عنوان مقاله:

رویکردی نوین برای جلوگیری از آسیب پذیری در قراردادهای هوشمند و مقابله با حملات Reentrancy بر بستر بلاک چین

محل انتشار:

یازدهمین کنگره ملی سراسری فناوریهای نوین در حوزه توسعه پایدار ایران (سال: 1400)

تعداد صفحات اصل مقاله: 12

نویسندگان:

محمودرضا پارسائیان - *دانشگاه تهران پردیس بین الملل کیش، تهران*

حسین صمیمی - *پژوهشگاه ارتباطات و فناوری اطلاعات*

خلاصه مقاله:

بیش از یک دهه از معرفی فناوری بلاک چین و پروتکل بیت کوین توسط ساتوشی ناکاموتو در سال ۲۰۰۸ می گذرد. پروتکل بیت کوین به عنوان یک نسخه ضعیف از مفهوم قرارداد هوشمند شناخته می شود و امکان برنامه نویسی در آن وجود ندارد. در راستای رفع اینمحدودیت، ارز دیجیتالی اتریوم (Ethereum) توسط ویتالیک بوترین و گاوین وود در سال ۲۰۱۴ معرفی شد. اتریوم اجازه میدهد تاقراردادهای هوشمند پیچیده بین طرفهای غیرقابل اعتماد، ایجاد و اجرا شوند. قراردادهای هوشمند با طیف وسیعی از شرکت ها مانندخدمات مالی، دفتر اسناد رسمی، املاک و اینترنت اشیا و مانند آنها سازگار هستند. از آنجا که ساختار بلاک چین بصورت توزیع شده‌است و حجم بالائی از پول در این معاملات جابجا می شود. در نتیجه برای بهره مندی از قابلیت های قراردادهای هوشمند چالش های بسیاری مانند احراز هویت ،امنیت تراکنش، محرمانه بودن، مسائل مربوط به حریم خصوصی و همچنین مقابله با حملات امنیتی مختلف وجود دارد که رفع آنها نیازمند تحقیقات بیشتری درآینده است.هدف از این مقاله، معرفی پرخطر ترین حمله سایبری بر روی قراردادهای هوشمند بر بستر بلاک چین با عنوان حمله ورود مجدد(entrancyRe) و ارایه راهکاری کارآمد برای جلوگیری از آن می باشد. در این چارچوب ابتدا یک نسخه از بلاک چین بر بستر EVM(Ethereum Virtual Machine) بنام BankBalance با قرارداد هوشمندی که با کد هائی به زبان برنامه نویسی شی گرای سطح بالایSolidity ، نوشته شده است، راه اندازی کرده ایم. این نسخه امکان کم کردن (Withdrew) یا اضافه کردن (Deposit) روی فیلدموجودی (balance) را در محیط وب در تعامل با بلاک چین، فراهم می کند. در قدم بعد نشان داده ایم که این بلاک چین در مقابل حمله ورود مجدد آسیب پذیر است و سپس با تحلیل این آسیب پذیری و شناسایی دلایل بروز آن، کدهای تکمیلی توسعه یافته واقدامات اصلاحی لازم بر روی قرارداد هوشمند موجود انجام داده ایم. نتایج حاصل از بررسی های انجام شده نشان می دهد که آسیب‌پذیری موجود برطرف شده و بلاک چین جدید توسعه یافت از حمله ورود مجدد در امان است.

کلمات کلیدی:

Blockchain, Smart contracts, Vulnerabilities of Smart Contract, Distributed ledger, Attacks on Smart Contracts

لینک ثابت مقاله در پایگاه سیویلیکا: