عنوان ارائه:

بررسی حمله‌ها و هک‌های صورت گرفته در رمزارزها

A Review on Hacks and Attacks on Cryptocurrencies

توسط: علیرضا صادقی نسب

استاد: دکتر وحید رافع

تاریخ ارائه: 1400/10/18

فهرست مطالب

- مقدمه
- حمله ۵۱ درصد
- حمله قراردادهای هوشمند
- حمله انعطاف‌پذیری تراکنش

مقدمه

- **چرا رمزارزها مورد حمله قرار می‌گیرند؟**

☆ ارزهای دیجیتال مبتنی بر فناوری بلاکچین هستند که غیرقابل تغییر در نظر گرفته می‌شوند

☆ با این حال، افزایش محبوبیت ارزهای دیجیتال، مجرمان سایبری را تشویق کرده است تا راه‌های خلاقانه‌ای برای حمله به بلاکچین پیدا کنند

☆ هک در ارزهای دیجیتال می‌تواند شامل مصادیق زیادی باشد. به عبارت ساده، اگر یک مهاجم بتواند از بخشی از یک زنجیره، قرارداد هوشمند، صرافی یا برداشت غیرقانونی ارز دیجیتال سوء استفاده کند، به عنوان هک یا سرقت تلقی می شود.

مقدمه

- **بلاکچین؛ غیرقابل تغییر یا قابل هک؟**

☆ هر حساب کریپتو توسط رمزنگاری غیرقابل شکسته شدن و یک کلید خصوصی که رشته‌ای از حروف و اعداد است و به عنوان کد شناسایی برای هر دارنده حساب رمزنگاری عمل می کند، قفل می شود. اما هکرها نشان داده‌اند که بلاکچین‌ها تغییرناپذیر نیستند

☆ یک قرارداد هوشمند با کدگذاری ضعیف می‌تواند توسط شخصی هک شود که دستورالعمل‌های خاصی را برای آن ارسال می‌کند. به طور خلاصه، خود قرارداد هوشمند را می‌توان هک کرد، اما بلاکچین را نه

☆ اگر هکرها به کیف پول دسترسی پیدا کنند، می‌توانند کلید خصوصی حساب را بشکنند، که راه دیگری برای هک کریپتو است.

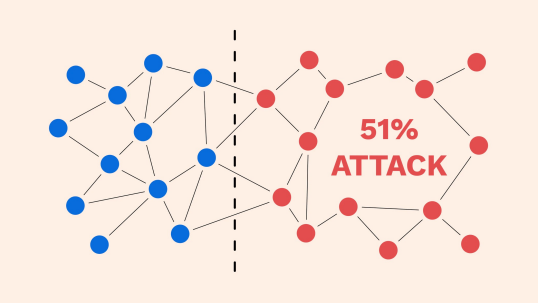
حمله ۵۱ درصد

- **حمله ۵۱ درصدی چیست؟**

☆ این حمله در ذات رمزارزهایی است که از PoW به عنوان پروتکل خود برای تایید تراکنش‌ها استفاده می‌کنند

☆ ماینری که به نحوی کنترل اکثریت قدرت استخراج شبکه را به دست می‌آورد، می‌تواند با ارسال تراکنش‌ها به سایر کاربران و سپس ایجاد نسخه جایگزینی از بلاکچین که در آن تراکنش‌ها هرگز انجام نشده‌اند، فریب دهد. این نسخه جدید fork نام دارد

☆ مهاجمی که بیشتر قدرت استخراج را کنترل می‌کند، می‌تواند fork را به نسخه معتبر زنجیره تبدیل کند و دوباره همان ارز دیجیتال را خرج کند. برای بلاکچین‌های محبوب، انجام این نوع سرقت احتمالاً بسیار گران است



حمله ۵۱ درصد

- **حمله ۵۱ درصد، از حرف تا عمل**

اجاره قدرت استخراج کافی برای حمله به بیتکوین در حال حاضر بیش از یک و نیم میلیون دلار در ساعت هزینه دارد. اما با پایین آمدن در لیست بیش از 1500 ارز دیجیتال موجود، به سرعت ارزان‌تر می شود

