

بِسْمِ اللَّهِ
الرَّحْمَنِ الرَّحِيمِ

۱

۳

۹

۷

مبانی بلاکچین

مقدمه‌ای غیرفنی در ۲۵ گام



سرشناسه: درشر، دنیل. Daniel Dresher / عنوان و نام پدیدآور: مبانی بلاکچین؛ مقدمه‌ای غیرفنی در ۲۵ گام/ دنیل درشر؛ ترجمه سیاوش تفضلی. / مشخصات نشر: تهران: صفحه سفید، ۱۳۹۷. / مشخصات ظاهری: ؟؟ ص؛ ۱۴/۲۱×۵/س م. / شابک: ۱-۳۲-۶۵۹۹-۹۶۴-۹۷۸ / وضعیت فهرست نویسی: فیبا/ یادداشت: عنوان اصلی: Blockchain Basics: A Non-Technical Introduction in 25 Steps / موضوع: رمزگذاری داده‌ها؛ Data Encryption؛ موضوع: بلاکچین Blockchain؛ شناسه افزوده: درشر، دنیل شناسه افزوده: تفضلی، سیاوش، ۱۳۶۴ / رده‌بندی کنگره: الف ۱۷۱۰ HG/د ۴م ۲ ۱۳۹۷ رده بندی دیویی: ۲۸/۱۷۸۰/۳۳۲

مبانی بلاکچین

مقدمه‌ای غیرفنی در ۲۵ گام

دنیل درشر

مترجم:
سیاوش تفضلی



مبانی بلاکچین، مقدمه‌ای غیرفنی در ۲۵ گام / ناشر: صفحه سفید / مؤلف: دنیل درشر / مترجم: سیاوش تفضلی /
ویراستار محتوایی: قاسم سرافرازی / ویراستار متن: یلدا شایسته‌فر / صفحه‌آرا: علیرضا کیوان / نوبت چاپ:
اول ۱۳۹۷ / شماره‌گان: ۱۰۰۰ نسخه / شابک ۱-۳۲-۶۵۹۹-۹۶۴-۹۷۸ / تمام حقوق این اثر محفوظ و متعلق
به موسسه شبکه عصر تراکنش (راه پرداخت) است تلفن: ۰۹۱۰۶۹۴۹۳۰۲ / دورنگار: ۸۹۷۸۴۹۰۲ / پست
الکترونیک: mediamanager.ir@gmail.com / پایگاه اینترنتی: Way2Pay.ir
نشانی انتشارات و مرکز پخش: تهران، خیابان طالقانی میدان فلسطین شماره ۹ تلفن ۸۹۸۰۹۶۳

۲۱	گام اول: تفکر در لایه‌ها و جوانب
۲۷	گام دوم: نظری به نمای کلی
۳۷	گام سوم: شناخت قابلیت‌ها
۴۹	گام چهارم: فهم مساله اصلی
۵۵	گام پنجم: شفاف‌سازی معنی
۶۱	گام ششم: درک مفهوم مالکیت
۷۱	گام هفتم: خرج دوباره پول
۸۱	گام هشتم: طرح کلی بلاکچین
۸۹	گام نهم: ثبت مالکیت
۹۷	گام دهم: هش کردن اطلاعات
۱۰۹	گام یازدهم: هش کردن در دنیای واقعی
۱۲۳	گام دوازدهم: شناسایی و حفاظت از حساب‌های کاربری

- گام سیزدهم: اعطای مجوز معاملات ۱۳۵
- گام چهاردهم: ذخیره داده‌های معاملاتی ۱۴۳
- گام پانزدهم: استفاده از انباره داده‌ها ۱۵۷
- گام شانزدهم: محافظت از انباره داده‌ها ۱۶۹
- گام هفدهم: توزیع انباره داده بین گره‌ها ۱۸۱
- گام هجدهم: تایید و افزودن معاملات ۱۹۱
- گام نوزدهم: انتخاب یک تاریخچه معاملاتی ۲۰۵
- گام بیستم: پرداخت برای یکپارچگی ۲۲۵
- گام بیست و یکم: گردهم‌آوری قطعات مجزا ۲۳۳
- گام بیست و دوم: مشاهده محدودیت‌ها ۲۵۱
- گام بیست و سوم: نوآفرینی بلاکچین ۲۶۱
- گام بیست و چهارم: استفاده از بلاکچین ۲۷۵
- گام بیست و پنجم: جمع‌بندی و افق پیش رو ۲۸۹

یادداشت حامی

«نمی توانم ترس مردم از ایده‌های جدید را درک کنم. من از ایده‌های کهنه و قدیمی می ترسم.»

جان گیچ

فین تک یعنی کاربرد نوآورانه فناوری در ارائه خدمات مالی. برآمدن فین تک از دل بحران اعتباری سال ۲۰۰۷ بوده است. امروز کسب و کارهایی مانند ریپل، کوین بیس، استرایپ، اسکوتر و izetl داستان‌های موفقیت دنیای فین تک هستند. با این حال توجه به فین تک در سال‌های گذشته به شکل اغراق آمیزی رشد داشته است. این رشد توجه در بین فعالان بانکداری، پرداخت، بورس و بیمه تا حدی است که توهم مانند قارچ بعد از رعد و برق رشد کرده است. اخیراً سوزان چیستی، ویرایشگر ارشد کتاب فین تک تحقیقی انجام داده و نتیجه گرفته بسیاری از متخصصان فین تک درباره دانش فین تکی خود بلوف می زنند! به گفته موسسه فین تک سیرکل، بسیاری از متخصصان حوزه فین تک ممکن است آن دانش و آگاهی که ادعایش را می کنند، نداشته باشند. به گفته این شرکت، ۹۴ درصد افراد فعال در حوزه سرویس‌های مالی می گویند که بسیاری از همکاران‌شان از لغات و کلماتی مانند «زنجیره بلوک» یا «هوش مصنوعی» استفاده می کنند؛ بدون اینکه حتی معنی آن را بدانند. جالب است حتی ۶۰ درصد افراد می گویند که چنین ادعا و به قول معروف بلوف زدن‌هایی، کاری رایج و معمول

است. در واقع این متخصصان بر این باورند که عدم آموزش در سازمان‌های خدمات مالی بزرگ‌ترین عاملی است که مانع توسعه دانش و مهارت‌های دیجیتال و فین‌تکی کارمندان می‌شود. این موسسه بر این باور است که هیچ‌وقت برای توسعه مهارت‌های فین‌تکی و دیجیتالی افراد فعال در این حوزه دیر نیست و امروزه هم در صنعت خدمات مالی، ارتباط مستقیمی میان دانش واقعی دیجیتالی افراد و ارتقا و پیشرفت شغلی آنها وجود دارد؛ به همین دلیل انستیتوی فین‌تک سیرکل ایجاد شد تا بتواند کارشناسان مالی را با دانش عملی فین‌تک توانمند کند.

بلاکچین یک ابر تکنولوژی 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 یک لایه ساختاری از یک بلاکچین را بررسی می‌کنید، متوجه خواهید شد که چندین قسمت تشکیل شده است؛ پایگاه داده، نرم‌افزار کاربردی، تعدادی از کامپیوترهای متصل به یکدیگر، مشتریان برای دسترسی به آن، محیط نرم‌افزاری برای توسعه آن، ابزار برای نظارت بر آن و قطعات دیگر.

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 بودیم، به زمان ورود وب برمی‌گردد. 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 ۱۹۳۳، یک زبان نشانه‌گذاری باعث تغییر حالت انتشار در وب شد. در سال ۱۹۹۵، جاوا یک زبان برنامه‌نویسی تحت وب را تغییر داد. چند سال قبل از آن TCP/IP که یک پروتکل شبکه کامپیوتری است با تغییر کامل شبکه در سراسر جهان شروع به تغییر کرد.

