بیت کوین. انقلابی در سیستم پولی

پادکست دایجست (دی ۱۳۹۶)

مقدمه:

خب ما امروز می خواهیم در مورد یکی از داغ ترین خبر هایی که این روزها درباره اش تقریباً در همه جا چیزی می شنویم، صحبت کنیم، و آن هم چیزی نیست جز بیت کوین. تقریباً می توان گفت بیت کوین تبدیل شده به داغ ترین خبر و کلمه این روز ها در تلویزیون، رادیو و مخصوصاً اینترنت. هرروز یک خبر می آید که بیت کوین قیمتش از فلان هزار دلار هم گذشت، دوباره فرداش تیتر روزنامه ها می شود که بیت کوین رکورد قبلی خودش را هم زده است و از این دست صحبت ها. اما با هم بررسی کنیم که این بیت کوین که مدام ازش صحبت هست چی هست، از کجا آمده و چگونه کار می کند.در این قسمت از پادکست دایجست یکم باید سعه صدر داشته باشید چرا که مفاهیم و کلمات همه جدید هستند و موضوع از لحاظ توضیح دادن کمی سخت.

بیت کوین چیست؟

بیت کوین در اصل یک رمز ارز یا به قول خودمان پول دیجیتاله. انگار یک پولی که فقط در فضای اینترنتی و دیجیتالی وجود دارد و مثل اسکناس های ما یک برگه ی چاپی نیست. در نتیجه کمی برای انسان لمسش سخته زیرا بعد فیزیکی ندارد. حالا چه مدل پول اینترنتی ای هست؟

بیت کوین پولی است که هیچ دولت و بانک مرکزی یا هیچ شخص خاصی کنترلش نمی کند . در حقیقت، این پولی که دست من و شماست یعنی ریال، دلار، پوند فرقی نمی کند، تمام این پول ها پشتشان دولت یک کشور است به همراه یک بانک مرکزی ای که تصمیم می گیرند چه میزان از آن چاپ کنند و وارد بازار کنند تا به دست من و شما برسد و اساساً وابستگی زیادی دارد به تصمیماتی که آن دسته از آدم ها آن بالا در دولت و بانک می گیرند. ولی در بیت کوین این داستان فرق می کند. در اصل هیچ کسی نیست که بگوید الان این میزان از پول باید زیاد بشود یا نشود و هیچ شخص خاصی کنترلش نمی کند. میدونم کلی سوال الان در ذهنتان هست ولی نگران نباشید بیشترش را جواب خواهیم داد . پس تا اینجا بیت کوین شد یک رمز ارز دیجیتالی که هیچ شخص و دولت خاصی کنترلش نمی کند. ولی قبل از اینکه بیشتر توضیح بدهیم که این پول چی هست، اصلاً ببینیم از کجا پیداش شد.

تاریخچه ی اجمالی پیدایش پول، بانکداری و انگیزه ی خلق بیت کوین:

در حقیقت بیت کوین اولین اجرا از یک تفکری به اسم رمز ارز بود که خود تفکر رمز ارز توسط یک شخصی به اسم وای دای در سال ۱۹۹۸ مطرح شد که حرفش این بود که رمز ارز یک پول جدید است که با استفاده از علم رمزنگاری می تواند مبادلات خودش را کنترل کند و نیازی به یک قدرت و محوریت مرکزی مثل یک صاحب یا دولت نیست. بعد بر اساس این مفهوم یک شخصی که هنوز هم که هنوزه هیچ کسی به هویتش پی نبرده سال ۲۰۰۸ در بحبوحه ی رکود مالی بانکها یک مقاله ای می نویسد که در آن بیت کوین و سیستم آن را معرفی می کند. به چه کسانی؟ به یک لیست ایمیلی از این آدمهای خوره ی رمزنگاری. اسم مستعاره این شخص که تا به الان دنیا نمیدونه کی

هست یا کی هستند ساتوشی ناکاماتو (Satoshi Nakamoto) است و بعد اولین بیت کوین در سال ۲۰۰۹ توسط ایشان خلق شد. حالا بریم سراغ اون قسمتی که اصلا چه شد چنین پولی خلق شد؟ انگیزه ساتوشی ناکاموتو از خلقت بیت کوین چه بود؟

هزاران سال قبل مردم وقتی می خواستند تجارت کنند چه کار می کردند؟ یکی مثلاً سیب زمینی داشت یکی هم گوشت . ۱۰ کیلو سیب زمینی می داد یک کیلو گوشت می گرفت . هم این یک گوشت سیب زمینی می خورد هم اون یک استیکی با سیب زمینی سرخ کرده ای. بعد گفتند آقا این سخته بیایم به جای اینکه هی این سیب زمینی و خیارو هویج را ببریم این ور اون ور به جاش پول درست کنیم.

