استفاده از نسل بعدی فناوری اینترنت، از حرف تا عمل

کسب و کار بلاکچین

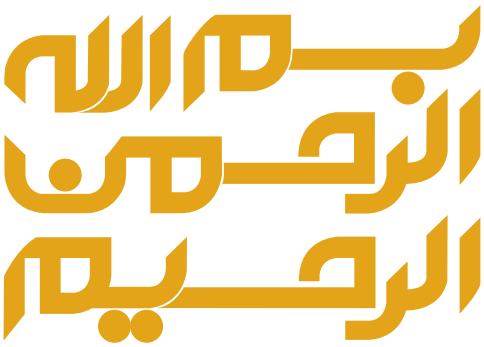
ویلیام موگایار

پیمان رحمانی

چاپ دوم

WILEY

انتشارات راه پرداخت


بسم الله
الرحمن
الرحيم

سرشناسه : موگایار، ویلیام،Mougayar, William
عنوان و نام پدیدآور : کسب‌وکار بلاکچین/ویلیام موگایار ؛ [مترجم] پیمان رحمانی ؛ ویراستار ارشد مینا والی ؛ ویراستار محتوایی قاسم سرافرازی ؛ ویراستار فنی یلدا شایسته‌فر.
مشخصات نشر : تهران: راه پرداخت، ۱۴۰۱.
مشخصات ظاهری : ۲۰۴ ص.
شابک : ۸-۴۰-۷۷۰۲-۶۲۲-۹۷۸:
وضعیت فهرست نویسی : فیپا
یادداشت : کتاب حاضر نخستین بار با عنوان «زنجیره بلوکی کسب و کار: وعده،عملکرد و کاربرد نسل جدید اینترنت» با ترجمه‌ی مرتضی موسی‌خانی، محمود البرزی، حامد حیدری توسط انتشارات دیباگران تهران در سال ۱۳۹۷ به چاپ رسیده است.
یادداشت : عنوان اصلی: The business blockchain: promise, practice, and application of the next Internet technology, c2016.
یادداشت : بالای عنوان: استفاده از نسل بعدی فناوری اینترنت، از حرف تا عمل.
عنوان دیگر : نجیره بلوکی کسب و کار: وعده،عملکرد و کاربرد نسل جدید اینترنت.
موضوع : اینترنت - نوآوری، Internet - Technological innovations
انتقال الکترونیکی وجوه، Electronic funds transfers
شناسه افزوده : رحمانی، پیمان، ۱۳۶۳ -، مترجم
شناسه افزوده : والی، مینا، ۱۳۶۳ -
شناسه افزوده : شایسته‌فر، یلدا، ۱۳۶۱-
رده بندی کنگره : HB۱۷۱۰
رده بندی دیویی : ۳۳۲/۱۷۸
شماره کتابشناسی ملی : ۸۹۹۳۸۶۳
اطلاعات رکورد کتابشناسی : فیپا

استفاده از نسل بعدی فناوری اینترنت، از حرف تا عمل

کسب و کار بلاکچین

ویلیام موگایار

پیمان رحمانی

راه کار

چاپ دوم

WILEY

عنوان: کسب و کار بلاکچین
ناشر: راه پرداخت
نویسنده: ویلیام موگایار
مترجمان: پیمان رحمانی
ویراستار ارشد: مینا والی
ویراستار محتوایی: قاسم سرافرازی
ویراستار فنی: یلدا شایسته‌فر
بازبینی نهایی متن: رضا قربانی
صفحه‌آرا: ایمان شاه‌سمندی
ناظر چاپ: قادر شهبازی
نوبت چاپ: دوم ۱۴۰۴
شمارگان: ۱۰۰ نسخه
شابک: ۸-۴۰-۷۷۰۲-۶۲۲-۹۷۸
تلفن: ۰۲۱-۴۴۴۳۹۶۶۶
دورنگار: ۸۹۷۸۴۹۰۲
ایمیل: publisher@way2pay.press
وب‌سایت: way2pay.press
لیتوگرافی: هنر اشکان
چاپ و صحافی: واژه

فروشگاه انتشارات راه‌پرداخت نشانی: تهران، جنت‌آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

way2pay.press w2ppress.ir way2paypress

فهرست

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 دربر 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 برمی‌گردد. 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 غیرمتمرکزسازی 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 غیرمتمرکز 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 غیرمتمرکز 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 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	پایگاه داده back-end (عقبه) که یک دفترکل توزیع شده را آزادانه حفظ و نگهداری می کند.
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 می کند 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 می کرد. 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.

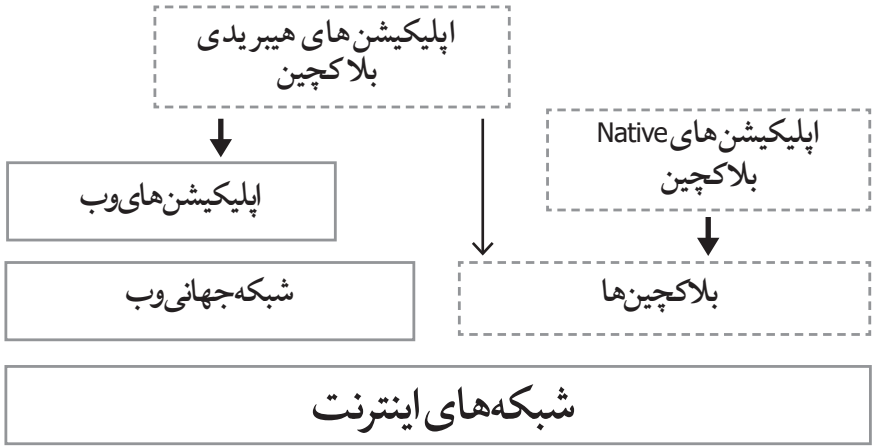
معرفی کاربردهای بلاکچین

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

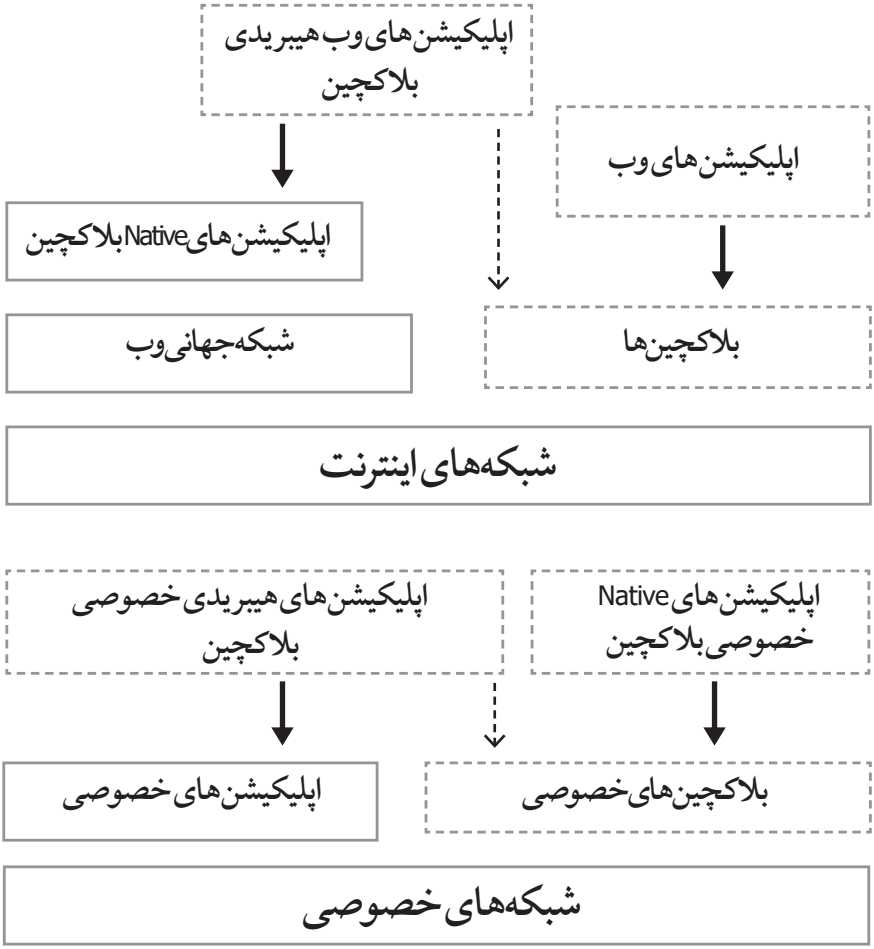
بیش از یک راه برای ساخت اپلیکیشن مبتنی بر بلاکچین وجود دارد، شما می‌توانید اپلیکیشن‌ها را به طور ساده روی یک بلاکچین بسازید، یا اینکه آنها را در اپلیکیشن‌های وب موجود ترکیب کنید که ما آن را یک چاشنی می‌نامیم: «اپلیکیشن‌های بلاکچین ترکیبی» (hybrid blockchain applications)

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).

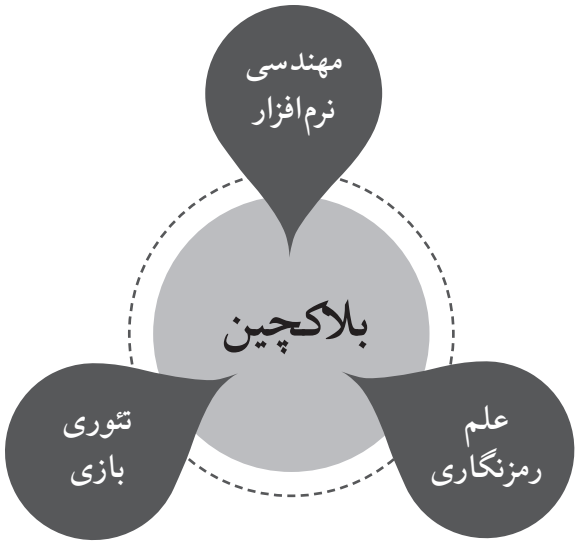
بلاکچین فقط یک تکنولوژی جدید نیست؛ بلکه نوعی تکنولوژی است که سایر تکنولوژی‌های نرم‌افزاری موجود را به چالش می‌کشد، زیرا بلاکچین این پتانسیل و قابلیت را دارد که جایگزین روش‌های موجود شده یا آنها را کامل کند. در اصل، بلاکچین یک تکنولوژی است که سایر تکنولوژی‌ها را تغییر می‌دهد.

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 بلاکچینی ایجاد کنند که عدم قطعیت ظاهری را با اطمینان ریاضی کاهش دهد.

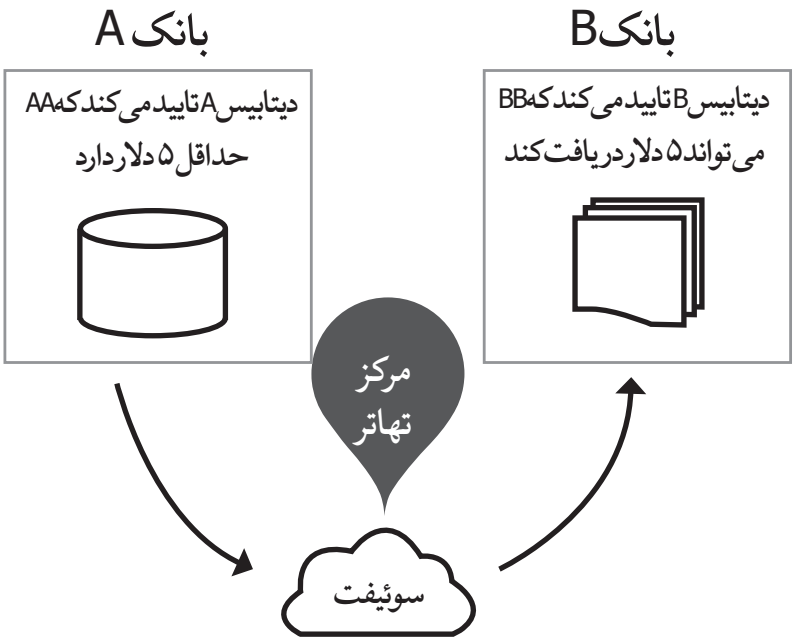
پایگاه داده در برابر دفترکل

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).



