پروژه ی نرم افزار دوره کارشناسی

گزارش شماره ۳ - عدم تمرکز و بحث بر اجماع

آریا رادمهر - ۹۷۴۶۳۱۲۵

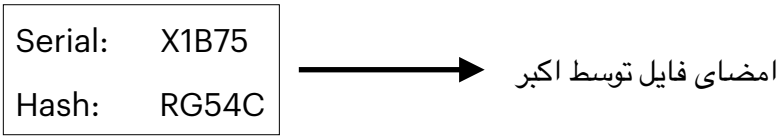
دکتر سجاد حق زاد کلیدبری

November 16, 2021

سکه ی اکبر و جمشید (عدم تمرکز)

برای اینکه به درک چالش های اجماع و بحث بر روی عدم تمرکز در بلاکچین پی ببریم، بگذارید تا با مثالی آن را شرح دهیم. اکبر را تصور کنید که تصمیم میگیرد سکه ای با نام خودش در دنیای دیجیتال بسازد. از قضا او تنها کسی است که میتواند این کار را انجام دهد.

سکه ی او در اصل یک فایل دیجیتالی میباشد که شماره سریالی یونیک را برای آن فایل، به عنوان سریال سکه ی خودش در نظر میگیرد. سپس او فایلی که دارای شماره سریال میباشد را هش کرده و با استفاده از کلید خصوصی خودش آن فایل را امضا میکند.



سکه ی اول

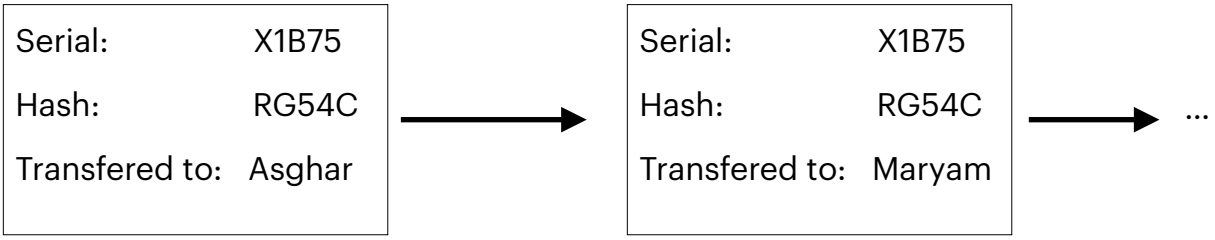
این به دیگران اطمینان میدهد که اولا شماره ی سریال آن سکه معتبر است (زیرا فایل سریال آن سکه هش شده) و دوما اکبر شخصا این سکه را ساخته (زیرا با کلید خصوصی خودش آنرا امضا کرده) است.

اکنون فرض کنید که اکبر سکه ی خود را به اصغر میدهد. اصغر همواره میتواند ثابت کند که آن سکه اصل بوده و توسط اکبر ساخته و امضا شده است و چنانچه کسی شک به اصالت سکه دارد میتواند با کلید عمومی اکبر از صحت اطلاعات محتوای سکه (که در اصل همان فایل دیجیتالی است) اطمینان حاصل نماید.

بعد از مدتی اصغر تصمیم میگیرد تا سکه ای که از اکبر گرفته بوده است را به مریم بدهد. اما مریم این سکه را قبول نخواهد کرد. او مطمئنا از اصغر میپرسد : از کجا معلوم است که تو این سکه را به من دادی؟ این سکه را که اکبر صادر کرده است!. این سکه اصلا متعلق به چه کسی است؟

در اینجا به این نکته دست میبابیم که همواره هش کردن و امضای دیجیتال، پاسخگوی مشکلات ما در سیستم ایمن بر بستر بلاکچین نخواهد بود. ابزاری که میتوانیم توسط آن مشکل را حل کنیم، ابزاریست که رد و بدل کردن سکه ها را ذخیره کند. برای اینکار اکبر در ابتدا اگر میخواهد که سکه ی خود را به اصغر بدهد، علاوه بر شماره سریال، بر روی آن مینویسد: «به اصغر انتقال داده شد» و سپس آن را امضا میکند. حال اگر اصغر این سکه را داشته باشد

ادعا میکند که سکه اصل بوده و همچنین توسط گفته ی اکبر به او منتقل شده است. اکنون اصغر میتواند سکه ی خود را به مریم بدهد و مریم سکه را به شرطی قبول خواهد کرد که اصغر بر روی آن بنویسد:«به مریم انتقال داده شد» و آنرا با کلید خصوصی خود امضا کند.



