
بسم الله
الرحمن
الرحيم

راهنمای بیت‌کوین

نگاهی به شیوه‌های دریافت، سرمایه‌گذاری و پرداخت اولین ارز رمزنگاری شده غیرمتمرکز جهان

راه پرداخت

سرشناسه: دی مارتینو، یان، DeMartino ،Ian/ عنوان و نام پدیدآور: راهنمای بیت کوین: نگاهی به شیوه‌های دریافت، سرمایه‌گذاری و پرداخت اولین ارز رمزنگاری شده غیر متمرکز جهان/ یان دی مارتینو؛ مترجم پیمان رحمانی، احمد میرادامادی، رضا قربانی؛ ویراستار یلدا شایسته‌فر. / مشخصات نشر: تهران: امین الضرب، ۱۳۹۶/ مشخصات ظاهری: ۳۰۴ ص./ شابک: ۱-۲۹-۹۹۷۷-۶۰۰-۹۷۸/ وضعیت فهرست نویسی: فیپا/ یادداشت: عنوان اصلی: The Bitcoin Guidebook: How to Obtain, Invest, and Spend the World's First Decentralized Cryptocurrency. / موضوع: بیت کوین/ موضوع: Bitcoin/ موضوع: انتقال الکترونیک وجوه/ موضوع: Electronic funds transfesr/ موضوع: رمزنگاری/ موضوع: Cryptography/ موضوع: پول/ موضوع: Money/ شناسه افزوده: میرادامادی، احمد، ۱۳۴۸ -، مترجم/شناسه افزوده: قربانی، رضا، ۱۳۶۳ -، مترجم/ رده‌بندی کنگره:/۱۳۹۶ ۲ر۹د/ HG۱۷۱۰/ رده‌بندی دیویی: ۳۳۲/۴۰۴/ شماره کتابشناسی ملی: ۵۰۵۷۱۹۵.

بیت کوین

راهنمای بیت کوین

نگاهی به شیوه‌های دریافت، سرمایه‌گذاری و پرداخت اولین ارز رمزنگاری شده غیرمتمرکز جهان

یان دی مارتینو
ترجمه: احمد میردامادی
رضا قربانی و پیمان رحمانی

راه پرداخت

راهنمای بیت کوین (نگاهی به شیوه‌های دریافت، سرمایه‌گذاری و پرداخت اولین ارز رمزنگاری شده غیر متمرکز جهان)/ ناشر: رضا قربانی/ مؤلف: یان دی مارتینو/ مترجم: احمد میردامادی، رضا قربانی و پیمان رحمانی/ ویراستار: یلدا شایسته‌فر/ صفحه‌آرا: ایمان شاه‌سمندی/ مدیر تولید: رسول قربانی/ نوبت چاپ: اول- ۱۳۹۶/ شمارگان: ۱۰۰۰ نسخه/ شابک: ؟-؟؟-؟؟؟؟-؟؟؟-؟؟؟/ لیتوگرافی: شادرنگ/ چاپ و صحافی: شادرنگ/ تمام حقوق این اثر محفوظ و متعلق شبکه راه پرداخت است/ نشانی انتشارات: تهران، جنت‌آباد جنوبی، پایین‌تر از میدان چهارباغ، نبش کوچه نوبختی، پلاک ۱، طبقه ۳، واحد ۴/ تلفن: ۰۹۱۰۶۹۴۹۳۰۲/ دورنگار: ۸۹۷۸۴۹۰۲/ پست الکترونیک: mediamanager.ir@gmail.com/ پایگاه اینترنتی: Way2Pay.ir

فهرست

تقدیم به:

پدر، مادر و همسر عزیزم

و به تمام آزادمردانی که نیک می‌اندیشند و عقل و منطق را پیشه خود کرده و جز رضای الهی و پیشرفت و سعادت جامعه، هدفی ندارند.

مطمئنا در این مسیر سخت و طولانی، اگر حمایت‌های شما نبود، هیچ‌وقت امکان پیشرفت و جایگاه فعلی برایم فراهم نمی‌شد، با تمام وجودم و احساسم از شما تشکر می‌کنم و این ترجمه به سرانجام نمی‌رسید؛ مگر با حمایت‌های خانواده‌ام که در ثانیه‌ثانیه لحظات سخت و آسان در کنارم بودند.

همچنین تشکر ویژه‌ای دارم از خانم دکتر شادی ترکیان، به‌دلیل یاری‌ها و راهنمایی‌های بی‌چشمداشت ایشان که بسیاری از سختی‌ها را برایم آسان‌تر کردند، مهندس کامبیز رستگار و مهندس رضا حسن‌پور شمس که در طول ترجمه این کتاب کمک‌های شایانی انجام داده و از ارکان اصلی و از حمایت‌کنندگان اصلی من در طول این مسیر بوده‌اند.

تقدیم به پسرانم سام و رایان عزیزم
پیمان رحمانی

به عبارت دیگر

«می‌خواهم از دریاچه کوچکی بگذرم. واقعا کوچک است، با این حال ساحل روبه‌رو در نظرم بسیار دور می‌آید، فراتر از توانم. می‌دانم وسط دریاچه بسیار عمیق است. با اینکه شنا بلدم، می‌ترسم تنها و بی‌تکیه‌گاه وسط آب گیر بیفتم.» این اولین پاراگراف کتابی است به نام «به عبارت دیگر» نوشته جومپا لاهیری. لاهیری هندی‌تبار است و در آمریکا زندگی می‌کند و سال‌ها به زبان انگلیسی کتاب نوشته است. حوالی ۵۰ سالگی، بعد از حدود ۲۰ سال شکست در آموختن زبان ایتالیایی، او کتابی به زبان ایتالیایی می‌نویسد که نامش را هم گذاشته «به عبارت دیگر». او برای رسیدن به این آرزوی دیرینه، بیشتر از دو سال در ایتالیا زندگی کرده و به این زبان نوشته و صحبت کرده و سخت‌تر از همه تلاش کرده به این زبان فکر کند. نوشتن به خارجی و فرار کردن از قفس تنگ مخاطب وطنی احتمالا رویای بسیاری از نویسنده‌های جهان است.

۳- بیت کوین همان زبان دیگر است. همان‌قدر که یاد گرفتن زبان دیگر برای ما سخت است، باید بدانیم که فهمیدن بیت کوین هم آسان نیست. اگر بخواهیم بیت کوین را با همان منطقی که تا پیش از این با آن پول‌های معمولی را درک می‌کردیم، بفهمیم، شکست می‌خوریم. برای درک بیت کوین لازم است اساسا با منطق دیگری به ماجرا نگاه کنیم. برای درک بیت کوین باید در آن زندگی کنیم. نمی‌توانیم کنار ساحل بنشینیم و انتظار

داشته باشیم آن را درک کنیم. نمی خواهم از بیت کوین مثبت بگویم یا از آن منفی بگویم. حرفم این است که باید بیت کوین را درک کنیم؛ پیش از اینکه بخواهیم عاشقش باشیم، یا دشمن آن.

۴- این کتاب حاصل همکاری افرادی اســت که تلاش کرده‌اند دل به آب بزنند. شاید این یک دریاچه کوچک باشد، با چشم‌انداز ساحلی که دور به نظر می‌آید، منتها لذتی که در تن به آب زدن هست، در هیچ چیز دیگری نیست. قدردان احمد میردامادی، پیمان رحمانی، یلدا شایسته‌فر، ایمان شاه‌سمندی، رسول قربانی، قاسم سرافرازی، مینا والی و بقیه کسانی هستم که در این کار با من همکاری کردند و امیدوارم نتیجه کار رضایت‌بخش شده باشد. امیدوارم بتوانیم با دوستانم در این مسیر استوار بمانیم و محتوای به‌دردبخور تولید کنیم.

یا حق
رضا قربانی
مدیرعامل شبکه راه پرداخت

پیش‌گفتار مترجم

پیتر دراکر (پدر مدیریت نوین) یک سوال ساده و اعجاب‌آفرین را مطرح می‌کند؛ اینکه در دنیای کسب‌وکار چه کارهایی نباید کرد؟ شاید ساده‌ترین پاسخ به این پرسش این است که لااقل باید از اشتباه کردن و تکرار اشتباه خودداری کنیم، اما واقعیت این است که در دنیای تجارت نوین در موارد مکرری در این باره با دشواری روبه‌رو شده‌ایم. در حوزه بانکداری دیجیتال و در دوره روش‌های مدرن پرداخت الکترونیکی، اگر نوآوری نداشته باشیم یا از رویکردهای نوآورانه گریزان باشیم، به مخمصه خواهیم افتاد؛ به نظر می‌رسد لااقل در دو حوزه، بی‌تدبیری می‌تواند مشکل‌آفرین‌تر باشد؛ اول حوزه ارزهای رمزنگاری‌شده مجازی و دیگری پرداخت همراه.

از اشکالاتی که مکرر را در موارد مشابه به آن برخورده‌ایم، این اســت که هرگاه فناوری نوینی پا به عرصه می‌گذارد، با مقاومت بخش‌هایی روبه‌رو می‌شود که متکی بر ابزارهای پیشین و فرایندهای کهنه‌اند؛ همچنین گاهی بدفهمی‌ها سبب می‌شود با نوآوری‌ها به‌شدت برخورد شود.

درباره ارزهای رمزنگاری‌شــده مجازی، نبود مرجع کنترل متمرکز که شــاید بزرگ‌ترین نقطه قوت این ارزهاست، می‌تواند با فهم نادرست و برخورد اشتباه به پاشنه‌آشیل آن تبدیل شود؛ به‌ویژه آنکه این ارزها ابزار

پرداخت بی‌واسطه و بدون محدودیت را محقق می‌کنند و فقدان‌شان می‌تواند خلاء جدی برای نوآوری‌های پیشران اقتصاد ایجاد کند.

در حوزه پرداخت همراه نیز نبود سیاست مشخص و مطمئن و فقدان راهکاری که به نیازهای بازار پاسخ دهد، سبب سردرگمی و تشتت در بازار شده است و امروزه هر اپلیکیشنی در نبود یک کیف پول متمرکز برای خود کیف پولی ساخته و در این ماجرا همچنان متهم ردیف اول، نهادهایی هستند که مانع ایجاد یک کیف پول ملی برای پرداخت‌های آنلاین و آفلاین شده‌اند.

