
بسم الله
الرحمن
الرحيم

سرشناسه : درشر، دنیل.Daniel Dresher
عنوان و نام پدیدآور : مبانی بلاکچین؛ مقدمه‌ای غیرفنی در ۲۵ گام
نویسنده : دنیل درشر
مترجم: سیاوش تفضلی
مشخصات نشر : راه پرداخت
مشخصات ظاهری : ۲۸۸
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۲۷-۹
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: Blockchain Basics: A Non-Technical Introduction in 25 Steps
موضوع : رمزگذاری داده‌ها
موضوع: بلاکچین
شناسه افزوده : تفضلی، سیاوش، ۱۳٦٤
رده بندی کنگره: الف ۱۷۱۰HG/ د٤ م۲ ۱۳۹۷
رده بندی دیویی : ۳۳۲/۱۷۸۰۲۸

مقدمه‌ای غیرفنی در ۲۵ گام

مبانی بلاکچین

دنیل درشر

سیاوش تفضلی

۱

عنوان : مبانی بلاکچین؛ مقدمه‌ای غیرفنی در ۲۵ گام
ناشر : راه‌پرداخت
نویسنده: دنیل درشر
مترجم: سیاوش تفضلی
ویراستار ارشد : مینا والی
ویراستار محتوایی : قاسم سرافرازی
ویراستار فنی: یلدا شایسته‌فر
بازبینی نهایی متن: رضا قربانی
صفحه‌آرا : علیرضا کیوان
ناظر چاپ : قادر شهبازی
نوبت چاپ: اول ۱۴۰۱
شمارگان : ۱۰۰۰ نسخه
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۲۷-۹
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

@Way2Paypress Way2Pay.press @Way2Paypress

فهرست

بخش یک

اصطلاحات و مبانی فنی ۱۷

گام اول: تفکر در لایه‌ها و جوانب ۱۸

یک مثال استعاری ۱۹

لایه‌ها و جنبه‌های یک سیستم نرم‌افزاری ۱۹

کاربرد در مقابل پیاده‌سازی ۱۹

جنبه‌های عملکردی در مقابل غیرعملکردی ۲۰

لایه‌ها و جنبه‌های مختلف در یک نما ۲۰

صحت کارکرد ۲۱

خلاصه ۲۱

گام دوم: نظری به نمای کلی ۲۳

یک مثال استعاری ۲۴

لایه‌ها و جنبه‌های یک سیستم پرداخت ۲۴

دو نوع معماری کامپیوتر ۲۵

مزایای سیستم توزیع‌شده ۲۶

قدرت محاسباتی بالاتر ۲۶

کاهش هزینه ۲۶

قابلیت اتکای بالاتر ۲۶

قابلیت رشد و مقیاس‌پذیری پیوسته ۲۷

معایب سیستم توزیع‌شده ۲۷

سرباره هماهنگ‌سازی سیستم ۲۷

سرباره ارتباطات ۲۸

وابستگی به شبکه ۲۸

پیچیدگی نرم‌افزاری بیشتر ۲۸

مسائل امنیتی ۲۸

سیستم‌های همتا به همتای توزیع‌شده ۲۸

سیستم‌های مرکب متمرکز و توزیع‌شده ۲۹
شناسایی ساختارهای توزیع‌شده ۳۰
هدف بلاکچین ۳۱
چشم‌انداز ۳۱
خلاصه ۳۱
گام سوم: شناخت قابلیت‌ها ۳۳
یک مثال استعاری ۳۴
چگونه یک سیستم همتابه‌همتا کلیت یک صنعت را تغییر می‌دهد؟ ۳۴
قابلیت‌های بالقوه سیستم‌های همتابه‌همتا ۳۵
اصطلاح‌شناسی و ارتباط با بلاکچین ۳۷
تعریف یک سیستم همتابه‌همتا ۳۷
معماری سیستم‌های همتابه‌همتا ۳۸
ارتباط بین سیستم‌های همتابه‌همتا و بلاکچین ۳۸
قابلیت‌های بلاکچین ۳۹
چشم‌انداز ۳۹
خلاصه ۳۹

بخش دو

چرا بلاکچین مورد نیاز است؟ ۴۱
گام چهارم: فهم مساله اصلی ۴۲
یک مثال استعاری ۴۳
اعتماد و صحت کارکرد در سیستم‌های همتابه‌همتا ۴۳
تهدیدهای صحت کارکرد در سیستم‌های همتابه‌همتا ۴۴
اشکالات فنی ۴۴
گره‌های مخرب ۴۴
مشکل اصلی که باید توسط بلاکچین حل شود ۴۵
چشم‌انداز ۴۵
خلاصه ۴۶
گام پنجم: شفاف‌سازی معنی ۴۷
اصطلاح بلاکچین ۴۸
یک ساختمان داده ۴۸
یک الگوریتم ۴۹
مجموعه‌ای از فناوری‌ها ۴۹
اصطلاحی فراگیر برای شبکه‌های همتابه‌همتای کاملا توزیع‌شده ۴۹
کاربرد این اصطلاح در کتاب حاضر ۴۹

یک تعریف موقتی ۵۰
نقش مدیریت مالکیت ۵۰
زمینه کاربردی بلاکچین در این کتاب ۵۱
چشم‌انداز ۵۱
خلاصه ۵۲
گام ششم: درک مفهوم مالکیت ۵۳
یک مثال استعاری ۵۴
مالکیت و شاهدها ۵۴
مبانی مالکیت ۵۵
گریز کوتاهی به امنیت ۵۷
شناسایی ۵۷
احراز هویت ۵۷
احراز صلاحیت ۵۸
کارکردها و ویژگی‌های یک دفترکل ۵۸
مالکیت و بلاکچین ۶۰
چشم‌انداز ۶۱
خلاصه ۶۱
گام هفتم: خرج دوباره پول ۶۳
یک مثال استعاری ۶۴
مشکل خرج دوباره ۶۴
شرح اصطلاح ۶۵
خرج دوباره به‌عنوان مشکلی برآمده از تکثیر کالاهای دیجیتال ۶۵
خرج دوباره به‌عنوان مساله‌ای در شبکه‌های همتابه‌همتای کاملا توزیع‌شده ۶۶
خرج دوباره به‌عنوان نمونه‌ای از نقض صحت کارکرد در یک شبکه همتابه‌همتای ۶۶
راه غلبه بر مساله خرج دوباره ۶۶
غلبه بر خرج دوباره به‌عنوان مشکلی برآمده از تکثیر کالاهای دیجیتال ۶۶
غلبه بر خرج دوباره به‌عنوان مساله‌ای در شبکه‌های همتابه‌همتای کاملا توزیع‌شده ۶۷
غلبه بر خرج دوباره به‌عنوان نمونه‌ای از نقض صحت کارکرد در یک شبکه همتابه‌همتای ۶۷
استفاده از اصطلاح خرج دوباره در این کتاب ۶۸
چشم‌انداز ۶۸
خلاصه ۶۸

بخش سه
بلاکچین چگونه کار می‌کند ۶۹
گام هشتم: طرح کلی بلاکچین ۷۰

هدف ۷۱
نقطه شروع ۷۱
راه پیش رو ۷۱
نکته اول: توصیف مالکیت ۷۲
نکته دوم: حفاظت از مالکیت ۷۲
نکته سوم: ذخیره‌سازی داده‌های مربوط به تراکنش‌ها و معاملات ۷۳
نکته چهارم: آماده‌سازی دفاتر کل برای توزیع در محیطی خالی از اعتماد ۷۳
نکته پنجم: توزیع دفاتر کل ۷۴
نکته ششم: اضافه‌کردن معاملات جدید به دفاتر کل ۷۴
نکته هفتم: تصمیم‌گیری درباره اینکه کدام دفتر کل اعلان‌گر حقیقت است ۷۴
چشم‌انداز ۷۵
خلاصه ۷۶
گام نهم: ثبت مالکیت ۷۷
یک مثال استعاری ۷۸
هدف ۷۸
چالش پیش رو ۷۸
ایده ۷۸
گریزی بر اطلاعات معاملات و فهرست اموال ۷۹
چگونگی کارکرد ۷۹
توصیف انتقال مالکیت ۷۹
نگهداری تاریخچه نقل‌وانتقالات ۸۰
چرا این روش کارایی دارد ۸۱
اهمیت چیدمان ۸۱
یکپارچگی تاریخچه معاملات ۸۲
صحت صوری ۸۲
صحت معنایی ۸۲
احراز صلاحیت ۸۳
چشم‌انداز ۸۳
خلاصه ۸۳
گام دهم: هش‌کردن اطلاعات ۸۵
یک مثال استعاری ۸۶
هدف ۸۶
چگونگی کارکرد ۸۶
تولید سریع مقدار هش برای انواع داده‌ها ۸۷
معین بودن ۸۷