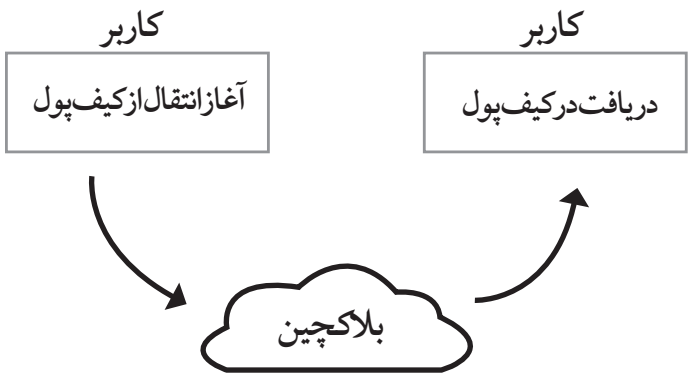
وقتی یک حساب بانکی باز می کنید، شما واقعا اختیار حساب خود را به بانک واگذار کرده‌اید. در واقع، آنها توهم دسترسی و فعالیت شفاف با آن حساب را به شما نشان داده‌اند. هر زمان که بخواهید پول را جابه‌جا کنید، به کسی پرداخت داشته باشید، یا سپرده‌ای داشته باشید، بانک به شما دسترسی صریح می دهد، زیرا شما به آنها 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:

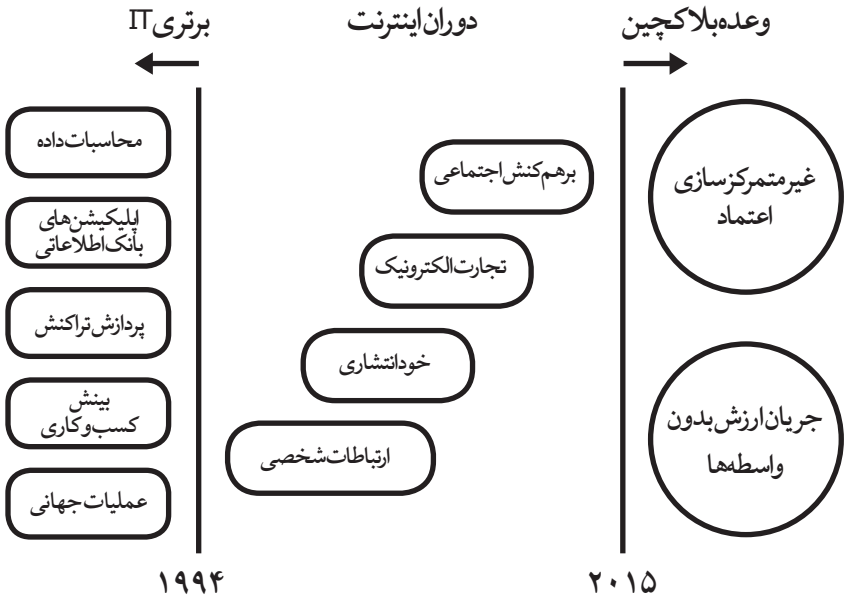
«آنچه منابع واقعا استراتژیک را ایجاد می‌کند و آنچه ظرفیت مزیت رقابتی پایدار را به وجود می‌آورد، حضور در همه جا نیست؛ بلکه کمیاب بودن است. شما فقط بر بالای کارهایی که رقبایتان نمی‌توانند انجام دهند می‌ایستید. در حال حاضر، توابع و عملکردهای اصلی ذخیره‌سازی داده‌های IT، پردازش داده‌ها و انتقال داده‌ها برای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

۲.غیرمتمرکز کردن محاسبات زیرساخت

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

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 اندازه گیری «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 سال ۲۰۱۹ به TPS ۱۰۰۰۰۰-۵۰۰۰۰ 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.

۶. 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 رمزنگاری شده 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 رمزنگاری شده فروکش کند، این موضوع محبوب خواهد شد. مشتقات، گزینه‌ها، مبادلات، ابزارهای ترکیبی، سرمایه‌گذاری، وام و بسیاری دیگر از ابزارهای سنتی، نسخه ارز رمزنگاری شده 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 بعداً 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 اجراشده 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. در عوض، 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 غیرمتمرکز» وجود دارد که یک اصل کلیدی برای انقلاب محاسباتی مبتنی بر رمزنگاری شده است.

توافق و اجماع غیرمتمرکز، 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 غیرمتمرکز (پروتکل‌های بلاکچین بر اساس آن هستند)، قدرت و اختیار را انتقال می‌دهد و به یک شبکه مجازی غیرمتمرکز 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 منحصربه‌فرد به وجود آورد که بلاکچین نام دارد. هر بلوک متوالی شامل یک «هش» (یک اثر انگشت منحصربه‌فرد) 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 غیرمتمرکز 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 پدر بزرگ 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 به‌صورتی 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

فصل دوم

بلاکچین چگونه به نفوذها اعتماد می کند؟

«نمی‌توانم ترس مردم از ایده‌های جدید را درک کنم. من از ایده‌های کهنه و قدیمی می‌ترسم.»
جان گیج[1]

رسیدن به اجماع، عنصر حیاتی عملیات بلاکچین به شمار می‌رود. با این وجود، بلاکچین، این کار را به شیوه‌ای غیر متمرکز که مدل قدیمی اجماع[2] متمرکز (روشی که بانک‌های اطلاعاتی متعارف برای تایید اعتبار تراکنش‌ها به کار می‌برند) را کنار می‌زند. طرح غیر متمرکزی که بلاکچین به آن متکی است، به شبکه‌ای غیر متمرکز اعتماد می‌کند و این امکان را فراهم می‌سازد تا داده‌های موجود در این شبکه بتوانند به‌صورت پیوسته و پشت سر هم، تراکنش‌هایشان را در یک بلوک عمومی ثبت کنند. این اتفاق، زنجیره منحصر به‌فردی به نام بلاکچین را شکل خواهد داد.

اگر چه باید شـــاهد تاثیر و نفوذ بلاکچین روی تقریبا همه چیزها باشیم، اما چالش ما در اینجا به

چگونگی، زمان و میزان این تاثیر بر می‌گردد. فصل اول، برخی از قابلیت‌های فناوری بلاکچین را معرفی کرد. این فصل، سنگ بنایی را برای درک کاربرد بلاکچین تشکیل می‌دهد و ما را به این باور می‌رساند که می‌توانیم بدون حضور واسطه‌هایی غیر از بلاکچین، تراکنش‌های فرد به فرد[۳] را به سرانجام برسانیم.

بلاکچین، ایده‌ای تک‌منظوره نیست، بلکه می‌توان در شکل‌های مختلفی از آن استفاده کرد.

اگر بلاکچین را به‌عنوان یک فناوری در نظر بگیریم، آنگاه امکان پیاده‌سازی آن به‌صورت فناوری وجود خواهد داشت. اگر بلاکچین را به‌عنوان یک ابزار برای تغییر کسب‌وکار در نظر بگیریم، آنگاه می‌توان آن را در فرایندهای کسب‌وکار مورد استفاده قرار داد. اگر بخواهیم آن را به‌عنوان ابزاری با پیامدهای حقوقی جدید در نظر بگیریم، آنگاه مشخصات مدیریتی جدیدش شما را حیرت‌زده خواهد کرد و اگر آن را به‌عنوان یک صفحه کاغذ سفید جهت طراحی امکانات جدیدی که پیش از این وجود نداشتند یا به چالش کشیدن امکانات قدیمی موجود در نظر بگیریم، آنگاه متوجه خلاقیت بالای این ایده در ارائه فرصت‌های جدید خواهید شد.

بر اساس آنچه در زمان تکوین و پیدایش مفهوم فوق‌الذکر مطرح شد، بلاکچین (و به‌طور قطع بیت‌کوین)، فناوری‌ای به‌شمار می‌رود که آمده است تا بدون هیچ همدردی، وضع موجود را به چالش بکشد. در هیچ جایی از مقاله ناکاموتو، به یکپارچگی آن با جهان موجود اشاره‌ای نشد، اگرچه کسانی که بعد از ناکاموتو، بیت‌کوین را مورد استفاده قرار دادند، به طرق مختلف از این یکپارچگی صحبت کردند.

در سطح کلان، آینده فناوری بلاکچین، آن‌گونه که به نظر می‌رسد، هم از نظر استقرار در بازار و هم از نظر پذیرش توسط کاربران، تفاوت زیادی با وب ندارد.

یک لایه اعتماد جدید

بلاکچین، باورهای قبلی ما در مورد اعتماد[۴] را زیر و رو و تعریف دیگری از آن ارائه می‌کند.

اگر معانی ضمنی معنوی، فلسفی و عاطفی مربوط به اعتماد را کنار بگذاریم، می‌توان از منظر معاملات تجاری، معانی زیر را برای آن در نظر گرفت: توکل[۵]، پیش‌بینی‌پذیری[۶]، اطمینان[۷]، حقیقت[۸]، ضمانت[۹]، باور[۱۰]، قطعیت[۱۱]، یقین[۱۲]، مسئولیت‌پذیری[۱۳] و وابستگی[۱۴].

اجازه بدهید تا به‌عنوان شهروند یا افراد درگیر کسب‌وکار، تعدادی از نهادهای معتمد که معمولا هر روز با آنها تعامل داریم را نام ببریم؛ بانک‌ها، دولت‌ها، شرکت‌های ارائه‌دهنده کارت اعتباری و شرکت‌های ارائه‌دهنده خدمات عمومی (مثل برق و گاز).

ما معمولا به این دلیل به سازمان‌های فوق‌الذکر اعتماد داریم که اکثر آنها، در بیشتر مواقع خدمات خوبی ارائه می‌کنند و به اعتماد ما پاسخ می‌دهند. بانک‌ها پولهایمان را نمی‌دزدند و هر زمانی که بخواهیم می‌توانیم آن را پس بگیریم، دولت‌ها در ازای مالیاتی که جمع‌آوری می‌کنند، خدمات ارائه می‌دهند، و شرکت‌های کارت اعتباری به ما پول قرض می‌دهند تا بتوانیم به راحتی از این تسهیلات در همه جا استفاده کنیم. شرکت‌های ارائه‌دهنده خدمات عمومی، تا زمانی که قبض‌هایمان را پرداخت می‌کنیم، برق، آب یا سرویس‌های ارتباط راه دور را در اختیار ما می‌گذارند.

شاید فکر کنید که هیچ ایرادی در این فرایند دیده نمی‌شود. با این وجود، می‌توان مواردی را نیز در نظر گرفت که هر یک از این سازمان‌ها می‌توانند از اعتماد ما سوءاستفاده کنند، آن را نادیده بگیرند یا گاهی اوقات هزینه‌های بسیار بالایی را بر دوش ما بیندازند.

بانک‌ها، حتی می‌توانند بعد از خرید چیزی بلافاصله حساب‌هایمان را بدهکار کنند یا در زمان تسویه چک‌هایمان، کارها را با تاخیر انجام دهند. دولت‌ها به‌سادگی پول مالیات‌مان را به باد می‌دهند و ما یا متوجه این موضوع نمی‌شویم یا اینکه نمی‌توانیم آن را ثابت کنیم. شرکت‌های کارت اعتباری، حتی در زمانی که نرخ بهره پایه تنها برابر با یک درصد است، بهره ۲۳ درصد را به ما تحمیل می‌کنند. شرکت‌های ارائه‌دهنده خدمات عمومی، بدون جبران خسارت، ارائه سرویس‌ها را قطع می‌کنند یا بدون اعلام قبلی، نرخ‌ها و شرایط ارائه خدمات‌شان را تغییر می‌دهند.

در اینجا، یک رابطه علت و معلولی وجود دارد. این نهادها به‌واسطه این تاثیرات ناگوار، با واکنش شدیدی مواجه نمی‌شوند، زیرا در ۹۵ درصد موارد به آنها اعتماد داریم و می‌توانیم در پنج درصد باقی‌مانده هم شکیبایی نشان دهیم. بر این اساس، بلاکچین چگونه می‌تواند با این مشکل برخورد کند؟

بلاکچین، برای نجات ما از پنج درصد مواردی که در بالا اتفاق افتاده‌اند کار زیادی انجام نخواهد داد. اما بر این باور هستیم که در ۹۵ درصد موارد دیگر که اعتماد به تراکنش‌ها وجود دارد، شفافیت را افزایش خواهد داد، به گونه‌ای که بتوان تاثیرات ناگوار عدم موفقیت در ایجاد اعتماد را از بین برد

یا حداقل پایین آورد. سازمان‌ها در صورت افزایش شـــفافیت در مورد لایه‌های اعتمادشان، با عدم موفقیت کمتری مواجه می‌شوند.

سازمان‌ها با ارائه شفافیت بیشتر، شکست‌های کمتری را تجربه خواهند کرد. نه فقط به این دلیل که آنها بیشتر محافظت می‌شوند بلکه به این دلیل که آنها می‌توانند شکست‌های بالقوه خود را غیر متمرکز کنند و به ما اجازه دهند بخشی از سیستم هشداردهنده اولیه باشیم. در نتیجه این باعث کاهش ریسک کلی آنها خواهد شد.

بلاکچین، میزان شفافیت و دسترسی به حقیقت را بالا می‌برد که مانع سلب اعتماد خواهد شد. اگر این فناوری جدید بتواند باز تعریفی از تابع اعتماد[۱۵] مورد استفاده واسطه‌ها ارائه کند و نتیجه مشابه و در عین حال، منافع بیشتری را به ارمغان بیاورد، آنگاه چه خواهد شد؟ لایه پایه و اساسی بلاکچین را حقیقت و شفافیت[۱۶] تشکیل می‌دهند و این در حالی است که شاهد هیچ یک از اینها از جانب نهادها و سازمان‌های معتمد نیستیم. این تفاوت، چالش جالبی را شکل می‌دهد.

منظور از غیرمتمرکزسازی اعتماد چیست؟

در صورت اســـتفاده از بلاکچین، با شـــیوه اعتماد جدیدی مواجه می‌شـــویم. پروتکل اجماع غیر متمرکز مبتنی بر بلاکچین[۱۷] که برای تحویل خدمات در بلاکچین مورد استفاده قرار می‌گیرد، اعتماد به انسان‌ها و سازمان‌های مرکزی را به اعتماد به رایانه‌ها و سازمان‌های غیر متمرکز تغییر خواهد داد. مدل قبلی، توجه ما را به سمت مراجع معتمد[۱۸] جلب می‌کند و به آنها اجازه می‌دهد تا تراکنش‌ها، داده‌ها، وضعیت حقوقی، دارایی‌ها و ثروت ما را کنترل کنند.

در مدل جدید، برخی بخش‌های مرتبط به فرایندهای اعتماد مرکزی، به بلاکچین محول می‌شوند که کارشان انجام این تابع اعتماد است. اگر بررسی اعتماد[۱۹] سنتی و قدیمی به کاری هزینه‌بر تبدیل شده است (عنصر پر از اصطکاک[۲۰] یک فرایند یا سرویس مشخص)، بلاکچین می‌تواند راهکاری برای این مشکل باشد.

