

مفاهیم اولیه بلاک چین

علیرضا سلطانی نشان

۳۰ دی ۱۴۰۲

فهرست مطالب

۲	۱ مجوز
۲	۲ مقدمه
۲	۳ تاریخچه
۲	۱.۳ مشکل Double spending
۲	۲.۳ ساختار پول
۲	۱.۲.۳ پول‌ها و ارزهای Fiat
۲	۲.۲.۳ پول‌ها و ارزهای دیجیتال
۲	۳.۲.۳ مشکلات
۲	۳.۳ راهکار Ledger
۳	۴ نظریه ارزش
۳	۵ خاصیت‌های هش مرسوم
۳	۶ خاصیت‌های هش رمزارها
۳	۷ امضاها
۴	۱.۷ خصوصیات کلید عمومی
۴	۸ بلاک چین چیست؟
۵	۹ مسئله اجماع
۵	۱۰ اجماع ضمنی
۵	۱.۱۰ مسئله Mempool
۶	۱۱ مفهوم Proof of Work (POW)
۶	۱.۱۱ مفهوم Nonce
۶	۲.۱۱ مفهوم Difficulty
۶	۳.۱۱ TRX Fee
۶	۴.۱۱ مفهوم Halving

۱ مجوز

به فایل مجوز که همراه این برگه قرار دارد توجه کنید. لازم به ذکر است که این برگه تابع مجوز GPLv۳ می باشد که به مخاطب اجازه می دهد بدون هیچ گونه محدودیتی، کد و خروجی/pdf مربوطه را به صورت رایگان منتشر و استفاده کند.

۲ مقدمه

جزوه ای که اکنون در حال خواندن آن هستید معرفی مفاهیم اولیه و بسیار مهم بلاک چین است که با تمرکز بر روی بیت کوین نوشته شده است. مرجع اصلی این جزوه کتاب Bitcoin and Cryptocurrency Technologies می باشد. دیدگاهی بسیار قابل توجهی در این جزوه بر اساس بستر بیت کوین می باشد.

۳ تاریخچه

۱.۳ مشکل Double spending

یکی از چالش های پول دیجیتال در دیدگاه اول، قابلیت کپی گرفتن و دوبار خرج کردن یک پول می باشد. یک کاربر نباید قادر به خرج مجدد یک پول باشد. پول های کاغذی را نمی توان به راحتی کپی کرد چرا که دشوار هستند و توسط یک نهاد یا بانک مرکزی اصطلاحاً تایید شده نمی باشد. اما در پول های دیجیتال چون در مفهوم دیجیتال و کامپیوتری شده پدید آمدند ممکن است امکان کپی کردن یک پول وجود داشته باشد. به همین خاطر برای جلوگیری از این پدیده باید یک مرکزی تعریف شود که تمام تراکنش های کاربران را در آن یادداشت می کند و در آن مشخص می شود که هر کاربر چه تراکنشی انجام داده است که در ادامه به مفهوم Ledger می پردازیم. مهم ترین پیچیدگی این پول ها در مصرف همزمان آنها می باشد.

۲.۳ ساختار پول

۱.۲.۳ پول ها و ارزهای Fiat

منشا اصلی تمام پول های امروزی که در حال استفاده از آنها هستیم دولت، بانک مرکزی و یا دیگر سازمان های معتبری در دولت (سطح کشوری و یا سطح جهانی مانند دلار) هستند که در واقع اصل بودن ارزش آنها را ثابت می کنند. با این وجود به دلیل تمرکز آنها به یک نهاد یا سازمان در عمل قابل کنترل و پیگیری هستند. تمام پول ها (شامل طلا و غیره) حاوی تاریخچه ای از تبادلات و دادوستدها هستند. برای مثال اگر امروز شما ۱۰۰ دلار بدست آورید کاملاً توسط دولت قابل پیگیری است که این ۱۰۰ دلار در بانک به نام شما ثبت شده است.

۲.۲.۳ پول ها و ارزهای دیجیتال

در پول های دیجیتال مهم ترین ایده رمز ارز بودن آن است که توسط الگوریتم های رمزنگاری تولید شده است. حاوی تاریخچه است که تمام تبادلات آن موجود می باشد. هش کردن و امضای دیجیتال از رویکردهای اولیه ساخت این پول می باشد.