یک سری سکه مثلا از جنس طلا و نقره که به صورت قراردادی برای هرکدامش ارزش تعیین کنیم و به جاش این ها را به هم دیگه برای تجارت بدهیم. باز کمی گذشت و بعد دیدند خب خود این سکه ها هم بعد از یک مدت دیگه سنگین هستند و حمل و نقلشان سخت و به این راحتی ها هم گویا نمی شود رقم های کوچکتر را به وسیله آن پرداخت کرد. گفتند خب بیاییم طلا و نقره هایمان را بگذاریم درگاو صندوق های یک جایی به اسم بانک و بعد یک سری برگه چاپ کنیم که به جاش آن ها را حمل و نقل کنیم اینطورکه مثلاً روی برگه نوشته شده صد عدد سکه طلا و این یعنی اینکه شما در بانک به اندازه آن کاغذ صد سکه طلا دارید و فقط این برگه را داد و ستد می کنید چون که حملش راحت تر است در نتیجه این طور بود که پول کاغذی ما به وجود آمد. حالا از این جا به بعدش جالبه.

بانک ها یواش یواش شروع کردن به پول چاپ کردن بیشتر از طلا و نقره ای که در گاو صندوق هایشان داشتند. مثلا اگه شما به میزان ۱۰۰ عدد سکه پول داشتید در بانک، این ها به میزان ۱۰۰۰ عدد سکه پول چاپ می کردند و وام می دادند. اینطوری می شد که هرچند وقت یک بار یکی از این بانک ها گند کارش در می آمد و ورشکست می شد و پول آدم هایی که بهش اعتماد کرده بودند را نمی توانست بازپرداخت کند.

از سر همین قضیه گفتند که اینطور نمی شود ، آمدن و یک چیزی درست کردن به اسم بانک مرکزی که هر بانکی برای خودش نره هرکار دلش خواست بکند ومثلاً جلوی این قضیه را به نحوی بگیرند و اینکه آن بانک مرکزی بیاید ضمانت بکند که اگر یک بانکی هم در این میان خراب کرد مردم متضرر نشوند. ولی چون هنوز هم در این سیستم بیشتر از اندازه ذخایر بانکی، پول چاپ می شد ریسک ورشکسته شدن کامل بانک از بین نرفت. در حقیقت تعداد دفعات این ورشکستگی ها کمتر شد ولی شدت و تاثییرشون بیشتر. هنوز هم بانک ها هرچند وقت یک بار ور شکسته می شدند. اما این بار دیگه اگر یک بانکی بدجور در مخمصه گیر می کرد باقی بانک ها را هم باخودش درگیرمی کرد و آن زمان دولت باید می آمد وسط که نجاتشان بدهد.

سر همین موضوع، در سال ۱۹۷۱ رییس جمهور آمریکا نیکسون رابطه پولی که چاپ می شد با طلا ودارایی که پشتوانش بود را قطع کرد. این باعث شد که دیگر هیچ محدودیتی برای تولید پول کاغذی وجود نداشته باشد.

از اینجا به بعد تمام پولی که خلق می شد به عنوان اعتبار و بدهی به وجود می آمد و دیگه پشتوانش دارایی ای مثل طلا نبود. یعنی وقتی وام می گرفتید، پول برای شما خلق می شد و به شما غرض داده می شد و شما هم این پول را با بهره ی مشخصی باز میگرداندی به بانک. بله درسته بانک ها هم باید یک مقدار به عنوان ذخیره نگه می داشتند اما خود این ذخیره هم از همان پول اعتباری بود دیگه و اینکه میزانش از مقدار وامی که داده می شد بسیار کمتر بود.

اینجا بود که دیگه تولید و عرضه پول ترکید و این یکی از دلایلی بود که ۲۰۰۶ سیستم های مالی دنیا سقوط کردند (به صورت خیلی کلی البته) .

و اینطوره که هرسال یک درصدی قیمت ها افزایش پیدا می کنند. چون پول در گردش زیاد در حال افزایش است . البته افزایش قیمت یک حدی کمتر از تولید و عرضه پول است و آن هم به خاطر اینه که بهره وری تولید و صنعت هی هر سال افزایش پیدا می کند. یعنی چی؟ یعنی شما کاری را که هی بیشتر و بیشتر انجام میدهید در آن باتجربه تر می شوید، علمتان بیشتر می شود، تکنولوژی های جدید می آید

و هر سال برای شما ارزان تر تمام می شود. پس احتمالاً می پرسید که چرا قیمت ها هرسال کمتر از سال قبل نمی شود؟ نمی شود چون تولید پول کماکان در جریان است و این باعث همین تورمی می شود که هرساله از آن صحبت می کنند.

بانک ها هم بعد از مدتها این کار را انجام دادن دیگه دستشان آمده که این میزان تولید و رشد پول را باید چند درصد محاسبه کنند که هم سیستم هایشان رشد کند و هم صدای مردم آنقدر در نیاید. جدا از این به اصطلاح مالیات هنگفتی که بر مردم اعمال می شود، هر چند سال یکبار هم این بانک ها مردم را با این روش ها به اسارت می برند. هر وقت یک بحران اقتصادی به وجود میاد باید دولت ها کمکشان کنند وگرنه نه سیستم از هم می پاشد.

جدا از همه این ها بانک ها کاری کردند که تقریباً هیچ کسی هیچ مبادله ی تجاری و مالی را بدون حضور واسطه ای آن ها نمی تواند انجام بدهد و اگر شما هم جز آن دسته از آدم هایی هستید که فکر می کنید تجارت کردن حق لاینفک شماست پس ممکنه این فکر یکم ترسناک هم حتی باشد. در حقیقت نبود یک پول درست ریشه ی همین مشکل ها بوده است. پول کاغذی به وجود آمده چون جایگزین بهتری نداشته . طلا و نقره هم که داستان خاص خودشان را دارند.

