

بِسْمِ اللَّهِ
الرَّحْمَنِ
الرَّحِيمِ

۱

۲

۹

۸

پایان پول

داستان بیت کوین، رمزارزها و انقلاب بلاکچین

NewScientist
INSTANT EXPERT

راه برداشت

سرشناسه: روتستین، آدام. Rothstein, Adam / عنوان و نام پدیدآور: پایان پول؛ داستان بیت‌کوین، رمزارزها و انقلاب بلاکچین / آدام روتستین؛ ترجمه فاطمه ندیمی. / مشخصات نشر: تهران: صفحه سفید، ۱۳۹۸. / مشخصات ظاهری: ۲۰۴ ص؛ ۱۴/۵×۲۱/۵ س.م. / شابک: ۲-۳۵-۶۵۹۹-۹۶۴-۹۷۸ / وضعیت فهرست نویسی: فیفا / یادداشت: عنوان اصلی: The End Of Money / موضوع: بلاکچین / موضوع: تکنولوژی؛ / شناسه افزوده: ندیمی، فاطمه ۱۳۷۳ - مترجم / رده‌بندی کنگره: HG۲۵۶ / ر۹پ۲ ۱۳۹۷ رده بندی دیویی: ۱۷۸/۳۳۲

پایان پول

داستان بیت کوین، رمزارزها و انقلاب بلاکچین

نویسنده:

آدام روتستین

مترجم:

فاطمه ندیمی

NewScientist
INSTANT EXPERT

راه برداشت

پایان پول؛ داستان بیت‌کوین، رمز ارزها و انقلاب بلاکچین / ناشر: صفحه سفید / مؤلف: آدام روتستین /
ویراستار: یلدا شایسته‌فر / صفحه‌آرا: علیرضا کیوان / نوبت چاپ: اول ۱۳۹۸ / شمارگان: ۱۰۰۰ نسخه /
شابک: ۳۵-۳۵۹۹-۶۶۴-۹۷۸ / تمام حقوق این اثر محفوظ و متعلق به موسسه شبکه عصر تراکنش (راه
پرداخت) است / تلفن: ۰۹۱۰۶۹۴۹۳۰۲ / دورنگار: ۸۹۷۸۴۹۰۲ / پست الکترونیک: [@mediamanager.ir](mailto:mediamanager.ir)

[Way2Pay.ir / gmail.com](mailto:Way2Pay.ir@gmail.com) پایگاه اینترنتی: Way2Pay.ir

نشانی انتشارات و مرکز پخش: تهران، خیابان ولیعصر، بالاتر از عباس آباد، برج سرو ساعی، طبقه اول تجاری،
واحد ۲. تلفن: ۸۸۷۰۲۰۷۶-۷۷

فهرست

۲۱	فصل یک: بیت کوین؛ اصول اولیه
۲۷	فصل دوم: تولد بیت کوین
۳۹	فصل سوم: چگونه یک ارز خلق کنیم، مسیر رمزنگاری
۵۱	فصل چهارم: بلاکچین
۶۷	فصل پنجم: معدن کاوی طلا به روش دیجیتال
۸۳	فصل ششم: موارد مصرف بیت کوین در روزهای اولیه
۹۵	فصل هفتم: تجربه ناگوار گاکس
۱۰۵	فصل هشتم: توسعه کامل بیت کوین
۱۲۱	فصل نهم: آیا بیت کوین واقعا پول است؟
۱۴۱	فصل دهم: رجعت و عزیمت ساتوشی ناکاموتو
۱۴۷	فصل یازدهم: اصلاح بیت کوین و افزایش آلت کوین ها
۱۶۳	فصل دوازدهم: این فصل درباره پول نیست
۱۷۹	فصل سیزدهم: از بیت کوین تا شرکت های خودمختار
۱۹۹	فصل چهاردهم: نتیجه گیری

نحوه تعامل با بلاکچین

در باره فین تک و بلاکچین در سال های گذشته محتوای زیادی تولید شده است. یکی از مراکز تحقیقاتی که گزارش های جامعی در این زمینه منتشر کرده «مجمع جهانی اقتصاد» است. این نهاد در گزارشی با عنوان «the future of financial infrastructure» به تاثیر به کارگیری فناوری دفاتر کل توزیع شده بین ۹ بخش گوناگون ارائه دهنده سرویس های مالی پرداخته است. یافته ها حاکی از این است که این فناوری پتانسیل برآورده ساختن انتظارات و تغییر سرویس های مالی را دارد، اما در عین حال برای موفقیت نیازمند همکاری نهادهای گوناگون و استفاده از دیگر فناوری های در حال ظهور، توسعه رگولاتوری ها و بخش های دیگر است.

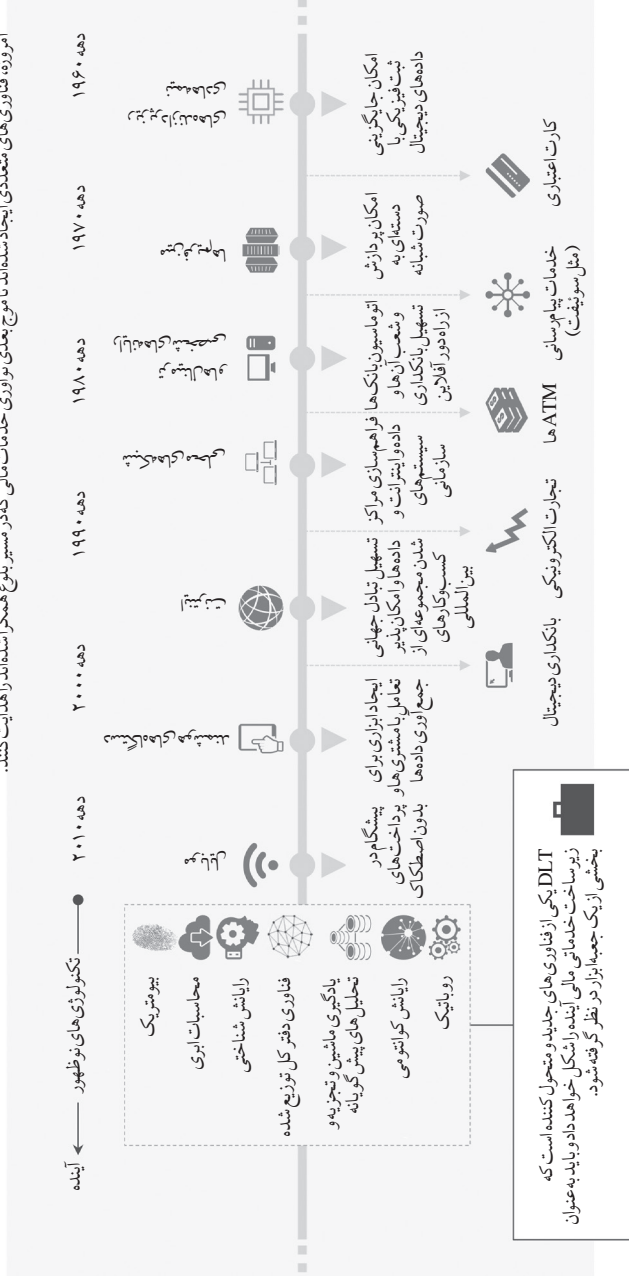


آگاهی نسبت به DLT به سرعت در حال افزایش است، اما موانع زیادی بر سر راه پیاده سازی آن در سطح گسترده وجود دارد. این موانع عبارت اند از:

محیط رگولاتوری بی ثبات و ناهماهنگ  تلاش های جمعی نو پا در استانداردسازی  فقدان چارچوب های قانونی رسمی

بخشی از گزارش آینده زیرساخت های مالی در باره اهمیت بلاکچین

امروزه، فناوری‌های متعددی ایجاد شده‌اند تا موجب پعضی نوآوری خدمات مالی که در مسیر بلوغ همگرا شده‌اند را هدایت کنند. در بیش از ۵۰ سال گذشته، نوآوری در حوزه فناوری، اساس تحول صنعتی خدمات مالی بوده است.