سوال اساســـی و محوری در اینجا این اســـت: آیا بلاکچین می‌تواند Trust 2.0 را در اختیار ما قرار بدهد؟ Trust 2.0، شکل بهتری از اعتماد است که همواره به واسطه‌های مرکزی‌ای که ممکن است به دلیل بزرگ بودن‌شان امکان شکست بالایی داشته باشند، یا به‌دلیل سیستم بوروکراسی مورد

استفاده‌شان ریسک بالایی را تولید کنند، یا به‌دلیل کند بودن بیش از حدشان امکان تغییر نداشته باشند، وابسته نیست.

هفت اصلی که پیش از باور داشتن به آینده اعتماد غیر متمرکز[۲۱] باید به آنها اعتقاد داشته باشیم عبارتند از:

۱. اینکه بلاکچین را ابزارهایی برای حذف واسطه‌های قابل اعتماد بدانیم، برچسب دقیقی نیست. واقعیت این است که آنها تنها می‌توانند واسطه‌های قابل اعتماد مجددی را شکل بدهند.
۲. بلاکچین‌ها، راه قابل اعتماد جدیدی را به روی ما باز می‌کنند. بلاکچین، نقش‌های برخی بازیگران قابل اعتماد موجود را به چالش می‌کشد و برخی از مسئولیت‌های آنها را بر عهده می‌گیرد و گاهی اوقات نیز قدرت آنها را تضعیف می‌کند.
۳. بلاکچین، اعتماد را از بین نمی‌برد، بلکه شکل آن را تغییر می‌دهد.
۴. همیشه به اعتماد نیاز داریم. چیزی که بلاکچین تغییر می‌دهد، نحوه ارائه اعتماد و نحوه به دست آمدن اعتماد است. هر کسی که اعتماد دیگران را کسب کرد، موفق به ایجاد رابطه می‌شود و اعتماد به بلاکچین نیز از این قاعده مستثنی نخواهد بود.
۵. بلاکچین، اعتماد را غیر متمرکز می‌کند و راه را برای احراز هویت توسط موجودیت‌هایی فراهم می‌سازد که به تنهایی بی‌ضرر هستند، اما وقتی در کنار هم قرار می‌گیرند، عنصر قدرتمندی را شکل خواهند داد.
۶. بلاکچین، ساختار اقتصاد اعتماد[۲۲] موجود را به هم می‌ریزد، زیرا با ورود بلاکچین، هزینه‌های تحویل و ارائه این اعتماد، بین گره‌های مختلف توزیع خواهند شد.
۷. اگرچه اعتماد مرکزی، ما را از هم دور کرد، اما اعتماد توزیع‌شده، ما را به هم نزدیک خواهد کرد.

شاید این بحث انتزاعی به نظر برسد، اما سرویس‌های جدید مبتنی بر اعتماد، از بلاکچین الهام می‌گیرند. به عبارت دیگر، این امکان برای ما فراهم خواهد شد تا بتوانیم صحت[۲۳] و اصالت[۲۴] اطلاعات، داده‌ها، فرایندها، رویدادها یا هر چیز دیگری را به‌سادگی گوگل کردن (جستجو کردن) اطلاعات و سرویس‌ها یا محصولات، بررسی و راستی‌آزمایی کنیم.

در صورت کامل شدن تکرارهای منطق اعتماد[۲۵]، شماره‌گیری (دایالینگ) یا گوگل کردن اعتماد امکان‌پذیر خواهد شد.

پیش از این منطق شـــبکه[۲۶] را کامل کرده‌ایم. رایانه شـــما بعد از اتصال به اینترنت کارش را ادامه می‌دهد. به محض ورود به گســـتره یک اتصال وای فای، رایانه‌تان پیدا می‌شود. می‌توانید از طریق بلوتوث، اتومبیل خودتان را به تلفن هوشمند متصل کنید. همه این کارها به طرزی اعجاب‌انگیز انجام می‌شوند، زیرا توانستیم منطق مربوط به اتصال شبکه‌ها و برقراری ارتباط آسان بین کاربران را درک کنیم. منطق دیگری که به درک و فهم وسیعی نیاز دارد، منطق اعتماد است. این منطق، به تعبیه اعتماد در داخل سیستم‌های سخت‌افزاری و نرم‌افزاری و قادر ساختن محصولات و سرویس‌های مختلف به تعامل آسان با یکدیگر مربوط می‌شود. تصور کنید که اگر به محصولات و عرضه‌های هوشمند مختلفی که بدون کمک انسان می‌توانند کارهای خاصی را به انجام برسانند، اعتماد کنیم، با چه گستره وسیعی از آنها مواجه خواهیم شد. دو نمونه از ویژگی‌های تکمیل کننده اعتماد، جست‌وجوی حقیقت و شفافیت هستند. شفافیت این سوال را مطرح می‌کند که «آیا می‌توانیم آن را ببینیم؟» و حقیقت این سوال را می‌پرسد که «آیا می‌توانیم آن را تایید کنیم؟»

Airbnb، چگونه اعتماد به غریبه‌ها را طراحی کرد؟

Airbnb چه ارتباطی با اعتماد مبتنی بر بلاکچین دارد؟ رابطه‌ای بسیار زیاد.

در صورت استفاده از سرویس Airbnb، از اینکه غریبه‌ها در خانه‌هایتان می‌خوابند هیچ ترسی نخواهید داشت. تطبیق دادن دو غریبه با هم و انجام ســـاده معامله بین آنها در این سرویس آنلاین، شباهت بسیار زیادی به بلاکچین دارد که امکان تعامل فرد به فرد بین دو یا چند گروه را که شناختی از هم ندارند، فراهم می‌سازد. ویژگی مشترک هر دوی این موارد، به میزان سهولت انجام معاملات و وقوع منظم و قابل اعتماد آنها بر می‌گردد. این عنصر مشترک، با به اشتراک گذاشتن یا تسهیم جزئیات مربوط به سوابق و اطلاعات هویتی افراد در ارتباط است. در Airbnb، میهمانان حجم زیادی از اطلاعات مربوط به خودشان را به اشتراک می‌گذارند. این اطلاعات به افزایش اعتماد میزبان‌ها کمک خواهد کرد. در بلاکچین، هویت[۲۷] و شهرت[۲۸]، دو فاکتور سطح ورود اولیه به‌شمار می‌روند که می‌توانند بر تراکنش فرد به فرد تاثیر بگذارند.

طبق نظر جو گبیـــا[۲۹]، یکی از بنیان‌گـــذاران Airbnb، عنصر کلیدی ایجاد اعتمـــاد در این مدل کسب‌وکار، سیستم اعتبارسنجی[۳۰] است که بسیار خوب طراحی شده آن است. علاوه بر این، می‌دانیم

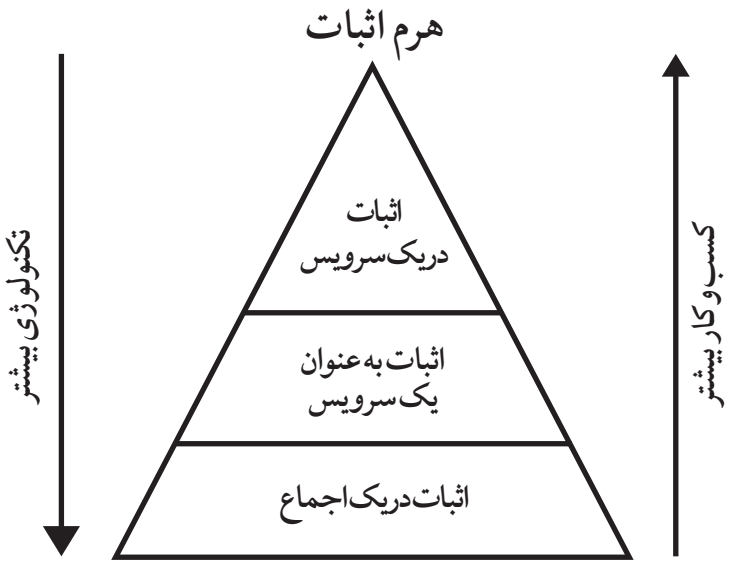
که اعتماد مناسب، مستلزم افشاگری مناسب نیز هست.

در حالی که Airbnb با اعتماد به انسان‌ها سروکار دارد، هدف از طراحی بلاکچین این بود تا بتوان از عنصر موازی اعتماد تراکنشی (معاملاتی) بهره گرفت که انسان نیز بخشی از آن را تشکیل می‌دهد و حضورش در بلاکچین، از طریق جایگاه هویتی و اعتباری‌اش تحقق می‌یابد.

در نهایت Airbnb می‌تواند هویت و شهرت بلاکچین کاربر را برای تکمیل اعتبار و روند شناسایی خود به کار گیرد. وقتی که بلاکچین یک جایگزین قابل اطمینان که قابل انتقال به سرویس‌های دیگر هم هست را ارائه می‌دهد، چرا چرخ را از نو اختراع کنیم؟

طیفی از سرویس‌های اعتماد مبتنی بر اثبات

مسئولیت اثبات اینکه چه چیزی اتفاق افتاده، به طور خاص بر عهده بلاکچین است. سلسله‌ای از روش‌های اثبات وجود دارد که شامل پروتکل اجماع[۳۱] (اثبات کار یا اثبات سهام) اثبات به عنوان خدمت[۳۲] (نظیر اثبات هویت یا مالکیت)، یا اثبات در یک خدمت[۳۳] به معنی ثابت کردن چیزی به عنوان بخشی از سرویس دیگر (نظیر دفتر ثبت زمین یا ثبت ازدواج) می‌شود.



جدول زیر مثال‌هایی در خصوص برخی از سـرویس‌های مبتنی بر اثبـات را ارائه می‌دهد. ما می‌توانیم منتظر لیست طولانی از نوآوری‌هایی باشیم که در دسته‌بندی اثبات به‌عنوان خدمت و اثبات در یک خدمت قرار می‌گیرد.

اثبات به‌عنوان یک خدمت	
اثبات دارایی	اثبات مالکیت
اثبات هویت	اثبات آدرس فیزیکی
اثبات اعتبار	اثبات منبع
اثبات فردیت	اثبات رسید

اثبات در یک خدمت	
دفتر ثبت ازدواج	معاملات طرف مقابل
دفتر ثبت زمین	حسابرسی
زنجیره‌های تامین	رای‌گیری
ثبت دارایی	انتقال سند

اثبات در یک اجماع	
اثبات کار	اثبات قدرت
اثبات سهام	اثبات وجود

چشم‌انداز بلاکچین

یک روش برای درک اینکه بازار بلاکچین چطور در حال رشد است این است که آن را با توجه به سه لایه معماری متوالی تفسیر کنید. برای این کار مجددا از دسته‌بندی‌های رایجی که در اواخر دهه ۱۹۹۰ در توصیف اینترنت از آنها بهره گرفتم، استفاده می‌کنم:

- پروتکل‌ها و زیرساخت‌ها؛
- میان‌افزارها[۳۴] و خدمات؛
- اپلیکیشن‌های کاربر نهایی[۳۵].

عموما داستان به همین شکل است. اولین گام برای پیاده‌سازی هر فناوری‌ای، ایجاد مجموعه‌ای از قابلیت‌های زیرساخت است که شالوده اساسی آن را تشکیل می‌دهند. برای اینترنت، می‌توانیم به بلوک‌های سازنده آن از قبیل TCP/IP و HTTP و SMTP اشاره کنیم. به همین ترتیب، زیرساخت بلاکچین نیز به پروتکل‌های بلاکچین مختلف نیاز دارد. گام بعدی، به تعدادی از سرویس‌ها و نرم‌افزارهای میانی یا میان‌افزارها مربوط می‌شود که بر اساس عناصر زیرساخت، ساخته شده یا ارائه می‌شوند. میان‌افزار، قابلیت کارکردی عناصر زیرساخت را توسعه می‌دهد و به تسهیل ایجاد برنامه‌های کاربردی کمک می‌کند. در واقع، میان‌افزار، همانند یک چسب بین زیرساخت و برنامه‌های کاربردی است. در پایان، هزاران برنامه کاربردی مختلف، با تکیه بر زیرساخت و سرویس‌ها یا نرم‌افزارهای میانی شکل می‌گیرند.

بلوغ بیشتر دو لایه پایینی باعث خواهد شد تا توسعه برنامه‌های کاربردی نیز با سهولت بالاتری انجام بگیرد. ایجاد و شکل‌گیری این سه لایه، ترتیب مشخصی ندارد. توسعه‌دهندگان، حتی در زمانی که لایه‌های زیرساخت و میانی کاملا شکل نگرفته‌اند، تولید برنامه‌های کاربردی را انجام می‌دهند. در نتیجه، لایه‌های مختلف، شاهد تکامل تکراری مربوط به خود خواهند بود.

منافع مستقیم و غیرمستقیم

با توجه به آنچه بیان شد، بلاکچین چه منافعی را به دنبال دارد و چه مشکلاتی را حل خواهد کرد؟

کارآفرینان و استارت‌آپ‌ها نیازی به این سوالات ندارند. آنها همانند اردک‌هایی که به سمت آب می‌روند، به سوی این فناوری جدید هجوم برده‌اند و هر روز، با استفاده از قوانین مختلف، کسب‌وکارها و سولوشن (راهکار)های جدیدی را خلق می‌کنند که جایگزین ابزارهای موجود خواهند شد.

