مفاهیم اولیه بلاک چین

علیرضا سلطانی نشان

۵ بهمن ۱۴۰۲

فهرست مطالب

۱ مجوز

۲ مقدمه

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

۳ تاریخچه

۱.۳ مشکل Double spending

یکی از چالش‌های پول دیجیتال در دیدگاه اول، قابلیت کپی گرفتن و دوبار خرج کردن یک پول می‌باشد. یک کاربر نباید قادر به خرج مجدد یک پول باشد. پول‌های کاغذی را نمی‌توان به راحتی کپی کرد چرا که دشوار هستند و توسط یک نهاد یا بانک مرکزی اصطلاحاً تایید شده نمی‌باشد. اما در پول‌های 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 تراکنش‌های کاربران را در آن یادداشت می‌کند و در آن مشخص می‌شود که هر کاربر چه تراکنشی انجام داده است که در ادامه به مفهوم Ledger می‌پردازیم. مهم‌ترین پیچیدگی این پول‌ها در مصرف همزمان آنها می‌باشد.

۲.۳ ساختار پول

۱.۲.۳ پول‌ها و ارزهای Fiat

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

۲.۲.۳ پول‌ها و ارزهای دیجیتال

در پول‌های دیجیتال مهم‌ترین ایده رمز ارز بودن آن است که توسط الگوریتم‌های رمزنگاری تولید شده است. حاوی تاریخچه است که تمام تبادلات آن موجود می‌باشد. هش کردن و امضای دیجیتال از رویکردهای اولیه ساخت این پول می‌باشد.

۳.۲.۳ مشکلات

مهم‌ترین چالش رمز ارزهای اولیه و پول‌های سنتی وجود سیستم‌های متمرکز و مشکل Double spending می‌باشد.

۳.۳ راهکار Ledger

دیتابیسی از سوابق تبادل و انتقالات تراکنش‌ها می‌باشد که مشخص می‌کند هر کاربر چه تراکنشی را به چه سمتی انتقال داده است. در این دیتابیس تمام موارد Double spend مورد بررسی قرار می‌گیرد 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 رمزارزها

۱. تصادم پذیر نباشد [۱]

(آ) هیچ فردی نتواند تصادم را پیدا کند

[۱] Collision resistance

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.

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

نکات

- داده‌ها در بلاک چین به صورت هش تبادل می‌شوند
- در بلاک چین نیازی به داشتن امضای دیجیتال نیست
- در رمزارزها نیازمند به امضاهای دیجتال 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 نسیت

(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.

[۲] Hiding
[۳] Puzzle friendliness
[۴] Elliptic Curve Digital Signature Algorithm

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:

```
{
    "hash": "0x453bb640641fe0c2555d07746efdf200993103ed07007f3236d855c66c358745",
    "blockHash": "0x2acb514f608fe7ace34e22103c3109d81bebc1b78e74ae089cf8902b9bc30836",
    "blockNumber": "19033018",
    "to": "0xe507c2e03593350135b79a4efba464f27912ba39",
    "from": "0xa9389f90a1a044a8e5a492447b5a5bb8f023e167",
    "value": "9600000000000000",
    "nonce": "143",
    "gasPrice": "32533243150",
    "gasLimit": "25397",
    "gasUsed": "21164",
    "data": "0x1020240118100046276945",
    "transactionIndex": "144",
    "success": true,
    "state": "CONFIRMED",
    "timestamp": "1705572059",
    "internalTransactions": []
}
```

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 مخصوصا 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 پیام آوران در ناحیه‌های مختلفی (کاملا 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 آن ها 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 کاملا 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 سیستم‌هایش 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.

۱.۱۰ 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.

نکته

شناخت Mempool همانند مفهوم Ledger می‌باشد اما در Ledger داده‌ها سعی می‌شد که به صورت تمرکز نگهداری شود و روش سنتی انتقال تراکنش‌ها بود اما در Mempool این مفهوم پیشرفت کرده و در ابعاد نامتمرکز بودن در شبکه بلاک چین به آن نگاه می‌شود.

