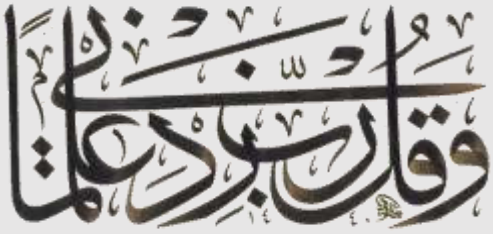


And say: **"My lord, increase me in knowledge."**

خودآموز کاربردی سرمایه گذاری در

مبتنی بر تکنولوژی واقعیت افزوده (AR)

حجت حاتمی شاه میر

بهنام هادی

الهام حاتمی شاه میر

زمستان ۱۳۹۸

سرشناسه : حاتمی شاه میر، حجت، ۱۳۶۲ –
عنوان و نام پدیدآور : خودآموز کاربردی سرمایه‌گذاری در بیت کوین و سایر ارزهای رمزنگاری شده مبتنی بر تکنولوژی واقعیت افزوده (AR)/مؤلف: حجت حاتمی شاه میر – بهنام هادی – الهام حاتمی شاه میر
مشخصات نشر : تهران: حریم دانش، ۱۳۹۸.
مشخصات ظاهری : ۲۱۰ص.
شابک : ۹۷۸-۶۲۲-۶۴۲۳-۴۰-۳
وضعیت فهرست نویسی : فیپا
موضوع : بیتکوین -- انتقال الکترونیکی وجوه -- ارز مجازی – رمزنگاری -- پول
موضوع: Money -- Cryptography – Digital currency -- Electronic funds transfers -- Bitcoin
شناسه افزوده : هادی، بهنام، ۱۳۵۶ –
شناسه افزوده : حاتمی شاه‌میر، الهام، ۱۳۶۶ –
رده‌بندی کنگره : HG۱۷۱۰
رده‌بندی دیویی : ۳۳۲/۴۰۴
شماره کتابشناسی ملی : ۶۰۷۵۴۸۸

عنوان کتاب: خودآموز کاربردی سرمایه گذاری در بیت کوین و سایر ارزهای رمزنگاری شده مبتنی بر تکنولوژی واقعیت افزوده (AR)
مولف: حجت حاتمی شاه میر – بهنام هادی – الهام حاتمی شاه میر
ویراستار: فرناز حکّی
ناشر: حریم دانش
نوبت چاپ: چاپ اول ۱۳۹۹
قیمت به همراه اپلیکیشن AR: ۱،۱۸۰،۰۰۰ تومان و بدون اپلیکیشن AR ۱۲۰،۰۰۰ تومان
تیراژ: ۱۰۰۰ جلد
شابک: ۹۷۸-۶۲۲-۶۴۲۳-۴۰-۳

پیشگفتار

مطالعات خود در زمینه تکنولوژی بلاک‌چین (زنجیره بلوکی) و ارزهای رمزنگاری شده را از سال ۱۳۹۳ خورشیدی آغاز کردیم و در این مدت منابع وکتاب‌های زیاد را مطالعه کردیم و تجربیات زیادی در زمینه خرید و فروش، استخراج بیت کوین و سایر رمزارزها کسب کردیم. با آغاز سال ۲۰۱۷ میلادی و اوج گیری قیمت ارزهای رمزنگاری شده و به ویژه بیت‌کوین تصمیم گرفتیم،کتاب کاربردی نحوه سرمایه گذاری در بازار ارزهای رمزنگاری شده را آماده کنیم تا علاقه‌مندان با آگاهی کامل نسبت به ریسک‌های موجود و به دور از هیجان و احساسات بتوانند سرمایه‌گذاری کم خطری را در این بازار تجربه کنند.

اخیرا در دنیا برای آموزش و تبلیغات از فناوری واقعیت افزوده[۱] که زیرمجموعه ی فناوری بزرگتری به نام واقعیت مجازی[۲] است، برای انتقال بهتر مفاهیم استفاده شده است. لذا بر آن شدیم تا از این فناوری به‌روز بر روی کتاب استفاده کنیم.

امیدواریم در کنار هم و با مطالعه مستمر، سرمایه‌گذاری پرسود و کم خطری را تجربه کنیم.

حجت حاتمی شاه میر

زمستان ۱۳۹۸

---

[۱] Augmented Reality

[۲] Virtual Reality

راهنمای استفاده از کتاب

همانطور که اشاره شد این کتاب مبتنی بر تکنولوژی واقعیت افزوده[1] منتشر شده است تا بتوانید از محتویات چند رسانه ای (ویدئوها و پادکست های آموزشی) آماده شده، استفاده نمایید.

با اجرای نرم افزار دوربین گوشی شما فعال می‌شود، حال کافیست آن را روی تصاویر از کتاب قرار دهید که با علامت  مشخص شده‌اند. اگر به هر دلیلی در دیدن ویدئوهای آموزشی با خطا مواجه شدید از طریق پشتیبانی اپلیکیشن با ما در ارتباط باشید.

ضمنا ویدئوهای آموزشی با ویرایش‌های جدید کتاب، بروزرسانی خواهد شد تا شما بتوانید به تناسب تغییرات روزآمد بازار ارزهای رمزنگاری شده همراه شوید.

---

۱ واقعیت افزوده (Augmented Reality) یک نمای فیزیکی زنده، مستقیم یا غیرمستقیم (و معمولاً در تعامل با کاربر) است، که عناصری را پیرامون دنیای واقعی افراد اضافه می‌کند. واقعیت افزوده تا حدودی شبیه به واقعیت مجازی (Virtual Reality) است که توسط یک شبیه‌ساز، دنیای واقعی را کاملاً شبیه‌سازی می‌کند. در واقع وجه تمایز بین واقعیت مجازی و واقعیت افزوده این است که در واقعیت مجازی کلیهٔ عناصر درک شده توسط کاربر، ساخته شده توسط کامپیوتر هستند. اما در واقعیت افزوده بخشی از اطلاعاتی را که کاربر درک می‌کند، در دنیای واقعی وجود دارند و بخشی توسط کامپیوتر ساخته شده‌اند.