امضای فایل توسط اکبر

امضای فایل توسط اصغر

اما مشکل بزرگی این وسط امنیت سکه های تولید شده توسط اکبر را تهدید میکند.

یکی از چالشی ترین و خطرناک ترین مسائل در دنیای ارز های دیجیتال، دوبار خرج کردن (Double Spending) میباشد. این مسئله به شکل ساده بیانگر آن است که واحد از یک ارز نباید بیش از یکبار توسط کسی خرج شود. ممکن است که اصغر به شکل همزمان پول را به مریم و شخص دیگری انتقال بدهد.

بگذارید برای حل این مشکل مثالی را طرح کنیم؛ تصور کنید جمشید نیز فردی است که عینا به مانند اکبر سکه های معتبری را تولید میکند. اما راه حل او برای مسئله این است که علاوه بر کاری که اکبر در انتقال سکه انجام میداد، او لیستی از نقل و انتقالات را بوجود می آورد که بر روی آن رد و بدل شدن سکه ها از فردی به فرد دیگر ثبت میشود. در اینجا چنانچه فردی بخواهد به شکلی سعی در double spend کردن سکه ی متعلق به خود کند، دیگر افراد میتوانند به آن لیست مراجعه کرده و از یک و فقط یکبار خرج شدن آن سکه اطمینان حاصل کنند.

Serial:	X1B75
Hash:	RG54C
Transfered to:	Sadegh

امضای فایل توسط جمیشد

Serial:	X1B75
Hash:	RG54C
Transfered to:	Sogol

امضای فایل توسط صادق

Serial:	X1B75
Hash:	RG54C
Transfered to:	Keyvan

امضای فایل توسط سوگل

دفتر کل نقل و انتقالات جمیشد

در مرحله اول

Serial:	X1B75
Is now for:	Sadegh

در مرحله دوم

Serial:	X1B75
Is now for:	Sadegh
Is now for:	Sogol

در مرحله سوم

Serial:	X1B75
Is now for:	Sadegh
Is now for:	Sogol
Is now for:	Keyvan

بیایید تا نگاهی کلی بر روی سیستم ساخت سکه ی جمشید داشته باشیم. این سیستم هرچند که مشکل دوبار خرج کردن سکه ها را حل کرده، ولی عملا بمانند یک بانک مرکزی عمل میکند. بنظر می آید که راه حل برطرف کردن مشکل دوبار خرج کردن در متمرکز کردن سیستم است؛ اما همانطور که در ابتدای بحث نیز گفته شد، دیدگاه بلاکچین بر خلاف این رویکرد و عدم تمرکز در سیستم است تا همواره یک بانک، یک مرکز، یک انبار ذخیره ی داده و ... وجود نداشته باشد.

مسئله ای که در اینجا مطرح میشود این است که در صورت پخش کردن این سیستم در دست چند نفر، مشکل به اجماع رسیدن در داده ها بوجود می آید. زیرا اگر تعدادی افراد دیگر نیز بخواهند سکه ای را که جمشید میساخته را بسازند، آن موقع در نقل و انتقالات آن دچار مشکل میشوند؛ چون هر کدام از آنها یک دفتر کل مخصوص به خود را نگه خواهند داشت و دیگر نمیتوانند بر سر معتبر بودن یک سکه یا نقل و انتقالات آن به اجماع برسند.