از نظر یک برنامه‌نویس، یکی از بزرگ‌ترین نمونه‌ها و پارادایم‌های تغییر که بلاکچین ادعا کرده است، به چالش کشیدن عملکرد و انحصاری بودن پایگاه داده‌های سنتی به آن شکلی است که ما آنها را می‌شناسیم. بنابراین ما باید عمیقاً درک کنیم که چگونه بلاکچین ما را مجاب می‌کند درباره سازه‌های پایگاه‌های داده موجود فکر کنیم. بنابراین لازم است بدانیم که وقتی داریم درباره بلاکچین صحبت می‌کنیم، صرفاً درباره یک فناوری معمولی حرف نمی‌زنیم. بلاکچین یک فناوری بنیادین است؛ چیزی که احتمالاً در سال‌های آینده ساختارهای مالی و اقتصادی و حتی اجتماعی و سیاسی را تغییر می‌دهد. اساساً قراردادها، تراکنش‌ها و ذخیره‌سازی این تراکنش‌ها، سیستم‌های سیاسی، حقوقی و اقتصادی جوامع را تعریف می‌کنند. اینکه ما مالک چه چیزهایی هستیم، مجاز به انجام چه کارهایی هستیم و نیستیم، اجازه ورود به چه مکان‌هایی را داریم یا نداریم و با چه کسانی مجاز به تعامل هستیم و بسیاری از آن چیزهایی که هویت ما را در جامعه تعریف می‌کنند؛ مبتنی بر قراردادها، تراکنش‌ها و البته شیوه‌های ذخیره‌سازی و دسترسی به آنها هستند. بنابراین این سه مورد، از دارایی‌های ما محافظت می‌کنند و مرزهای سازمان‌ها را مشخص می‌کنند. هویت ما وابسته به این سه موضوع است و تعامل بین ملت‌ها، سازمان‌ها، گروه‌ها، افراد و حاکمیت را تعریف می‌کنند. متأسفانه بوروکراسی حاکم بر سازمان‌ها هنوز نتوانسته با تحول دیجیتال کنار بیاید. سازمان‌ها و رویه‌های آنها مانند ترافیک سنگینی می‌مانند که یک ماشین مسابقه‌ای فرمول‌وان را گیر انداخته‌اند. در دنیای دیجیتال نحوه تنظیم مقررات و حفظ و کنترل مدیریت امور باید تغییر کند.

امیدوارم این کتاب گامی در راستای توسعه دانش و مفاهیم فناوری‌های مالی در ایران باشد.

بابک رهنماپور

مدیرعامل شرکت پرداخت الکترونیک سپهر

یادداشت حامی

«هایپ» بهترین واژه برای توضیح بسیاری از صحبت‌ها درباره بیت‌کوین و بلاکچین است. در سال‌های گذشته فناوری و نوآوری چهره خدمات مالی در دنیا را تغییر داده است؛ منتها شدت تغییرات به اندازه‌ای زیاد بوده است که بخش زیادی از ادعاهایی که مطرح می‌شود توخالی است. در زمینه ارزهای رمزنگاری شده مانند بیت‌کوین و بلاکچین به کرات این اتفاق تکرار شده است. برای همین پیش از اینکه هایپ ما را با خودش ببرد، لازم است از خودمان پرسیم که آیا به بلاکچین نیازی داریم؟ پیش از پاسخ به این سوال باید از خودمان پرسیم که آیا به پول نقد دیجیتال نیازی داریم؟ اگر پاسخ مثبت است، می‌توان بیت‌کوین را پیشنهاد داد و اگر پاسخ منفی است ما نیازی به بلاکچین نداریم. فراموش نکنیم بیشتر صحبت‌هایی که این روزها درباره بلاکچین در دنیا مطرح می‌شود یک «هایپ» است.

بلاکچین چیست؟

بلاکچین یک دفترکل توزیع شده غیر متمرکز است. «بلاک» اطلاعات دیجیتالی است که در یک دیتابیس عمومی ذخیره شده است که به آن زنجیره می‌گوییم. در بلاک‌ها اطلاعاتی درباره تراکنش‌ها ذخیره می‌شود؛ مواردی مانند تاریخ، زمان و ارزش. تراکنش‌ها یک امضای دیجیتال منحصر به فرد دارند. هر بلاک هم کد منحصر به فردی

دارد که به آن هاش گفته می‌شود که معرف بلاک است. هر تراکنشی در یک بلاک ذخیره می‌شود و آن تراکنش باید توسط یک شبکه از کامپیوترها تایید شده باشد. وقتی تراکنش‌ها تایید شد، بلاک با هاش مخصوص خود به بلاکچین (زنجیره بلوک) اضافه می‌شود. هر کامپیوتری که در شبکه حضور دارد، دقیقاً یک کپی یکسان از بلاکچین نگهداری می‌کند. میلیون‌ها کامپیوتر اینچنینی در شبکه وجود دارد که به آنها نود گفته می‌شود. این فرم دفترکل توزیع شده به شدت در مقابل دستکاری ایمن است و اطلاعات ذخیره شده قابل تغییر نیست.

بلاکچین چه مزایایی دارد؟

بلاکچین صرفاً یک دستاورد فنی نیست. بلاکچین نقطه وصل مفاهیم دنیای توزیع شده است؛ مهم‌ترین نکته‌ای که بلاکچین به ما یادآوری کرد، تمرکززدایی بود. اعتماد در بی‌اعتمادی یکی از دستاوردهای بلاکچین است؛ یعنی برای انجام تراکنش‌ها در محیطی که افراد به هم اعتماد ندارند، نیازی به واسطه‌ها وجود ندارد. همیشه این واسطه‌ها بوده‌اند که نقش ایجاد اعتماد در محیط‌های بدون اعتماد را به عهده گرفته‌اند. حالا این نقش به بلاکچین سپرده شده است. مواردی مانند حاکمیت افراد بر پروتکل، مقاوم در برابر سانسور و تغییر و ضد تورم بودن از ویژگی‌های مثبت بلاکچین است. به عبارتی بلاکچین زمینه حاکمیت اثربخش مردم را فراهم می‌کند و افراد می‌توانند دیدگاه‌هایشان را از طریق پروتکل به قانون تبدیل کنند.

چه معایبی وجود دارد؟

انجام پردازش‌های سنگین‌تر برای یک کار یکسان؛ حذف تمامی اختیارات انسانی؛ کارایی پایین، گران و کند (در بیشتر اپلیکیشن‌ها)؛ بنابراین بسیاری از صحبت‌هایی که مطرح می‌شود که بلاکچین ابزاری ارزان برای انتقال پول است، اشتباه است. یا مثلاً اینکه بلاکچین کارایی بالایی دارد و می‌توان به‌آسانی از طریق آن پول منتقل کرد، درست نیست. بلاکچین ابزاری کند، گران و با کارایی پایین است؛ بلاکچین فناوری است که به‌طور خاص برای این طراحی شده که واسطه‌ها را حذف کند.

برای رسیدن به این هدف نیاز به مصرف انرژی بسیار زیادی وجود دارد. راه‌حل‌های متمرکز عموماً سریع‌تر، ارزان‌تر و کارایی بیشتری دارند که وظیفه ایجاد اعتماد را یک واسطه طرف سوم ایجاد می‌کند. نکته جالب اینجاست که تقریباً تمام راه‌حل‌های مبتنی بر بلاکچین فعلی جایی نیاز به طرف سوم و واسطه پیدا می‌کنند که این با فلسفه بلاکچین در تضاد است؛ بنابراین تمرکززدایی باید به اندازه کافی جذاب باشد که افراد حاضر شوند هزینه بیشتر و کارایی کمتر را به جان بخرند؛ همان‌گونه که این موضوع در بیت‌کوین جواب داده است.

پتانسیل‌های بلاکچین

فعلاً در سه حوزه پتانسیل‌های بلاکچین تقریباً بالفعل شده است؛ پرداخت‌های دیجیتال مانند بیت‌کوین؛ قراردادهای هوشمند مانند اتریوم و مدیریت دیتابیس و رکوردها. در مورد پرداخت‌های دیجیتال مانند بیت‌کوین به اندازه کافی صحبت شده است. اجازه دهید اندکی درباره دو موضوع دیگر صحبت کنیم.

قراردادهای هوشمند

اتریوم یک سیستم رمزنگاری هوشمند است که قراردادها را در بستر بلاکچین به صورت خودکار درمی‌آورد. توجه داشته باشیم که هیچ بازگشتی در این قراردادها وجود ندارد و هیچ نظارتی توسط نهادهای نظارتی و پلیس امکان‌پذیر نیست. اگر باگی در نرم‌افزار وجود داشته باشد، این موضوع باعث از کار افتادن قرارداد می‌شود. یادمان باشد که اکوسیستم اتریوم پیش از این یک بار دچار مشکل شده و در کدهک صورت گرفت. دقت کنیم که کد قانون نیست. اگر دادگاه‌ها را با کد جایگزین کنیم، آنگاه برنامه‌نویس‌ها را هم باید با و کلا جایگزین کنیم. چه می‌شود اگر چیزی به شکل خطار رخ دهد؟ آیا به دادگاه‌ها احتیاج نخواهیم داشت؟

کاربردهای بالقوه در آینده گسترده‌تر خواهد بود. قراردادهای هوشمند در آینده که «سواد کد» در میان مردم افزایش یافته و کدها قابل پیش‌بینی‌تر و قابل اعتمادتر از

امروز باشند، کاربردهای قراردادهای هوشمند هم جدی تر می شود. امروز حتی در زمینه قراردادهای هوشمند هم بیشتر با یک هایپ سروکار داریم؛ مگر اینکه قراردادها ساده باشند و کد بتواند به آسانی تایید و درک شود.