یکی از بخش‌هایی که پاسخ به این سوالات برایشان اهمیت دارند، سازمان‌های بزرگ تجاری‌اند، زیرا منافع حاصل از بلاکچین برای آنها کاملا شناخته‌شده نیست. از نگاه شرکت‌های بزرگ،

بلاکچین، در ابتدای امر، ایده‌ای دردسرساز بود. بلاکچین چیزی بود که هنوز این شرکت‌ها برای آن برنامه‌ریزی خاصی ترتیب نداده بودند.

یک حقیقت نگران‌کننده در زیر سوال بردن منافع بلاکچین وجود دارد؛ اگر از وضع موجود راضی هستید، آنگاه تصور خواهید کرد که بلاکچین، هیچ ارزش جدیدی را تولید نمی‌کند. درست است، بلاکچین قرار نیست تا همه کارها را انجام بدهد، بلکه اگر مشغول حفاظت از چیزی هستید و بلاکچین را برای این کار نادیده بگیرید، ممکن است روزی که یک شرکت مبتنی بر بلاکچین، روی کسب‌وکار شما تاثیر بگذارد، متوجه اشتباه‌تان شوید.

بلاکچین، در زمان ظهور و پیدایش، از اصل کلوچه شانس[۳۶] برنادت جیوا[۳۷] رنج برده است: «مردم کلوچه‌های شانس را می‌خرند، نه به این دلیل که مزه آنها بهتر از هر کلوچه دیگر قابل عرضه است، بلکه دلیل آن به شوق و لذتی بر می‌گردد که در پایان یک وعده غذایی به افراد می‌دهند. برای فروش کلوچه شانس، بازاریاب‌ها باید وقت زیادی را صرف یافتن راهی جهت ایجاد شانس‌های بیشتر و بهتر کنند. شکی نیست که شغل شما پخت کلوچه‌های خوب به بهترین نحو ممکن است، اما علاوه بر آن باید از شیوه بیان خوب در مورد این کلوچه‌ها نیز اطلاع داشته باشید».

از نظر توسعه‌دهندگان، بلاکچین معنا و مفهوم مهمی دارد. آنها قبل از خوردن این کلوچه، داستان شانس آن را پیدا کرده‌اند (از قابلیت‌های آن آگاه شده‌اند). اما از نظر عموم کاربران و بسیاری از سازمان‌ها، بیت‌کوین، بلاکچین و ارزهای رمزنگاری‌شده، معنا و مفهوم زیادی ندارند، زیرا آنها کلوچه‌هایی هستند که فروخته شده‌اند.

هدف مهندسی معمولا حل یک مشکل فنی است، اما اگر حل این مشکل فنی، به حل مشکل کاربر نهایی منجر نشود، آنگاه این سوال در ذهن کاربران تداعی خواهد شد که «آیا این راهکاری برای حل یک مشکل هست... زیرا من چنین مشکلی را نمی‌بینم».

کاربر نهایی فقط به دنبال راهکارهای ساده‌ای است که جواب می‌دهند. از نظر کاربر نهایی، اینکه چه کسی یک فناوری جدید خاص را خلق کرد، اهمیت ندارد. ذی‌نفع‌های کسب‌وکار نیز بخشی از این معادله‌اند، زیرا می‌دانند که مشکلات، هزینه‌های مالی آنها را افزایش خواهند داد و به همین دلیل، به دنبال راهکارهایی می‌گردند که بتوانند این مشکلات را حل کنند.

به‌طور کلی، منافع بلاکچین را می‌توان در حوزه‌های زیر مورد بررسی قرار داد:

- **صرفه‌جویی درهزینه:** مستقیم یا غیر مستقیم؛
- **سرعت:** حذف تاخیرهای زمانی؛
- **شفافیت:** ارائه اطلاعات درست به افراد درست؛
- **حریم شخصی بهتر:** حفاظت مشتریان و کسب‌وکارها از طریق کنترل‌های گسترده‌تر؛
- **ریسک کمتر:** قابلیت دید بهتر، افشای کمتر اطلاعات، کلاهبرداری کمتر، دستکاری کمتر؛
- **دسترسی:** دسترسی منصفانه‌تر؛
- **بهره‌وری:** خروجی کار بیشتر؛
- **کارایی:** گزارش‌گیری یا پردازش سریع‌تر؛
- **کیفیت:** خطاهای کمتر یا رضایت بیشتر؛
- **نتایج:** سودها و رشد.

بلاکچین، قرار نیست تا جایگزین فرایندهای دیگر بشود، بلکه هدفش بهبود فرایندهای موجود است، زیرا بهبود فرایندهایی که اکنون وجود دارند، راحت‌تر از ایجاد یک فرایند جدید است. حداقل، نظر قاطبه مردم و روش کار رایج در داخل سازمان‌های بزرگ این موضوع را نشان می‌دهد.

بله، شـــما می‌توانید فرایند موجود را به اندازه ۱/۵ یا ۲ برابر بهبود بدهید و این موفقیتی قابل قبول است، اما چه می‌شود اگر بتوانیم میزان این بهبود را به ۱۰ برابر برسانیم؟

دوگانگی عجیبی بین نگاه استارت‌آپ‌ها و شرکت‌های بزرگ به بلاکچین وجود دارد. شرکت‌های نوپا بلاکچین را راه‌حلی برای همه چیزها می‌دانند، در حالی که از نظر شرکت‌های بزرگ، این فناوری چیزی جز دردسر نیست، زیرا فرایندهای موجود را به چالش می‌کشد.

توضیح برخی توابع پایه

دارایی هوشمند

دارایی هوشمند[۳۸]، دارایی‌ای اســـت که مالکیتش از طریق بلاکچین و با کمک قراردادها کنترل می‌شود و جزء مهمی در عملیات بلاکچین به شمار می‌رود. برای درک این مفهوم، دو نمونه از پیشینیان آن به نام‌های «فایل دیجیتال»[۳۹] و «دارایی دیجیتال»[۴۰] را در نظر بگیرید. دارایی دیجیتال، نســـخه

دیجیتالی شده یک محصول است که حقوق ویژه استفاده از آن محصول را در بر می گیرد و معمولا دارای ارزش است. اگر ایده مورد بحث، حقوق استفاده از محصول را در بر نگیرد، دیگر یک دارایی به‌شمار نمی‌رود و چیزی بیش از «فایل دیجیتال» نیست. به‌عنوان مثال، ترانه، کتاب الکترونیکی، عکس یا لوگو نمونه‌هایی از دارایی دیجیتال محسوب می‌شوند. قبل از اختراع بیت‌کوین، استفاده از پول به‌عنوان یک دارایی دیجیتال منطقی به نظر نمی‌رسید، زیرا هنوز مشکل خرج مضاعف[۴۱] یا ارسال مضاعف[۴۲] حل نشده بود و در نتیجه، به‌راحتی امکان کلاهبرداری وجود داشت. خرج مضاعف چه مفهومی دارد؟ بگذارید مثالی هر چند دور بزنم تا مفهوم اندکی روشن شود. وقتی عکسی را از تلفن هوشمندتان برای فردی ارسال می‌کنید، هنوز رونوشتی از آن عکس در اختیار شما هم قرار دارد و هر دو، مالک و صاحب آن عکس هستید. در دنیای پول و دارایی هایی که ارزش واقعی دارند، چنین وضعیتی قابل قبول نیست و نمی‌توان مشترکا مالک یک چیز بود.

دارایی هوشمند، از قابلیت‌های ایده دارایی دیجیتال بهره می‌گیرد و دارایی را به گونه‌ای به بلاکچین مورد نظر متصل می‌کند که هرگز امکان خرج مضاعف، مالکیت مضاعف یا ارسال مضاعف وجود نداشته باشد. اگر شما خالق یا مالک این دارایی‌های دیجیتال هستید، می‌توانید به گونه‌ای غیر قابل بازگشت، مالکیت یا حقوق خودتان را حفظ کنید، مگر آنکه خودتان تصمیم به انتقال یا فروش دارایی‌هایتان گرفته باشید. این کار، با کنترل شما و بدون دخالت افراد دیگر صورت می‌گیرد.

با توجه به آنچه بیان شد، شما امکان ایجاد یک دارایی هوشمند را خواهید داشت که می‌داند چه کسی مالکش است. دارایی هوشمند تنها به محصولات صرفا دیجیتال محدود نمی‌شود، بلکه می‌تواند یک شیء فیزیکی نیز باشد که به‌واسطه اتصال صریح یا ضمنی به بلاکچین مربوطه، هوشمند شده است. به‌عنوان مثال می‌توانیم یک قفل، ماشین، یخچال یا حتی خانه را نیز به دارایی هوشمند تبدیل کنیم. بلاکچین می‌تواند به شکل بانک اطلاعاتی قابل ممیزی، به امضای رمزنگاری‌شده شما متصل بشود. بدین طریق، دارایی هوشمندتان به یک اثر انگشت دیجیتالی منحصربه‌فرد متصل خواهد شد. جنبه‌های دیگر بلاکچین از قبیل سودآوری، انعطاف‌پذیری و قابلیت کشف[۴۳]، فاکتورهای مهم دیگری جهت حرکت به سمت تجارت، دادوستدهای مالی و تراکنش‌های فرد به فرد غیر متمرکز به‌شمار می‌روند. دارایی هوشمند شکل جدیدی از مته‌های دیجیتال است که برای ریل‌های بلاکچین ساخته شده‌اند.

برچسب زمانی

برچسب زمانی[۴۴]، یکی از توابع پایه است که دائما به محض وقوع یک عملیات خاص در بلاکچین، روی آن ثبت می‌شود. به‌عنوان مثال، می‌توان به ثبت تغییر مالکیت یک دارایی، انجام معاینات پزشکی یا یک تراکنش خاص اشاره کرد. برچسب زمانی، کمک می‌کند تا در هر لحظه بتوانیم وقوع واقعی یک رویداد در زمان مشخصی در گذشته را اثبات یا تایید کنیم. برچسب زمانی، به محض ثبت شدن روی بلاکچین، غیر قابل انکار و غیر قابل بازگشت است و به همین دلیل، ابزار مفیدی برای جست‌وجوی حقیقت محسوب می‌شود.

تراکنش‌های چندامضایی

قابلیت چندامضایی[۴۵] یا multisig، به فرایندی می‌گویند که در آن، برای روشن شدن وضعیت یک معامله یا تایید آن، به بیش از یک امضا نیاز داریم. قابلیت فوق‌الذکر، معادل نیاز به چند امضا برای معتبر شدن یک توافق کاغذی است، با این تفاوت که به‌صورت خودکار و سریع روی بلاکچین رخ می‌دهد. چیزی که این روش را حتی از آنچه هست قدرتمندتر می‌کند، این است که می‌توانید منطق کسب‌وکار را نیز در بین امضاهای چندگانه درج کنید، به گونه‌ای که هر امضا بتواند یک عملیات جدید را راه بیندازد که به خلق سرویس‌های حساب امانی[۴۶] به‌عنوان بخشی از این تراکنش‌ها کمک می‌کند.

قراردادهای هوشمند

قراردادهای هوشمند[۴۷]، زیربنای مهم و حیاتی فناوری بلاکچین به‌شمار می‌روند. اگر قراردادهای هوشمند را درک نکنید، آنگاه به توان واقعی بلاکچین نیز پی نخواهید برد. تحولی که آنها ایجاد کرده‌اند کمتر از اختراع زبان نشانه‌گذاری HTML نیست که امکان انتشار آزادانه اطلاعات و اتصال به وب را فراهم ساخت. قراردادهای هوشمند امکان برنامه‌نویسی دنیای اطراف را روی بلاکچین فراهم می‌سازند و به‌صورت بالقوه می‌توانند جایگزین برخی از توابعی بشوند که اکنون توسط واسطه‌های قدیمی، کند یا پرهزینه انجام می‌گیرند.

مفهوم قراردادهای هوشمند، ابتدا در سال ۱۹۹۴ توسط نیک زابو[۴۸] مطرح شد، اما از آنجایی که پلتفرمی وجود نداشت تا بتواند قراردادهای هوشمند را اعمال کند، برای مدت زیادی مورد توجه قرار نگرفت، تا اینکه به محض ظهور و پیدایش فناوری بلاکچین بیت‌کوین در سال ۲۰۰۹ بر سر زبان‌ها افتاد. از سال ۲۰۱۵، قراردادهای هوشمند روزبه‌روز رواج بیشتری پیدا می‌کنند و حجم استفاده از

آنها به‌خصوص از زمانی که اتریوم، قابلیت برنامه‌نویسی آنها را در توان بلاکچین خود قرار داد، رایج‌تر شدند.