شبه‌تصادفی بودن ۸۷
یک‌طرفه بودن ۸۷
مقاومت در برابر همکوبی (Collision Resistant) ۸۸
خودتان امتحان کنید! ۸۸
الگوهای هش‌کردن اطلاعات ۹۰
هش‌کردن مستقل ۹۱
هش‌کردن مکرر ۹۱
هش‌کردن ترکیبی ۹۲
هش‌کردن متوالی ۹۳
هش‌کردن سلسله‌مراتبی ۹۴
چشم‌انداز ۹۵
خلاصه ۹۵
گام یازدهم: هش‌کردن در دنیای واقعی ۹۶
مقایسه داده‌ها ۹۷
هدف ۹۷
ایده ۹۷
چگونه کار می‌کند؟ ۹۷
چرا این روش کارآمد است؟ ۹۷
تشخیص تغییرات در داده‌ها ۹۷
هدف ۹۸
ایده ۹۸
چگونه کار می‌کند؟ ۹۸
چرا این روش کارآمد است؟ ۹۸
ارجاع به داده‌ها به روشی حساس به تغییر (Change-Sensitive) ۹۹
هدف ۹۹
ایده ۹۹
چگونه کار می‌کند؟ ۹۹
یک تصویر شماتیک ۱۰۰
چرا این روش کارآمد است؟ ۱۰۲
ذخیره داده‌ها به شیوه‌ای حساس به تغییر ۱۰۲
هدف ۱۰۲
ایده ۱۰۲
چگونه کار می‌کند؟ ۱۰۳
الگوی زنجیره‌ای ۱۰۳
الگوی درختی ۱۰۴

چرا این روش کارآمد است؟ ۱۰۴
ایجاد محاسبات زمانبر (time-consuming computations) ۱۰۵
هدف ۱۰۵
ایده ۱۰۵
چگونه کار می‌کند؟ ۱۰۶
یک مثال روشنگر ۱۰۷
سطح دشواری ۱۰۸
چرا این روش کارآمد است؟ ۱۰۸
استفاده از هش‌کردن در بلاکچین ۱۰۹
چشم‌انداز ۱۰۹
خلاصه ۱۰۹
گام دوازدهم: شناسایی و حفاظت از حساب‌های کاربری ۱۱۰
یک مثال استعاری ۱۱۱
هدف ۱۱۱
چالش ۱۱۱
ایده ۱۱۲
گریزی بر رمزنگاری ۱۱۲
ایده بنیادین رمزنگاری ۱۱۲
واژگان ۱۱۳
رمزنگاری متقارن ۱۱۳
رمزنگاری نامتقارن ۱۱۴
کاربرد رمزنگاری نامتقارن در عمل ۱۱۶
ایجاد و توزیع کلیدها ۱۱۶
استفاده از کلیدها ۱۱۷
عمومی به خصوصی ۱۱۷
خصوصی به عمومی ۱۱۷
رمزنگاری نامتقارن در بلاکچین ۱۱۸
شناسایی حساب‌ها ۱۱۸
اعطای مجوز معاملات ۱۱۸
چشم‌انداز ۱۱۹
خلاصه ۱۱۹
گام سیزدهم: اعطای مجوز معاملات ۱۲۱
یک مثال استعاری ۱۲۲
هدف ۱۲۲
چالش ۱۲۲

ایده ۱۲۲
گریزی بر امضای دیجیتالی ۱۲۳
ایجاد یک امضا ۱۲۳
صحت‌سنجی داده‌ها با استفاده از امضای دیجیتالی ۱۲٤
شناسایی تقلب با استفاده از امضای دیجیتالی ۱۲۵
این روش چگونه کار می‌کند؟ ۱۲٦
امضای یک معامله ۱۲٦
صحت‌سنجی یک معامله ۱۲۷
چرا این روش کارآمد است؟ ۱۲۷
چشم‌انداز ۱۲۸
خلاصه ۱۲۸
گام چهاردهم: ذخیره داده‌های معاملاتی ۱۲۹
یک مثال استعاری ۱۳۰
هدف ۱۳۰
چالش ۱۳۰
ایده ۱۳۱
تبدیل یک کتاب به ساختمان داده بلاکچین ۱۳۱
نقطه شروع: یک کتاب ۱۳۱
تغییر اول: ارتباط اختصاصی صفحات با هم ۱۳۲
تغییر دوم: برون‌سپاری محتوا ۱۳۳
تغییر سوم: جایگزینی شماره صفحه‌ها ۱۳٤
تغییر چهارم: ایجاد شماره ارجاع‌ها ۱۳۵
تغییر پنجم: رهایی از صحافی کتاب ۱۳٦
هدف حاصل شد، ارزیابی نتیجه ۱۳٦
ساختمان داده بلاکچین ۱۳۷
واحد ذهنی شامل صفحه‌ای از فهرست تواتر و صحفه محتوای مرتبط با آن ۱۳۹
فهرست تواتر ۱۳۹
صفحات محتوا ۱۳۹
شماره‌های مرجع فهرست تواتر ۱٤۰
شماره ارجاع محتوا ۱٤۰
ذخیره معاملات در ساختمان داده بلاکچین ۱٤۰
چشم‌انداز ۱٤۲
خلاصه ۱٤۲
گام پانزدهم: استفاده از انباره داده‌ها ۱٤۳
یک مثال استعاری ۱٤٤

اضافه کردن معاملات جدید ۱۴۴
تشخیص تغییرات ۱۴۶
تغییر محتوای داده‌های معاملاتی ۱۴۷
تغییر یک ارجاع هش در درخت مرکل ۱۴۷
جایگزینی یک معامله ۱۴۸
تغییر ریشه درخت مرکل ۱۴۹
تغییر ارجاع یک هدر بلوک ۱۵۰
ایجاد تغییر بدون اشکال در داده‌ها ۱۵۰
تغییرات پذیرفتنی و ناپذیرفتنی (Intended vs. Unintended Changes) ۱۵۱
چشم‌انداز ۱۵۲
خلاصه ۱۵۲
گام شانزدهم: محافظت از انباره داده‌ها ۱۵۴
یک مثال استعاری ۱۵۵
هدف ۱۵۶
چالش ۱۵۶
ایده ۱۵۶
گریزی بر تغییرناپذیری ۱۵۶
چگونه کار می‌کند: تصویر جامع ۱۵۷
آشکارسازی دستکاری‌ها ۱۵۷
لزوم بازنویسی کلی تاریخچه به‌منظور جازدن تغییرات جدید ۱۵۸
هزینه محاسباتی بالا برای اضافه‌کردن داده‌ها ۱۵۸
چگونه کار می‌کند: جزئیات ۱۵۸
داده‌های اجباری ۱۵۹
فرایند ایجاد بلوک جدید ۱۵۹
قواعد اعتبارسنجی ۱۶۰
چرا این روش کارآمد است؟ ۱۶۱
هزینه‌های دستکاری در ساختمان داده بلاکچین ۱۶۱
انباره داده تغییرناپذیر در دنیای واقعی ۱۶۲
چشم‌انداز ۱۶۲
خلاصه ۱۶۳
گام هفدهم: توزیع انباره داده بین گره‌ها ۱۶۴
یک مثال استعاری ۱۶۵
هدف ۱۶۵
چالش ۱۶۵
ایده ۱۶۶

چگونه کار می‌کند؛ مرور کلی ۱۶۶
چگونه کار می‌کند؛ جزئیات ۱۶۸
زنده نگه داشتن ارتباطات موجود ۱۶۸
ایجاد اتصالات جدید ۱۶۹
توزیع اطلاعات جدید ۱۶۹
چرا این روش کارآمد است؟ ۱۷۰
چشم‌انداز ۱۷۰
خلاصه ۱۷۱
گام هجدهم: تایید و افزودن معاملات ۱۷۳
یک مثال استعاری ۱۷۴
نتایج ۱۷۴
هدف ۱۷۵
چالش ۱۷۵
ایده ۱۷۶
چگونه کار می‌کند؛ بلوک‌های ساختمان ۱۷۶
قواعد اعتبارسنجی ۱۷۶
قواعد اعتبارسنجی برای داده‌های معاملاتی ۱۷۷
قواعد اعتبارسنجی برای هدر بلوک‌ها ۱۷۷
پاداش ۱۷۷
تنبیه ۱۷۸
رقابت ۱۷۸
رقابت بر سر سرعت ۱۷۹
رقابت بر سر کیفیت ۱۷۹
نظارت همتایان ۱۸۰
چگونه کار می‌کند؛ اسکلت ۱۸۰
چگونه کار می‌کند؛ جزئیات فرایند ۱۸۱
چرا این روش کارآمد است؟ ۱۸۲
برخورد با عملکرد نادرست ۱۸۳
چشم‌انداز ۱۸۴
خلاصه ۱۸۵
گام نوزدهم: انتخاب یک تاریخچه معاملاتی ۱۸۷
یک مثال استعاری ۱۸۸
هدف ۱۸۸
چالش ۱۸۸
ایده ۱۸۹

