پروژه ی نرم افزار دوره کارشناسی

گزارش شماره ۸ - نگهداری ها

آریا رادمهر - ۹۷۴۶۳۱۲۵

دکتر سجاد حق زاد کلیدبری

February 8, 2022

تا به اینجای کار درک کردیم که تراکنش ها چگونه در بلاکچین ثبت و ذخیره میشوند و همچنین سکه ها چگونه منتقل میشوند، اما سوالی که مطرح میشود این است که چگونه میتوان سکه ها را ذخیره کرد؟

در گذشته بررسی کردیم که هر شخص برای امضای یک تراکنش و مابقی کار ها نیاز به دو کلید خصوصی و عمومی داشت، حال باید بگوییم که عملیات های ذخیره سازی و انتقال و ارسال پول نیز از طریق کلید خصوصی قابل انجام میباشند.

رویکردهای مختلف برای مدیریت کلیدها، مبادلات متفاوتی بین در دسترس بودن، امنیت و راحتی ارائه می دهد.

روش های مختلفی برای ذخیره سازی سکه ها وجود دارد.

۱- فضا های ذخیره سازی متصل به شبکه یا دستگاه (Hot Storage):

این فضا های ذخیره سازی عموما دستگاه ها و device هایی هستند که توسط کامپیوتری پیاده سازی و مدیریت میشوند و به شبکه ی بلاکچین نیز میتوانند به صورت مستقیم متصل شوند. کیف پول های دیجیتال مثال خوبی برای نحوه ی ذخیره سازی به صورت hot هستند.

کیف پول (wallet) های دیجیتال که مرسوم ترین نحوه ی ذخیره سازی ارز های دیجیتال میباشند، میتوانند به صورت یک برنامه روی کامپیوتر، یک اپلیکیشن موبایل و یا یک وبسایت وجود داشته باشند. آنها به این صورت عمل میکنند که در هنگام ثبت اطلاعات اولیه در آن و یک پسورد، یک جفت کلید خصوصی و عمومی برای شما میسازند. کلید خصوصی توسط برنامه مورد امنیت قرار میگیرد و فقط و فقط دارنده ی کیف پول باید آنرا به همراه داشته باشد. از طرف دیگر کلید عمومی برای همگان میتواند مورد استفاده قرار بگیرد؛ مثلا وقتی شخصی آدرس کیف پول خود را به شخص دیگری میدهد، در حقیقت مقدار کلید عمومی خودش را با آن شخص به اشتراک میگذارد. پس در هنگام جا به جایی یک پول صاحب آن از کلید خصوصی خود استفاده میکند اما دریافت پول از طریق داشتن کلید عمومی امکان پذیر است.

طبق این تقاسیر میتوان ادعا کرد که نگهداری سکه ها در حقیقت به نگهداری و مدیریت کلید های خصوصی خلاصه میشود.

اکنون فرض کنید میخواهیم در ازای خرید یک کالا مقداری سکه به فروشنده آن بدهیم، در ابتدا آدرس کیف پول فروشنده که همانطور که گفته شد کلید عمومی کیف پول اوست را دریافت میکنیم و در کیف پول دیجیتال خود میزان سکه ای را برای این مبادله در نظر میگیریم. حال کاری که کیف پول شما انجام میدهد این است که با داشتن کلید خصوصی شما، یک درخواست انتقال سکه با کلید عمومی از طرف شما به کلید عمومی فروشنده ایجاد میکند.

سپس این درخواست را به گره های شبکه میفرستد، آنها این درخواست را در mempool خود قرار داده و سپس عملیات استخراج بلاک جدید را آغاز میکنند. حال بعد از مدت زمانی، چنانچه بلاک جدیدی توسط گره ها استخراج شود که یکی از تراکنش های داخل آن تراکنش شما باشد، آن میزان سکه از شما به فروشنده منتقل میشود.
کیف پول های دیجیتال دارای مزایای دیگری نیز هستند، آنها میتوانند لیست تراکنش های شما شامل ارسال و یا دریافت سکه ها، آدرس کیف پول های افرادی که قبلا با آنها تبادل سکه داشته ایم و یا قابلیت اسکن کلید خصوصی افراد از روی متن بر روی یک کاغذ و یا به صورت کد QR را مدیریت کنند. اما در نهایت همه چیز به کلید خصوصی در کیف پول ها بازمیگردد.

۲- فضا های ذخیره سازی ایزوله (Cold Storage):

این فضا های ذخیره سازی عموما ذخیره ی جفت کلید ها به دور از هر دستگاه کامپیوتری متصل به شبکه و یا بر روی کامپیوتر میباشند. راه و روش های مختلفی برای ذخیره ی داده ها به صورت clod وجود دارد. میتوان کلید ها را به صورت یک فایل متنی (text) در داخل یک حافظه ی خارجی (external) ذخیره کرد، در حافظه سپرد و یا حتی بر روی کاغذ نوشت و در جایی امن قرار داد. به طور کلی انتخاب روش ذخیره سازی به شخص بازمیگردد.

حال باید بدانیم که شکل واقعی کلید خصوصی یا عمومی کلید ها به چه صورت است.

در دنیای دیجیتال و کامپیوتر همه چیز در انتها تعدادی صفر و یک است و کلید ها هم از این قاعده مستثنی نیستند. آنها به صورت کلی یک رشته ی بسیار طولانی از صفر و یک ها (در مبنای ۲) هستند که برای راحتی کار عموما در مبناهای بالاتر مثل مبنای ۵۸ قرار میگیرند و خوانده میشوند تا هم امکان ساخت تعداد بیشماری کلید و در نتیجه کیف پول فراهم شود و هم از طرفی تعداد کاراکتر های رشته ی ساخته شده بیش از حد طولانی نشود.

برای مثال شکل یک کلید عمومی میتواند به صورت زیر باشد:

```
Public key:
63FaC9201494f0bd17B9892B9fae4d52fe3BD377
```

```
Private key:
8da4ef21b864d2cc526dbdb2a120bd2874c36c9d0a1fb7f8c63d7f7a8b41de8f
```