بحث بر اجماع

هنگامی که قرار است سیستمی با ساختار غیر متمرکز پیکر بندی شود، همواره پنج اصل مهم درباره ی آن مطرح میباشد که عبارتند از:

۱- چه افرادی مجاز هستند که دفتر کل داده ها را نگه داری کنند؟

۲- چه افرادی میتوانند صحت اطلاعات (برای مثال تراکنش ها یا حتی اطلاعات دفتر کل داده ها) را چک کنند؟

۳- چه افرادی میتوانند داده ی جدید (برای مثال در اینجا سکه ی جدید) را تولید کنند؟

۴- چه افرادی قوانین و خط مشی سیستم را تعیین خواهند کرد؟

۵- چگونه داده های تولیدی (بمانند سکه ها) ارزش گذاری خواهند شد؟

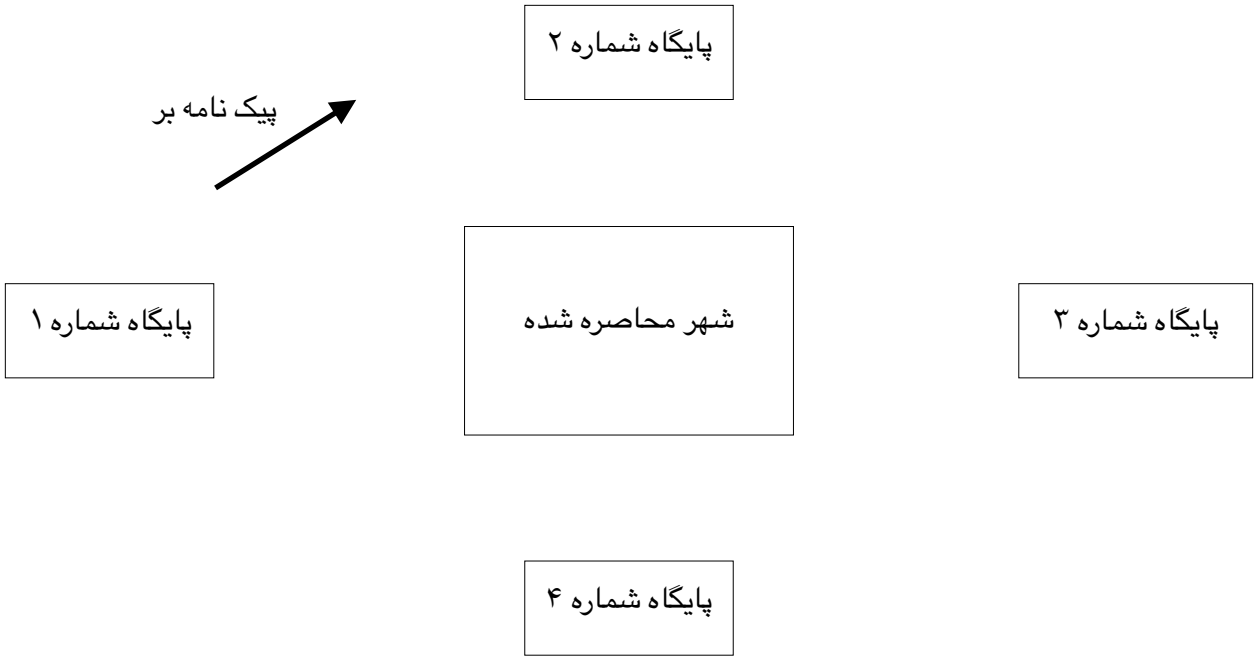
توجه کنید که همواره ۳ اصل اول از اصول بالا، از مباحث تکنیکال سیستم های غیر متمرکز هستند. در حالی که اصول ۴ و۵ از بیشتر رویکرد مدیریتی و اقتصادی دارند. این سوالات همواره با روشی درست از اجماع و توافق نظر بین افراد شرکت کننده در سیستم پاسخ داده خواهد شد. (گفتنیست که در دنیای رمز ارز ها ابتدا بیتکوین بود که جواب تمامی سوالات بالا را با روشی نوین طرح کرد و باعث شگفتی و توجه همگان شد.)