دیتابیس و مدیریت رکورد

توکنایز کردن یکی از کاربردهای بلاکچین است. بلاکچین یک دیتابیس قابل اعتماد یا یک سیستم ثبت دارایی در ارز مخصوص خودش (native currency) است. این به این معناست که این ارز در مقابل حمله‌ها مقاوم است. بلاکچین در پیچه جدیدی به روی ما باز کرده و قطعا در سال‌های آتی و با بلوغ فناوری شاهد رشد بیشتر این فناوری در حوزه‌های گوناگون خواهیم بود. منتها باید توجه داشته باشیم که این مهم دست نخواهد داد مگر با شناخت همه‌جانبه ابعاد مختلف فناوری. امیدوارم این کتاب زمینه‌آشنایی بیشتر مردم ایران با این فناوری بنیادین را فراهم کند.

یاشار نجف‌زاده

رئیس هیات‌مدیره شرکت پرداخت الکترونیک سپهر

یادداشت مترجم

از حدود دو سال و نیم گذشته که تب بلاکچین ناگهان همه گیر شد، بارها با پرسش‌های گوناگونی در رابطه با چیستی این فناوری مواجه شده‌ام. سوای این که برخی از این پرسش‌ها اساساً از حیثه دانش من فراتر می‌رفتند، یکی از پرسش‌های بی‌پاسخ، درخواست معرفی منبع مناسب فارسی در زمینه بلاکچین بود. ترجمه کتاب حاضر به سادگی تلاشی است برای پاسخ به این پرسش! یک کتاب شناخته شده و پرفروش که با زبانی غیرفنی به شرح مفاهیم پایه‌ای برای درک فناوری بلاکچین می‌پردازد. البته از زمان شروع ترجمه تاکنون کتاب‌های مفید دیگری هم در این زمینه در بازار نشر فارسی عرضه شده است، امیدوارم این کتاب هم بتواند نقشی در راستای گسترش آشنایی درست با بلاکچین میان خوانندگان فارسی‌زبان ایفا کند.

آشنایی من با بلاکچین به سال‌های اول عرضه بیت‌کوین باز می‌گردد. نوآوری هوشمندانه‌ای که در آن زمان ابعاد و پتانسیل‌های آن برایم هنوز آشکار نشده بود. طی این سال‌ها، این فناوری هم به لحاظ ابعاد بازار و هم به لحاظ کارکردها و جامعه متخصصین رشد قابل توجهی کرده و می‌توان امروزه آن را داغ‌ترین موضوع بحث جاری در دنیای کامپیوتر به شمار آورد. جریانی که علاوه بر خوره‌های فناوری و استارت‌آپ‌های کوچک، شرکت‌های بزرگ بین‌المللی را هم با خود همراه کرده است.

به منظور همراهی با این روند نوآورانه و به فراخور ارتباط بلاکچین با فناوری‌های مالی، بخشی از منابع و امکانات مجموعه نیلین که در آن مشغول به کار هستیم را به این زمینه و به طور خاص به توسعه محصولات بر پایه اتریوم اختصاص داده‌ایم. بارها برای درک مفاهیم بلاکچین از همراهی، مباحثه و مشاجره! با دوستانم در نیلین بهره برده‌ام. از آنجا که این شناخت سازمانی در آماده‌سازی کتاب حاضر هم تأثیرگذار بوده است، مایل‌م نام همگی ایشان را در اینجا ذکر کنم. از مریم نعمتی، علی دهقانی، نوید اقبالی، کوروش عظیمی، افشین تفضلی، امین شفیعی، محمد نعمتی، بهراد ختائی‌زاده، فاطمه ایمانی‌پور، پیمان عرب و علی‌الخصوص دکتر مهدی محجوبی سپاسگزارم.

سیاوش تفضلی

بخش یک

اصطلاحات و مبانی فنی

این بخش با توضیح مفاهیم اساسی مهندسی نرم افزار، معماری کامپیوتر و موضوع صحت کارکرد، ارتباط کلی آنها با بلاکچین را مطرح کرده و پایه ای استاندارد برای صحبت درباره فناوری فراهم می سازد. با مطالعه این بخش به برداشتی کلی از هدف بلاکچین و پتانسیل آن نائل می شوید.

گام اول

تفکر در لایه‌ها و جوانب

تحلیل سیستم با تفکیک لایه‌ها و جنبه‌های مختلف

این گام به مفاهیم مبنایی استاندارد برای تحلیل سیستم و فناوری می‌پردازد. مفاهیمی که گفت‌وگوی ما در رابطه با بلاکچین بر اساس آنها صورت می‌گیرد. چگونگی تحلیل یک سیستم نرم‌افزاری بر پایه لایه‌ها و جنبه‌های مختلف آن و ارتباط چنین تحلیلی با بلاکچین شرح داده شده و در پایان به توضیح کوتاهی از مفهوم صحت کارکرد (Integrity) نرم‌افزار و اهمیت آن ختم می‌شود.

یک مثال استعاری

شما احتمالاً تلفن همراه دارید! چقدر درباره پروتکل‌های مختلف بی‌سیم یا امواج الکترومغناطیسی که اساس ارتباطات بی‌سیم موبایلی هستند، می‌دانید؟ اغلب افراد در رابطه با این موارد دانش زیادی ندارند؛ چراکه اطلاع درباره موارد ذکر شده برای استفاده روزمره و عادی از موبایل ضرورتی ندارد. ما به صورت ذهنی فناوری تلفن همراه را به دو بخشی که لازم است درباره آن اطلاع داشته باشیم و بخشی که اطلاع درباره آن ضرورتی ندارد، تقسیم می‌کنیم. چنین رهیافتی در تعامل با فناوری محدود به تلفن همراه نبوده و در رابطه با سایر فناوری‌ها؛ از تلویزیون گرفته تا ماشین ظرفشویی یا خودرو هم رایج است. البته سطح این تفکیک بسته به افراد مختلف با توجه به شرایطی که دارند، متفاوت بوده و به فناوری، تجربیات و نیازهای آنها وابسته است. این تفاوت ممکن است در تعاملات بین افراد در رابطه با یک فناوری خاص ایجاد اشکال کند؛ بنابراین یکسان‌سازی نحوه تفکیک یک سیستم به لایه‌های مختلف و از جنبه‌های گوناگون، برای گفت‌وگو یا آموزش آن فناوری ضرورت دارد.

لایه‌ها و جنبه‌های یک سیستم نرم‌افزاری

در این کتاب، تفکیک سیستم به دو شکل زیر صورت می‌گیرد:

- کاربرد در مقابل پیاده‌سازی؛
- جنبه‌های عملکردی در مقابل جنبه‌های غیرعملکردی.

کاربرد در مقابل پیاده‌سازی

تفکیک ذهنی نیازهای کاربر از جنبه‌های فنی سیستم به لایه‌بندی کاربرد در مقابل پیاده‌سازی منجر می‌شود. مواردی مانند گرفتن عکس، گوش دادن به موزیک یا مرور صفحات وب، در لایه کاربرد قرار می‌گیرند، لایه پیاده‌سازی بر «عملی کردن» موارد لایه کاربرد تمرکز دارد؛ برای نمونه دریافت پیکسل‌های رنگی در دوربین و تبدیل به اطلاعات دیجیتال، تبدیل اطلاعات دیجیتال به صدا و ارسال و دریافت اطلاعات بر بستر اینترنت.

جنبه‌های عملکردی در مقابل غیر عملکردی

یک سیستم از جنبه‌های عملکردی مختلف و چگونگی آن عملکردها قابل تحلیل است. برای نمونه ارسال اطلاعات در بستر اینترنت، پخش موزیک و برداشتن عکس عملکردهای مختلف یک موبایل هستند، از سوی دیگر رابط کاربری زیبا، اجرای سریع نرم‌افزارها و حفظ اطلاعات به صورت امن، جنبه‌های غیر عملکردی موبایل به شمار می‌روند. یکی از جنبه‌های غیر عملکردی سیستم صحت کارکرد (integrity) است. به این معنا که سیستم به همان ترتیبی که انتظار می‌رود، به درستی عمل کند. یک راه سریع برای تشخیص جنبه‌های عملکردی و غیر عملکردی رجوع به گرامر زبانی است؛ مواردی که به صورت فعل ذکر می‌شوند به جنبه‌های عملکردی اشاره دارند و مواردی که به صورت قید ذکر می‌شوند، ناظر بر جنبه‌های غیر عملکردی هستند. برای نمونه «راه رفتن» به عنوان یک فعل به جنبه‌ای عملکردی اشاره دارد، در حالی که فرد می‌تواند همین عمل را با کیفیت‌های مختلف «به آهستگی» و «به سرعت» انجام دهد.