عملیاتی که در اجماع ضمنی رخ می‌دهد

۱. تمام نودها تراکنش‌های جدید را به یکدیگر اعلام می‌کنند

۲. هر نودی تراکنش‌های جدید خود را در یک بلاک جمع‌آوری می‌کند

۳. در هر بازه زمانی یکی از نودها که به صورت تصادفی انتخاب می‌شود بلاک جمع‌آوری تراکنش خود را به بقیه نودها اعلام می‌کند

۴. بقیه نودها زمانی بلاک منتخب را قبول می‌کنند که تراکنش‌های 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 می‌دهند.

[۵] Incentive

۱۱ حمله ۵۱ درصد

حمله ٪۵۱ معمولا در شبکه‌های بلاک چین به ویژه در رمزارز بیت کوین استفاده می‌شود. در این حمله اگر گورهی از شرکت کنندگان شبکه بلاک چین حداقل ٪۵۱ از قدرت محاسباتی شبکه را در اختیار داشته باشند (برای مثال یک شخصی چند کامپیوتر را تهیه می‌کند که از قدرت محاسباتی بالایی برخوردار هستند و آنها در شبکه بلاک چین ثبت می‌کند که شانس بدست آوردن پاداش خود را افزایش دهد.). آنها می‌توانند کنترل تراکنش‌ها به طور تقریبی به دست گیرند. این حمله ممکن است توسط افراد یا گروه‌هایی که فصد خراب کردن یا تغییر شبکه را داشته باشند، استفاده می‌شود. برای از بین بردن حمله ٪۵۱ از رویکردهایی که در ادامه توضیح داده خواهد شد استفاده شده است.

۱۲ مفهوم Proof of Work (POW)

راهکاری برای جلوگیری از حملات Sybil می‌باشد. معیاری برای اثبات تلاش نودها برای پیدا کردن یک Mempool. یک مکانیزم مربوط به اجماع است که نیازمند تعداد قابل توجهی از تلاش‌های محاسباتی از شبکه‌ای از دستگاه‌ها می‌باشد.

۱۳ مفهوم Proof of Stake (PoS)

به بیانی ساده، هر چقدر تعداد سکه‌هایی که یک کاربر در اختیار دارد بیشتر باشد، فرصت بیشتری را برای انتخاب جهت تولید بلاک و دریافت پاداش خواهد داشت. این روش به صورت قابل توجهی انرژی کمتری نسبت به الگوریتم PoW مصرف می‌کند در حالی که در بیت کوین استفاده می‌شود و همچنین احتمال وقوع حمله ٪۵۱ را نیز کاهش می‌دهد.

۱.۱۳ مفهوم Nonce

معیاری برای نشان دادن میزان زحمت یک نود می‌باشد. هر هش دنباله‌ای از اعداد است که به آن number used once یا nonce گفته می‌شود. مقدار nonce بعد از ایجاد یک هش برابر با **صفر** می‌باشد.

۲.۱۳ 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 می‌کند. اگر هش از مقدار Difficulty کوچک‌تر بود، برنامه ماینینگ مقدار عدد ۱ را به nonce اضافه می‌کند و دوباره یک هش می‌سازد.

۳.۱۳ TRX Fee

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

۴.۱۳ مفهوم Halving

بعد از گذشت ۴ سال یا ایجاد ۲۱۰۱۴۰ بلاک ارزش رمزارز نصف می‌شود. این عمل را Halving می‌گویند. ماین کردن عملا نگهداشتن شبکه بلاک چین می‌باشد که جلوگیری از حمله ۵۱ درصد می‌کند. به همین خاطر مقدار رمزارز نصف می‌شود تا بقیه را از تمایل به ماین کردن منصرف کند.