رویکرد درست اجماع در سیستم های غیر متمرکز ممکن است بسیار دشوار و حتی غیر ممکن باشد. برای درک بهتر اجماع در این سیستم ها بگذارید تا یکی از مسائل کلاسیک مرتبط با این مسئله را مطرح کنیم.

مسئله ی ژنرال های بیزانسی:

در این مسئله، گروهی از ژنرال های بیزانسی شهری را محاصره کرده اند. ژانرال ها به علت کمبود نیرو، امکان حمله مستقل به شهر را ندارند. در نتیجه ژنرال ها به توافقی برای حمله یا عقب نشینی احتیاج دارند. آنها برای انتقال پیام و نظر خود تنها میتوانند از هر پایگاه یک پیک به پایگاه های دیگر بفرستند.

در مسئله ژانرال های بیزانسی، به جز چالش زندانی شدن پیک ها، چند چالش دیگر هم وجود دارد. چالش نخست با تاخیر رسیدن، گم شدن یا نابودی پیام است. چالش دوم این است که به علت خطرات، ژنرال ها امکان تغییر رای ندارند. چالش سوم این است که شاید ژنرال یا ژنرال هایی خیانتکار باشند. جالب اینجا است که در صورت افزایش تعداد ژنرال های خیانتکار، آن ها می توانند حمله را مختل کنند.



آن چنان که احتمالا تاکنون حدس زده اید این حالت دقیقا مدل ارتباط گره ها (node) در شبکه بلاکچین است.

(توجه کنید که در مسئله ی ما هر فردی که در سیستم غیر متمرکز مشارکت دارد یک گره تلقی میشود) هر گره نقش ژنرالی است که باید نظرش را درباره هر حمله یا تراکنش اعلام کند.

راه حل ها و حتی فرمول های بسیار زیادی برای اجماع در چنین مسائلی بیان شد بطوری که حتی گفته میشود در چنین سیستم هایی چنانچه یک سوم افراد مشارکت کننده بر خلاف انتظار عمل کنند، اجماع با شکست مواجه خواهد شد. اما دو راه ساده برای اجماع در دنیای دیجیتال مطرح شد.

۱- هر کسی در قبال مشارکت خود پاداش میگیرد.

برای مثال در سیستم غیر متمرکزی که از آن یاد کردیم، هر فرد در صورت امضای یک بلاک مقداری سکه را به عنوان پاداش دریافت میکند. این باعث میشود تا افراد در سیستم بر خلاف عرف عمل نکنند بلکه صاحب پاداش شوند.

۲- ساخت و افزودن بلاک ها به سیستم باید به نحوی به صورت شانسی و random صورت بگیرد.

در اینجا نکته ی حائز اهمیت این است که تصمیم درمورد ساخت بلاک به صورت شانسی در افراد ممکن است باعث وقوع حمله ی سیبیل (Sybil Attack) شود. این حمله به صورتیست که امکان دارد شخصی چندین و چند کپی و node از خود در سیستم ایجاد نماید تا امکان پیروزی وی در این سیستم random بیشتر شود.

اجماع ضمنی (implicit)

برای اجماع به صورت ضمنی همواره پنج گام اساسی نیاز است.

۱- تراکنش های جدید به تمام گره ها پخش (broadcast) میشوند.

۲- هر گره تراکنش های جدید را در یک بلاک ذخیره میکند. (به این روند ذخیره سازی تراکنش ها در بلاک mempool گفته میشود)

۳- در هر راند (زمان معین شده) یک گره به صورت رندوم بلاک ساخته شده ی خود را برای تمامی گره ها broadcast میکند.

۴- گره های دیگر آن بلاک را به عنوان بلاک جدید میپذیرند، تنها به شرطی که تمامی تراکنش های داخل بلاک معتبر باشند. (سکه ها خرج نشده باشند، دارای اعتبار باشند و امضا شده باشند)

۵- گره ها پذیرش بلاک را با گنجاندن هش آن در بلاک بعدی که ایجاد می کنند، بیان می کنند.

با این شیوه میتوانیم ادعا کنیم که مشکل ها و چالش هایی که پیش از این با آنها رو به رو بودیم را حل کرده ایم.