«بلاکچین» یک موضوع برآمده از دل فناوری است؛ ولی در این یادداشت از چهار زاویه متفاوت به اهمیت آن می‌پردازیم و با طرح چند پرسش اهمیت بلاکچین را بررسی می‌کنیم.

۱

نظام مالی جایگزین؛ چگونه؟

مهم‌ترین کارکرد بانک‌های مرکزی در جهان حفظ ارزش پول است؛ ولی عموم بانک‌های مرکزی جهان کارنامه موفقیتی در این زمینه نداشته‌اند؛ این موضوع در همه کشورهای جهان صدق می‌کند و به عنوان نمونه در ایران در طول ۵۰ سال گذشته هر سال به طور متوسط ۲۰ درصد از ارزش پول ملی کاسته شده است؛ ضعف در حفظ ارزش پول ملی این پرسش را پیش می‌کشد که چگونه می‌توان سیستم تصمیم‌سازی توزیع شده‌ای ساخت که بتواند کارکردهای رگول‌تورهای پولی را انجام دهد؟ پس با توجه به ضعف‌های رگول‌توری متمرکز پولی، چگونه می‌توان از یک نظام رگول‌توری پولی توزیع شده استفاده کرد؟ برخلاف محصول سیستم پولی متمرکز که هر سال شاهد تورم و کاهش ارزش دارایی‌ها هستیم، در محصولات شناخته شده و اصلی سیستم‌های توزیع شده در ۱۰ سال گذشته شاهد تورم منفی و افزایش ارزش دارایی‌ها به صورت مستمر بوده‌ایم. منتها هنوز زمان زیادی نگذشته و در آینده نزدیک ابعاد بیشتری از موضوع برای ما روشن می‌شود.

بلاکچین چیست؟

بلاکچین نوعی دفترکل توزیع شده (DLT) است و این وعده را می‌دهد که با ایجاد اعتماد، شفافیت و کاهش اصطکاک بین اکوسیستم‌های کسب و کار، کاهش هزینه‌ها، کاهش زمان تسویه و تصفیه تراکنش و بهبود جریان پولی باعث دگرگونی صنایع شود. امروزه به بانک‌ها، شرکت‌های تسویه و تصفیه و جوه، دولت‌ها و دیگر موسسه‌هایی اعتماد می‌کنیم که به عنوان مراجع مرکزی این حیطه شناخته شده و «تنها نسخه حقیقی تراکنش‌ها» را به شیوه‌ای امن در پایگاه داده خود دارند.

مدل مرکزی اعتماد باعث ایجاد تاخیر و هزینه در تراکنش‌ها می‌شود (کمسیون، کارمزد و ارزش زمانی پول). بلاکچین مدل اعتماد جایگزینی را در اختیارمان می‌گذارد و نیاز به مراجع مرکزی برای داوری تراکنش‌ها را از میان بر می‌دارد.

ایجاد محدودیت برای فساد؛ چگونه؟

فساد افسارگسیخته ریشه در نواقص ذاتی ساختارهای متمرکز دارد. تا امروز سیستم متمرکز را با همه آسیب‌های آن امتحان کرده‌ایم؛ آیا می‌توان راه جدیدی را تجربه کرد؟ فساد در سیستم‌های متمرکز در واسطه‌ها رخ می‌دهد. سوال درست این است که سیستم‌های توزیع شده چگونه فساد را محدود می‌کنند؟ با توجه به تعریفی که از بلاکچین ارائه شد، آیا می‌توان انتظار داشت که با جایگزینی واسطه‌های مبادله ارزش با سیستم‌های مبتنی بر بلاکچین شاهد تغییر در ساختارهای فساد باشیم؟ تجربه ۱۰ سال گذشته برای پاسخ به این سوال کافی نیست، ولی همین تجربه‌های اندک توانایی‌های جدی بلاکچین در ایجاد محدودیت برای فساد را نشان داده است.

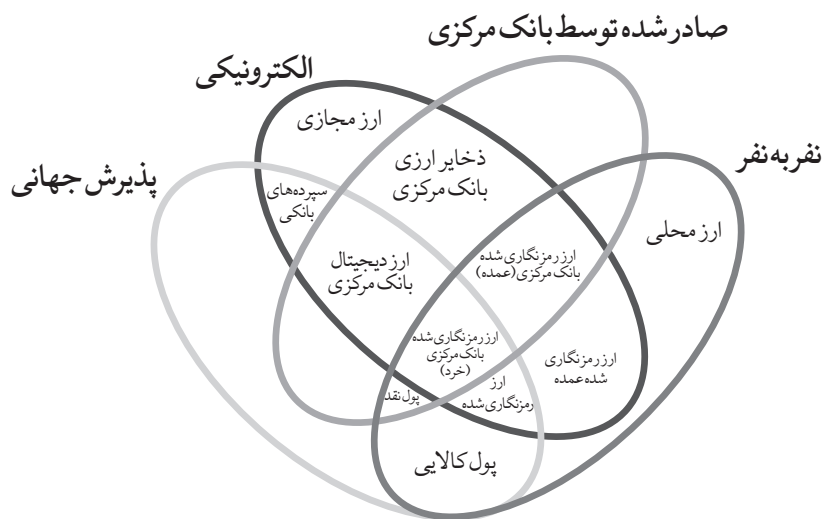
جبران ناکارآمدی‌های ذاتی پول؛ چگونه؟

«فریدریش آگوست فون هایک»، اقتصاددان و فیلسوف سیاسی در سال ۱۹۷۶ پیشنهاد ملی‌زدایی از پول را مطرح کرد. آن زمان پیشنهاد او چندان جدی گرفته نشد. تا اینکه بحران مالی سال ۲۰۰۷ نشان داد سیستم اقتصادی سرمایه‌داری از ناکارآمدی‌های درونی رنج می‌برد. هایک سال‌ها قبل از بحران مالی پیشنهاد خلق پول توزیع شده را داده بود. در دهه ۷۰ میلادی ابزارهای لازم برای آزمون این ایده وجود نداشت، اما در ۱۰ سال گذشته بلاکچین زمینه خلق و آزمون ایده پول توزیع شده را فراهم کرده است. کارکردهای سه‌گانه ارز؛ ذخیره ارزش، ابزار مبادله و واحد اندازه‌گیری است. سوال درست این است که با نگاهی به کارکردهای سه‌گانه ارز، پول‌های ملی در جهان چه وضعیتی دارند؟ آیا آنها توانسته‌اند در زمینه ذخیره ارزش و واحد اندازه‌گیری عملکرد مطلوبی داشته باشند؟ چگونه می‌توان محدودیت‌های ذاتی پول را مدیریت کرد؟ در سال ۱۳۴۰ با ۱۷ هزار تومان می‌شد یک خانه خرید. با ۱۷ هزار تومان امروز چه می‌توان خرید!

