Cryptocurrencies

ارزهای دیجیتالی

3rd revision

در این کتاب می‌خوانید:

مروری بر ارزهای دیجیتال

استانداردهای ارزهای دیجیتال

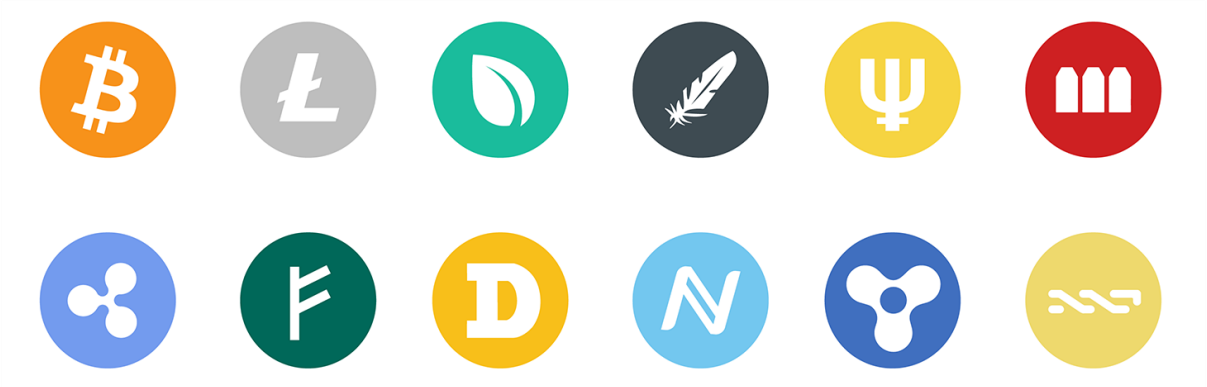
روش‌های تهیه ارزهای دیجیتال

امنیت و ارزهای دیجیتال

و بسیاری موارد ریز و درشت دیگر...

Mohsen Salehi

تا تاریخ نگارش این کتاب، بیش از 2100 نوع ارز دیجیتال ایجاد شده است و با توجه به توانایی‌ها و قابلیت‌هایی که این نوع پول ارائه می‌دهد، سازمان‌ها و دولت‌ها کم کم به سوی ایجاد ارز دیجیتال مختص خود پیش می‌روند.



برای دیدن فهرست کامل ارزهای دیجیتالی و ارزش لحظه‌ای آنها به لینک‌های زیر بروید:

coinmarketcap.com | investing.com

در تصویر زیر، ما در وبسایت coinmarketcap.com فهرست با ارزش‌ترین ارزها را می‌بینیم:

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ Exchanges ▾ Watchlist USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$62,582,944,120	$3,577.48	$4,951,873,434	17,493,587 BTC	-0.58%	
2	XRP	$13,149,844,764	$0.320412	$368,682,342	41,040,405,095 XRP *	-0.20%	
3	Ethereum	$12,311,087,072	$117.82	$2,473,227,263	104,493,812 ETH	-1.59%	
4	Bitcoin Cash	$2,161,754,153	$122.98	$195,155,366	17,578,463 BCH	-0.61%	
5	EOS	$2,127,647,854	$2.35	$741,062,528	906,245,118 EOS *	-0.20%	

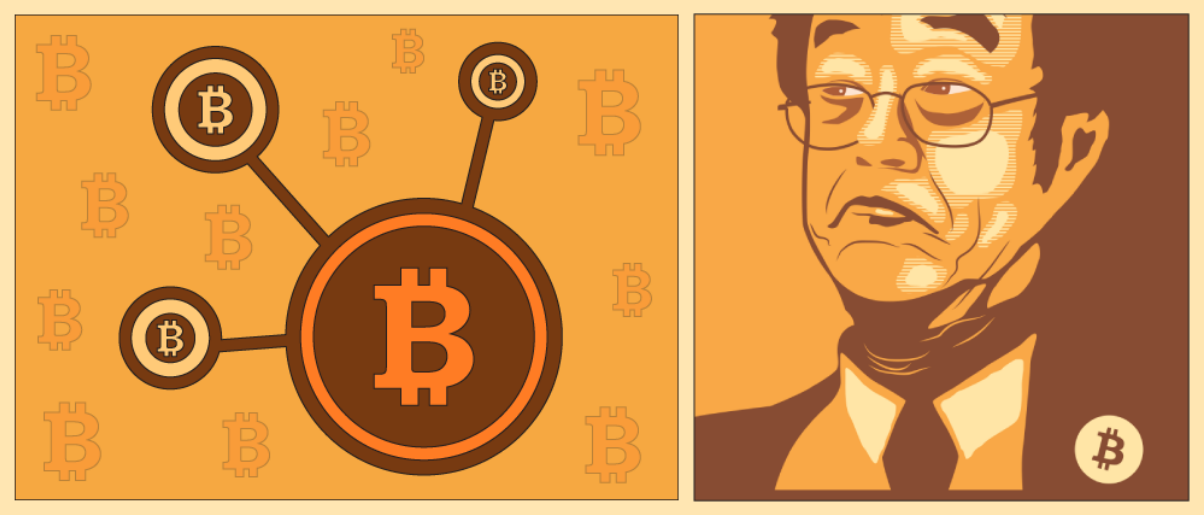
۵ ارز برتر بازار (بر اساس میزان ارزش کل آنها در بازار) در ابتدای فهرست هستند.

در جدول بالا، ارزش فعلی ارزها در بازار (مقدار موجود در بازار) تحت عنوان Market Cap نشان داده شده است.

همچنین Circulating Supply مشخص کننده سرمایه موجود در گردش ارز مد نظر است.

الباقی فاکتورها، نوسانات و تغییرات نرخ ارزها را در بازه‌های زمانی مختلف نشان می‌دهد.

فاکتورهای متعددی در وبسایت‌هایی که در بالا معرفی کردیم (و وبسایت‌های متعدد دیگر) در رابطه با بررسی نوسانات، تحلیل‌ها و بازار ارزهای دیجیتالی فهرست شده است. وبسایت investing.com که در بالا معرفی شد، اطلاعات به روز و لحظه‌ای جامعی درباره آخرین تغییرات نرخ ارزهای دیجیتال در اختیار ما قرار می‌دهد.