۳.۲.۳ مشکلات

مهم ترین چالش رمز ارزهای اولیه و پول های سنتی وجود سیستم های متمرکز و مشکل Double spending می باشد.

۳.۳ راهکار Ledger

دیتابیس از سوابق تبادل و انتقالات تراکنش ها می باشد که مشخص می کند هر کاربر چه تراکنشی را به چه سمتی انتقال داده است. در این دیتابیس تمام موارد Double spend مورد بررسی قرار می گیرد که یک کاربر نتواند از یک تراکنش دوبار عمل انتقال را انجام دهد. در

حقیقت راهکاری برای جلوگیری از کلون و کپی گرفتن از انتقال تراکنش‌ها می‌باشد.

۴ نظریه ارزش

کمیاب بودن یک چیز باعث ارزشمند شدن آن می‌شود. اگر طلا ارزشمند است چون منابع طلا همه جا نیست.

۵ خاصیت‌های هش مرسوم

یک هش مرسوم سه ویژگی دارد:

۱. ورودی آزاد

۲. طول مشخص خروجی تابع

۳. در یک زمان معقول قابل پردازش باشد $O(n)$

۶ خاصیت‌های هش رمزارها

۱. تصادم پذیر نباشد^۱

(آ) هیچ فردی نتواند تصادم را پیدا کند

۲. مخفی باشد^۲

(آ) رمزنگاری یک طرفه می‌باشد که از خروجی هیچ وقت نمی‌توان به ورودی رسید

۳. قابل جست و جوی فراگیر نباشد^۳

(آ) سرعت آن بهینه باشد ولی به قدری سریع نباشد که بتوان از طریق تکنیک‌های Bruteforce خیلی راحت به جواب رسید.

۷ امضاها

بر اساس کلیدهای خصوصی-عمومی کار می‌کند. دو قفل وجود دارد که کاربر می‌تواند پیام اصلی خود را با استفاده از قفل خصوصی آن را رمزنگاری کند و به یک امضا برسد و در نهایت با استفاده از کلید عمومی و با شرایطی خاص به پیام اصلی برسد. هر پیامی می‌تواند با کلید خصوصی منجر به تولید یک امضا شود. هر کسی می‌تواند به کلید عمومی کاربری دسترسی داشته باشد. اما تا زمانی که صاحب کلید نباشد نمی‌تواند به اصل پیام برسد. به عبارتی دیگر اگر کاربری بخواهد با استفاده از کلید عمومی، پیام اصلی و امضای تولید شده یک کاربر دیگر به کلید خصوصی برسد با استفاده از تابعی امکان پذیر می‌باشد.

الگوریتم‌های تولید کلید

۱. PGP

۲. GPG: بر گرفته از بنیاد GNU می‌باشد.

^۱ Collision resistance

^۲ Hiding

^۳ Puzzle friendliness

۳. ECDSA: ساخته شده توسط دولت آمریکا می‌باشد که بر اساس فرمول ریاضی کار می‌کند. ۴

نکات

- داده‌ها در بلاک چین به صورت هش تبادلی می‌شوند
- در بلاک چین نیازی به داشتن امضای دیجیتال نیست
- در رمزارزها نیازمند به امضاها یا دیجیتال هستیم

۱.۷ خصوصیات کلید عمومی

۱. کلید خصوصی شناسه اصلی کاربر می‌باشد:

(آ) نیازی به نام کاربری نیست

(ب) نیازی در مراجعه به تولید کننده کلید نیست

(ج) یک کاربر می‌تواند تعداد زیادی کلید عمومی تولید کند که مربوط به خودش باشد اما کاربران دیگران نمی‌توانند از طریق این کلیدهای عمومی به شخص مورد نظر برسند.

۸ بلاک چین چیست؟

در ابتدا باید مفهوم بلاک را بتوانیم درک کنیم. هر بلاک ساختمان داده‌ای است که محتوای آن شامل بخش‌های زیر می‌باشد:

- تراکنش‌ها (TRX)
- زمان اتفاق تراکنش‌ها (Timestamp)
- و سپس هش آن محاسبه شود

به مجموعه‌ای از این بلاک‌ها که اطلاعات آنها به یکدیگر متصل و مرتبط می‌باشد بلاک چین یا زنجیره‌ای از بلاک‌هایی که ساختار آنها را درک کردیم می‌گویند. یک شکلی از دیتابیس توزیع شده است که ارزهای دیجیتال مانند بیت‌کوین بر اساس آن طراحی شده است. بلاک چین بدون بیت‌کوین وجود دارد و می‌توان از طریق آن داده‌های مختلفی را انتقال داد. داده‌ها در قالب بلاک‌ها نگهداری می‌شوند. یک شبکه توزیع شده و هیچ بدون هیچ مرکزیت داده‌ای.