فهرست مطالب

مقدمه

در این کتاب سعی شده است مباحثی را مطرح کنیم که کمتر به آن پرداخته شده است و نگاهی عمیق‌تر و دقیق‌تر به تکنولوژی بلاک‌چین و رمز ارزها داشته باشیم. ضمناً در این کتاب بیش از ده‌ها ابزار، سایت و صرافی‌های داخلی و خارجی معتبر جهت خرید و فروش ارزهای رمزنگاری شده معرفی شده است و نحوه استفاده از آن‌ها را بصورت تصویری آموزش داده‌ایم. این کتاب حاصل تحقیقات و پژوهش‌های علمی و عملی شرکت پیشرو آساک است. موضوع فعالیت شرکت در ابتدا طراحی و بهینه سازی سایت بود که به مرور حیطه‌های برنامه نویسی تحت وب، ویندوز و بعدها اندروید و آی او اس[۱] هم به آن اضافه شد. با توجه به اینکه رسالت اصلی شرکت پیشرو آساک تحقیق و پژوهش در زمینه‌های فناوری‌های مدرن و نوظهور است. تکنولوژی واقعیت افزوده[۲] و واقعیت مجازی[۳] هم به موضوعات پژوهشی شرکت افزوده شدند، و در زمینه فناوری واقعیت افزوده چندین پروژه به سفارش سازمان ها و شرکت‌های خصوصی و دولتی طراحی و به اجرا درآمده است. ضمنا این کتاب مبتنی بر فناوری واقعیت افزوده به نگارش در آمده است و شما می توانید با دانلود و نصب نرم افزار تحت موبایل که در بخش راهنمای استفاده از کتاب آمده است به ویدئوهای آموزشی دسترسی داشته باشید. در حال حاضر شرکت پیشرو آساک همزمان با انجام پروژه‌های مرتبط با فعالیت خود؛ مطالعات جدی

---

۱. iOS
۲. Augmented Reality
۳. Virtual Reality

بر روی تکنولوژی‌هایی همچون هوش مصنوعی[۱]، کلان داده ها[۲]، داده کاوی[۳]، اینترنت اشیا[۴]، بلاک چین[۵]، هش گرف[۶]، رادیکس[۷] و ... را با هدف بومی سازی و اجرایی نمودن دستاوردهای شرکت‌ها و استارتاپ‌های موفق دنیا در دستور کار دارد.

کتاب خودآموز کاربردی سرمایه گذاری در بیت کوین و سایر ارزهای رمزنگاری شده حاصل ساعت‌ها کار مطالعاتی و تجربه‌های فردی و گروهی است و علیرغم تلاش ما در تشریح تمام مطالب و مباحث برای افرادی که علاقه‌مند به ورود به بازار ارزهای رمزنگاری شده هستند، با این حال با توجه به گستردگی بازار ارزهای رمزنگاری شده، طبیعی است ایراداتی به کم و کیف کتاب وارد است و امید داریم با نقد و نظرات خوانندگان عزیز بتوانیم این ایرادات را در نگارش‌های بعدی برطرف سازیم. ضمناً با توجه به تحولات روزآمد بازار ارزهای رمزنگاری شده نسخه‌های بعدی این کتاب به تناسب بروزرسانی خواهد شد.

---

۱ Artificial Intelligence
۲ Big Data
۳ Data Mining
٤ Internet of Things
٥ Blockchain
٦ Hashgraph
۷ Radix

فصل اول

تکنولوژی بلاک‌چین (زنجیره‌ی بلوکی) چیست؟ و چگونه کار می‌کند؟

قبل از ورود به بازار ارزهای رمزنگاری شده باید تکنولوژی بلاک‌چین[۱] که به‌عنوان یک تکنولوژی انقلابی و زیرساختی برای ارزهای رمزنگاری شده عمل می‌کند را بهتر بشناسیم و نحوه عملکرد آن را بدانیم. شاید تاکنون نام بیت‌کوین یا ارزهای رمزنگاری شده[۲] به گوش شما خورده باشد. ارزش بیت‌کوین به عنوان اولین ارز الکترونیکی موفق، از سال ۲۰۰۸ تا کنون بیش از چندین هزار دلار رشد کرده است.

این ارز رمزنگاری شده در بستر تکنولوژی اعجاب انگیز بلاک‌چین (زنجیره بلوکی) معرفی و عرضه شده است که به عقیده کارشناسان اهمیت این فناوری به مراتب بیش از بیت‌کوین[۳] و دیگر ارزهای رمزنگاری شده مانند اتریوم[۴]، ریپل[۵]، بیت‌کوین‌کش[۶]، آیوتا[۷]، نئو[۸]، کاردانو[۹] و ... است و می‌توان از آن به‌عنوان یک انقلاب در عصر جدید یاد کرد. اگر تکنولوژی بلاک‌چین را به عنوان یک سیستم عامل تصور کنیم، بیت کوین را می‌توان به عنوان یک نرم افزار قابل نصب روی این سیستم عامل در نظر گرفت، بدین ترتیب می‌توان عظمت بلاک چین را نسبت به بیت‌کوین سنجید.

---

۱. Blockchain
۲. Cryptocurrencies
۳. Bitcoin
٤. Ethereum
٥. Ripple
٦. Bitcoin Cash
۷. IOTA
۸. NEO
۹. Cardano

۱-۱: معرفی تاریخچه تکنولوژی بلاک‌چین (زنجیره‌ی بلوکی)

احتمالاً بسیاری از افراد به‌جز آن‌هایی که به‌تازگی وارد این مبحث شده‌اند، اسم ساتوشی ناکاموتو[۱] را شنیده باشند. می‌دانیم که بیت‌کوین در بستری با عنوان تکنولوژی بلاک‌چین عرضه شد؛ اما تکنولوژی بلاک‌چین کمی قبل‌تر از ارائه بیت‌کوین، معرفی و خلق شد. پیشینه تکنولوژی بلاک‌چین به سال ۱۹۹۱ میلادی باز می‌گردد که دو نفر از دانشمندان رایانه‌ای به نام اسکات استورنتا[۲] و استوارت هابر[۳] این تکنولوژی را معرفی کردند. شاید تصور کنید که ساتوشی ناکاموتو اولین کسی بود که از فناوری بلاک‌چین و شبکه غیرمتمرکز توزیع شده برای خلق بیت کوین استفاده کرد، در حالی که این‌طور نیست. در اینجا به مواردی اشاره می‌کنیم که پیش از ساتوشی ناکاموتو ایده استفاده از ارزهای رمزنگاری شده و بهره‌مندی از فناوری غیرمتمرکز توزیع شده را اجرایی نمودند یا به عنوان سندی علمی منتشر کرده‌اند:

۱-۲: پول نقد الکترونیکی دیوید چام

دیوید چام[۴] فعال رمزنگاری در زمینه ارتباطات ناشناس، سیستم های رای گیری و ارزهای دیجیتال بود. او چندین رمزنگاری اولیه جدید همانند امضاهای کور و امضای گروهی را معرفی کرد. نظامی برای پرداخت‌های الکترونیکی ناشناس به نام پروتکل پول الکترونیکی پیشنهاد داد و شرکتی را برای تجاری سازی این فناوری تاسیس کرد. در سال ۱۹۸۲ سیستم پرداخت قابل ردیابی را بر اساس امضای کور[۵] پیشنهاد داد. این سیستم پرداخت اجازه می‌داد تا کاربران در به دست آوردن نشانه ناشناس از یک بانک اقدام کنند. هر نشانه مقدار ثابتی از پول را نمایندگی می‌کرد. در ابتدا، کاربر شماره سریالی کور را به بانک ارائه می‌کرد. پس از آن بانک، شماره سریال کور را امضا کرده به بانک ارائه می‌کرده و مقدار مربوطه را از حساب کاربر کم می‌کرد.