تاریخچه ارزهای دیجیتال

تاریخچه ایجاد اولین ارز دیجیتال به سال ۲۰۰۹ باز می‌گردد که با Bitcoin شروع شد.

ارزهای دیجیتالی از یکسری استانداردهای مشترک پیروی می‌کنند که ما در این کتاب Bitcoin که تا به این تاریخ ارزشمندترین ارز دیجیتال است را به عنوان مرجع آموزش در نظر می‌گیریم.

خالق Bitcoin، Satochi Nakamoto* قصد داشت ارز دیجیتالی تهیه کند که وابسته به تئوری‌ها و محاسبات ریاضی باشد، نه به اقتصادها و بازارهای پر نوسان.

در مورد اینکه چه کسی در واقع Bitcoin را ایجاد کرده، نظرات متفاوتی است. افراد و سازمان‌های مختلف، حتی از CIA هم به عنوان ایجاد کننده این ارز نام برده شده است.

Cryptocurrency

Cryptocurrency معرف ارزهای دیجیتال یا مجازی است که با استفاده از روش‌های رمزنگاری (Cryptography) ایمن (Secured) شده‌اند.

Cryptography به تکنیک‌های رمزنگاری جهت صحت و ایمن بودن تراکنش‌ها اشاره دارد.

لغاتی که در این میان به چشم می‌خورد Token و Coin است. لازم به ذکر است که همه Coin ها و Token ها به عنوان Cryptocurrency شناخته می‌شوند، حتی در شرایطی که برای برخی از آنها امکان تبدیل از طریق صرافی (Exchange) وجود ندارد و حتی به عنوان یک ارز کارایی ندارند.

لغت Cryptocurrency ممکن است یک واژه گمراه کننده به نظر بیاید، به این دلیل که ارزهای رسمی، مشمول بر یک واحد شمارش، ارزش اندوخته و قابلیت تبادل هستند. همه خواص ذکر شده در ارزی مانند Bitcoin موجود است اما در این میان ارزهایی پا به عرصه گذاشته‌اند که موارد ذکر شده را به عنوان یک ارز جامع در بر نمی‌گیرند.

عمومی‌ترین طبقه‌بندی Cryptocurrency ها شامل این دو هستند:

1. Alternative Cryptocurrency Coins (Altcoins)
2. Tokens

Altcoin ها

Altcoin ها در اصل بر پایه Bitcoin و Open-source برنامه نویسی شده‌اند اما در همین حال، خواص و قابلیت‌های متفاوتی ارائه می‌دهند. نمونه‌هایی از این Altcoin ها شامل Litecoin، Peercoin و Auroracoin هستند.

همچنین Altcoin های دیگری نیز وجود دارند که کاملاً مستقل از Bitcoin و به صورت open-source هستند. این Altcoin ها Blockchain و Protocol مختص خود را دارند. از نمونه این ارزها می‌توان Ethereum و Ripple را نام برد.

Token ها

Token ها معرف یک ابزار یا سرمایه خاص هستند که معمولاً بر روی یک Blockchain قرار می‌گیرد. Token عملاً می‌توانند هر نوع سرمایه که قابل معامله و تبدیل به پول هست را شامل شوند، از کالاهای متنوع گرفته تا کارت‌های اعتباری و حتی دیگر Cryptocurrency ها.

ایجاد یک Token به سختی و پیچیدگی ایجاد Cryptucurrency نیست چرا که برای شکل گرفتن آن می‌توان از یک قالب استاندارد (مانند Ethereum) برای ایجاد آن در Blockchain استفاده کرد.

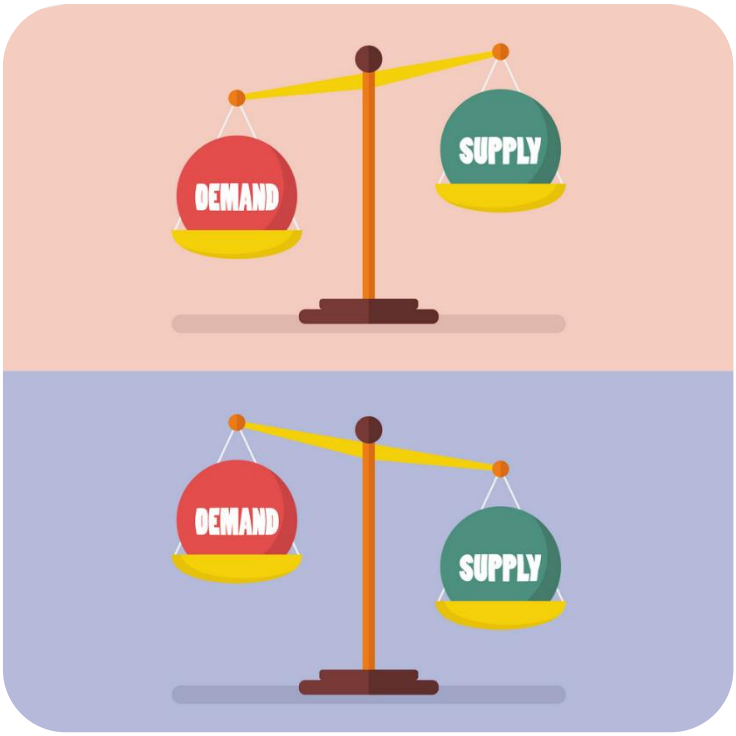
ارزهای نو

امروزه با جرأت می‌توان گفت که ما هر روز شاهد ارائه یک ارز دیجیتال از سوی شرکت‌های بزرگ و حتی افراد مطرح هستیم. در اینجا این سوال پیش می‌آید که با توجه به اینکه دیگران این ارز را mine می‌کنند، چگونه شخص یا شرکت معرفی کننده ارز، از این قضیه سود می‌برد؟

چالش‌های زیادی در رابطه با ایجاد یک ارز نو وجود دارد و این رقابت با به پا گذاشتن ارزهای جدید مدام سخت تر می‌شود. فرض را بر این می‌گیریم که یک ارز نو، مراحل اولیه را طی کرده و اکنون به صورت فعال در بازار خرید و فروش می‌شود. شرکتی که این ارز را معرفی کرده، در ابتدای معرفی ارز سهمی از حداکثر میزان این ارز را برای خود نگه می‌دارد که این مقدار در ابتدی معرفی ارز مشخص شده است. اگر این ارز موفق شود، ایجاد کننده ارز سود زیادی از این رویداد می‌برد.

