ارزهای دیجیتال از کجا آمده اند، و در مورد این نوع پول های الکترونیکی و نوین چه چیزهایی باید بدانیم؟

همزمان با رشد ارزش بیت کوین در سال ۲۰۱۷، ارزهای دیجیتال به یک جریان اصلی در دنیا تبدیل شدند. معمولا به ارزهای دیجیتال نام «طلای دیجیتال» نسبت داده می شود. زیرا، برخی از ویژگی های بیت کوین و سایر ارزهای دیجیتال با این فلز گران بها برابری می کنند. اما این مقایسه درستی نیست.

کریپتوکارنسی یا ارز دیجیتال به یک سیستم انتقال وجه الکترونیک گفته می شود که برای تایید تراکنش ها و تشکیل واحدهای جدید، متکی به بانک های مرکزی نبوده و نیازی به شخص ثالث ندارند. در عوض در سیستم ارزهای دیجیتال تراکنش ها در یک دفتر کل توزیع شده به نام بلاک چین ثبت و رمزنگاری می شوند، و این موضوع امکان پرداخت های مستقیم و همتا به همتا را فراهم می کند.

در این مطلب به موضوعات زیر پرداخته شده:
۱- خلق بیت کوین و بلاک چین (فناوری که بستر فعالیت تمام ارزهای دیجیتال غیر متمرکز را تشکیل داده است)

۲- بلاک چین چطور مشکلات مرتبط با ارزهای دیجیتال پیشگام را حل می کند؟

۳- تراکنش ارزهای دیجیتال چطور بدون دخالت بانک مرکزی تکمیل می شود؟

۴- نقش ماینرها در بازار ارز دیجیتال چیست؟

۵- چگونه ارز دیجیتال بخریم

تاریخچه ارزهای دیجیتال

در سال ۲۰۰۹، یک برنامه نویس کامپیوتر با نام مستعار ساتوشی ناکاموتو، اولین ارز دیجیتال دنیا یعنی بیت کوین را اختراع کرد. ساتوشی مخترع فناوری بلاک چین نیز هست! فناوری که بستر فعالیت ارزهای دیجیتال غیرمتمرکز را به وجود آورده است. در واقع ساتوشی

مجموعه ای از ایده‌هایی مانند هش، ثبت جمعی و ... را در کنار یکدیگر استفاده کرد و ایده ی بلاک چین را خلق نمود.

هدف از اختراع بلاک چین، ارائه یک راه حل برای «مشکل دوبار خرج کردن» در ارزهای دیجیتال بود، زیرا کپی کردن اطلاعات دیجیتال کار آسانی است. در جریان این نقص، دارنده یک سکه نقدی جایگزین آن را در یک جا صرف و از کد منحصر به فرد خود برای یک تراکنش در جای دیگر استفاده می کند. مانند این که کسی یک زمین را همزمان به دو نفر بفروشد.

اما ساتوشی ناکاموتو تصمیم گرفت یک پول غیر متمرکز را توسعه بدهد، یعنی برای تایید تراکنش ها در شبکه کاربران بیت کوین یک راه جدید پیدا کند. در چکیده گزارش اولیه (WhitePapet) بیت کوین نوشته شده است:

> تراکنش ها با ذکر دقیق اطلاعات زمانی در یک زنجیره ادامه دار از اثبات انجام کار مبتنی بر هش، درج خواهند شد. سوابق این تراکنش ها غیر قابل تغییر خواهد بود، مگر آنکه فرایند اثبات انجام کار مجددا انجام شود.

این در واقع اولین تعریفی است که برای فناوری بلاک چین ارائه شده...

چرا این نام برای بلاک چین انتخاب شده است؟

بیت کوین هر بلاک مجموعه ای از اطلاعات تراکنش های انجام شده در شبکه است. به عبارت ساده تر، هر بلاک می گوید که شخص A، چقدر پول برای شخص B، و شخص X چقدر پول برای شخص Y ارسال کرده است.

همچنین در هر بلاک اطلاعات مهمی قرار دارد که به بقیه شبکه در تایید اعتبار بلاک کمک می کند، مثل اثبات انجام کار.

علاوه بر این، در هر بلاک اطلاعاتی قرار دارد که به بلاک قبل از آن بر می گردد. در نتیجه، هر بلاک با بلاک قبل از خود یک نوع ارتباط ارجاعی داشته و یک زنجیره را در شبکه به وجود می آورد. به این اطلاعات هش گفته می شود. توابع هش در بلاک یک مجموعه خاص از اطلاعات را به صورت زنجیره ای از حروف و اعداد به نام digest در می آورند. اگر داده های موجود تغییر پیدا کنند، هش نیز تغییر می کند. وجود هش در بلاک، امنیت شبکه را تضمین می کند.

