قفل زمانی بیت کوین (Timelock) چیست؟

قفل زمانی (Timelock) یکی از کاربردی ترین قابلیت های بیت کوین است که به شما امکان می دهد تا اقدامات را طبق یک سری پارامترها برنامه ریزی کرده و در نتیجه، بیت کوین را بهتر و کاربردی تر از پول و به عنوان یک پول دیجیتال قابل برنامه ریزی استفاده کنید. در حقیقت قفل زمانی بیت کوین اجازه می دهد تا یک تراکنش بیت کوین به شکلی ایجاد شود که گیرنده خروجی ها نتواند آن ها را برای مدت زمان مشخصی خرج کند. مقدار زمان را می توان با معیارهای مختلفی تعیین کرد. قفل زمانی بیت کوین در قسمت اختصاصی هر تراکنش مشخص شده است. با این حال، اکثر تراکنش ها به سادگی قفل زمانی را خالی می گذارند تا از بکارگیری این قابلیت اجتناب شود. قفل های زمانی برای ایجاد قراردادهای قفل زمانی رمزگذاری شده (HTLC – Hashed Timelock Contract)، که شبکه لایتنینگ را هدایت می کنند، مفید می باشند. اگر سوالاتی در ارتباط با اندیکاتور پیشرو و انواع آن دارید، ما را تا انتهای این مطلب از بلاگ کیف پول من همراهی کنید.

ویژگی های قفل زمانی

هر تراکنش بیت کوین از زمان انتشار اولیه بیت کوین، حاوی حداقل یک فیلد زمان قفل است که در حالت پیش فرض خود [00) 00000000x) یا FFFFFFFF0x (4294967295)] وجود دارد. با این حال، آن ها عمدتاً تا چند رویداد مربوط به بهبود بیت کوین (BIP) بلااستفاده مانده بودند.
تراکنش های بیت کوین که از قفل های زمانی استفاده می کنند، دارای سه ویژگی هستند: مکان، هدف یا جهت و اطلاعات بلوک.

قفل زمانی براساس مکان

قفل های زمانی می توانند بر اساس **مکان** باشند، یعنی قفل زمانی در سطح تراکنش یا سطح اسکریپت صورت پذیرد. اگرچه هر دو این موارد به عنوان محدودیت شمرده می شوند، اما اهداف متفاوتی را دنبال می کنند. به طوری که قفل زمانی در سطح تراکنش تضمین می کند که تراکنش تا زمان مشخصی به اعتبارسنجی ادامه نمی دهد، حتی اگر امضای دیجیتال آن درست باشد. از سوی دیگر، قفل زمانی در سطح اسکریپت تضمین می کند که ارزیابی اسکریپت امضاهای دیجیتال تا زمانی که تراکنش قفل نشود، نامعتبر می ماند. به طور خلاصه، تفاوت اصلی بین این دو آیتم این است که قفل های زمانی در سطح تراکنش تعیین می کنند که یک تراکنش چه زمانی می تواند اجرا شود، در حالی که یک قفل زمانی در سطح اسکریپت تعیین می کند که چه تراکنش هایی می توانند به طور کلی در شبکه انجام شوند.

قفل زمانی براساس هدف یا جهت

براساس این ویژگی، قفل های زمانی یا به صورت **مطلق** هستند و یا به شکل **نسبی**. برای توضیح ساده این موضوع، می توان این گونه گفت که هر دو قفل مبتنی بر زمان، نسبت به زمان خاصی هستند. آن ها به سادگی از این نظر متفاوت هستند که زمان قفل مطلق نیاز به تایم مشخصی داشته و تراکنش تا هنگامی که زمان مشخص شده (مثلاً 13:00) سپری نشود، نامعتبر است. از طرف دیگر، قفل های زمان نسبی نیاز به شمارش معکوس برای اولین زمانی دارند که ماینرها می توانند تراکنش را تأیید کنند (یعنی اگر تراکنش به مدت 12 ساعت قفل شود، شمارش معکوس برای آن بازه زمانی شروع می شود و تراکنش تنها پس از تکمیل شمارش معکوس معتبر است).

قفل زمانی براساس اطلاعات بلوک

دو معیار در شبکه بیت کوین وجود دارد: شماره بلوک و زمان ایجاد بلوک. این بدان معناست که قفل های زمانی می توانند با تعیین یک شماره بلوک خاص وجود داشته باشند که قبل از آن تراکنش نامعتبر باقی بماند یا با یک تگ زمانی خاص که تراکنش برای آن معتبر می شود ثبت شوند.