بد نیست در پایان نکته تامل‌برانگیز پیتر سنکه (استاد تجارت مدرن) را مرور کنیم: «بیست یا سی سال آینده را تصور کنید، انتظار نمی‌رود روزگار پیش‌رو آرام‌تر از بیست سال گذشته باشد، بی‌گمان یک چیز مقطعی است، چالش‌های پی‌در‌پی توان ما را خواهند گرفت و اگر در شیوه کارهایمان تجدیدنظر نکنیم، همچنان دچار مخمصه خواهیم بود.»

باور دارم که این کتاب در کاهش اشتباهات و برداشت‌های نادرست از مفهوم ارزهای رمزنگاری‌شده مفید خواهد بود و امید دارم با تکیه بر تجارب سال‌های دور و نزدیک اشتباه (یا اشتباهات) را تکرار نکنیم که این بار خسارت بسی فزون‌تر و فرصت‌سوزتر خواهد بود؛ آن‌هم در شرایطی که جامعه به اقتصادی پویا و فرصت‌آفرین نیاز دارد!

پیش‌گفتار نویسنده

این اولین کتاب من است و به همین دلیل، ادعا نمی‌کنم به چیزهایی که قرار است در اینجا مورد بحث قرار گیرند، اشراف کامل دارم. تنها چیزی که می‌دانم این است که وقتی می‌خواهید کتابی بنویسید، باید بدانید که مخاطبین کتاب شما چه کسانی هستند. این موضوع، در مورد نوشتن هر چیزی صدق می‌کند، اما به‌طور قطع، در مورد کتاب‌هایی که طول کلمات آنها بیش از ۸۰ هزار لغت است، شناخت مخاطب، اهمیت بیشتری خواهد داشت. هیچ‌کسی دوست ندارد که بعد از مدت‌ها تلاش، نتیجه کارهایش هدر برود. به همین دلیل، زمانی را به این موضوع اختصاص دادم که قرار است در این کتاب به چه موضوعاتی پرداخته شود. از ابتدا هم قرار نبود تا وارد فاز برنامه‌نویسی شوم. من برنامه‌نویس نیستم و به‌طور قطع، یک برنامه‌نویس، مفاهیم لایه‌های پایین‌تر بیت‌کوین را بهتر از من درک می‌کند. اگر برنامه‌نویس هستید، کتاب «مهارت در بیت‌کوین: گشودن رمز و راز ارزهای رمزنگاری شده دیجیتال»[1]، نوشته آندریاس آنتونوپولوس، اطلاعات بسیار بهتری را در اختیار شما قرار خواهد داد. نکته بعدی این است که سرمایه‌گذاران نیز مد نظر این کتاب نیستند. درآمد قابل تصرف من هرگز آنقدر زیاد نبوده است که به‌صورت جدی، به دادوستد یک‌روزه ارزهای رمزنگاری شده فکر کنم. کتاب‌های الکترونیکی زیادی از طرف سرمایه‌گذاران وال‌استریت و افراد درگیر در خرید و فروش یک‌روزه بیت‌کوین، منتشر شده‌اند که تجربیات آنها در این حوزه، خیلی بیشتر از من است.

قبل از شروع نگارش جدی این کتاب، تصمیم گرفتم مطالعاتی را در رابطه با بیت‌کوین انجام دهم و به همین دلیل، کتابی را که در سال ۲۰۱۲ در مورد بیت‌کوین نوشته شده بود، انتخاب کردم.

به‌دنبال کتابی بودم که توضیحاتش در مورد بیت‌کوین، برای من قابل فهم باشد و در عین حال، نقاط ضعف و قوت ارزهای رمزنگاری شده را برای من روشن کند. به نظر می‌رسید که طرفداران دوآتشه بیت‌کوین، جنبه‌های منفی آن را از دید دیگران مخفی کرده‌اند و به همین دلیـــل می‌خواهم در این کتاب، همه چیزهای مربوط به بیت‌کوین را برای خواننده بیان کنم.

در این مسیر، کتابی به نام «بیت‌کوین: حقیقت محض در مورد بیت‌کوین»[۲]، برخی از این موضوعات را پوشش می‌داد، اما نسبتا کوتاه بود و به‌جای آنکه نگاه صریح و صادقانه‌ای به موضوع داشته باشد، به‌صورت ایدئولوژیک به آن می‌پرداخت و ایرادات زیادی داشت.

در اینجا، از گفتن چیزهای بد در مورد بیت‌کوین، ابایی نداریم، ولی در عین حال، نقاط قوت آن را نیز نادیده نخواهیم گرفت. هدف من این است که خواننده، بعد از پایان مطالعه این کتاب، بتواند در مورد فوت‌وفن‌های بیت‌کوین، از گذشته تا حال و آینده آن، با دیگران بحث کند. خواندن کتاب پیش رو، شما را به فاز برنامه‌نویسی سرویس بیت‌کوین وارد نمی‌کند، بلکه به شما این توانایی را می‌دهد تا وقتی شخصی در یک میهمانی شام، این موضوع را مطرح کرد، بتوانید پا به پای او، در بحث شرکت کنید. ادعا نمی‌کنم که مطالعه کتاب، باعث اشراف کامل شما در مورد همه ابعاد بیت‌کوین شود. در عوض، هدف من آن است تا شما را به فردی همه‌کاره در زمینه بیت‌کوین تبدیل کنم. پس از مطالعه کتاب، درک شما از بیت‌کوین، نحوه استفاده از آن و خاستگاهش بیشتر می‌شود و از مسیر حرکت بیشتر در این حوزه، آگاهی پیدا می‌کنید.

با این حال، اکنون که کتاب پیش رویتان قرار دارد، از اینکه زمانی را به مطالعه آن اختصاص می‌دهید، از شما تشکر می‌کنم و امیدوارم اطلاعات آن، کمک مفیدی را در اختیارتان قرار بدهد.

رفع مسئولیت: اگرچه تلاش من بر این بوده است تا کتاب پیش رو تا حد امکان دقیق باشد، اما ارزهای رمزنگاری شده، مفاهیم پیچیده‌ای هستند که دائما مسیر رشد و توسعه را پشت سر می‌گذارند. بنابراین، لازم می‌دانم تا در همین ابتدای کار، مواردی را ذکر کنم: از تحقیق در این زمینه، دست برندارید، زیرا همه چیز، ماه به ماه و هفته به هفته در حال تغییر است. همچنین در مورد مشروعیت شرکت‌های ذکرشده در این کتاب نیز ادعایی ندارم، زیرا ممکن است موقعیت آنها هر لحظه دستخوش تغییر شود.

کلیدواژه‌ها

altcoin: معادل فارسی آن، آلت‌کوین است و مخفف عبارت «Alternative Cryptocurrency» به معنای «ارز رمزنگاری شده جایگزین» است. آلت‌کوین، ارز رمزنگاری شده دیگری مشابه با بیت‌کوین است. در حال حاضر، بیش از هزار آلت‌کوین وجود دارند. اکثر آنها، رونوشت (کپی)های کاملا دقیق ارزهای رمزنگاری شده موفق‌تر به‌شمار می‌روند، اما برخی از آنها نیز ایده‌های کاملا جدیدی محسوب می‌شوند.

ASIC: مخفف عبارت «Application-Specific Integrated Circuit» به معنای «مدار مجتمع با کاربرد خاص» است. ASIC، به قطعه سخت‌افزاری‌ای اشاره دارد که تنها و تنها برای انجام یک کار، طراحی شده است. در دنیای ارز رمزنگاری شده، ASIC، به یک الگوریتم خاص، مثل SHA256 و Scrypt، اشاره می‌کند.

BFGMiner: دومین نرم‌افزار محبوب استخراج بیت‌کوین است.

Bitcoin/bitcoin: معادل فارسی آن، بیت‌کوین است. Bitcoin با حرف بزرگ انگلیسی، به سیستم، شبکه یا ارز بیت‌کوین، به مفهوم کلی آن اشاره می‌کند، اما bitcoin با حرف کوچک انگلیسی، به بیت‌کوین‌های مجزا اشاره دارد، مثل اینکه بگوییم «من پنج بیت‌کوین دارم».

Bitcoin-Qt : نام دیگر آن هسته بیت‌کوین[۳] است که به پیاده‌سازی اولیه بیت‌کوین اشاره دارد و پایه و اساس همه کیف پول‌ها و سرویس‌ها را تشکیل می‌دهد.

Bitcoin XT: پیاده‌سازی جایگزینی برای هسته بیت‌کوین است که با پیاده‌سازی اصلی فعلی بیت‌کوین سازگار است و ابتدا توسط گوین آندرسن و مایک هیرن مطرح شد. از این نرم‌افزار، برای تست ویژگی‌های جدید استفاده می‌شود و دلیل مطرح شدن آن به عدم توافق بر سر اندازه بلوک در Bitcoin-Qt بر می‌گشت. اپلیکیشن فوق‌الذکر، بلوک‌های با اندازه ۲۰ مگابایت را به‌عنوان یک ویژگی اولیه، معرفی کرد.

block: معادل فارسی آن بلوک است. تراکنش‌های موجود در زنجیره بلوک، به بلوک‌های مختلفی تقسیم می‌شوند و این بلوک‌ها، تقریبا هر ۱۰ دقیقه، توسط استخراج‌گرها، تایید می‌شوند. در حال حاضر، اندازه آنها به یک مگابایت محدود می‌شود، اما احتمالا در آینده نزدیک تغییر خواهد کرد.

blockchain: معادل فارسی آن، زنجیره بلوک است. زنجیره بلوک، دفتر کلی غیر متمرکز به‌شمار می‌رود که مبنای کار بیت‌کوین است. هر تراکنش و حساب، از طریق این دفتر کل، ردیابی خواهد شد. این نام را با نام وبگاه Blockchain.info یا شرکت Blockchain، اشتباه نگیرید. این عبارت، به هر فناوری جدیدی که از یک دفتر کل برای ردیابی ارزش دیجیتال استفاده می‌کند نیز اشاره دارد.

block explorer: معادل فارسی آن، کاوشگر بلوک است. کاوشگر بلوک، به یک وبگاه یا قطعه نرم‌افزاری اشاره دارد که امکان مشاهده و دنبال کردن تراکنش‌های بیت‌کوین را از طریق زنجیره بلوک، فراهم خواهد ساخت. علاوه بر این، می‌توان از آن جهت توصیف سیستم‌های مشابه موجود در زنجیره‌های بلوکی آلت‌کوین‌ها نیز استفاده کرد.