برای دیدن ارزهایی که به تازگی معرفی شده‌اند و منتظر سرمایه گذاری دیگران هستند می‌توانید به لینک زیر بروید:

cryptocompare.com



تعریف واژه‌های Circulating Supply، Total Supply و Max Supply

برآورد ارزش یک ارز دیجیتال بدون در نظر گرفتن شرایط حال و آیندهٔ مقدار قابل عرضه یا موجودی (Supply) غیر ممکن است.

موجودی یک ارز دیجیتال یکی از فاکتورهای مهم در تعیین قیمت آن و البته یکی از موارد گیج کننده نیز است. ما موجودی در حال گردش (Circulating Supply) داریم، حداکثر موجودی (Max Supply) داریم، Token های از دست رفته (Lost Tokens)، تورم و خیلی موارد دیگر نیز هستند که بر روی ارزش سهام (Market Cap) یک ارز تأثیر گذارند.

Circulating Supply در ساده‌ترین تعریف، به مقدار سکه‌ای گفته می‌شود که در تبادلات روزمره در دنیای واقعی وجود دارد و از طریق سرویس‌های Exchange (صرافی‌های آنلاین) مبادله می‌شود.

Total Supply معادل مقدار سکه‌های درون Circulating Supply است به علاوه سکه‌هایی که جدیداً Mine می‌شوند. ممکن است افرادی سکه‌های خود را در کیف پول الکترونیکی خود نگه داشته باشند، ارز افراد قفل یا رزرو شده باشد که این سکه‌ها عملاً در گردش نیستند اما در مقدار Total Supply در نظر گرفته می‌شوند.

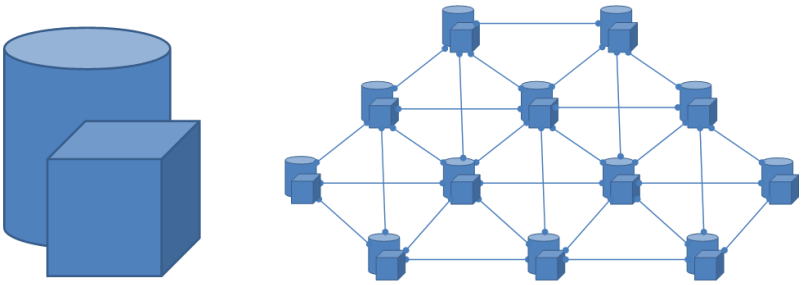
Max Supply مشخص کننده حداکثر مقداری است که یک ارز می‌تواند تولید شود. برای مثال، Bitcoin محدودیتی معادل ۲۱ میلیون سکه دارد و بعد از رسیدن به این مقدار، Mine کردن آن متوقف می‌شود، مگر آنکه تا آن زمان الگوریتم و ساختار Bitcoin تغییر کند.

خواص کلی ارزهای دیجیتالی

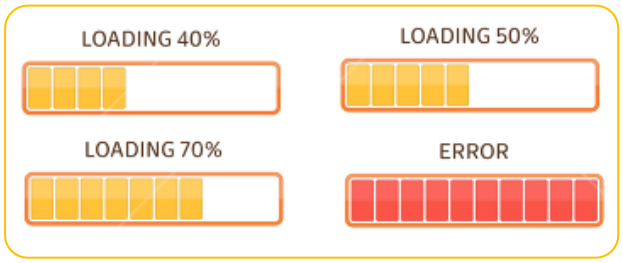
عدم داشتن ماهیت فیزیکی، به این معنی که این نوع پول به صورت الکترونیکی ذخیره می‌شود، مانند اسکناس نبوده و در نتیجه قابل دستکاری توسط افراد نیست.

با توجه به غیر فیزیکی بودن این نوع سرمایه، بسیاری از مشکلات عمده که ممکن است برای سرمایه‌های فیزیکی به وجود بیاید منتفی می‌شود. با این وجود، متصل بودن به شبکه جهانی و دنیای الکترونیک نیز ناامنی‌های مختص خود را دارد.

غیر متمرکز بودن (Decentralised)، به این معنی که هیچ سازمان مالی خاصی شبکه مالی Bitcoin را مدیریت نمی‌کند و این ارز به هیچ مرکزی وابستگی ندارد. در نتیجه، مشکلات اقتصادی و خواسته‌های شخصی تأثیری در کاهش یا افزایش نرخ Bitcoin ندارد. طبق شکل زیر، در سیستم متمرکز (Centralised)، هر قسمت (Node) به صورت مستقل فعالیت می‌کند، در حالی که در سیستم غیر متمرکز (Decentralised)، بخش‌ها به یکدیگر متصل هستند و مرکزیت خاصی وجود ندارد. به این ترتیب، در صورتی که یک یا چند بخش از کار بیفتد، سیستم همچنان به کار خود ادامه خواهد داد.



Centralised **Decentralised**

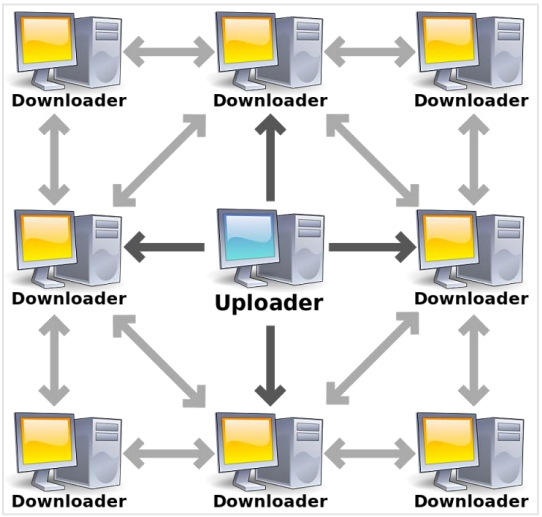


برای درک بهتر این موضوع، یک مثال می‌زنیم. فرض کنید می‌خواهید یک فایل دانلود کنید. اگر این فایل از روی یک وبسایت و Server خاص دانلود شود، به این معنیست که فقط یک مسیر جهت دانلود در اختیارمان قرار داده شده است، و اگر به هر دلیلی مشکلی برای این وبسایت یا Server رخ دهد، این سرویس قطع و از دسترس خارج می‌شود.