لایه‌ها و جنبه‌های مختلف در یک نما

لایه‌های کاربردی و پیاده‌سازی در کنار جنبه‌های عملکردی و غیر عملکردی موبایل در جدول زیر نشان داده شده است.

جدول ۱-۱: نمونه‌ای از تفکیک تلفن همراه در قالب جنبه‌ها و لایه‌های مختلف

جنبه‌های غیر عملکردی	جنبه‌های عملکردی	
رابط کاربری زیبا راحتی استفاده ارسال سریع پیام	عکاسی تماس تلفنی ارسال ایمیل مرور اینترنت ارسال پیام در پیام‌رسان	لایه کاربرد
ذخیره امن اطلاعات مصرف بهینه انرژی صحت کارکرد حفظ حریم خصوصی کاربر	ذخیره اطلاعات کاربر اتصال به نزدیک‌ترین آنتن موبایل دسترسی به پیکسل‌های دوربین دیجیتال	لایه پیاده‌سازی

جنبه‌های عملکردی لایه کاربرد، روشن‌ترین بخش‌های یک سیستم هستند. از سوی دیگر، جنبه‌های غیرعملکردی لایه پیاده‌سازی، عموماً خیلی به چشم نمی‌آیند و وجود آنها به عنوان مبانی کار در نظر گرفته می‌شود.

صحت کارکرد

صحت کارکرد یکی از جنبه‌های غیرعملکردی بسیار مهم هر سیستم نرم‌افزای است که شامل موارد زیر می‌شود:

- **صحت کارکرد اطلاعاتی (Data integrity):** اطلاعات ذخیره‌شده در سیستم کامل، درست و فارغ از مغایرت و تناقض باشد.
- **صحت کارکرد رفتاری (Behavioral integrity):** سیستم به همان نحو مورد انتظار، رفتار کرده و بدون خطاهای منطقی باشد.
- **امنیت (Security):** سیستم بتواند دسترسی به اطلاعات و عملکرد خود را صرفاً برای کاربران مجاز فراهم کند.

اغلب ما ممکن است صحت کارکرد یک سیستم را امری مفروض و بدیهی به‌شمار بیاوریم؛ چراکه عموماً با سیستم‌هایی دارای صحت کارکرد مواجه بوده‌ایم، اما چنین وضعی با تلاش فراوان برنامه‌نویس‌ها و مهندسان نرم‌افزار و طی آزمون‌های مختلف پیش از عرضه محصول حاصل شده است. پیش فرض بدیهی بودن صحت کارکرد زمانی به چالش کشیده می‌شود که با نرم‌افزاری دارای اشکال مواجه شویم. از دست رفتن یا لورفتن اطلاعات، عملکردهای غیرمعقول یا اشتباه و مواردی از این دست، علاوه بر عصبانی کردن ما، اهمیت بسیار بالایی صحت کارکرد نرم‌افزاری را روشن می‌سازند. به دلیل همین اهمیت بالاست که متخصصان نرم‌افزار زمان بسیار طولانی را برای جنبه‌های به‌ظاهر کوچک غیرعملکردی در لایه پیاده‌سازی صرف می‌کنند.

خلاصه

- سیستم‌ها را می‌توان با تفکیک به لایه‌ها و جنبه‌های مختلف تحلیل کرد:
- لایه‌های کاربرد و پیاده‌سازی؛

- جنبه‌های عملکردی و غیرعملکردی.
- لایه کاربرد، ناظر بر نیازهای کاربر است؛ در حالی که لایه پیاده‌سازی به عملی شدن موارد لایه کاربرد می‌پردازد.
- موضوع جنبه‌های عملکردی، کاری است که انجام می‌شود؛ در حالی که جنبه‌های غیرعملکردی به چگونگی و کیفیت آن عملکرد می‌پردازند.
- اغلب کاربران به جنبه‌های عملکردی لایه کاربرد توجه دارند، جنبه‌های غیرعملکردی سیستم علی‌الخصوص در لایه پیاده‌سازی کمتر مورد توجه است.
- صحت کارکرد یک جنبه مهم غیرعملکردی در هر سیستم نرم‌افزاری است و شامل سه مورد می‌شود:
 - صحت کارکرد اطلاعاتی؛
 - صحت کارکرد رفتاری؛
 - امنیت.
- اغلب خطاهای نرم‌افزاری مانند از دست رفتن اطلاعات، کارکردهای غیرمنطقی یا اعطای دسترسی غیرمجاز به افراد در نتیجه ضعف در صحت کارکرد رخ می‌دهند.

گام دوم نظری به نمای کلی

معماری نرم افزار و ارتباط آن با بلاکچین

این گام به ارائه نمایی کلی از موقعیت بلاکچین می پردازد. به این منظور ابتدا مفهوم معماری نرم افزار و ارتباط آن با تفکیک لایه ها و جنبه های مختلف یک محصول نرم افزاری طرح شده؛ سپس با اشاره به ارتباط میان بلاکچین و معماری نرم افزار، هدف اصلی بلاکچین در یک جمله بیان می شود. درک هدف بلاکچین در شناخت مفهوم آن و فهم سایر گام های این کتاب نقش کلیدی دارد.

یک مثال استعاری

همان‌طور که می‌دانید، موتور خودروهای سواری انواع متفاوتی دارد. این موضوع برای انواع مختلف یک مدل خودرو خاص هم صادق است. (برای نمونه از جنبه سوخت می‌تواند دیزل، بنزینی یا الکتریکی باشد.) این وضعیت که پیمان‌سازی یا مدولاسیون (Modularization) خوانده می‌شود، حاصل اعمال تفکر لایه‌بندی بر تولید خودروها است. وجود گزینه‌های متنوع در زمان خرید انواع مختلف یک مدل خودرو می‌تواند به تنوع جالب توجهی منجر شود. دو خودروی سواری با ظاهر یکسان ممکن است از نظر قدرت موتور و کارایی بسیار متفاوت باشند. به علاوه، انتخاب یک مدل خاص از خودرو می‌تواند بر موارد گوناگون دیگری همچون قیمت، هزینه نگهداری، نوع سوخت مصرفی و ... تاثیرگذار باشد. با در نظر داشتن این مثال، درک نقش بلاکچین در نمای کلی که ارائه خواهد شد به مراتب آسان‌تر می‌شود.

لایه‌ها و جنبه‌های یک سیستم پرداخت

می‌خواهیم روش تفکیکی گام قبلی را بر یک سیستم پرداخت اعمال کنیم. جدول ۱-۲ جنبه‌ها و لایه‌های مختلف یک سیستم پرداخت را نشان می‌دهد.
جدول ۱-۲: جنبه‌ها و لایه‌های یک سیستم پرداخت

جنبه‌های غیر عملکردی	جنبه‌های عملکردی	
رابط کاربری زیبا راحتی استفاده انتقال سریع پول	واریز پول برداشت پول انتقال پول دریافت گزارش تراکنش	لایه کاربرد
۲۴ ساعته بودن مقاوم در برابر تقلب دارا بودن صحت کارکرد حفظ حریم خصوصی کاربر	؟	لایه پیاده‌سازی

توجه شما هم به آن علامت سوال در بخشی از جدول که قاعدتا باید به اطلاعاتی درباره فناوری اشاره می‌کرد، جلب شد؟ این بخش همان جایی است که باید درباره قرار

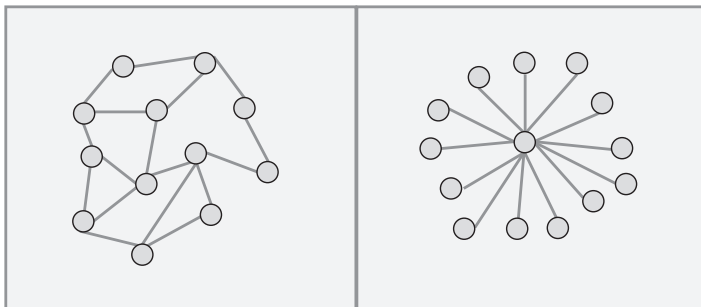
دادن «موتور» پیشران سیستم تصمیم بگیریم. در ادامه بیشتر درباره معادل موتور خودرو در سیستم‌های نرم‌افزاری صحبت می‌کنیم.