اگر یک هکر بخواهد بلاک خاصی را در شبکه دستکاری کند، باید کل بلاک های بعد از آن را نیز عوض کند. زیرا اگر یک بلاک در شبکه تغییر کند، هش بلاک های بعد از آن معتبر نخواهند بود. طول این زنجیره، متناسب با افزایش قدرت پردازش در شبکه، افزایش پیدا می کند. با افزایش سطح پردازش لازم برای حل معادلات و افزودن بلاک جدید به زنجیره، دستکاری بلاک چین سخت تر می شود. در این صورت هکرها تنها در ص ست بگیرند.

تراکنش‌های ارز دیجیتالی چطور انجام می‌شوند؟

ارزهای دیجیتال در پرداخت های مستقیم و همتا به همتا در سراسر دنیا کاربرد دارند. سرعت انجام این تراکنش ها وابسته به نوع ارز دیجیتال، و الزامات فرایند تایید، متغیر است. اما اصولا تراکنش ها در سیستم الکترونیک ارزهای دیجیتال در مقایسه با سیستم بانکداری سنتی با سرعت بیشتری انجام می شوند. انتقال وجه در بانک ها چند روز طول می کشد، این در حالی است که ارزهای دیجیتال تنها ظرف چند دقیقه به مقصد مورد نظر می رسند.

به طور کلی پیش از آنکه سابقه یک تراکنش در بلاک چین ثبت شود، مراحل زیر طی می شود:

۱- یک نفر تراکنش خاصی را درخواست می کند، و درخواست او به کل شبکه ارسال می شود.

۲- هر کامپیوتر حاضر در شبکه تراکنش های همزمان را در یک بلاک جمع می کند، و به هر یک برچسب زمانی می زند.

۳- هر کامپیوتر روی حل معادلات پیچیده کار می کند، تا با حل آن موفق به افزودن یک بلاک جدید به شبکه بلاک چین بشود. به این فرایند «استخراج یا ماینینگ» گفته می شود.

۴- زمانی که یک کامپیوتر به جواب درست برسد، خبر استخراج بلاک جدید را به بقیه شبکه اطلاع می دهد.

۵- شبکه نیز جواب را چک می کند و تراکنش های ثبت شده در آن را با بلاک چین مقایسه کرده و تطبیق می دهد تا از نقص دو بار خرج کردن در شبکه جلوگیری شود.

۶- بلاک جدید به زنجیره موجود اضافه می شود، و این به منزله تکمیل عملیات تراکنش است.

وقتی یک بلاک جدید به زنجیره بلاک چین اضافه شد، آن بلاک یک هش دریافت می کند که در تولید بلاک بعد استفاده خواهد شد. این فرایند به طور دنباله دار تکرار می شود.

به همین ترتیب، معاملات عملا غیرقابل برگشت خواهند بود، انگار که به یک نفر پول نقد داده باشید. (از این جهت مشکلی ندارد از این فناوری به یک سیستم پولی الکترونیک یاد کنیم)

همانگونه که گفته شد، هر بلاک با بلاک قبل از خود در ارتباط است. این یعنی اگر کسی بخواهد تراکنش ها را دستکاری کند، مجبور است کل زنجیره را تغییر بدهد. زیرا امکان تغییر یک تراکنش به خودی خود وجود ندارد!

فرض بر اینکه یک نفر موفق به تغییر کل زنجیره شود، از آنجایی که مدام بلاک های جدیدی به زنجیره افزوده می شوند، به شدت احتمال آن ضعیف است که او بتواند پیش از ورود یک بلاک جدید به شبکه، آن را وارد بلاک چین کند.

هر تراکنش به یک امضا نیاز دارد

ارزهای دیجیتال از یک امضا دیجیتال استفاده می کنند، درست مثل کارت های اعتباری که برای تایید خرید توسط دارنده کارت، از امضای شخص استفاده می کنند.

تراکنش ها از طریق یک سیستم رمزنگاری امن تحت عنوان «رمزنگاری کلید عمومی»، ایمن می شوند. هر یک از کاربران شبکه یک کلید عمومی و یک کلید خصوصی دارد، که به حساب کاربری اش مربوط است.