اما در سیستم غیر متمرکز اینطور نیست. نمونه بارز یک مثال برای تعریف سیستم غیر متمرکز Torrent ها هستند.

جهت درک بهتر موضوع غیرمتمرکز بودن ارزها، توضیحات torrent را به صورت مفصل در ادامه خواهیم داد.

Torrent یک روش اشتراک گذاری فایل است که در آن به جای اینکه از یک سیستم Server به عنوان میزبان استفاده شود، از تمام سیستم‌هایی که آن فایل را به اشتراک گذاشته‌اند استفاده می‌شود و هر کاربر سهمی در به اشتراک گذاری فایل دارد. حال اگر پهنای باند یک کاربر بیشتر باشد، سرعت بیشتری برای دیگر کاربران که در حال دانلود فایل هستند ارائه می‌دهد. حالت کلی عملکرد Torrent به شکل زیر است:



برای درک بهتر این موضوع، Torrent و کار با آن را به صورت عملی توضیح می‌دهیم. همانند نرم‌افزارهای مدیریت دانلود، برای مدیریت و دانلود Torrentها نیز ما نرم‌افزارهای متعدد رایگانی در اختیار داریم. معروف‌ترین آنها شامل دو نرم‌افزار زیر هستند:

BitTorrent

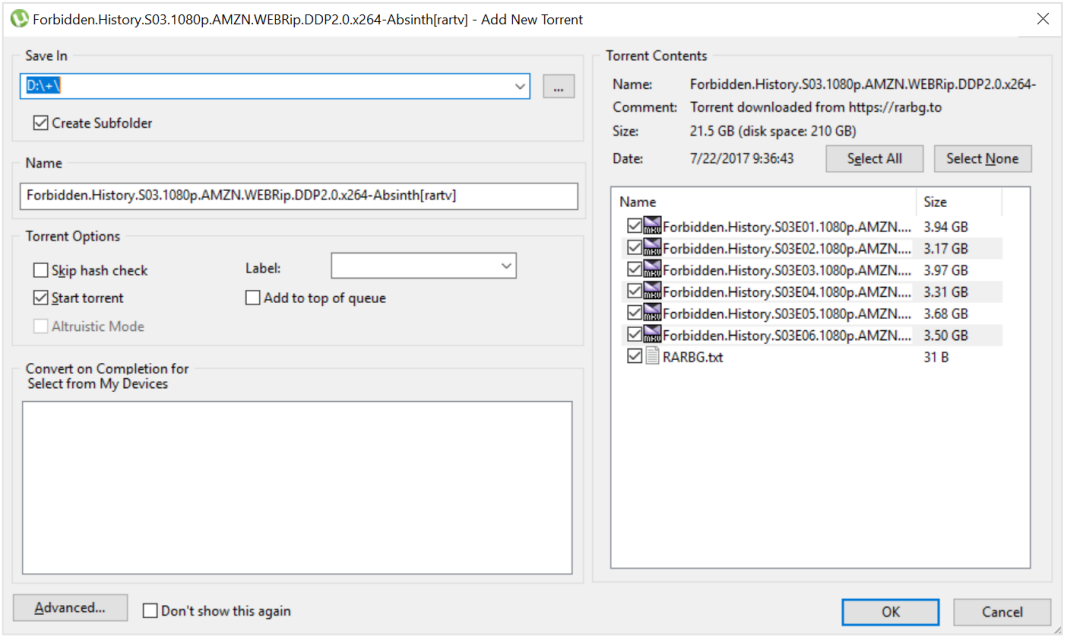
µTorrent

ابزارهای فوق به طور رایگان در دسترس هستند و محیطی کاملاً شبیه به یکدیگر دارند. برای اینکه ببینیم چگونه با Torrentها می‌توان کار کرد، کافیست از یکی از وبسایت‌های زیر یک فایل .torrent که حجم کمی (معمولاً زیر 100KB) دارند را دانلود کنیم:

torrentdownloads.me | 1337x.to | rarbg.to

دقت داشته باشید که وبسایت‌های میزبان Torrent همگی فیلتر هستند، اما محتوای فایل .torrent غیر قابل فیلتر شدن است.

بعد از اینکه یک فایل .torrent دانلود کردیم، کافیست آن را با یکی از نرم‌افزارهای فوق باز کنیم. بعد از باز شدن این فایل، محتوای درون آن به صورت زیر به ما نشان داده می‌شود:



همانطور که در تصویر بالا می‌بینید، محتویات فایل .torrent ما 21.5GB حجم دارد در حالی که خود فایل .torrent تنها 55KB فضا اشغال کرده است.

سوال اینجاست که این فایل‌ها کجا قرار دارد؟ کدام Server یا وبسایت میزبانی این حجم از اطلاعات را به عهده گرفته است؟

این اطلاعات، هیچ جایی قرار ندارد به جز روی کامپیوترهای معمولی کاربرانی که هر کدام در گوشه‌ای از این سیاره هستند. طبق شکل زیر، فهرست آدرس‌هایی که ما در حال دانلود این فایل‌ها از آنها هستیم را می‌بینید.

بعد از تأیید و شروع دانلود، در پایین صفحه و با کلیک بر روی آن Torrent جزئیات این فهرست را می‌بینید:

Files | Info | Peers | Trackers | Pieces | Speed | Logger | Related

IP	Client	Flags	%	Down Speed	Up Speed	Reqs	Uploaded	Downloaded	Peer dl.
54.39.68.205 [uTP]	Deluge 1.3.15	UD X	0.3	2.2 kB/s	61.3 kB/s	4 | 0	3.95 MB	192 kB	682.6 kB/s
24.202.104.241	qBittorrent/4.0.4.0	UD HX	6.7	160.2 kB/s	19.0 kB/s	77 | 0	2.62 MB	10.0 MB	273.0 kB/s
27.253.50.230	Vuze 5.7.6.0	UD X	10.9		0.8 kB/s	5 | 0	5.70 MB	96.0 kB	318.5 kB/s
46.103.19.189 [uTP]	BitTorrent 7.10.3	d XeP	42.0						
59.149.186.71	Transmission 2.94	DS HX	100.0			1 | 0			
81.150.177.58	qBittorrent/4.1.0	UD H	50.1	0.2 kB/s		2 | 0	160 kB	80.0 kB	
92.189.122.61 [uTP]	µTorrent 3.5.3	d HX	9.6						
94.61.157.203	Transmission 2.93	d HXE	62.8						2.1 MB/s
175.137.147.211 [uTP]	qBittorrent/4.0.3	XP	0.0						
178.195.221.213	Transmission 2.92	ud XE	28.5						955.7 kB/s

هر فایل Torrent، شامل Seeder و Leecher است.