دیدگاه فقهی و پشتوانه؛ چگونه؟

بدون پشتوانه بودن پول در حال حاضر و خلق افسارگسیخته آن بعد از کنفرانس برتن وودز در جهان یک واقعیت است. با توجه به قانون پولی و بانکی کشور در حال حاضر ۵۵/۱۰۸ گرم طلا معادل ۱۰۰۰

تومان (۱۰۰۰۰ ریال) است! این در حالی است که در حال حاضر هر گرم طلا حدود ۴۰۰ هزار تومان است. پول ملی ایران هم مانند پول هر کشور دیگری بدون پشتوانه است. چگونه می توان پولی ساخت که پشتوانه داشته باشد؟ پول امروز ایران پشتوانه ای مانند طلا ندارد و ایراد بدون پشتوانه بودن فقط شامل ارزهای رمزنگاری شده (کریپتوکارنسی) نمی شود.



گل پول

با توجه به چهار زاویه دید و طرح چهار سوال لازم است گل پول را هم معرفی کنیم. گل پول یک تاکسونومی از پول است و جایگاه انواع گوناگون پول را نشان می دهد. در گل پول با توجه به چهار شاخص، پول ها مرز بندی شده اند: پذیرش جهانی (قابل استفاده بودن در محیط های گوناگون)، الکترونیکی بودن، قابل استفاده بودن به صورت نفر به نفر و صدور توسط بانک های مرکزی. به عنوان مثال پول نقد پولی است که توسط یک بانک مرکزی صادر شده و نفر به نفر قابل استفاده است و پذیرش جهانی دارد، ولی الکترونیکی نیست. همین پول نقد اگر به شکل الکترونیکی در بیاید، دیگر به صورت نفر به نفر (بدون واسطه) قابل استفاده نیست، ولی الکترونیکی است و پذیرش جهانی دارد و توسط بانک مرکزی صادر شده است. ر مزارز (پول یا ارز مبتنی بر بلاکچین) پولی الکترونیکی و نفر به نفر (بدون واسطه) است و پذیرش جهانی دارد، اما هیچ بانک مرکزی آن را صادر نکرده است. بنابراین اهمیت ر مزارزهایی

مانند بیت کوین این است که برای اولین بار به کمک فناوری پولی خلق شده که اعتبار و اعتماد آن از بانک مرکزی نمی آید و افرادی که به آن اعتماد می کنند، به آن اعتبار می دهند.

کسب و کارهای مبتنی بر دفاتر کل توزیع شده

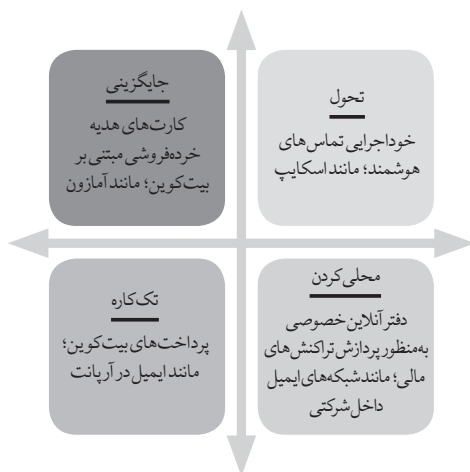
در صورتی که بخواهیم از مزایای دفاتر کل توزیع شده و بلاکچین نهایت استفاده را ببریم، باید بدانیم که تمام بخش های این اکوسیستم باید به صورت همزمان مورد توجه قرار بگیرند و توجه بیش از حد به یک بخش، باعث رشد ناقص اکوسیستم می شود؛ بخش های گوناگون اکوسیستم بلاکچین شامل حداقل ۱۲ بخش زیر است و همه آنها به صورت همزمان باید مورد توجه قرار بگیرند.

ارائه دهندگان زیرساخت	صرافی ها	ماینها
کارآفرینان	سرمایه گذاران	نودها
پژوهشگران	پذیرندگان	توسعه دهنده ها
اینفلوئنسرها	سرویس دهنده های پرداخت	کیف پول ها

مسیر تحول پیشنهادی

هنوز هیچ برنامه مشخص، تدوین شده و استراتژی مناسبی برای توسعه در زمینه بلاکچین وجود ندارد؛ چون هنوز کسی نیست که مسیر را به صورت کامل طی کرده باشد؛ بنابراین فعلاً بهترین راه آزمون و خطاست. موضوع بلاکچین فراتر از یک کسب و کار، صنعت یا نهاد است و همه بازیگران بخش های گوناگون اقتصاد تحت تاثیر آن قرار می گیرند و بنابراین باید نسبت به آن آگاه باشند؛ هر چقدر که زمان از دست برود و با موضوعات کم اهمیت دست و پنجه نرم کنیم، فرصت را به کلی از دست می دهیم؛ بهترین کاری که دولت و حاکمیت در زمینه بلاکچین می توانند انجام دهند، اقدام به ایجاد محیط سنبداکس برای انجام فعالیت در این زمینه است. منظور از سنبداکس کارگروهی از افراد متخصص در دولت و بخش های گوناگون کسب و کارها برای بررسی پیوسته فعالیت کسب و کارهای گوناگون در زمینه بلاکچین است. به عبارت دیگر لازم نیست دولت با ابزاری مانند مجوز به فکر سامان دهی این حوزه باشد؛ بنابراین صرفاً باید نقش نظاره گر را بازی کند و اجازه دهد روند تکاملی این فناوری در ایران طی شود. در صورت رشد ارگانیک و ملایم می توان انتظار داشت از مزایای فناوری بلاکچین و دفاتر کل توزیع شده برای حل چهار مساله گفته شده و برخی مسائل دیگر استفاده کرد. اما در صورت ورود زودهنگام یا عدم به روزرسانی

ذهنیت دولت، باید نظاره‌گر آثار تخریبی این فناوری باشیم. شایان ذکر است با نظر به ذات توزیع شده این فناوری، در صورتی که مانند موارد پیشین نتوانیم یا نخواهیم این فناوری را به صورت صحیح استفاده کنیم، آسیب‌های آن به مشکلات فعلی ما اضافه خواهد شد. همچنین با توجه به عدم بلوغ این فناوری حتماً باید فاکتور زمان را در نظر بگیریم. بنابراین تلاش برای بهره‌برداری پیش از موقع اشتباه است و نتایج فاجعه‌باری دارد، همچنان که بی‌توجهی و عدم به‌روزرسانی در این زمینه هم فاجعه‌بار است.



در همین زمینه و نظر به تغییرات در نظام مالی دنیا، کتاب «پایان پول» روایتی است غیرفنی از تغییراتی که فناوری در اقتصاد ایجاد خواهد کرد. اگر تا امروز جلوه‌های گوناگون به کارگیری فناوری را در ابزارها و سخت‌افزارها و حتی نرم‌افزارها و اپلیکیشن‌های گوناگون دنیای مالی دیده‌ایم، به لطف توسعه فناوری شاهد یک تغییر پارادایم جدی هستیم. نکته اینجاست که هنوز کسی از آینده پیش رو چیزی نمی‌داند و ممکن است شاهد تغییرات متعددی در مفاهیم مبهم امروز باشیم. این کتاب باروایت داستان گونه خود ماجرابی که امروز بخش‌های گوناگون فعالان اقتصادی را درگیر خود کرده، بسیار جذاب و کاربردی بیان می‌کند و خواندن آن به تمامی فعالان بخش‌های گوناگون اقتصادی علی‌الخصوص حوزه پرداخت توصیه می‌شود. امیدواریم انتشار این کتاب زمینه‌آشنایی بیشتر فعالان اقتصادی با زمینه‌های تغییرات در دنیای جدید را فراهم کند.