---

۱ Satoshi Nakamoto
۲. Scott Stornetta
۳. Stuart Haber
٤ David Chaum
٥ Blind Signature

این شماره سریال به صورت تصادفی توسط کاربر انتخاب شده بود و به بانک ابلاغ نمی‌شد. بدین ترتیب در زمان امضا زدن، بانک این شماره سریال را نمی‌دانست.

کاربر پس از آن می‌توانست نوار نشانه کور را خش داده و شماره سریال اصلی امضا شده توسط بانک را به دست آورد. شماره سریال امضا شده، نشانه‌ای است که می‌تواند توسط هر کسی در بانک امضا کننده، بازخرید شود. کاربر می‌تواند محصولات خود را از فروشنده خریداری کند و در عوض به فروشنده این نشانه را ارائه دهد. فروشنده پس از آن، نشانه رمزنگاری شده را به بانک ارائه می‌کند. بانک ابتدا صحت امضای نشانه را تایید می‌کند و سپس بررسی می‌کند که شماره سریال قبلا خرج نشده باشد (بانک، پایگاه داده‌ای را که حاوی شماره سریال‌های خرج شده است، نگهداری می‌کند) و در نهایت اعتبار حساب کاربری فروشنده را با مقدار موجود در نشانه شارژ می‌کند. (یا نشانه دیگر با نام تجاری جدید برای فروشنده صادر می‌کند).

برداشت کردن و خرج کردن شبیه هم نیستند. بانک نمی‌داند صاحب اصلی شماره سریال چه کسی بوده است زیرا شماره سریال را به صورت کورکورانه امضا کرده است. همه بانک‌ها می‌دانند که آیا این شماره سریال در گذشته استفاده شده است یا خیر. پیاده‌سازی اصلی سیستم‌های پرداخت غیر قابل ردیابی دیوید چام می‌تواند با دوبار خرج کردن[۱] یک وجه، تحت حمله قرار گیرد. صاحب یک نشانه می‌تواند آن را به دو فروشنده مختلف ارائه دهد. بنابراین این سیستم تنها می‌تواند به عنوان سیستم پرداخت آنلاین استفاده کرده و فروشنده قبل از پذیرش پرداخت، نشانه را باید با بانک بررسی کند.

پول نقد الکترونیکی[۲] پیشنهاد شده در شرکت چام و همکاران[۳] بهبودی بر سیستم است که برای انجام تراکنش های آفلاین پیشنهاد شده است. روش پول نقد الکترونیکی نیز انجام امضای کور است. با این حال کاربران شماره سریال تصادفی را به بانک ارسال نمی‌کنند، بلکه تکه

---

۱ Double-Spending
۲ Ecash
۳ Chaum et al. (۱۹۹۰)

داده ای که شامل شماره سریال تصادفی و نیز برخی از اطلاعات پنهان در مورد کاربر است، ارسال می‌کند. فروشنده وقتی نشانه پرداختی را دریافت کرد، به اطلاعات شناسایی در مورد کاربر دسترسی پیدا نخواهد کرد، اما اگر دو فروشنده نشانه پرداختی را دریافت کنند، این نشانه‌ها می‌توانند با یکدیگر ترکیب شده و هویت پنهان شخص خرج کننده آن را برملا سازند. بنابراین اگر کاربر تنها یک بار از نشانه استفاده کند، هویت او حفظ می‌شود. اما اگر از یک نشانه بیش از یک بار استفاده کند هویت او برملا خواهد شد. توجه داشته باشید، قبل از امضای نشانه، بانک بررسی می‌کند که اطلاعات شناسایی درست باشد؛ یعنی اطلاعات پنهان هویت واقعی کاربر را کامل نشان می‌دهد. طراحی پول نقد الکترونیکی اجازه می دهد در حالی که شماره سریال آشکار نیست، بانک به بررسی اطلاعات هویتی بپردازد. در نتیجه ویژگی عدم ردگیری برای کاربر از صادق حفظ خواهد شد. خلاصه‌ای از چگونگی کارکرد پول نقد الکترونیکی را می‌توان در فینی[۱] بیافت نمود.

فرآیند شناسایی متخلفان امیدوار بود تا کاربران را از دوبار خرج کردن یک وجه منصرف سازد، با این حال فرایند کشف و هویت یک فریبکار اگر قادر به دیدن مقدار زیادی از منابع مالی باشد، ممکن است به اندازه کافی بازدارنده نباشد. یا برخی از مهاجمین ممکن است، کیف پول کاربران قانونی را مورد حمله قرار داده و بارها و بارها مبالغ داخل کیف پول را خرج کنند. مقصر در این مورد، کاربری است که کیف پولش مورد حمله قرار گرفته است. مشکل دیگر پول نقد الکترونیکی این است که هر نشانه‌ای نشان دهنده مقدار ثابتی از پول است.