اینجا بود که ساتوشی ناکاماتو در پاسخ به تمام مشکلات سیستم های بانکی یک سیستم پولی الکترونیک فرد به فرد به اسم بیت کوین را خلق کرد و اولین جمله ای که در اولین بلاکش نوشت، تیتری از روزنامه تایمز لندن بود که نوشته بود صدر اعظم درشرف دومین کمک به بانک ها است و بعد هم تاریخ ۳ ژانویه ۲۰۰۹. این خبر حاکی از این بود که دولت میلیارد ها پول را میخواست به سیستم دوباره تزریق کند.

این بود هدف ساتوشی از خلق بیت کوین. انقلابی در سیستم پولی که دیگر بانک درآن کنترلی نخواهد داشت. ولی بریم سراغ خود بیت کوین دیگه الان.

ساختار و ویژگی های بیت کوین:

خب یادتونه گفتیم مشکلات سیستم بانکی و پولی چه بود. اینکه مثلا بانک ها همینطور پول چاپ می کنند. خب بیت کوین اینطوری نیست. اول از همه اینکه هیچ بانکی پشت آن نیست و دوم اینکه بی نهایت بیت کوین وجود ندارد. بیت کوین انتها دارد و یک روزی بیت کوین های روی کره زمین دیگه تولید نمی شوند. در حقیقت کل بیت کوینی که وجود خواهد داشت ۲۱ میلیون عدد است که با آمار ریاضی که تخمین زده شده سال ۲۱۴۰ آخرین بیت کوین تولید یا استخراج می شود. حالا راجع به نحوه تولید یا استخراج بیت کوین جلوتر توضیح میدهم. تا همین الان یک چیزی حدود ۱۶ میلیون و ۷۵۰ هزار بیت کوین استخراج شدند.

دلیلی هم که میگم استخراج این است که مدل بیت کوین بیشتر شبیه یک معدن طلاست. اولاً مثل طلا یک روزی تمام می شود و دیگر پیدا نخواهد شد و دوم اینکه شما برای تولید بیت کوین جدید باید از معادن رمزنگاری شده ، بیت کوین را استخراج کنید . به این آدم هایی هم که اینکارو میکنن میگن معدن چی یا همانMiner . نگران نباشید توضیح میدهم.

ولی قبلش به این سوال بپردازیم که خب حالا این پول به وجود آمد ولی چگونه ارزش پیدا کرد؟ چگونه گسترش پیدا کرد؟ الان اگه من و شما هم تازه مثلاً نابغه ریاضی و کامپیوتر و اقتصاد باشیم بعد یک پولی برای خودمان اختراع کنیم مگر ارزش پیدا می کند؟ مگر اصلاً کسی از آن استفاده می کند؟

چیزی که باید بدونیم راجع به ارزش یه ارز این است که هرپولی که به وجود می آید باید یک سری از آدم ها توافق کنند که بین هم رد و بدلش کنند و برای آن ارزش تعیین کنند. مثلاً اولین معامله ای که با بیت کوین با دنیای حقیقی شکل گرفت این بود که ۱۰،۰۰۰ بیت کوین دادند تا دوتا پیتزا باهاش بخرند. فکر کن اونی که الان اون ۱۰،۰۰۰ بیت کوین را در اختیار دارد اگر نگه اش داشته باشد الان ۷۲۰

میلیارد تومن پول دارد. آن هم با دو تا پیتزا فقط. ولی به صورت کلی دو، سه دسته آدم جز اولین کسانی بودند که این پول را تبدیل کردند به این پولی که الان هست. این آدم ها جذب ۳ تا چیز در بیت کوین شدند.

اول اینکه کاملا غیرمتمرکز است و دست شخص خاصی یا بانکی یا دولتی این وسط نیست. دوم اینکه هویت شما وقتی از بیت کوین استفاده می کنید محرمانه باقی می ماند، یعنی کسی نمی تواند رد شما را بگیرد و سوم اینکه شما برای نقل و انتقالات پول بیت کوینی کمیسیونی در حد صفر پرداخت میکنید انگار اصلاً چیزی نمی دهید.

حالا بسیاری از آدمهایی که اولین بودند کسایی بودند که مثلاً گرایشات سیاسی داشتند، نمی خواستند که دولت ها بدانند چه کار می کنند یا کسانی بودند که کلاً با این ایده که دولت هر موقع صلاح دانست پول چاپ کند مشکل داشتند. در حقیقت این تفکر ایدئولوژیک اولیه اون چیزی بود که باعث شد که اینها به سمت بیت کوین بیایند و از آن استفاده کنند.

بعد از اینها، یک دسته دیگه ای از آدم ها بودند که علاقه مند به استفاده از بیت کوین شدند. آنها کسانی بودند که دوست نداشتند ردشان گرفته شود. حالا میان این آدم ها خلافکار ها هم بودند که مثلاً مواد مخدر، اسلحه یا خیلی چیز های دیگر مثل بازی های شرط بندی آنلاین معامله می کردند. مثلاً از بیت کوین خیلی در سایت سیلک رود (Silk Road) ازش استفاده می شد.

