کوین ایران

تکنیک‌های امنیت و حریم خصوصی مورد استفاده در بلاک‌چین

فهرست مطالب

تکنیک‌های امنیت و حریم خصوصی مورد استفاده در بلاک‌چین ...۱

روش Mixing ۱

سرویس Mixcoin ۲

سرویس CoinJoin ۲

امضاهای ناشناس ۲

امضای گروهی ۲

امضای حلقه‌ای ۳

رمزگذاری همگن ۴

رمزگذاری مبتنی بر خصیصه ۵

محاسبات چندبخشی امن ۵

اثبات دانش صفر غیرتعاملی ۶

قراردادهای هوشمند مبتنی بر محیط اجرای قابل اعتماد ۷

قراردادهای هوشمند مبتنی بر بازی ۷

منابع ۸

کوین ایران نخستین پایگاه خبری آموزشی فارسی زبان بیت‌کوین، رمز ارز و بلاک‌چین است. این وب‌سایت در سال ۱۳۹۲ توسط بابک جلیلوند و آرش محبوب، با هدف اطلاع‌رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه‌مند به رمز ارزها راه‌اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید. هدف کوین ایران از معرفی این فناوری، ایجاد محیط پویای پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به ایرانیان است.

نویسنده: تورج اکبری

turaj.akbati68@yahoo.com

تکنیک‌های امنیت و حریم خصوصی مورد استفاده در بلاک‌چین

دستیابی به امنیت و حریم خصوصی در سیستم‌های بلاک‌چین پیچیده نیازمند توجه به الزامات امنیت و حریم خصوصی متعددی بر اساس ویژگی‌های منتخب است. در تأمین امنیت و حریم خصوصی بلاک‌چین باید توجه داشت که هیچ فناوری واحدی نمی‌تواند نوش‌داروی امنیت و حریم خصوصی بلاک‌چین باشد. بنابراین بر اساس الزامات امنیت و حریم خصوصی و همچنین زمینه کاربردی مورد نظر باید از تکنیک‌های مناسبی بهره گرفت. در حالت کلی، به کارگیری ترکیبی از چندین فناوری بسیار مؤثرتر از استفاده از یک فناوری واحد است. همچنین فناوری‌ای وجود ندارد که بی‌نقص یا از همه جوانب کامل باشد. معمولاً اضافه کردن فناوری جدید به یک سیستم پیچیده در کنار تمام مزایای آن با چالش‌هایی نیز همراه است. بنابراین اضافه کردن فناوری جدید نیازمند توجه دقیق به مشکلات و مضرات احتمالی آن برای برخی از تکنیک‌های امنیت و حریم خصوصی در بلاک‌چین است. در ضمن، همواره باید تعادلی مابین امنیت-حریم خصوصی و بهره‌وری ایجاد کرد. باید به سمت تکنیک‌هایی حرکت شود که همزمان با بهبود امنیت و حریم خصوصی بلاک‌چین بتوانند استقرار عملی کاربردهای بلاک‌چین با عملکرد قابل قبول را ترویج نمایند. بلاک‌چین از روش‌های متفاوتی برای تأمین امنیت و حریم خصوصی استفاده می‌کند که در ادامه مورد بررسی قرار گرفته‌اند.

روش Mixing

بلاک‌چین بیت کوین نمی‌تواند گمنامی کاربران را تضمین کند. تراکنش‌های بیت کوین از آدرس‌های مستعار استفاده می‌کنند و به صورت عمومی قابل تأیید می‌باشند؛ درنتیجه، هرکسی می‌تواند به راحتی با تحلیل تراکنش‌های انجام شده، ارتباطات میان تراکنش‌های هر کاربر را استخراج نماید. به طور جدی‌تر، هنگامی‌که آدرس تراکنش‌ها با هویت واقعی یک کاربر مرتبط شود ممکن است باعث نشت تمام تراکنش‌های کاربر شود؛ بنابراین، سرویس Mixing یا ترکیب که با نام Tumbler نیز شناخته می‌شود برای جلوگیری از ایجاد ارتباط مابین آدرس‌های مورد استفاده کاربر طراحی شد. در واقع Mixing مکانیسمی برای تبادل تصادفی کوین‌های یک کاربر با دیگر کاربران است. در این روش، ناظر بیرونی نمی‌تواند مالک واقعی کوین‌های مبادله شده در تراکنش‌ها را تشخیص دهد؛ با این حال، امکان سرقت کوین‌ها در سرویس‌های Mixing نیز وجود دارد. در ادامه دو مورد از سرویس‌های Mixing مورد بررسی قرار گرفته و ویژگی‌های امنیت و حریم خصوصی آن‌ها تحلیل می‌شود [۱].