PoW 51% Attack Cost

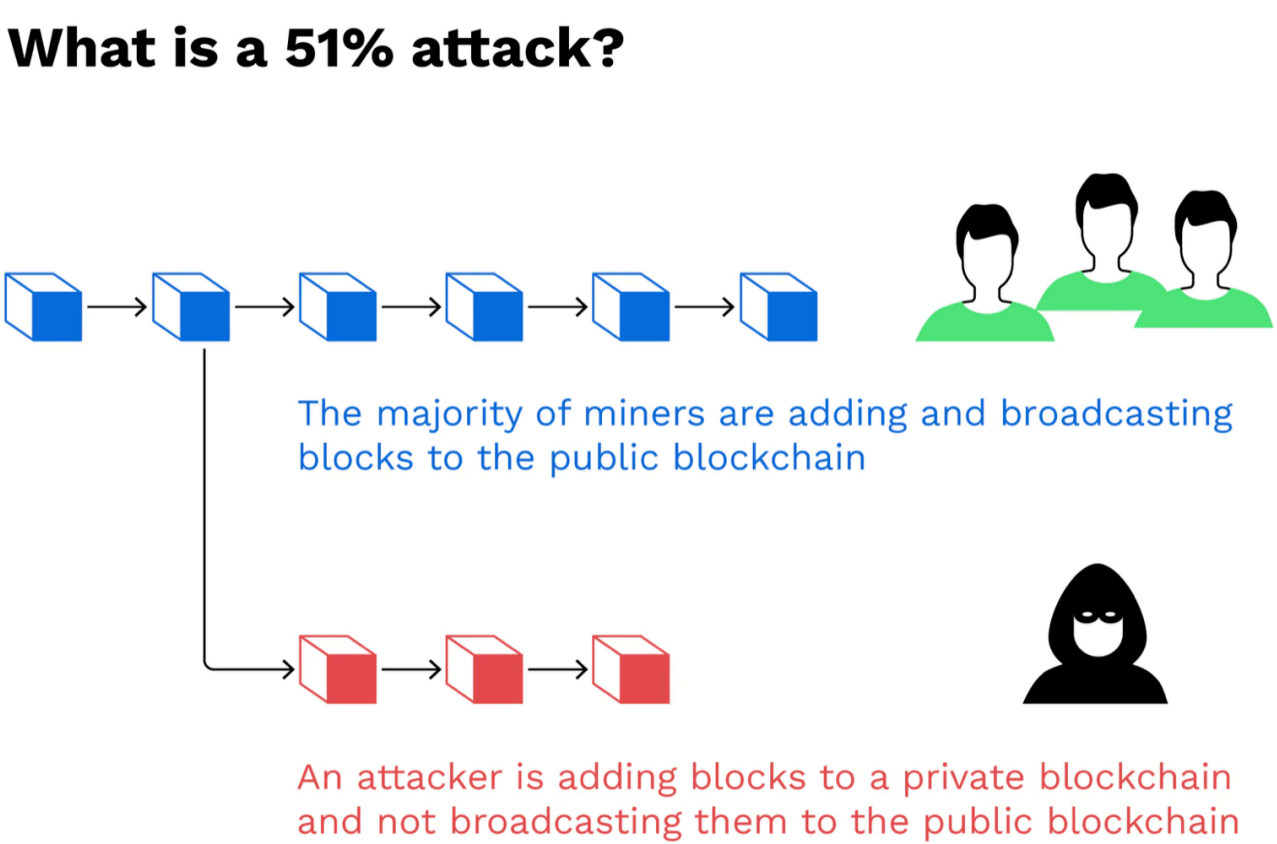
This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More ⚡ Tip