سیلک رود تقریباً می شود گفت که اولین سایت خرید آنلاین مواد مخدر در دنیا بود که پول رایجی که در آن استفاده می شد همین بیت کوین بود که خب با سیستم بانکداری و پولی معمولی و سنتی نمی شد خرید بکنند، زیرا آن وقت صاحب سیلک رود باید می رفت به یک بانکی و حساب باز می کرد که وقتی مردم پول می ریزند انتقال پیدا کند به آنجا . به این شکل هم پلیس یک دقیقه ای هم صاحب سایت را دستگیر می کرد هم آن شخصی که پول واریز کرده بود. در نتیجه فقط بیت کوین چاره ی راه بود. داستان جالبیه. اگر علاقه مند به ماجرای سیلک رود هستید یک پادکست خوبی به اسم کانال بی (Channelb) هست که چند تا از اپیزود هاش فقط در رابطه با همین ماجراست. پیشنهاد میکنم گوشش کنید.

ولی فقط این سایت های خلافکاری نبودند که نمی توانستند با سیستم پولی و بانکی کار کنند بلکه مثلاً سایتی به اسم ویکی لیکس (wikileaks) هم که اسناد سیاسی لو رفته را انتشار می داد از بیت کوین استفاده می کرد چون که توسط دولت ها تحریم شده بود. ولی مسئله اینه که این دوگروه از افراد آنقدر زیاد نبودند که بتوانند بیت کوین را در این حد رایج کنند.

در حقیقت ویژگی سوم بیت کوین یعنی حق کمیسیون بسیار ناچیز و سرعت بالای انتقالاتش بود که باعث می شد قشر عامی از جامعه را مخاطب خودش کند. شما الان بخواهید مثلاً ده هزار دلار واریز کنید به حساب یک نفر در یک جای دیگر دنیا اولاً کلی زمان می برد و دوماً مثلاً باید ۱۰۰ دلار هم پول کمیسیون بانک را بدهید . این دلیل در حقیقت همان چیزی است که لازم بود تا افراد بیشتری عضو بیت کوین شوند. یا مثلاً شما اگر پرداختی ای با کارت های اعتباری داشته باشید مثل ویزا یا مستر یا حساب پی پال دارن تقریباً به طور میانگین یک چیزی حدود ۲,۵ درصد دارند هزینه مبادله می دهند و خب بیت کوین هزینه مبادله اش نزدیک به صفراست.

مسئله دیگر مایکروترانزکشن ها یا همان مبادلات خرد هستند . الان اگر شما بخواهید با کارت اعتباری مثلا ۱۰ سنت واریز کنید به حساب یکی دیگه کارت اعتباری شما یک حداقل مثلا ۳۰ سنت را ازشما پول می گیرد به علاوه ۲,۵ درصد از هزینه مبادله. یا اگر شما بخواهید به یک خیریه ای یک دلار با کارتتان پرداخت کنید فقط حدود یک سوم آن را باید بابت هزینه مبادله پرداخت کنید. ولی با بیت کوین هزینه مبادله شما تقریباً صفراست .

خلاصه این دسته از آدم ها کسانی بودن که خواسته و ناخواسته دست به دست هم دادند و این پول را آوردند در رادار مردم و رسید به این جایی که شما از هر در و دیواری الان تبلیغ بیت کوین را میبینید و می شنوید. حالا بریم سراغ اینکه بیت کوین چه طوری کار می کند.

مکانیزم های کاری بیت کوین :

خب خیلی سادش این هست که هر کسی تو این سیستم یک کیف پول بیت کوین دیجیتالی دارد که از طریق آن می تواند پول بفرستد و دریافت کند . پس اول از همه یک کیف پول بیت کوینی لازم دارید. خب ما گفتیم که بیت کوین هیچ سیستم مرکزی پشتش نیست . پس چه طور کار می کند؟ اگر بانکی این وسط نیست پس سیستم از کجا می فهمد که من پول دادم به فلانی یا یک شخصی برای من پول واریز کرده؟ کی حسابش را نگه می دارد؟ برای فهمیدن جواب این سوال ما باید اول متوجه یکی از تکنولوژی هایی که بیت کوین از آن استفاده می کند بشویم و آن تکنولوژی اسمش بلاک چین است.

بلاک چین (Block Chain)چیست و چگونه کار می کند؟

بلاک چین تکنولوژیی است که نقش آن در حال افزایش در همه ابعاد زندگی ما از خرید کردن تا هر چیز دیگه ای است. بلاک چین در واقع یک دیتا بیس غیر متمرکزه که به جای اینکه دست یک نفر باشد، دست همه است. این همان تکنولوژی است که بیت کوین از آن استفاده می کند. برای بهتر توضیح دادن این تکنولوژی من باید از یک مثال استعاری استفاده کنم.

فرض کنید شما با همه ی دوستانتان میروید شمال و شب که شد میگویید بچه ها بشینیم بازی کنیم. کارت ها را می گذارید جلو که بازی کنید . بعد میگویید که خب پول هایتان را بگذارید وسط که آخر هر دست هر کسی پول هایش را جمع کند بعد نگاه می کنید می بینید که ای دل غافل پول نقد هیشکی نداره. بعد می گویید خب اشکال ندارد یک برگه بگذاریم جلو و در آن بنویسیم که چه کسی چه قدر برد و چه کسی چه قدر باخت.