میناوالی

مدیرعامل موسسه تراکنش

یادداشت

کتاب «پایان پول» یکی از بهترین روایت‌ها در زمینه بیت‌کوین، کریپتوها و بلاکچین است؛ کتابی کم‌ادعا که ماجرا را روان‌تعریف می‌کند؛ آن‌هم چه تعریف‌کردنی! جذاب و البته کاربردی. نه بیش از حد فنی است که خوانش آن سخت باشد و نه کاسبکارانه و بازاری و سوار بر موج «چگونه با بیت‌کوین یک‌شنبه پولدار شویم». با اینکه برخی مطالب کتاب مشمول مرور زمان شده، ولی هنوز تمام مطالب کتاب درست است. «پایان پول» یکی از خوش‌روایت‌ترین هادرز مینه‌آینده پول است و هر کسی که می‌خواهد در باره آینده پول بداند، این کتاب را دوست خواهد داشت.

پایان پول به دور از پیچیدگی‌های معمول کتاب‌های اقتصادی و به دور از سخت‌فهمی‌های جافتاده در متن‌های فنی است. این کتاب به همه کمک می‌کند تصویر درستی در باره بخشی از آینده پیدا کنند. کتاب «پایان پول» یکی از جذاب‌ترین کتاب‌هایی است که ما تا امروز در راه پرداخت منتشر کرده‌ایم.

همان‌طور که بسیاری از مخاطبان ما می‌دانند، وب‌سایت راه‌پرداخت دوم اردیبهشت‌ماه ۱۳۹۰ فعالیت خود را شروع کرد؛ اولین شماره ماهنامه چاپی عصر تراکنش را تیرماه ۱۳۹۶ چاپ و منتشر کردیم که تا امروز به صورت مرتب و منظم هر ماه یک شماره ۱۱۶ صفحه‌ای از آن منتشر شده است؛ سال ۱۳۹۷ هم فعالیت‌های انتشار کتاب را به صورت جدی‌تر کلید زدیم و تا امروز ۳۲ هزار نسخه کتاب چاپ کرده‌ایم؛ سال ۱۳۹۸ در زمینه «وایت‌پیپر» جدی‌تر شدیم و تا امروز حدود ۴۰ وایت‌پیپر منتشر کرده‌ایم.

روند رشد راه‌پرداخت در طول هشت سال گذشته آهسته و پیوسته بوده است. در طول همه این سال‌ها تلاش کردیم یاد بگیریم و به دور از هیاهوها به تولید محتوای مفید و اثربخش بپردازیم. تمرکز ما بر ارائه محتوای مفید در زمینه‌های مرتبط با فین‌تک بوده است. فین‌تک به معنای کاربرد نوآورانه فناوری در خدمات مالی است. خدمات مالی نیز سه بخش اساسی دارد: بانکداری و پرداخت؛ بورس و بیمه. ما ابتدا بر حوزه‌های پرداخت و بانکداری متمرکز بودیم و به مرور بخش‌های دیگر را هم مورد توجه قرار دادیم. بیمه و بورس دو حوزه‌ای هستند که در یکی، دو سال اخیر به آنها پرداخته‌ایم؛ رویکرد ما هم این بوده که بخش‌هایی را مورد توجه قرار دهیم که رسانه‌های جریان اصلی کمتر به آنها می‌پردازند. سعی کردیم سلیقه راه‌پرداخت یک سلیقه متمایز باشد و

کسانی که راه پرداخت رادنبال می‌کنند، همیشه حس خوبی داشته باشند. این در حالی است که در طول سال‌های گوناگون تلاش کردیم یک رسانه مستقل در بخش خصوصی ایران باشیم. در این مسیر اعتماد مخاطبان ارزشمند راه پرداخت زمینه دست یافتن به بسیاری از اهداف را فراهم کرده است؛ این اعتماد به دست نمی‌آمد، اگر تیم همراه راه پرداخت در این سال‌ها جان‌برکف فعالیت نمی‌کردند.

به همین دلیل پرورش منابع انسانی متناسب با فرهنگ راه پرداخت آسان نیست. راه پرداخت سعی کرده سلیقه خاص خودش را داشته باشد و تیمی بسازد که در عین تنوع، همراه باشند و یک هدف مشترک رادنبال کنند. هدف مشترک همه ما هم تولید محتوای مفید و اثربخش در زمینه‌های مرتبط با فین‌تک ایران است. به مرور اعتماد فعالان بخش‌های گوناگون اقتصاد ایران به تیم راه پرداخت افزایش یافته و ما برای پاسخ به این اعتماد آرام‌آرام در حال توسعه راه پرداخت هستیم. ولی تلاش می‌کنیم این توسعه ما را از اهداف اصلی مان دور نکند. امیدواریم کماکان اعتماد مخاطبان راه پرداخت را همراه خودمان داشته باشیم و شایسته این اعتماد باقی بمانیم.

رضا قربانی

رئیس هیات مدیره موسسه تراکش

فصل یک

بیت کوین؛ اصول اولیه

بیت کوین دقیقا چیست؟ چگونه می توانی آن را به دست آورد؟ و چه چیزی می توانی با آن بخری؟

بیت کوین دقیقاً چیست؟

بیت کوین گونه جدیدی از ارز دیجیتال است که ارزش رمزنگاری شده نامیده می شود. بیت کوین توسط بانک ها کنترل نمی شود و حکومت ها از آن پشتیبانی نمی کنند، اما توسط شبکه نامتمرکز از کامپیوترهایی که از نرم افزار برای حل مسائل ریاضی استفاده می کنند، ایجاد شده است. بیت کوین به فناوری رمزنگاری که بلاکچین نام دارد، متکی است. بیت کوین اولین و در عین حال بزرگ ترین ارز رمزنگاری شده است، اگر چه اکنون تعداد زیادی از آنها وجود دارد.

چطور از بیت کوین استفاده کنم؟

بیت کوین ها وجود فیزیکی ندارند. آنها همانند دلار و یورو به کاغذ و فلز تبدیل نمی شوند؛ در عوض آنها در یک فایل دیجیتالی به نام «کیف پول» (Wallet) ذخیره می شوند. این کیف پول برای ارسال بیت کوین به دیگران استفاده می شود و همانند یک نرم افزار روی گوشی های هوشمند و همچنین رایانه ها نصب می شود.

چگونه بیت کوین به دست بیاورم؟

راه های زیادی وجود دارد. اولین راه استخراج (Mining) آنهاست. شما با تنظیم کامپیوترتان برای انجام محاسبات پیچیده رمزنگاری می توانید این شانس را داشته باشید که مقدار اندکی بیت کوین به دست بیاورید. در اصل این روشی است که ارزهای رمزنگاری شده توزیع می شوند. امروزه رقابت بر سر استخراج بیت کوین خیلی جدی است و به دست آوردن یک بیت کوین از این طریق بدون داشتن سرمایه ای عظیم بسیار دشوار است. با این حال شما می توانید با پرداخت پول از سرویس های «استخراج ابری» (Cloud mining)^۱ استفاده کنید (سرویسی که در آن شخص دیگری برای شما کار استخراج را انجام می دهد).

۱. استخراج ابری یک راه جایگزین برای ماینینگ بیت کوین است که در آن، شما می توانید از قدرت پردازشی دستگاه هایی که در پایگاه های داده به اشتراک گذاشته شده استفاده کنید. این شیوه به ویژه برای کسانی که از جزئیات فنی سردرمنی آورند یا نمی خواهند وقت زیادی به این کار اختصاص دهند، بسیار مناسب و کارآمد است.

راه دیگر برای به دست آوردن بیت کوین، خرید نقدی از شخصی است که مقداری از آن را دارد. وبسایت‌هایی نظیر لوکال بیت کوین (Localbitcoin.com) افرادی را که در پی فروش بیت کوین در قبال گرفتن ارزهای سنتی نظیر دلار یا یورو هستند، به یکدیگر متصل می‌کند.