۱-۳: پول نقد هشی آدم بک[۲]

او در سال ۱۹۹۷ پول نقد هشی را به عنوان روشی برای محدود کردن هرزنامه پست الکترونیک[۳] معرفی کرد. پول نقد هش کش[۴] پیشنهاد اضافه کردن یک نشانه به نام «هش کش»

---

۱ Finney
۲ Adam Back
۳ Email
٤ Hashcash

به سربرگ[۱] پیام‌های ارسالی از پست الکترونیکی را داد. نشانه مزبور برای ایجاد، نیاز به هزینه های محاسباتی دارد. اما در فاز بررسی، هزینه ناچیز است. اضافه کردن یک نشانه به ایمیل ملاحظه های اقتصادی اسپمرها را تحت تاثیر قرار داده و آنها را مجبور به خرج مقدار قابل توجهی هزینه محاسباتی خواهد کرد. پول نقد هشی، سیستم پرداخت الکترونیکی نیست. با این حال احتمالاً نقشی الگویی برای ساخت بیت کوین توسط ساتوشی ناکاموتو را بازی می‌کرد. برای ایجاد یک نشانه هش کش، کاربر باید پازل رمزنگاری را حل کند. وی باید اقدام به پیدا کردن مقدار شمارنده نماید که وقتی آن به سربرگ اضافه می‌شود نتایج رشته هشی با تعداد معینی از بیت های صفر شروع شود. تعداد بیت ها با شروع صفر در مقدار هش، میزان سختی یافتن شمارنده را کنترل کرده و می‌تواند در نقطه ای دلخواه (جایی که در آن محاسبات هش کش برای کاربر قابل توجه نیست) تنظیم شود. اما این مقدار مانع از فعالیت اسپمرها می شود. این هزینه محاسباتی به طور معمول نیم ثانیه در هر ایمیل در یک رایانه معمولی است. برای پیدا کردن مقدار شمارنده خالق هش کش، فرستنده ایمیل با مقداری در شمارنده شروع شده و پی در پی آن را افزایش می دهد و در هر تکرار نتیجه تابع هش کش را محاسبه می‌کند تا زمانی که بتواند درجه دشواری مورد نیاز را حل کند.

هر نشانه هش کش خاص گیرنده بود به طوری که دریافت کننده می تواند اعتبار آن را بدون نیاز به شخص ثالث مورد اعتماد که باعث می شود پول نقد هشی غیر متمرکز شود، تایید کند. این نشانه همچنین ناشناس بوده و هر کسی می‌تواند یک نشانه هش کش معتبر را ایجاد کند و در نتیجه قابل مبادله خواهد بود. هر کسی با قدرت محاسباتی اختصاص داده شده می تواند نشانه های هش کش را بر حسب تقاضا تولید کند. در نتیجه، کاربران از نیاز به صرف قدرت محاسباتی خود جهب این کار آزاد می شوند. نوآوری اصلی معرفی شده توسط پروتکل پول نقد هشی تابع اثبات کار[۲] آن است. تابع اثبات کار بسیار کارآمد و به راحتی قابل تنظیم است و زیربنای دفتر توزیع تراکنش های بیت کوین را تشکیل داده است.

---

۱ Head

۲ Proof of Work (POW)

۱-٤: بیت گولد نیک زابو و بی مانی وی دای

در سال ۱۹۹۸ نیک زابو[۱] و وی دای[۲] به طور مستقل روش توزیع پول های دیجیتال به نام بیت گولد[۳] و بی مانی[۴] را ارائه نمودند. هیچکدام از پول های مزبور نیاز به سرور مرکزی برای عملکرد نداشتند و ایده اصلی پشت طرح، مانده حسابی بود که در پایگاه داده توزیع شده نگهداری می‌شد. در بی مانی پول با ارائه راه حلی برای یک مسئله سخت محاسبات، ایجاد می‌شود و تایید راه حل (یعنی یک گواهی تایید کار) نیز ساده است. مقدار پول ساخته شده متناسب با درجه سختی مسئله است. چگونگی تنظیم درجه سختی گواهی تایید کار، توسط شبکه و از طریق رای‌گیری، تصمیم‌گیری می‌شود. این سیستم در مقابل یک موجودیت واحد که با منابع محاسباتی زیاد اقدام به قطع کردن شبکه با مقدار زیادی از پول تازه ایجاد شده، قبل از اینکه شبکه فرصت پیدا کند درجه سختی را به روز رسانی کند، آسیب پذیر است.

در بیت گولد نیز پول با حل مسئله گواهی تایید کار به وجود می آید، با این تفاوت که گواهی تایید کار هر یک از مسائل به راه‌حل قبلی مرتبط شده و این موضوع باعث می‌شود ایجاد پول به صورت ترتیبی باشد. این به شبکه اجازه می‌دهد تا این فرصت را داشته باشد، سختی گواهی تایید کار را در مواقعی که رشد ایجاد پول در حال افزایش است، تنظیم کند. با این حال هیچ کدام از این طرح‌ها به طور کامل چگونگی توافق مشارکت شرکت کنندگان در رشد عرضه پول را پاسخ ندادند. کاربران توسط کلیدهای عمومی[۵] در هر دو طرح تبیین شده‌اند و یک کاربر می‌تواند منابع مالی را به کاربر دیگر با امضای پیام توسط کلید عمومی (بسیار شبیه به راهی که تراکنش‌های بیت کوین، کار انتقال را انجام می‌دهند.) انتقال دهد.

وی دای برای بی مانی قراردادهای لازم الاجرا را پیشنهاد داد که در آن شرکت کنندگان، وجوهی را ارسال کردند تا در حساب امانی توسط شبکه با هدف بازدارندگی قرار داده شود.

---

۱ Nick Szabo
۲ Wei Dai
۳ Bit Gold
٤ B-Money
٥ Public key

اگر قرارداد یا معامله با موفقیت اجرا شود و شرکا به توافق برسند، وجوه سپرده آزاد می‌شود اما اگر شرکت کنندگان در معامله به توافق نرسند، هر دو طرف، پیشنهادهای خود را برای استفاده از منابع مالی به حساب امانی ارسال کرده و گره‌ها در شبکه تصمیم می‌گیرند، چگونه اقدام به تقسیم وجوه حساب امانی کنند. البته در این پیشنهاد به جزئیات و چگونگی اجماع گره‌ها یا چگونگی مقابله با حمله های سیبل[۱] در شبکه اشاره نشده است. زابو از طرفداران اولیه قراردادهای هوشمند[۲] بوده و بسیاری از ایده های او در حال حاضر، در حال اجرا و پیاده‌سازی است. هر دو طرح مزبور مبتنی بر نام مستعار است که در آن نام مستعار، کلید عمومی کاربر است. هنگامی که تراکنش‌ها به طور عمومی در شبکه پخش می‌شود با استفاده از تجزیه و تحلیل شبکه به یکدیگر متصل می‌شود. بنابراین این طرح گمنامی کامل را همانند بیت‌کوین فراهم نمی‌کند.