طبق معمول، وقتی اصطلاحی رواج و گسترش بیشتری یافت، مورد استفاده بیشتر و البته استفاده نادرست و سوءاستفاده بیشتر قرار خواهد گرفت. به همین دلیل، افراد مختلف، چیزهای مختلفی را در مورد این اصطلاح بر سر زبان می‌آورند. در اینجا به برخی حقایق در مورد قراردادهای هوشمند اشاره می‌کنیم:

- **حقیقت اول:** قراردادهای هوشمند با توافق‌های قراردادی[۴۹] فرق دارند. اگر به ایده اولیه نیک زابو مراجعه کنید، قراردادهای هوشمند، هزینه نقض توافق را بالا می‌برند، زیرا دارایی باارزش جهان حقیقی را از طریق ابزارهای دیجیتال کنترل می‌کنند. بنابراین، قرارداد هوشمند می‌تواند به پیاده‌سازی عملی یک نیاز خاص کمک کند و نقض یا عدم نقض شرایط توافق را به اثبات برساند. قراردادهای هوشمند می‌توانند پیاده‌سازی‌های سخت‌گیرانه‌ای از توافقات موجود باشند. به‌عنوان مثال، اگر پرداخت بدهی یک ماشین به موقع انجام نگیرد، ماشین مربوطه، تا زمان دریافت مبلغ توافق، از نظر دیجیتالی قفل خواهد شد.
- **حقیقت دوم:** قراردادهای هوشمند، با قراردادهای ریکاردی[۵۰] فرق دارند. قراردادهای ریکاردی که ابتدا توسط یان گریگ[۵۱] مطرح شدند، به دسته‌ای از بازنمایی‌های معنایی[۵۲] گفته می‌شود که می‌توانند مسئولیت یک توافق واقعی بین طرفین قرارداد را ردیابی کنند. این نوع قراردادها را نیز می‌توان با یا بدون استفاده از قرارداد هوشمند، روی یک بلاکچین پیاده‌سازی کرد. معمولا، امضاهای چندگانه بخشی از انجام یک قرارداد ریکاردی را تشکیل می‌دهند.
- **حقیقت سوم:** قراردادهای هوشمند قانون نیستند. قراردادهای هوشمند، برنامه‌های رایانه‌ای برای کمک به فناوری موجود هستند، اما نتیجه کار آنها می‌تواند بخشی از یک توافق حقوقی را تشکیل بدهد. به‌عنوان مثال، می‌توان با استفاده از یک قرارداد هوشمند، مالکیت سهام را از یک شخص به شخص یا گروه دیگر انتقال داد. از سال ۲۰۱۶ به بعد، شاخه‌های حقوقی مختلفی در رابطه با قراردادهای هوشمند تشکیل شده‌اند. نتیجه هر قرارداد هوشمند را می‌توان برای پیگیری در جهت اثبات رعایت یا عدم رعایت مفاد توافق حقوقی مورد استفاده قرار داد.
- **حقیقت چهارم:** قراردادهای هوشمند هوش مصنوعی را در بر نمی‌گیرند. قراردادهای

هوشمند، کدهای نرم‌افزاری‌ای جهت بازنمایی منطق کسب‌وکار به‌شمار می‌روند که روی بلاکچین اجرا می‌شوند و با استفاده از برخی داده‌های خارجی که امکان تغییر داده‌های دیگر را به آنها خواهند داد، راه‌اندازی می‌شوند. آنها بیش از آنکه به هوش مصنوعی نزدیک باشند، به یک ساختار رویدادگرا شباهت دارند.

- **حقیقت پنجم:** قراردادهای هوشمند، با اپلیکیشن‌های بلاکچین فرق دارند. قراردادهای هوشمند معمولا بخشی از یک اپلیکیشن (بلاکچین) غیرمتمرکزند. هر اپلیکیشن خاص می‌تواند حاوی چندین قرارداد باشد. به‌عنوان مثال، در صورت برآورده شدن شروط خاص یک قرارداد هوشمند، برنامه امکان به‌روزرسانی یک بانک اطلاعاتی را پیدا خواهد کرد.
- **حقیقت ششم:** برنامه‌نویسی قراردادهای هوشمند نسبتا ساده است. نوشتن یک قرارداد ساده کاری ندارد، به‌خصوص اگر از یک زبان قرارداد هوشمند خاص (مثل زبان Solidity اتریوم) استفاده کنید که امکان نوشتن فرایندهای پیچیده را تنها با چند خط کد فراهم می‌سازد. با این وجود، پیاده‌سازی‌های پیشرفته‌تری از قراردادهای هوشمند هم وجود دارند که از اوراکل‌ها[۵۳] بهره می‌گیرند. اوراکل‌ها، منابع داده (دیتاسورس)ای هستند که اطلاعات قابل طرح در دادگاه را به سمت قراردادهای هوشمند می‌فرستند.
- **حقیقت هفتم:** قراردادهای هوشمند، تنها به توسعه‌دهندگان اختصاص ندارند. نسل بعدی قراردادهای هوشمند، نقاط ورود کاربرپسند از قبیل مرورگرهای وب را در بر خواهند گرفت. این به استفاده‌کننده هر کسب‌وکاری امکان خواهد داد تا قراردادهای هوشمند را از طریق رابط کاربر گرافیکی یا احتمالا یک ورودی زبان متنی پیکربندی کند.
- **حقیقت هشتم:** قراردادهای هوشمند، امن هستند. حتی در پیاده‌سازی اتریوم نیز، قراردادهای هوشمند به‌صورت برنامه‌های کامل شبه‌تورینگ[۵۴] اجرا می‌شوند. به عبارت دیگر، در زمان اجرا ریسک گیر کردن در حلقه بی‌نهایت در آنها وجود ندارد.
- **حقیقت نهم:** قراردادهای هوشمند، دامنه کاربرد وسیعی دارند. همانند HTML، محدودیت برنامه‌های کاربردی دیگر نیز به کسی که آنها را نوشته است بستگی خواهد داشت. قراردادهای هوشمند، شیوه ایده‌آلی برای تعامل با دارایی‌های جهان حقیقی، دارایی هوشمند، اینترنت اشیا (IoT) و ابزارهای سرویس‌های مالی به‌شمار می‌روند. کاربرد آنها تنها به نقل‌وانتقال

پول محدود نمی‌شود. قراردادهای هوشمند را می‌توان تقریبا برای هر چیزی که وضعیتش با گذشت زمان تغییر می‌کند و می‌توان ارزشی را به آن نسبت داد، به کار گرفت.

در حال حاضر، توسعه‌دهندگانی که در قراردادهای هوشمند تخصص داشته باشند، خریدار خواهند داشت. یادگیری قراردادهای هوشمند، امکان ورود به بلاکچین را بدون درگیر شدن مستقیم با جزئیات بلاکچین فراهم می‌سازد. بسیاری از زبان‌های قراردادهای هوشمند، مشتقات C++ یا جاوا یا پایتون که سه نمونه از محبوب‌ترین زبان‌های نرم‌افزاری‌اند، می‌باشند و همین امر یادگیری آنها را ساده‌تر خواهد کرد.

قراردادهای هوشمند، بخشی از معماری فناوری بلاکچین هستند که نتوانسته‌اند ارزش واقعی خود را به نمایش بگذارند. با این وجود، مطمئنا به افزایش قدرت بلاکچین در آینده کمک خواهند کرد.

اگر اعتماد را به‌عنوان جزئی‌ترین واحد بلاکچین در نظر بگیریم، قراردادهای هوشمند چیزهایی هستند که تنوع اعتماد در برنامه‌های کاربردی خاص را برنامه‌نویسی می‌کنند. در آینده‌ای نزدیک، میلیون‌ها قرارداد هوشمند که بازنمایی‌های منطقی جهان واقعی ما هستند، بلاکچین را اشغال خواهند کرد و این تحول خوبی است که انتظارش را نیز داریم.

اوراکل‌های هوشمند

اوراکل‌ها مفهوم جالبی هستند که با قراردادهای هوشمند ارتباط دارند. می‌توانیم اوراکل‌ها را به‌عنوان منابع داده خارج از زنجیره[۵۵] در نظر بگیریم که قرارداد هوشمند می‌تواند با استفاده از آنها رفتارش را تغییر بدهد. اوراکل‌های هوشمند حاوی بازنمایی اطلاعات جهان حقیقی از قبیل هویت، آدرس یا گواهینامه هستند و علاوه بر این می‌توانند از یک ویژگی شبه‌عاملی[۵۶] نیز جهت هدایت قراردادهای هوشمند به سمت یک رفتار خاص بهره بگیرند.

اوراکل‌های هوشمند با هم هماهنگ هستند، زیرا یکی از آنها روی بلاکچین (قراردادهای هوشمند) و دیگری در بیرون از زنجیره (اوراکل‌های هوشمند) قرار دارد. به‌عنوان مثال، قرارداد هوشمندی که در ارتباط با تابع KYC (شناسایی کامل مشتری)[۵۷] است، می‌تواند با اوراکل هوشمندی که حاوی اطلاعات هویتی است تعامل برقرار کند. یا اگر یک افسر پلیس می‌خواهد وضعیت گواهینامه راننده‌ای را بررسی کند، به جای شماره‌گیری بانک اطلاعاتی وسایل نقلیه موتوری، می‌تواند بلاکچین

را بررسی کرده و آخرین اطلاعات مربوط به اعتبار گواهینامه، تاریخ انقضا یا سایر اطلاعات مربوط به راننده را به دست بیاورد.

بلاکچین معتمد (قابل اعتماد)، در چه حوزه‌هایی قابل استفاده است؟

برای یادآوری حوزه‌هایی که بلاکچین با آنها ارتباط دارد، پیشنهاد می‌کنم کلمه ATOMIC را به یاد بیاورید؛ A حرف اول assets یا دارایی‌ها، T حرف اول trust یا اعتماد، O حرف اول ownership یا مالکیت، M حرف اول money یا پول، I حرف اول identity یا هویت و C حرف اول contracts یا قراردادها هستند.

در واقع، بلاکچین موارد زیر را عرضه می‌کند: دارایی‌های برنامه‌پذیر[۵۸]؛ اعتماد برنامه‌پذیر؛ مالکیت برنامه‌پذیر؛ پول برنامه‌پذیر؛ هویت برنامه‌پذیر؛ قراردادهای برنامه‌پذیر.

این شش مفهوم، سرعت درک ما از حوزه‌های کاربردی بلاکچین در هر وضعیت خاص را افزایش خواهند داد. اجازه بدهید تا به برخی از آنها بپردازیم.

ایجاد و انتقال بلادرنگ دارایی‌های دیجیتال

می‌توانیم دارایی‌های دیجیتال را بدون متحمل شـــدن تاخیرهای مربوط به تصفیه ناشی از وجود واسطه‌ها، روی بلاکچین ایجاد کرده، مدیریت کنیم و انتقال بدهیم. عدم نیاز به دخالت انسان یا بانک اطلاعاتی مرکزی در فرایند تایید تراکنش‌های مالی، نوآوری بنیادی و بسیار مهمی به‌شمار می‌رود.

تعبیه قوانین اعتماد در داخل تراکنش‌ها و تعاملات

بلاکچین می‌تواند با درج قوانین نشان‌دهنده اعتماد در داخل تراکنش‌ها، روش جدیدی را جهت اعتبارسنجی این تراکنش‌ها از طریق منطق موجود در شبکه و نه از طریق یک مرجع مرکزی یا بانک اطلاعاتی شکل دهد. بنابراین، فاکتور اعتماد جدیدی شکل می‌گیرد که بخشی از خود تراکنش است.

برچسب زمانی، حقوق و اسناد مالکیت

بلاکچین امکان برچسب‌گذاری زمانی اسنادی را که نشان‌دهنده حقوق یا مالکیت هستند، فراهم می‌سازد و در نتیجه، ســـندهای غیر قابل انکاری را ارائه می‌کند که به‌واسطه رمزنگاری، محافظت شده‌اند. ویژگی فوق‌الذکر این امکان را فراهم خواهد ساخت تا بتوان انواع اپلیکیشن‌ها را بر اساس قابلیت‌های تایید (راستی‌آزمایی)[۵۹] جدید و یکپارچه ایجاد کرد.

خوداجرایی[۶۰] منطق کسب‌وکار

از آنجایی که تایید از طریق جعبه سیاه بلاکچین اتفاق می‌افتد و مولفه اعتماد نیز بخشی از تراکنش است، نتیجه نهایی، یک تراکنش خودتصفیه‌گر[۶۱] است. تصفیه[۶۲] و تسویه[۶۳] دارایی‌ها با هم ادغام می‌شوند.

حریم شخصی و شفافیت انتخابی

این کار از طریق فناوری‌های رمزنگاری صورت می‌گیرد و سطوح جدیدی از امنیت و حریم شخصی غیرمتمرکز داده را شکل می‌دهد، به گونه‌ای که تراکنش‌ها را می‌توان بدون افشای اطلاعات مربوط به هویت صاحبانش مورد راستی‌آزمایی قرار داد. شفافیت، اصول خلاقی یک کسب و کار را افشا می‌کند و به همین دلیل با مقاومت مواجه خواهد شد. با این وجود، افزایش شفافیت می‌تواند به افزایش سطوح اعتماد نیز بینجامد.

مقاومت در مقابل سانسور یا نقاط شکست منفرد

از آنجایی که بلاکچین حاوی چندین منبع یا رایانه غیرمتمرکز است، در نتیجه هیچ نقطه شکست منفردی وجود نخواهد داشت. بنابراین، عکس‌العمل شبکه در این حالت بیشتر از زیرساخت‌های تحت کنترل متمرکز خواهد بود. به‌دلیل ماهیت متمرکز ذخیره‌سازی داده، رمزگذاری و کنترل‌های نظیر به‌نظیر در لبه شبکه، بلاکچین معمولا در برابر سانسور نیز مقاوم است.

هویت، مالکیت و بازنمایی

امکان ثبت منحصر به‌فرد هویت‌های گمنام[۶۴]، دارای نام مستعار[۶۵] یا واقعی روی بلاکچین وجود دارد. در نتیجه، می‌توانید هویت خودتان را حفظ کنید و امکان کنترل آن را از طریق گوگل یا فیس‌بوک از بین ببرید.