CGMiner: محبوب‌ترین نرم‌افزار استخراج بیت‌کوین است.

cold wallet: معادل فارسی آن، کیف پول برون‌خط (آفلاین) یا سرد است. کیف پول سرد، به کیف پولی روی یک رایانه یا دیسک ذخیره‌ساز اطلاق می‌شود که به اینترنت متصل نیست. این نوع کیف پول، باید برای تایید تراکنش‌ها، به اینترنت متصل شده و به یک کیف پول برخط تبدیل شود. بعد از تایید و امضای تراکنش، کیف پول برخط، می‌تواند مجددا به کیف پول برون‌خط تبدیل شود.

core developer: معادل فارسی آن، توسعه‌دهنده هسته است. توسعه‌دهنده هسته، به فرد توسعه‌دهنده یک ارز رمزنگاری شده می‌گویند که به دستورات git commit واقع در صفحه پلتفرم توسعه سایت GitHub دسترسی دارد.

cryptocurrency: معادل فارسی آن، ارز رمزنگاری شده است. به هر ارز دیجیتال که برای تامین امنیت سیستمش یا هویت کاربران و نگهدارندگان حساب، از فناوری رمزنگاری[۴] بهره می‌گیرد، ارز رمزنگاری شده می‌گویند.

Dark web: معادل فارسی آن، وب تاریک است. به بخشی از وب عمیق که از سرویس‌های خاصی ساخته

می‌شود، وب تاریک می‌گویند. مثلا فعالیت‌های حوزه مواد مخدر، در چنین محیطی انجام می‌شوند. به‌طور کلی، هر فعالیتی از قبیل روزنامه‌نگاری که ممکن است مستلزم ناشناس ماندن افراد باشد، در محیط وب تاریک، قابل انجام خواهد بود.

Decentralization: معادل فارسی آن، غیر متمرکزسازی است. مطابق این ایده، مالکیت یک شبکه، سرویس یا شرکت را می‌توان بین گروه بزرگی از افراد، توزیع کرد، به نحوی که هیچ نقطه شکست متمرکزی وجود نداشته باشد. مثلا، اینترنت، یک شبکه ارتباطی سراسری و غیر متمرکز به‌شمار می‌رود.

Deep Web: معادل فارسی آن، وب عمیق یا وب پنهان است. به همه داده‌های موجود در اینترنت که توسط مرورگرهای وب معمولی قابل مشاهده نیستند، از اطلاعات بانکداری گرفته تا بازارهای غیرقانونی مواد مخدر، وب عمیق می‌گویند.

ecash/emoney: معادل فارسی آن، پول[5] الکترونیکی است. پول الکترونیکی، به هر نوعی از پول دیجیتال اطلاق می‌شود که از دنیای واقعی فاصله دارد. معمولا به ارزهای دیجیتال قبل از بیت‌کوین، پول الکترونیکی می‌گویند.

faucet: فاست‌ها، سرویس‌هایی روی وب هستند که برای انجام وظایف کوچکی از قبیل مشاهده تبلیغات، بخش کمی از بیت‌کوین را به‌صورت مجانی در اختیار کاربران قرار می‌دهند. به بیان دیگر، به فاست‌ها، سرویس‌های کسب درآمد قطره‌ای بیت‌کوین می‌گویند. وقتی بیت‌کوین ارزش چندان بالایی نداشت، فاست‌ها، بیت‌کوین‌های کامل را نیز در اختیار کاربران قرار می‌دادند. اما امروزه، حتی بخش بسیار کوچکی از یک بیت‌کوین هم، درست به اندازه همان بیت‌کوین‌های کامل قبلی، با بخش‌های کوچکی از یک سنت، برابری می‌کنند.

51% attack: معادل فارسی آن، حمله ۵۱درصدی است. بیت‌کوین، برای اعتبارسنجی زنجیره بلوک، از سیستمی به نام «سند کار»[6] بهره می‌گیرد. سند کار، برای اعتبارسنجی و تایید تراکنش‌ها، به توان محاسباتی بالایی نیاز دارد. تغییر یک تراکنش، داده‌های قابل تایید موجود در همه تراکنش‌های بعدی را تغییر خواهد داد. بنابراین، اگر دو زنجیره بلوک رقیب، با تاریخچه‌های تراکنش مختلف وجود داشته باشند، زنجیره بلوک طولانی‌تر، به‌عنوان زنجیره بلوک غیرکاذب یا true در نظر گرفته خواهد شد، زیرا بیشترین توان محاسباتی را در اختیار دارد. از آنجایی که بازیگران خرابکار، معمولا به‌تنهایی کار می‌کنند، بعید است که هیچ گروه منفردی بتواند در قیاس با زنجیره بلوک حقیقی، توان محاسباتی بیشتری را برای زنجیره بلوک اصلاح‌شده‌اش، در اختیار بگیرد. با این حال، اگر گروهی بتواند نرخ هش بیشتری را نسبت به نرخ هش ترکیبی همه استخراج‌گرهای در حال کار روی زنجیره بلوک، در دست بگیرد، آنگاه موفق‌تر از زنجیره معتبر

عمل خواهد کرد و تایید اعتبار زنجیره بلوک خودش را دریافت خواهد کرد. به این اتفاق، حمله ۵۱درصدی می‌گویند.

fork: معادل فارسی آن، انشعاب است. به رونوشت (کپی) کردن یک کد منبع‌باز و تغییر دادن آن، انشعاب می‌گویند. در حوزه ارزهای رمزنگاری شده، زمانی که استخراج‌گرها، به‌صورت تصادفی یا به‌منظور خرابکاری، به استخراج یک زنجیره بلوک غیرکاذب دست می‌زنند نیز، فرایند انشعاب اتفاق می‌افتد.

full node: معادل فارسی آن، گره کامل است. یک کیف پول بیت‌کوین محلی که کل زنجیره بلوک را ذخیره می‌سازد و به اعتبارسنجی و گسترش تراکنش‌های تاییدشده از طریق استخراج‌گرها، کمک می‌کند. بر خلاف استخراج‌گرها، گره‌های کامل، به هیچ سخت‌افزار اختصاصی‌ای نیاز ندارند و هیچ پاداشی را نیز دریافت نمی‌کنند.

git commit: به هر تغییر ممکن در کد منبع‌باز واقع در وبگاه GitHub، اطلاق می‌شود.

GitHub: وبگاهی است که کدهای منبع‌باز را جهت کار مشترک روی آنها، میزبانی می‌کند.

GUIMiner: محبوب‌ترین نرم‌افزار استخراج بیت‌کوین بوده که دارای رابط کاربر گرافیکی است.

hard fork: معادل فارسی آن، انشعاب سخت است. به آن دسته از تغییرات صورت‌گرفته در کد ارز رمزنگاری شده که پس از انجام آنها، کاربران باید جهت ادامه کار با کلاینت‌های ارتقایافته، نرم‌افزارشان را ارتقا بدهند، انشعاب سخت می‌گوییم. اگر بخش عمده کاربران، ارتقای نرم‌افزاری را انجام ندهند، نرم‌افزار قدیمی‌تر، همچنان عمل استخراج را روی زنجیره بلوک‌اش ادامه خواهد داد. از آنجایی که این زنجیره بلوک، طولانی‌تر خواهد بود و از نرخ هش بیشتری بهره خواهد گرفت، در نتیجه، شبکه کوین، به دو قسمت تقسیم می‌شود که احتمال بروز فاجعه را بالا خواهد برد. با این حال، انشعاب‌های سخت موفق، در اغلب اوقات، تنها شیوه برای انجام تغییرات قابل توجه در کد ارز رمزنگاری شده به‌شمار می‌روند.

hash: معادل فارسی آن، هش یا درهم‌سازی است. هش، یک واحد اندازه‌گیری محسوب می‌شود که میزان توان محاسباتی ارائه‌شده در شبکه را نشان خواهد داد.

hashing power: معادل فارسی آن، توان هشینگ یا توان درهم‌سازی است، عبارت انگلیسی دیگری برای hashrate است.

hashrate: معادل فارسی آن، نرخ هش یا نرخ درهم‌سازی است. به تعداد کل هش‌های ارائه‌شده در یک شبکه، نرخ هش می‌گویند. تعداد کل هش‌ها، برابر با تعداد معادلات محاسباتی انجام‌گرفته در شبکه بیت‌کوین (یا سایر ارزهای رمزنگاری شده) است. منظور از نرخ هش THs/1، آن است که شبکه می‌تواند یک تریلیون محاسبه را در هر ثانیه انجام بدهد.

hot wallet: معادل فارسی آن، کیف پول برخط (آنلاین) یا گرم است. به کیف پول متصل به اینترنت، کیف پول برخط می‌گویند. در صورتی که رایانه یا گذرواژه مربوط به کیف پول، فاقد امنیت باشد، احتمال خطر دزدیده شدن بیت‌کوین‌ها وجود خواهد داشت. کیف پول برخط، برای ذخیره‌سازی کوتاه‌مدت و خرج کردن پول، مناسب است. همه کیف پول‌های وب، کیف پول‌های برخط هستند.

lead developer: معادل فارسی آن، توسعه‌دهنده پیشرو است. توسعه‌دهنده پیشرو، تعیین می‌کند که کدام توسعه‌دهندگان می‌توانند به دستورات git commit، دسترسی داشته باشند.

local wallet: معادل فارسی آن، کیف پول محلی است. هر یک از کیف پول‌های برون‌خط یا برخط که روی رایانه شما ذخیره شده‌اند، کیف پول محلی به‌شمار می‌روند.

miner: معادل فارسی آن، استخراج‌گر است. به هر شرکت‌کننده در شبکه بیت‌کوین که محاسبات ریاضی پیچیده‌ای را برای تامین امنیت شبکه بیت‌کوین انجام می‌دهد و علاوه بر آن، هر تراکنش صورت‌گرفته از طریق رمزنگاری را تایید می‌کند، استخراج‌گر می‌گویند. همچنین، به سخت‌افزار کامپیوتری واقعی‌ای که این کار را انجام می‌دهد و همچنین افراد یا شرکت‌هایی که مالک این سخت‌افزار هستند استخراج‌گر می‌گوییم.

mining: معادل فارسی آن، استخراج است. به فرایند تایید تراکنش‌های بیت‌کوین، در قالب گروه‌هایی به نام بلوک، از طریق حل کردن محاسبات ریاضی پیچیده و سپس ارسال این تراکنش‌ها به بقیه بخش‌های شبکه، استخراج گفته می‌شود. برای انجام این کار، استخراج‌گرها، بخش کمی از بیت‌کوین را به‌عنوان جایزه دریافت می‌کنند که نحوه ایجاد بیت‌کوین‌های جدید را نشان خواهد داد. علاوه بر این، استخراج‌گرها، کارمزدهای کوچکی را نیز که به هر تراکنش پیوست شده است، دریافت خواهند کرد که با توجه به تعداد ۲۱ میلیون بیت‌کوین استخراج‌شده کنونی، برآورد می‌شود که تعداد آنها در سال به ۲۱۴۰ عدد برسد. استخراج‌گرها، همواره در حال رقابت با یکدیگر هستند.

