهد تا هر تراکنش را طوری اعتبارسنجی کند که دیگر هیچ محاسبه مضاعفی انجام

نشود. این دفترکل را می‌توان از طریق طرف‌های متعدد به اشتراک گذاشت و می‌تواند خصوصی، عمومی یا نیمه‌خصوصی باشد.

اگرچه یک دفترکل توزیع‌شده از معاملات و تراکنش‌ها توصیف رایجی از بلاکچین است و برخی آن را مانند بهترین برنامه می‌دانند، اما این فقط یکی از ویژگی‌های بلاکچین است.

٦. پلتفرم توسعه نرم‌افزار

برای توسعه‌دهندگان، بلاکچین اولین و بهترین مجموعه تکنولوژی‌های نرم‌افزاری است. بله، آنها زمینه‌های سیاسی و اجتماعی‌ای دارند که در حال پی‌ریزی است (تمرکززدایی)، اما آنها با خودشان نوآوری تکنولوژیکی را نیز به ارمغان می‌آورند. این مجموعه جدید از ابزارهای توسعه یک رویداد هیجان‌انگیز برای مهندسان نرم‌افزاری است. بلاکچین شامل تکنولوژی‌هایی برای ایجاد نسل جدیدی از اپلیکیشن‌هاست که غیرمتمرکز هستند و از طریق رمزنگاری امن شده‌اند. بنابراین، بلاکچین روش جدیدی برای ساخت این اپلیکیشن‌هاست.

بلاکچین‌ها می‌توانند طیف متنوعی از رابط‌های برنامه‌نویسی کاربردی (API) را داشته باشند که شامل زبان برنامه‌نویسی تراکنش، رابط برنامه‌نویسی گره‌های ارتباطی فرد به فرد و یک رابط برنامه نویسی مشتری برای بررسی معاملات و تراکنش‌ها در شبکه است. من جنبه توسعه نرم‌افزاری را بیشتر در فصل ۶ کتاب توضیح می‌دهم.

۷. نرم‌افزارهای منبع‌باز

اکثر بلاکچین‌های قدرتمند منبع‌باز هستند که نه‌تنها به معنای این است که منبع نرم‌افزار عمومی است، بلکه به این معنا نیز هست که نوآوری می‌تواند به‌صورتی مشارکتی، بر بالای هسته نرم‌افزاری انجام شود.

به‌عنوان مثال، هسته پروتکل بیت‌کوین منبع‌باز است. از زمان توسعه اولیه آن توسط خالق آن ساتوشی ناکاموتو، این پروتکل توسط گروهی از توسعه‌دهندگان هسته‌ای نگهداری شده است که این گروه از توسعه‌دهندگان این پروتکل را در طول زمان تقویت کرده و بهبود می‌بخشند. علاوه بر این، هزاران توسعه‌دهنده مستقل با محصولات، خدمات و اپلیکیشن‌های مکمل از ثبات و قدرت

پروتکل بیت‌کوین بهره می‌برند و به نوآوری می‌پردازند.

این واقعیت که نرم‌افزار بلاکچین منبع‌باز است، یک ویژگی قدرتمند به حساب می‌آید. هرچه هسته بلاکچین بازتر باشد، اکوسیستم اطراف آن قوی‌تر خواهد بود.

۸. بازار خدمات مالی

پول در قلب و مرکز بلاکچین‌های مبتنی بر رمزنگاری قرار دارد. وقتی ارز رمزنگاری‌شده همانند هر ارز دیگری در نظر گرفته شود، می‌تواند به یکی از ابزارهای مالی تبدیل شود که به توسعه انواع مختلفی از محصولات مالی جدید و متنوع منجر خواهد شد.

بلاکچین‌ها یک محیط نوآوری منحصربه‌فرد و خارق‌العاده را برای نسل بعدی خدمات مالی ارائه می‌دهند. همان‌طور که نوسانات قیمتی ارز رمزنگاری‌شده فروکش کند، این موضوع محبوب خواهد شد. مشتقات، گزینه‌ها، مبادلات، ابزارهای ترکیبی، سرمایه‌گذاری، وام و بسیاری دیگر از ابزارهای سنتی، نسخه ارز رمزنگاری‌شده خودشان را خواهند داشت و بنابراین یک بازار تجاری جدید برای خدمات مالی ایجاد می‌شود.

