10 اصل بیت کوین که هر سرمایه گذار باید بداند

توسط **ایمان کیمیایی** آخرین به روز رسانی **10 اکتبر 2018**

بیت کوین اخبار برگزیده بلاک چین

سرمایه گذاران معمولا بی ثبات هستند و اغلب به سمت هر چیزی که برای سرمایه گذاری پیشنهاد شود و به نظر می رسد که سریع تر به سود و ثروت می رسند، گرایش دارند. در سال 2017 افزایش بیش از 10000 دلاری بیت کوین در طول مدتی کوتاه، سبب شد که سرمایه گذاران

زیادی را به سمت خود جلب کند. اما کاهش چشمگیر قیمت آن در سال 2018 موجب شد تا سرعت پذیرش این ارز رمزنگاری کاهش یابد. با این وجود، چیزی که سرمایه گذاران نمی توانند آن را انکار کنند این است که بیت کوین در حال پیدا کردن بازار و جایگاه خود در جهان است. که این مهم را از طریق افزایش قیمت و افزایش علاقمندان در سرمایه گذاری و نیز افزایش گرایش به فناوری بلاک چین به دست می آورد.

همانطور که سرمایه گذاران خاطرات بحران مالی 10 سال پیش را به خاطر دارند، سالگرد دیگری را نیز به خاطر می آورند. در اکتبر سال 2008، فردی با نام مستعار ساتوشی ناکاموتو مقاله ای را در مورد مفهوم بیت کوین منتشر کرد. حتی بعد از گذشت یک دهه این مقاله توضیح مناسبی را در مورد چگونگی کار بیت کوین بیان می کند و خواندن آن برای هر کسی که می خواهد در بیت کوین سرمایه گذاری کند، ضروری است. در این جا به مناسبت دهمین سالگرد بیت کوین به 10 نکته کلیدی در این مقاله ناکاموتو اشاره می شود.

1) بیت کوین بدون واسطه است

> تجارت در اینترنت تقریبا به طور انحصاری در دست موسسات مالی است که به عنوان شخص ثالث مورد اعتماد قرار دارند. آنچه لازم است، جایگزینی یک سیستم پرداخت الکترونیکی مبتنی بر اثبات رمزنگاری به جای اعتماد است.

طرفداران و علاقمندان ارز رمزنگاری این واقعیت را دوست دارند که بیت کوین تحت اختیار و سلطه یک قدرت متمرکز مثل بانک نیست، به خصوص زمانی که این قدرت متمرکز توانایی و پتانسیل نقض کردن را داشته باشد. به عنوان مثال شرکت های ارائه دهنده کارت های اعتباری در

بعضی شرایط، این امکان را به خریداران می دهند تا عملیات تراکنش خود را معکوس انجام داده و پول خود را پس بگیرند. این باعث شده تا فروشنده از پرداخت وجه مطمئن نباشد. بیت کوین با حذف شخص ثالث از معاملات باعث انجام پرداخت های مطمئن و غیرقابل برگشت شده است.

2) آسیب پذیری اساسی بیت کوین

> سیستم تا زمانی که نودهای درست و صحیح، تحت کنترل مجتمعی از پردازنده های قوی است، نسبت به هر حمله مهاجمان، امن است.

برای ادامه کار کردن، شبکه بیت کوین باید به اندازه کافی سخت باشد تا افرادی که قصد دارند یک زنجیره جعلی از تراکنش ها را جایگزین در زنجیره اصلی بلاک چین کنند، نتوانند در شبکه نفوذ کنند. این امر نیاز به قدرت محاسباتی بالایی دارد و مشخص می کند در نهایت چه چیزی می تواند تهدیدی برای ارزهای رمزنگاری باشد: افرادی که تلاش زیادی برای از بین بردن قدرت تسلط بیت کوین دارند، می توانند خطرناک باشد.

3) اساس اعتماد به بیت کوین

> ما به راهی نیاز داریم که شخص دریافت کننده بداند که صاحب قبلی ارز، این تراکنش و انتقال این ارز را با شخص دیگری انجام نداده است. پیشنهاد ما به عنوان راه حل، ثبت لحظه ای تراکنش ها در یک سرور است.