روش دیگر برای دستیابی به بیت کوین مراجعه به صرافی‌های آنلاین بیت کوین است که این امکان را به شما می‌دهند که یک ارز نظیر دلار، پوند، یورو، یوان یا بیت کوین را به ارز دیگری تبدیل کنید (درست مثل اتفاقی که در صرافی‌های فیزیکی می‌افتد). «مت گاکس» (Mt.Gox) روزی بزرگ‌ترین مرکز مبادلات بیت کوین بود تا اینکه در سال ۲۰۱۴ فروپاشید. در پایان سال ۲۰۱۶ بزرگ‌ترین صرافی بیت کوین به لحاظ حجم معاملات «بیت مکس» (BitMEX) بود.

اخیراً خدماتی ارائه می‌شود که به مشتریان این امکان را می‌دهد که حساب‌های بانکی‌شان را به حساب ارز رمزنگاری شده خود متصل کنند و به آنها اجازه می‌دهد که بیت کوین‌هایشان را با استفاده از کارت‌های بانکی به یک ارز محلی و سنتی نظیر دلار و پوند تبدیل کنند و برعکس. کوین بیس (Coinbase) و بیت پی (Bitpay) از جمله شرکت‌هایی هستند که چنین خدماتی را ارائه می‌دهند.

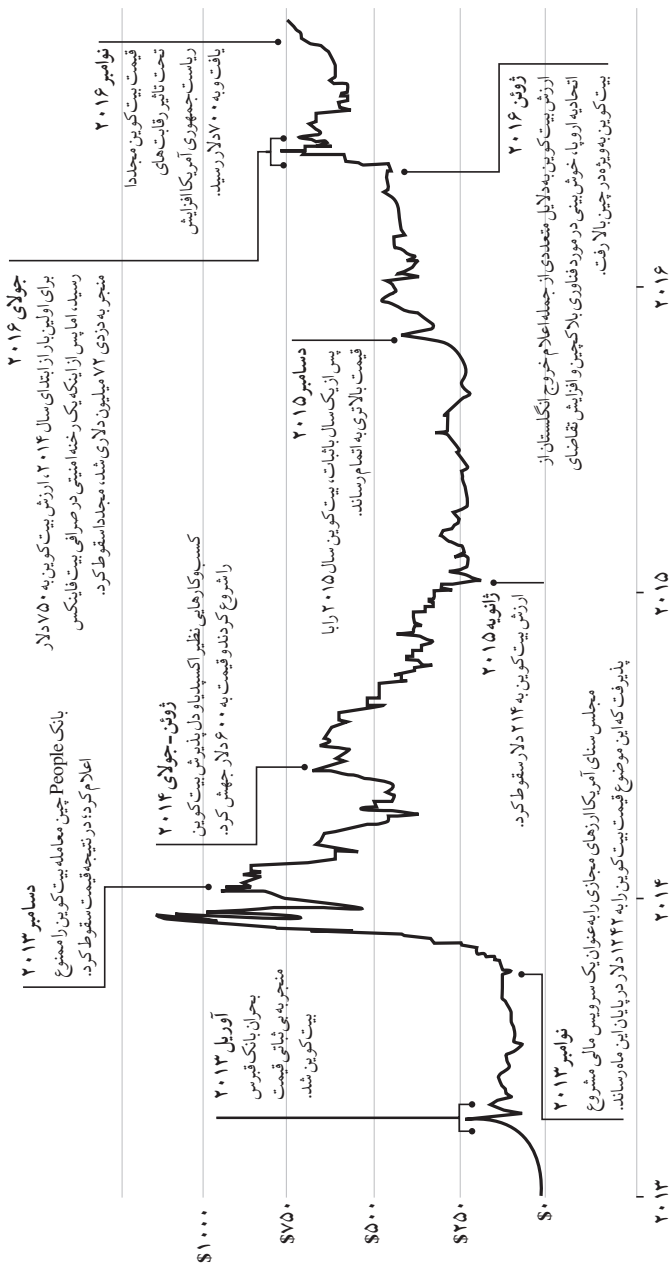
و در آخر، یک راه مستقیم برای به دست آوردن بیت کوین این است که در قبال فروش کالاها و خدمات آنها را بپذیرید. شرکت‌هایی نظیر «استرایپ» و «پی میوم» چنین خدماتی را برای کمک به تاجران جهت پذیرش ارزهای رمزنگاری شده در کسب و کارشان ارائه می‌دهند.



شکل ۱: سمبل بیت کوین که توسط ساتوشی ناکاموتو بلافاصله بعد از اختراع این ارز رمزنگاری شده ساخته شده است.

چه چیزی رامی توانم با بیت کوین بخرم؟

در اوایل پیدایش بیت کوین، افراد زیادی وجود نداشتند که بتوانند با آن چیزی بخرند. بازار مواد مخدر و دیگر اقدامات غیرقانونی جزء اصلی ترین بازارهایی بودند که در ابتدا، بیت کوین را در معاملات خود به کار بردند. امروزه بسیاری از کسب و کارهای اصلی مستقیماً بیت کوین را پذیرش می کنند و شرکت هایی نظیر بیت پی و کوین بیس امکانی برای مشتریان شان فراهم آورده اند که بتوانند برای هر تراکنش کارت اعتباری از بیت کوین استفاده کنند.



شکل ۲: ۱: فراز و فرود: مالکان بیت کوین باید برای نوسانات قیمتی آماده باشند.

*نسخه به روز شده این نمودار در بخش ضمایم کتاب ارائه شده است

فصل دوم

تولد بیت کوین

در سال ۲۰۰۸ شخصی که وجود خارجی نداشت، یک ایده داشت. در سال ۲۰۱۱ ارزش آن ایده بیش از ۵۴ میلیون دلار بود. این داستان اختراع یک ارز رادیکال جدید بود.

ایده‌های مالی تغییر جهان معمولاً به صورت ناگهانی و غیرمنتظره در صندوق‌های پستی الکترونیکی ظاهر نمی‌شوند. بنابراین «آدام بک» که در حوزه رمزنگاری فعالیت می‌کرد، توجه چندانی به ایمیلی که در آگوست ۲۰۰۸ از جانب فردی به نام ساتوشی ناکاموتو دریافت کرده بود، نشان نداد. در آن ایمیل ناکاموتو ایده‌ای برای توسعه یک ارز مجازی جدید ارائه داده بود. اکثر افرادی که در فهرست ایمیل سایفرپانک‌ها^۱ حضور داشتند (از جمله آدام بک که از سال ۱۹۹۲ از اعضای این فهرست بوده است) ایده‌هایی برای ساخت یک ارز که صرفاً در بین رایانه‌ها وجود داشته باشد، در سر داشتند و این موضوع برای آدام موضوع جدیدی نبود. بنابراین او وقت زیادی را صرف بررسی ایمیل ناکاموتو نکرد، به خصوص آنکه از طرف یک فرد ناشناس ارسال شده بود.



هویت مخترع بیت‌کوین ساتوشی ناکاموتو در حاله‌ای از ابهام قرار دارد.

این اولین باری بود که کسی در مورد ناکاموتو چیزی شنیده بود؛ نامی که تصور می‌شود توسط یک فرد یا گروهی ناشناس ساخته شده باشد. آن ایده (که در آن زمان آزمایش و اثبات نشده بود) بیت‌کوین نامیده شد. کمتر از سه سال بعد، زمانی که دیگر خبری از ساتوشی ناکاموتو در فضای وب نبود، ارزش کل بیت‌کوین‌های موجود بیش از ۵۴/۵ میلیون دلار بود، اما مبدع این ارز رمزنگاری شده هنوز به طور قطعی شناخته نشده است. زمانی که ناکاموتو ناپدید شد، کد

۱. سایفرپانک‌ها گروهی بودند که به طور گسترده‌ای از رمزنگاری برای بالا بردن امنیت در اینترنت استفاده می‌کردند. آنها در گروه‌های غیررسمی و همچنین با استفاده از پست الکترونیک با یکدیگر ارتباط برقرار می‌کردند. سایفرپانک‌ها در اواخر دهه ۸۰ میلادی به یک جنبش فعال در ایالات متحده تبدیل شدند.