این روش چگونه کار می‌کند؟ ۱۹۱
معیار بلندترین زنجیره ۱۹۱
معیار سنگین‌ترین زنجیره ۱۹۶
پیامدهای انتخاب یک زنجیره ۱۹۷
بلوک‌های یتیم ۱۹۸
بازپس‌گیری پاداش ۱۹۸
شفاف‌سازی مالکیت ۱۹۸
بازپردازش معاملات ۱۹۹
یک تنه عمومی در حال رشد ۱۹۹
سازگاری نهایی ۲۰۰
استحکام در برابر دستکاری ۲۰۱
تهدیدهای مترتب بر ساختار رای‌گیری ۲۰۲
نقش معمای هش ۲۰۲
چرا این روش کارآمد است؟ ۲۰۳
چشم‌انداز ۲۰۳
خلاصه ۲۰۴
گام بیستم: پرداخت برای یکپارچگی ۲۰۷
یک مثال استعاری ۲۰۸
نقش کارمزدها در بلاکچین ۲۰۸
تاثیر بر یکپارچگی سیستم ۲۰۹
تاثیر بر باز بودن سیستم ۲۰۹
تاثیر بر فلسفه سیستم ۲۱۰
خصوصیات مطلوب برای ماهیت پاداش پرداختی به گره‌ها ۲۱۰
راهی به سوی ایجاد ارزهای رمزنگارانه ۲۱۱
چشم‌انداز ۲۱۲
خلاصه ۲۱۲
گام بیست‌ویکم: گردهم‌آوری قطعات مجزا ۲۱۳
بررسی مفاهیم و فناوری‌ها ۲۱۴
بلاکچین چیست؟ ۲۱۶
هدف بلاکچین: جنبه‌های عملکردی، لایه کاربرد ۲۱۶
شفاف‌سازی مالکیت ۲۱۶
انتقال مالکیت ۲۱۶
خصوصیات بلاکچین؛ جنبه‌های غیرعملکردی ۲۱۷
به‌شدت در دسترس ۲۱۷
مقاوم در برابر سانسور ۲۱۷

قابل اعتماد ۲۱۷
باز ۲۱۸
شبه‌ناشناس ۲۱۸
امن ۲۱۸
پایدار ۲۱۸
سازگاری نهایی ۲۱۸
حفظ یکپارچگی ۲۱۹
عملکرد داخلی: جنبه‌های عملکردی، لایه پیاده‌سازی ۲۱۹
منطق مالکیت ۲۱۹
امنیت معاملات ۲۲۰
منطق پردازش معاملات ۲۲۱
منطق ذخیره‌سازی ۲۲۲
معماری همتا به همتا ۲۲۳
منطق اجماع ۲۲٤
به دست آوردن تصویری انتزاعی ۲۲٤
چشم‌انداز ۲۲۵
خلاصه ۲۲٦

بخش چهار
محدودیت‌های بلاکچین و چگونگی غلبه بر آن‌ها ۲۲۹
گام بیست‌ودوم: مشاهده محدودیت‌ها ۲۳۰
چالش ۲۳۱
محدودیت‌های فنی بلاکچین ۲۳۱
فقدان حریم خصوصی ۲۳۱
مدل امنیتی ۲۳۲
مقیاس‌پذیری محدود ۲۳۳
هزینه‌های زیاد ۲۳۳
تمرکز پنهان ۲۳٤
عدم انعطاف‌پذیری ۲۳٤
اندازه بحرانی ۲۳۵
محدودیت‌های غیرفنی بلاکچین ۲۳۵
عدم پذیرش قانونی ۲۳٦
عدم پذیرش کاربران ۲۳٦
غلبه بر محدودیت‌ها ۲۳٦
محدودیت‌های فنی ۲۳۷

محدودیت‌های غیرفنی ۲۳۷
چشم‌انداز ۲۳۷
خلاصه ۲۳۸
گام بیست‌وسوم: نوآفرینی بلاکچین ۲۳۹
یک مثال استعاری ۲۴۰
تعارض میان اهداف بلاکچین ۲۴۰
شفافیت در مقابل حریم خصوصی ۲۴۰
امنیت در مقابل سرعت ۲۴۱
ریشه تعارض‌ها ۲۴۱
برطرف کردن تعارض‌ها ۲۴۲
انتخاب میان شفافیت و حریم خصوصی ۲۴۲
انتخاب میان امنیت و سرعت ۲۴۲
چهار نسخه بلاکچین ۲۴۳
نتایج ۲۴۴
معماری همتا به همتا ۲۴۴
ماهیت توزیع‌شده ۲۴۴
هدف ۲۴۵
مرور اهداف بلاکچین ۲۴۶
کاربرد اصطلاح بلاکچین در این کتاب ۲۴۶
چشم‌انداز ۲۴۷
خلاصه ۲۴۷

بخش پنج
استفاده از بلاکچین خلاصه و چشم‌انداز ۲۴۹
گام بیست‌وچهارم: استفاده از بلاکچین ۲۵۰
یک مثال استعاری ۲۵۱
ویژگی‌های بلاکچین ۲۵۱
الگوهای عمومی کاربرد بلاکچین ۲۵۲
اثبات وجود ۲۵۲
اثبات عدم وجود ۲۵۲
اثبات زمان ۲۵۲
اثبات ترتیب ۲۵۳
اثبات هویت ۲۵۳
اثبات تالیف ۲۵۳
اثبات مالکیت ۲۵۴

کاربردهای خاص ۲۵۴
تحلیل کاربردهای بلاکچین ۲۵۵
آیا ملزومات استفاده از بلاکچین فراهم آمده است؟ ۲۵۶
چه نوعی از بلاکچین مورد استفاده قرار گرفته است؟ ۲۵۷
ارزش افزوده استفاده از یک سیستم همتا به همتای کاملا توزیع شده چیست؟ ۲۵۷
ایده محوری خدمت ارائه شده چیست؟ ۲۵۸
چه مدل کسب و کاری به کار گرفته شده است؟ ۲۵۹
چگونه منافع گره‌ها برای مشارکت در فراهم کردن منابع سیستم تامین می‌شود؟ ۲۶۰
چشم‌انداز ۲۶۰
خلاصه ۲۶۱
گام بیست و پنجم: جمع‌بندی و افق پیش رو ۲۶۳
یک مثال استعاری ۲۶۴
مسیرهای مختلف توسعه پیش رو ۲۶۴
بهبودها و تغییرات جزئی فنی ۲۶۵
بهبود مقیاس‌پذیری ۲۶۵
تحولات مفهومی بنیادین ۲۶۶
حق دسترسی‌ها ۲۶۶
حریم خصوصی ۲۶۶
اجماع ۲۶۷
معاملات ۲۶۸
فهرست اموال ۲۶۹
ساختمان داده ۲۶۹
اهم دستاوردهای بلاکچین ۲۷۰
واسطه‌زدایی ۲۷۰
خودکارسازی ۲۷۱
استانداردسازی ۲۷۱
ساده‌سازی فرایندها ۲۷۱
افزایش سرعت عملیات ۲۷۱
کاهش هزینه ۲۷۲
حرکت به سوی اعتماد بیشتر به پروتکل‌ها و فناوری ۲۷۲
تبدیل اعتبار و اعتماد به یک دارایی ۲۷۲
افزایش آشنایی با فناوری ۲۷۳
عوارض ناخواسته احتمالی ۲۷۳
از بین رفتن حریم خصوصی ۲۷۴
از بین رفتن مسئولیت پاسخگویی ۲۷۴

نابودی مشاغل ۲۷۵
ایجاد واسطه‌گری مجدد ۲۷۵
آینده ۲۷۵
پروژه‌های محدود توسط علاقه‌مندان ۲۷۶
کاربردهای بزرگ‌مقیاس تجاری ۲۷۶
پروژه‌های دولتی ۲۷۶
چشم‌انداز ۲۷۷
خلاصه ۲۷۷

یادداشت مترجم

سیاوش تفضلی

از حدود دو سال و نیم گذشته که تب بلاکچین ناگهان همه‌گیر شد، بارها با پرسش‌های گوناگونی در رابطه با چیستی این فناوری مواجه شده‌ام. سوای این که برخی از این پرسش‌ها اساسا از حیطه 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 هستم 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 آماده سازی 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.

یادداشت ناشر

رضا قربانی / انتشارات راه پرداخت

بلاکچین بیش‌تر از این که یک فناوری بنیادین باشد یک فلسفه است. در سال‌های گذشته ما مراحل مختلفی از هایپ بلاکچین را پشت سر گذاشتیم. از این که بلاکچین قرار است همه مسائل ما از شیر مرغ گرفته تا جان آدمی‌زاد را مدیریت کند گذشته‌ایم. بالا و پایین‌ها را دیده‌ایم و حالا کمی واقع‌بین‌تر به ماجرا نگاه می‌کنیم. نه تصور حل همه مسائل را داریم و نه تصور می‌کنیم بلاکچین یک شو پوچ توخالی است. بلاکچین هم مانند همه دست‌ساخته‌های بشری راه خودش را پیدا کرده است و ما می‌توانیم برای افزایش کیفیت زندگی روی آن حساب کنیم. بلاکچین را نباید صرفا محدود به دنیای فناوری ببینیم. بلاکچین شیوه نوینی از نگاه کردن به مسائل را به ما آموزش می‌دهد. ما می‌توانیم با کمک بلاکچین مسائل همیشگی را به شیوه متفاوتی حل کنیم. مسئله اعتماد یکی از اساسی‌ترین مسائل تاریخ بشر است. نهادهای واسطه شکل گرفته‌اند که این مسئله را حل کنند و ما بتوانیم در کنار هم زندگی کنیم. درک بلاکچین که مدعی است می‌تواند جایگزین همه سیستم‌های اعتمادساز شود برای همه مردم لازم است. قاعدتا زبان فنی بلاکچین بسیاری را می‌راند و باعث می‌شود نتوانیم با اصل موضوع ارتباط برقرار کنیم. به همین دلیل آزمون شیوه‌های متفاوت برای بیان فلسفه بلاکچین لازم و ضروری است. کتاب «مبانی بلاکچین» در همین راستا منتشر می‌شود. این کتاب به زبانی غیرفنی مسائل فنی پشت بلاکچین را بیان می‌کند. درک این موضوعات به ما کمک می‌کند بتوانیم فناوری بنیادین بلاکچین را به شیوه درست و منطقی درک کنیم. امیدوارم این تلاش‌ها در توسعه دانش و سواد مالی مردم ایران فایده داشته باشد و این مطالب برای کسی مفید باشد و در زندگی به کارش بیاید.

