علی اسمعیلی سراجی
۹۴۲۲۲۱۰۲

گزارش بلاک‌چین و رمز ارزها

چکیده

یک سیستم یک-به-یک انتقال‌دهنده وجه الکترونیکی امکان معامله اشخاص بدون وجود سازمانی مرکزی را می‌دهد. امضای دیجیتال و استفاده از ledgerها می‌تواند قسمتی از حل این مساله باش ولی برای نگه‌داری تراکنش‌ها هنوز هم به شخص-سوم مورد اعتماد طرفین لازم است. در این گزارش راه‌حلی با استفاده از بلاک‌چین‌ها ارایه می‌شود. ساخت بلاک‌هایی که از تابع‌های هش و مقادیر Work-of-Proof پر شده است، قابلیت ایجاد اعتماد بدون نیاز به اعتماد شخص-سوم را فراهم می‌آورد. در این روش از قدرت پردازش مساله استفاده می‌شود و شخص غیرقابل اعتماد برای دور زدن پروتکل نیاز به توان پردازش بسیار بالایی دارد.

مقدمه

اقتصاد در شبکه اینترنت به طور روز افزون بر شرکت‌های مالی و انحصاری، به عنوان شخص-سوم مورد اعتماد برای انجام تراکنش‌های مالی متکی می‌شود. با این که این سیستم‌ها به خوبی کار می‌کنند، دارای ضعف ذاتی مدل نیاز به اعتماد به شخص-سوم می‌باشند. در این سیستم تراکنش‌های کاملا غیرقابل برگشت‌پذیر به طور واقع‌بینانه ممکن نیست، چرا که سازمان‌های واسطه می‌توانند درگیر مشکلات واسطه‌گری و اختلافات بین افراد می‌شوند. همین‌طور از آنجا که یک سازمان مرکزی مسؤولیت انجام تمامی تراکنش‌ها را برعهده دارد، هزینه انجام هر تراکنش بالاست و این موضوع باعث محدودیت در انجام تراکنش‌ها با مقدار کم می‌شود. این مساله باعث عدم قطعیت در انجام تراکنش و امکان ایجاد اشتباهات را نیز بالا می‌برد.

قبل از این، تنها راه‌حل مشکلات و هزینه‌های ذکر شده انجام معاملات به صورت فیزیکی و عدم استفاده از سازمان‌ها و اشخاص واسطه بود.

در اینجا نیاز سیستم انتقال وجه الکترونیکی بر پایه ریاضیات رمزنگاری به جای اعتماد نیاز است، به طوری که هر دو نفر بتوانند به صورت مستقیم به تبادل وجه بدون نیاز به شخص-سوم بپردازند. تراکنش‌هایی که به صورت محاسباتی غیر قابل برگشت پذیر هستند، می‌توانند در حل این مساله استفاده شوند.

در این گزارش راه‌حلی توزیع‌شده و یک-به-یک، با روش ایجاد اعتماد با تولید پیچیدگی محاسباتی ارایه می‌کنیم. سیستم تا زمانی که توان محاسباتی بیشتر در اختیار سیستم‌های صادق است، امن می‌ماند.

تراکنش‌ها

در این سیستم تراکنش‌ها به صورت رکوردهایی از نام فرستنده، نام گیرنده، مقدار تراکنش است.

برای جلوگیری از جعل تراکنش، هر فرستنده، تراکنش را با استفاده از کلید خصوصی خود با استفاده از الگوریتمی رمزگذاری نامتقارن، امضا می‌کند و هر کسی می‌تواند با استفاده از کلید عمومی فرستنده صحت رکورد اطلاعاتی را چک کند. برای جلوگیری از حملات double-spending، هر تراکنش دارای کلیدی یکتا است... در صورتی که حمله‌کننده به نحوی دوبار یک رکورد تراکنش را وارد چرخه پردازش کند، از آنجا که یکتایی کلید رکورد نقض می‌شود، می‌توان دریافت که تراکنش مذکور بی‌اعتبار است.

با داشتن مجموعه تراکنش‌ها می‌توان مقدار تغییرات اعتبار هر فرد را تعیین کرد.