در هر دو سیستم سرورها با یکدیگر ارتباط برقرار کرده تا پایگاه داده مشترک را حفظ کنند در نتیجه مشکل ژنرال بیزانس هویدا می‌شود. مسئله‌ی ژنرال بیزانس، یک مساله‌ی ذهنی در علوم کامپیوتر است. مشکل ژنرال بیزانس اشاره به مسئله‌ای است که در آن باید چند ژنرال بر روی یک استراتژی در صحنه نبرد توافق کرده و با توجه به جدایی فیزیکی شان از یکدیگر، باید با استفاده از قاصد با یکدیگر ارتباط برقرار کنند؛ در نتیجه قاصدها می‌توانند در بین راه اسیر شوند یا خائنی می‌تواند وجود داشته باشد تا به عمد، پیام اشتباهی را ارسال نماید. ژنرال‌های وفادار باید مسئله رسیدن به استراتژی مشترک را در محیطی که قاصدها می‌توانند به مشکل بر بخورند و خائنی وجود داشته باشد، حل کنند. در خصوص بی مانی و بیت گولد مسئله این است که چگونه شبکه می‌تواند بر روی حالت پایگاه داده توزیع شده، زمانی که هر دو پیام ها بین گره‌ها می‌تواند خراب بوده و ممکن است قاصد بکوشد، مانع از پایگاه داده توزیع شده

---

۱ وقوع حمله Sybil بدان معنی است که یک گره مخرب در شبکه هویت چند گره دیگر را جعل کرده و خود را به جای آنها جا بزند. این نوع حمله می‌تواند بر روی الگوریتم های مسیریابی، تراکم داده، رای گیری، اختصاص عادلانه منابع، تشخیص رفتار مشکوک و همچنین شکست مکانیزم ذخیره سازی در سیستم های توزیع شده تاثیرگذار باشد.

۲ Smart contracts

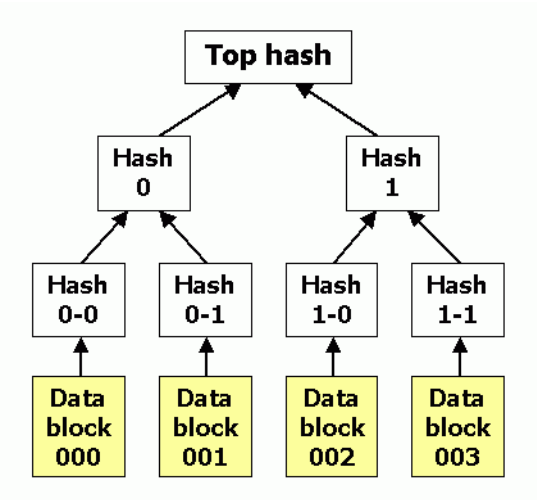
شود، توافق کنند. بی مانی مشکل ژنرال‌های بیزانس را پاسخ نداده است.
زابو در مقاله‌ای پیشنهاد داده است یک سیستم «حد نصاب بیزانس[۱]» که متکی بر رسیدن به حد نصابی از آدرس های شبکه است، توسط بیت گولد به عنوان پروتکلی برای پذیرش تغییرات در پایگاه داده توزیع شده مورد استفاده باشد. هر دو طرح پول های دیجیتال مزبور پیشنهادهای نظری را ارائه کردند ولی آنها در عمل اجرا یی نشده اند. با این حال بیت کوین به بسیاری از ایده های موجود در طرح های مزبور جامه عمل پوشانیده و جزئیات مهمی را حل کرده است.

۱-۵: پول نقد الکترونیکی ناشناس توماس ساندر و امنون

در سال ۱۹۹۹ توماس ساندر و امنون یک سیستم پول الکترونیکی ناشناس[۲] را پیشنهاد کردند که به سرور مرکزی صدور امضای کور نیاز نداشت. در سیستم ساندر و امنون[۳] یک سکه توسط هش شماره سریال خود ارائه می شود. همچنین لیستی از سکه های معتبر که توسط بانک نگهداری می شود توسط درخت مرکل[۴] ارائه شد به طوری که برای ذخیره سازی و انتقال بهینه بود. ریشه درخت مرکل به صورت عمومی ساخته شده و بانک آن را به شرکت کنندگان در سیستم مزبور می‌فرستاد. برای اثبات اینکه سکه متعلق به درخت است، تنها زنجیره ای از هش ها از برگ درخت (که در آن هش سکه وجود دارد.) به ریشه درخت مورد نیاز بود. زمانی که سکه های جدید به درخت اضافه می‌شود، ریشه به روز شده و دوباره به شرکت‌کنندگان ارسال می‌شود.

---

۱ Byzantine Quarum System
۲ Anonymous Electronic Cash
۳ Sander and Ts-shma's Auditable
۴ درخت‌های درهم سازی (Hash Tree) شاخه‌ای از فهرست‌های درهم‌سازی هستند. به این درخت‌ها درخت‌های مرکل (Merkle Tree) نیز می‌گویند. در رمزنگاری و علوم کامپیوتری، درخت درهم‌سازی نوعی از داده ساختارها هستند که شامل یک درخت که خلاصهٔ اطلاعات یک دادهٔ بزرگتر را در خود جای داده‌است و برای تشخیص محتویات آن داده به کار می‌رود.



شکل ۱: نمونه ای از درخت مرکل

طرح مزبور هنگامی که تراکنش ها به یکدیگر متصل نیستند به گمنامی کامل دست پیدا می کند. عملیات برداشتن نمی‌تواند به عملیات خرج کردن ارتباط داشته باشد. در مقایسه با سیستم های پرداخت ناشناس قبلی، این روش از اثبات با دانش صفر (اثبات دانایی صفر[۱]) به جای امضاهای کور استفاده کرده است؛ این باعث می شود این طرح از نظر قدرت محاسباتی و از نظر اندازه اطلاعات مورد نیاز برای ایجاد و تایید عملیات تا حدودی هم ناکارآمد باشد.

ساتوشی می توانست برخی از بینش های گمنامی موجود در روش مزبور را در بیت کوین تجمیع کند، اما معلوم نیست آیا او هنگامی که در حال انتشار بیت کوین بود از این طرح آگاه بوده است یا اینکه به دلیل هزینه محاسباتی بالا از ویژگی مزبور چشم‌پوشی کرده است یا حتی اینکه او آگاهانه تصمیم به ترک گمنامی مطلق در بیت کوین گرفته است.

---

۱ اثبات دانایی صفر (Zero Knowledge) یا پروتکل دانایی صفر در رمزنگاری روشی است که طرف (اثبات‌کننده) می‌تواند به طرف (تصدیق‌کننده) ثابت کند بیانیهٔ ارائه‌شده صحیح است. این روش فقط صحت بیانیه را تصدیق می‌کند و هیچ اطلاعات اضافه‌ای را بجز این حقیقت که بیانیه واقعاً صحت دارد ارسال نمی‌کند.