هویت مبتنی بر بلاکچین، به افراد مختلف امکان می‌دهد تا بتوانند هویت‌شان را کاملا کنترل کنند. در نتیجه می‌توانید بدون نیاز به افشای اطلاعات شخصی، از پیچ‌وخم‌های نقاط دسترسی (اکسس پوینت) مختلف عبور کرده، از سرویس‌های مختلف استفاده کنید و تراکنش‌های مربوط به دارایی‌های دیجیتال را انجام بدهید.

در ساده‌ترین شکل، بلاکچین می‌تواند برای احراز هویت[۶۶] منحصر به‌فرد، به شیوه غیرقابل انکار و غیرقابل بازگشت استفاده شود، زیرا کلیدهایی که در بلاکچین به شما اختصاص یافته‌اند، هویت‌تان

را تشکیل می‌دهند. از آنجایی که هر سرویس مورد استفاده به کلید جداگانه‌ای نیاز دارد، در نتیجه افراد مختلف از چندین کلید استفاده می‌کنند. در این حالت، چه اتفاقی خواهد افتاد؟ حالتی را در نظر بگیرید که پنج کلید برای خانه‌تان دارید و بسته به روزها یا نقاط ورود مختلف، مجبور خواهید بود تا از کلید متفاوتی استفاده کنید. یا حالتی را در نظر بگیرید که پنج خانه مختلف در بخش‌های مختلف دنیا دارید و قطعا مجبور خواهید بود تا برای نگهداری کلیدهایتان از روش‌های مختلفی کمک بگیرید. قطعا این امکان وجود دارد، اما وضعیت چندان مطلوبی نیست.

اگرچه ابزارهای ذهنی یا نوشتاری مختلفی جهت یادآوری گذرواژه‌های مختلف وجود دارند، اما امکان هک شدن یا فراموش کردن گذرواژه‌های آنلاین خیلی زیاد است. تصور می‌کنم که راهکار (سولوشن)های دسترسی و تشخیص هویت[۶۷] به کمک بلاکچین می‌توانند در ارائه راه‌حل‌های بهتر جهت این مشکل به ما کمک کنند.

دنیای ایده‌آل از نظر من، دنیایی است که در آن هویت‌های آنلاین و آفلاین با هم فرق زیادی نداشته باشند. چرا تنها گواهینامه‌های رانندگی فیزیکی اعتبار داشته باشند و هویت‌های آنلاین (مثل فیس‌بوک) را نتوان در بخش امنیتی فرودگاه یا بانک به کار گرفت؟ البته، پاسپورت‌هایی که جدیدا صادر می‌شوند شروعی برای کم شدن این شکاف به‌شمار می‌روند. این پاسپورت‌ها را در کیوسک‌های فرودگاه اسکن می‌کنیم و اطلاعات هویتی‌مان را از طریق اسکن شبکیه یا بخش‌های اطلاعاتی دیگر، جهت سه گوش کردن[۶۸] آنها روی هویت‌مان تکمیل می‌کنیم.

در دنیای بلاکچین، رویکردهای مختلفی جهت مورد هدف قرار دادن امنیت شخصی و هویت، از قبیل اعطای دسترسی به داده و سرویس‌ها وجود دارند. برخی از این رویکردها مستلزم استفاده از راه‌حل‌های سخت‌افزاری جدید و برخی نیازمند به‌کارگیری راه‌حل‌های نرم‌افزاری هستند و تعدادی از آنها نیز با راه‌حل‌های B2B[۶۹] یکپارچه شده‌اند.

- **سخت‌افزار:** به‌عنوان مثال، می‌توان به پاسپورت یا کارت شناسایی دولتی دیگر از قبیل گواهینامه رانندگی اشاره کرد. این کارت‌ها امکان انجام مسافرت یا حق رانندگی با اتومبیل را به ما می‌دهند. برخی از راه‌حل‌های واقع در بلاکچین، این اطلاعات را با داده‌های بیومتریک ترکیب می‌کنند تا احراز هویت کامل‌تری اتفاق بیفتد. به‌عنوان مثال، می‌توانیم به ShoCard و Case اشاره کنیم.

- **نرم‌افزار:** بهترین نمونه در این بخش، تشخیص هویت مبتنی بر OAuth هستند که وقتی برای ورود به برخی وبگاه‌ها از شناسه‌های گوگل یا توئیتر یا فیس‌بوک‌مان استفاده می‌کنیم، اتفاق می‌افتد. با این وجود، در راهکارهای بلاکچین، نقش‌ها برعکس خواهند شـــد؛ شما ابتدا اطلاعات شناسایی خودتان را ثبت می‌کنید[۷۰] و سپس به حساب‌های شبکه‌های اجتماعی‌تان وصل می‌شوید. به‌عنوان مثال، می‌توان به Netki و OneName و BitIID و Idenifi اشاره کرد.
- **یکپارچه‌سازی:** در حالی که نقطه شروع دورویکرد اول را معمولا مشتری تشکیل می‌دهد، اولین گام در این بخش، درک ملزومات یکپارچه‌ســـازی با راهکارهای موجود کسب‌وکار است. به‌عنوان مثال، می‌توان به Cambridge Blockchain و Trunomi و uPort و Tradle و Ripple KYC Gateway اشاره کرد.

طرح‌های تشـــخیص هویت مبتنی بر بلاکچین فرصتی را پیش روی ما قـــرار می‌دهند، اما عدم قطعیت‌هایی در مورد آنها وجود دارد. در سمت مشتری این سوال مطرح می‌شود که آیا می‌توانیم به جای اتصال به فیس‌بوک، گوگل یا توئیتر از آنها استفاده کنیم؟

در سمت کســـب‌وکار این ســـوال مطرح می‌شـــود که آیا این طرح‌ها می‌توانند جایگزینی برای راهکارهای قدرتمند قدیمی از قبیل سیستم مولتی‌بانک 3SKey سوئیفت (جامعه جهانی ارتباطات مالی بین‌بانکی) به‌عنوان یک راه‌حل برای تشـــخیص هویت فردی چندشبکه‌ای یا پروتکل KYC موسسه Markit باشند یا خیر؟

راهکارهای مبتنی بر بلاکچین، با مشکلاتی از قبیل سهولت انجام کارها و رسیدن به تعداد بالای کاربران دست‌وپنجه نرم می‌کنند و این در حالی است که گوگل، فیس‌بوک و توئیتر میلیون‌ها کاربر دارند و هزاران نهاد مالی دیگر، در حال استفاده از سوئیفت یا Markit هستند.

البته صنعت بلاکچین می‌تواند برای همه این مشکلات راه‌حل ارائه کند. چرا هر بار که می‌خواهیم در یک صرافی جدید ارزهای رمزنگاری‌شده ثبت نام کنیم، باید فرایندهای تکراری KYC را پشت سر بگذاریم؟ بیایید تا اشتباهات جهان فیزیکی را تکرار نکنیم.

در زمان پیاده‌سازی و توسعه راهکارهای بلاکچین، با برخی چالش‌ها و سوالات مواجه خواهیم شد که به شرح زیر هستند:

سوالات مشتری

کدام کاربردها ما را بر آن می‌دارند تا از این شکل‌های جدید بازنمایی هویت استفاده کنیم؟ انگیزه کاربر از سیر در دنیای فیس‌بوک و گوگل، دسترسی به رسانه‌های اجتماعی و اسناد است. اما در دنیای بلاکچین، اکثر ارائه‌دهندگان راهکارهای تشخیص هویت تلاش می‌کنند تا قبل از مشخص شدن نوع کاربرد یک راهکار شدید، آن را عرضه کنند.

- **سوال اول:** آیا یک لایه تشخیص هویت شخصی آنلاین خودگردان[۷۱] می‌تواند جای استاندارد غیر رسمی فعلی استفاده از فیس‌بوک یا گوگل جهت احراز هویت افراد و دسترسی به اطلاعات را بگیرد؟
- **سوال دوم:** آیا کاربران تمایلی به مدیریت خودگردان پیچیدگی ناشی از سطوح بالاتر قوانین امنیتی و سطوح دسترسی دارند یا خیر؟
- **سوال سوم:** معنای دقیق قابلیت انتقال یا انتقال‌پذیری[۷۲] در فرایند تشخیص هویت چیست؟ آیا این راهکار نهایتا ما را به مدیریت هویت‌های چندگانه وامی‌دارد و با کابوسی همانند مدیریت گذرواژه‌ها مواجه می‌شویم؟
- **سوال چهارم:** فناوری دانایی صفر، در حفاظت از محرمانگی تراکنش‌ها و حریم شخصی افراد چه نقشی دارد؟
- **سوال پنجم:** نقش تلفن هوشمند چیست؟ آیا همان‌گونه که اکنون به کیف پول دیجیتال ما تبدیل شده است، می‌تواند به پاسپورت دیجیتال ما نیز تبدیل شود؟

ملاحظات بخش کسب‌وکار

اگر کارت ضمانتی یا کلیدهای خصوصی‌مان را گم کردیم، چه اتفاقی خواهد افتاد؟ آیا می‌توان به کاربران معمولی اعتماد کرد تا به همان سادگی که از دارایی‌هایشان در خانه محافظت می‌کنند، دسترسی به داده‌هایشان را نیز خودشان کنترل کنند؟

- **سوال اول:** آیا برای تایید این سیستم‌های تشخیص هویت، به انواع جدیدی از مراجع اعطای گواهینامه[۷۳] نیاز داریم؟
- **سوال دوم:** آیا امکان پیکربندی دقیق‌تر دسترسی به اطلاعات به گونه‌ای وجود دارد که قوانین

امنیتی نظیر به‌نظیر بتوانند جای راهکارهای مبتنی بر فایروال (دیوار آتش) را بگیرند؟

- **سوال سوم:** رابطه آنها با شیوه‌های فعلی KYC چگونه است و آیا راهکارهای جدید تشخیص هویت، لایه امن‌تری را جهت تسهیل AML و انواع فعالیت‌های ضدتروریسم ارائه خواهند داد؟
- **سوال چهارم:** آیا این به استفاده بیشتر از اپلیکیشن‌های سمت مشتری یا اپلیکیشن‌های تجاری کمک خواهد کرد؟
- **سوال پنجم:** آیا موانع قانونی یا حقوقی‌ای وجود دارند که جهت استقرار کامل این نوع از راهکارها باید از پیش رو برداشته شوند؟

سوالات اخلاقی

تغییر عادات یکی از بزرگ‌ترین موانع در پذیرش فناوری به‌شمار می‌رود و حوزه بلاکچین نیز از این قاعده مستثنی نیست. با این وجود نمی‌دانیم که آیا حرکت به سمت هویت‌های دیجیتال، به افزایش سوءاستفاده، کاهش درگیری یا افزایش تعامل کاربر منجر خواهد شد یا خیر.

- **سوال اول:** آیا جداسازی داده و هویت، کار خوبی است؟ آیا این اتفاق، باعث خلق شبه‌هویت‌های چندگانه نمی‌شود؟
- **سوال دوم:** تاریخچه (سابقه) تراکنش چه تاثیری روی شهرت ما دارد؟ آیا درجه‌بندی شهرت آنلاین ما، شیوه امتیازبندی اعتباری[۷۴] جدیدی از جانب مشتریان است؟
- **سوال سوم:** آیا گمنام ماندن چیز خوبی است و آیا نمی‌تواند مورد سوءاستفاده افراد خرابکار قرار بگیرد؟
- **سوال چهارم:** آیا این راهکار، به فراگیری مالی[۷۵] کمک می‌کند و آیا میزان پذیرش کاربران را بالاتر می‌برد؟

امنیت داده‌های غیرمتمرکز

بلاکچین، راهکارهایی را جهت ایجاد موازنه بین امنیت و حفظ حریم شخصی مبتنی بر تراکنش، هویت و داده ارائه می‌کند.

ما پیش از این شاهد نقض حریم شخصی و نفوذهای امنیتی در داخل سازمان‌های متمرکز بزرگ از قبیل Ashley Madison، Blue Cross، Sony، Target و دولت ترکیه بوده‌ایم که این سوال را به ذهن ما تداعی کرده که آیا باز هم می‌توان به امنیت وب یا بانک‌های اطلاعاتی بزرگ اعتماد کرد یا خیر؟ این امکان وجود دارد تا حریم شخصی اطلاعات مشتریان، شهروندان و تاریخچه تراکنش‌ها در معرض خطر قرار بگیرند که تاثیراتی را بر امنیت داده‌های اپلیکیشن‌ها و هویت‌های آنلاین به جای خواهند گذاشت.

ظهور و پیدایش بلاکچین و اپلیکیشن‌های غیر متمرکز مبتنی بر آن، امکان ارائه راهکارهای مربوط به امنیت داده را فراهم ساخت، زیرا رمزگذاری مبتنی بر امنیت کریپتوگرافیک، بخش استاندارد اپلیکیشن‌های بلاکچین را به‌خصوص در رابطه با داده‌های اطلاعاتی تشکیل می‌دهد. به‌طور پیش‌فرض، هر چیزی رمزگذاری می‌شود.

به‌دلیل غیر متمرکزسازی عناصر معماری اطلاعات، هر کاربری می‌تواند مالک داده‌های خصوصی خودش باشد و انبارهای ذخیره‌سازی مرکزی، کمتر در معرض گم شدن داده یا نقض حریم داده قرار می‌گیرند، زیرا تنها اطلاعات رمزگذاری‌شده و اشاره‌گرهای کدگذاری‌شده را روی مکان‌های ذخیره‌سازی توزیع‌شده‌ای قرار می‌دهند که در سراسر شبکه‌های رایانه‌ای توزیع‌شده گسترش پیدا کرده‌اند. در نتیجه، امکان سوءاستفاده هکرها از بین خواهد رفت و آنها نمی‌توانند اطلاعات را بازسازی کنند یا تغییری در آن ایجاد کنند. حداقل از لحاظ تئوری این فرایند کار می‌کند و می‌خواهد به واقعیت تبدیل کند.