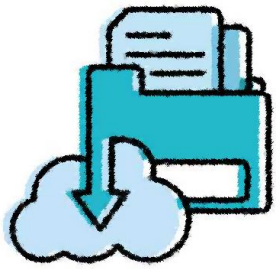
Seeder ها افرادی هستند که کامپیوتر خود را روشن گذاشته‌اند و از پهنای باند آنها برای Upload فایل‌ها و دانلود آنها توسط دیگران استفاده می‌شود.

Leecher ها افرادی هستند که در حال دانلود یک Torrent و فایل‌های آن از روی کامپیوتر Seeder ها هستند.

هنگامی که شما در سیستم Torrent شروع به دانلود می‌کنید، حتماً باید میزبان همان فایل برای Upload کردن آن باشید، به این معنی که هم Leecher هستید و هم Seeder.

مادامی که یک فایل خاص نزد کاربران ارزش دارد و افراد زیادی مشغول Seed کردن آن فایل هستند، سرعت دانلود آن فایل و بقای آن تضمین شده است. اما بعد از مدتی ممکن است یک فایل خاص (مثلا یک ویدئو، موزیک یا برنامه) محبوبیت خود را کم کم از دست بدهد، به این ترتیب، Seeder ها دیگر فضایی برای به اشتراک گذاری این فایل در اختیار شبکه قرار نمی‌دهند، در نتیجه این فایل و Torrent محو می‌شود.

سیستم Blockchain و چرخه بقای ارزهای دیجیتال را می‌توان به سیستم Torrentها مشابه کرد.



BLOCKCHAIN

Blockchain به عنوان Public Ledger یا دفتر حساب کتاب عمومی برای ارزهای دیجیتالی همچون Bitcoin (BTC)، Bitcoin Cash (BCH) و Ether (ETH) استفاده می‌شود و میزبان نقل و انتقالات این ارزها است.

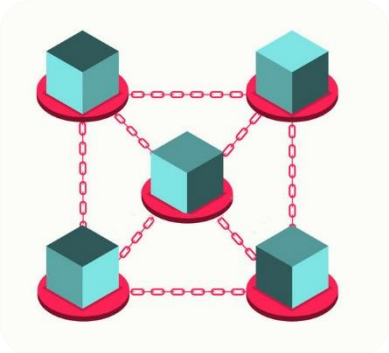
هر کامپیوتری که به شبکه Bitcoin وصل می‌شود، یک کپی از Blockchain دریافت می‌کند.

Blockchain محلی است برای ذخیره همه اطلاعات و ذره ذره Bitcoin ها (و دیگر ارزهای پشتیبانی شده). این سیستم، به عنوان پایگاه داده دائمی جهت نقل و انتقالات Bitcoin در دنیا عمل می‌کند. به عبارت دیگر، یک دفتر حساب است که تبادلات را به صورت Chronological (ترتیب زمانی) و همگانی ثبت می‌کند.

> معنی لغوی Blockchain برابر با "زنجیره‌ای از بلوک‌ها" است که در دنیای واقعی نیز همین عنوان را تداعی می‌کند.

کاربران Bitcoin می‌توانند چندین حساب کاربری داشته باشند که هیچ گونه مشخصاتی از کاربر (شامل اطلاعات شخصی مانند نام و غیره) در آنها ثبت نشده باشد. برای ایجاد حساب‌های کاربری نیازی نیست هزینه‌ای پرداخت کنید و همگی کاملاً رایگان هستند.

Block چیست؟



یک Block، بخش به روز شده Blockchain است که Transactionها (تراکنش‌ها) را ثبت می‌کند و به محض کامل شدن، به Chain (زنجیره) باز می‌گردد.

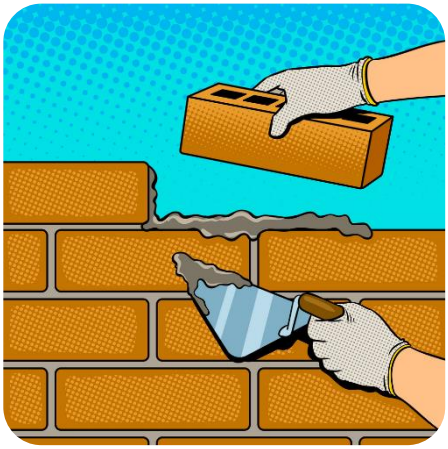
هر Block درون Chain به Block های دیگر به ترتیب زمانی Link شده است.

مشکل اصلی Blockchain اندازه (Size) بالای آن است.

DAG file

این فایل در ارزهایی که بر پایه EtHash هستند (مانند Ethereum) استفاده می‌شود و کاربرد آن اثبات کارکرد Miner است (POW – Proof of work). ارزی مانند Ether، به مرور زمان عمل Mining را با Memory بالاتر الزامی کرده است. به این ترتیب که با شکل گرفتن هر 30.000 بلاک، یک قطعه از اطلاعات (یک DAG) که برای Mine کردن بلاک‌های جدید لازم است، ایجاد می‌شود. هر گروه جدید از این 30.000 بلاک یک Epoch نامیده می‌شود و هنگامی که DAG بعدی Load شد، عمل Epoch Switch اتفاق می‌افتد.

DAG مخفف Directed Acyclic Graph است.



حجم فایل DAG رابطه مستقیم با GPU Memory دارد.

تا تاریخ نگارش این نوشتار، حجم DAG file ارز Ether معادل 2.85GB است. به این معنی که شما دیگر نمی‌توانید با یک کارت گرافیک ۲ گیگابایتی این ارز را Mine کنید.