۱-٦: گواهی تایید کار قابل استفاده مجدد هال فینی

هال فینی[۱] گواهی تایید کار قابل استفاده مجدد[۲] را در سال ۲۰۰۴ معرفی کرد. این گواهی تعمیمی از پروتکل پول نقد هشی بوده که پیش از این درباره آن توضیح دادیم و در آن به جای ایجاد نشانه هش کش، دارای پیوند با آدرس ایمیل خاص است. مشتریان می توانند نشانه گواهی تایید کار را با انجام محاسبات گواهی تایید کار ایجاد کنند. گواهی تایید کار قابل استفاده مجدد از نشانه هش کش به عنوان سیستم گواهی تایید کار استفاده می کند.

نوآوری اصلی معرفی شده توسط فینی اجازه تبادل نشانه گواهی تایید کار را بدون نیاز به باز تولید دوباره آنها می‌دهد یک نشانه ابتدا توسط کاربری که گواهی تایید کار هش کش را انجام می دهد تولید می شود و زمانی که کاربر تصمیم می‌گیرد آن را خرج کند، آن را به کاربری دیگر (کسی که آن را در سرور گواهی تایید کار قابل استفاده مجدد بازخرید می کند تا نشانه جدید را علامت گذاری نماید) ارسال می‌کند. توجه داشته باشید زمانی که کاربری نشانه گواهی تایید کار را دریافت می کند باید آن را به سرعت به سمت سرور گواهی تایید کار قابل استفاده مجدد تغییر جهت داده و آن را برای نشانه گواهی تایید کار جدید، جهت جلوگیری از دوبار خرج کردن یک وجه، تبادل کند. بنابراین سیستم گواهی تایید کار قابل استفاده مجدد، نظامی آنلاین است. سرور گواهی تایید کار قابل استفاده مجدد اجازه استفاده مجدد ترتیبی از نشانه‌ها را داده و یک نشانه گواهی تایید کار جدید را زمانی که یکی از آنها به او ارائه شده باشد، دوباره صادر می کند.

سیستم گواهی تایید کار قابل استفاده مجدد وابسته به سرور مرکزی بوده و پایگاه داده ای با تمام نشانه های گواهی تایید کار را نگهداری می‌کند. این سرور قادر به ایجاد نشانه جدید نیست و تنها به صدور مجدد نشانه ها (زمانی که با نشانه های خرج نشده قبلی ارائه می‌شوند) می‌پردازد. فینی یک سرور گواهی تایید کار قابل استفاده مجدد را ایجاد کرده و آن را تحت

---

۱ Hal Finney

۲ Reusable Proof-Of-Work (PROW)

مجوز متن‌باز[۱] منتشر کرد. گواهی تایید کار قابل استفاده مجدد در سروری که شامل کمک پردازنده رمزنگاری شده است، تنظیم شده و اجازه تایید هویت از راه دور و با استفاده از تکنیک محاسبات قابل اعتماد انجام می دهد. کمک پردازنده رمزنگاری یک کپی از کلید خصوصی[۲] که هرگز کمک پردازنده را ترک نخواهد کرد، نگه داشته و می‌تواند از کلید خصوصی برای امضای کد هشی که بر روی سرور در حال اجراست، استفاده کند. کاربران بررسی می‌کنند که کد در حال اجرا در سرورکد منتشر شده و دستکاری نشده باشد. با این حال اگر مهاجم قادر به دریافت یک کپی از کلید خصوصی از تولیدکننده کمک پردازنده رمزگذاری شده باشد، می‌تواند به طور بالقوه سرور گواهی تایید کار قابل استفاده مجدد را با سروری که یک نسخه مخرب از کد در حال اجرا دارد (کسی که نشانه جدید را برای مهاجم ضرب کرده است) جایگزین کند. سرور می پندارد: «کسی که نشانه جدید را برای مهاجم ضرب کرده است در نهایت آفلاین شده و خدمات آن قطع خواهد شد.» جزئیات پروتکل گواهی تایید کار قابل استفاده مجدد را می توان در فینی یافت نمود و برای درک نحوه حضور اولیه فیینی در بیت کوین، مقاله گرینبرگ[۳] را مطالعه کنید.

در سال ۲۰۰۱ میلادی شخصی به نام برام کوهن[۴] از یک شبکه غیرمتمرکز همتا به همتا در ساخت یک سامانه[۵] به نام بیت تورنت[۶] استفاده کرد که در موضوع نقل و انتقال فایل‌ها روی بستر غیرمتمرکز همتا به همتا پایه ریزی شده بود که نمی‌توان گفت مشابه همان نسخه بلاک‌چینی بود که در سال ۱۹۹۱ معرفی شد، اما موضوع این بود که بیت تورنت که در حال حاضر نیز فعال است، اظهار داشت که ما می‌توانیم فایل‌های حجیم و سنگین را بدون نیاز به درگیری یک سرور مرکزی، روی بستر همتا به همتا منتقل کنیم.

---

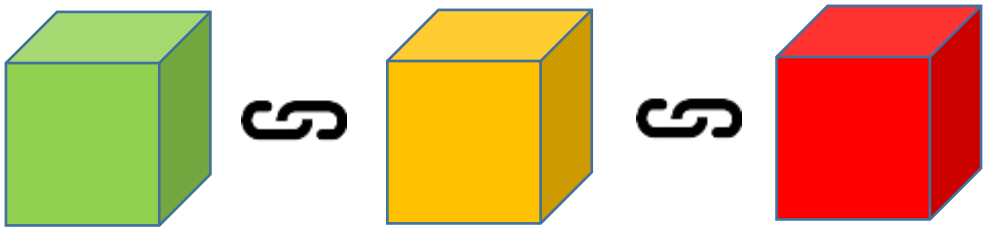
۱ Open Source
۲ Private Key
۳ Greenberg
٤. Bram cohen
٥ Platform
٦. Bittorrent

۱-۷: نرم افزار غیرمتمرکز همتا به همتا نقل و انتقال داده های حجیم بیت تورنت

بیت تورنت از تکنولوژی غیرمتمرکز همتا به همتا به منظور نقل و انتقالات داده‌ها استفاده کرد. همین مفهوم را ساتوشی ناکاموتو به شکل دیگری استفاده نمود. پیشنهاد او بهره‌گیری از تکنولوژی بلاک‌چین برای نقل و انتقالات بدون واسطه ارزش بود و اسم این ارزش را بیت‌کوین گذاشت. تکنولوژی بلاک‌چین به خودی خود قدرتمند بوده و دارای محاسن خیلی زیادی است و می‌تواند آینده نقل و انتقالات دارایی‌های دیجیتال، دیتا و سایر ابعاد زندگی بشری را متحول و با یک انقلاب مواجه کند. اکنون خیلی از استارت‌آپ‌های موفق دنیا روی بلاک‌چین مطالعه می‌کنند. به عقیده صاحب نظران فناوری بلاک چین جزو ۱۰ فناوری برجسته در قرن ۲۱ می باشد و از بسیاری جهات حائز اهمیت است. توجه داشته باشید که فناوری بلاک‌چین به‌مراتب از بیت‌کوین و سایر ارزهای رمزنگاری شده[۱] مهم‌تر است.