دو نوع معماری کامپیوتر

راه‌های مختلفی برای پیاده‌سازی سیستم‌های نرم‌افزاری وجود دارد، اما یکی از مهم‌ترین تصمیمات در زمان طراحی یک سیستم، معماری آن است. یعنی روشی که اجزای سیستم ساماندهی شده و به هم مرتبط می‌شوند. دو نوع اصلی معماری سیستم نرم‌افزاری عبارتند از: متمرکز (Centralized) و توزیع شده (Distributed).

در یک سیستم نرم‌افزاری متمرکز، اجزای سیستم در اطراف یک بخش مرکزی و در ارتباط با آن ساماندهی می‌شوند. در مقابل، اجزای یک سیستم توزیع شده در عین ارتباط با یکدیگر به هیچ جزء مرکزی متصل نیستند.

شکل ۱-۲ نمایی از این دو نوع معماری را نشان می‌دهد. دایره‌ها نشانگر اجزای سیستم هستند که گره (Node) خوانده می‌شوند، خطوط هم نشانگر ارتباط بین اجزاست. فعلاً لازم نیست به نقش گره‌ها و اطلاعات رد و بدل شده بین آنها بپردازیم. در سمت چپ شکل یک سیستم توزیع شده را می‌بینید؛ در عین ارتباط اجزا با هم، هیچ گرهی با همه موارد دیگر ارتباط مستقیم ندارد. با وجود این، هر گرهی با یا بدون واسطه به همه گره‌ها متصل است. در سمت راست تصویر، یک سیستم متمرکز را می‌بینید که در آن همه گره‌ها به یک هسته مرکزی متصل شده‌اند و هیچ ارتباط مستقیم دیگری هم با یکدیگر ندارند.



شکل ۱-۲: معماری سیستم توزیع شده (چپ) و متمرکز (راست)

مزایای سیستم توزیع شده

مزایای اصلی سیستم‌های توزیع شده عبارتند از:

- قدرت محاسباتی بالاتر؛
- کاهش هزینه؛
- قابلیت اتکای بالاتر؛
- قابلیت رشد و مقیاس پذیری پیوسته.

قدرت محاسباتی بالاتر

از آنجایی که قدرت محاسباتی یک سیستم توزیع شده از تجمیع قدرت اجزای آن حاصل می‌شود، چنین سیستم‌هایی عموماً قابلیت محاسباتی بالاتری نسبت به یک کامپیوتر تنها دارند. چنین امری گاهی در مقایسه سیستم‌های توزیع شده متشکل از کامپیوترهای ضعیف در مقابل با ابر کامپیوترهای مستقل هم صدق می‌کند.

کاهش هزینه

هزینه کامپیوترها از جنبه‌های مختلف شامل حافظه، فضای دیسک و تجهیزات شبکه طی ۲۰ سال گذشته به میزان زیادی کاهش یافته است. از آنجایی که سیستم‌های توزیع شده متشکل از تعداد زیاد کامپیوتر متصل به هم هستند، هزینه اولیه یک سیستم توزیع شده بیشتر از هزینه اولیه یک کامپیوتر مستقل است. اما هزینه‌های ساخت، نگهداری و استفاده از ابر کامپیوترها هنوز بسیار بیشتر از هزینه‌های ساخت، نگهداری و استفاده از سیستم‌های توزیع شده است. این امر تا حدودی از آنجا ناشی می‌شود که جایگزین کردن یک کامپیوتر خاص از یک سیستم توزیع شده می‌تواند بدون ایجاد تاثیر محسوس بر سیستم صورت پذیرد.

قابلیت اتکای بالاتر

اگر یکی از گره‌ها در یک سیستم توزیع شده دچار اشکال شود، سیستم می‌تواند با تکیه بر بقیه اجزا و بدون مشکل به عملکرد خود ادامه دهد. در یک سیستم متمرکز،

ایجاد اشکال در کامپیوتر مرکزی می تواند به توقف عملکرد سیستم منجر شود. بنابراین یک ابر کامپیوتر مستقل عموماً قابلیت اتکای پایین تری نسبت به یک سیستم توزیع شده دارد.

قابلیت رشد و مقیاس پذیری پیوسته

قابلیت محاسباتی یک شبکه توزیع شده برآمده از قدرت محاسباتی اجزای آن است. با افزودن کامپیوترهای بیشتر به شبکه می توان قدرت محاسباتی آن را در هر گام افزایش داد. به این ترتیب می توان به راحتی افزایش نیاز پیوسته به قدرت محاسباتی را پاسخ گفت. در مقابل، در سیستم متمرکز، برای افزایش قدرت محاسباتی باید کامپیوترها با انواعی دارای قدرت محاسباتی بالاتر جایگزین شوند و افزایش قدرت محاسباتی به صورت پیوسته انجام نمی گیرد.

معایب سیستم توزیع شده

در مقابل سیستم های متمرکز، سیستم توزیع شده معایب زیر را دارد:

- سر باره هماهنگ سازی سیستم؛
- سر باره ارتباطات؛
- وابستگی به شبکه؛
- پیچیدگی نرم افزاری بیشتر؛
- مسائل امنیتی.

سر باره هماهنگ سازی سیستم

سیستم های توزیع شده فاقد هسته مرکزی جهت هماهنگ سازی سیستم هستند و هماهنگ سازی باید توسط اعضای خود سیستم صورت گیرد. هماهنگ سازی در این سیستم ها پیچیده بوده و بخشی از قدرت محاسباتی سیستم را نیز به خود تخصیص می دهد. قدرت محاسباتی که می توانست صرف عملکردها و خدمات اصلی سیستم شود.

سرباره ارتباطات

هماهنگ‌سازی مستلزم ارتباط اجزاست. بنابراین کامپیوترهای یک شبکه توزیع شده باید با هم ارتباط داشته باشند. این امر نیازمند یک پروتکل ارتباطی برای ارسال، دریافت و پردازش پیام‌هاست که بخشی از قدرت محاسباتی کامپیوترها را مصرف خود می‌کند.

وابستگی به شبکه

هر نوع ارتباطی نیازمند بستر ارتباطی است که اطلاعات را بین طرفین منتقل کند. کامپیوترهای یک سیستم غیر متمرکز نیازمند شبکه‌ای هستند که زیرساخت ارتباطی آنها را فراهم کند. شبکه ارتباطی مسائل و مشکلات خود را به همراه دارد که بر ارتباط و هماهنگی اجزای سیستم اثر می‌گذارد. با این وجود بدون بستر ارتباطی بین اجزای سیستم، اساساً سیستم غیر متمرکز معنایی ندارد و چنان سیستمی به شبکه ارتباطی وابسته است.

پیچیدگی نرم‌افزاری بیشتر

با توجه به محدودیت‌هایی که ذکر شد، نرم‌افزار به کار گرفته شده در سیستم غیر متمرکز باید بر مسائل مرتبط با هماهنگی، ارتباط و شبکه ارتباطی فائق شود. این امر پیچیدگی نرم‌افزارها در فضای سیستم‌های غیر متمرکز را بیشتر می‌کند.

مسائل امنیتی

ارتباط بین اجزای یعنی ارسال و به اشتراک‌گذاری اطلاعاتی که دارای اهمیت محاسباتی و کارکردی هستند. با این وجود ارسال اطلاعات در شبکه مسائل امنیتی خاص خود را به همراه دارد و ممکن است اطلاعات حیاتی به دست افراد غیر مجازی بیفتد که به شبکه دسترسی پیدا کرده‌اند. مدیریت این مسائل امنیتی در یک سیستم غیر متمرکز از سیستم متمرکز پیچیده‌تر است.

سیستم‌های همتابه‌همتای توزیع شده

سیستم‌های همتابه‌همتا (Peer-to-Peer) نوع خاصی از سیستم‌های توزیع شده هستند. این سیستم‌ها متشکل از تعدادی کامپیوتر مستقل هستند (گره (Node) خوانده می‌شوند)

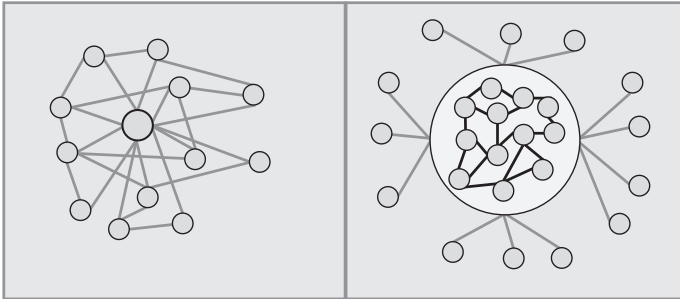
که قدرت محاسبه، ذخیره اطلاعات، یا پهنای باندشان را به طور مستقیم و بدون دخالت یک هسته مرکزی هماهنگ کننده در اختیار سایر اجزای شبکه قرار می دهند. گره های شبکه از نظر نقش و رتبه برابر هستند و همگی همزمان فراهم کننده و مصرف کننده منابع به شمار می روند.