بزرگترین تهدید جهت استفاده از بیت کوین به عنوان یک سیستم پرداخت، داشتن پتانسیل دو بار پرداخت است. در استفاده از پول های فیزیکی دو بار پرداخت غیر ممکن است، زیرا شما وجه را به فروشنده تحویل می دهید. اعتماد اساسی بیت کوین از این ایده ریشه می گیرد که همه از تراکنش قبلی مطلع هستند، و این امکان را فراهم می کند که به چیزی که قبلا انجام شده اعتماد کنند.

4) ضرورت اثبات کار

> هنگامی که توان یک پردازشگر(CPU) صرف انجام اثبات کار(POW) می شود، بدون دوباره انجام دادن کار نمی توان بلاک را تغییر داد. از آنجا که سایر بلاک ها به طور زنجیره ای پس از آن قرار دارد، تلاش برای تغییر یک بلاک شامل انجام دوباره تمام بلاک هایی است که بعد از آن قرار دارند.

یکی از دلایلی که بیت کوین تا حد زیادی انعطاف پذیر شده این است که با گذشت زمان قوی تر شده است و اثبات کار جزء ضروری این قدرت است. زنجیره بلاک چین در طول زمان گسترده تر و طولانی تر شده است که امکان موفقیت حمله به آن را کاهش داده. با افزایش سختی اثبات کار در طول زمان، بیت کوین قدرت دفاع خود را افزایش داده است.

5) بیت کوین چطور به رشد خود ادامه می دهد

> نودها همیشه طولانی ترین زنجیره را به عنوان زنجیره صحیح در نظر می گیرند و همچنان برای گسترش آن تلاش می کنند.

یکی از مسائلی که باعث رشد محبوبیت بیت کوین شده این است که تمام نودهای شبکه بیت کوین همیشه آخرین نسخه بلاک چین را ندارند. با این حال با گذشت زمان، تراکنش های بعدی روی بلاک چین طولانی تر گسترش می یابند و به این ترتیب امکان گسترش کل شبکه را فراهم می کند.

6) انگیزه استخراج بیت کوین

> طبق قرارداد، اولین تراکنش در شبکه یک تراکنش ویژه خواهد بود که یک بیت کوین جدید را که تحت مالکیت سازنده بلاک است، ایجاد می کند. این امر باعث افزایش انگیزه نودهایی می شود که شبکه را حمایت می کنند و راهی برای توزیع اولیه ارزهای در گردش است.

استخراج بیت کوین همواره بخش جذابی از حرکت ارز رمزنگاری بوده است و با افزایش قیمت بیت کوین، حجم زیادی از افرادی که دارای دستگاه هایی با قدرت محاسبات بالا هستند، تلاش می کنند تا بلاک های جدید را حل و باز کنند و در نتیجه موفقیت، مقداری بیت کوین دریافت

کنند. طبق مقاله ساتوشی، استخراج به کسانی که قدرت محاسباتی بالایی دارند نیز انگیزه می دهد تا به دنبال خرابکاری در بلاک چین نباشند، زیرا می توانند از این طریق مالک بیت کوین جدید شوند.

7) مواجهه با بلاک چین رو به رشد

> هنگامی که آخرین تراکنش بعد از تعداد کافی از بلاک ها قرار گرفت، تراکنش های انجام شده قبل از آن می توانند به منظور حفظ فضای کافی، حذف شوند.

هر چه محبوبیت بیت کوین بیشتر شده است سرعت پردازش آن نیز کند تر شده. توسعه دهندگان بیت کوین نیاز به هرس و اصلاح رشد بلاک چین را پیش بینی کرده اند. این روش شامل فشرده سازی بلاک های قدیمی با استفاده از هش های کوتاه تر است که برای متراکم کردن تراکنش های قبلی کافی است. با این حال، این تئوری اصلاح بلاک چین ثابت شده مشکلات بیشتری را نسبت به آن چه که در مقاله گفته شده است، دارد؛ با توجه به این حقیقت که هیچ کس نمی تواند ضمانت کند، هر بلاکی که اصلاح می شود حاوی اطلاعاتی که برای دیگر اعضای بلاک چین حیاتی است، نباشد.