نمونه‌ای از ساختار یک بلاک انتقال داده در شبکه توزیع شده بلاک چین:

```
۱ {
۲   "hash": "0x453bb640641fe0c2555d07746efdf200993103ed07007f3236d855c66c358745",
۳   "blockHash": "0x2acb514f608fe7ace34e22103c3109d81bec1b78e74ae089cf8902b9bc30836",
۴   "blockNumber": "19033018",
۵   "to": "0xe507c2e03593350135b79a4efba464f27912ba39",
۶   "from": "0xa9389f90a1a044a8e5a492447b5a5bb8f023e167",
۷   "value": "9600000000000000",
۸   "nonce": "143",
۹   "gasPrice": "32533243150",
۱۰  "gasLimit": "25397",
۱۱  "gasUsed": "21164",
۱۲  "data": "1020240118100046276945",
۱۳  "transactionIndex": "144",
۱۴  "success": true,
```

```

۱۵ "state": "CONFIRMED",
۱۶ "timestamp": "1705572059",
۱۷ "internalTransactions": []
۱۸ }

```

از آنجایی که هر کدام از بلاک‌ها، هش بلاک قبلی را دارا می‌باشند، بلاکی که در روز اول به عنوان اولین بلاک داده معرفی شده است را با نام Genesis Block می‌شناسند.

۹ مسئله اجماع

بزرگ‌ترین چالش در سیستم‌های توزیع شده مسئله اجماع می‌باشد مخصوصاً در شرایطی که برخی از اجزا ممکن است عملکرد نامناسبی داشته باشند و از کار بیفتند و یا غیر قابل اعتماد باشند. به همین خاطر در مورد اجماع در سیستم‌های توزیع شده تئوری ژنرال‌های بیزانس مطرح می‌شود. در حالی که ژنرال‌ها در انتظار دریافت پیام از پیام‌آوران در ناحیه‌های مختلفی (کاملاً به صورت توزیع شده در شهرهای مختلف) هستند ممکن است به دلایل مختلفی پیام حمله برای هر ژنرالی با مشکلی مواجه شود. ممکن است یکی از پیام‌آوران در هنگام آمدن به سمت ژنرال شهر (آ) از گشنگی بمیرد و یکی دیگر از پیام‌آوران حمله به ژنرال شهر (ب) به اسارت گرفته شود و نتواند پیام حمله را به سمت ژنرال آن شهر ببرد در همین حال سه پیام‌آور دیگر به شهرهای مقصد به سلامتی می‌رسند و پیام را به ژنرال‌ها انتقال می‌دهند اما چون خبری از اقدامات بقیه ژنرال‌ها در شهرهای مختلف ندارند، فرض را بر این می‌گذارند که ژنرال‌های شهرهای دیگر پیام حمله را دریافت کردند. به همین خاطر به دلیل آن که هیچ ژنرالی با ژنرال‌های دیگر به اجماع نرسیدند احتمال موفقیت آن‌ها به شدت کم خواهد بود و ممکن است شکست خورند.

در دیتابیس‌های بلاک چین نیز همین مسئله وجود دارد. برای رسیدن به اجماع در عمل یکسری شرایط وجود دارد:

- برای سیستم‌ها و افرادی که در دیتابیس‌های بلاک چین عملکرد خوبی دارند مشوقی^۵ در نظر گرفته شود که آنها به خوب بودن خودشان ادامه دهند.
- انتخاب افراد خوب به صورت کاملاً تصادفی می‌باشد

اما در این بین باید فراموش نکرد که برای رسیدن به این اجماع می‌تواند سختی‌هایی هم وجود داشته باشد:

- تا آنجایی که می‌شود از حمله‌های Sybil جلوگیری شود. چرا که ممکن است هر کامپیوتر در شبکه توزیع شده بلاک چین از خود چندین کپی گیرد و چون تعداد سیستم‌های زیاد است احتمال دریافت تشویقش زیادتر نسبت به بقیه سیستم‌های حاضر در شبکه می‌شود
- انتخاب‌ها نباید همینطوری به صورت تصادفی باشد زیرا هر گره در این شبکه لزومی ندارد یک سیستم عادل و شایسته‌ای برای دریافت تشویق باشد.