Mt.Gox: معادل فارسی آن، مت گاکس است. مت گاکس، وبگاه برخطی است که هدف اولیه آن به خرید و فروش کارت‌های Magic The Gathering Card بر می‌گشت، اما در نهایت، به اولین و بزرگ‌ترین مرکز مبادلات بیت‌کوین و اولین بازار آزاد متمرکز در این حوزه تبدیل شد. شرکت مت گاکس، بعد از خرابی‌های امنیتی مختلف و متهم شدن به کلاهبرداری، در اوایل سال ۲۰۱۴، اعلام ورشکستگی کرد. پس از این اتفاق، هنوز هم بهای بیت‌کوین، (در زمان نگارش کتاب) کاملا به وضعیت قبل از آن دوره برنگشته است.

node runner: معادل فارسی آن، اداره‌کننده گره است. اداره‌کننده گره، شرکت‌کننده‌ای در شبکه بیت‌کوین است که کل زنجیره بلوک را دانلود می‌کند و کار استخراج‌گر را مورد بررسی مضاعف قرار می‌دهد، اما در

رقابت جهت استخراج بیت‌کوین شرکت ندارد و هیچ جایزه‌ای را دریافت نمی‌کند، ولی با این وجود، بخش مهمی در فرایند تامین امنیت شبکه بیت‌کوین به‌شمار می‌رود. با بزرگ‌تر شدن اندازه زنجیره‌های بلوکی و کاهش تعداد افرادی که می‌خواهند کل یک چیز را دانلود کنند، بحث افزایش مشوق‌ها برای اداره‌کننده‌های گره، مورد توجه بیشتری قرار گرفته است.

open-source: معادل فارسی آن، منبع‌باز یا اوپن‌سورس است. به کدی که باز باشد و هر کسی بتواند آن را تغییر بدهد، منبع‌باز می‌گویند.

paper wallet: معادل فارسی آن، کیف پول کاغذی است. به کلید خصوصی یا عمومی که روی یک تکه کاغذ، نوشته یا چاپ می‌شود، کیف پول کاغذی می‌گوییم.

pre-mine: معادل فارسی آن، پیش‌استخراج است. وقتی آلت‌کوین‌ها برای اولین بار ایجاد می‌شوند، سازندگان آنها گاهی اوقات قبل از فعال شدن شبکه، تعدادی کوین را تولید می‌کنند و افراد مختلف می‌توانند به شیوه‌ای منصفانه، آنها را استخراج کنند. به‌طور کلی، پیش‌استخراج، نشانه اسکم (کلاهبرداری) است، اما اگر تعداد کوین‌ها پایین باشد و این کار با شفافیت بالایی صورت بگیرد، در آن صورت، برنامه کوین، فاقد اسکم خواهد بود.

proof-of-burn (PoB): معادل فارسی آن، سند حیف و میل است. به استفاده از زنجیره بلوک، برای اثبات این موضوع که بیت‌کوین یا ارز رمزنگاری شده دیگری دارد به یک آدرس غیرقابل مصرف می‌رود و برداشتن موثر آن در سیستم، سند حیف و میل می‌گویند.

proof-of-stake (PoS): معادل فارسی آن، سند سهام است. سند سهام، نوعی اثبات رمزنگاری به‌شمار می‌رود که امنیت زنجیره بلوک‌ای را که رای‌ها را بر اساس توان محاسباتی اندازه‌گیری می‌کند، تضمین خواهد کرد.

public-key encryption: معادل فارسی آن، رمزگذاری کلید عمومی است. در این شیوه، هر فرد غیرخودی، می‌تواند اطلاعات را بدون افشای آن، از طریق یک کلید قابل شناسایی عمومی، تایید کند. با استفاده از کلید فوق‌الذکر، می‌توان مشخص کرد که آیا یک پیغام، از جانب فردی که کلید خصوصی مرتبط با آن را در اختیار دارد، برای شما آمده است یا خیر. در این فرایند، نیازی به افشای جزئیات مربوط به آن کلید خصوصی نیست.

Scrypt: الگوریتم رایانه‌ای استفاده‌شده توسط لایت‌کوین[۷] و بسیاری از ارزهای رمزنگاری شده جایگزین دیگر، جهت تامین امنیت شبکه مربوط به آنها. این الگوریتم، مقاومت بیشتری نسبت به ASIC‌ها دارد.

SHA256: الگوریتم رایانه‌ای استفاده‌شده توسط بیت‌کوین و بسیاری از ارزهای رمزنگاری شده دیگر،

جهت تامین امنیت شبکه مربوط به آنها.

sidechain: معادل فارسی آن، زنجیره جانبی است. زنجیره جانبی، راهکاری برای تغییر مقیاس بیت‌کوین به‌شمار می‌رود. به عبارت دیگر، زنجیره‌های جانبی، دفاتر کل شبه‌زنجیره بلوک هستند که تعداد زیادی از تراکنش‌های اضافه‌شده به زنجیره بلوک نهایی را به‌صورت فشرده، ردیابی خواهند کرد.

soft fork: معادل فارسی آن، انشعاب نرم است. در انشعاب نرم، کد ارز رمزنگاری شده، تغییر قابل توجهی پیدا می‌کند و با وجود اینکه ممکن است به دلایل امنیتی یا دلایل دیگر، به ارتقای نرم‌افزار کیف پول نیاز داشته باشیم، اما نرم‌افزار قدیمی‌تر، همچنان می‌تواند تراکنش‌ها را ارسال، دریافت و اعتبارسنجی کند و امکان اعتبارسنجی اتفاقی و تصادفی زنجیره‌های بلوکی دیگر وجود نخواهد داشت.

wallet: معادل فارسی آن، کیف پول است. این عبارت کلی، به نرم‌افزاری اشاره دارد که جهت تایید و امضای تراکنش‌های صورت‌گرفته با استفاده از آدرس بیت‌کوین شما، باید با شبکه بیت‌کوین ارتباط برقرار کند.

web wallet: معادل فارسی آن، کیف پول وب است. به هر کیف پولی که از طریق وبگاه نگهداری‌شده توسط شرکت دیگر، کنترل و محافظت می‌شود، کیف پول وب می‌گویند. امنیت و میزان اعتماد کیف پول وب، تنها به شرکتی بستگی دارد که آن را میزبانی کرده است. به‌طور کلی، این نوع کیف پول، فقط به درد خرج کردن پول می‌خورد، اما برخی از این سرویس‌ها، امنیت بیشتری را فراهم می‌کنند و به‌دلیل استفاده از فناوری چندامضایی[۸] و تولید کلید برون‌خط، استفاده از آنها برای ذخیره‌سازی کوتاه‌مدت تا میان‌مدت، مانعی ندارد.

X11: الگوریتم استفاده‌شده توسط Dash و تعدادی از ارزهای دیگر است. الگوریتم مزبور، همان‌طور که از نامش پیداست، از ۱۱ الگوریتم مختلف بهره می‌گیرد.

فهرست اشخاص

یان دی مارتینو[۹]: نویسنده کتاب.

گوین آندرسن[۱۰]: توسعه‌دهنده هسته بیت‌کوین که مدتی با ساتوشی ناکاموتو همکاری داشت که بخش‌های کلیدی بیت‌کوین را پایه‌ریزی کرده بود.

آندریاس آنتونوپولوس[۱۱]: نویسنده، طرفدار بیت‌کوین و متخصص امنیت.

بنیاد بیت‌کوین[۱۲]: سازمانی تجاری که پیش از این، پایه‌گذار اصلی توسعه‌های هسته بیت‌کوین بود.

دفتر یا اتاق بازرگانی دیجیتال[۱۳]: یک گروه پرنفوذ طرفدار بیت‌کوین.

هال فینی[۱۴]: رمزنگار قدیمی‌ای که به ایجاد PGP کمک کرد. او حامی قدیمی بیت‌کوین است و کسی بود که اولین تراکنش بیت‌کوین را دریافت کرد.

مایک هیرن[۱۵]: توسعه‌دهنده بیت‌کوین و کارمند گوگل. وی فناوری Lighthouse را ایجاد کرد و یکی از طرفداران Bitcoin XT است.

اولیویر جانسنز[۱۶]: یکی از استفاده‌کنندگان قدیمی بیت‌کوین که به فرشته کسب‌وکار[۱۷] در این حوزه تبدیل شد. او تامین مالی ایجاد فناوری Lighthouse را بر عهده داشت. فناوری Lighthouse، برنامه‌ای است که

هدف از طراحی‌اش، جمع‌سپاری[۱۸] نسخه‌های ارتقایافته کد هسته بیت‌کوین بود، اما تاکنون، عمدتا برای پروژه‌های غیر مرتبط با جمع‌سپاری استفاده شده است.

مارک کارپلس[۱۹]: مدیرعامل و مالک مت گاکس در زمان ورشکسته شدن این بازار مبادلات.

ولادیمیر وان در لان[۲۰]: توسعه‌دهنده پیشروی فعلی بیت‌کوین.

جد مک کالب[۲۱]: بنیانگذار و مالک قبلی مت گاکس و یکی از بنیانگذاران ریپل و استلار.

ساتوشی ناکاموتو[۲۲]: خالق ناشناس بیت‌کوین که به یک یا چند نفر اشاره دارد.