سرویس Mixcoin

Mixcoin امکان پرداخت ناشناس[۱] (گمنام) با بیت‌کوین و دیگر رمز ارزهای مشابه با بیت‌کوین را فراهم می‌نماید. این سرویس در سال ۲۰۱۴ معرفی شد. Mixcoin برای مقابله با مخالفان منفعل[۲]، مجموعه ناشناسی را گسترش می‌دهد تا به همه کاربران اجازه دهد تا کوین‌ها را به صورت همزمان مخلوط کنند. این سرویس برای مقابله با مخالفان فعال از ترکیب مورد استفاده در ارتباطات سنتی بهره می‌برد. علاوه بر این، Mixcoin از مکانیسم پاسخ‌گویی برای تشخیص سرقت استفاده می‌کند [۲].

سرویس CoinJoin

CoinJoin در سال ۲۰۱۳ و به عنوان روش ناشناسی جایگزین برای تراکنش‌های بیت‌کوین معرفی شد. این سرویس با انگیزه پرداخت مشترک شکل گرفت. کاربری را تصور کنید که می‌خواهد پرداختی انجام دهد. او یک کاربر دیگر متقاضی پرداخت را پیدا می‌کند. این دو کاربر از طریق مذاکره[۳] یک پرداخت مشترک انجام می‌دهند. با پرداخت مشترک، احتمال ایجاد ارتباط مابین تراکنش‌های انجام‌شده و رهگیری مسیر دقیق تراکنش‌های مالی به شدت کاهش می‌یابد [۳].

امضاهای ناشناس

فناوری امضای دیجیتال در نسخه‌های متفاوتی توسعه داده شده است. برخی از نسخه‌های امضای دیجیتال می‌توانند ناشناسی امضاکننده را تضمین کنند که به آن‌ها امضای ناشناس نیز گفته می‌شود. روش‌های دیگر مانند امضای گروهی و امضای حلقه‌ای[۴] نیز در کنار طرح امضای ناشناس توسعه یافته‌اند که از روش‌های معمول و مهم امضای ناشناس می‌باشند.

امضای گروهی

امضای گروهی نوعی طرح رمزنگاری‌ست که برای اولین بار در سال ۱۹۹۱ پیشنهاد شد. در این روش هرکدام از اعضای گروه می‌توانند با استفاده از کلید مخفیانه شخصی خود پیامی را به صورت ناشناس برای تمامی اعضای گروه امضا نماید. دیگر اعضای گروه می‌توانند از کلید عمومی گروه برای اعتبارسنجی و تأیید پیام امضا شده توسط هرکدام