بخش یک

اصطلاحات و مبانی فنی

این بخش با توضیح مفاهیم اساسی مهندسی نرم‌افزار، معماری کامپیوتر و موضوع صحت کارکرد، ارتباط کلی آنها با بلاکچین را مطرح کرده و پایه‌ای استاندارد برای صحبت درباره فناوری فراهم می‌سازد. با مطالعه این بخش به برداشتی کلی از هدف بلاکچین و پتانسیل آن نائل می‌شوید.

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

شـما احتمالا تلفن همراه دارید! چقدر دربـاره پروتکل‌های مختلف بی‌سـیم یا امواج الکترومغناطیسی که اساس ارتباطات بی‌سیم موبایلی هستند، می‌دانید؟ اغلب افراد در رابطه با این موارد دانش زیادی ندارند؛ چراکه اطلاع درباره موارد ذکرشـده برای استفاده روزمره و عـادی از موبایل ضرورتی ندارد. مـا به‌صورت ذهنی فناوری تلفن همـراه 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 اشـکال کند؛ بنابراین یکسان‌سـازی 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 سیسـتم به لایه‌بندی کاربرد در مقابل پیاده‌سـازی منجر می‌شـود. مواردی مانند گرفتن عکس، گوش دادن به موزیک یا مرور صفحات وب، در لایه کاربرد قرار می‌گیرند، لایه پیاده‌سـازی بر «عملی‌کردن» 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 غیرعملکردی

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 به‌صورت امن، جنبه‌های غیرعملکردی موبایل به‌شمار می‌روند. یکی از جنبه‌های غیرعملکردی سیستم صحت کارکرد (integrity) است. به این معنا که سیستم به همان ترتیبی که انتظار می‌رود، به‌درستی عمل کند. یک راه سریع برای تشخیص جنبه‌های عملکردی و غیرعملکردی رجوع به گرامر زبانی است؛ مواردی که به‌صورت فعل ذکر می‌شوند به جنبه‌های عملکردی اشاره دارند و مواردی که به صورت قید ذکر می‌شوند، ناظر بر جنبه‌های غیرعملکردی هستند. برای نمونه «راه‌رفتن» به‌عنوان یک فعل به جنبه‌ای عملکردی اشاره دارد، در حالی که فرد می‌تواند همین عمل را با کیفیت‌های مختلف «به‌آهستگی» و «به‌سرعت» انجام دهد.

لایه‌ها و جنبه‌های مختف در یک نما

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

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

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

جنبه‌های عملکردی لایه کاربرد، روشن‌ترین بخش‌های یک سیستم هستند. از سوی دیگر، جنبه‌های غیرعملکردی لایه پیاده‌سازی، عموما خیلی به چشم نمی‌آیند و وجود آنها به‌عنوان 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 صرفا برای کاربران مجاز فراهم کند.

اغلب ما ممکن است صحت کارکرد یک سیستم را امری مفروض و بدیهی به‌شمار بیاوریم؛ چراکه عموما 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. پیش‌فرض بدیهی‌بودن صحت کارکرد زمانی به چالش کشیده می‌شود که با نرم‌افزاری دارای اشکال مواجه شویم. از دست رفتن یا لو رفتن اطلاعات، عملکردهای غیرمعقول یا اشتباه و مواردی از این دست، علاوه بر عصبانی کردن ما، اهمیت بسیار بالای صحت کارکرد نرم‌افزاری را روشن می‌سازند. به‌دلیل 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 عملی‌شدن 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 نرم‌افزار و ارتباط آن با بلاکچین

این گام به ارائه نمایی کلی از موقعیت بلاکچین می‌پردازد. به این منظور ابتدا مفهوم معماری نرم‌افزار و ارتباط آن با تفکیک لایه‌ها و جنبه‌های مختلف یک محصول نرم‌افزاری طرح شده؛ سپس با اشاره به ارتباط میان بلاکچین و معماری نرم‌افزار، هدف اصلی بلاکچین در یک جمله بیان می‌شود. درک هدف بلاکچین در شناخت مفهوم آن و فهم سایر گام‌های 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 پیمانه‌سازی 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. به‌علاوه، 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 عملکردی	جنبه‌های غیرعملکردی
لایه کاربرد	واریز پول برداشت پول انتقال پول دریافت گزارش تراکنش	رابط کاربری زیبا راحتی استفاده انتقال سریع پول
لایه پیاده‌سازی	؟	۲۴ساعته بودن مقاوم در برابر تقلب دارا بودن صحت کارکرد حفظ حریم خصوصی کاربر

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

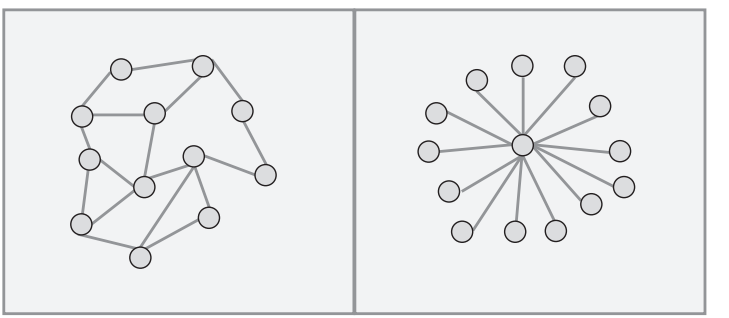
«موتور» پیشران سیستم تصمیم بگیریم. در ادامه بیشتر درباره معادل موتور خودرو در سیستم‌های نرم‌افزاری صحبت می‌کنیم.

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 توزیع‌شده (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 توزیع‌شده 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. فعلا لازم نیست به نقش گره‌ها و اطلاعات ردوبدل‌شده بین آنها بپردازیم. در سمت چپ شکل یک سیستم توزیع‌شده 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 توزیع‌شده (چپ) و متمرکز (راست)

مزایای سیستم توزیع‌شده

مزایای اصلی سیستم‌های توزیع‌شده عبارتند از:

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

قدرت محاسباتی بالاتر

از آنجایی‌که قدرت محاسباتی یک سیستم توزیع‌شده از تجمیع قدرت اجزای آن حاصل می‌شود، چنین سیستم‌هایی عموما قابلیت محاسباتی بالاتری نسبت به یک کامپیوتر تنها دارند. چنین امری گاهی در مقایسه سیستم‌های توزیع‌شده متشکل از کامپیوترهای ضعیف در مقابل با ابرکامپیوترهای 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 توزیع‌شده متشکل از تعداد زیاد کامپیوتر متصل به هم هستند، هزینه اولیه یک سیستم توزیع‌شده بیشتر از هزینه اولیه یک کامپیوتر مستقل است. اما هزینه‌های ساخت، نگهداری و استفاده از ابرکامپیوترها هنوز بسیار بیشتر از هزینه‌های ساخت، نگهداری و استفاده از سیستم‌های توزیع‌شده است. این امر تا حدودی از آنجا ناشی می‌شود که جایگزین کردن یک کامپیوتر خاص از یک سیستم توزیع‌شده می‌تواند بدون ایجاد تاثیر محسوس بر سیستم صورت پذیرد.

قابلیت اتکای بالاتر

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

متمرکز، ایجاد اشـکال در کامپیوتر مرکـزی می‌تواند به توقف عملکرد سیسـتم منجر شود. بنابراین یک ابرکامپیوتر مستقل عموما قابلیت اتکای پایین‌تری نسبت به یک سیستم توزیع‌شده دارد.

قابلیت رشد و مقیاس‌پذیری پیوسته

قابلیت محاسباتی یک شبکه توزیع‌شده برآمده از قدرت محاسباتی اجزای آن است. با افزودن کامپیوترهای بیشتر به شبکه می‌توان قدرت محاسباتی آن را در هر گام افزایش داد. به این ترتیب می‌توان به‌راحتی افزایش نیاز پیوسـته به قدرت محاسـباتی را پاسـخ گفت. در مقابل، در سیستم متمرکز، برای افزایش قدرت محاسباتی باید کامپیوترها با انواعی دارای قدرت محاسباتی بالاتر جایگزین شوند و افزایش قدرت محاسباتی به‌صورت پیوسته انجام نمی‌گیرد.

معایب سیستم توزیع‌شده

در مقابل سیستم‌های متمرکز، سیستم توزیع‌شده معایب زیر را دارد:

- سرباره هماهنگ‌سازی سیستم؛
- سرباره ارتباطات؛
- وابستگی به شبکه؛
- پیچیدگی نرم‌افزاری بیشتر؛
- مسائل امنیتی.

سرباره هماهنگ‌سازی سیستم

سیستم‌های توزیع‌شده فاقد هسته مرکزی جهت هماهنگ‌سازی سیستم هستند و هماهنگ‌سـازی بایـد توسـط اعضـای خود سیسـتم صـورت گیـرد. هماهنگ‌سـازی در این سیسـتم‌ها پیچیده بوده و بخشـی از قدرت محاسـباتی سیسـتم را نیـز به خود تخصیص می‌دهد. قدرت محاسباتی که می‌توانست صرف عملکردها و خدمات اصلی سیستم شود.