سیستم های همتابه همتا کاربردهای جالبی همچون اشتراک گذاری فایل، انتشار محتوا و امنیت اطلاعات دارند. اغلب این کاربردها بر مبنای یک ایده ساده، اما قدرتمند قرار دارند؛ تبدیل قابلیت محاسباتی کامپیوترهای کاربران به گره های شبکه غیر متمرکز که به شکل گیری کل شبکه کمک می کنند. به این ترتیب هر چه تعداد کاربران بیشتر شود، قابلیت محاسباتی شبکه هم افزایش می یابد. این ایده، نتایج آن و چالش های پیش روی آن در گام های بعدی مورد بحث قرار خواهد گرفت.

سیستم های مرکب متمرکز و توزیع شده

هر کدام از دو نوع معماری متمرکز و توزیع شده که از لحاظ فنی در تقابل با هم هستند، مزایای خاص خود را دارند. این وضعیت الهام بخش مهندسانی بوده که با ترکیب دو نوع معماری ساختارهای جدیدی با اثرث بری خصوصیات خوب معماری متمرکز و توزیع شده ایجاد کرده اند. آشنایی با این ساختارهای ترکیبی در درک بهتر بلاکچین مفید خواهد بود؛ ساختارهایی که نوعی مرکزگرایی را بر سیستم های توزیع شده اعمال می کنند و ساختارهایی که نوعی توزیع شدگی را در سیستم های متمرکز شکل می دهند.

طرح گرافیکی سمت چپ در شکل ۲-۲ یک ساختار توزیع شده اما حاوی بخشی متمرکز را نشان می دهد. در نگاه اول به نظر می رسد اجزای سیستم یک در یک معماری توزیع شده قرار گرفته اند، اما همه دایره ها با دایره بزرگ تر مرکزی در اتصال هستند. طرح سمت راست شکل ۲-۲ رهیافت متفاوتی را نشان می دهد. در وهله اول این ساختار متمرکز به نظر می رسد، چرا که همه دایره های بخش بیرونی با دایره بزرگ تر مرکزی اتصال دارند، اما دایره مرکزی بزرگ خود در برگیرنده یک ساختار غیر متمرکز است.



شکل ۲-۲: ترکیب ساختارهای متمرکز و توزیع شده

از نقاط مشترک این دو طرح پیچیدگی تبیین آنهاست! این ساختارها توزیع شده هستند یا متمرکز؟ ضرورتی ندارد آنها را به گروه خاصی تعلق دهیم، اما لازم است به ماهیت دوگانه آنها آگاه باشیم. اهمیت این امر زمانی که به تجاری سازی بلاکچین می پردازیم، روشن تر خواهد شد.

شناسایی ساختارهای توزیع شده

ارائه یک تعریف روشن و مقبول عام از ساختارهای توزیع شده از حوصله این کتاب خارج است. در حد این کتاب لازم است تصویری کلی از ماهیت ساختار توزیع شده و تفاوت آن با سایر ساختارها در ذهن داشته باشیم. یک قاعده ساده که می تواند به طور نسبی در تشخیص ساختار توزیع شده یاری رسان باشد، به این ترتیب است: کل ساختار را بررسی کنید، اگر یک جزء خاص (برای نمونه بانک اطلاعاتی، یک جزء کاربری خاص یا یک سوییچ شرایط اضطراری) بتواند فعالیت تمام سیستم را متوقف کند، آن ساختار توزیع شده نیست.

نکته: اگر یک جزء ساختار، برای نمونه یک کلید خاموش کردن، بتواند تمام سیستم را از کار بیندازد، آن ساختار توزیع شده نیست.

هدف بلاکچین

تصمیم گیری درباره معماری سیستم در زمان طراحی یک نرم افزار، همچون انتخاب

موتور خودرو است. انتخاب معماری می تواند مستقل از جنبه های عملکردی لایه کاربرد صورت پذیرد. بنابراین می توان برای هدف عملکردی یکسان در لایه کاربرد از معماری های توزیع شده یا متمرکز استفاده کرد. یک سیستم پرداخت هم می تواند در قالب توزیع شده یا متمرکز پیاده سازی شود.

هر کدام از معماری ها، مزایا و محدودیت های خاص خود را داشته و به روش متفاوتی عمل می کنند. انتخاب یک معماری خاص در نحوه انجام جنبه های عملکردی و غیرعملکردی سیستم تاثیر خواهد داشت. به طور خاص، هر معماری شیوه متفاوتی برای حصول صحت کارکرد (Integrity) دارد. بلاکچین ابزاری است برای حصول صحت کارکرد در قالب معماری توزیع شده.

نکته: هدف بلاکچین حصول و حفظ صحت کارکرد در یک سیستم توزیع شده است.

چشم انداز

حصول صحت کارکرد در یک ساختار توزیع شده امری است بسیار فنی و ممکن است برای بسیاری جذاب نباشد، اما کارکردهای ساختارهای توزیع شده و قابلیت جایگزینی آنها با ساختارهای متمرکز برای بسیاری جالب توجه است. بخش بعدی به تاثیر سیستم های همتابه همتا در دنیای ما و نقش بلاکچین در حصول صحت کارکرد در سیستم های توزیع شده و تغییر دنیای می پردازد.

خلاصه

- معماری یک سیستم نرم افزاری چگونگی ساماندهی و ارتباطات بین اجزای آن را تعیین می کند.
- معماری های نرم افزاری متمرکز و توزیع شده دو نوع اصلی و متقابل معماری هستند.
- یک سیستم توزیع شده متشکل از کامپیوترهای مستقلی است که با همکاری یکدیگر و به واسطه ارتباطات از طریق یک بستر ارتباطی، بدون دارا بودن هیچ جزء مرکزی هماهنگ یا مدیریت کننده به انجام هدف می پردازد.
- به عنوان یک قاعده ساده، در صورتی که بتوان کارکرد یک سیستم را از طریق یک

جزء خاص متوقف کرد، آن سیستم توزیع شده نیست؛ فارغ از اینکه معماری آن، چه مقدار پیچیده به نظر برسد.

- بلاکچین بخشی از لایه پیاده‌سازی سیستم نرم‌افزاری توزیع شده است.
- هدف بلاکچین تامین یک جنبه غیر عملکردی سیستم‌های نرم‌افزاری توزیع شده است، یعنی: حصول و حفظ صحت کارکرد.

گام سوم

شناخت قابلیت‌ها

سیستم‌های همتابه‌همتا چگونه می‌توانند دنیا را تغییر دهند؟

این گام فهم ما از هدف بلاکچین را با نظر داشت نوع خاصی از شبکه‌های توزیع شده، یعنی سیستم‌های همتابه‌همتا، عمیق‌تر می‌کند. در نتیجه با چرایی جذابیت بلاکچین برای متخصصان فناوری و تجارت بیشتر آگاه می‌شویم. گام حاضر همچنین به زمینه‌های اصلی که بلاکچین می‌تواند در آنها مایه تغییرات شود و نیز مواردی از کاربرد سیستم‌های همتابه‌همتا در دنیای واقعی اشاره می‌کند.

یک مثال استعاری

آخرین باری را که یک سی دی موزیک خریده‌اید، به خاطر می‌آورید؟ اغلب افراد مدت طولانی است که چنین کاری انجام نداده‌اند، زیرا صنعت موسیقی طی سال‌های اخیر تغییرات چشم‌گیری داشته است. امروزه بیشتر مردم موزیک‌ها را به طرق مختلف از جمله دانلود هر موزیک از پایگاه‌های عرضه موسیقی یا دریافت از طریق نرم‌افزارهای استریم موزیک دریافت می‌کنند و آنها را با دوستان‌شان به اشتراک می‌گذارند. این جریان با ظهور نرم‌افزاری آغاز شد که به افراد اجازه می‌داد فایل‌های موزیک را با یکدیگر به اشتراک بگذارند، اما چه چیزی درباره این نرم‌افزار جالب توجه بود؟ به این جمله از زبان یکی از طراحان آن دقت کنید:

«درباره این سیستم، جذاب‌ترین چیزی که وجود دارد این است که با گره‌ها تعامل می‌کنید، اطلاعات را با فردی در همین خیابان رد و بدل می‌کنید.»