در این دنیای جدید، فناوری‌های غیر متمرکز، امنیت، حریم شخصی و الزامات مالکیت داده بخشی از طراحی هستند نه چیزی که بعدا به آن فکر کنیم. آنها تازه از راه رسیده‌اند.

با این حال بلاکچین بی‌عیب و نقص نیست و با چالش هایی در زمینه امنیت در سه حوزه کلیدی مواجه است:

- موتورهای اجماع روی بلاکچین؛
- غیر متمرکزسازی معماری‌های رایانشی؛
- کلاینت‌های* نظیر به نظیر.

*یک نرم‌افزار کاربردی است که از طریق یک شبکه به خدمات یک سامانه رایانه‌ای دیگر به نام سرور دسترسی دارد.

از آنجایی که فرایند اجماع در بلاکچین عمومی[۷۶] سراسری است، در نتیجه، از نظر تئوری در معرض حملات معروف سیبل[۷۷] قرار خواهد گرفت، اگرچه تاکنون چنین حمله‌ای اتفاق نیفتاده است. روند مربوط به معماری‌های رایانش غیر متمرکز، مستلزم چارچوب ذهنی جدیدی جهت پیاده‌سازی و نوشتن اپلیکیشن‌هاست که با چارچوب ذهنی مربوط به معماری‌های وب قدیمی فرق دارد. وقتی یک کلاینت نرم‌افزاری را دانلود می‌کنید که روی رایانه‌تان قرار گرفته و به شبکه گوش می‌دهد، به‌صورت بالقوه در معرض ریسک‌های امنیتی مختلف قرار خواهید داشت، مگر اینکه پیاده‌سازی مناسبی را برای آن انجام داده باشید.

توجه به این نکته حائز اهمیت است که افزاره‌های اینترنت اشیا (IoT) نیز در معرض نفوذهای امنیتی بالقوه قرار دارند، زیرا هر جایی که منبع رایانشی خاصی در لبه وجود داشته باشد، آسیب‌پذیری آن در برابر نفوذها بیشتر خواهد بود.

خوشبختانه برخی راهکارها در این رابطه معرفی شده‌اند که می‌توان به‌عنوان نمونه به بلاکچین خصوصی[۷۸]، سندهای دانایی صفر[۷۹] و امضاهای حلقه‌ای[۸۰] اشاره کرد، اما قصد نداریم در این کتاب به این قلمروهای فنی ورود پیدا کنیم.

نکته حائز اهمیت دیگر آن است که نیازی به بازآفرینی امنیت غیر متمرکز، داده‌های غیر متمرکز و نحوه نوشتن اپلیکیشن‌های غیر متمرکز نیست، زیرا پلتفرم‌های جدیدی وجود دارند که این بلوک‌های سازنده را به‌عنوان یکی از قابلیت‌های حیاتی‌شان در اختیار شما قرار خواهند داد.

اگر توسعه‌دهنده هستید، پیامدهای مربوط به آینده به شرح زیر هستند:

۱. تامین امنیت داده‌های داخل اپلیکیشن‌ها، در حین نوشتن آنها؛
۲. غیر متمرکز کردن داده‌های کاربر جهت حفاظت از آنها؛
۳. آگاهی به فناوری‌های غیر متمرکزسازی و بلاکچین؛
۴. نوشتن قراردادهای هوشمند روی معماری‌های ابری جدید (بدون حضور سرویس‌دهنده‌ها)؛
۵. بازاندیشی در مورد مالکیت‌های هویت مربوط به مشتریان‌تان.

امنیت و حریم شخصی باید بخشی از طرح اولیه شما را تشکیل بدهند و نباید توجه به آنها را به بعد از طراحی موکول کنید.

گمنامی و ارتباطات غیر قابل ردیابی

بلاکچین امکان گمنام ماندن[۸۱] اختیاری کاربر را فراهم می سازد که یکی از آزاردهنده‌ترین ویژگی ها برای قانون‌گذاران و مراجع گزارش گیری مالی، به‌خصوص در اپلیکیشن های سطح مشتری به‌شمار می‌رود. چالش های موجود در این رابطه که ذهن قانون‌گذاران را به خود مشغول کرده‌اند، به پولشویی، تجارت غیرقانونی و فعالیت‌های تروریستی مربوط می‌شوند. در نتیجه این قابلیت، کاربران می‌توانند با استفاده از هویت‌های شبه‌گمنام[۸۲] مخفی بمانند و قبل از شناسایی، به مدت طولانی به فعالیت‌های غیرقانونی خود ادامه بدهند. مشخص است که هدف از طراحی بلاکچین عمومی یا اپلیکیشن‌های غیر متمرکز وابسته به این زنجیره‌ها چنین چیزی نیست. اگرچه این موارد، از دید افراد معمولی، حالت‌های جنبی و کم اهمیتی به‌شمار می‌روند، اما می‌توانند موانعی را بر سر راه سیاست‌گذاران و سازمان‌های دولتی شکل بدهند.

هرچند نمی‌توان ریسک‌های بالقوه مربوط به حفاظت ضمنی از جنایتکاران و افراد غیر قابل اعتماد را نادیده گرفت، اما مواردی هم وجود دارند که نشان می‌دهد استفاده از ارتباطات غیر قابل ردیابی، چیز بدی نیست.

از نگاه دیوید شاوم[۸۳]، مخترع فناوری‌های حریم شخصی و پول نقد دیجیتال، ارتباطات غیر قابل ردیابی[۸۴] پایه و اساس آزادی تحقیق، آزادی بیان و همچنین حریم شخصی آنلاین، از قبیل آنچه در ارتباطات نفر به نفر می‌بینیم را تشکیل می‌دهد. جهت برآورده ساختن این نیازها باید با حفظ گمنامی، قابلیت‌های زیر را در اختیار کاربر قرار بدهیم؛ گپ (chat)، به اشتراک‌گذاری عکس و ویدئو، دنبال کردن فیدها[۸۵]، جست‌وجو، ارسال پست و پرداخت‌ها. همه این قابلیت‌ها، باید همراه با انواع مختلف احراز هویت مبتنی بر نام مستعار ارائه شوند.

در سال ۱۹۹۴، کوین کلی[۸۶]، نویسنده کتاب «خارج از کنترل»[۸۷]، به موارد زیر اشاره کرد: «هر جامعه خوب و کامل، به چیزی بیشتر از گمنامی نیاز دارد. تمدن آنلاین[۸۸] مستلزم گمنامی آنلاین، تشخیص هویت آنلاین، احراز هویت آنلاین، شهرت‌های آنلاین، دارندگان اعتماد آنلاین، امضاهای آنلاین، حریم شخصی آنلاین و دسترسی آنلاین است. همه اینها عناصر سازنده و اساسی یک جامعه باز به‌شمار می‌روند».

متاسفانه تا سال ۲۰۱۶ این ایده محقق نشد و از «جامعه آنلاین، باز و کاملا خوب» فاصله زیادی

داشتیم. بلاکچین می‌تواند به بهبود این وضعیت کمک کند، زیرا تعداد بسیار زیادی از شرکت‌های وب، متمرکز هستند و مجموعه سرویس‌هایی را که امکان غیر متمرکز شدن بیشتری داشته‌اند در داخل خود جای داده‌اند.

این امید وجود دارد که بتوانیم بین گمنامی و حسابرسی[۸۹] موازنه‌ای برقرار کرده و تعادل خوبی را میان آنها ایجاد کنیم که به‌واسطه آن بتوان افراد شرور داخل شبکه را شناسایی کرد و در عین حال، بخش عمده کاربران خوب بتوانند کارهای معمول خودشان را ادامه بدهند.

بلاکچین در قالب ابر

علاوه بر آنچه بیان شد، می‌توان بلاکچین را به‌صورت یک زیرساخت مشترک در نظر گرفت که چیزی شبیه به شرکت ارائه‌دهنده خدمات عمومی است. تامین مالی زیرساخت فعلی اینترنت از طریق پرداخت ماهانه کارمزدها به ارائه‌دهندگان سرویس اینترنت صورت می‌گیرد. به محض رواج بلاکچین عمومی و اجرای میلیون‌ها قرارداد هوشمند و سرویس تایید هویت روی آن، می‌توانیم از طرق مختلف از قبیل پرداخت از طریق تراکنش‌های خرد[۹۰]، کارمزدهای تراکنش[۹۱]، عوارض[۹۲] قراردادهای هوشمند، دکمه‌های کمک بلاعوض[۹۳] یا طرح‌های «پرداخت به ازای استفاده»[۹۴]، حمایت مالی این کارها را انجام بدهیم.

بلاکچین، همانند یک رایانه مجازی است که در جایی در یک ابر توزیع شده[۹۵] مجازی قرار دارد و در آن، نیازی به پیکربندی سرویس‌دهنده نیست. هر کسی که یک گره بلاکچین را باز کرد، سرویس‌دهنده را اجرا می‌کند و کاربران و توسعه‌دهندگان دیگر، این توانایی را ندارند.

بنابراین، بلاکچین همانند یک زیرساخت شبکه‌بندی‌شده از تجهیزات رایانشی است. بر این اساس می‌توان به‌سادگی نحوه اجرای برنامه‌های رایانه‌ای روی این زیرساخت جدید را تصور کرد.

با این وجود، نباید از قیاس رایانش ابری برداشت تحت‌اللفظی بشود. زیرساخت بلاکچین، جایگزینی برای رایانش ابری نیست، بلکه وسیله‌ای جهت دموکراتیزه کردن بخش‌های مختلف آن به حساب می‌آید.

محتمل‌ترین تعریف آن است که زیرساخت بلاکچین را شبیه به یک لایه از زیرساخت رایانش ابری در نظر بگیریم. قابلیت‌های ماشین‌های مجازی بلاکچین، در قیاس با سرویس‌های ابری معمولی از

قبیل سرویس های وب آمازون یا DigitalOcean، خیلی هزینه‌بر هستند، اما قطعا برای قراردادهای هوشمند که منطق‌شان را روی ماشین‌های مجازی بلاکچین یا اپلیکیشن‌های غیر متمرکز اجرا می کنند (Dappها) مفید خواهند بود. در آینده نزدیک، گره‌های کلاینت می توانند مستقیما با هم صحبت کنند که البته با هزینه بالا یا کندی بلاکچین مواجه خواهند شد.

وقتی اپلیکیشنی را در فضای ابری اجرا می کنید (به‌عنوان مثال، روی سرویس های وب آمازون یا پلتفرم Azure مایکروسافت)، هزینه صورت‌حساب شما با توجه به زمان، فضای ذخیره‌سازی، انتقال داده و سرعت رایانشی مورد نیاز محاسبه می‌شود. نکته جدید در مورد قیمت‌گذاری ماشین مجازی این است که بابت اجرای منطق تجاری روی بلاکچین پول پرداخت می کنید. اگر بلاکچین وجود نداشته باشد، می توان منطق تجاری را روی سرویس‌دهنده‌های فیزیکی و زیرساخت ابری موجود اجرا کرد. اما مزیت بلاکچین در اینجا آن اســت که نیازی به نگرانی در مورد پیکربندی سرورهای موجود در آن نیست، زیرا سرویس‌دهنده‌ها توسط کاربران دیگری مدیریت می‌شوند که بابت اجرای این زیرساخت از طریق استخراج[۹۶] پول دریافت خواهند کرد.

بنابراین، ابر بلاکچین از یک مدل قیمت‌گذاری ارزش خرد[۹۷] بهره می گیرد که شبیه به پشته رایانش ابری سنتی است، اما این کار را با کمک لایه‌ای جدید به انجام می‌رساند. ابر بلاکچین، از نظر فیزیکی جدا نیست، بلکه لایه جدیدی از اعتبارسنجی تراکنش مبتنی بر رمزنگاری و ثبت انتقال حالت‌ها[۹۸] روی یک ابر موازی و در عین حال نازک‌تر است.

با این وجود، اجرای اپلیکیشن‌های روی این زیرساخت جدید کار چندان ساده‌ای نیست. جهت انجام این کار باید از مدل جدیدی از اپ‌های غیر متمرکز بهره بگیریم که مطابق با معماری لایه‌ای جدیدی به نام web3 است که توســط گاوین وود[۹۹] ابداع شد. Web3 معماری‌ای است که به‌طور خاص روی بلاکچین کار می کند. بگذارید به‌عنوان مثال اتریوم را در نظر بگیریم. در اینجا، معماری web3 موارد زیر را دربر می گیرد: ۱) یک مرورگر پیشرفته به‌عنوان کلاینت؛ ۲) دفترکل بلاکچین[۱۰۰] به‌عنوان منبع مشترک؛ ۳) یک شــبکه مجازی از رایانه‌ها که برنامه‌های منطق تجاری هوشمند را به گونه‌ای غیر متمرکز و از طریق تعامل با موتور اجماع بلاکچیــن که وظیفه‌اش تصفیه تراکنش‌ها یا تغییر یک مقدار است، اجرا می کند. مدل جدید فوق‌الذکر، واقعا به هموار شدن مسیر آتی رایانش غیر متمرکز مبتنی بر رمزنگاری کمک می کند و نــوع تغییر یافته‌ای از معماری اپ‌های وب موجود

است که در آن، کدهای جاوااسکریپت در داخل مرورگرها و کد سمت سرور (server-side) روی سرویس‌دهنده‌های شرکت اجرا می‌شوند.