حالا فکر کنید بازی اینطوری است که زمانی که یکی بخواد پول بده به این و اون باید در جمع اعلام کند. قبل از اینکه بازی شروع بشود میگویند خب چه کسی مسئول نوشتن شود بعد یه سری ها میگویند فرشاد حساب ها را بنویسد بعد یکهو یکی از آن طرف اتاق داد می زند که آقا من به فرشاد اعتماد ندارم، همیشه تقلب می کند و یک چیز دیگر می نویسد. بعد مطرح می شود که خب چه کسی حساب را نگه دارد پس؟ اون دوستمون دوباره میگه آقا اصلاً من به هیچ کسی اعتماد ندارم. هر کی برای خودش بنویسه . همه هم میگن باشه . هر کس یه برگه بزاره جلوش و در آن بنویسد که چه کسی چه قدر داد به چه کسی. اینطوری جلوی تقلب هم تا یک حدی گرفته می شود همه هم کنترل آن را دارند.

حالا چون من از این مثال برای توضیح این تکنولوژی استفاده می کنم بیاید با هم یک توافقی بکنیم، از اینجا به بعد من به آن برگه کاغذ بگم بلاک همینطوری چون بلاک اسم قشنگیه مثلاً. پس از اینجا به بعد من به اون برگه ها میگم بلاک.

خب بازی شروع می شود. در بازی دست هی می چرخد و آدمها مبادلاتشان را انجام می دهند. گفتیم هم که هرکسی باید این مبادلات را در جمع اعلام کند.به این شکل مثلاً من بلند می شوم و میگویم آقا من ۱۰۰ تومان دادم به علی. بعد همه در بلاک هایشان می نویسند فرشاد ۱۰۰ تومان داد به علی.

بعد مثلاً از آن طرف سالار بلند می شود می گوید من ۲۵۰ تومان دادم به مونا. دوباره همه در بلاک هایشان می نویسند سالار ۲۵۰ تومان داد به مونا. خلاصه تا صبح می شینید بازی کردن. صبح که می شود می گویید بسه دیگه بریم بخوابیم. حساب کنید ببینیم چه کسی چه قدر به چه کسی باید بدهد. هر کدام هم ده تا بلاک یا برگه پر کردین از بس که بازی کردین. همه حساب می کنند و بعد فرشاد می گوید بنا به برگه ای که من نوشتم، من الان باید ۱۰۰۰ تومان پول داشته باشم. بعد یکی دیگه اونطرف میگه ببین مطمنی ؟ چون من به حسابم تو باید الان ۵۰۰ تومن داشته باشی؟ یکی دیگه میگه نه باید ۷۰۰ تومن داشته باشه. خلاصه همه چک می کنند و هر کسی یک عددی

دارد. عدد رقم های بقیه هم نمی خواند. چه شده این وسط؟ یا یک سری تقلب کردن برای خودشون پول بیشتر نوشتن یا اشتباه شنیدن و اشتباه هم نوشتند.

خلاصه بازی حساب کتابش خراب می شود . بعد میایید یه قراری میگزارید که فردا شب سر هر بلاک عدد رقم ها رو با هم چک کنید که نگزارید تا آخر همینطوری خراب پیش برود . فردا که می شود شروع می کنید به بازی. این بار هر بلاکتون که تموم می شود و میخواهید بروید به بلاک بعدی همه بلاک ها رو میگذارند وسط که با هم چک کنند که مغایرت نداشته باشد. خب یک راه چک کردن این است که از بالا خط به خط بخوانید و بیایید پایین که خب این طول می کشد. اینجاست که یه راه حل دیگه می آید به ذهنتان.

اینجا هم دیگه حالا فرض بگیرید این جمعی که دارید با هم بازی میکنید چند نفر دیگه نیستید مثلا جمعاً یک میلیون نفر هستید. سخته تصورش همه در شمال. میدونم ولی فرض کنید حالا اینترنتی همه به شما وصل شدند. من هی یواش یواش دارم مثال را بسط میدهم. اینجاست که یک نفر میاد پیشنهاد یه راه حل ریاضی را میدهد. چه طور؟ میاد میگه آقا این راه حلش دست یه تابع ریاضیه به اسم هش (Hash).

خب حالا هش چیه؟ هش یک تابع ریاضیه که چیکار می کند ؟ در حقیقت یک داده ی ورودی با هر سایزی را تبدیل می کند به یک داده خروجی با یک سایز مشخص. مثال:

مثلاً این اعداد را به عنوان داده ورودی در نظر بگیرید. اعداد ۱ ۲ ۳ ۴ حالا مثلاً تابع هش میگه همه این ها را با هم جمع کن و جمعشان یعنی عدد ۱۰ می شود خروجی ای که یک سایز مشخص دارد به جای ۴ تا سایز متفاوت. تابع هش خیلی در رمز نگاری استفاده می شود. در حقیقت اگر شما ورودی را داشته باشید خیلی راحت می توانید خروجی را حساب کنید ولی اگر خروجی را به شما بدهند به این راحتی ها نمیتوانی بفهمی ورودی چه بوده است.