۹. شبکه فرد به فرد

بلاکچین هیچ چیز مرکزی ندارد. از نظر ساختاری و معماری، لایه اصلی بلاکچین یک شبکه فرد به فرد است. یک بلاکچین از طریق پردازش‌های همسان در محل گره‌هایش تمرکززدایی می‌کند. شما هر تراکنشی را در سطح فرد به فرد تایید می‌کنید. و هر یک از معاملات دیگر را در سطح فرد به فرد اعتبارسنجی می‌کند. در واقع، یک بلاکچین را می‌توان یک ابر محاسباتی نازک در نظر گرفت که واقعا تمرکززدایی شده است.

هر کاربر می‌تواند بلافاصله با کاربر دیگری معامله کند، آن هم بدون در نظر گرفتن ساعت‌های کاری و بدون توجه به جایی که در جهان هستند. هیچ واسطه‌ای برای فیلتر کردن، مسدود کردن یا تاخیر انجام معاملات بین دو یا چند کاربر یا بین گره‌هایی که از یک معامله استفاده می‌کنند مورد نیاز نیست. هر گره در شبکه مجاز می‌تواند خدمات را بر اساس دانش خود از معاملات در هر جای دیگری در آن شبکه ارائه دهد.

علاوه بر ایجاد یک شبکه فنی P2P، بلاکچین‌ها نیز بازاری از کاربران را ایجاد می‌کنند. شبکه‌ها و اپلیکیشن‌های بلاکچین اقتصاد (توزیع‌شده) خودشان را با اندازه‌ها و ظرافت‌های مختلف ایجاد می‌کنند. بنابراین، بلاکچین‌ها با خودشان مدل‌های اقتصادی را به ارمغان می‌آورند که یک ویژگی کلیدی است که بعدا در این کتاب بسط داده می‌شود.

۱۰. لایه خدمات اعتمادی

همه بلاکچین‌ها به‌عنوان یک واحد اتمی و تجزیه‌ناپذیر از خدمات، اعتماد جلب می‌کنند. در اصل، این یک تابع و یک سرویس است که تحویل داده شـــده است. اما اعتماد تنها به معاملات و تراکنش‌ها محدود نمی‌شـــود. اعتماد به داده‌ها، خدمات، فرایندها، هویت، منطق کسب‌وکاری، شرایط یک قرارداد یا اشیای فیزیکی بسط داده شده است و تقریبا به هر چیزی که بتواند به‌عنوان یک دارایی (هوشمند) با ارزش ذاتی یا وابسته مربوط به آن دیجیتالی شود، قابل اعمال است.

حال مخلوطی احتمالی از نوآوری‌های ممکن را تصور کنید که این ۱۰ ویژگی قدرتمند را تقویت می‌کنند. با ترکیب آنها، شما می‌توانید قدرت باورنکردنی بلاکچین‌ها را درک کنید.

ماشین‌های حالت (state machines) یا جداول حالت (STATE TRANSITIONS) کدام یک؟

بلاکچین را نمی‌توان برای هر چیزی استفاده کرد و هر چیزی با پارادایم بلاکچین مطابقت ندارد. بلاکچین یک ماشین حالتی است که این مفهوم دیگری است که باید درک شود.

از لحاظ فنی، یک حالت (state) یا وضعیت به معنای «اطلاعات ذخیره‌شده» در یک مقطع زمانی خاص است. یک ماشین حالت کامپیوتر یا دستگاهی است که حالت و وضعیت چیزی را که در آن لحظه از زمان ارائه شده است به خاطر می‌سپارد. بر اساس برخی ورودی‌ها ممکن است تغییر کند و برای این تغییرات اجرا شده یک خروجی ارائه می‌دهد. پیگیری تراکنش‌ها و معاملات این حالت‌ها و وضعیت‌ها بسیار مهم است و به همین دلیل است که بلاکچین خوب کار می‌کند و تغییرناپذیر است. درعوض، رکوردها و سوابق پایگاه داده قابل تغییر است، زیرا ممکن است چندین بار بازنویسی شود. همه پایگاه‌های داده دارای پیگیری‌های حسابرسی نیستند و اگر هم دارای پیگیری‌های حسابرسی باشند، ممکن است به‌دلیل نداشتن مدرکی برای دستکاری نشدن آن یا نابود شده یا از دست برود. در بلاکچین اتریوم یک درخت حالت (state tree) مجزا ذخیره شده که نشان‌دهنده توازن پولی هر

آدرس است و یک «لیست تراکنشها» نشان‌دهنده تراکنش‌هایی است که بین بلوک فعلی و بلوک قبلی در هر بلوک انجام شده است.