بیایید به نحوه انجام کار در این فرایند بپردازیم. در اینجا شاهد یک لایه‌برداری در قطعات مختلف فناوری هستیم:

نکته ۱: در حال حاضر، رابط‌های برنامه‌نویسی کاربردی (API)[۱۰۱]، به یک زیرساخت عمومی تعلق دارند که از امنیت رمزنگاری بهره می‌گیرد (بلاکچین).

نکته ۲: بلاکچین به‌عنوان شکل جدیدی از بانک اطلاعاتی به کار گرفته می‌شوند. مثلا می‌توان آنها را به‌عنوان فضایی جهت ذخیره‌سازی دائمی کلیدهای رمزنگاری تغییرناپذیر (یا hashها) در جداول هش توزیع‌شده (DHT)[۱۰۲] مورد استفاده قرار داد. جداول هش توزیع‌شده، به مقادیر داده بزرگ‌تری که خارج از زنجیره ذخیره شده‌اند، اشاره می‌کنند.

نکته ۳: نوع جدید مرورگرها به کاربران امکان می‌دهند تا علاوه بر صفحات وب بتوانند اپ‌های غیرمتمرکز (Dapp) را نیز اجرا کنند (مثل مرورگر Mist مربوط به اتریوم).

نکته ۴: پروتکل فرامتن اولیه و اصلی وب، با کمک پروتکل فرارسانه‌ای جدیدی به نام سیستم فایل بین‌سیاره‌ای (IPFS)[۱۰۳] تقویت می‌شود که سیستم فایل توزیع‌شده نظیر به‌نظیر است و همه افزاره‌های رایانشی را با یک سیستم فایل واحد به هم متصل می‌کند.

نکته ۵: حقوق قراردادی به بخش‌های کوچک‌تری تقسیم می‌شود. به‌عنوان مثال، می‌توانیم به قراردادهای ریکاردی اشاره کنیم که بدهی یک شخص به شخص دیگر را ردیابی می‌کنند. مثلا OpenBazzar آنها را در پروتکل تجارت الکترونیک نظیر به‌نظیر مورد استفاده قرار می‌دهد.

بلاکچین می‌تواند سازمان‌های بزرگ را هم تحت تاثیر قرار بدهد. کاربران کسب‌وکار نیز می‌توانند قراردادهای هوشمندشان، اپ‌های نظیر به‌نظیر (P2P) و سایر اپ‌ها را بدون کسب مجوز از دپارتمان‌های فناوری اطلاعات روی بلاکچین باز، اجرا کنند. شیوه انجام این کار همانند راهکار اولیه «نرم‌افزار در قالب سرویس یا SaaS»[۱۰۴] است که یک اسب تروجان بود و به کارمندان امکان می‌داد تا بدون اختلال در زیرساخت‌های شرکت بتوانند جهت دریافت سرویس‌ها، به‌تنهایی ثبت نام کنند.

دلیل امکان استفاده از این شکل جدید از SaaS این است که می‌توانیم بر اساس هزینه مشترک و قابلیت نظیر به‌نظیر، لایه زیرساخت جدیدی را ایجاد کنیم. هزینه‌های این زیرساخت رایانشی جدید،

به احتمال زیاد پایین و برابر با هزینه امروزی دسترسی به اینترنت خواهند بود. اگر چنین اتفاقی بیفتد و هزینه پایین باشد، می توان قابلیت‌های اپلیکیشن‌های موجود در این حوزه را باز هم افزایش داد.

این ابر نازک[۱۰۵]، آزادی و انعطاف‌پذیری را برای کاربران و توسعه‌دهندگان به ارمغان می‌آورد و به افراد مختلف امکان می‌دهد تا بتوانند منطق تجاری خودشان را در رابطه با مالکیت، تجارت، حقوق قراردادی، قالب‌های تراکنش و توابع انتقال حالت، بدون نگرانی در مورد پیکربندی زیرساخت شکل بدهند.

نباید اهمیت این ابر نازک را به‌عنوان یکی از پیامدهای حاصل از زیرساخت‌های بلاکچین مختلف نادیده بگیریم و باید اپلیکیشن‌های خلاقانه‌ای را جهت اجرا روی این ابر نازک ایجاد کنیم.

نزدیک شدن به میلیون‌ها بلاکچین

در سال ۱۹۹۴ که با ظهور و پیدایش وب همراه بود، وب‌سایت‌ها ایده جدید و نویی بودند و تا حول و حوش سال‌های ۱۹۹۸، فهرست‌های زیادی را از ۵۰۰ شرکت برتر، با یا بدون وب‌سایت در اختیار داشتیم. تقریبا سه سال طول کشید تا اکثر شرکت‌ها به این موج بپیوندند. تعداد بسیار زیادی از این سایت‌های اولیه، به‌دلیل وجود فرم‌های اطلاعاتی و بروشورهای مجلل مورد نقد قرار گرفتند. یکی از چند شرکت بزرگی که توانست کسب‌وکار خوبی در اینترنت راه بیندازد، آمازون بود.

به‌سرعت به سال ۲۰۱۶ و پس از آن برمی‌گردیم. به زبان استعاره، بلاکچین چیزی همانند یک وب‌سایت جدید خواهد بود. بله، بلاکچین‌ها، گیک‌پسند[۱۰۶] (مترجم: مطابق با تعریف دیکشنری https://www.thefreedictionary.com، به فرد مصمم یا موفق در کارهای فنی یا علمی که البته از نظر اجتماعی ضعیف است گیک یا نرد گفته می‌شود. اگرچه در واقعیت امر، گیک‌ها و نردها دقیقا مثل هم نیستند) هستند، اما هر شرکتی می‌تواند در نوعی از بلاکچین، از قبیل خصوصی، نیمه‌خصوصی یا عمومی مشارکت داشته باشد یا مالکیت آن را بر عهده بگیرد.

همانند وب‌سایت‌ها در اینجا نیز شرکت‌ها می‌توانند از رویکرد پورتالی مشابهی برای ارائه سرویس‌های مختلف بلاکچین و تسهیل فرایند ورود و استقرار[۱۰۷] کاربران جدید و در عین حال به نمایش گذاشتن قابلیت‌های بلاکچین کمک بگیرند.

اولین گام به یافتن ابزار مناسب برای بلاکچین برمی‌گردد که با عملیات فعلی شما شروع می‌شود.

درست همان‌طور که قبل از ایجاد وب‌ســـایت‌تان باید در مورد نوع اطلاعات منتشرشده روی آن به نتیجه برسید، جهت شروع کار با بلاکچین نیز باید در ابتدای امر، موردهای استفاده بالقوه بلاکچین و سرویس‌های تبادل ارزش نظیر به‌نظیر مختلف آن مشخص بشوند.

تقریبا تصور اینکه وقتی ساتوشی ناکاموتو[۱۰۸] کد مربوط به اولین بلاکچین بیت‌کوین را در سال ۲۰۰۹ منتشر کرد، فقط از دورایانه و یک توکن کمک گرفته بود، غیرممکن است. پس از این تاریخ، بلاکچین مورد اشاره رشد و توسعه یافت، زیرا هر کسی می‌توانست یک برنامه نرم‌افزاری را دانلود کند و آن را به‌عنوان گره مشابه دیگری که همان کد را اجرا خواهد کرد به شبکه متصل کند. در نتیجه، شبکه‌ای شکل گرفت که خودبه‌خود در حال رشد بود.

بیت‌کوین اولین بلاکچین عمومی به‌شمار می‌رفت و بقیه بلاکچین‌ها از آن الهام گرفتند. زنجیره عمومی مهم دیگر اتریوم نام داشت که به‌سرعت رو به رشد است و پس از بیت‌کوین، دومین بلاکچین عمومی بزرگ به‌شمار می‌رود که چند منظوره است.

یکی از فرق‌های مهم بین بلاکچین عمومی و خصوصی آن است که بلاکچین عمومی معمولا هدف کلی و عمومی دارند و اســـتفاده از آنها با هزینه کمتری اتفاق می‌افتد، در حالی که بلاکچین خصوصی، از کاربرد اختصاصی‌تری برخوردارند و هزینه پیکربندی آنها به‌دلیل تعداد کمتر صاحبان آنها بیشتر خواهد بود. علاوه بر این، بلاکچین عمومی تک‌منظوره از قبیل Zcash نیز شکل گرفته‌اند که ادعا می‌کنند که حریم شخصی کامل را در اختیار کاربر قرار خواهند داد.

با افزایش تعداد بلاکچین عمومی، خصوصی، نیمه‌خصوصی، تک‌منظوره و انواع دیگری از آنها، در آینده‌ای نزدیک، شاهد میلیون‌ها بلاکچین خواهیم بود.

نکات مهم فصل دوم

۱. بلاکچین، مدل جدیدی را جهت پیاده‌سازی اعتماد تراکنشی ارائه می‌کند. باید ذهن‌مان را باز کنیم و بپذیریم که می‌توان به جای تایید اعتماد از طریق انسان‌ها، این اعتماد را توسط ماشین‌ها محاسبه کرد.
۲. می‌توان با افزایش شفافیت، یعنی به اشتراک گذاشتن اطلاعات شهرت و هویت به اعتماد رسید.
۳. بلاکچین از اثبات وقوع یک چیز کمک می‌گیرد. با دسترســـی‌ای شـــبیه به شیوه گوگل کردن

اطلاعات، می توان میلیون‌ها مورد از این حالت‌ها را در اختیار داشت.

۴. گمنامی، هویت، داده‌های غیر متمرکز و امنیت، موضوعاتی هستند که به‌خوبی در بلاکچین مورد توجه قرار گرفته‌اند.

۵. قراردادهای هوشمند و دارایی هوشمند، سنگ بناهای کلیدی و مهم عملیات یک بلاکچین به‌شمار می‌روند و زمینه اســتفاده از امکانات و اپلیکیشن‌های زیادی را فراهم می‌سازند. این وضعیت باعث شده است تا توسعه‌دهندگان، به‌صورت فزاینده‌ای به ایجاد اپلیکیشن‌های مبتنی بر قرارداد هوشمند دست بزنند و نگران یادگیری عناصر داخلی بلاکچین نباشند.

پی‌نوشت

1. John Gage
2. consensus
3. peer to peer transactions
4. trust
5. reliance
6. predictability
7. confidence
8. truth
9. assurance
10. credence
11. certainty
12. certitude
13. responsibility
14. dependence
15. trust function
16. transparency
17. blockchain-based decentralized consensus protocol
18. trusted authorities
19. trust checking
20. friction-rich
21. decentralized trust
22. economics of trust
23. veracity
24. authenticity
25. trust logic
26. network logic
27. identity
28. reputation

29. Joe Gebbia
30. reputation system
31. consensus protocol
32. Proof-as-a-Service
33. Proof-in-the-Service
34. middleware
35. End-User
36. fortune cookie
37. Bernadette Jiwa
38. smart property
39. digital file
40. digital asset
41. double-spend
42. double-send
43. discoverability
44. timestamping
45. multisignature
46. escrow services
47. smart contracts
48. Nick Szabo
49. contractual agreement
50. Ricardian contract
51. Ian Grigg
52. semantic representation
53. oracle
54. quasi-Turing
55. off-chain
56. agent-like
57. Know Your Customer
58. programmable

59. verification
60. self-execution or self-enforcement
61. self-clearing
62. clearing
63. settlement
64. anonymous
65. pseudonymous
66. authentication
67. identification
68. triangulate
69. Business-to-business
70. self-register
71. self-managed
72. portability
73. certificate authorities
74. credit score
75. financial inclusion
76. public blockchain
77. Sybil
78. private blockchain
79. zero-knowledge proofs
80. ring signatures
81. anonymity
82. pseudo-anonymous
83. David Shaum
84. untraceable communication
85. feed following
86. Kevin Kelly
87. out of control
88. online civilization

89. accountability
90. micro-transactions
91. transaction fees
92. tolls
93. donation
94. pay-per-use
95. distributed cloud
96. mining
97. micro-value pricing model
98. state transition
99. Gavin Wood
100. blockchain ledger
101. Application Programming Interface
102. Distributed Hash Table
103. Interplanetary File System
104. Software-as-a-service
105. thin cloud
106. geeky
107. on-boarding
108. Satoshi Nakamoto

پیام‌های ندیده عهد نوز

بلاکچین یکی از روندهای تاثیرگذار فناوری است که در سال‌های گذشته تغییراتی در دنیای کسب‌وکار ایجاد کرده است. به نظر می‌رسد هنوز پتانسیل‌های این فناوری به‌صورت کامل ظهور و بروز نیافته و احتمالا در سال‌های آتی و با بلوغ بیشتر این فناوری شاهد ابعاد بیشتری از آن باشیم. اهمیت این فناوری در آینده لزوم مطالعه و شناخت آن را به ما گوشزد می‌کند. کتاب کسب‌وکار بلاکچین یکی از سه کتاب خوب و مهمی است که در جهان در زمینه این موضوع منتشر شده و برای اولین بار به زبان فارسی منتشر می‌شود. اگر می‌خواهید درباره ابعاد مختلف این فناوری آینده‌ساز بیشتر بدانید، فرصت مطالعه این کتاب را از دست ندهید.

WILEY

کتاب کسب و کار بلاکچین با حمایت کارخانه نوآوری راه‌کار منتشر شده و ناشر اصلی آن انتشارات وایلی است

راه‌کار
کارخانه نوآوری راه‌کار
way2work.ir

ISBN 978-622-7702-40-8
۵۰۰ هزار تومان

انتشارات راه پرداخت
ناشر فناوری و نوآوری
way2pay.press