نرم افزار منبع بازش برای این گونه جدید از ارز، بارها و بارها بازنویسی شده بود؛ به گونه ای که مشکل می توان گفت ساتوشی ناکاموتو این نرم افزار را نوشته است. برآورد شده است کمتر از یک سوم کدهای رایانه ای بیت کوین که در حال حاضر استفاده می شود، توسط ناکاموتو نوشته شده است.

واقعیت این است که همانند بسیاری از چیزهایی که اینترنت را تشکیل داده، در حال حاضر بیت کوین متعلق به همه است و هیچ فردی نمی تواند خود را مالک آن بداند. ایده های عجیبی نظیر بیت کوین در بین همه متخصصان کامپیوتر، برنامه نویسان، ریاضی دانان و سایفرپانک های دنیا (که طرح های پیچیده بسیاری را برای تضمین امنیت فناوری طراحی می کنند) مشترک است. آنها در ابتدا ایده های شکاکانه ای هستند که به عنوان «کار بزرگ بعدی» مورد ستایش قرار می گیرند. همچنان که بیت کوین نیز محتمل بود یکی دیگر از ایده هایی باشد که در گمنامی از بین می رود. بیت کوین نخستین ایده برای ارز مجازی نبود و هیچ یک از طرح های پیش از آن نیز به طور کامل حذف نشده بودند.

لطفا ساتوشی ناکاموتوی واقعی خودش را معرفی کند!

تلاش های زیادی صورت گرفته تا هویت واقعی خالق بیت کوین را آشکار سازد، اما همه آنها با شکست همراه شده است.

در اکتبر ۲۰۱۱ «جاشوا دیویس» خبرنگار مجله «نیو یورکر» این ادعا را مطرح کرد که «مایکل کلین» متخصص کامپیوتر همان ساتوشی ناکاموتو است. وی ادعایش را بر اساس سوابق او در حوزه رمزنگاری، مشخصات نگارشی مورد استفاده وی (با تطبیق دادن با نوشته های ساتوشی ناکاموتو) و عدم انکار مایکل کلین در نخستین باری که از او در این رابطه سوال شد، بنا نهاد (هرچند بعدها کلین این موضوع را کاملاً رد کرد).

«آدام پنبرگ» (از مجله Fast company) معتقد است که ناکاموتو باید یکی از این سه رمزنگار یعنی «نیل کینگ»، «ولادیمیر اوکسمن» یا «چارلز بری» باشد که نام شان در یک اپلیکیشن ارز رمزنگاری شده، درست سه روز قبل از اینکه ساتوشی ناکاموتو دامنه Bitcoin.org را ثبت کند، مشاهده شده است، اما در نهایت کاشف

به عمل آمد که این ارتباطات اتفاقی بوده است.

گروهی از کاربران انجمن

میلیارد دلار

۹/۲۹

ارزش کل بیت کوین‌های موجود (اگوست ۲۰۱۶) بیت کوین در سال ۲۰۱۲ از «جد مک کالب»^۱ بنیان‌گذار

«مت‌گاکس»^۲ نام بردند و این ادعا را مطرح کردند که ممکن است اوساتوشی باشد. متون دیگر انجمن‌ها حول و حوش تئوری توطئه می‌چرخید؛ تا جایی که این اعتقاد وجود داشت که بیت کوین توسط سازمان سیا یا آژانس امنیت ملی ایالات متحده به منظور به دام انداختن مجرمان از همه‌جایی خبر بنیان گذاشته شده است. در سال ۲۰۱۳ و پس از دستگیری «راس اولبریکت»^۳ بنیان‌گذار فروشگاه غیرقانونی سیلک‌رود^۴ در وب تاریک، دو پژوهشگر اسرائیلی به این نتیجه رسیدند که اولبریکت همان ناکاموتوی معروف است.

در مارس ۲۰۱۴ «لی مک‌گراث» خبرنگار هفته‌نامه «نیوزویک» ادعایی را مطرح کرد که مثل بمب ترکیب. او گفت که نام اصلی خالق بیت کوین، واقعاتاتوشی ناکاموتو است. هرچند او با نام کوچکش «دوریان» شناخته می‌شود. او ادعایش را بر اساس تجربه و مهارت برنامه‌نویسی دوریان ناکاموتو و اقامت طولانی مدت وی در سیلیکون‌ولی مطرح کرد.

«اندی گرینبرگ» نویسنده مجله فوربس برای از اعتبار ساقط کردن فرضیه پیشین (دوریان ناکاموتو) تحقیقات خود را آغاز کرد و به این نتیجه رسید که این امکان وجود دارد که «هال فینی» (از پیشگامان و توسعه‌دهندگان بیت کوین) ناکاموتوی واقعی باشد، اما خیلی زود این فرضیه را رد کرد.

«ناتانائیل پوپر» نویسنده کتاب «طلای دیجیتال» اظهار می‌کند که «نیک زاو» (سایفرپانک، سرمایه‌گذار بیت کوین و خالق نخستین ارز مجازی یعنی بیت‌گولد)

1. Jed McCaleb

2. MT. Gox

3. Ross Ulbricht

4. Silk road

ساتوشی ناکاموتو است. زابو علنا این ادعا را رد کرده است.

در اواخر سال ۲۰۱۵ مجله «وایرد» و همچنین وبسایت «گیز مودو» به اسنادی دست پیدا کردند که نشان می‌داد کریگ رایت برنامه‌نویس استرالیایی ساتوشی ناکاموتوی واقعی است. او هرچند در ابتدا این موضوع را انکار کرد، اما در بهار سال ۲۰۱۶ اعلام کرد که ناکاموتو است و او بوده که با همکاری «دیو کلايمن» (در زمان حیاتش) بیت کوین را ساخته است. هرچند کریگ رایت توانست شواهد قابل توجهی را در این زمینه ارائه دهد، اما این برای راضی کردن بسیاری از افراد شکاک کافی نبود و بنابراین این راز همچنان ناشناخته باقی ماند (برای اطلاع بیشتر در این زمینه فصل ۱۰ را بخوانید).

اولین بیت کوین

ناکاموتو پس از فرستادن ایمیل به آدام بک (و دریافت نکردن پاسخ) تسلیم نشد. او ایده خود را به ایمیل افرادی که در حوزه رمزنگاری فعالیت می‌کردند، فرستاد. ناکاموتو همچنین ایده‌اش را روی وبسایت P2PFUNDATION که در حوزه فناوری‌های همتا به همتا فعالیت می‌کرد، قرار داد. یک برنامه‌نویس با نام هال فینی که روی پروژه PGP (یک نرم‌افزار رمزگذاری رایگان) کار می‌کرد، ارزش بیت کوین را فهمید. جذابیت نهفته بیت کوین و خاصیت توزیع‌شدگی آن، هال فینی را به همکاری با ساتوشی ترغیب کرد. او در اوایل سال ۲۰۰۹ برای اولین بار یک بیت کوین را از ساتوشی ناکاموتو دریافت کرد، هرچند در آن زمان ارزش چندانی نداشت. به آهستگی و با اطمینان، بیت کوین رشد خود را آغاز کرد. دو برنامه‌نویس تازه‌کار به نام‌های «گوین اندرسون» و «مارتی مالمی» از ایده بیت کوین خوش‌شان آمد و به ناکاموتو در ایجاد یک وبسایت و همچنین توسعه و بهبود کد بیت کوین کمک کردند. آنها اصطلاح «رمزارز»^۱ را برای توصیف ارز مجازی که با استفاده از رمزنگاری ساخته شده، ابداع کردند. همچنین در پاییز سال ۲۰۰۹ انجمنی را برای جامعه نوظهور گیک‌های رمزنگاری، آزادی‌خواهان و برنامه‌نویسانی تأسیس کردند که رویاهای عجیب و غریبی برای ساختن ارزی

غیر متمرکز که بتواند واقعا کار کند در سر داشتند.