شاوون فنینگ (Shawn Fanning)، هم‌بنیان‌گذار نپستر (Napster)

آنچه فنینگ و همکارانش اختراع کردند یک سیستم همتا به همتا برای به اشتراک‌گذاری موسیقی بود. این نرم‌افزار در زمان عرضه خود در سال‌های پایانی دهه ۹۰، طلوع عصر جدیدی بود برای مدل کسب و کاری جدید در عرصه صنعت موسیقی. گام حاضر به این موضوع می‌پردازد که برآمدن نپستر (Napster)، آغاز دوران کاهش فروش سی‌دی‌ها و تغییرات مهم در عرصه موسیقی چه تاثیری بر بلاکچین گذاشتند.

چگونه یک سیستم همتا به همتا کلیت یک صنعت را تغییر می‌دهد؟

روند کار در صنعت موسیقی برای مدت طولانی به این شیوه بود؛ هنرمندان موسیقی قراردادهایی با استودیوها می‌بستند، استودیوها موسیقی را ضبط کرده، آن را روی بسترهای مختلف (صفحات وینیل، سی‌دی، نوار کاست و...) و از طریق روش‌های مختلف فروشگاهی به مشتریان عرضه می‌کردند. استودیوها در واقع به عنوان عامل واسطی میان هنرمندان و مردم علاقه‌مند به شنیدن موسیقی عمل می‌کردند. این

بنگاه‌ها با تکیه بر توانایی و دانش خود در تولید، بازاریابی و عرضه موسیقی، جایگاه خود را حفظ می‌کردند، اما در دهه اول قرن ۲۱، محیط کسب و کار استودیوهای موسیقی دچار تغییرات اساسی شد.

دیجیتالی شدن موسیقی، در دسترس قرار گرفتن تجهیزات ضبط با هزینه مناسب، گسترش استفاده از کامپیوترهای شخصی و اینترنت باعث کاهش ضرورت وجود استودیوهای موسیقی شد. سه کارکرد اصلی استودیوهای موسیقی (یعنی تولید، بازاریابی و عرضه) حالا توسط خود هنرمندان و مردم قابل انجام بود. نیستر نقشی اساسی در جایگزینی نقش واسط استودیوهای موسیقی داشت. با وجود این پلتفرم، مردم دیگر برای دسترسی به آخرین موسیقی‌ها نیازی به استودیوها نداشتند. نیستر امکان اشتراک‌گذاری هر فایل موسیقی با تمام مردم جهان را بدون نیاز به سی‌دی و با تکیه بر شبکه اینترنت فراهم آورد. رهیافت همتابه‌همتا نیستر به مساله و ایجاد یک بازار برای فایل‌های mp3، طیف گسترده‌تری از موسیقی‌ها را به راحتی در اختیار علاقه‌مندان قرار داد و به عدم ضرورت وجود استودیوهای موسیقی و ضررهای فراوان برای این صنعت منجر شد.

قابلیت‌های بالقوه سیستم‌های همتابه‌همتا

ماجرای نیستر به ما آموخت که سیستم‌های همتابه‌همتا قابلیت ایجاد بازاریابی ساختاری اساسی در یک صنعت را بر اساس یک ایده ساده دارا هستند؛ جایگزین کردن واسط با نیستر همتابه‌همتا. در مورد صنعت موسیقی، استودیوهای سنتی که در روش‌های بازاریابی و توزیع خود، نقش واسط را میان هنرمندان و مشتریان ایفا می‌کردند، توسط شبکه همتابه‌همتا جایگزین شدند. ویژگی عمده‌ای که باعث آسیب‌پذیری صنعت مبتنی بر استودیوهای موسیقی در مقابل شبکه همتابه‌همتا شد، ویژگی غیرمادی و هزینه اندک تکثیر و انتقال اطلاعات بود.

قدرت سیستم‌های همتابه‌همتا به صنعت موسیقی محدود نمی‌شود. هر صنعتی که به‌طور عمده به‌عنوان یک واسطه بین تولیدکنندگان و مشتریان کالاها و خدمات غیرمادی یا دیجیتال عمل می‌کند، در معرض خطر جایگزینی توسط سیستم‌های

همتابه‌همتااست. بزرگ‌ترین سیستم واسط از این قبیل صنعت مالی و پرداخت است. چه چیزی در حساب بانکی یا کارت اعتباری خود دارید؟ آیا آنچه دارید واقعا پول است؟ مدت‌هاست که موجودی شما در حساب‌های بانکی به رشته‌هایی از بیت‌ها و بایت‌ها بدل شده است. تنها مقدار اندکی از پول واقعی در قالب سکه و اسکناس وجود دارد. بخش اعظم پول و دارایی جهان در قالب بیت‌ها و بایت‌ها در سیستم‌های متمرکز نهادهای مالی قرار دارد. بانک‌ها و بسیاری از بازیگران دیگر صنعت مالی و پرداخت، فقط در نقش واسط بین تولیدکنندگان و مصرف‌کنندگان بیت‌ها و بایت‌هایی که پول و ثروت ما را تشکیل می‌دهند، عمل می‌کنند. اعمال قرض گرفتن، قرض دادن یا انتقال پول از یک حساب به یک حساب دیگر، صرفا انتقال چیزهایی غیرمادی توسط واسط‌هاست. تعداد واسط‌هایی که ممکن است در یک تراکنش ساده درگیر باشند، شگفت‌آور است. (برای نمونه، انتقال پول از یک حساب بانکی به یک حساب بانکی در کشوری دیگر ممکن است تا پنج واسط را درگیر خود کند که هر کدام نیازمند زمانی برای انجام عملیات مربوط به خود و خواهان هزینه خدمت هستند.) در نتیجه، عملیات ساده‌ای همچون یک انتقال مالی بین دو حساب بانکی در دو کشور مختلف مستلزم صرف زمان و هزینه بالای انجام تراکنش است. در یک سیستم همتابه‌همتا، عملیات انتقال مشابه می‌تواند بسیار ساده‌تر و در قالب انتقال مستقیم بیت‌ها و بایت‌ها میان دو گره از سیستم صورت گیرد.

مزیت سیستم‌های همتابه‌همتا نسبت به سیستم‌های متمرکز این است که تعامل به صورت مستقیم میان اجزای ذی‌ربط صورت پذیرفته و اجزای واسط دیگری در آن درگیر نمی‌شوند. این امر افزایش سرعت و کاهش هزینه عملیات را به دنبال دارد. مزیت‌های استفاده از سیستم‌های همتابه‌همتا به انتقال پول محدود نمی‌شود. هر صنعتی که به طور عمده به عنوان یک واسطه بین تولیدکنندگان و مشتریان کالاها و خدمات غیرمادی یا دیجیتال عمل می‌کند، در معرض جایگزینی توسط سیستم‌های همتابه‌همتااست. با ادامه روند دیجیتالی شدن امور، موارد بیشتر و بیشتری در زندگی روزمره در قالب خدمات و کالا‌های دیجیتالی و غیرمادی عرضه شده و در نتیجه

می‌توان از امکانات سیستم‌های همتابه‌همتا در مورد آنها بهره‌مند شد. طرفداران سیستم‌های همتابه‌همتا ادعا می‌کنند که تقریباً تمامی جنبه‌های زندگی ما با گسترش سیستم‌های دیجیتالی و همتابه‌همتا دستخوش تحول خواهد شد؛ مواردی از جمله پرداخت، پس‌انداز پول، قرض و وام، بیمه و همچنین صدور و اعتبارسنجی گواهی تولد، گواهینامه رانندگی، گذرنامه، کارت شناسایی، مدرک تحصیلی، گواهی ثبت اختراع و قراردادهای کاری. بسیاری از این موارد در حال حاضر در قالب خدمات دیجیتالی توسط سازمان‌ها و سیستم‌های متمرکز ارائه می‌شود که نقش واسط میان تامین‌کنندگان و مصرف‌کنندگان را ایفا می‌کنند.

نکته: جایگزینی واسطه میانی، حذف واسطه (Disintermediation) هم خوانده می‌شود. این امر تهدیدی جدی برای کسب‌وکارهایی به‌شمار می‌رود که نقش واسطه میان گروه‌های مختلفی از افراد، همچون فروشنده و خریدار، وام‌دهنده و وام‌گیرنده یا تولیدکننده و مصرف‌کننده را ایفا می‌کنند.

اصطلاح‌شناسی و ارتباط با بلاکچین

حالا بعد از آگاهی به قابلیت‌های سیستم‌های همتابه‌همتا، به روشن‌ساختن اصطلاحات و شرح مسأله و ارتباط آن با بلاکچین می‌پردازیم. به‌طور خاص، موارد زیر باید مورد بحث قرار گیرند:

- تعریف یک سیستم همتابه‌همتا؛
- معماری سیستم‌های همتابه‌همتا؛
- ارتباط بین سیستم‌های همتابه‌همتا و بلاکچین.