مثلاً در همین مثال خیلی ساده هزاران شکل مختلف هست که اعداد می توانند خروجی ۱۰ را درست کنند. برای نمونه دو تا ۵ تا یا ۳ تا ۳ تا ویک ۱ یا یک ۶ و یک ۴ یا ... .تنها راهی که می شود فهمید که این عدد ورودی چند بوده این است که انقدر حدس بزنی تا برسی به عدد های درست و یک نکته مهم این است که اگر کوچکترین تغییری در ورودی اتفاق بیوفته کل نتیجه خروجی عوض می شود. حالا تابع هشی هم که بیت کوین از آن استفاده می کند نامش هست SHA256 یا Secure Hash algorithm 256 bit الگوریتم امن هش ۲۵۶ بایتی که در اصل توسط سازمان امنیت ملی آمریکا درست شده است .

حالا این هش در بازی ما چه معنی دارد؟ شما فرض بگیرید که هر بلاکتون یک داده ورودی هست. در حقیقت یک بلاک پر از ثبت مبادلات مالی می باشد که چه کسی چه قدر داد به چه کسی . میایید می گویید آقا این داده ورودی که قاعدتاً باید مال همه شبیه هم باشد را بیاید به یک عدد شانسی ای مثلاً اضافه کنیم که وقتی ازش هش می گیرید خروجی برای مثال یک عددی باشد کوچکتر از ۱۰۰. پس چی شد؟ ورودی شد اطلاعات هر بلاک به علاوه یک عددی که نمی دانیم که در نهایت خروجی هش آن بشود زیر ۱۰۰ مثلاً.

حالا آن عدد چی باید باشد که اون خروجی را در بیاورد؟ یک سری ها داوطلب می شوند که آن عدد شانسی را پیدا کنند که بتوانند هر بلاک را به نحوی امضا کنند باهاش و تاییدش کنند که در نهایت بگویند آقا این بلاک درسته بریم بلاک بعدی.

این داوطلب ها کامپیوترهایشان را آماده می کنند. بعد هی شانسی عدد های مختلفی را مثلاً جمع می کنند با ورودی اون بلاک که ببینن هشش زیر ۱۰۰ میشه یا نمیشه. مثلاً یک بار عدد ۱ را میزنند و می بینند هشش شد ۱۵۴۷ میگن خب این که نمیشه. یک بار ۲ را میزنند می بینند که این هشش شد ۴۳۷ میگن خب باز این هم نمیشه. همینطور هی اعداد مختلف را حدس میزنند که وقتی هش ازش می گیرند خروجیش بشود یک عددی زیر ۱۰۰. حالا این عدد ۱۰۰ مثال هستش و برای اینکه مکانیزم را متوجه بشوید از آن استفاده می کنیم.

بعد از چند دقیقه که این داوطلب ها در حال حدس زدن هستند یکی از آن طرف داد می زند که یافتم آقا یافتم. اون عدد مثلا ۱۲۰ است. اگر این عدد را با اطلاعات بلاک جمع کنند و ازش هش بگیرند خروجیش می شود ۹۵. همه تست کنید ببینید میشه یا نه.

همه بلاک هایشان را به علاوه مثلاً ۱۲۰ می کنند و بعد از آن هش می گیرند . قاعدتاً اگر بلاک همه شبیه هم باشد همه باید به عدد ۹۵ برسند. وقتی رسیدن به این عدد می گویند اره اره درسته زیر ۱۰۰ شد. پس به توافق می رسند که اون بلاک تاییده و بعد دوباره ادامه بازی و یه بلاک دیگه.

تازه برای اینکه یکی بعداً هم نرود و بلاک های قبلی را تغییر ندهد خود داده بلاک قبلی رو هم به سر بلاک بعدی اضافه میکنند که زنجیره وار به هم وصل شود که کسی نتواند بلاک هایی که قدیمی تر هستند را هم تغییر دهد. در حقیقت دلیلی هم که نام این تکنولوژی بلاک چین است همین می باشد . یعنی chain ای یا زنجیره ای از بلاک ها. حالا اگر یکی این وسط شیطونی کرده باشد و اعداد اشتباهی در بلاکش نوشته باشد وقتی بلاکش را به علاوه ۱۲۰ کند و از آن هش بگیرد دیگر عدد ۹۵ به دست نمی آید و مثلاً می شود ۷۸۹. بعد سریع سیستم بلاکش و بر میدارد و یک کپی از بلاک درست را برای او جایگزین می کند . میگه این درسته از این استفاده کن. در نتیجه تقلب نمیشه کرد.حالا در دنیای واقعی اون داوطلب ها باید کلی زحمت بکشند که اون عدد شانسی را پیدا کنند. کامپیوتر های آنها کلی باید برق مصرف کنند، کلی باید تجهیزات کامپیوتری خریداری شود .

سوال براتون پیش میاد که چه انگیزه ای هست که یکی داوطلب شه اگه انقدر براش زحمت داره؟ اینجاست که بیت کوین به هر کس که این کار را کند وعده داده که برای اینکه انگیزه داشته باشی که این بلاک ها رو تایید کنید و حساب ها را آپدیت نگه دارید ، من به خودت بیت کوین جایزه میدهم.