۱-۸: تکنولوژی بلاک‌چین چگونه کار می‌کند؟

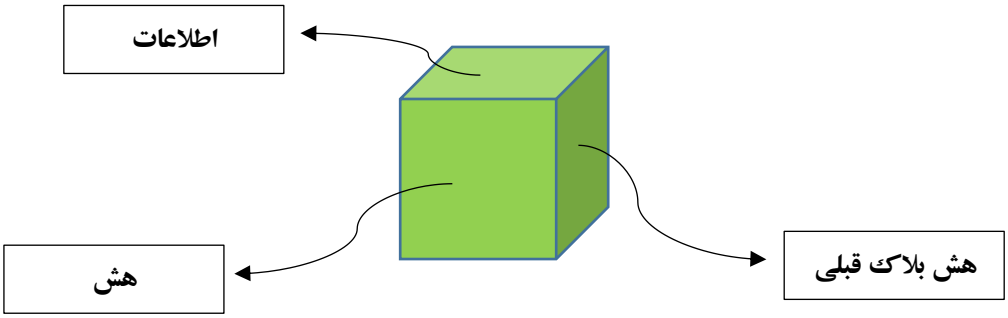
در این بخش به‌صورت خلاصه و مفید نحوه عملکرد تکنولوژی بلاک‌چین توضیح خواهیم داد. بلاک‌چین از دو کلمه «بلاک» و «چِین» ساخته می‌شود. بلاک همان بلوک است و چِین هم به معنای زنجیره است که معادل فارسی آن به معنای زنجیره‌ی بلوکی است. در تصویر زیر سه بلوک مشاهده می‌شود که با دو زنجیر (اتصال) به هم وصل شده‌اند و یک زنجیره‌ی بلوکی را تشکیل داده‌اند.



شکل ۲: تصویر شماتیک یک زنجیره ی بلوکی

۱ Cryptocurrency

همه این زنجیرها (اتصال‌ها) رمزنگاری شده هستند. اما بلوک‌ها حاوی چه اطلاعاتی هستند؟ همان‌طوری که گفته شد بلاک‌چین اولین بار سال ۱۹۹۱ معرفی شد و سال ۲۰۰۹ توسط ساتوشی ناکاموتو از این تکنولوژی برای اختراع بیت‌کوین استفاده شد و بدین ترتیب این ارز رمزنگاری شده معرفی شد. شرکت‌های حقوقی دفتری به اسم دفتر کل دارند. در این دفتر، کل دخل و خرج‌ها، بدهی‌ها و بستانکاری‌ها خود را در آن وارد می‌کنند و در انتهای سال برای محاسبه مالیات در کنار ارائه اظهارنامه سالیانه این دفتر کل را نیز ارائه می‌دهند. تصور کنید این دفتر کل برای تمامی تراکنش‌هایی که تابه حال در شبکه بلاک‌چین بیت‌کوین اتفاق افتاده وجود دارد اما این دفتر کل دست یک شخص یا سازمان مرکزی نیست، بلکه دفتر کل به‌صورت غیرمتمرکز بین افرادی حاضر در شبکه توزیع شده است. یعنی هر یک از این افراد یا گره‌ها یک نسخه برابر اصل این دفتر کل را نزد خود نگهداری می‌کنند. حالا تصور کنید که شما هم یکی از این گره ها هستید و یک دفتر کل دارید و باید تمامی تراکنش‌های بیت‌کوین را در آن ثبت کنید. هر بلاک شامل سه بخش است: اطلاعات، هَش[۱] و هَش بلاک قبلی[۲] (شکل ۳)؛

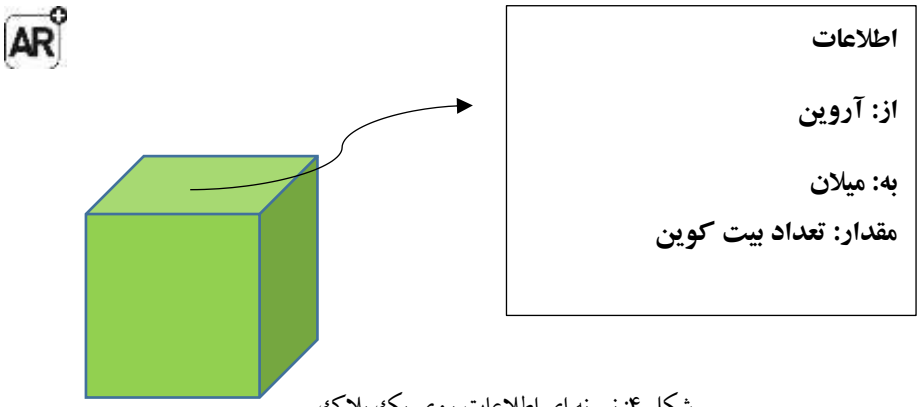


شکل ۳: تصویر شماتیک یک بلاک و محتویات آن

اما اطلاعات روی هر بلاک شامل: تعداد بیت‌کوین، ارسال کننده و دریافت کننده (شکل ۴) می‌باشد.

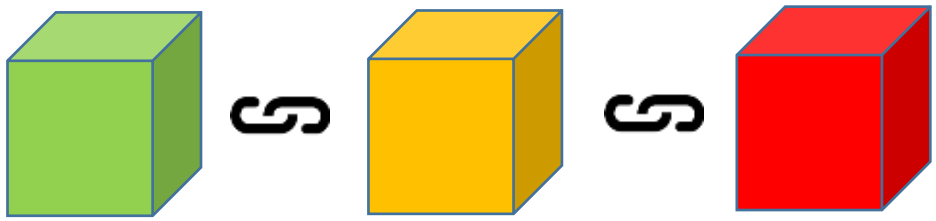
---

۱ Hash
۲ Hash of Previous Block



شکل ۴: نمونه ای اطلاعات روی یک بلاک

افراد در شبکه بلاک‌چین پشت یک آی‌دی پنهان هستند، شبیه به یک شماره کارت بانکی که برای انتقال پول از آن استفاده می‌کنید. اما نکته اینجاست که هویت شما از طریق شماره ۱۶ رقمی روی کارت شتابی قابل شناسایی است و مالکیت آن کارت مشخص است، چون قبلاً در بانک صادرکننده کارت، اطلاعات خود را جهت افتتاح حساب ارائه کرده‌اید. اما در شبکه غیرمتمرکز بلاک‌چین، مالکیت آی‌دی افراد پنهان است.