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$791.66 B	SHA-256	177,596 PH/s	*$1,595,411*	0%
Ethereum	ETH	$382.41 B	Ethash	896 TH/s	*$1,846,790*	7%
Litecoin	LTC	$9.22 B	Scrypt	385 TH/s	*$131,118*	11%
BitcoinCash	BCH	$7.39 B	SHA-256	1,712 PH/s	*$15,378*	31%
Zcash	ZEC	$1.85 B	Equihash	7 GH/s	*$15,835*	8%
Dash	DASH	$1.34 B	X11	7 PH/s	*$4,889*	2%
Ravencoin	RVN	$1.20 B	KawPow	11 TH/s	*$34,314*	9%
BitcoinGold	BTG	$655.06 M	Zhash	3 MH/s	*$1,293*	20%

https://www.crypto51.app

حمله ۵۱ درصد


What is a 51% attack?
The majority of miners are adding and broadcasting blocks to the public blockchain
An attacker is adding blocks to a private blockchain and not broadcasting them to the public blockchain

حمله ۵۱ درصد

- **قربانیان حمله ۵۱ درصد**

☑ سال ۲۰۱۶: رمزارزهای کریپتون و شیفت

☑ سال ۲۰۱۸: رمزارزهای موناکوین، ورج، ورت‌کوین و اتریوم کلاسیک

☑ سال ۲۰۱۹: بیتکوین گلد

☑ سال ۲۰۲۰: بیتکوین گلد

☑ سال ۲۰۲۱: بیتکوین SV

حمله ۵۱ درصد

- **استخرهای ماین و حمله ۵۱ درصد**

☆ استعداد حمله ۵۱ درصدی در استخرهای ماین نیز وجود دارد. برای مثال با توجه به محبوبیت استخر استخراج Ghash، بسیاری از افراد در جامعه بیتکوین نگران احتمال حمله 51 درصدی بودند. در جولای 2014، استخر استخراج Ghash برای مدت کوتاهی از آستانه 51 درصد فراتر رفت

☆ بزرگی این تهدید به گونه‌ای بود که پیتر تاد، توسعه‌دهنده برجسته بیتکوین، نیمی از دارایی‌های خود را بفروشد. طبق گزارش‌ها، این خبر باعث شد که قیمت بیتکوین از 633 دلار به 600 دلار در آن زمان کاهش یابد

☆ استخر Ghash یک بیانیه داوطلبانه منتشر کرد و قول داد که از 40٪ از کل هش بیتکوین تجاوز نخواهد کرد

حمله قراردادهای هوشمند

- **قرارداد هوشمند**

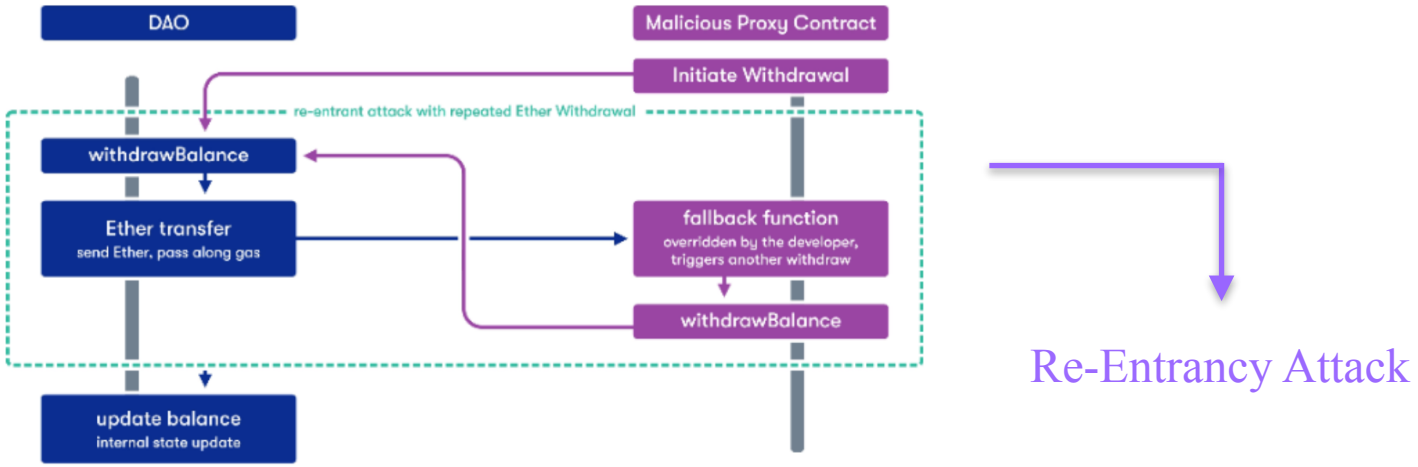
☆ قرارداد هوشمند یک برنامه کامپیوتری است که بر روی شبکه بلاکچین اجرا می‌شود. می‌توان از آن برای خودکار کردن نقل و انتقال ارزهای دیجیتال طبق قوانین و شرایط تجویز شده استفاده کرد

