عنوان مقاله:
ارائه ساز و کاری برای نظارت مالک بر قرارداد هوشمند در اتریوم

محل انتشار:
هفدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1399)

تعداد صفحات اصل مقاله: 6

نویسندگان:
مرتضی امیرمحسنی - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر-رایانش امن، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران*

صادق دری نوگورانی - *استادیار دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران ،*

خلاصه مقاله:
قراردادهای هوشمند برنامه هایی هستند که بر روی زنجیره بلوک ثبت شدهاند و کاربران می توانند از طریق تراکنش ها آنها را اجرا کنند. نتایج اجرای قراردادهای هوشمند توسط اعضا بررسی و بر روی زنجیره بلوک ثبت می شود. ممکن است مبلغ قابل توجهی رمزارز در اختیار یک قرارداد هوشمند باشد و با اجرا شدن آن، این دارایی مدیریت و جابجا شود؛ بنابراین ضروری است که قرارداد درمقابل تهدیدها و حملات امن باشد. در حوزه امنیت قراردادهای هوشمند پژوهش هایی انجام شده، و ابزارهایی برای بررسی کد قرارداد قبل از قرارگرفتن روی زنجیره بلوک ارائه شده است. این ابزارها با بررسی کد قرارداد آسیب پذیری های آن را برای اصلاح به برنامه نویس اعلام می کنند. با وجود این ممکن است قرارداد دارای نوعی آسیب پذیری باشد که توسط ابزارهای موجود قابل شناساییینیست. در برخی از چنین مواردی میتوان در زمان حمله نشانه هایی را تشخیص داد که دال بر سوءاستفاده هستند. در این مقاله ساز و کاری معرفی شده است تا امکان نظارت زمان اجرا بر روی قراردادهای هوشمند بستر اتریوم را فراهم می کند. با این ساز و کار مالک هنگام قرارگیری کد بر روی زنجیره بلوک، تعدادی محافظ امنیتی برای قرارداد مشخص می کند. با تغییراتی که در فرایناددرستی سنجی تراکنش ها در استخراج گر اتریوم داده می شود، به محض برقرار شدن شرایط محافظ ها، استخراج گر جلوی اجرای تراکنش مربوط به آن را خواهد گرفت. ساز و کار پیشنهادی مکمل روش های تحلیل کد (ایستا و پویا) است و توانایی تشخیص و جلوگیری از حملاتی را دارد که برای ابزارهای تحلیل کد ناممکن است.

کلمات کلیدی:
زنجیره بلوک، قرارداد هوشمند، آسیب پذیری، نظارت زمان اجرا