۵.۱۳ مفهوم Gas Fee

این مفهوم با بیان یک مثال ساده قابل درک خواهد بود. اگر کاربری بخواهد یک تراکنش از کیف پول خود به کیف پول دوست خود انجام دهد یا یک قرارداد هوشمند را اجرا کند، کاربر باید هزینه Gas Fee را برای پرداخت به ماینرها (دقیقاً کسانی که تراکنش‌ها را تایید می‌کنند) در نظر گیرد. این هزینه ممکن است بر اساس پیچیدگی تراکنش یا عملیات، حجم تراکنش و و نیازمندی‌های شبکه تغییر کند.

نکته

برای جلوگیری از همزمانی تعداد برابر ماین‌های انجام شده بیشتر به طول زنجیره دقت می‌شود که به آن کلاستر بتواند پاداش دهد.

انواع ماشین‌های ماینینگ

۱. CPU

۲. GPU

۳. FPGA

۴. ASIC

۶.۱۳ حمله Withholding

بعد از پیدا کردن بلاک، اعلام Mempool انجام نمی‌شود (حداقل تا یک دقیقه) تا بتواند حداقل یک بلاک دیگر در طی این زمان بسازد و سپس بعد از آن اعلام پیدا کردن بلاک را انجام دهد.

۷.۱۳ حمله Punitive Forking

اگر در بلاکی که ماین شده یک شناسه فیلتر شده باشد آن را قبول نمی‌کند و ادامه ماین کردن در فورک دیگر ادامه داده می‌شود.

۱۴ مسئله Anonymity

اصطلاحاً به آن ناشناسی و یا بدون اسم بودن می‌گویند. ناشناسی و شبه ناشناس با یکدیگر متفاوت است. در سمت ارسال کننده می‌تواند آدرس Public key هر بار تغییر کند و در قسمت دریافت کننده کاملا مشخص است که چه کسی با چه کلیدی تراکنش را انجام داده است. از نظر سنتی بخواهیم مسئله ناشناس بودن بیت‌کوین را با ارزهای فیات و کارت‌های امروز مقایسه کنیم، حتی متوجه خواهیم شد که به شکلی واضحی تراکنش‌ها در بیت‌کوین (کلا در شبکه بلاک چین) کاملا قابل ردیابی هستند که مشخص کننده آن است، تراکنشی که الان شخص (آ) به شخص (ب) داده است شخص (ب) آن را بعد از دریافت به چه شخص دیگری پرداخت کرده است. از مهم‌ترین ابزارهای ناشناسی مانند سیستم TOR می‌باشد. TOR برای اولین بار توسط نیرو دریایی آمریکا توسعه داده شد و از آنجایی که قصد در ناشناس بودن خود داشتند این پروژه را آزاد اعلام کردند که امروزه از آن به منظور اهداف مختلف در سیستم‌های مختلف استفاده می‌شود.

چه اتفاقاتی رخ می‌دهد که ناشناس بودن از بین می‌رود؟

۱۵ مسئله Deanonymyzation

نیازمند پرسش است.

۱۶ اسکریپت نویسی داخل بیت‌کوین

۱.۱۶ مسئله Proof of Burn

اسکریپتی است که هیچ وقت اجازه نمی‌دهد که تراکنش بازگشت داشته باشد، می‌توانیم مطمئن از مصرف شدن کامل تراکنش مورد نظر باشیم که باعث از بین رفتن رخداد Double spending می‌شود.

۲.۱۶ مفهوم MULTISIG

فرایند بررسی امضای صاحب رمزارز می‌باشد بطوری که قابل برنامه ریزی هستند. برای مثال مشخص می‌کنیم که این رمزارز زمانی می‌تواند پذیرفته شود که از ۳ امضا ۲ امضا درست را داشته باشد.

۳.۱۶ مفهوم Green addresses

ساخت آدرسی که مشخص می‌کند تراکش‌ها باید از چه کانالی انجام شوند. برای مثال زمانی که یک نود آفلاین است ممکن است این ایده و رویکرد استفاده شود.