اغلب توسعه دهندگان ایده اولیه را اصلاح، روی آن کار کردند و نیز توسعه دادند. به نظر می‌رسید آنها می‌خواهند بیت کوین را به چیزی بیشتر از صرفاً یک ایده تبدیل کنند. کد کار می‌کرد و انعطاف‌پذیر بود. هرچه تعداد بیشتری از افراد نرم‌افزار را دانلود و کامپیوترشان را تنظیم می‌کردند تا وظایف لازم برای استخراج ارز را انجام دهد، بیت کوین استوارتر ظاهر می‌شد. اگرچه جنبه فنی بیت کوین خوب به نظر می‌رسید، اما سایر جنبه‌ها همچنان کمبود داشتند. تا آغاز سال ۲۰۱۰ هنوز روش خوبی برای خرید بیت کوین وجود نداشت و همچنین هیچ چیزی نمی‌شد با آن خرید. تنها برخی وبسایت‌های کوچک بودند که برخی کالاهای منتخبشان نظیر تی‌شرت یا استیکر را در ازای بیت کوین می‌فروختند. اما یک رخداد مشهور در آوریل سال ۲۰۱۰ رخ داد؛ یکی از علاقه‌مندان به بیت کوین با نام «لازلو هانیچ» در انجمن گفت‌وگوی بیت کوین، دو پیتزا را در ازای پرداخت ۱۰ هزار بیت کوین سفارش داد، در حالی که آن زمان بیت کوین به سختی ابزاری قابل اعتماد برای سفارش پیتزا قلمداد می‌شد.

انتشار ویروسی

در جولای ۲۰۱۰، وبسایت اسلش دات^۱ (اخبار فناوری روز دنیا) در صفحه اول خود مقاله‌ای در خصوص بیت کوین منتشر کرد. پس از انتشار این مقاله، دانلود برنامه تقریباً هفت برابر شد. بیت کوین به صورت ویروسی در حال انتشار بود، اما هنوز راهی برای اینکه همه علاقه‌مندان به بیت کوین، بتوانند آن را داشته باشند، وجود نداشت.

شبکه بیت کوین، بیت کوین‌های جدید را در ازای محاسبات پیچیده‌ای که «اثبات کار»^۲ نام دارد، توزیع می‌کند (فصل ۴ را مشاهده کنید). در روزهای ابتدایی وقتی یک کامپیوتر نرم‌افزار را اجرا می‌کرد تا یکی از این «بلوک‌ها»^۳ را حل کند، برای این تلاشش ۵۰ بیت کوین جدید به عنوان پاداش دریافت می‌کرد و به کیف پول مجازی‌اش اضافه می‌شد (فصل ۵ را مشاهده کنید). در واقع فرایند اثبات کار این مساله مهم که این بیت کوین از کجا آمده را حل می‌کرد، چرا که هیچ بانک مرکزی وجود نداشت

1. Slashdot
2. Proof of work
3. Block

که آن را توزیع کند.

آدام بک زمانی که تنها چند کامپیوتر در شبکه وجود داشت، این ادعا را مطرح کرد که گرفتن پاداش (یا همان بیت کوین) کار سختی نیست. تخمین زده می شود در سال نخست اختراع بیت کوین و زمانی که کامپیوتر ساتوشی ناکاموتو تنها کامپیوتر موجود در شبکه بود، در کیف پول الکترونیکی او حدود یک میلیون بیت کوین ذخیره شده باشد. اما وقتی تعداد بیشتری از افراد شروع به اجرای نرم افزار کردند، حل کردن بلوک ها سخت تر و سخت تر شد (به فصل ۵ مراجعه کنید). افراد زیادی وجود داشتند که فرایند اثبات کار را انجام می دادند و برای یک کامپیوتر شخصی اتصال به شبکه و شانس برنده شدن یک بلوک تقریباً غیر ممکن شد و به برنده شدن در یک لاتاری شبیه بود. در آن زمان، هنوز بیت کوین بهای چندانی نداشت. وقتی افراد آنها را با پول نقد معاوضه می کردند، هر کدام تنها چند سنت ارزش داشتند. این معاملات به عنوان یک آگهی ویژه در انجمن های اینترنتی به وسیله ایمیل انجام می گرفت. اگر سیستمی وجود نداشته باشد که بتوان از طریق آن به راحتی ارزش دلاری بیت کوین را به دست آورد، چطور افراد می توانند از آن به عنوان ارز استفاده کنند؟ این نیاز به شدت احساس می شد که مردم بتوانند به نرخ بازار، بیت کوین بخرند و برای خرید کالاهای مورد نیازشان از آن استفاده کنند.

آیا اهمیت دارد که ساتوشی کیست؟

هویت بنیان گذار بیت کوین یکی از بزرگ ترین رازهای دنیای اینترنت است. اما آیا واقعا اهمیتی دارد که او کیست؟

نه تنها ساتوشی ناکاموتو یک شخصیت تاریخی است که انبار دیجیتال بزرگی از ارزش را بنانهاده است، بلکه او احتمالا کنترل بخش قابل توجهی از این ارزش را نیز در دست دارد. کارشناسان تخمین می زنند ارزش بیت کوین هایی که در اختیار اوست، بیش از ۶۰۰ میلیون دلار باشد که صرف نظر از ارزش مبادله ای بیت کوین، این مقدار نزدیک به پنج درصد از کل بیت کوین های موجود در شبکه است که روزی ظرفیت آن تکمیل می شود (مترجم: پس از اینکه ۲۱ میلیون بیت کوین استخراج شد، استخراج بیت کوین متوقف می شود)؛ در نتیجه هر فردی که بخشی از این ارز را نگاری شده را کنترل کند، قطعاً می تواند تسلط زیادی روی آن داشته باشد. با این حال بسیاری از علاقه مندان به رمزارزها، از ناشناخته ماندن هویت واقعی

ساتوشی ناکاموتو خوشحال هستند. بدون یک بنیان گذار، دیگر هنری فورد یا استیو جابزی هم وجود نخواهد داشت. هیچ شخصیت محوری و کاریزماتیکی نیست که با اعلام نظرش بخواهد مسیر توسعه بیت کوین را تعیین کند. در عوض هر فردی با یک ایده جذاب که قابلیت پیاده سازی و فروش داشته باشد، می تواند در این شبکه ترفیع پیدا کند.

کنجکاوی های سیری ناپذیر در مورد هویت ساتوشی ناکاموتو متوقف نخواهد شد. اینکه هویت یک شخصیت عمومی تا این اندازه در پوششی از رمز و راز قرار گرفته باشد، پدیده ای نادر است؛ کسی که بدون باقی گذاشتن هیچ اثری از خود ناپدید شد. نظر او در مورد توسعه ارزهای رمزنگاری شده چیست؟ ایده بیت کوین از کجا آمد؟ او در حال حاضر به چه کاری مشغول است؟ ممکن است پاسخ این سوالات را هرگز پیدا نکنیم.