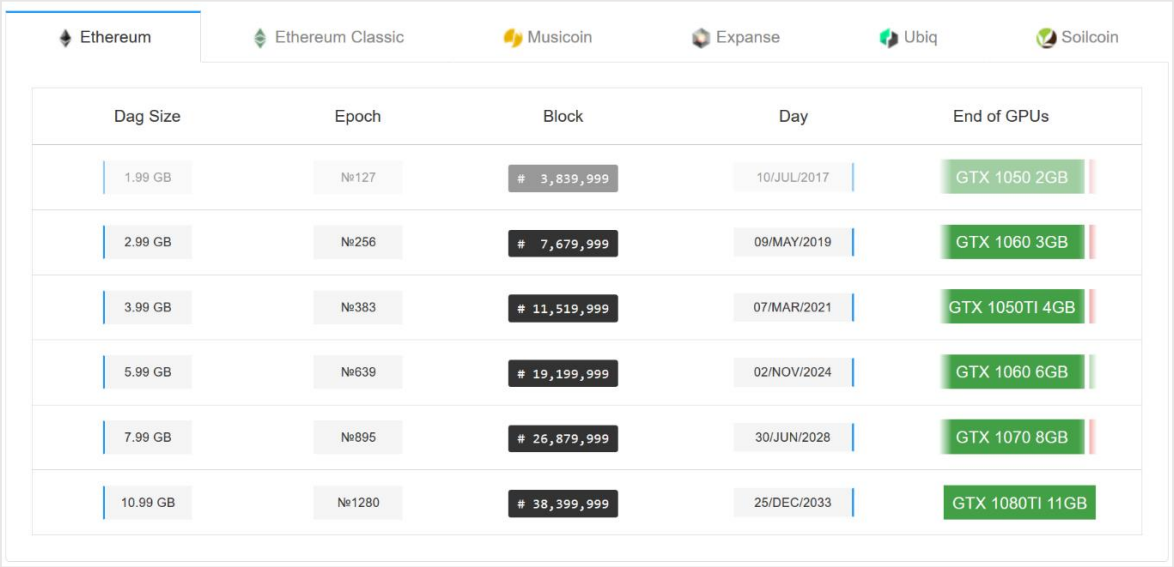
مانند شکل سمت راست، DAG file مثل یک دیوار با ارتفاع نامشخص است که لحظه به لحظه بلوک‌ها بر روی یکدیگر قرار می‌گیرند و این دیوار بالاتر می‌رود و بزرگتر می‌شود.

بدین ترتیب، اگر قبلاً شما با یک پله ۲ متری به بالای دیوار می‌رسیدید، اکنون که ارتفاع آن به ۳ متر رسیده، دیگر پله قبلی عملاً برای رسیدن به بالای این دیوار کارایی نخواهد داشت.

لینک زیر ارزهایی که وابسته به این فایل هستند را فهرست کرده و حجم فعلی DAG file را نشان داده است:

investoon.com

در وبسایت بالا، فهرستی از کارت گرافیک‌های مطرح بازار و تاریخ کنار رفتن آنها برای Mine کردن یکسری از ارزهای مطرح را می‌بینید:



همانطور که در تصویر بالا مشاهده می‌کنید، Ethereum را در فهرست بالا انتخاب کردیم و می‌بینیم که از تاریخ July/2017 کارت گرافیک GTX 1050 2GB دیگر برای Mine کردن این ارز قابل استفاده نیست.

عدد موجود در ستون Block نشان دهنده تعداد Block ایجاد شده تا آن تاریخ برای ارز انتخاب شده است که مستقیماً با حافظه کارت گرافیک و حجم DAG file در ارتباط است.

عدد موجود در ستون Block را اگر بر 30.000 (حجم یک Block) تقسیم کنید، مقداری که در ستون Epoch است به دست می‌آید. برای مثال:

$$\frac{7,697,999}{30,000} = 256,59$$

که نتیجه عدد بالا (256,59) معادل با مقدار Epoch ستون دوم در تصویر بالا است.

Transaction fee یا کارمزد تراکنش

تنها زمانی که از شما هزینه (و آن هم خیلی ناچیز) دریافت می‌شود، هنگام نقل و انتقال ارز دیجیتال است.

بستری که شما این نقل و انتقال را در آن انجام می‌دهید (برای مثال Blockchain)، به ازای هر Transaction یک Fee یا حق‌الزحمه در نظر می‌گیرد. این Fee در نهایت به عنوان پاداش برای Miner هایی که در تراکنش‌ها نقش داشته‌اند در نظر گرفته می‌شود.

پرداخت‌هایی که با ارزهای دیجیتال انجام می‌شود هیچ تفاوتی با کارت‌های اعتباری ندارد و همه به یک صورت است.

کیف پول یا Wallet

همانند حساب‌های بانکی که مختص شما هستند و سرمایه شما را نگه می‌دارند، ارزهای دیجیتال نیز از همین قاعده پیروی می‌کنند.

برای اینکه ارز دیجیتال خود را در یک مکان امن نگه دارید به یک حساب تحت عنوان Wallet یا کیف پول احتیاج دارید.

سرویس‌های متعددی وجود دارند که در این زمینه قابلیت‌های مختلفی نیز ارائه می‌دهند و با استفاده از آنها شما می‌توانید ارز دیجیتالی را که خریداری یا Mine کردید به آن Wallet واریز کنید.

Wallet به شما اجازه می‌دهد که کلیدهای دیجیتال (Digital Keys) که مختص هر Bitcoin (یا دیگر ارزهای دیجیتال) هستند را ذخیره کنید.

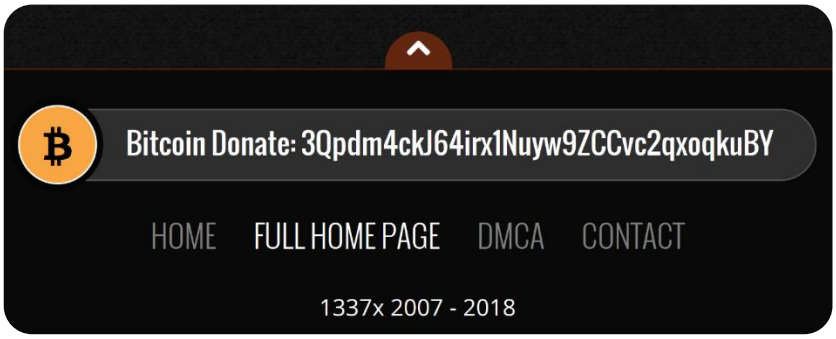
برای نمونه، Bitcoin Wallet شامل دو کلید است، یکی آدرس کیف پول شما که Public Key است، و دیگری Private Key شماست.

Public Key برای دریافت ارز دیجیتال به کار می‌رود.

Private Key برای ارسال ارز دیجیتال به کار می‌رود.