8) رسیدگی به معاملات بزرگتر

> اگر چه این امکان وجود دارد که ارزها را به صورت واحد های جداگانه انتقال داد، اما این که بخواهیم برای هر سنت یک تراکنش جداگانه انجام دهیم باعث سنگین شدن شبکه می شود. این که بخواهیم مقادیر از هم جدا شده و ترکیب شوند، تراکنشها شامل چندین ورودی و خروجی می شود.

ارزهای فیات در واحدهای متفاوتی ارائه می شوند. به عنوان مثال سکه 50 تومانی و یا اسکناس 1000 تومانی. بیت کوین نیز به لحاظ تئوری به همین شیوه، با واحدهای مجزا، برنامه ریزی شده است. این کاربر را قادر می سازد تا بتواند 4 بیت کوین را به وسیله یک تراکنش انجام دهد، به جای این که چهار تراکنش یک بیت کوینی را ثبت کند؛ مانند این که یک تراکنش 2000 تومانی را را با 4 اسکناس 500 تومانی انجام داد.

9) حفظ حریم خصوصی بیت کوین

> همه می توانند مقدار بیت کوینی را که یک فرد به فرد دیگر انتقال داده است را مشاهده کنند، اما اطلاعاتی که با تراکنش هر فرد همراه است، قابل رویت نیست. این امر مشابه اطلاعاتی است که در بازار مبادلات سهام منتشر می شود. یعنی زمان و اندازه هر معامله به صورت عمومی منتشر می شود، اما این که طرفین چه کسانی هستند مشخص نیست.

حریم خصوصی یک مزیت ارزشمند در معاملات ارزهای رمزنگاری در مقایسه با سایر روش های پرداخت است. بیت کوین حریم خصوصی را مطابق آنچه که اغلب کاربران می خواهند فراهم نکرده است و این باعث شده تا رقبا برای ایجاد یک حریم خصوصی بیشتر تلاش کنند. با این وجود مقاله ناکاموتو اشاره می کند که کاربران بیت کوین می توانند اقدامات دیگری را انجام دهند. از جمله این که اطلاعات کلیدی متفاوتی را در هر معامله وارد نمایند.

10) مکانیسم دفاعی بیت کوین

> گره ها پرداخت تراکنش های نامعتبر را قبول نمی کند و گره های درست هرگز بلاک حاوی این نوع اطلاعات را نمی پذیرند. هکر می تواند تنها یکی از تراکنش های خود را تغییر دهد تا بتواند پولی را که صرف کرده بود، برگرداند.

در نهایت این مقاله عنوان می کند که هکر این شانس را دارد تا بلاک چین متناوبی را ایجاد کند. برای انجام این کار، هکر باید به قدر کافی سریع باشد تا نسخه اشتباهش پذیرفته شود. در غیر این صورت اگر نسخه اشتباه هکر پشت دیگر گره ها بیفتد، احتمال تراکنش معکوس قبلی نزدیک به صفر می رسد.

آیا بیت کوین زنده خواهد ماند؟

کاهش شدید قیمت بیت کوین سبب شد که اغلب سرمایه گذاران باور کنند که بیت کوین می تواند مدت های زیادی زنده بماند. در حال حاضر با توجه به کارا بودن اصول اساسی مقاله ساتوشی، بیت کوین خود را به عنوان یک فناوری کلیدی معرفی کرده است و جدا از آنچه برای قیمت بیت کوین رخ می دهد، با توجه به اصول آن می تواند در دراز مدت زنده بماند.

منبع fool.com

ارز دیجیتال | ارز رمزنگار | ارز رمزنگاری شده | استخراج بیت کوین | بلاک چین | بیت کوین | ساتوشی ناکاموتو | فناوری بلاک چین

ایمان کیمیایی