در تایید اعتبار یک تراکنش، لازم است که کاربران ثابت کنند کلید خصوصی را می دانند و آن را در یک تابع هش، مشابه هشی که بلاک ها را به هم مرتبط ساخته، وارد کنند. به این فرایند «امضاء digest» گفته می شود. پس کلید خصوصی در نگارش یک امضا دیجیتال نقش اساسی دارد. از ا

و اما کلید عمومی، در اختیار کل کامپیوترهای حاضر در شبکه قرار می گیرد. کلید عمومی برای رمزگشایی اطلاعات استفاده شده و این موضوع را تایید می کند که آیا اطلاعات توسط کلید خصوصی حساب درخواست کننده رمزنگاری شده اند یا خیر.

البته، کلید عمومی نمی تواند برای تعیین کلید خصوصی که امنیت دارایی دیجیتال افراد را تضمین می کند، استفاده شود.

نقش ماینرها در شبکه چیست؟

در مورد چاپ و صدور پول های کاغذی، بانک مرکزی تصمیم گیرنده است، اما در مورد ارزهای دیجیتال چطور؟

وقتی این بانک مرکزی نیست که تصمیم می گیرد ارزهای دیجیتال چه زمان تولید شوند، پس این نوع از ارزها چطور تکثیر می شوند؟

به همین دلیل لازم است ارزهای دیجیتال تولید واحد جدید را در شبکه تعریف کنند. بسیاری از ارزهای دیجیتال مثل بیت کوین واحدهای جدید را به عنوان پاداش بین ماینرها توزیع می کنند تا تراکنش ها را در بلاک چین تایید کنند.

ماینرها تلاش می کنند تا مشکلات پیچیده ریاضی یا سایر سیستم های اثبات انجام کار در هر یک از بلاک های موجود در بلاک چین را حل کنند، و سپس هر یک از راه حل ها را تایید کنند.

اما انجام تمام این محاسبات، هزینه دارد. و این هزینه به هیچ عنوان مجازی نیست، مثل هزینه ای که صرف خرید تجهیزات سخت افزاری یا مصرف برق می شود.

سختی این معادلات به صورت خودکار وابسته به قدرت پردازش در شبکه تنظیم می شود. به گونه ای که حل هر مساله میانگین ۱۰ دقیقه طول بکشد.

زمانی که یک ماینر با موفقیت بلاک جدیدی را به بلاک چین اضافه می کند، حق دریافت پاداش به او اعطا می شود. آدرس بیت کوین ماینر برنده نیز به همراه سایر اطلاعات، در بلاک جدید ثبت می شود.

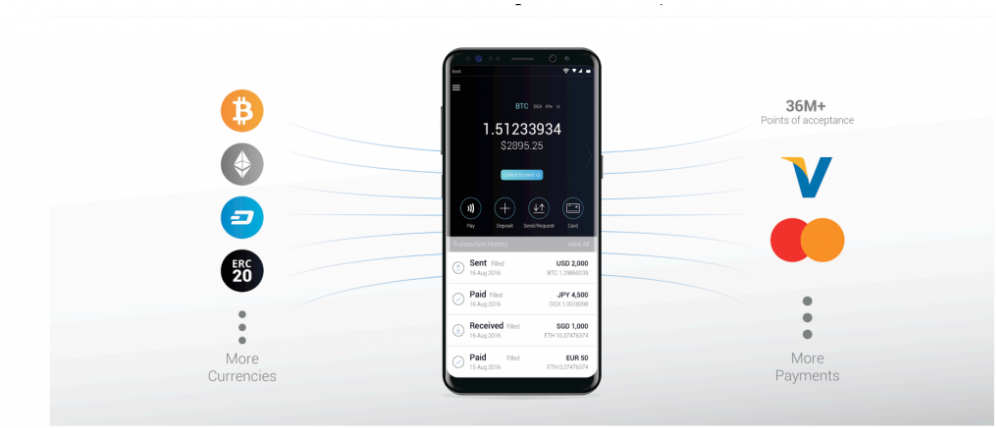
میزان پاداش از ۵۰ بیت کوین در ازای هر بلاک شروع شد. این تعداد هر ۲۱۰۰۰۰ بلاک یکبار (یا تقریبا هر ۴ سال یکبار) نصف می شود. در حال حاضر جایزه هر بلاک ۱۲/۵ بیت کوین است، این عدد نزدیک سال ۲۰۲۰ به ۶/۲۵ کاهش پیدا خواهد کرد.