ما برای ارسال ارز، نیاز به Public Key شخص گیرنده داریم، دقیقاً مانند دستگاه خودپرداز بانک که به شماره حساب یا کارت جهت انتقال وجه نیاز است.

تصویر زیر، یک نمونه از وجه عمومی بودن Public Key را به ما نشان می‌دهد که مربوط به بخش زیرین وبسایت 1337x.to است که Public Key خود را در این بخش از سایت جهت اهدای کمک‌های مردمی قرار داده است:



انواع مختلف Wallet

Online Wallets: کیف پول‌های آنلاین به شما اجازه می‌دهند که Private Key ها را در محیط اینترنت ذخیره کنید. در نتیجه، در هر مکان و زمان به سکه‌های خود دسترسی خواهید داشت. مطرح‌ترین Online Wallet ها در زیر فهرست شده‌اند:

blockchain.info | coinbase.com | strongcoin.com | xapo.com

کیف پول xapo علاوه بر فضای اینترنت، از Cold Storage یا حافظه فیزیکی نیز برای ذخیره Private Key استفاده می‌کند.

Hot Storage یا Online Wallet به معنی استفاده از فضای اینترنت برای ذخیره کردن اطلاعات ارز دیجیتال است.

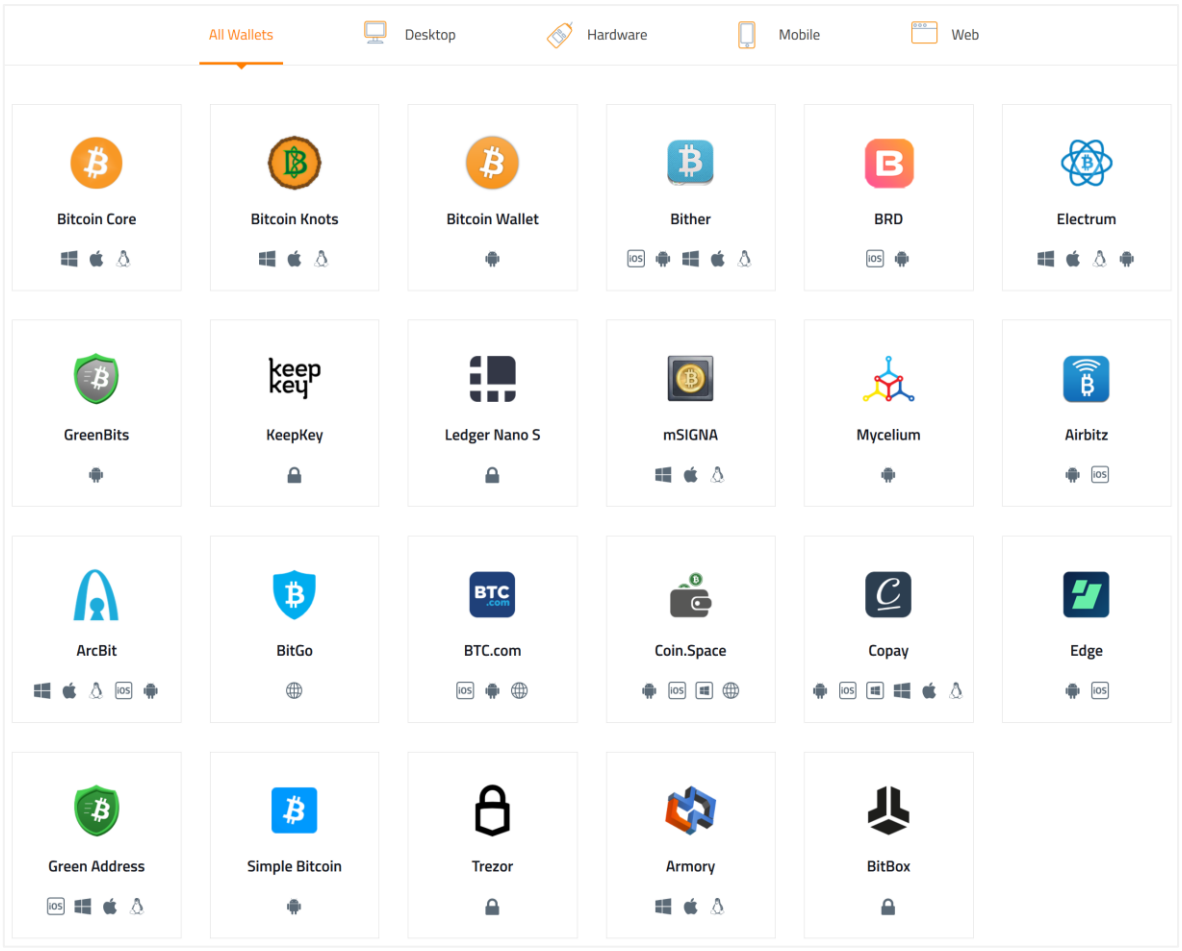
Cold Storage یا Offline Wallet به معنی نگهداری کیف پول و Private Key در محیط offline است (روی کامپیوتر offline یا روی کیف پول سخت افزاری). در شکل بالا یک نمونه Hardware Wallet می‌بینید.

هنگامی که با Online Wallet ها کار می‌کنید، بحث امنیت بسیار مهم است چرا که همیشه امکان به سرقت رفتن اطلاعات کاربر در فضای وب وجود دارد. Cold Storage ها به همین دلیل ارائه شدند تا امکان سرقت سرمایه و اطلاعات توسط هکرها به کلی از بین برود.