پاداش هر سیستمی که بتواند بلاکی را پیدا کند یک مقدار مشخصی از بیت‌کوین می‌باشد.

۱۰ اجماع ضمنی

لزومی ندارد که تمام سیستم‌ها طبق یک فرمول دقیق یک Ledger وجود داشته باشد بلکه به صورت ضمنی امروزه این اجماع دیده می‌شود.

۱۰.۱ مسئله Mempool

تمام نودهای شبکه بلاک چین تراکنش‌هایی که در حال انجام است را به یکدیگر اعلام می‌کنند. این عمل باعث بررسی درستی انجام تراکنش‌ها می‌شود. ممکن است یکی از نودها به صورت تصادفی در یک زمان تصادفی تراکنش‌هایی که در حافظه خود است را داخل یک بلاک بگذارد، آن را رمزنگاری (هش) کند و سپس به نودهای دیگر در شبکه بلاک چین اعلام کند که تراکنش‌های جدید در شبکه وارد شده است. در رمزارز بیت‌کوین برای سیستمی که عمل Mempool را نسبت به سیستم‌های دیگر انجام داده است، پاداشی در نظر گرفته می‌شود.

^۵Incentive

نکته

شناخت Mempool همانند مفهوم Ledger می باشد اما در Ledger داده ها سعی می شد که به صورت تمرکز نگهداری شود و روش سنتی انتقال تراکنش ها بود اما در Mempool این مفهوم پیشرفت کرده و در ابعاد نامتمرکز بودن در شبکه بلاک چین به آن نگاه می شود.

عملیاتی که در اجماع ضمنی رخ می دهد

۱. تمام نودها تراکنش های جدید را به یکدیگر اعلام می کنند
۲. هر نودی تراکنش های جدید خود را در یک بلاک جمع آوری می کند
۳. در هر بازه زمانی یکی از نودها که به صورت تصادفی انتخاب می شود بلاک جمع آوری تراکنش خود را به بقیه نودها اعلام می کند
۴. بقیه نودها زمانی بلاک منتخب را قبول می کنند که تراکنش های داخل آن معتبر باشد (منظور از آنکه Double spend رخ نداده باشد)
۵. نودها توافق خود را با اضافه کردن بلاک منتخب به آخرین بلاک خود، نشان می دهند.

۱۱ مفهوم Proof of Work (POW)

راهکاری برای جلوگیری از حملات Sybil می باشد. معیاری برای اثبات تلاش نودها برای پیدا کردن یک Mempool. یک مکانیزم مربوط به اجماع است که نیازمند تعداد قابل توجهی از تلاش های محاسباتی از شبکه ای از دستگاه ها می باشد.

۱.۱۱ مفهوم Nonce

معیاری برای نشان دادن میزان زحمت یک نود می باشد. هر هش دنباله ای از اعداد است که به آن number used once یا nonce گفته می شود. مقدار nonce بعد از ایجاد یک هش برابر با صفر می باشد.

۲.۱۱ مفهوم Difficulty

سطحی برای سنجش میزان نزدیکی مقدار Nonce و سختی شبکه است. در حقیقت یک نتیجه ریاضی از فرمولی است که به یک عدد هگزادسیمال تبدیل شده است که سطح دشواری استخراج را تعیین می کند. اگر هش از مقدار Difficulty کوچک تر بود، برنامه ماینینگ مقدار عدد ۱ را به nonce اضافه می کند و دوباره یک هش می سازد.

۳.۱۱ TRX Fee

بعد از تشکیل Mempool، انتقال پول به خود را در آن یادداشت می شود مقدار Halving در آن قرار می گیرد و سپس تصمیم به جست و جوی سطح Difficulty نسبت با Nonce می گیرد.

۴.۱۱ مفهوم Halving

بعد از گذشت ۴ سال یا ایجاد ۲۱۰۱۴۰ بلاک ارزش رمزارز نصف می شود. این عمل را Halving می گویند.

نکته

برای جلوگیری از همزمانی تعداد برابر ماین های انجام شده بیشتر به طول ذنجیره دقت می شود که به آن کلاستر بتواند پاداش دهد.