---

[۱] Anonymous

[۲] Passive Adversaries

[۳] Negotiation

[۴] Ring Signature

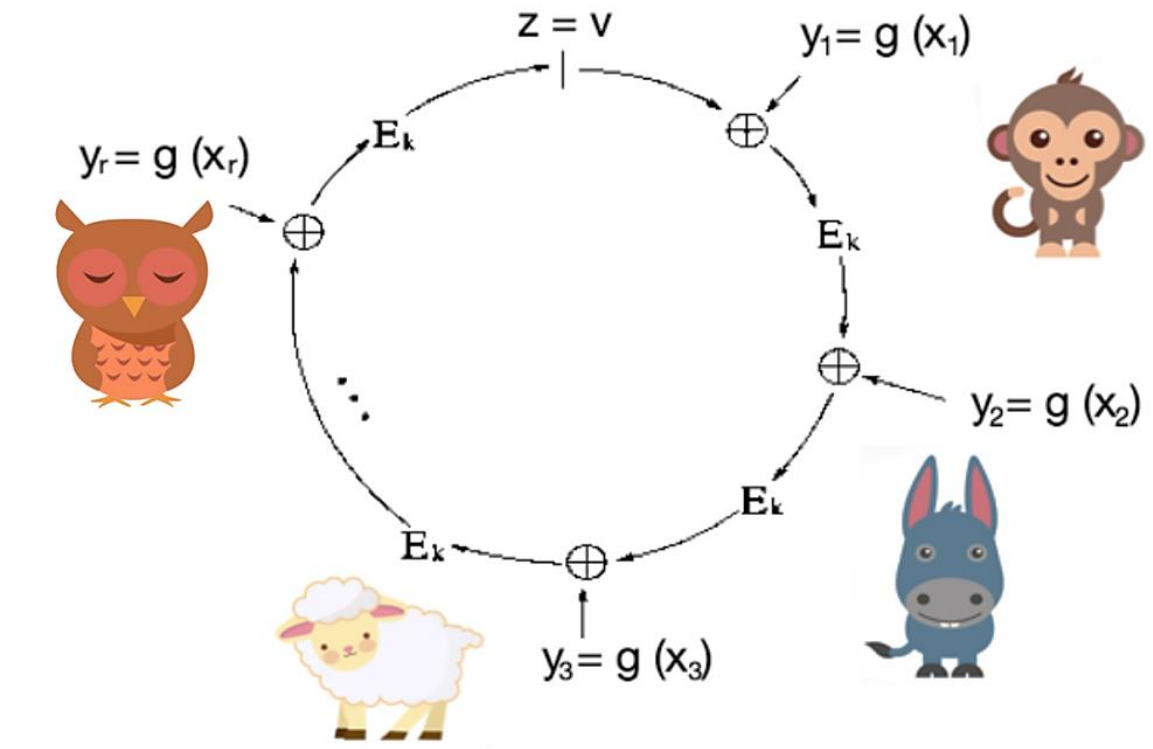
از اعضا استفاده کنند. فرآیند تأیید امضا هیچ گونه اطلاعاتی در مورد هویت امضاکننده آشکار نمی‌کند به‌جز اینکه امضاکننده عضوی از گروه بوده است.

امضای گروهی دارای یک مدیر گروه است که وظیفه اضافه کردن اعضای جدید و رسیدگی به اختلافاتی مانند فاش کردن امضای اصلی را برعهده دارد. در سیستم بلاک‌چین، به موجودیت مرجعی نیاز است تا ایجاد و ابطال گروه، اضافه کردن، حذف/ ابطال پویای عضویت در گروه را انجام دهد. از آنجایی که امضای گروهی نیازمند مدیر گروهی برای ایجاد گروه است این نوع امضا برای بلاک‌چین‌های خصوصی/ کنسرسیومی بسیار مناسب است.

امضای حلقه‌ای

ناشناسی در امضای حلقه‌ای از طریق پنهان کردن هویت امضاکننده حاصل می‌شود. اصطلاح امضای حلقه‌ای از الگوریتم امضایی نشأت می‌گیرد که از ساختاری مانند حلقه استفاده می‌کند. این نوع امضا در صورتی ناشناس است که تشخیص امضاکننده از میان اعضای گروه به سختی امکان‌پذیر باشد.

امضای حلقه‌ای در دو اصل مهم با امضای گروهی متفاوت است. نخست اینکه در طرح امضای حلقه‌ای در صورت بروز اختلاف، هویت واقعی امضاکننده به دلیل نبود مدیر گروه قابل افشا نیست. در ثانی، هر گروه از کاربران می‌توانند بدون نیاز به هرگونه تنظیمات پیچیده بین خود یک حلقه ایجاد کنند. بنابراین می‌توان از امضای حلقه‌ای در بلاک‌چین‌های عمومی نیز استفاده کرد چراکه به راحتی می‌تواند ارتباطات میان آدرس‌های فرستنده‌ی تراکنش را پنهان نماید.