درید پیرات رابرتز[۲۳]: رهبر بازار زیرزمینی بدنام Silk Road که به یک یا چند نفر اشاره دارد.

امیر تاکی[۲۴]: یکی از ایجادکنندگان کیف پول تاریک و توسعه‌دهنده پیشروی پروژه Darkmarket که بعدها به OpenBazaar تغییر نام داد.

پیتر تاد۵۲: توسعه‌دهنده هسته بیت‌کوین

راس اوبریخت[۲۶]: کسی که متهم شد که دریدپیرات رابرتز است و پرونده‌اش در مرحله استیناف یا فرجام‌خواهی قرار دارد.

راجر ور[۲۷]: فرشته کسب‌وکار و طرفدار دوآتشه بیت‌کوین. او مدیرعامل Memorydealers.com (یکی از اولین سایت‌هایی که از بیت‌کوین استفاده کرده است) و بنیانگذار شرکت Blockchain است.

کودی ویلسون[۲۸]: یکی از ایجادکنندگان کیف پول تاریک و طراح تفنگ ساخته‌شده از طریق پرینترهای سه‌بعدی.

کرایگ رایت[۲۹]: فردی جدید در لیست افرادی که ادعا می‌کنند ساتوشی ناکاموتو هستند. مجله Wired، اخیرا گزارش داد که شاید او خالق بیت‌کوین باشد. در ماه مه سال ۲۰۱۶، وی با امضای یک پیغام با استفاده از حساب وابسته به ساتوشی ناکاموتو، تلاش کرد تا ثابت کند که خالق اصلی بیت‌کوین است. در آن زمان، بسیاری از قبیل گوین آندرسن قانع شدند. با این حال، هنوز بسیاری از اعضای جامعه بیت‌کوین، به این موضوع شک داشتند. با وجود اینکه قول داده بود تا شواهد بیشتری را ارائه کند، اما نتوانست به این ادعا جامه عمل بپوشاند.

بخش نخست
بیت‌کوین چیست؟

فصل۱
بیت‌کوین ۱۰۱: فناوری زنجیره بلوک

این همان چیزی است که منتظرش بودیم. انگار آلبوم آهنگ گروه موسیقی راک هوی متال[۳۰] و ویشز رومرز[۳۱] را وارد بازار کرده باشند. بالاخره کار فعالانی که مدت‌ها داشتند به بانک مرکزی آمریکا (فدرال رزرو) فشار می‌آوردند، دارد جواب می‌دهد.

مکس کایزر[۳۲]، خبرنگار شبکه تلویزیونی راشا تودی[۳۳]

از دو جنبه می‌توان این سوال را که «بیت‌کوین چیست؟» مطرح کرد. هر دو سوال، هم به نحوی با هم در ارتباط هستند و هم از زوایایی با یکدیگر فرق دارند. سوال اول به ماهیت واقعی بیت‌کوین و سوال دوم به قابلیت‌های آن بر می‌گردد. علاوه بر این، هدف من در این کتاب آن است تا در پاسخ به این سوال که «شیوه کار بیت‌کوین به چه نحوی است؟»، در واقع به هر سه پرسش مطرح‌شده در اینجا جواب بدهم.

به زبان ساده، بیت‌کوین، درست همانند یورو یا دلار، شکل جدیدی از ارز است که معادل دیجیتال پول نقد به‌شمار می‌رود. هر شخصی می‌تواند به‌صورت دیجیتالی، یک بیت‌کوین، چندین بیت‌کوین، یا بخشی از بیت‌کوین را در سراسر جهان یا در داخل یک اتاق، با فرد دیگری دست به دست کند. در اینجا،

شیوه انتقال پول، همانند دست به دست کردن پول نقد است و بر خلاف سایر سیستم‌های مالی دیجیتال قدیمی‌تر، به واسطه‌هایی مثل بانک یا شرکت‌های دیگر نیازی نداریم. نقاط قوتی که در ادامه به آنها خواهم پرداخت، باعث شده است تا استفاده از آن در بین مردم رواج پیدا کند.

یکی از فناوری‌های مورد استفاده در اینجا، فناوری دفتر کل توزیع‌شده[۳۴] است. در این فناوری، تراکنش‌ها و ترازهای مربوط به هر کیف پول بیت‌کوین، ثبت می‌شوند و می‌توان کیف پول بیت‌کوین را درست همانند یک حساب بانکی در نظر گرفت. به این دفتر کل، زنجیره بلوک[۳۵] نیز می‌گوییم. هر کیف پول، به‌جای آنکه در پایگاه داده یک بانک ذخیره شود، در این دفتر کل قرار دارد. هر کیف پول، دارای کلید عمومی و کلید خصوصی خودش است. به کلید عمومی[۳۶]، آدرس بیت‌کوین[۳۷] نیز می‌گوییم. طول کاراکترهای هر آدرس بیت‌کوین، بین ۲۵ تا ۳۶ کاراکتر حرفی-عددی است و در ابتدای آن، یکی از ارقام ۱ یا ۳ قرار دارند. هر کسی می‌تواند این آدرس را مشاهده کند و از طریق آن، بیت‌کوین‌ها را به دیگران انتقال بدهد. همانند رایانامه‌ها، کیف‌های پول بیت‌کوین را نیز می‌توان تقریبا بلافاصله ایجاد کرد و با همان سرعت نیز به افراد دیگر انتقال داد.

کلید خصوصی ۸۳، ظاهری مثل 5JJqKVLu29gfafXvCjva9BtVapjrE8qNerXWt9RTAv4ebbDX4E دارد، و باید به هر قیمت ممکن، از آن حفاظت کرد. غالبا گفته می‌شود که اگر چیزی را در اختیار داشته باشید، دیگران به‌سختی می‌توانند آن را از شما بگیرند. در رابطه با بیت‌کوین، کلید خصوصی، نشان‌دهنده اختیار کامل قانونی شماست. هر کسی که کلید خصوصی را در اختیار دارد، می‌تواند بیت‌کوین‌های موجود در کیف پول متناظر با آن را برای دیگران ارسال کند. هیچ راهی برای به عقب برگرداندن یک تراکنش بیت‌کوین وجود ندارد و به همین دلیل، کلید خصوصی، مهم‌ترین اصل مورد استفاده در بیت‌کوین محسوب می‌شود. ممکن است با شنیدن این جملات، کمی گیج شده باشید. شاید اگر خودتان را در وضعیتی در نظر بگیرید که مجبور هستید یک ارز جدید را بدون حضور فیزیکی ایجاد کنید، فهم مطالب بالا کمی برایتان آسان شود.

تصور کنید که همراه با ۱۹ فرد دیگر، در جزیره متروکه‌ای گیر افتادید. غذا و آب شیرین کافی برای زنده ماندن موجود است، اما امکان نجات یا فرار وجود ندارد. تنها کاری که برای زنده ماندن باید انجام دهید، همکاری دسته‌جمعی و توزیع منصفانه منابع هستند. شاید هم نیاز باشد تا بفهمید که چه کسانی برای چه مدتی و برای چه افرادی کار می‌کنند. برای انجام این کار، باید نوع جدیدی از یک سیستم مالی پیاده‌سازی شود. می‌توانید از صدف‌های دریایی یا سنگ‌های براق یا هر چیز نادری مانند آنها استفاده کنید، اما بی‌شک، هر کسی می‌تواند این سیستم مالی را فریب دهد. وقتی می‌توان به‌سادگی با قدم زدن در کنار

ساحل، صدف دریایی پیدا کرد، دیگر چه نیازی است که دوستان‌تان در قبال دریافت دو صدف دریایی، در ساختن کلبه به شما کمک کنند؟ در چنین محیطی، چگونه می‌توان نظام پولی‌ای را پایه‌ریزی کرد که افراد حاضر در آن، در قبال ساعات کاری‌شان، حقوق منصفانه‌ای دریافت کنند؟

یکی از راهکارها جهت حل مشکل فوق‌الذکر، ایجاد فهرست یا دفتر کل است. دفتر کل، میزان کاری را که هر فرد انجام داده است، بر حسب واحدهای کاری مورد قبول، ثبت می‌کند. دفتر کل، مقدار دارایی هر فرد را نشـــان می‌دهد و به افراد اجازه می‌دهد تا سپرده خود را به حســـاب شخص دیگری بریزند. اگر دفتر کل، میزان عرضه سهام[۳۹] هر فرد و هر دادوستد رخ‌داده را ثبت کند، در آن صورت هیچ کسی نخواهد توانست تراز یا مانده حسابش را با اضافه کردن صدف‌های دریایی یا سنگ‌های براق یا هر واحد کاری[۴۰] دیگری خارج از سیستم مالی، افزایش دهد. مشـــکل راهکار دفتر کل این است که همه شرکت‌کنندگان باید مطمئن باشند که فردی که دفتر کل را در اختیار دارد، منصفانه رفتار می‌کند. اگر تنها یک موجودیت (نهاد) یا گروه، دفتر کل را در دست بگیرد، در نهایت، توانایی کنترل میزان پول هر فرد را در اختیار خواهد داشت و در اختیار داشتن این توانایی، می‌تواند هر کسی را به وسوسه بیندازد.

برای حل این مشکل، می‌توانیم به غیرمتمرکزسازی متوسل شویم. می‌توان دو رونوشت (کپی) از دفتر کل را در اختیار دو فرد معتمد گروه قرار داد. در نتیجه، آنها می‌توانند دفاتر کل یکدیگر را به‌صورت متقابل بررسی کنند تا از این طریق، همخوانی و تطبیق رکوردهای ثبت‌شده، تضمین شود. با این وجود، هنوز هم مشکل اعتماد، سر جای خودش باقی است، تنها تفاوتش این است که این بار، به‌جای یک گروه، باید به دو گروه اعتماد کنیم. اگرچه این شیوه، نسبت به واگذاری همه قدرت نگهداری دفتر کل به یک گروه، بهتر است، اما از وضعیت ایده‌آل فاصله زیادی دارد.