برای همینه که به این داوطلب ها میگن معدنچی. در حقیقت اونجا که بود گفتیم بیت کوین چاپ نمیشه استخراج میشه . منظور همین بود . هر بار که یک معدنچی بلاک را تایید می کند، بیت کوین های جدیدی را برای خودش استخراج می کند. این بیت کوین ها که استخراج می شوند تقریباً هر ۴ سال یک بار تعدادشان نصف می شود . اینطور می شود که به جمع ۲۱ میلیون می رسیم. مثلاً اوایلش از ۲۰۰۹ تا ۲۰۱۲ هر بار استخراج ۵۰ بیت کوین جایزه بود. چهار سال بعد شد ۲۵ تا یعنی تا ۲۰۱۶ و الان تا سال ۲۰۲۰ ۱۲,۵ بیت کوین هست و بعد می شود ۶,۲۵ و همینجور نصف می شود و ادامه پیدا می کند و هرچی هم میگذرد سخت تر میشه.

یک نکته جالب این که حتی این کار برای خودش شده صنعت. بهش می گویند صنعت mining .یک سری از افراد گروهی شرکت تاسیس می کنند و صبح تا شب کارشان این است که بیت کوین استخراج کنند. یک زمانی اون اوایل پیدایش بیت کوین ، بعد از اینکه دو سه روز کامپیوترتان روشن می ماند، شما با یک لپ تاپ هم می توانستید بیت کوین استخراج کنید ولی الان حتماً باید دستگاه های خاص خودش را خریداری کنید که برق وحشتناکی مصرف می کنند و هرروز هم که میگذرد قدرت پردازش گر بیشتری لازم دارید . چرا ؟ چون بالاتر گفتم که هر بلاک یک صفحه است. حالا شما فرض بگیرید هر بلاک ده دقیقه مبادله است که به جای اینکه صفحه ای باشد، وابسته به زمان است. به دلیل این که ممکن است تعداد این داوطلب های معدنچی زیاد شود در نتیجه این احتمال هست که به جای اینکه هر ده دقیقه جوابش را پیدا کنند، مثلاً جواب ۵ دقیقه ای به دست بیاید. اینجاست که بیت کوین درجه سختی آن عدد شانسی رو میبرد بالا . میگه مثلاً حالا که تعدادتان زیاد شده پس بروید یک عددی پیدا کنید که وقتی هش آن را می گیرید جواب کوچکتر از ۲۵ بشود.در نتیجه احتمال کمتر می شود . بعد دوباره بیت کوین می بیند همه سختشان شده و جواب پیدا کردن ۱۵ دقیقه طول کشید میگه خب باشه گناه دارید، بیایید یک عددی پیدا کنید که هش آن کوچکتر از ۵۰ بشود. در حقیقت انقدر درجه سختی رو بالا پایین می کند تا فیکس جواب سر ده دقیقه پیدا شود.

بحث دیگری که مطرح می شود این است که با فرض اینکه تکنولوژی بلاک چین جلوی تقلبات از این دست را می گیرد و حساب کل هم نگه می دارد ولی از کجا معلوم یکی به جای من اصلاً اعلام نکند که من انقدر دادم به فلانی ؟ یعنی چی؟

شما برای اینکه از حساب بیت کوین خودتان بیت کوین برای کسی بفرستید فقط به ۳ چیز احتیاج دارید . یکی شماره حساب خودتان ، دوم حساب آن شخص و سوم مقدار بیت کوینی که می خواهید بفرستید. یعنی رمزی پسووردی چیزی نمیخواد؟ چرا می خواهد.

هر کیف پول دو کلید دارد. یکی کلید عمومی و یکی کلید شخصی و محرمانه خودتان. کلید عمومی تان را همه می بینند . تنها حالتی که یکی می تواند از حساب شما پول واریز کند این است که اون کلید شخصی شما را داشته باشد. یک جور امضای دیجیتالیه به این معنی که عزیز جان این خود منم که دارم این تعداد بیت کوین را برای شما ارسال می کنم. پس در نتیجه هر کیف پول هم یک امضای دیجیتالی محرمانه دارد. درضمن یک پادکستی هست به اسم رادیو گیک که یکی از قسمت هاش خاص همین بلاک چین هست . اگر دوست داشتید پیشنهاد میدم گوشش کنید. جزییات بیت کوین زیاد داره ولی اینایی که گفتم یه مقدار اطلاعات اولیه ایبه که لازم داریم تا ببینیم این پول چه طور کار می کند. حالا برویم سراغ یک سری از فواید و معایب این بیت کوین.

فواید و معایب بیت کوین

۳ تا فایده اصلیش را که قبلاً گفتیم. یک اینکه هزینه مبادلاتش پایین است. دوم اینکه هویت شما محفوظه وایمنه چون ثبت اطلاعات فردی لازم نیست و سوم اینکه تقلبی توش وجود نداره.

ولی عیب های اصلیش این است که یک هکری ممکن است وارد کامپیوتر شما بشود و برود داخل حسابتان و کیف پول شما را به سرقت ببرد. در حقیقت کیف پول بیت کوینیی خود را یا باید داخل کامپیوتر نگه دارید یا در یک هارد درایو خارجی که ریسکش این است که یا یکی به کامپیترشما نفوذ کند و یا اصلاً هارد را گم کنید. بعد بدیش هم این است که اگر هارد را گم کنید و یا پولتان را به سرقت ببرند تقریباً دستتان به هیچ جا بند نیست. در سیستم پولی خودمان یک جورایی بانک مثلا اگر کارت اعتباریتان را گم کنید کمکتان خواهد کرد. برای مثال حسابتان را قطع می کند یا پیگیری می کند که این پول به حساب چه کسی رفته است و پلیس می تواند پیگیری کند. اما اینجا اگر بیت کوین شما رفت دیگه رفت فراموشش کنید.