Bettercrypto.com

رمزگذاری همگن

رمزگذاری همگن[۱] (HE) یک روش رمزنگاری قدرتمند است. این روش می‌تواند انواع مشخصی از محاسبات را به صورت مستقیم بر روی متن رمزنگاری[۲] انجام دهد. رمزگذاری همگن تضمین می‌کند که عملیات انجام شده بر روی داده‌های رمزگذاری شده در هنگام رمزگشایی نتایج محاسباتی، نتایج یکسانی با عملیات انجام شده بر روی متن ساده ایجاد خواهد کرد. در کنار سیستم‌های همگن کامل، سیستم‌های مربوط به رمزگذاری همگن جزئی[۳] نیز توسعه داده شده‌اند.

تکنیک‌های رمزگذاری همگن می‌توانند برای ذخیره‌سازی داده بر روی بلاک‌چین‌هایی مورد استفاده قرار گیرند بدون اینکه تغییرات قابل توجهی در ویژگی‌های بلاک‌چین ایجاد کنند. این روش تضمین می‌کند که داده‌های موجود بر روی بلاک‌چین رمزگذاری خواهند شد. رمزگذاری همگن می‌تواند نگرانی‌های مربوط به حریم خصوصی در بلاک‌چین‌ها را مرتفع نماید. این روش رمزنگاری علاوه بر محافظت از حریم خصوصی، امکان دسترسی به داده‌های

---

[۱] Homomorphic Encryption (HE)

[۲] Ciphertext

[۳] Partially Homomorphic

رمزنگاری شده برای ممیزی و اهداف دیگری مانند مدیریت هزینه کارمندان را نیز فراهم می‌نماید. قراردادهای هوشمند اتریوم از روش رمزگذاری همگن داده‌های ذخیره شده در بلاک‌چین به منظور محافظت از حریم خصوصی و کنترل بیشتر استفاده می‌کنند.

رمزگذاری مبتنی بر خصیصه

رمزگذاری مبتنی بر خصیصه[۱] (ABE) یک روش رمزنگاری است که برای اولین بار در سال ۲۰۰۵ معرفی شد. خصیصه‌ها در این روش به عنوان فاکتورهای تعریف‌کننده و تنظیم‌کننده متن رمزگذاری شده توسط کلید خصوصی کاربر مورد استفاده قرار می‌گیرند. تنها در صورتی می‌توان داده‌های رمزگذاری شده را با استفاده از کلید محرمانه کاربران رمزگشایی کرد که خصیصه‌های کاربر مطابق با خصیصه‌های متن رمزگذاری شده باشند. مقاومت در برابر تبانی[۲] یکی از ویژگی‌های امنیتی مهم روش رمزگذاری مبتنی بر خصیصه می‌باشد. این ویژگی تضمین می‌کند زمانی که یک کاربر خرابکار با دیگر کاربران تبانی کند به جز داده‌هایی که با کلید خصوصی خود می‌تواند آن‌ها را رمزگشایی کند به داده‌های دیگران دسترسی نداشته باشد.

نسخه‌های اولیه رمزگذاری مبتنی بر خصیصه با محوریت یک مرجع واحد[۳] توسعه داده شده بودند. پس از آن تغییراتی در مفاهیم پایه اولیه آن ایجاد شد که تعریف چندین مرجع برای تولید مشترک کلیدهای خصوصی کاربران و طرح‌های[۴] رمزگذاری مبتنی بر خصیصه برای پوشش گزاره‌های دلخواه را شامل می‌شد. مراجع مورد استفاده می‌توانند در یک شبکه غیرمتمرکز قرار داشته باشند. برای نمونه می‌توان از شاهدان[۵] برای ایفای نقش این مراجع در بلاک‌چین استفاده کرد.