سرباره ارتباطات

هماهنگ‌سازی مستلزم ارتباط اجزاست. بنابراین کامپیوترهای یک شبکه توزیع‌شده 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 مصروف خود می‌کند.

وابستگی به شبکه

هر نوع ارتباطی نیازمند بستر ارتباطی است که اطلاعات را بین طرفین منتقل کند. کامپیوترهای یک سیستم غیرمتمرکز 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، اساسا سیستم غیرمتمرکز معنایی ندارد و چنان سیستمی به شبکه ارتباطی وابسته است.

پیچیدگی نرم‌افزاری بیشتر

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

مسائل امنیتی

ارتباط بین اجزا یعنی ارسال و به‌اشتراک‌گذاری 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 غیرمجازی بیفتد که به شبکه دسترسی پیدا کرده‌اند. مدیریت این مسائل امنیتی در یک سیستم غیرمتمرکز از سیستم متمرکز پیچیده‌تر است.

سیستم‌های همتابه‌همتای توزیع‌شده

سیستم‌های همتابه‌همتا (Peer-to-Peer) نوع خاصی از سیستم‌های توزیع‌شده

هستند. این سیستم‌ها متشکل از تعدادی کامپیوتر مستقل هستند (گره (Node) خوانده می‌شوند) که قدرت محاسبه، ذخیره اطلاعات، یا پهنای باندشان را به‌طور مستقیم و بدون دخالت یک هسته مرکزی هماهنگ‌کننده در اختیار سایر اجزای شبکه قرار می‌دهند. گره‌های شبکه از نظر نقش و رتبه برابر هستند و همگی همزمان فراهم‌کننده و مصرف‌کننده منابع به‌شمار می‌روند.

سیستم‌های همتابه‌همتا کاربردهای جالبی همچون اشتراک‌گذاری 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 گره‌های شبکه غیرمتمرکزی که به شکل‌گیری کل شبکه کمک می‌کنند. به این ترتیب هرچه تعداد کاربران بیشتر شود، قابلیت محاسباتی شبکه هم افزایش می‌یابد. این ایده، نتایج آن و چالش‌های پیش روی آن در گام‌های بعدی مورد بحث قرار خواهد گرفت.

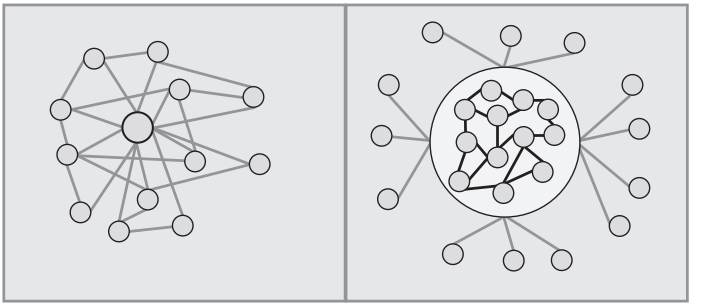
سیستم‌های مرکب متمرکز و توزیع‌شده

هر کدام از دو نوع معماری متمرکز و توزیع‌شده که از لحاظ فنی در تقابل با هم هستند، مزایای خاص خود را دارند. این وضعیت الهام‌بخش مهندسانی بوده که با ترکیب دو نوع معماری ساختارهای جدیدی با ارث‌بری خصوصیات خوب معماری متمرکز و توزیع‌شده ایجاد کرده‌اند. آشنایی با این ساختارهای ترکیبی در درک بهتر بلاکچین مفید خواهد بود؛ ساختارهایی که نوعی مرکزگرایی را بر سیستم‌های توزیع‌شده اعمال می‌کنند و ساختارهایی که نوعی توزیع‌شدگی را در سیستم‌های متمرکز شکل می‌دهند.

طرح گرافیکی سمت چپ در شکل ۲-۲ یک ساختار توزیع‌شده اما حاوی بخشی متمرکز را نشان می‌دهد. در نگاه اول به نظر می‌رسد اجزای سیستم یک در یک معماری توزیع‌شده قرار گرفته‌اند، اما همه دایره‌ها با دایره بزرگ‌تر مرکزی در اتصال هستند. طرح سمت راست شکل ۲-۲ رهیافت متفاوتی را نشان می‌دهد.

در وهله اول این ساختار متمرکز به نظر می‌رسد، چراکه همه دایره‌های بخش بیرونی

با دایره بزرگ‌تر مرکزی اتصال دارند، اما دایره مرکزی بزرگ خود دربرگیرنده یک ساختار غیرمتمرکز است.



شکل ۲-۲: ترکیب ساختارهای متمرکز و توزیع‌شده

از نقاط مشترک این دو طرح پیچیدگی تبیین آنهاست! این ساختارها توزیع‌شده 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 تجاری‌سازی بلاکچین می‌پردازیم، روشن‌تر خواهد شد.

شناسایی ساختارهای توزیع‌شده

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

نکته: اگر یک جزء ساختار، برای نمونه یک کلید خاموش‌کردن، بتواند تمام سیستم را از کار بیندازد، آن ساختار توزیع‌شده نیست.

هدف بلاکچین

تصمیم‌گیری درباره معماری سیستم در زمان طراحی یک نرم‌افزار، همچون انتخاب موتور خودرو است. انتخاب معماری می‌تواند مستقل از جنبه‌های عملکردی لایه کاربرد صورت پذیرد. بنابراین می‌توان برای هدف عملکردی یکسان در لایه کاربرد از معماری‌های توزیع‌شده یا متمرکز استفاده کرد. یک سیستم پرداخت هم می‌تواند در قالب توزیع‌شده یا متمرکز پیاده‌سازی شود.

هر کدام از معماری‌ها، مزایا و محدودیت‌های خاص خود را داشته و به روش متفاوتی عمل می‌کنند. انتخاب یک معماری خاص در نحوه انجام جنبه‌های عملکردی و غیرعملکردی سیستم تاثیر خواهد داشت. به‌طور خاص، هر معماری شیوه متفاوتی برای حصول صحت کارکرد (Integrity) دارد. بلاکچین ابزاری است برای حصول صحت کارکرد در قالب معماری توزیع‌شده.

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

چشم‌انداز

حصول صحت کارکرد در یک ساختار توزیع‌شده امری است بسیار فنی و ممکن است برای بسیاری جذاب نباشد، اما کارکردهای ساختارهای توزیع‌شده و قابلیت جایگزینی آنها با ساختارهای متمرکز برای بسیاری جالب توجه است. بخش بعدی به تاثیر سیستم‌های همتابه‌همتا در دنیای ما و نقش بلاکچین در حصول صحت کارکرد در سیستم‌های توزیع‌شده و تغییر دنیا می‌پردازد.

خلاصه

- معماری یک سیستم نرم‌افزاری چگونگی ساماندهی و ارتباطات بین اجزای آن را تعیین می‌کند.
- معماری‌های نرم‌افزاری متمرکز و توزیع‌شده دو نوع اصلی و متقابل معماری هستند.
- یک سیستم توزیع‌شده متشکل از کامپیوترهای مستقلی است که با همکاری

یکدیگر و به‌واسطه ارتباطات از طریق یک بستر ارتباطی، بدون دارا بودن هیچ جزء مرکزی هماهنگ یا مدیریت‌کننده به انجام هدف می‌پردازد.

- به‌عنوان یک قاعده ساده، در صورتی که بتوان کارکرد یک سیستم را از طریق یک جزء خاص متوقف کرد، آن سیستم توزیع‌شده نیست؛ فارغ از اینکه معماری آن، چه مقدار پیچیده به نظر برسد.
- بلاکچین بخشی از لایه پیاده‌سازی سیستم نرم‌افزاری توزیع‌شده است.
- هدف بلاکچین تامین یک جنبه غیرعملکردی سیستم‌های نرم‌افزاری توزیع‌شده 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 نظرداشت نوع خاصی از شبکه‌های توزیع‌شده، 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 سی‌دی 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 استریم‌موزیک 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.»

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

آنچه فنینگ و همکارانش اختراع کردند یک سیستم همتابه‌همتا برای به‌اشتراک‌گذاری موسیقی بود. این نرم‌افزار در زمان عرضه خود در سال‌های پایانی دهه ۹۰، طلیعه عصر جدیدی بود برای مدل کسب‌وکاری 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 همتابه‌همتا 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 به‌عنوان 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 کسب‌وکار استودیوهای موسیقی دچار تغییرات اساسی شد.

دیجیتالی‌شدن 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. نپستر نقشی اساسی در جایگزینی نقش واسط استودیوهای موسیقی داشت. با وجود این پلتفرم، مردم دیگر برای دسترسی به آخرین موسیقی‌ها نیازی به استودیوها نداشتند. نسپتر امکان اشتراک‌گذاری هر فایل موسیقی با تمام مردم جهان را بدون نیاز به سی‌دی و با تکیه بر شبکه اینترنت فراهم آورد. رهیافت همتابه‌همتا نپستر به مساله و ایجاد یک بازار برای فایل‌های mp3، طیف گسترده‌تری از موسیقی‌ها را به‌راحتی در اختیار علاقه‌مندان قرار داد و به عدم ضرورت وجود استودیوهای موسیقی و ضررهای فراوان برای این صنعت منجر شد.