شکل ۵: نحوه ارتباط بین بلاک ها در یک زنجیره ی بلوکی

مورد بعدی هَش است. هَش به نوعی شبیه یک اثر انگشت عمل می کند و یک نشانه شامل اعداد و حروف است که منحصر به فرد بوده و تکراری نیست. طریقه ساخت این هَش‌ها طبق یک سری الگوریتم‌های پیچیده ریاضی انجام می‌شود که کاملاً بدون اشتباه عمل می‌کند. وجه سوم یک بلاک، هَشِ بلوکِ قبلی است. یک زنجیره زمانی ساخته می‌شود که یک بلوکی که در

اینجا بلوک سبز است قبل از یک بلوک دیگری قرار گیرد و همین‌طور این بلوک‌ها به‌صورت زنجیروار به هم متصل‌اند. هرکدام از این بلوک‌ها، بلوک یک، دو و سه شامل هَش و هَش متعلق به بلوک قبلی است. اگر دقت کنید هَش بلوک سه یا همان بلوک سبز، ۱Z۸F است. (البته این هش‌ها بلندتر از این اعداد و ارقام هستند و فقط برای نمونه این هش به‌صورت مختصر آورده شده است) هش بلوک قبل در بلوک سوم (قرمز) با هش بلوک دوم (زرد) یکی است و همچنین هش بلوک قبل روی بلوک دوم (زرد) با هش بلوک اول (سبز) یکسان است.

به کمک هش بلوک قبلی، هر بلوک به‌نوعی مؤید بلوک قبلی است و این به‌صورت زنجیروار در شبکه صادق است؛ اما نکته اینجاست در مورد بلوک اول چون بلوک قبل از آن وجود ندارد بنابراین هَش بلوک قبلی نیز وجود ندارد و به همین علت اصطلاحاً به آن بلوک پیدایش یا بلوک ریشه[۱] می‌گوییم. ولی بعد از آن همه‌ی بلوک‌ها شامل این سه شاخص دیتا، هَش و هَش قدیم هستند. اگر کسی بخواهد این زنجیره را مختل، هک یا دست‌کاری کند، مجبور است که هَش بلوک دو را دست‌کاری کند و یک هَش دیگر را معرفی کند اما نکته اینجاست که این هَش جدید با بلوک بعدی همخوانی ندارد، بنابراین از اعتبار ساقط است. چون هَش باید تغییر کند تا هکر بتواند به این بلوک که شامل یک سری تراکنش و دیتا است، دسترسی پیدا کند و مثلاً به‌جای اطلاعات دریافت کننده، آدرس کیف پول خود را وارد کند؛ برای این کار مجبور است هَش این بلوک را تغییر دهد. برای این منظور هکرها باید کنترل بیش از ۵۰ درصد از شبکه را داشته باشند تا بتوانند در آن دخل و تصرف کنند که به اصطلاح به آن حمله ۵۱ درصد[۲] گفته می شود. این کار مستلزم صرف هزینه های بسیار هنگفتی است که تقریبا انجام آن توسط افراد و یا گروه های مختلف غیرممکن است (دقت داشته باشید که از کلمه تقریبا استفاده شده است.) بسیاری از افراد تصور می‌کنند چون ساتوشی ناکاموتو این سیستم را خلق کرده است، اگر هویت او نیز فاش شود، احتمالا خود شبکه بیت کوین هم تحت الشاع قرار می گیرد. واقعیت امر این است که بیت‌کوین ارزی است که به‌صورت منبع باز طراحی

---

۱ Genesis Block
۲ Attack %۵۱

شده است. اما چرا؟

سیستم عامل لینکوس[۱]، اندروید[۲]، وردپرس[۳] و بسیاری دیگر از سیستم‌های مدیریت محتوا[۴] منبع‌باز ارائه شده‌اند، به این دلیل که توسعه‌دهندگان و برنامه‌نویس‌ها بتوانند آن ها را ارتقا دهند، ایرادات عملکردی و امنیتی را برطرف کنند و امکانات جدیدی را به آن ها اضافه کنند. زمانی که سند علمی (شفاف نامه) بیت کوین توسط ساتوشی ناکاموتو در سال ۲۰۰۸ معرفی شد، این توسعه دهندگان بودند که راه او را ادامه دادند. اگر ساتوشی ناکاموتو طبق ادعای خود از سال ۲۰۱۱ دیگر روی بیت‌کوین و بلاک‌چین کار نمی کند و به موضوع جدیدی می پردازد و ارتباط خود را با توسعه‌دهندگان هسته اصلی بیت کوین[۵] قطع کرده باشد با اینحال منتظر اتفاق خاصی برای شبکه نباشد، چون بیت کوین با و یا بدون ساتوشی ناکاموتو نیز همچنان مسیر خود را می‌رود.

هر بلوک جدیدی در بیت‌کوین، حدود ده دقیقه زمان می برد. این شبکه را در اصل سازمان‌ها و سرورهای مرکزی نظارت نمی‌کنند، بلکه یک سری سرورهای غیرمتمرکز توزیع شده در شبکه اینترنت هستند که آن را مدیریت می‌کنند و البته مدیریت به معنی نظارت کردن و حفظ کردن امنیت شبکه است نه دست‌کاری در آن. شما تمامی تراکنش‌هایی که از ابتدای پیدایش بیت‌کوین تا اکنون انجام شده است را می‌توانید در مرورگرهای مربوط به شبکه مشاهده کنید اما قادر نیستید، هویت افراد را از آن استخراج کنید.

اما زمانی که یک بلوک جدید ساخته می‌شود، در صورتی تأیید می‌شود که تمامی افراد (گره‌ها یا اتصالات) بلوک جدید را تأیید کنند یعنی چون همه‌ی این افراد یک کپی از آن دفتر کل را در اختیار دارند زمانی که همه‌ی اطلاعات، هَش و هَش بلوک قبلی مورد تأیید است و هیچ مشکلی وجود ندارد، آن را به زنجیره متصل می‌کنند.

---

۱ Linux
۲ Android
۳ Wordpress
٤ Content Manager System (CMS)
٥ Bitcoin Core