پروژه ی نرم افزار دوره کارشناسی

گزارش شماره ۷ - درک تراکنش ها

آریا رادمهر - ۹۷۴۶۳۱۲۵

دکتر سجاد حق زاد کلیدبری

January 29, 2022

برای فهم چگونگی انتقال پول ها و انجام تراکنش ها، نکته ی حائز اهمیت این است که به طور کلی در این ساختار ایده ی کلی جا به جایی یک پول دیجیتال است و نه پول واقعی. از این رو نوع نگاه به نحوه ی شکل دهی ساختاری برای مدیریت و ردیابی پول های دیجیتال بسیار با اهمیت است.

پول های دیجیتال به دو صورت قابل پیاده سازی هستند.
مدل اول پیاده سازی، مدلی در فرم پیاده سازی مبتنی بر حساب است (account based). در این مدل که اصولا ساده ترین مدل پیاده سازی به شما می آید، تراکنش ها به صورت رویداد هایی ثبت میشوند و نحوه ی انتقال پول ها را شرح میدهند به طوری که در حالت کلی یک سیاهه ای از تراکنش ها بر حسب انتقالات از شخصی به شخص دیگر یا در صورت دقیق تر از حسابی به حساب دیگر تشکیل میشود.
برای مثال حالت زیر را در نظر بگیرید.

10 coins credit to Ali	(Asserted by miners)
Transfer -> 3 coins from Ali to Sohrab	Signed(Ali)
Transfer -> 2 coins from Sohrab to Hanie	Signed(Sohrab)
Transfer -> 2 coins from Hanie to Ali	Signed(Hanie)
Transfer -> 5 coins from Ali to Sajjad	Signed(Ali)

این شیوه ی قابل قبولی از نگهداری تراکنش هاست؛ اما یک مشکل اساسی در آن وجود دارد و آن این است که اگر در این لحظه بپرسیم که سهراب چند سکه دارد، میبایست از تاریخ شروع فعالیت سهراب، تراکنش های او را رهگیری کنیم و سپس به زمان حال برسیم تا به جواب دست پیدا کنیم.
اما راه بهتری برای ردیابی دارایی های افراد در دنیای رمز ارز ها وجود دارد که بجای ردیابی حساب ها، به ردیابی سکه ها میپردازد و سکه ها را track میکند. این مدل عموما به عنوان شیوه ی ledger based شناخته میشود.

در این مدل به صورت دقیق تر، تراکنش ها بر اساس ورودی و خروجی ها ذخیره میشوند. این حالت تشخیص تعداد سکه های هر فرد را در لحظه بسیار ساده تر میکند و همچنین امکان چک کردن معتبر بودن تراکنش ها را نیز فراهم میکند زیرا معماری این نوع از مدل به صورت غیر قابل تغییر (immutable) میباشد.

حالت زیر چگونگی پیاده سازی این شیوه را بیان میکند.

1	Inputs: Ø Outputs: 20.0 -> Ali	
2	Inputs: 1[0] Outputs: 17.0 -> Soheil, 8.0 -> Ali	Signed(Ali)
3	Inputs: 2[0] Outputs: 8.0 -> Hanie, 9.0 -> Soheil	Signed(Soheil)
4	Inputs: 2[1] Outputs: 6.0 -> Amir, 2.0 -> Ali	Signed(Ali)

در جدول بالا ابتدا هر تراکنش یک شماره به خود میگیرد. همچنین هر تراکنش شامل یک ورودی (input) و یک خروجی (output) میباشد. در ورودی اشاره به شماره ی تراکنش مرجع میشود و در خروجی تقسیم سکه ها قابل مشاهده است.

همانطور که میبینیم، فرض کنید که ۲۰ سکه توسط ماینر ها به علی داده شده است.

در تراکنش دوم، مشاهده میکنیم inputs: 1[0] است، یعنی علی میخواهد با استفاده از دارایی های خود در تراکنش مرجع شماره یک ، تقسیم سکه انجام دهد. او در بخش خروجی ۱۷ سکه از ۲۵ سکه ی خود را به سهیل میدهد (Soheil -> 17.0) و مابقی را نیز برای خود نگه میدارد(Ali -> 8.0) و آنرا با کلید شخصی خود امضا میکند.

در تراکنش سوم، سهیل میخواهد با توجه به سکه هایی که از تراکنش مرجع شماره ۲ در اختیار دارد (تعداد ۱۷ سکه)، ۸ سکه را به هانیه بدهد و ۹ سکه را نیز برای خود نگه دارد.

و در تراکنش چهارم، علی با استفاده از تعداد سکه هایی که در تراکنش مرجع شماره ۲ در اختیار دارد، ۶ سکه را به امیر و ۲ سکه را برای خود نگه میدارد.

اکنون اگر بپرسیم علی چند سکه دارد، میگوییم ۲ سکه. اگر بپرسیم سهیل چند سکه دارد، میگوییم ۹ سکه و دیگر افراد را نیز به همین صورت میتوان مورد بررسی قرار داد.