☆ این کار کاربردهای بالقوه بسیاری دارد، مانند تسهیل قراردادهای حقوقی واقعی یا تراکنش‌های مالی پیچیده. استفاده دیگر آن، ایجاد مکانیزم رای‌گیری است که از طریق آن همه سرمایه‌گذاران در یک صندوق سرمایه‌گذاری خطرپذیر می‌توانند به طور جمعی تصمیم بگیرند که چگونه پول را تخصیص دهند

حمله قراردادهای هوشمند

- **حمله در قراردادهای هوشمند**

☆ صندوقی به نام سازمان غیرمتمرکز خودمختار (DAO) در سال 2016 با استفاده از سیستم بلاکچین به نام اتریوم راه‌اندازی شد. مدت کوتاهی پس از آن، یک مهاجم با سوء استفاده از یک نقص پیش‌بینی نشده در یک قرارداد هوشمند که بر DAO حاکم بود، بیش از 60 میلیون دلار ارز دیجیتال را به سرقت برد. در اصل، این نقص به هکر این امکان را می‌دهد که به درخواست پول از حساب‌ها ادامه دهد، بدون اینکه سیستم ثبت کند که پول قبلاً برداشت شده است



حمله قراردادهای هوشمند

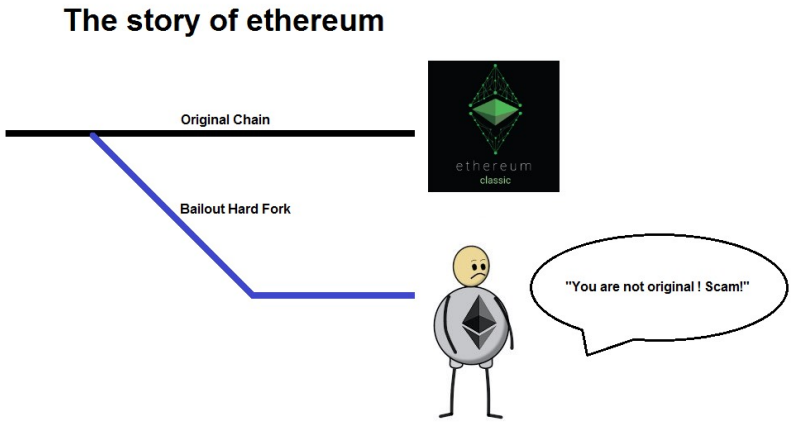
- **هزینه تغییر در قراردادهای هوشمند**

☆ در نرم افزارهای سنتی، یک باگ را می توان با یک وصله (patch) برطرف کرد. در دنیای بلاکچین، این کار چندان ساده نیست. پتار تسانکوف، دانشمند پژوهشی در ETH زوریخ و یکی از بنیان‌گذاران یک استارتاپ امنیتی قراردادهای هوشمند به نام ChainSecurity می‌گوید از آنجایی که تراکنش‌های یک بلاکچین قابل لغو نیستند، استقرار یک قرارداد هوشمند کمی شبیه پرتاب یک موشک است. "نرم افزار نمی‌تواند اشتباه کند."