محاسبات چندبخشی امن

مدل محاسبات چندبخشی[۶] (MPC) یک پروتکل چندبخشی تعریف می‌کند. این پروتکل به مشارکت‌کنندگان اجازه می‌دهد تا بدون نقض حریم خصوصی ورودی‌ها، محاسبات مشترکی را بر روی ورودی‌های داده‌های خصوصی انجام دهند. مخالفان در این روش جز خروجی محاسبات مشترک چیزی در مورد مشارکت‌کنندگان به دست نمی‌آورند.

---

[۱] Attribute-Based Encryption (ABE)

[۲] Collusion-resistance

[۳] Single Authority

[۴] Schemes

[۵] Witnesses

[۶] Multi-Party Computation (MPC)

نسخه اولیه این روش در سال ۱۹۸۲ و برای محاسبات دوبخشی ارائه شده بود و در سال ۱۹۸۷ پیشنهاد مربوط به تغییر پروتکل برای محاسبات چندبخشی ارائه گردید. پروتکل جدید با فرض محرمانگی همه ورودی‌های محاسبات و اثبات دانش صفر در اشتراک‌گذاری معرفی شد. این تعمیم به عنوان پایه و اساس بسیاری از پروتکل‌های کارآمد بعدی محاسبات چندبخشی مورد استفاده قرار گرفت. موفقیت محاسبات چندبخشی در رأی‌گیری توزیع شده، مناقصه‌های خصوصی و بازیابی اطلاعات محرمانه آن را به راه‌حلی محبوب برای مسائل دنیای واقعی تبدیل کرده است [۴].

محاسبات چندبخشی در سال‌های اخیر برای محافظت از حریم خصوصی کاربران در سیستم‌های بلاک‌چین مورد استفاده قرار گرفته است. پروتکل‌های محاسبات چندبخشی امن از سال ۲۰۱۴ در سیستم بیت کوین پیاده‌سازی شده است. این پروتکل‌ها برای قرعه‌کشی‌های چند جانبه امن و بدون هیچ‌گونه مرجع قابل اعتماد تهیه شده‌اند. این پروتکل بدون توجه به چگونگی رفتار کاربران متقلب می‌تواند انصاف برای کاربران صادق را تضمین نماید. اگر کاربری پروتکل را نقض کند، بازنده می شود و بیت‌کوین‌های او به کاربران صادق منتقل می‌شود.

اثبات دانش صفر غیرتعاملی

اثبات دانش صفر غیرتعاملی[۱] (NIZK) فناوری رمزنگاری دیگری است که بر اساس ویژگی حافظ حریم خصوصی اثبات دانش صفر عمل می‌کند. ایده اصلی، این است که یک اثبات رسمی می‌تواند برای تأیید اجرای برنامه‌ای با ورودی‌های محرمانه کاربر تنظیم شود و خروجی‌های عمومی بدون افشای اطلاعات دیگر تولید کند. به عبارت دیگر، یک مرجع تأیید گواهی[۲] می‌تواند صحت برخی از ادعاها[۳] را بدون ارائه اطلاعات مفیدی به تأییدکننده[۴] به او ثابت نماید. بر این اساس، اثبات دانش صفر غیرتعاملی یک نفر بدون نیاز به تعامل مرجع تأیید گواهی و تأییدکننده می‌تواند به دانش صفر محاسباتی دست یابد مشروط بر اینکه مرجع تأیید گواهی و تأییدکننده یک رشته مرجع مشترک را به اشتراک بگذارند. در بلاک‌چین، موجودی تمامی حساب‌های کاربری، رمزنگاری شده و بر روی زنجیره ذخیره شده است. زمانی که یک کاربر مقداری پول به کاربر دیگر انتقال می‌دهد با استفاده از اثبات دانش صفر به آسانی و بدون افشای موجودی واقعی حساب می‌تواند نشان دهد که موجودی کافی برای انتقال را دارد [۵].