قابلیت‌های بالقوه سیستم های همتابه‌همتا

ماجرای نپستر به ما آموخت که سیستم‌های همتابه‌همتا قابلیت ایجاد بازآرایی ساختاری اساسی در یک صنعت را بر اساس یک ایده ساده دارا هستند؛ جایگزین‌کردن واسط با بستر 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 همتابه‌همتاست. 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 قرض‌گرفتن، قرض‌دادن 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 به‌صورت مستقیم میان اجزای ذی‌ربط صورت پذیرفته و اجزای واسط دیگری در آن درگیر نمی‌شوند. این امر افزایش سرعت و کاهش هزینه عملیات را به‌دنبال دارد.

مزیت‌های استفاده از سیستم‌های همتابه‌همتا به انتقال پول محدود نمی‌شود. 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 همتابه‌همتاست. با ادامه روند دیجیتالی‌شدن امور، موارد بیشتر و بیشتری در زندگی روزمره در قالب خدمات و کالاهای دیجیتال و غیرمادی عرضه شده و در نتیجه می‌توان از امکانات سیستم‌های همتابه‌همتا در مورد آنها بهره‌مند شد.

طرفداران سیستم‌های همتابه‌همتا ادعا می‌کنند که تقریبا 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 متمرکزی ارائه می‌شود که نقش واسط میان تامین‌کنندگان و مصرف‌کنندگان را ایفا می‌کنند.

نکته: جایگزینی واسطه میانی، حذف واسط (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 مساله 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 به‌اشتراک‌گذاری 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، توزیع‌شده 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، جایابی و تایید گره‌های دیگر سیستم را بر عهده دارند. چنین معماری ترکیبی از مزایای هر دو نوع معماری متمرکز و توزیع‌شده 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 توزیع‌شده 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 توزیع‌شده و بلاکچین به استفاده آن سیستم‌ها برای دستیابی و حفظ صحت کارکرد بازمی‌گردد.

قابلیت‌های بلاکچین

رابطه بین سیستم‌های توزیع‌شده صرفا همتابه‌همتا با بلاکچین این است که اولی از دومی به‌عنوان ابزاری برای رسیدن به صحت کارکرد و یکپارچگی و حفظ آن بهره می‌برد. از این رو، جنبه جذاب بلاکچین این است: کمک به شکل‌گیری شبکه‌های همتابه‌همتای کاملا توزیع‌شده با قابلیت‌های تجاری فراوان برای جایگزینی سیستم‌های متمرکز و ایجاد تغییرات کلی و اساسی در صنایع مختلف از طریق حذف واسط‌ها. از آنجا که این سیستم‌های توزیع‌شده همتابه‌همتا برای حفظ یکپارچگی و صحت کارکرد از بلاکچین بهره می‌برند، اهمیت اساسی این فناوری روشن می‌شود. حقیقتی که باعث جذابیت بلاکچین برای مردم می‌شود، قابلیت آن برای حذف واسط‌هاست. 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 توزیع‌شده همتابه‌همتا ناشی می‌شود که می‌تواند به ایجاد تغییرات اساسی در زمینه‌های مختلف و حذف واسط‌ها بینجامد.

چشم‌انداز

این گام به چیستی کلی سیستم‌های همتابه‌همتا و قابلیت آنها در ایجاد تغییرات اساسی در صنایع مختلف و حذف واسطه‌ها پرداخت. به‌علاوه اشاره شد که فناوری بلاکچین به عملی‌شدن چنان هدفی برای سیستم‌های همتابه‌همتا یاری می‌رساند. با این حال، این سوال که چرا دستیابی و حفظ یکپارچگی و صحت کارکرد در سیستم‌های توزیع‌شده 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 مستقیما در اختیار یکدیگر قرار می‌دهند.

- مزیت سیستم‌های همتابه‌همتا این است که به کاربران اجازه می‌دهند که مستقیما با یکدیگر ارتباط داشته باشند؛ بدون نیاز به واسطی که عملا ارتباط را به‌صورت 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 کاملا توزیع‌شده باشند.
- سیستم‌های همتابه‌همتای کاملا توزیع‌شده در قالب شبکه‌ای از اعضا ساماندهی شده‌اند که در آن هر عضو به‌صورت مستقیم با بقیه در تماس بوده و هیچ گره هماهنگ‌کننده مرکزی در آنها وجود ندارد.
- نپستر قدرت شبکه‌های همتابه‌همتا را برای به‌اشتراک‌گذاری 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 همتابه‌همتاست.
- بخش عظیمی از سیستم مالی و پرداخت دنیا به عملکرد واسط میان تامین‌کنندگان 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 تاثیرپذیری صنعت موسیقی از نپستر دچار تحولات عظیم شود.
- با گسترش روند دیجیتالی‌شدن، جنبه‌های بیشتری از زندگی و کالاها و خدمات بیشتری به‌صورت 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 نشات می‌گیرد.

۲

بخش دو

چرا بلاکچین مورد نیاز است؟

این بخش به شرح موضوع و اهمیت مساله‌ای می‌پردازد که بلاکچین برای حل آن ساخته شده است. بخش حاضر همچنین به درک بیشتر از موضوعیت بلاکچین و زمینه‌ای که این فناوری حائز بیشترین اهمیت است و همچنین رابطه آن با اعتماد، حفظ صحت عملکرد و مدیریت مالکیت می‌پردازد. در پایان این بخش به فهمی عمیق‌تر از هدف بلاکچین و برداشتی متفاوت از اصطلاح بلاکچین نائل می‌شوید.

گام چهارم

فهم مساله اصلی

چگونه گروهی از کامپیوترهای مستقل را در ارتباط با هم ساماندهی کنیم؟

دو گام قبلی به هدف بلاکچین به‌طور عمومی و روشن‌سازی اهمیت آن برای شبکه‌های همتابه‌همتای توزیع‌شده اختصاص داشت. روشن شد که حفظ یکپارچگی و صحت کارکرد در شبکه توزیع‌شده، هدف اصلی استفاده از بلاکچین است. اما چرا حفظ یکپارچگی و صحت کارکرد در سیستم‌های توزیع‌شده و سیستم‌های همتابه‌همتای صرفا توزیع‌شده، چالش‌برانگیز است؟ این گام با اشاره به رابطه ظریف میان قابلیت اعتماد و یکپارچگی و صحت کارکرد شبکه‌های همتابه‌همتای کاملا توزیع‌شده، در پی پاسخگویی به پرسش مذکور است. در نتیجه، گام حاضر فهم ما را از اهمیت یکپارچگی و صحت کارکرد افزایش داده و مساله‌ای را که با بلاکچین حل می‌شود، روشن‌تر می‌سازد. در پایان، این گام زمینه و شرایطی را که انتظار می‌رود بلاکچین در آن حائز بیشترین اهمیت باشد، شرح می‌دهد.

یک مثال استعاری

بسیاری از زبان‌ها ضرب‌المثل‌هایی برای توصیف شرایط فردی دارند که می‌خواهد گروه بی‌نظمی را ساماندهی کند. برای مثال در زبان انگلیسی از اصطلاح تلاش برای گله‌کردن گربه‌ها استفاده می‌شود؛ تصویری که نمایانگر چالشی بزرگ است؛ ساماندهی گروهی از حیوانات لجباز که زیر بار فرامین هیچ نهاد کنترل‌کننده‌ای نمی‌روند. این شرایط، یعنی تلاش برای ساماندهی نقاط مستقلی که پذیرای فرامین هیچ نهاد کنترل‌کننده مرکزی نمی‌شوند، آشنا به نظر می‌رسد؟ چنین وضعیتی همان است که در یک شبکه همتابه‌همتای کاملا توزیع‌شده به وقوع می‌پیوندد. شبکه‌ای متشکل از گره‌های مستقل که هیچ گره کنترل‌کننده مرکزی آنها را مدیریت و ساماندهی نمی‌کند. این گام به یکی از مهم‌ترین چالش‌های یک شبکه همتابه‌همتای کاملا توزیع‌شده و ارتباط آن با بلاکچین می‌پردازد.

اعتماد و صحت کارکرد در سیستم‌های همتابه‌همتا

اعتماد و صحت کارکرد دو روی یک سکه هستند. در یک سیستم نرم‌افزاری، صحت کارکرد جنبه‌ای غیرعملکردی از سیستم برای امن، کامل (Complete)، سازگار (Consistent)، درست (Correct) و خالی از خطا و اشکال‌بودن است. اعتماد هم به معنای اعتقاد عمیق انسان‌ها به قابلیت اتکا، صداقت یا قابلیت فرد یا چیزی بدون نیاز به شواهد و استدلال است. اعتماد در وهله اول شکل می‌گیرد و با گذر زمان بر حسب تعاملات و نتایج، افزایش یا کاهش می‌یابد.

در رابطه با یک سیستم همتابه‌همتا، کاربران به شبکه اضافه شده و در صورتی که به آن اعتماد کنند، به استفاده از شبکه و مشارکت در آن ادامه می‌دهند. صحت کارکرد سیستم برای برآوردن انتظارات کاربران و تقویت اعتماد آنها اهمیت دارد. اگر اعتماد کاربران به‌دلیل نبود صحت کارکرد سلب شود، آنها سیستم را ترک کرده و در نهایت چنین روندی به نابودی شبکه منجر می‌شود. با توجه به اهمیت اعتماد برای وجود سیستم‌های همتابه‌همتا، سوال عمده این است: صحت کارکرد در این سیستم‌ها چگونه به دست

آمده و حفظ می‌شود؟

حصول و حفظ صحت کارکرد در سیستم‌های کاملا توزیع‌شده بستگی به عوامل مختلفی از جمله این موارد دارد:

- اطلاع درباره تعداد گره‌ها؛
- اطلاع درباره قابلیت اعتماد گره‌ها.