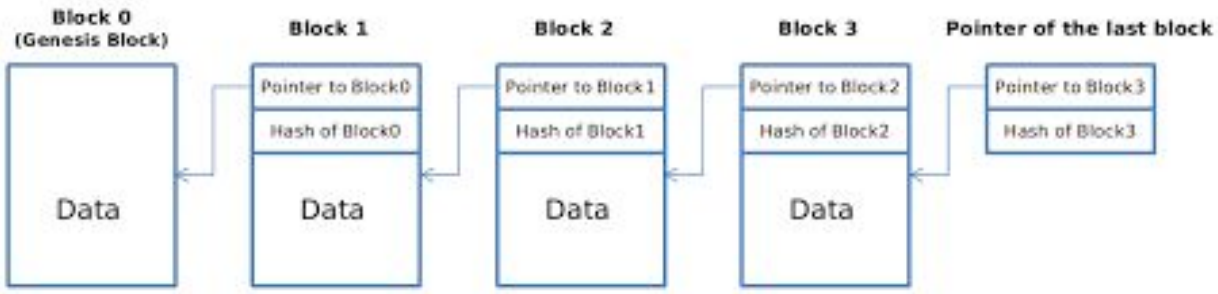
ID: 58217	From: Alice	To: Bob	Value: 3	Signature: AA...c

بلاک‌چین

برای بی‌نیازی از اطمینان به شخص‌سوم، از داده ساختاری به نام بلاک‌چین استفاده می‌شود.

بلاک‌چین دادساختاری مانند Linked List است که در آن هر علاوه بر فیلدهای دلخواه، دارای دو فیلد اضافه مقدار Hash گره قبلی، و مقدار Hash تمامی فیلدهای گره فعلی (از جمله مقدار فیلد Hash گره قبلی) است.

این خاصیت باعث تغییر ناپذیری کل زنجیره می‌شود به طوری که در صورت تغییر فیلدی از یک بلاک دلخواه، مقدار Hash این بلاک، و تمامی بلاک های بعدی تغییر می‌کند. و بنابراین تمامی آن‌ها باید دوباره محاسبه شوند.



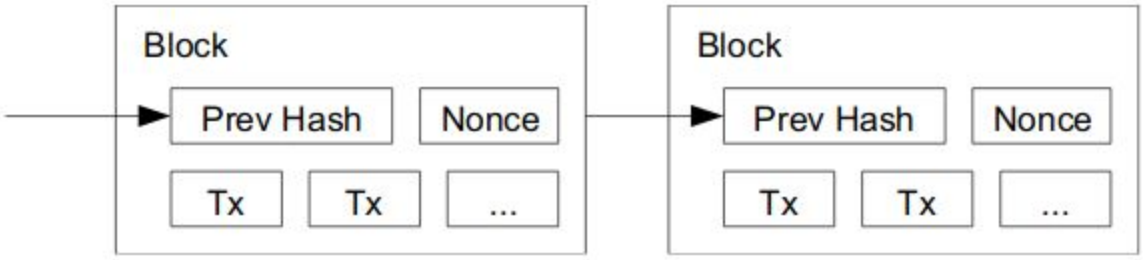
بلاک‌چین و Proof-of-Work

کامپیوترهای امروزی دارای قدرت پردازشی بالایی هستند، و می‌توانند هزاران مقدار Hash را در یک ثانیه محاسبه کنند. بنابراین در صورتی که مقداری از زنجیره بلاک‌ها به سادگی می‌توان تمامی Hashهای تغییر کرده گره‌های بعدی را در زمان کوتاه محاسبه کرد. برای افزایش پیچیدگی زمان محاسبه Hash هر گره، محدودیتی به صورت مساله برای هر بلاک عنوان می‌شود که برای حل کردن بهینه این مساله، تا کنون هیچ راه‌حل بهینه‌ای پیدا نشده و برای حل آن تنها می‌توان از سعی و خطا استفاده کرد. این مساله می‌تواند به

صورتی عنوان شود که با تعیین فیلد خاصی که معمولا نام آن Proof-of-Work است، تعداد n بیت اول Hash بلاک، به صورت صفر و یا یک باشد.

در صورتی که مقدار این n، برای مثال ۳۰ انتخاب شود، به صورت میانگین از بین هر 2^{30} حدس، یک مقدار دارای این خاصیت خواهد بود.

بنابراین با این روش می‌توان مقدار محاسبات مورد نیاز برای محاسبه Hash هر بلاک را تنظیم کرد.



حل مساله نیاز به اعتماد شخص‌سوم

در روشی که فقط از تراکنش‌های امضا شده استفاده شود، نیاز به مکانی قابل اعتماد برای ذخیرسازی رکوردهای تراکنش‌ها است. برای حل این مساله، می‌توان به صورتی عمل کرد که همگی افراد نسخه‌ای از تمامی تراکنش‌ها را داشته باشند و هر کس برای انتقال اعتبار می‌تواند تراکنشی با امضای خود ایجاد کرده و آن را برای تمامی افراد بفرستند. بدین صورت همه مقادیر یکسانی از تراکنش‌ها در اختیار دارند.