ماشین‌های حالتی برای اجرا و پیاده‌سازی سیستم‌های توزیع‌شده‌ای که در برابر خطا مقاوم هستند، مناسب‌اند.

الگوریتم‌های توافق

در مرکز درک شـــدت انتقال و تغییر پارادایم بلاکچین این درک اساسی از مفهوم «توافق و اجماع غیر متمرکز» وجود دارد که یک اصل کلیدی برای انقلاب محاسباتی مبتنی بر رمزنگاری شده است.

توافق و اجماع غیر متمرکز، پارادایم‌های توافق‌های متمرکز قدیمی را می‌شکند؛ منظور زمانی است که یک پایگاه داده مرکزی برای اداره اعتبار معاملات و تراکنش‌ها مورد اســـتفاده قرار می‌گیرد. یک طرح غیر متمرکز (پروتکل‌های بلاکچین بر اساس آن هستند)، قدرت و اختیار را انتقال می‌دهد و به یک شبکه مجازی غیر متمرکز اعتماد می‌کند و گره‌های آن را قادر می‌سازد تا به‌طور پیوسته و به‌طور دنباله‌ای معاملات و تراکنش‌ها را در بلوک‌های عمومی ثبت کند و یک زنجیره خاص و منحصر به‌فرد به وجود آورد که بلاکچین نام دارد. هر بلوک متوالی شامل یک «هش» (یک اثر انگشت منحصر به‌فرد) از کدهای قبلی است و بنابراین برای ایمن کردن سندیت منابع معاملات و تراکنش‌ها و حذف نیاز به یک واسطه مرکزی از رمزنگاری (از طریق کدهای هش) استفاده شده است. ترکیب تکنولوژی رمزنگاری و بلاکچین تضمین می‌کند که هرگز یک تراکنش یا معادله دوبار ثبت نشود. در اینجا چیزی که از همه چیز مهم‌تر است اینکه با این درجه از جداسازی، منطق توافقی از خود برنامه جدا می‌شود و بنابراین برنامه‌ها را می‌توان بازنویسی کرد تا در اصل غیر متمرکز شوند و این جرقه‌ای برای نوآوری‌های تغییردهنده سیستم‌های مختلف در ساختار نرم‌افزاری برنامه است؛ حال چه این نوآوری‌ها به پول مربوط باشند یا به پول ارتباطی نداشته باشند.

شما می‌توانید اجماع و توافق را اولین لایه معماری تمرکززدایی تصور کنید. این پایه و مبنایی برای پروتکل‌های اساسی به حساب می‌آید که عملیات بلاکچین را اداره می‌کنند.

یک الگوریتم توافقی، هسته‌ای از یک بلاکچین است که نشان‌دهنده روش یا پروتکل انجام‌دهنده معامله یا تراکنش است. این الگوریتم به این دلیل مهم است که ما باید به این معاملات و تراکنش‌ها

اعتماد کنیم. به‌عنوان یک کاربر تجاری، شما نیازی به درک روش دقیق کار این الگوریتم ندارید، فقط کافی است به امینت و قابلیت اطمینان آن باور داشته باشید.

بیت‌کوین آغازگر روش توافقی اثبات کار (POW) است و می‌توان آن را پدربزرگ این الگوریتم‌ها دانست. اثبات کار بر الگوریتم تحمل خطای عملی بیزانس متکی است که به تراکنش‌ها و معاملات اجازه می‌دهد به‌طور ایمن و طبق وضعیت داده‌شده عمل کنند. یک جایگزین اثبات کار برای دستیابی به اجماع و توافق، اثبات سهام است. پروتکل‌های توافقی دیگری نظیر DPOS، RAFT و Paxos نیز وجود دارند که ما به سراغ مقایسه آنها با یکدیگر نمی‌رویم، زیرا آنها در طول زمان به‌عنوان خط سیر استاندارد مشاهده می‌شوند. چیزی که از همه مهم‌تر است، قدرت ابزارها و تکنولوژی‌های میان‌ابزاری است که در بالای الگوریتم‌ها ایجاد می‌شوند و همچنین اکوسیستم بازیگران ارزشی اضافه‌شده که آنها را احاطه کرده‌اند.