صرافی

جد مک کالب یکی از خیل مشتاقان بیت کوین بود. او یکی از توسعه دهندگان برنامه ای برای به اشتراک گذاری فایل با نام yeknoD-e بود که با استفاده از فناوری همتا به همتا کار می کرد. مک کالب با استفاده از دامین یک وبسایت قدیمی که به پروژه بازی کارتی M:cigaT:GehTgnirehta مربوط بود، یک صرافی بیت کوین با نام مت گاکس را راه اندازی کرد که در آن هر کسی بر اساس نرخ بازار (بر مبنای میزان عرضه و تقاضا) و با استفاده از دلار آمریکا می توانست بیت کوین خرید و فروش کند. هنگامی که وبسایت معروف اسلش دات مت گاکس را معرفی کرد، بر شهرتش افزوده شد و خیلی زود عنوان اولین صرافی واقعی بیت کوین را از آن خود کرد.

حالا امکان خرید بیت کوین به وسیله دلار فراهم شده بود، اما همچنان نمی شد با بیت کوین چیزی را خرید. ولی دو رخداد در ابتدای سال ۲۰۱۱ باعث به وجود آمدن تغییری شد. در دسامبر ۲۰۱۰ هنگامی که وبسایت افشاگر «ویکی لیکس» اطلاعات طبقه بندی شده دولت آمریکا را روی اینترنت منتشر کرد، پی پال و دیگر شرکت های پرداخت، ارائه خدمات مالی به ویکی لیکس را قطع کردند. آزادی خواهان، سایفرپانک ها و فعالان



قیمت بیت کوین پس از بازگشایی صرافی
مت گاکس (جولای ۲۰۱۰)

اینترنتی این حرکت را به عنوان سانسور نگوئید و در میان آنان بیت کوین به عنوان یک راه حل بالقوه برای حل این مساله و ارائه کمک مالی به ویکی لیکس مورد بحث قرار گرفت. کاربران می توانستند با استفاده از بیت کوین و بدون اینکه شرکتی این مساله را کنترل کند، کمک های مالی خود را به هر فرد یا سازمانی که می خواستند پرداخت کنند و هیچ دولتی هم نمی توانست کسی را به تبعیت از تحریم های ویکی لیکس مجبور کند. با این اتفاق قیمت بیت کوین در عرض یک ماه در صرافی مت گاکس، ۳۰ سنت افزایش پیدا کرد.

بازار

دو ماه بعد، ایده آلیست دیگری تصمیم گرفت توانایی بیت کوین برای دور زدن اعتبار و قدرت دولت را مورد آزمایش قرار دهد. شخصی که خودش را فقط با اسم مستعار «رابرت دزد دریایی ترسناک»^۱ معرفی می کرد، وب سایتی با نام «سیلک رود» راه انداخت که هدفش ساخت فروشگاه های همانند آمازون برای محصولات غیر قانونی و قاچاق با هدف به سرخه گرفتن نظارت و کنترل دولت بود. سیلک رود یک فلسفه داشت و آن هم فروش محصولات نظیر مواد مخدر و اسناد جعلی دولتی بود که صدمه جانی برای دیگران نداشته باشند و این در حالی بود که فروش اسلحه، پورنوگرافی های غیر مجاز و کارت های شناسایی سرقتی ممنوع بود. وب سایت سیلک رود تنها برای کاربرانی که از سامانه ای به نام تور^۲ (که برای ناشناس ماندن کاربران در محیط اینترنت به کار می رود) استفاده می کردند، قابل نمایش و استفاده بود. این ناحیه پنهان شده به عنوان وب تاریک^۳ شناخته می شود. بیت کوین تنها ارزی بود که در سیلک رود مورد پذیرش قرار می گرفت. خرید و فروش با بیت کوین در قیاس با کارت های اعتباری، گمنامی به مراتب بیشتری را برای کاربران به ارمغان می آورد. به همین دلیل بود که قاچاقچیان مواد مخدری که به خوبی از امکانات اینترنت برای پیشبرد مقاصدشان بهره می بردند، سیلک رود را با وجود آسیب پذیری اش یک مکان عالی قلمداد می کردند.

سیلک رود اینقدر محبوب شد که چندین بار در طول نیمه اول سال ۲۰۱۱ به علت شدت



بالاترین قیمت بیت کوین در تاریخ تا نوامبر ۲۰۱۳

1. Dread Pirate Roberts

2. Tor

3. Dark web

ترافیک از کار افتاد. مقاله‌ای در وبسایت Gawker (که در حال حاضر فعالیتش متوقف شده) با موضوع سیلک‌رود در ماه ژوئن همان سال منتشر شد. بلافاصله بعد از انتشار مقاله، کسب‌وکار سیلک‌رود به شدت رونق گرفت. اکنون چیزی هرچند غیرقانونی برای مردم وجود داشت تا بتوانند با بیت‌کوین هایشان آن را بخرند. قیمت یک بیت‌کوین در صرافی مت‌گاکس از ۷۰ سنت در فوریه ۲۰۱۱ به حدود ۱۰ دلار در ماه مه و ۳۲ دلار در اواسط ماه ژوئن رسید.

رونق سیلک‌رود توجه عمومی ناخواسته‌ای به سمت بیت‌کوین روانه کرد. در ۵ ژوئن ۲۰۱۱ چاک شوهر، سناتور آمریکایی ضمن برگزاری یک کنفرانس مطبوعاتی، سیلک‌رود و بیت‌کوین را محکوم کرد و با فشار به مقامات فدرال خواستار نابودی آنها شد. سازمان مبارزه با مواد مخدر و وزارت دادگستری آمریکا با انتشار یک بیانیه مطبوعاتی نگرانی خود را در این زمینه اعلام کردند. در ماه ژوئن «رابرت دزد در یایی ترسناک» به طور داوطلبانه و به امید اینکه تنش‌ها کاهش پیدا کند، سیلک‌رود را تعطیل کرد.

با افزایش بدنامی بیت‌کوین، عده‌ای سعی کردند فاصله خودشان را از آن حفظ کنند. جد مک کالب، بنیان‌گذار مت‌گاکس غرق در استرس محافظت از سایت در برابر نفوذ هکرها بود. پیش از این چنین حمله‌ای از سوی هکرها باعث نفوذ به سایت شده و بر اثر آن در ژانویه ۲۰۱۱، معادل ۴۵ هزار دلار بیت‌کوین ربوده شده بود. در ماه مارس، مک کالب، مت‌گاکس را به توسعه‌دهنده دیگری فروخت.

در آوریل ۲۰۱۱ توسعه‌دهندگان نرم‌افزار

بیت‌کوین شاهد آخرین صحبت‌های

ساتوشی ناکاموتو بودند. او در چندین ایمیل

کوتاه، نگرانی‌هایش را در مورد اصرار بر

استفاده از بیت‌کوین برای انجام اعمال

ضد حکومتی و همچنین استفاده از نام

مستعارش که به افسانه‌ای بدنام در بین هواداران بیت‌کوین تبدیل شده، بیان کرد و بدین ترتیب خالق اولین ارز رمزنگاری شده سخنان خود را برای همیشه به پایان رساند.

پس از آن نام کاربری ناکاموتو در انجمن بیت‌کوین حذف و ایمیل‌هایش نیز متوقف شد و خالق ناشناس بیت‌کوین به همین سادگی به موجودیتش پایان داد.

۴۵۰
میلیون دلار
ارزش بیت‌کوین‌های دزدیده‌شده در مت‌گاکس.
(فوریه ۲۰۱۴)