بهترین راهکار که برای مشـــکل فوق می‌توان مطرح کرد، توزیع ۲۰ رونوشت از دفتر کل در بین همه افرادی اســـت که در این جزیره حضور دارند. در پایان روز، هر کسی می‌تواند تراکنش‌های اتفاق‌افتاده با افراد دیگر را مورد بررسی متقابل قرار بدهد. در این راهکار، بدون آنکه اختیار دفتر کل، تنها به دست یک فرد سپرده شده باشد، می‌توان به اجماع رســـید. در نهایت، افراد ساکن در جزیره، متوجه خواهند شد که آنچه واقعا اهمیت دارد، صدف دریایی نیست، بلکه دفتر کل است. اهمیتی ندارد که چه صدف دریایی‌ای را از جزیره جمع کرده‌اید، بخش مهم این راه‌حل، دفتر کل است که یادآوری می‌کند، هر فردی چه چیزی را در اختیار داشـــته و چه چیزی را خرید و فروش کرده است. حتی ممکن است برخی افراد، صدف‌های دریایی را مانعی در مقابل تجارت بدانند، زیرا باید جایی را نیز به گردآوری، نگهداری و ردیابی صدف‌های دریایی قانونی و مجاز اختصاص بدهیم. صدف‌های دریایی، همانند همه ارزها، برای تعیین میزان کار،

مورد استفاده قرار می‌گیرند. اگر دفتر کل، قبل از انتخاب صدف‌های دریایی، به‌عنوان ارز، مشغول به کار بوده باشد، آنگاه خود صدف‌های دریایی، عناصر خارجی و بیگانه به‌شمار می‌روند. ارزهای واقعی، «واحدهای کاری» موجود در دفتر کل هستند و صدف‌های دریایی و سایر اشیای فیزیکی، تنها برای ردیابی و تعیین میزان کار افراد، مورد استفاده قرار می‌گیرند. آنچه در این سیستم اهمیت دارد، خود کار است که ارز واقعی به‌شمار می‌رود.

با توجه به مثال بالا، می‌توان بیت‌کوین را به‌عنوان ارز و زنجیره بلوک را به‌عنوان دفتر کل در نظر گرفت. اگرچه اینترنت، فضایی را برای برقراری ارتباط تقریبا فوری فراهم ساخت، اما این قابلیت تا مدتی به کار گرفته نشده بود، تا اینکه موجودیت ناشناسی به نام ساتوشی ناکاموتو، دفتر کل غیرمتمرکزی را پیاده‌سازی کرد که مبادلات همه افراد در داخل آن ثبت می‌شدند. هر شرکت‌کننده کامل در بیت‌کوین، رونوشتی از دفتر کل را در اختیار دارد. همه افراد می‌توانند رونوشت‌های خودشان را با هر دفتر کل دیگری مقایسه کنند و از این طریق، از دقت آن اطمینان یابند. فرایند مزبور، شیوه تایید و بررسی میزان دقت دفتر کل را پیچیده‌تر می‌کند، اما اصلی اساسی است که باید حتما آن را رعایت کنیم.

اختلاف کاملا روشن بین مثال ما و بیت‌کوین، این است که بیت‌کوین، در مقیاسی جهانی کار می‌کند، اما جزیره تنها به ۲۰ نفر محدود بود. به همین دلیل، بدون کمک گرفتن از رایانه‌ها و اینترنت، نمی‌توان بیت‌کوین را مورد استفاده قرار داد. علاوه بر این، هیچ فضای فیزیکی‌ای در اینترنت موجود نیست. شما نمی‌توانید صدف‌های دریایی را از طریق یک کابل فیبر نوری، برای دیگران ارسال کنید. بنابراین، ارز دیجیتال، فاقد هویت فیزیکی است.

چالش اصلی و مهم در فرایند ایجاد ارزهای دیجیتال کارا، آن است که این ارزها، حداقل آن‌گونه که ما تصور می‌کنیم، وجود فیزیکی ندارند. در گذشته، تعریف واژه «بودگی یا وجود»[۴۱]، ساده‌تر بود. هر چیزی، یا وجود داشت یا وجود نداشت. شما می‌توانستید هر چیزی را در دست داشته باشید یا نداشته باشید. اما اکنون که دنیای مجازی شکل گرفته است، چه تعریفی را می‌توان برای بودگی ارائه داد؟ آیا یک کتاب، وقتی روی کاغذ چاپ شد، واقعی‌تر می‌شود؟ آیا بودگی نسخه فیزیکی یک کتاب، نسبت به نسخه الکترونیکی‌اش، اعتبار بیشتری دارد؟ شکی نیست که در دنیای فیزیکی، نسخه چاپی، ملموس‌تر از نسخه الکترونیکی خواهد بود، اما تعداد افرادی که ادعا می‌کنند نسخه فیزیکی کتاب، اعتبار بیشتری نسبت به نسخه الکترونیکی‌اش دارد، چندان زیاد نیست. این دو نسخه، حرف جداگانه‌ای برای گفتن ندارند.

از یک نگاه، پول، معرف میزان کار است، اما برای آنکه این مفهوم را انتقال بدهد، لزوما نیازی نیست تا آن را روی یک قطعه کاغذ چاپ کنیم. برای راحتی کار، می‌توانیم پول را روی قطعه‌ای از کاغذ یا تکه‌ای

از فلز چاپ کنیم یا اینکه در داخل یک سرور رایانه‌ای ذخیره کنیم. بخش عمده پول، از دلار گرفته تا یورو و یوآن، به‌صورت الکترونیکی وجود دارد. دیگر به کســی که پول نقد زیادی نداشته باشد، اما میلیون‌ها دلار را در حساب بانکی‌اش بخواباند، فقیر نمی‌گویند. اگر پول نقد فیزیکی و بازنمایی[۴۲] الکترونیکی آن، هر دو دارای اعتبار یکسانی باشند، آنگاه شیوه این بازنمایی الکترونیکی، چگونه خواهد بود؟ و حال که بازنمایی‌های دیجیتال پول سنتی در دسترس همگان قرار دارد، آیا واقعا به یک ارز صرفا دیجیتالی از قبیل بیت‌کوین نیاز داریم یا خیر؟

خرید برخط، پدیده جدید و تازه‌ای است. اگرچه در سال ۲۰۱۲، ۲۸۹ بیلیون دلار، در حوزه تجارت الکترونیک صرف شد[۴۳]، اما در اوایل دهه ۱۹۹۰، خرید برخط، برای بخش عمده مصرف‌کنندگان، قابل تصور نبود. تاریخ تولد تجارت الکترونیک، به ســال ۱۹۹۴ و زمانی برمی‌گردد که اولین تراکنش امن، یعنی خرید ۱۲/۴۸ دلاری آلبوم Ten Summoner's Tales استینگز در وبگاه Netmarket، اتفاق افتاد[۴۴].

شماره کارت اعتباری استفاده‌شده برای خرید سی‌دی مزبور، رمزگذاری شد و عموم مصرف‌کنندگان متوجه شدند که اینترنت، بازار قابل قبولی به‌شمار می‌رود. سال بعد، آمازون و ایی‌بی، کارشان را شروع کردند.

قبل از اتفاقات فوق، بحث‌های تئوری زیاد و خوبی در مورد آمادگی اینترنت در اقتصاد مطرح شده بود. نیکولا تسلا[۴۵] و مارشال مک لوهان[۴۶]، در مورد مراکز عصبی مرکزی بی‌سیم جهانی، مطالعاتی را ترتیب داده بودند. مک لوهان، در کتاب «درک رسانه»[۴۷] که در ســال ۱۹۶۴ نوشته بود، شکلی تعاملی و به هم پیوسته از رسانه‌ها را مورد اشاره قرار داد که شباهت زیادی به اینترنت و واقعیت مجازی دارد. وی، پیش از این، در کتاب «کهکشان گوتنبرگ»[۴۸]، اصطلاحی با عنوان «دهکده جهانی»[۴۹] را بر سر زبان‌ها انداخته بود که هنوز هم برای توصیف اینترنت امروزی، به کار گرفته می‌شود. علاوه بر این، اصطلاح دیگری که برای اولین بار، مک لوهان به کار گرفته بود، «رسانه، همان پیام است»[۵۰] است. معنا و مفهوم این اصطلاح آن است که روش انتقال اطلاعات در جامعه، تاثیر عمیق‌تری را نسبت به اطلاعات واقعی بر جای خواهد گذاشت. با توجه به این مفاهیم، ســوال دیگری که مطرح می‌شود این اســت که فرهنگ در یک جامعه به‌هم‌پیوسته الکترونیکی، چه جایگاهی دارد؟ با این وجود، نگرانی اصلی مک لوهان، به جای اقتصاد، به ارتباطات و رسانه‌ها معطوف بود.

خوانندگان قدیمی‌تر ممکن است شبکه‌های خرید خانگی[۵۱] اواخر دهه ۱۹۷۰ را به یاد داشته باشند. در این شبکه‌ها، کاربران، فهرست الکترونیکی را در رایانه‌های شخصی‌شان پر می‌کردند و آنها را از طریق خط تلفن، برای داروخانه یا فروشگاه‌های رفاه مورد نظرشان می‌فرستادند. اگرچه این شیوه، ایده بدی در

آن زمان نبود، اما این نوع از شبکه‌ها، بعد از رشد و توسعه اینترنت، کارایی خود را از دست دادند و منسوخ شدند. با این وجود، استفاده از شبکه‌های خرید خانگی نشـــان می‌دهد که ایده سفارش دادن چیزهای مختلف از طریق رایانه شخصی، حتی در سال ۱۹۹۴ نیز مفهوم جدیدی نبود. تنها ایراد آن زمان این بود که هیچ راه امن و مناسبی برای انجام این کار وجود نداشت.

وقتی نت مارکت، اولین فروش خود را انجام داده بود، از نظر همه کسانی که این اتفاق را زیر نظر داشتند، این تنها به خرید یک چیز از طریق اینترنت محدود نمی‌شد، بلکه عصر جدیدی در حال ظهور و پیدایش بود. این اولین فروشی بود که در آن، خریدار به میزان قابل قبولی، به تامین امنیت اطلاعات کارت اعتباری خود، اطمینان داشت. قبل از معامله نت مارکت، هیچ فرد خریدار برخطی، مطمئن نبود که فردی که در سمت دیگر ارتباط اینترنتی قرار دارد، این اطلاعات را سرقت نکند.