در یک زمان نامشخص پاداش حل هر بلاک در بلاک چین بیت کوین بی نهایت کم می شود. تا پیش از سال ۲۱۴۰ ماینرها موفق به استخراج تمام ۲۱ میلیون بیت کوین در شبکه خواهند شد.

بدین ترتیب پاداش ماینرها برای بروزرسانی و تایید بلاک چین روی هزینه کارمزد تراکنش ها حساب می شود. از این رو کارمزد تراکنش های برخی از ارزهای دیجیتال نسبتا بالا است.

هزینه کارمزد های بیت کوین در حال حاضر نسبتا پایین است، ولی اگر حجم تراکنش ها برای جبران کاهش پاداش بلاک ها بالا نرود، به ناچار هزینه کارمزد ها افزایش پیدا می کند تا پاداش ماینرها جبران شود.

چگونه ارز دیجیتال بخریم؟



دیگر استفاده از کامپیوتر شخصی و یا حتی کامپیوترهای مخصوص ماینینگ در استخراج بیت کوین یا سایر ارزهای دیجیتال کارآمد نیست. بسیاری از افراد از صرافی ها ارز دیجیتال تهیه می کنند و از این راه سود بیشتری عایدشان می شود.

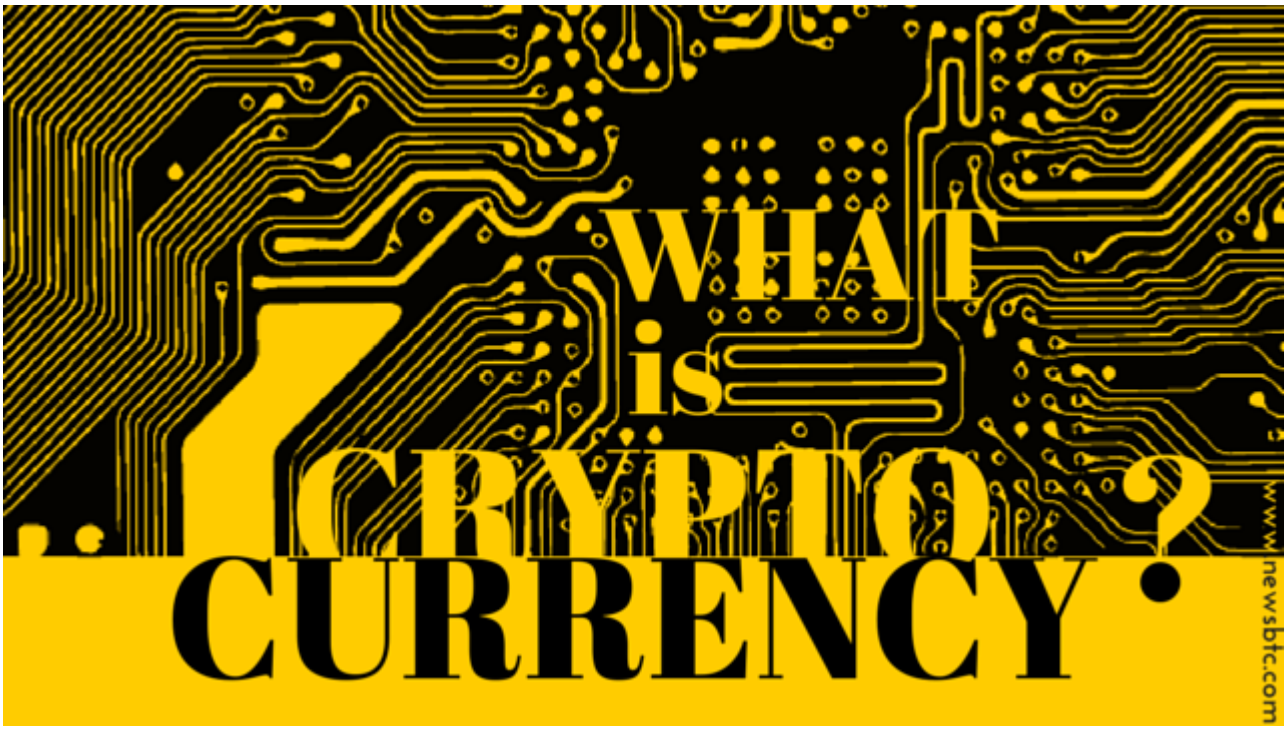
از طریق صرافی ها می توان پول فیات (مثل دلار) را به ارزهای دیجیتال (مثل بیت کوین) تبدیل کرد.