مثلاً GOX یک شرکتی بود که تا اوایل ۲۰۱۴، هفتاد درصد از کل مبادلات بیت کوینی دنیا را انجام می داد.در حقیقت یک صرافی بیت کوینی بود. یعنی اشخاصی که می خواستند بیت کوین هایشان را به پول تبدیل کنند می رفتند آنجا. بعد به ناگهان در ۲۰۱۴ اعلام ورشکستگی کرد و در شرکت را بست. دلیلش چه بود؟ این شرکت اعلام کرد که حدود ۸۵۰ هزار بیت کوین از او دزدیده شده است یعنی به ارزش آن زمان یک چیزی حدود ۴۵۰ میلیون دلار.

مشکل دیگر بیت کوین این است که قیمتش حداقل الان پایدار نیست . مثل سهام می ماند .یک موقعی بیت کوین نیم دلار بود الان هر یک بیت کوین تبدیل شده به حدود۱۸ الی ۱۹ هزار دلار و هرروز هم که قیمتش عوض می شود. در نتیجه ریسک سرمایه گذاری هم در آن وجود دارد. دیگه الان همینطور قیمتش در حال افزایش است و خیلی ها می گویند که این وضعیت حباب است و به خاطر این است که همه دارند می شنوند بیت کوین، بیت کوین در نتیجه هی تقاضا برایش بالا می رود و قیمتش هم متعاقباً افزایش پیدا می کند. البته خود طرفدارهای بیت کوین می گویند هر یک بیت کوین حتی به چند صد هزار دلار هم می رسد چون که تعدادش محدود است و به دلیل اینکه بعد از یک زمانی عرضه محدود می شود، آرام آرام ارزش آن بالا می رود .اما به صورت کلی می توان گفت که ریسک سرمایه گذاری آن بالاست.

سرمایه گذاری در بیت کوین

حالا فرض بگیریم که به این پی بردیم که بیت کوین خوب است و میخواهیم روی آن سرمایه گذاری کنیم اما چگونه؟ شما چندراه دارید.

یک اینکه بروید معدن چی شوید و با اون راهی که گفتم بیت کوین استخراج کنید. دو اینکه مثلاً بروید کالایی یا خدمتی به کسی بفروشید و بگویید پولش را به بیت کوین به شما بدهند. مثلاً پیتزا بفروشید و بیت کوین هم قبول کنید. الان احتمالاً سوال براتون پیش میاد که یک بیت کوین که الان ۶۰ الی ۷ میلیون تومان است و این خریدهای خورد را که نمی شود با آن انجام داد. محض اطلاع شما، هر بیت کوین تا ۸ رقم اعشار توانایی خرد شدن دارد و کمترین میزان بیت کوین را می گویند یک ساتوشی به افتخار خالقش مثل یک شاهی قدیم. و سوم اینکه پول بدهید و بیت کوین خریداری کنید. سوال این است که از کجا بیت کوین بخریم.؟ چند راه وجود دارد.

یک سری صرافی آنلاین وجود دارند که مختص این کار هستند مثل coinbase .در همین گوگل هم اگر فارسی سرچ کنید ده تا لینک شرکت های ایرانی باز می شود که بیت کوین می فروشند. یا اینکه می توانید بروید به سایت هایی مثل local bitcoins که آنجا از دست خود فروشنده مستقیم بیت کوین بخرید. تعداد محدودی هم ATM در دنیا وجود دارند که از آن ها هم می شود بیت کوین خرید ولی تعدادشان زیاد نیست. که فکر کنم دوبی هم گویا دارد.

آینده بیت کوین

خلاصه که بیت کوین آمده در رادار دولت ها و دولت ها هنوز دقیقاً نمی دانند چه کار در مقابلش باید انجام دهند. مثلاً چین، کلاً بیت کوین را ممنوع کرده است یا در همین ایران خودمان، دولت و مجلس در حال بررسی آن هستند و در حال حاضر نه تاییدش کردند و نه ممنوعش کردند.

در حقیقت بسیاری از دولت ها فعلاً موضعی نسبت بهش نگرفتند. هر موضعی که دولت ها در مورد بیت کوین بگیرند، یکی از عوامل افزایش قیمت بیت کوین یا ترکیدن حبابش خواهد بود. در ضمن، یک چیزی حدود هزار و دویست، سیصد مدل رمز ارز در دنیا وجود دارد و فقط یکی از آنها بیت کوین است. مثلاً رمز ارزهایی وجود دارند به اسم لایت کوین، دش کوین، نیم کوین، اتریوم و .....که هرکدامشان یک سری تفاوت باهم دارند.

نکته آخر هم اینکه می گویند نزدیک به یک تا یک و نیم میلیون از بیت کوین های موجود در دنیا متعلق به خود ساتوشی ناکاماتو خالق بیت کوین است . یعنی اگر بیت کوین یک روزی آن ارزشی را که همه می گویند پیدا کند، این شخص می تواند ثروتمند ترین فرد جهان شود.