بخت دستیابی به صحت کارکرد در یک سیستم همتابه‌همتای کاملا توزیع‌شده در صورت دانستن تعداد گره‌ها و قابلیت اعتماد آنها بالاتر می‌رود. این شرایط در عین حال، سخت‌ترین شرایط برای دستیابی به صحت کارکرد در یک شبکه همتابه‌همتای توزیع‌شده در زمانی است که تعداد و قابلیت اعتماد گره‌ها نامعلوم باشد. این همان شرایطی است که با راه‌اندازی یک شبکه همتابه‌همتای توزیع‌شده عمومی روی اینترنت با آن مواجه هستیم؛ شبکه‌ای که هر کسی می‌تواند عضو آن شود.

تهدیدهای صحت کارکرد در سیستم‌های همتابه‌همتا

به‌طور ساده می‌توان دو تهدید عمده برای صحت کارکرد در سیستم‌های همتابه‌همتا نام برد:

- اشکالات فنی؛
- گره‌های مخرب (Malicious).

اشکالات فنی

سیستم‌های همتابه‌همتا از کامپیوترهای کاربرانی تشکیل شده‌اند که از طریق شبکه با هم در ارتباط هستند. تمام سخت‌افزارها و نرم‌افزارهای مشارکت‌کننده در سیستم با خطر ذاتی بروز با خطا و اشکال مواجه هستند. از این رو، هر سیستم توزیع‌شده‌ای با مساله عدم کارکرد یا کارکرد همراه با اشتباه اجزایش روبه‌رو می‌شود.

گره‌های مخرب

اعضای مخرب دومین تهدید صحت کارکرد در سیستم‌های همتابه‌همتاست. این

منبع مخل اعتماد، ریشه فنی نداشته؛ بلکه حاصل رفتار اعضایی از شبکه است که خواهان ایجاد اشکال در سیستم هستند. می‌توان به عبارتی این موضوع را بیشتر امری مرتبط با جامعه‌شناسی به‌شمار آورد تا فناوري. اعضای مخرب و متقلب بزرگ‌ترین تهدید یک سیستم همتابه‌همتا هستند؛ چراکه پایه مبنایی شکل‌گیری این سیستم‌ها؛ یعنی اعتماد را سست می‌کنند. به محض اینکه کاربری از گره‌های دیگر شبکه سلب اعتماد کند، منابع خود را از شبکه خارج کرده و دیگر در آن مشارکت نمی‌کند. با کاهش تعداد کاربران، جذابیت کل سیستم برای باقی کاربران هم کمتر شده و این امر خود به روند خروج سایرین از شبکه و نابودی آن دامن می‌زند.

مشکل اصلی که باید توسط بلاکچین حل شود

دستیابی به صحت کارکرد و اعتماد در صورت مهیا بودن همه شرایط آسان است، اما رسیدن به این موارد در صورت مهیا نبودن آن شرایط در یک سیستم همتابه‌همتای توزیع‌شده یک چالش اساسی است. این همان مشکلی است که بلاکچین برای حل آن ساخته شده است. مشکل اصلی که باید توسط بلاکچین حل شود، دستیابی و حفظ صحت کارکرد در یک سیستم همتابه‌همتای کاملا توزیع‌شده با تعداد نامعلوم گره‌ها و میزان نامعلوم قابلیت اعتماد آنهاست. این مساله جدیدی نبوده و در واقع مساله‌ای شناخته‌شده در علوم کامپیوتر است که با نام مساله ژنرال بیزانسی (Byzantine general problem) خوانده می‌شود.

نکته: مشکل اصلی که باید توسط بلاکچین حل شود، دستیابی و حفظ صحت کارکرد در یک سیستم همتابه‌همتای کاملا توزیع‌شده با تعداد نامعلوم گره‌ها و میزان نامعلوم قابلیت اعتماد آنهاست.

چشم‌انداز

این گام به روشن‌ساختن اهمیت صحت کارکرد و اعتماد در سیستم‌های همتابه‌همتا اختصاص یافت. علاوه بر این، گام حاضر به مساله اصلی که باید توسط بلاکچین حل شود و اهمیت این فناوری برای حصول صحت کارکرد و اعتماد در سیستم‌های

همتابه‌همتا، اشـاره داشـت. با این حال، هنوز به تعریفـی از بلاکچین نرسـیده‌ایم. این موضوع گام بعدی خواهد بود.

خلاصه

- صحـت کارکـرد و اعتمـاد، دغدغه‌هـای اصلی مرتبـط بـا سیسـتم‌های همتابه‌همتا هستند.
- مردم در صورت اعتماد به یک سیستم همتابه‌همتا به آن می‌پیوندند و در آن مشارکت می‌کنند، این مشارکت در صورت حفظ اعتماد به سیستم ادامه پیدا می‌کند.
- سلب اعتماد کاربران از یک سیستم همتابه‌همتا به ترک سیستم می‌انجامد که نهایتا در روندی افزایشی می‌تواند به نابودی کل سیستم منجر شود.
- تهدیدهای عمده صحت کارکرد در سیستم‌های همتابه‌همتا عبارتند از:
  - اشکالات فنی؛
  - گره‌های مخرب.
- دستیابی به صحت عملکرد در یک سیستم همتابه‌همتا وابسته است به:
  - اطلاع درباره تعداد گره‌ها؛
  - اطلاع درباره قابلیت اعتماد به گره‌ها.
- مشـکل اصلی که باید توسـط بلاکچین حل شـود، دسـتیابی و حفظ صحت کارکرد در یک سیستم همتابه‌همتای کاملا توزیع‌شده با تعداد نامعلوم گره‌ها و میزان نامعلوم قابلیت اعتماد آنهاست.

گام پنجم

شفاف‌سازی معنی

چهار روش برای تعریف بلاکچین

در گام‌های قبل به هدف کارکردی بلاکچین و رابطه آن با اعتماد و صحت کارکرد سیستم نرم‌افزاری پرداختیم، اما جای تعریفی از بلاکچین همچنان خالی است. این گام به ارائه تعریفی از این اصطلاح و کاربردهای مختلف آن می‌پردازد. در این گام تعریفی موقتی از بلاکچین ذکر می‌شود که می‌تواند ما را در ادامه مسیر کتاب یاری کند. در نهایت، این گام اهمیت بالای بلاکچین را برای مدیریت مالکیت روشن می‌سازد.

اصطلاح بلاکچین

در کتاب حاضر، مراد از اصطلاح بلاکچین می‌تواند این موارد باشد:

- به‌عنوان نامی برای یک ساختمان داده (data structure)؛
- به‌عنوان نامی برای یک الگوریتم؛
- به‌عنوان نامی برای یک مجموعه از فناوری‌ها؛
- به‌عنوان یک اصطلاح فراگیر برای شبکه‌های همتابه‌همتای کاملا توزیع‌شده.

یک ساختمان داده

ساختمان داده در علوم کامپیوتر و مهندسی نرم‌افزار، راهی است برای سازماندهی داده‌ها بدون در نظر گرفتن محتوای اطلاعاتی آنها. می‌توان آن را همچون طرح ساختمان در معماری به‌شمار آورد. طرح ساختمان بدون توجه به کارکرد بخش‌های مختلف، به فضاهای مختلف داخل ساختمان و ارتباط و جدایی بین بخش‌های مختلف با استفاده از دیوارها و طبقات و پله‌ها می‌پردازد. هنگامی که اصطلاح بلاکچین برای اشاره به یک ساختمان داده به کار گرفته شود، منظور اصلی نحوه قرارگیری اطلاعات در قالب واحدهایی است که بلوک نامیده می‌شوند. می‌توان این بلوک‌ها را مشابه صفحات یک کتاب تصور کرد. بلوک‌ها همچون اجزای یک زنجیر به هم پیوند خورده‌اند، لفظ بلاکچین هم از همین‌جا نشات می‌گیرد. در ارتباط با یک کتاب، آنچه در صفحات ذخیره می‌شود، کلمات و جملات هستند؛ اطلاعاتی که به عوض نوشته‌شدن، روی یک نوار قرقره‌ای بلند در صفحات مختلف جای گرفته‌اند. صفحات بر اساس جایگاهی که در کتاب دارند و شماره صفحه به هم متصل شده‌اند. برای تشخیص اینکه کسی صفحه‌ای از کتاب را جدا نکرده باشد، کافی است شماره صفحات آن را بررسی کنید. علاوه بر این، اطلاعات در داخل هر صفحه نیز همچون صفحات کتاب به نحوی ساختارمند در کنار هم قرار گرفته‌اند. ترتیب قرارگیری بسیار مهم است. ترتیب قرارگیری بلوک‌های داده در ساختمان داده‌ها به‌واسطه نحوه بسیار خاصی از شماره‌گذاری صورت می‌گیرد که با وضعیت شماره صفحات در یک کتاب معمولی بسیار متفاوت است.