انواع قفل زمانی بیت کوین (در سطح تراکنش و اسکریپت)

بیت کوین در حال حاضر 4 راه برای ایجاد قفل زمانی ارائه می کند. دو مورد از این ابزارها در سطح تراکنش و دو مورد دیگر در سطح اسکریپت هستند. در این قسمت هر یک از این موارد را بررسی کرده ایم:

1. قفل زمانی مطلق در سطح تراکنش (nLockTime)

این تنها قفل زمانی است که در نسخه اصلی نرم افزار بیت کوین موجود بود. nLockTime برابر یا بزرگتر از ارتفاع بلوک فعلی است. بنابراین تراکنش ها تا زمانی که به بلوک تعیین شده نرسیدند اعتبارسنجی نشدند. در این قفل ها، زمان به صورت اعداد صحیح 32 بیتی و به صورت بدون علامت بیان می شود. اگر عدد کمتر از 500 میلیون باشد، به عنوان ارتفاع بلوک تعبیر می شود. برعکس، اگر بیشتر از 500 میلیون باشد، به عنوان علامت زمان یونیکس در نظر گرفته می شود.

در نسخه 0.1.6 بیت کوین، تعبیر nLockTime تنظیم شد تا قفل مبتنی بر زمان را نیز مجاز کند . سپس، با شروع بلوک 31001، محدودیت های nLockTime به عنوان قاعده ای فعال شدند که برای پذیرش بلوک نیز اعمال می شد. بعدها و در ژوئیه 2016، قفل های مبتنی بر زمان تغییر کردند تا به جای مهر زمانی بلوک، بر روی میانگین زمان گذشته کار کنند. یک nLockTime می تواند یک تراکنش را تا 9.500 سال با استفاده از اعداد بلوک و 2.106 سال با استفاده از مهرهای زمانی مسدود کند. همچنین اگرچه هر تراکنش در حال حاضر حاوی تابع nLockTime است، اما اکثر کیف پول ها آن را از پیش روی 0 تنظیم کرده اند. این بدان معناست که تراکنش ها را می توان در هر بلوکی از زنجیره تأیید کرد.

2. قفل زمان نسبی در سطح تراکنش (nSequence)

در این قفل زمانی، از اعداد ترتیبی برای ایجاد قفل های زمانی نسبی در سطح تراکنش استفاده می شود. این امر به یک ورودی اجازه می دهد تا اولین زمانی را که می تواند به یک بلوک اضافه شود مشخص نماید. هنگام استفاده از nSequence چندین شرایط زمانی مختلف را می توان در یک تراکنش تنظیم کرد. بنابراین، برای معتبر بودن معامله، باید همه شرایط وجود داشته باشد و اگر این اتفاق رخ ندهد، کل تراکنش رد خواهد شد. بر خلاف nLockTime، قفل زمانی nSequences فقط از 18 بیت از مجموع 32 بیت استفاده می کند، بنابراین 14 بیت برای پیاده سازی های بعدی رزرو می شود و از آن 18 بیت در حال استفاده، 16 بیت برای رمزگذاری زمان قفل شدن در نظر گرفته شده است. بنابراین قفل های nSequence به 65.535 واحد بلوک محدود می شوند.

3. مسدود کردن زمان مطلق در سطح اسکریپت (CLTV: CheckLockTimeVerify)

جزئیات این حالت در سافت فورک BIP 65 و در اواخر سال 2015 توسط پیتر تاد به شبکه معرفی شد. این پیشنهاد امکان انجام معامله ای را فراهم می کند که در آن تاریخ خاصی که در آن لازم الاجرا می شود را می توان مشخص کرد (یعنی تاریخی که گیرنده می تواند از وجوه ارسال شده استفاده کند). یکی از توابع پیشرفته ای که CTLV به آن مجوز می دهد، تغییر پارامتر احراز هویت یک آدرس چند امضایی است. به عنوان مثال، اگر یک آدرس چند امضایی با طرح 2 از 3 ایجاد شده

باشد، CLTV می تواند پارامتر مذکور را تحت معیارهای خاصی به طرح 1 از 3 تغییر دهد. به این ترتیب، فرد می تواند وجوه را تحت شرایط خاص و توافق شده قبلی بازیابی کند.

4. قفل زمان نسبی در سطح اسکریپت (CSV:CheckSquenceVerify)

این قفل زمانی بخشی از سافت فورک BIP 68 بود اما در BIP 112 و در اواسط سال 2016 اضافه شد. CSV زمان مسدودسازی نسبی را فراهم می کند، به همان شکلی که CLTV برای زمان انسداد مطلق یک زمان را فراهم می کند. به همین خاطر این دو قفل زمانی بسیار شبیه به یکدیگر هستند. با این حال، به جای بررسی زمان مانند CLTV، قفل زمانی در سطح اسکریپت استک بالایی را با فیلد ورودی بررسی می کند.