صرافی های ارز دیجیتال با بقیه صرافی ها تفاوتی ندارند، و درست مثل بورس اوراق بهادار عمل می کنند. سفارش خریداران و فروشندگان از میان یک لیست با یکدیگر تطبیق داده می شوند. زمانی که سفارشات در یک لیست درج می شوند، صرافی درخواست خریدارانی که مایلند مبلغ مورد نظر فروشنده (یا بیشتر) را بپردازند، را با درخواست فروشندگان تطبیق می دهد.

قیمت ارزهای دیجیتال صرفا از روی دلیل خرید افراد تعیین می شود. همینطور، هر صرافی لیست سفارش خرید منحصر به فرد خودش را دارد و بدین ترتیب قیمت های آن می تواند با صرافی های دیگر کاملا متفاوت باشد.

اصولا، صرافی هایی که بالاترین حجم خریدار و فروشنده را دارند، قیمت هایشان بهتر است.

ارز دیجیتال به چه معناست؟



خلاصه اینکه، در ابتدای مقاله گفته شد ارز دیجیتال نوعی سیستم پولی الکترونیک است، که برای تایید تراکنش ها و تولید پول احتیاجی به بانک های مرکزی یا اشخاص ثالث مورد اطمینان ندارد. در عوض، این سیستم برای تایید تراکنش ها، از سیستم رمزنگاری استفاده می کند، و تراکنش های آن در یک دفتر کل توزیع شده تحت عنوان بلاک چین ثبت می شود. بدین ترتیب امکان پرداخت همتا به همتای مستقیم در آن وجود دارد.

اکنون کمی بیشتر این سیستم را توضیح می دهیم:

۱- ارزهای دیجیتال یک سیستم پولی الکترونیک هستند: این بدین معنا است که ارز دیجیتال صورت فیزیکی ندارند و تنها به صورت الکترونیک قابل استفاده است. حق مالکیت این نوع پول ها در قالب سوابق دیجیتال روی بلاک چین ذخیره می شود.

۲- ارز دیجیتال از رمزنگاری استفاده می کند: درخواست تراکنش ها از طریق رمزنگاری کلید خصوصی تایید می شود. بلاک چین هم برای پیوند بلاک ها به یکدیگر از فرایند رمزنگاری استفاده می کند.

۳- تایید تراکنش ها: زنجیره اطلاعات تراکنش ها در هر بلاک به شبکه در جلوگیری از نقص دو بار خرج کردن، تایید تراکنش های جدید، و در نهایت درج سابقه هر یک در دفتر کل کمک می کند.

۴- بلاک چین یک دفتر کل توزیع شده و عمومی است: دفتر کل بلاک چین برای تمام کامپیوترهای حاضر در شبکه قابل دسترس است. در واقع این ویژگی در عملکرد کل شبکه نقش دارد. وقتی تمام کامپیوترها به نسخه بروزرسانی شده این دفتر کل دسترسی داشته باشند، از اطلاعات شبکه و سابقه تراکنش ها در برابر تغییر محافظت می شود.

۵- پرداخت های همتا به همتای مستقیم: این عبارت به این معنی است که فرایند پرداخت های ارز دیجیتالی هرگز زیر نظر سیستم بانک مرکزی یا شخص ثالث انجام نشده و مبلغ مورد نظر مستقیم از شخص پرداخت کننده به دریافت کننده ارسال می شود.

۶- ارز دیجیتال یک صورت پیچیده از پول الکترونیک است. با توجه به اینکه فرایند انتقال وجه از طریق این سیستم کاملا مستقیم است، هزینه و زمان لازم برای انجام تراکنش ها و انتقال پول به نقاط مختلف در دنیا کمتر از روش سنتی است.

۷- هر روز کاربرد جدیدی به کاربردهای بلاک چین و ارزهای دیجیتال افزوده می شود. امیدوارم اکنون با مطالعه این توضیحات ساده، مفهوم ارز دیجیتال برایتان ملموس تر شده باشد.

منبع: fool.com

تهیه شده توسط وبسایت آتادکس

دیدگاهتان را بنویسید

نشانی ایمیل شما منتشر نخواهد شد. بخش‌های موردنیاز علامت‌گذاری شده‌اند *

دیدگاه *

Fill out this field

نام *

Fill out this field

ایمیل *

لطفاً یک نشانی ایمیل معتبر بنویسید.

ارسال دیدگاه