---

[۱] Non-Interactive Zero-Knowledge (NIZK) Proof

[۲] Certifier

[۳] Assertion

[۴] Verifier

قراردادهای هوشمند مبتنی بر محیط اجرای قابل اعتماد

یک محیط اجرایی در صورت فراهم‌سازی محیط کاملاً ایزوله برای اجرای برنامه، یک محیط اجرای قابل اعتماد[۱] (TEE) است. محیط اجرای قابل اعتماد به طور مؤثری از دستکاری برنامه‌های نرم‌افزاری دیگر و سیستم‌های عامل در برنامه اجرا شده جلوگیری کرده و مانع از آگاهی آن‌ها از وضعیت درحال اجرا می‌شود. Intel Software Guard eXtensions (SGX) نمونه‌ای از فناوری‌های پیاده‌سازی محیط اجرای قابل اعتماد است. به عنوان مثال، Ekiden یک راه‌حل مبتنی بر SGX برای قراردادهای هوشمند حافظ محرمانگی است. Ekiden محاسبات را از اجماع جدا می‌کند و محاسبات قرارداد هوشمند را در یک محیط اجرای قابل اعتماد و بر روی گره‌های خارج از زنجیره[۲] انجام می‌دهد. پس از آن Ekiden از یک پروتکل تصدیق راه دور برای اعتبارسنجی صحت اجرا گره محاسباتی بر روی زنجیره استفاده می‌کند. گره‌های اجماع برای نگهداری بلاک‌چین مورد استفاده قرار می‌گیرند و نیازی به استفاده از سخت‌افزارهای قابل اعتماد ندارند. Enigma از محیط اجرای قابل اعتماد در نسخه فعلی خود استفاده می‌کند تا کاربران بتوانند قراردادهای هوشمند حافظ حریم خصوصی را با استفاده از الگوریتم رتبه‌بندی اعتبار غیرمتمرکز ایجاد کنند.

قراردادهای هوشمند مبتنی بر بازی

راه‌حل‌های مبتنی بر بازی[۳] برای تأیید قراردادهای هوشمند، از تحولات اخیر می‌باشند که توسط TrueBit و Arbitrum ارائه شده‌اند. به عنوان نمونه، TrueBit از بازی تأیید[۴] تعاملی برای تصمیم‌گیری در مورد درستی انجام یک کار محاسباتی استفاده می‌کند. این روش از نظام اهدای پاداش برای تشویق بازیگران به منظور کنترل وظایف محاسباتی و یافتن باگ‌ها استفاده می‌کند، به طوری که یک قرارداد هوشمند می‌تواند یک کار محاسباتی را به شکلی امن و با ویژگی‌های قابل تأیید انجام دهد. علاوه بر این، تأییدکننده در هر دور از بازی تأیید به صورت بازگشتی زیرمجموعه‌های کوچک و کوچک‌تری از محاسبات را کنترل می‌کند. این کار به TrueBit اجازه می‌دهد تا بار محاسباتی گره‌های خود را به طرز چشم‌گیری کاهش دهد [۶].

---

[۱] Trusted Execution Environment (TEE)

[۲] Off Chain

[۳] Game-based

[۴] Verification Game

منابع

[۱] R. Zhang, R. Xue و L. Liu, "Security and Privacy on Blockchain",*ACM Comput* ,۱ جلد , ,۱ شماره p. 35, 2019 .

[۲] mixcoin, "ANONYMOUS BITCOIN MIXER-STAY SAFE BY MIXING BITCOINS," mixcoin .Available: https://mixcoin.pro.[۲۰۱۹] ./

[۳] M. Gregory, "CoinJoin: Bitcoin privacy for the real world," CoinJoin, 2013.

[۴] wikipedia, "Secure multi-party computation," wikipedia .Available: https://en.wikipedia.org/wiki/Secure_multi-party_computation.[۲۰۱۹] .

[۵] J. Groth و R. Ostrovsky, "Perfect Non-Interactive Zero Knowledge for NP," U.C.L.A. Department of Computer Science, 2005.

[۶] J. Teutsch و C. Reitwießner, "TrueBit: A scalable verification solution for blockchains," 2017.