هنگامی که کد CSV فراخوانی می شود، باعث از کار افتادن اسکریپت می شود، مگر اینکه nSequence در تراکنش نشان دهد که مقدار نسبی زمان قفل برابر یا بیشتر از پارامتر ارائه شده به کد CSV گذشته است. این امر تضمین می کند که وقتی قفل زمانی مبتنی بر CSV منقضی شده است، تراکنش می تواند در یک بلوک معتبر گنجانده شود. با این کد عملیات، تراکنش ها می توانند حداکثر برای 65.535 بلوک، که معادل تقریباً 455 روز است، مسدود شوند.

قفل زمانی در سایر ارزهای دیجیتال

Timelock یک ویژگی متمایز پروتکل بیت کوین است که در همه ارزهای دیجیتال وجود ندارد. به عنوان مثال، اتریوم، دومین ارز دیجیتال بزرگ از نظر ارزش بازار، دارای ویژگی قفل زمانی داخلی نیست. با این حال، راه حل های قرارداد هوشمند را می توان برای ایجاد عملکرد مشابه به کار برد. سایر ارزهای دیجیتال، مانند لایت کوین و بیت کوین کش، ویژگی های قفل زمانی مشابهی را در پروتکل های خود گنجانده اند. با این حال، ویژگی های عملکرد این ویژگی ها ممکن است با اجرای بیت کوین متفاوت باشد.

کاربردهای قفل زمانی

قابلیت قفل زمانی (Timelock) را می توان برای اهداف مختلفی استفاده کرد، از جمله:

ایجاد تراکنش چندامضایی

Timelock می تواند برای ایجاد یک تراکنش چند امضایی استفاده شود که چندین طرف را ملزم می کند تا به یک تراکنش قبل از اجرای آن مجوز بدهند. این امر می تواند برای خدمات امانی مفید باشد، حالتی که شخص ثالث وجوهی را تا زمانی که تراکنش نهایی شود، حفظ می کند.

ایجاد حساب پس انداز

از قفل زمانی می توان برای ایجاد یک حساب پس انداز استفاده کرد که در آن وجوه فقط پس از سپری شدن دوره زمانی مشخص قابل دسترسی باشد. این امر می تواند برای اهداف پس انداز بلندمدت یا برای ایجاد صندوق سرمایه گذاری برای یک کودک مفید باشد. به این شکل، این اطمینان وجود دارد که وجوه صندوق پس از گذشت مدت زمانی که خود شخص تعیین کرده قابل برداشت خواهد بود.

ایجاد کانال های پرداخت مستقیم

Timelock می تواند برای ایجاد کانال های پرداخت مورد استفاده قرار گیرد، جایی که دو طرف می توانند بدون نیاز به ارسال هر تراکنش به بلاکچین، وجوه خود را مبادله کنند. این امر می تواند کارمزد تراکنش ها را کاهش داده و سرعت تراکنش را افزایش دهد.

سرمایه گذاری در سایت ها

همان طور که می دانید، در سال های اخیر کلاهبرداری های زیادی در بازار کریپتو رخ داده است. به طوری که بسیاری از سایت ها و پلتفرم ها با تشویق کاربران به سرمایه گذاری و واریز وجوه به حساب هایشان، پس از مدتی ناپدید شده و سایت و پلت فرم خود را به کلی تعطیل می کنند. این افراد شیاد به این شکل مبالغ هنگفتی را از کاربران کلاهبرداری کرده و سطح اعتماد جامعه به بازار کریپتو را کاهش می دهند. قابلیت قفل زمانی برای جلوگیری از پیاده سازی ترفند این افراد کلاهبردار بسیار عالی عمل می کند و قادر است تا نقشه شوم پروژه های کلاهبرداری را به کلی منحل سازد. بدین ترتیب از قابلیت قفل زمانی می توان برای واریز وجوه به حساب پروژه ها و مسدود کردن آن تا زمانی که پروژه به ثمر بنشیند استفاده کرد.

جمع بندی نهایی

ویژگی قفل زمانی بیت کوین یکی از قابلیت های کاربردی است که در بلاکچین بیت کوین و برای کاربران این شبکه تعبیه شده است. براساس این قابلیت، تراکنش ها تا زمانی که برخی معیارهای ایجاد شده عملی نشوند، قابل برداشت نخواهند بود. ما در این مقاله از مجله آموزشی کیف پول من، با بیانی شیوا و صریح به معرفی این قابلیت پرداخته و با بررسی جنبه های گوناگون آن، کاربردهای مهم قفل زمانی را مرور کردیم. امیدواریم این مطلب مورد استفاده شما عزیزان قرار گرفته باشد. شما می توانید دیدگاه ها، انتقادات و سوالات خود را از طریق بخش نظرات به سمع و نظر ما و سایر کاربران برسانید.