برای کار در نت مارکت، مشتریان باید نرم‌افزار اختصاصی‌ای را که مبتنی بر برنامه افسانه‌ای PGP بود، دانلود می‌کردند. PGP یا «حریم شـــخصی خیلی خوب»[۵۲]، به فناوری‌ای اشاره دارد که امکان برقراری ارتباط خصوصی و امن بین دو طرف اینترنت را با استفاده از رمزگذاری فراهم می‌ساخت. الگوریتم‌های رمزگذاری فناوری PGP که اتفاق مهمی در حوزه رمزنگاری به‌شـــمار می‌روند، برای چندین دهه، پایه و اساس این صنعت را تشکیل می‌دادند. هنوز هم امروزه از نرم‌افزار منبع‌باز مبتنی بر فناوری PGP استفاده می‌شود.

بعد از تراکنش نت مارکت، فرایند خرید برخط چیزهای مختلف، ساده‌تر شد، اما سطح امنیت خریدها، همیشه به یک میزان نبود. با رشـــد و توســـعه خرید برخط، دیگر، رمزگذاری کارت اعتباری، امن‌ترین روش تراکنش برخط به‌شمار نمی‌رود. تجارت اولیه، از وجود اسکم‌ها و هک‌های کارت‌های اعتباری رنج می‌برد. نت مارکت، بعد از نشت تصادفی حدود یک میلیون سفارش در سال ۱۹۹۹، درگیر مناقشه بزرگی شد[۵۳]. نشت اطلاعات شخصی تا به امروز نیز ادامه دارد. همین ترس باعث شد تا افراد آینده‌پژوه و توسعه‌دهندگان، قبل از استفاده از سرویس‌هایی از قبیل پی‌پال، این سوال را مطرح کنند که آیا اینترنت، به ارز مخصوص به خودش نیاز دارد یا خیر.

این ایده، آنقدرها که فکر می‌کنید احمقانه نیست. در گذشـــته، ارزها معمولا به مناطق یا کشورهای خاصی محدود می‌شـــدند. برای قرن‌های متمادی، این شیوه مورد اســـتفاده قرار می‌گرفت، زیرا چندان معمول نبود که فردی از یک گوشه دنیا، با ارز محلی خودش، با فردی در گوشه دیگر دنیا که از ارز دیگری اســـتفاده می‌کند، معامله کند. با این حال، پیدایش اینترنت، این امکان را برای افراد فراهم ساخت تا هم مرزهای سیاسی و هم مرزهای جغرافیایی را درنوردند. ناگهان، فضای اینترنت، زمینه‌ای را مهیا کرد تا افراد

یک بخش از سیاره، با افراد سایر نقاط سیاره، ارتباط برقرار کنند. در نتیجه، برقراری ارتباط جهانی رشد پیدا کرد و نیاز به نوع جدیدی از تجارت شکل گرفت.

مشکلی که در اینجا وجود داشت این بود که هر فرد به شخصی که در سمت دیگر این رابطه وجود داشت، بی‌اعتماد بود. در واقع، دست به دست شدن شماره کارت اعتباری، با فرد ناشناسی که در قلمرو قانونی دیگری قرار دارد، قابل قبول نبود. علاوه بر موضوعات مربوط به سازگاری نهادهای مالی (مانند اینکه آیا کارت اعتباری ایالات متحده، از نظر بانک بازرگانی روسیه اعتبار دارد یا نه)، فرایند مزبور، امنیت لازم را نداشت. در اینجا، شماره کارت اعتباری شما، در اکثر موارد به‌صورت رمزگذاری‌نشده، برای فرد ناشناسی ارسال می‌شد که ممکن بود هر جایی باشد. اگرچه بی‌شک، میزان امنیت خرید برخط، نسبت به اولین روزهای ظهور و پیدایش اینترنت، بیشتر شده است، اما همچنان امنیت، فاکتور بسیار مهمی به‌شمار می‌رود و انگیزه اصلی و اولیه انجام بسیاری از تحقیقات در رابطه با پول الکترونیکی یا ارز اینترنتی محسوب می‌شود. اگرچه حواله ارزی، تامین مالی توزیع‌شده، پرداخت‌های خرد و سرمایه‌گذاری قابل دسترسی، غالبا به‌عنوان حوزه‌های مهم مورد نظر در سیستم بیت‌کوین مورد اشاره قرار می‌گیرند، اما انگیزه اصلی و اولیه پول‌های نقد الکترونیکی، به حل نگرانی‌های امنیتی موجود بر می‌گشت.

سردبیر مجله Wired به نام کوین کلی[۵۴]، در کتاب سال ۱۹۹۴ خود با عنوان «خارج از کنترل: بیولوژی جدید ماشین‌ها، سیستم‌های اجتماعی، و دنیای اقتصاد»[۵۵]، به اموری که برای رشد اقتصاد اینترنت مورد نیاز هستند، اشاره کرد. «کلی» ادعا کرد که هر جامعه خیلی خوب، به چیزی فراتر از ناشناس ماندن صرف نیاز دارد. شکل‌گیری تمدن برخط، مستلزم عوامل زیر است: ناشناس بودن برخط، شناسایی برخط[۵۶]، احراز هویت برخط[۵۷]، خوشنامی برخط[۵۸]، نگهدارندگان اعتماد برخط، امضاهای برخط[۵۹]، حریم شخصی برخط و دسترسی برخط. همه این موارد، عناصر اصلی هر جامعه باز و آزادی را تشکیل می‌دهند. طبق نظر «کلی»، اینترنت، برای تامین حریم شخصی، شناسایی، تایید و خوشنامی، به ناشناس ماندن و برای تامین امنیت، به امضاها نیاز دارد. به نظر می‌رسد که دو نیاز فوق، در تعارض با یکدیگرند. چگونه می‌توان هم حریم شخصی و هم شناسایی برخط را تضمین کرد؟ پاسخ به این سوال، در رمزنگاری و رمزگذاری کوین کلی و سایفرپانک[۶۰]های آن دوران نهفته است:

«به نظر من، فناوری رمزگذاری[۶۱]، به سرریز عظیم دانش و داده‌هایی که سیستم‌های شبکه‌ای تولید می‌کنند، نظم می‌بخشد. بدون این قابلیت، شبکه، به تار عنکبوتی تبدیل خواهد شد که در چنگال خودش گرفتار شده است و دارد با استفاده از اتصالات بسیار زیادش خفه می‌شود. رمز[۶۲]، پیکره انرژی[۶۳] جسم فیزیکی[۶۴] شبکه را تشکیل می‌دهد که نیروی مخفی کوچکی است که می‌تواند

اتصالات به‌هم‌پیوسته انفجاری ایجادشده توسط سیستم‌های توزیع‌شده و غیرمتمرکز را مهار کند.»

به‌طور خاص، رمزگذاری کلید عمومی، این خواسته را محقق کرد. رمزگذاری کلید عمومی این امکان را فراهم می‌سازد تا کاربران، بدون شناسایی شدن، تایید شوند. پایه و اساس رمزگذاری سنتی را کلید توافقی[۶۵]، تشکیل می‌دهد که با استفاده از آن می‌توان یک پیغام را رمزگشایی کرد. استفاده از کلید توافقی در حین کار با طرف دوم قابل اعتماد رابطه، ایرادی ندارد، اما وقتی با گروه‌های بزرگ یا منابع ناشناس زیادی سروکار داریم، به‌دلیل در معرض خطر قرار گرفتن کلید، شیوه ایده‌آلی به‌شمار نمی‌رود. در رمزگذاری کلید عمومی، هر کاربر، دو کلید را در اختیار خواهد داشت؛ یک کلید عمومی و یک کلید خصوصی. کلید عمومی، آزادانه به اشتراک گذاشته می‌شود و این امکان را به هر فرد می‌دهد تا پیغامی را رمزگذاری کند که تنها کلید خصوصی، امکان رمزگشایی آن را خواهد داشت. کلید عمومی را نمی‌توان برای کشف کلید خصوصی به کار گرفت. به همین دلیل، به اشتراک گذاشتن آن خطری ندارد. از سوی دیگر، با استفاده از تکنیکی به نام امضای دیجیتال، عکس این کار نیز قابل انجام خواهد بود. اگر به‌جای آنکه کاربر دیگری، پیغامی را با استفاده از کلید عمومی شما رمزگذاری کند، این کار را از طریق کلید خصوصی‌تان انجام دهد، آنگاه این پیغام، تنها با استفاده از کلید عمومی شما رمزگشایی خواهد شد. در نتیجه، کاربران، امکان امضای دیجیتالی یک پیغام یا سند را به‌گونه‌ای خواهند داشت که نتوان آنها را جعل کرد. نکته مهم‌تر در فرایند توسعه بیت‌کوین آن است که هیچ کسی، در صورت امضای دیجیتال چیزی، نمی‌تواند ادعا کند که آن را ارسال نکرده است. این لایه امنیت قابل تایید اضافی، بخش مهمی برای کارکرد مناسب هر ارز دیجیتال محسوب می‌شود.

بگذارید به مثال قبلی‌مان در مورد ۲۰ فرد بازمانده در یک جزیره متروکه برگردیم. فرض کنید در موردی خاص، عدم توافق وجود دارد. فردی ادعا می‌کند که در قبال دریافت کالا یا خدمات، مبلغ را به طرف مقابل پرداخت کرده است، اما فرد دوم، چنین چیزی را قبول ندارد. هیچ فرد دیگری، این تراکنش مشکوک را ثبت نکرد و به همین دلیل کسی هم نمی‌تواند بگوید که کدام دفتر کل، دقیق‌تر است. در این سناریو، تعیین این موضوع که چه کسی راست و چه کسی دروغ می‌گوید، کار ساده‌ای نیست. شبکه بیت‌کوین، هر شرکت‌کننده را مجبور می‌کند تا در صورت انجام هر تراکنش، دست به امضای دیجیتالی بزند و به همین دلیل قابلیت اعتماد را بسیار بالاتر خواهد برد.