تعریف یک سیستم همتابه‌همتا

سیستم‌های همتابه‌همتا ساختارهای نرم‌افزاری توزیع‌شده‌ای متشکل از گره‌ها (کامپیوترهای مستقل) هستند که هر گره منابع محاسباتی خود (مانند قدرت پردازش، حافظه و انتقال اطلاعات) را به‌طور مستقیم در اختیار سایر بخش‌های سیستم قرار می‌دهد. هر کاربر با اتصال به یک سیستم همتابه‌همتا، کامپیوترش را به گرهی از شبکه

با امکانات و وظایف برابر با سایرین بدل می‌کند. اگرچه کاربران مختلف از جنبه منابع و میزان مشارکت متفاوت هستند، اما هر گره از نظر نوع عملکرد و مسئولیت با بقیه یکسان است. بنابراین کامپیوتر هر کاربر همزمان در نقش فراهم‌کننده و مصرف‌کننده منابع ظاهر می‌شود. برای مثال، در یک سیستم به اشتراک‌گذاری فایل هم‌تابه‌همتا، فایل‌ها در دستگاه‌های کاربران ذخیره می‌شود. وقتی فردی بخواهد فایلی را از این سیستم دانلود کند، عملیات دانلود در قالب انتقال از حافظه یکی دیگر از گره‌های شبکه صورت می‌گیرد؛ گره دیگری که می‌تواند در خانه همسایه بغلی باشد یا آن سوی کره زمین.

معماری سیستم‌های هم‌تابه‌همتا

سیستم‌های هم‌تابه‌همتا از دیدگاه ساختاری، توزیع شده هستند. با این وجود، سیستم‌های هم‌تابه‌همتایی با جنبه‌های متمرکز هم وجود دارند. چنین انواعی از سیستم‌های هم‌تابه‌همتا دارای یک گره مرکزی هستند که برقراری ارتباط میان سایر گره‌ها، نگهداری لیستی از خدمات قابل ارائه توسط هر گره یا جست‌وجو، جابجایی و تایید گره‌های دیگر سیستم را بر عهده دارند. چنین معماری ترکیبی از مزایای هر دو نوع معماری متمرکز و توزیع شده بهره می‌برد. معماری این سیستم‌ها ترکیبی است از ساختارهای متمرکز و توزیع شده، مشابه آنچه که در سمت چپ تصویر ۲-۲ نشان داده شد. از سوی دیگر سیستم‌های هم‌تابه‌همتای خالص حاوی هیچ گره مرکزی هماهنگ‌کننده یا کنترل‌کننده‌ای نیستند. از این رو، تمام گره‌ها در این سیستم‌ها به انجام وظایف یکسانی مشغول هستند؛ تامین و مصرف منابع و خدمات. نپستر نمونه‌ای است از یک سیستم هم‌تابه‌همتای دارای هسته مرکزی؛ هسته‌ای که بانک اطلاعاتی در همه گره‌های متصل و آهنگ‌های قابل دسترس از هر گره را نگهداری می‌کند.

ارتباط بین سیستم‌های هم‌تابه‌همتا و بلاکچین

همان‌طور که در گام ۲ مطرح شد، بلاکچین را می‌توان ابزاری برای حصول و حفظ

یکپارچگی و صحت کارکرد در سیستم‌های توزیع شده به‌شمار آورد. سیستم‌های همتابه‌همتای خالص می‌توانند از بلاکچین برای دستیابی و حفظ یکپارچگی و صحت کارکرد بهره‌مند شوند. از این رو، ارتباط بین سیستم‌های همتابه‌همتای توزیع شده و بلاکچین به استفاده آن سیستم‌ها برای دستیابی و حفظ صحت کارکرد بازمی‌گردد.

قابلیت‌های بلاکچین

رابطه بین سیستم‌های توزیع شده صرفاً همتابه‌همتا با بلاکچین این است که اولی از دومی به‌عنوان ابزاری برای رسیدن به صحت کارکرد و یکپارچگی و حفظ آن بهره‌می‌برد. از این رو، جنبه جذاب بلاکچین این است: کمک به شکل‌گیری شبکه‌های همتابه‌همتای کاملاً توزیع شده با قابلیت‌های تجاری فراوان برای جایگزینی سیستم‌های متمرکز و ایجاد تغییرات کلی و اساسی در صنایع مختلف از طریق حذف واسطه‌ها. از آنجا که این سیستم‌های توزیع شده همتابه‌همتا برای حفظ یکپارچگی و صحت کارکرد از بلاکچین بهره‌می‌برند، اهمیت اساسی این فناوری روشن می‌شود. حقیقتی که باعث جذابیت بلاکچین برای مردم می‌شود، قابلیت آن برای حذف واسطه‌هاست. در واقع بلاکچین راهکاری است برای نیل به این هدف. **نکته:** جذابیت هیجان‌انگیز بلاکچین از نقش ابزاری این فناوری در دستیابی و حفظ یکپارچگی و صحت کارکرد در سیستم‌های توزیع شده همتابه‌همتا ناشی می‌شود که می‌تواند به ایجاد تغییرات اساسی در زمینه‌های مختلف و حذف واسطه‌ها بینجامد.

چشم‌انداز

این گام به چپستی کلی سیستم‌های همتابه‌همتا و قابلیت آنها در ایجاد تغییرات اساسی در صنایع مختلف و حذف واسطه‌ها پرداخت. به‌علاوه اشاره شد که فناوری بلاکچین به عملی شدن چنان هدفی برای سیستم‌های همتابه‌همتا یاری می‌رساند. با این حال، این سوال که چرا دستیابی و حفظ یکپارچگی و صحت کارکرد در سیستم‌های توزیع شده حائز اهمیت فراوان است، هنوز پاسخ داده نشده و گام بعدی بیشتر به این موضوع می‌پردازد.

خلاصه

- سیستم‌های همتابه‌همتا متشکل از کامپیوترهایی هستند که منابع خود را مستقیماً در اختیار یکدیگر قرار می‌دهند.
- مزیت سیستم‌های همتابه‌همتا این است که به کاربران اجازه می‌دهند که مستقیماً با یکدیگر ارتباط داشته باشند؛ بدون نیاز به واسطی که عملاً ارتباط را به صورت غیرمستقیم برقرار می‌سازد.
- جایگزینی سیستم‌های متمرکز مبتنی بر واسط با سیستم‌های همتابه‌همتا، سرعت انجام عملیات را افزایش و هزینه آن را کاهش می‌دهد.
- سیستم‌های همتابه‌همتا می‌توانند دارای جزء متمرکز بوده یا کاملاً توزیع شده باشند.
- سیستم‌های همتابه‌همتای کاملاً توزیع شده در قالب شبکه‌ای از اعضا ساماندهی شده‌اند که در آن هر عضو به صورت مستقیم با بقیه در تماس بوده و هیچ گره هماهنگ‌کننده مرکزی در آنها وجود ندارد.
- نیستر قدرت شبکه‌های همتابه‌همتا را برای به اشتراک گذاری فایل‌ها نشان داده و با جایگزینی عملکرد کلاسیک استودیوهای موسیقی که نقش واسط میان هنرمندان و مشتریان را ایفا می‌کردند، عصر جدیدی را در صنعت موسیقی آغاز کرد.
- هر صنعتی که به‌طور عمده به‌عنوان یک واسطه بین تولیدکنندگان و مشتریان کالاها و خدمات غیرمادی یا دیجیتال عمل می‌کند، در معرض جایگزینی توسط سیستم‌های همتابه‌همتا است.
- بخش عظیمی از سیستم مالی و پرداخت دنیا به عملکرد واسط میان‌تامین‌کنندگان و مصرف‌کنندگان پول در قالب کالایی دیجیتال و غیرمادی می‌پردازد. از این رو، با گسترش ساختارهای دیجیتال و همتابه‌همتا، صنعت مالی و پرداخت می‌تواند همچون تأثیرپذیری صنعت موسیقی از نیستر دچار تحولات عظیم شود.
- با گسترش روند دیجیتالی شدن، جنبه‌های بیشتری از زندگی و کالاها و خدمات بیشتری به صورت غیرمادی درآمده و از قابلیت‌ها و مزایای شبکه‌های همتابه‌همتا

بهره‌مند می‌شوند.

- جذابیت بلاکچین از نقش این فناوری به‌عنوان ابزاری برای حصول و حفظ یکپارچگی و صحت کارکرد سیستم‌های توزیع‌شده همتابه‌همتا در جهت ایجاد تغییرات اساسی در صنایع مختلف و حذف واسطه‌ها نشأت می‌گیرد.