حمله قراردادهای هوشمند

- **هزینه تغییر در قراردادهای هوشمند – ادامه**

☆ تنها راه برای بازیابی پول، به طور مؤثر، بازنویسی تاریخ است. بازگشت به نقطه بلاکچین قبل از وقوع حمله، ایجاد یک fork برای یک بلاکچین جدید و اینکه همه افراد در شبکه موافقت کنند که از آن استفاده کنند. این همان کاری است که توسعه‌دهندگان اتریوم تصمیم گرفتند انجام دهند. بیشتر جامعه (اما نه همه) به زنجیره جدیدی روی آوردند که اکنون آن را با نام اتریوم می‌شناسیم. گروه کوچکتری از نگهدارنده‌ها به زنجیره اصلی چسبیده بودند که به اتریوم کلاسیک تبدیل شد

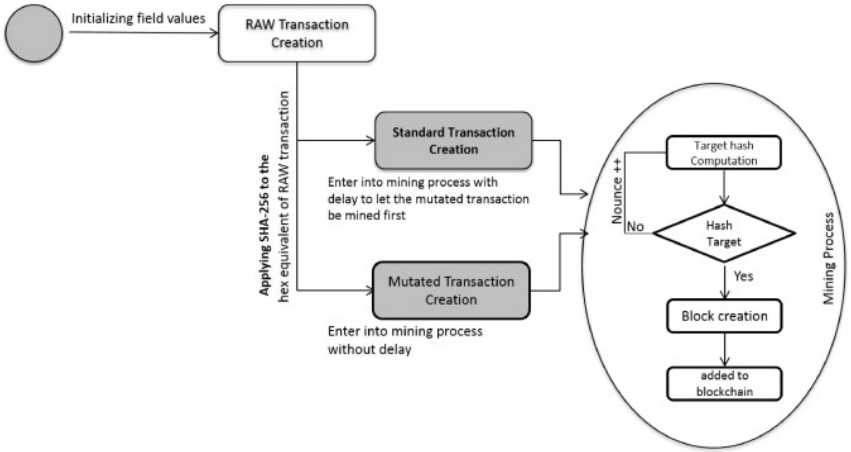


حمله انعطاف‌پذیری تراکنش

- **حمله انعطاف‌پذیری تراکنش چیست؟**

☆ بلاکچین به گونه‌ای ایجاد شده است که کاملاً تغییرناپذیر باشد. این مهم از طریق توابع هش رمزنگاری به دست می‌آید. معنای اصلی آن این است که وقتی داده‌ها در بلاکچین قرار می‌گیرند، نمی‌توان آنها را دستکاری کرد. فقط همین کیفیت به تنهایی به ارزهای دیجیتال مبتنی بر بلاکچین امنیت فوق العاده‌ای می بخشد

☆ حال اگر دستکاری داده‌ها قبل از قرار دادن داده‌ها در بلاکچین اتفاق بیفتد، چه؟ حتی اگر دستکاری مورد توجه قرار گیرد، وقتی وارد بلاکچین شود، هیچکس نمی‌تواند کاری برای آن انجام دهد. به این انعطاف‌پذیری تراکنشی می‌گویند



حمله انعطاف‌پذیری تراکنش

- **فاجعه** Mt.Got

☆ این اتفاق در سال ۲۰۱۴ برای صرافی Mt.Got پیش آمد. به طور خاص، در یک تراکنش انتقال، مهاجم (گیرنده) می‌توانست امضای فرستنده را قبل از اینکه وارد بلاکچین شود دستکاری کند و شناسه تراکنش را تغییر دهد. این تراکنش جدید و دستکاری شده این شانس را دارد که تراکنش اصلی فرستنده را بازنویسی کند. در این سناریو، مهاجم وجوه را دریافت می‌کند، اما به نظر می‌رسد فرستنده تراکنش اصلی را با موفقیت در زنجیره بلوکی قرار نمی‌دهد. بنابراین مهاجم (گیرنده) می‌تواند درخواست انتقال اضافی کند که در نهایت دو بار وجوه را دریافت می کند. این اتفاق موجب زیان ۳۵۰ میلیون دلاری (سرقت ۷۵۰ هزار بیتکوین) این صرافی شد و موجب ورشکستگی آن شد

با تشکر از توجه شما