اما در این بین به فرایندی برای مشکل عدم تطابق داده‌ها نیاز داریم. این عدم تطابق داده ممکن است تلاشی برای دور زدن فرایند سیستم از سمت یک کاربر، یا بروز خطا در انتقال اطلاعات بین افراد پیش آید.

پروتکل زیر را تعریف می‌کنیم:

- هر فرد فرستنده، برای انجام تراکنش، آن را امضا کرده و برای همه می‌فرستد.
- افرادی تحت عنوان استخراجگرها این تراکنش‌ها را جمع آوری می‌کنند.
- استخراجگرها با قرار دادن تراکنش‌ها در یک بلاک، سعی در پیدا کردن مقدار Proof-of-Work برای مقدار قراردادی n می‌کنند.
- اولین استخراجگری که مقدار Proof-of-Work مناسب را پیدا کرد، بلاک جدید را برای همه می‌فرستد.
- هر فرد بلاک‌های دریافت شده را بازبینی می‌کند و تمامی بلاک‌های تایید شده را نگه می‌دارد. بلاکی که طول بیشتری دارد، دارای قابلیت اطمینان بیشتری است. چرا که فرض کردیم تعداد افراد صادق بیشتر، و دارای قدرت محاسباتی بیشتری هستند. پس بنابراین در مدت زمانی محدود، تعداد بیشتری بلاک را می‌توانند تولید کنند.

حمله بر علیه شبکه

حالتی را فرض می‌کنیم که مهاجمی زنیجرمجایگزینی طولانی‌تر نسبت به زنجیره اصلی را تولید کرده باشد.

این زنجیر نمی‌تواند شامل تراکنش‌هایی برای انتقال اعتبار از دیگر افراد به خودش باشد، چرا که کلید خصوصی دیگران را ندارد و نمی‌تواند تراکنش را امضا کند و افراد صادق، این بلاک را رد صلاحیت می‌کنند.

پس مهاجم تنها می‌تواند زنجیری تولید کند که از زنجیر اصلی طولانی تر باشد، و اعتباری که پرداخت کرده است را دوباره به خود برگرداند از آنجایی که فرض کردیم .

اعتبار برای استخراجگرها

برای تشکیل اکوسیستم، به توان پردازشی استخراجگرها نیاز است. بنابراین هر استخراجگر که بلاکی را استخراج می‌کند می‌تواند نام خود را به عنوان سازنده آن بلاک درون فیلدی خاص جای دهد و از این طریق مقدار تعیین شده‌ای اعتبار کسب کند.

همچنین هر فرستنده، می‌تواند در فیلدی در رکورد تراکنش، اعتبار را برای استخراجگر قرار دهد. فرض کنیم احتمال جلو رفتن زنجیر صادقانه p و احتمال جلو رفتن زنجیر مهاجم q است. این مساله تبدیل به مساله Gambler's Ruin می‌شود با تعداد نامتناهی اعتبار اولیه می‌شود. ثابت می‌شود اگر مقدار p بزرگتر q باشد، احتمال جلو بودن زنجیر در مرحله z به سرعت نزدیک به یک می‌شود و حد آن در بی‌نهایت یک است.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012
```

نتیجه‌گیری

در این گزارش سیستمی الکترونیکی برای تراکنش‌های مالی مبتنی بر عدم اطمینان معرفی شد. با استفاده از روش مرسوم امضا تراکنش‌ها شروع کردیم که روشی قدرتمند برای جابه‌جایی تراکنش‌ها است. ولی باز هم نیاز به اطمینان به شخص-سومی و مرکزی برای نگه‌داری پایگاه‌داده تراکنش ها بودیم. برای حل این، شبکه‌ای یک-به-یک از تمامی افراد در نظر گرفتیم که همگی تاریخچه تمامی تراکنش‌ها را نگه می‌دارند. با استفاده از بلاک‌چین و مفهوم Proof-of-Work، به دلیل افزایش مداوم حجم پردازشی مورد نیاز مهاجم، می‌توان به زنجیره‌های بلندتر و تراکنش‌های قدیمی‌تر درون زنجیره اعتماد کرد. این شبکه نیز به دلیل عدم نیاز به جهت‌دهی پیام‌های انتقالی درون شبکه، دارای ساختار پیچیده‌ای نیست و پیاده‌سازی آن را راحت‌تر می‌کند.

منابع:

- https://bitcoin.org/bitcoin.pdf
- https://en.wikipedia.org/wiki/Blockchain
- https://en.wikipedia.org/wiki/Bitcoin
- https://youtu.be/SSo_ElwHSd4
- https://youtu.be/bBC-nXj3Ng4
- https://youtu.be/9V1bipPkCTU