یکی از ضعف‌های الگوریتم اثبات کار این است که از نظر محیطی دوستانه نیست، زیرا به مقدار زیادی قدرت و توان پردازشی به دست آمده از ماشین‌آلات تخصصی نیاز دارد تا بتواند انرژی فراوان و بیش از اندازه‌ای را تولید کند. یک رقیب قوی برای اثبات کار الگوریتم اثبات سهام (POS) است که بر مفهوم کندوکاو مجازی و رای‌گیری مبتنی بر نشانه متکی است که همانند اثبات کار به پردازش کامپیوتری شدید و زیاد نیازی ندارد و دسترسی به امنیت به صورتی مقرون‌به‌صرفه را وعده می‌دهد.

در نهایت برای بررسی الگوریتم توافقی، باید روش «اجازه دادن» که کنترل را در دست دارد و در فرایند و پردازش توافقی شرکت می‌کند را در نظر بگیرید. سه نوع انتخاب برای اجازه دادن عبارتند از:

- عمومی (مثل اثبات کار و اثبات سهام)؛
- خصوصی (استفاده از کلیدهای مخفی برای ایجاد مجوز در یک بلاکچین محصور)؛
- نیمه‌خصوصی (مثل، استفاده‌های مبتنی بر کنسرسیوم، از روش سنتی تحمل خطای بیزانس به صورتی متعهد).

نکات مهم فصل نخست

۱- بلاکچین مثل شبکه جهانی وب، یک لایه از تکنولوژی بر بالای اینترنت است.

۲- یک بلاکچین توصیفات فنی، کسب و کاری و قانونی دارد.

۳- اثبات‌های رمزنگاری یک روش مورد اعتماد است که بلاکچین برای تصدیق اعتبار و نهایی بودن تعاملات و تراکنش‌های بین طرفین از آن استفاده می‌کند.

۴- بلاکچین هنگام ایجاد واسطه‌های جدید، نقش واسطه‌های موجود را دوباره تعریف می‌کند (البته اگر آنها قبول کنند تغییر کنند) و در نتیجه مرزهای ارزشی سنتی را مختل می‌کند.

۵- بلاکچین ۱۰ ویژگی دارد و همه آنها باید به‌صورت کلی درک شوند.

پی‌نوشت

بیت‌کوین یک سیستم پول الکترونیکی فرد به فرد است، https//bitcoin.org/en/bitcoin-paper.

بیشینه‌گرایی بیت‌کوین، به این نکته اشاره دارد که فقط در ازای سایر پروژه‌های مربوط به ارز رمزنگاری شده یا بلاکچین از بیت‌کوین حمایت می‌کند، زیرا بیشینه‌گراها باور دارند که برای رسیدن به مزایای کارآمد شبکه‌ای مورد نظر فقط یک بلاکچین و فقط یک ارز مورد نیاز است.

پتانسیل‌های استفاده‌نشده از روایت‌های مشترک

http://edgeperspectives.typepad.com/edge_perspectives/2013/ 1 0/ the-untapped-potential-of-corporate-narrativeshtml

میرسون، راجر. ب (۱۹۹۱) نظریه بازی: تجزیه‌وتحلیل جنگ، انتشارات دانشگاه هاروارد

لسلی لامپورت، رابرت شستاک، و مارشال پیز، مساله ژنرال بیزانس،

https://research.microsoft.com/en-us/um/people lamport/pubs/byz.pdf

IT اهمیتی ندارد، https://hbr.org/2003/05/it-doesnt-matter

وب‌سایت پی‌پال، https://www.paypal.com/webapps/ mpp/about

ارتباط شخصی با ویتالیک بوترین، فوریه ۲۰۱۶

تحمل خطای بیزانس، https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

اثبات سهام، https://en.wikipedia.org/wiki/wiki/Proof-of-stake