یک الگوریتم

در علوم کامپیوتر، الگوریتم به توالی از دستورها که باید توسط کامپیوتر اجرا شوند، گفته می‌شود. مراد از اصطلاح بلاکچین به‌عنوان یک الگوریتم، مجموعه دستورالعمل‌هایی است که محتوای اطلاعاتی تعداد زیادی نسخه ساختمان داده بلاکچینی موجود در یک شبکه همتابه‌همتای کاملا توزیع شده را به روشی مشابه با یک رای‌گیری دموکراتیک به توافق و اجماع می‌رساند.

مجموعه‌ای از فناوری‌ها

هنگامی که از اصطلاح بلاکچین برای اشاره به مجموعه‌ای از فناوری‌ها استفاده شود، مقصود ترکیبی است از بلاکچین به‌عنوان ساختمان داده و بلاکچین به‌عنوان یک الگوریتم و در عین حال فناوری‌های رمزنگاری و امنیت که در کنار هم برای حصول و حفظ صحت کارکرد در یک شبکه همتابه‌همتای کاملا توزیع‌شده به کار گرفته می‌شوند. فارغ از اینکه هدف کارکردی آن شبکه همتابه‌همتا چه چیزی باشد.

اصطلاحی فراگیر برای شبکه‌های همتابه‌همتای کاملا توزیع‌شده

بلاکچین را می‌توان به‌عنوان اصطلاحی فراگیر برای اشاره به شبکه‌های همتابه‌همتای کاملا توزیع‌شده‌ای از دفاتر کل (Ledgers) به کار برد که از بلاکچین به‌عنوان مجموعه‌ای از فناوری‌ها استفاده می‌کنند. توجه داشته باشید که ذیل این اصطلاح، بلاکچین برای اشاره به کلیت یک شبکه همتابه‌همتای کاملا توزیع‌شده به کار گرفته می‌شود و نه واحد نرم‌افزاری که جزئی از شبکه توزیع‌شده است.

کاربرد این اصطلاح در کتاب حاضر

طی این کتاب، از اصطلاح بلاکچین برای اشاره به شبکه‌های همتابه‌همتای کاملا توزیع‌شده‌ای از دفاتر کل استفاده می‌شود که بلاکچین را به‌عنوان مجموعه‌ای از فناوری‌ها به کار می‌برند. در صورتی که معانی دیگر مدنظر باشد، به‌طور روشن عبارات بلاکچین به‌عنوان ساختمان داده، بلاکچین به‌عنوان الگوریتم یا بلاکچین به‌عنوان مجموعه

فناوری، مورد تاکید قرار می‌گیرند.

نکته: فناوری که امروزه بلاکچین خوانده می‌شود، در سال ۲۰۰۸ طی مقاله‌ای منتشرشده توسط فرد یا گروهی با نام ساتوشی ناکاموتو (Satoshi Nakamoto) مطرح شد. البته هویت حقیقی منتشرکنندگان هنوز آشکار نشده است.

یک تعریف موقتی

تعریفی که در ادامه ذکر می‌شود کامل نبوده و فاقد جزئیات مهمی است که هنوز مورد اشاره قرار نگرفته‌اند، اما به‌عنوان تعریفی موقتی و میانی در راه درک کامل‌تر اصطلاح بلاکچین مفید است:

بلاکچین شبکه همتابه‌همتای کاملاً توزیع شده‌ای از دفاتر کل است که از یک واحد نرم‌افزاری بهره می‌برد. این نرم‌افزار برای حصول و حفظ یکپارچگی و صحت کارکرد، با اتکا به فناوری‌های رمزنگاری و امنیت و نیز الگوریتم خاص خود محتوای اطلاعاتی بلوک‌های داده مرتب و متصل به یکدیگر را ساماندهی می‌کند.

نقش مدیریت مالکیت

تعریف موقتی مطرح‌شده دربردارنده هیچ توضیحی در رابطه با بیت‌کوین (Bitcoin) یا مالکیت رمزارز (Cryptographic money) نیست. این امر شاید عجیب به نظر برسد، چراکه بسیاری از مقالات و کتاب‌های نوشته‌شده در زمینه بلاکچین مدعی هستند که هدف این فناوری مدیریت ارزهای دیجیتال است. در حقیقت، مدیریت مالکیت رمزارز یک کارکرد بسیار برجسته و اساسی استفاده از بلاکچین است، اما تنها کارایی آن نیست. بلاکچین دارای طیف گسترده و متنوعی از کارکردهای گوناگون است. با این حال، دو دلیل عمده برای چرایی مطالب زیاد در رابطه با کارکرد بلاکچین برای مدیریت مالکیت دارایی‌های دیجیتال وجود دارد؛ اول اینکه چنین کارکردی ساده‌ترین راه شرح و فهم بلاکچین است.

دوم اینکه چنین کارکردی بیشترین تاثیر را بر اقتصاد وارد می‌کند. مفهوم مالکیت و حفظ و اعمال حق مالکیت تقریبا مبانی اصلی در تمامی جوامع انسانی هستند.

(چنین مفهومی حتی در تعاملات بسیاری از حیوانات وجود داشته و برای حفظ و اعمال حق مالکیت با یکدیگر به نزاع برمی‌خیزند.) بخش بزرگی از فعالیت‌های بانک‌ها، شرکت‌های بیمه، وکلا و دادگاه‌ها صرفا صرف مدیریت مالکیت و حفظ و حمایت از حق مالکیت می‌شود. از این رو، مدیریت مالکیت یک بازار چندین میلیارد دلاری است و هر فناوری که بتواند روش مدیریت مالکیت را تغییر دهد، تاثیر بسیار بزرگی خواهد داشت. به نظر می رسد بلاکچین می‌تواند شیوه مدیریت مالکیت ما را به نحوی چشم‌گیر تغییر دهد.

زمینه کاربردی بلاکچین در این کتاب

بلاکچین به‌عنوان یک مجموعه فناوری، آنگاه که برای مدیریت شبکه همتابه‌همتای کاملا توزیع‌شده‌ای از دفاتر کل مورد استفاده قرار گیرد، می‌تواند کاربردهای متنوعی از جمله مدیریت مالکیت دارایی‌های دیجیتال یا رمزارزها داشته باشد. با این حال در کتاب حاضر به عمد از تمرکز بر یک زمینه کاربردی خاص دوری شده است تا توجه کامل بر موضوع اصلی مورد بحث قرار گیرد. با این حال به‌منظور فهم راحت‌تر، در این کتاب کاربرد عمومی بلاکچین برای مدیریت مالکیت مورد اشاره قرار می‌گیرد؛ البته بدون توجه به ماهیت دارایی‌های مدیریت‌شده. در نتیجه، هدف کلی مدیریت دارایی می‌تواند به‌عنوان یک راهنمای ذهنی در مسیر یادگیری برای ایجاد تصویری ذهنی از بلاکچین یاری‌رسان باشد.

چشم‌انداز

این گام به روشن‌سازی بلاکچین و ارائه تعریفی موقتی از آن اختصاص داشت. کتاب حاضر به کاربرد عمومی مدیریت و شفاف‌سازی مالکیت به‌عنوان یکی از کارکردهای بلاکچین می‌پردازد، اما موضوع مالکیت باید به نحوی روشن‌تر مورد بحث قرار گیرد. درک دقیق‌تر از مالکیت به فهم عمیق‌تر بلاکچین یاری می‌رساند. گام بعدی به ذکر دقیق‌تر مبانی مالکیت و دارایی تخصیص یافته است.

خلاصه

- اصطلاح بلاکچین می‌تواند برای افراد مختلف بسته به سیاق سخن (Context) معانی متفاوت داشته باشد.
- بلاکچین می‌تواند به موارد زیر اشاره داشته باشد:
  - ساختمان داده؛
  - یک الگوریتم؛
  - مجموعه‌ای از فناوری‌ها؛
  - اصطلاحی فراگیر برای شبکه‌های همتابه‌همتای کاملا توزیع‌شده با زمینه کاربردی مشترک.
- مدیریت و شفاف‌سازی مالکیت، مهم‌ترین کاربرد بلاکچین است، اما تنها کاربرد آن نیست.
- بلاکچین شبکه همتابه‌همتای کاملا توزیع شده‌ای از دفاتر کل است که از یک واحد نرم‌افزاری بهره می‌برد. این نرم‌افزار برای حصول و حفظ یکپارچگی و صحت کارکرد، با اتکا به فناوری‌های رمزنگاری و امنیت و نیز الگوریتم خاص خود محتوای اطلاعاتی بلوک‌های داده مرتب و متصل به یکدیگر را ساماندهی می‌کند.

گام ششم

درک مفهوم مالکیت

چرا چیزی مال ماست؟

در گام۵ تعریفی موقتی از بلاکچین ارائه شد. همچنین مدیریت مالکیت به‌عنوان مهم‌ترین کاربرد بلاکچین مورد اشـاره قرار گرفت. این گام به تشریح بیشـتر رابطه بلاکچین و کاربرد آن در مدیریت مالکیت می‌پردازد. به عبارت دیگر، این گام به ارتباط میان اعتماد و صحت کارکرد در یک شبکه همتابه‌همتای کاملا توزیع‌شده و مدیریت مالکیت می‌پردازد. علاوه بر این، تصویری کلی از ماهیت مالکیت و نیز مفاهیم اولیه امنیت در این گام مطرح می‌شود.