در دنیای بیت‌کوین، به دفتر کل، زنجیره بلوک می‌گویند. هر حساب در شبکه بیت‌کوین که به کیف پول معروف است، از طریق زنجیره بلوک ردیابی می‌شود. به محض اینکه تراکنشی در شبکه ارسال شود، فرستنده، امضای دیجیتالی را در پای آن قرار می‌دهد و یک مهر زمانی[۶۶]، از طریق این تراکنش شکل

می‌گیرد. در ادامـــه کار، مهر زمانی، در گروهی از تراکنش‌هایی که همراه با هم پردازش می‌شـــوند، قرار می‌گیرد و نسخه فشـــرده‌ای از گروه قبلی تراکنش‌ها، به این گروه اضافه می‌شـــود. از آنجایی که هر گروه جدید از تراکنش‌ها، حاوی نسخه فشرده‌شده گروه قبلی است، در نتیجه، تغییر هر چیزی در این فرایند، تاریخچه تراکنش را تغییر می‌دهد و زنجیره را بی‌اعتبار می‌سازد. اگر فردی خواست به عقب برگردد و یکی از تراکنش‌های قدیمی‌تر را حذف کرده یا تغییر دهد، برای انجام این کار، باید محاسبات ریاضی پیچیده تشکیل‌دهنده دفتر کل تا آن نقطه را مجددا انجام بدهد[۶۷]. معنا و مفهوم این کار آن است که زنجیره بلوک، عملا تغییرناپذیر است.

وقتی تراکنشی به شبکه ارسال می‌شود، همیشه در داخل زنجیره بلوک ثبت خواهد شد. نیازی نیست تا بقیه گروه، وقت خود را صرف برقراری ارتباط بین هر یک از دو طرف شـــرکت‌کننده کنند. یا تراکنش، در داخل زنجیره بلوک ثبت می‌شود و نسخه فشرده‌شـــده که به آن هش می‌گوییم را می‌توان مورد وارسی رمزنگاری قرار داد، یا اینکه چنین کاری ممکن نیست. هیچ چیز اضافی‌ای برای بحث وجود ندارد.

برای اینکه شبکه مزبور به‌درستی کار کند، به فردی نیاز داریم تا مسئولیت پردازش معادلات ریاضی پیچیده جهت وارســـی هش‌های هر تراکنش را بر عهده بگیرد. به این شـــرکت‌کننده‌ها، اســـتخراج‌گر می‌گوییم. استخراج‌گرها در قبال انجام این تراکنش‌ها و افزودن آنها به زنجیره بلوک، بیت‌کوین‌های تازه ایجادشده و عایدات حاصل از کارمزد استخراج‌گر کوچک پیوست‌شده به هر تراکنش را به‌عنوان پاداش دریافت خواهند کرد. در فصل‌های بعد، به‌طور مفصل‌تری در مورد استخراج بیت‌کوین صحبت می‌کنیم، اما نکته‌ای که در اینجا حائز اهمیت است، آن است که زنجیره بلوک، در قطعه‌های تقریبا ۱۰ دقیقه‌ای که به آنها بلوک گفته می‌شود، ثبت می‌شود. هر بار که استخراج‌گری، گروهی از تراکنش‌ها را به‌درستی تایید کند، پاداش دریافت می‌کند.

زنجیره بلوک، امکان ثبت، ردیابی و وارسی هر تراکنش و تراز حساب را فراهم می‌سازد. علاوه بر این، رمزنگاری و غیرمتمرکزسازی، مهارت‌های نسبتا پایه کاربر برای ناشناس ماندن قابل قبول در تراکنش‌ها را افزایش می‌دهند و در نتیجه، امنیت و حریم شـــخصی، همزمان با هم تامین می‌شود. علاقه‌مندان به بیت‌کوین، در پاسخ به انتقادات مربوط به فروش برخط کالاهای غیرقانونی، خواهند گفت که بیت‌کوین ناشناس نیست، بلکه به نام مستعار وابسته است. ناشـــناس بودن، بدان معناست که هیچ شناسه[۶۸]ای در اختیار شما قرار ندارد، اما وابسته به نام مستعار بودن، بدان معناست که شناسه‌ای در اختیار شما قرار دارد که مستقیما به هویت زندگی واقعی شما اشاره نمی‌کند (همانند آدرس بیت‌کوین).

با وجود آنچه پیش‌تر بیان شـــد، در بعضی از تکنیک‌های بیت‌کوین بالاتر از سطح ابتدایی، وابسته به

نام مستعار ماندن، به‌سادگی جایش را به ناشناس ماندن خواهد داد. با این وجود، بیت‌کوین همان چیزی است که آینده‌پژوهان و اقتصاددانان دهه ۱۹۹۰، هم به آن تمایل داشتند و هم از آن می‌ترسیدند. در این مورد که آیا ارزهای اینترنتی، همان‌طور که بیان شـد، ناشـناس یا قابل ردیابی هستند، همواره اختلاف نظرهایی وجود دارد. اما پاسخ به این سوال، هر دو مورد را در بر می‌گیرد. به بیان دیگر، هر چیزی ردیابی می‌شود، اما کاربران می‌توانند هویت واقعی خودشان را مخفی کنند.

با این حال، از مدت‌ها قبل از اختراع یک شکل قابل استفاده از پول، هشدارهای زیادی در مورد خطرات بالقوه ارزهای دیجیتال مطرح شـده بود. برخی از این می‌ترسیدند که این دسـته از ارزها، مورد استفاده تروریست‌ها، فروشندگان مواد مخدر، باج‌گیرها، بچه‌بازها و سایر مجرمین قرار بگیرند. دوروثی دنینگ[۶۹]، در مقاله سال ۱۹۹۴ خودش در ژورنال «آموزش عدالت کیفری» و سپس در دانشگاه جورج‌تاون[۷۰]، به یکی از این خطرات اشاره کرد:

«برای پیاده‌سازی پول نقد غیرقابل رهگیری و تراکنش‌های ناشناس و غیر قابل رهگیری، می‌توانیم از رمزنگاری بهره بگیریم. اگرچه چنین سرویس‌هایی منافع زیادی را از لحاظ حریم شخصی فراهم خواهند ساخت، اما می‌توانند شیوه پولشویی و کلاهبرداری را نیز تسهیل کنند»[۷۱].

دنینگ تنها کسی نبود که چنین عدم اطمینانی را بیان می‌کرد. اسـتیون لوی[۷۲]، در مقاله دسامبر سال ۱۹۹۴ مجله Wired، از قـول یکی از اعضای انجمن بانکداران آمریکا، به نـام کاویکا داگویو[۷۳]، چنین می‌نویسد:

«به نظر من، اینکه اجازه تولید ارز دیجیتال با ارزش نامحدود و غیر قابل رهگیری را بدهیم، کاری غیرمنطقی و غیر قابل قبول اسـت. با این کار، راه برای سوءاستفاده افراد جنایتکار باز خواهد شد. در دنیای فیزیکی، پول، جا اشغال می‌کند و می‌توان افراد را ردیابی کرد. بنابراین، در صورت ثبت شماره‌های سریال و مشاهده پول در محل، می‌توان سارق را دستگیر کرد. پول نقد کاملا ناشناس، احتمال جعل و کلاهبرداری را بالا می‌برد.»[۷۴].

انتقاد داگویو از توان بالقـوه ارزهای دیجیتال ناشـناس، دقیقا همانند انتقادهایی اسـت که امروزه به بیت‌کویـن وارد می‌کنند. یعنی در مورد بیت‌کوین نیز از احتمال سوءاسـتفاده مجرمان، سـارقان و باج‌گیرها صحبت می‌شود. من، هم در مورد سوءاسـتفاده از ارز دیجیتال و هم در مورد استفاده بیشتر و طولانی‌مدت‌تر مجرمان از پول نقد، هیچ بحثی ندارم. اما واقعیت این اسـت که ارزهای دیجیتال، برای فعالیت‌های مجرمانه، از پول نقد مناسب‌ترند. بیت‌کوین، ابزار مفیدی به‌شمار می‌رود و همانند هر فناوری دیگری، خوبی‌ها و بدی‌هایی دارد. شـکی ندارم که فعالیت‌های مجرمانه در رابطه با ارزهای دیجیتال،

در آینده، پیچیده‌تر می‌شوند، اما در عین حال، استفاده از نوآوری‌ها و سرمایه‌گذاری‌های قانونی در این حوزه نیز افزایش خواهد یافت.

بیت‌کوین، یک ارز برخط، دفتر کل توزیع‌شده و یک شبکه غیرمتمرکز است، اگرچه هنوز هم ترس‌های بیان‌شده توسط پیشقراولان قدیمی اینترنت، در مورد آن مطرح هستند.

1- mastering bitcoin: unlocking digital cryptocurrencies
2- bitcoin: the naked truth about bitcoin
3- Bitcoin core
4- cryptography
5- money
6- proof of work
7- litecoin
8- multisig
9- Ian Demartino
10- Gavin Andresen
11- Andreas Antonopoulos
12- Bitcoin Foundation
13- Chamber of Digital Commerce
14- Hal Finney
15- Mike Hearn
16- Olivier Janssens
17- angel investor
18- crowdsource
19- Mark Karpeles
20- Wladimir van der Laan
21- Jed McCaleb
22- Satoshi Nakamoto
23- Dread Pirate Roberts
24- Amir Taaki
25- Peter Todd
26- Ross Ulbricht
27- Roger Ver
28- Cody Wilson
29- Craig Wright
30- Heavy Metal
31- Vicious Rumors
32- Max Keiser

33- Russia Today
34- distributed ledger
35- blockchain
36- public key
37- bitcoin address
38- private key
39- units
40- work unit
41- existence
42- representation
43- "Statistics and Facts about Online shopping", Statista, June 2014
44- "Attention Shoppers: Internet Is Open", The New York Times, Friday, August 12, 1994
45- Nikola Tesla
46- Marshal McLuhan
47- Understanding Media
48- Gutenberg Galaxy
49- global village
50- the medium is the message
51- in-home shopping
52- Pretty Good Privacy
53- Wolverton, Troy (May 10, 1999). "Netmarket exposes customer order data". CNET
54- Kevin Kelly
55- Out of Control: The New Biology of Machines, Social Systems, & the Economic World
56- online identification
57- online authentication
58- online reputation
59- online signature
60- cypherpunk
61- encryption
62- cipher
63- yin
64- yang
65- agreed-upon key
66- timestamp
67- Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Directory System"
68- identifier
69- Dorothy Denning
70- George Town
71- Crime and crypto on the information superhighway. Dorothy E. Denning Georgetown

University
72- Steven Levy
73- Kawika Daguio
74- Steven Levy, "E-Money (That's What I Want)," Wired Magazine