در لینک زیر، می‌توانید فهرستی از Wallet ها برای سیستم عامل‌ها و دستگاه‌های مختلف بیاید. همچنین توضیحات لازم در مورد هر کدام از این Wallet ها در این وبسایت داده شده است (شامل نقاط قوت و ضعف):

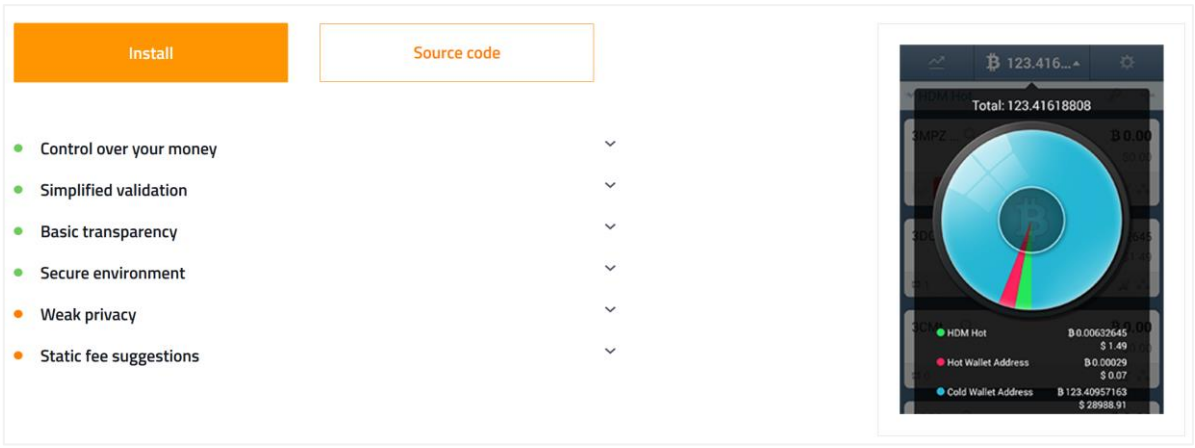
bitcoin.org

بعد از باز کردن لینک بالا، صفحه‌ای به شکل زیر برای شما باز می‌شود که در آن می‌توانید کیف پول مد نظر خود را بر اساس معیارهای مشخص شده (سیستم عامل، قابلیت‌ها) انتخاب کنید:



برای شروع، کافیست اشاره گر موس را مانند شکل زیر بر روی کیف پول و سیستم عامل مد نظر ببرید و کلیک کنید (در اینجا ما Bither را انتخاب کردیم):

با انتخاب سیستم عامل، به صفحه دانلود کیف پول هدایت می‌شویم. در این صفحه فهرستی از نقاط قوت و ضعف کیف پول برای ما لیست شده است. همچنین تصویری از محیط کیف پول را نیز می‌بینید:



همانطور که مشاهده کردید، سیستم عامل‌های مختلف برای کیف پول‌های مختلف در این وبسایت فهرست شده و توضیحات ضروری با زبان ساده برای ما ارائه شده است.

در ادامه انواع کلی Wallet که در وبسایت بالا وجود دارد را توضیح می‌دهیم.

Desktop Wallets: همانطور که در وبسایت مشاهده کردید، نوع دیگر کیف‌های پول مختص Desktop هستند که بر روی سیستم عامل نصب می‌شوند و شما می‌توانید با استفاده از آنها یک آدرس ایجاد کنید که تراکنش‌ها با آن انجام شود. برای نمونه، کیف پول Armory هنگامی که offline هستید، به شما قابلیت Cold-Storage هم می‌دهد.

Mobile Wallet هم نوع دیگری از Wallet است و کاربرد آن برای افرادی مناسب است که مدام در حال جابجایی هستند. کیف پول‌های همراه، حداقل قابلیت‌های مورد نیاز و ضروری را برای مدیریت کیف ارائه می‌دهند چرا که گوشی‌های همراه توانایی پردازش محدودی دارند. برخی از این کیف پول‌ها را در زیر فهرست کردیم:

wallet.mycelium.com | greenAddress.it | brd.com

Hardware Wallet، همان Cold-Storage است و می‌تواند بر روی کاغذ نیز چاپ شود که به مدل کاغذی آن Paper Wallet می‌گوییم. Paper Wallet چون دارای ماهیت فیزیکی است، Hardware Wallet توصیف می‌شود اما به صورت کلی هنگامی که از Hardware Wallet اسم می‌بریم، دستگاه‌های الکترونیکی ذخیره ارز دیجیتال مد نظر است.

شکل زیر یک نمونه Paper Wallet را نشان می‌دهد:

شکل زیر کیف پول سخت‌افزاری Ledger Nano S را نشان می‌دهد:

کیف پول Ledger Nano S، تقریباً از همه ارزهای مطرح برای ذخیره سازی پشتیبانی می‌کند.

ما می‌توانیم درون Flash Drive هایی (که به آنها Pen Drive، Thumb Drive هم گفته می‌شود) و مختص ارزهای دیجیتال هستند Private Key ها را ذخیره کنیم.

برای Paper Wallet، Private Address مان را بر روی کاغذ چاپ و هنگام استفاده، توسط QR Code آن را فراخوانی می‌کنیم.

توجه: Private Key ها آدرس یکتای مختص ارزهای دیجیتال شما هستند. اگر این آدرس‌ها به هر نحوی در دسترس دیگران قرار بگیرند، ارز شما ممکن است سرقت شود.

موارد امنیتی در رابطه با Wallet ها

رمزگذاری یا Encryption

یک رمز پیچیده برای Wallet خود انتخاب کنید. رمز پیچیده (متشکل از حروف، اشکال و اعداد) خود به تنهایی یک لایه محکم امنیتی برای Wallet شما ایجاد می‌کند. برای اینکه ببینید رمزی که انتخاب کردید چقدر امن است و چه مدت برای شکسته شدن آن زمان صرف می‌شود، از وبسایت زیر کمک بگیرید:

howsecureismypassword.net

همچنین می‌توانید از ابزارهای Password Generator مانند زیر استفاده کنید:

passwordsgenerator.net

ابزارهای متنوعی هم برای مدیریت رمزهای عبور وجود دارد که می‌توان برای جلوگیری از فراموشی رمز از آنها استفاده کرد:

Password Vault Manager

LastPass password manager

Dashlane

تهیه نسخه پشتیبان یا Backup

از محتوا نسخه پشتیبان تهیه کنید.

نه فقط در مبحث ارزها، بلکه برای همه فایل‌های ضروری و اطلاعات حیاتی، همیشه باید یک مکان ثانویه جهت ذخیره این اطلاعات در نظر گرفته شود و چه بهتر که در چند محل این کار را انجام دهیم.

Offline بودن یا Cold-Storage

همین که به اینترنت و دنیای ارتباطی متصل نباشید، همه تهدیدها از جانب افراد و نرم‌افزارهای مخرب و هکرها از بین می‌رود و این خود یک روش ایمن سازی است.

نصب یک Antivirus مطرح

حتماً و در تمام شرایط بدون وجود Antivirus کاری انجام ندهید چرا که اطلاعات حیاتی شما هر لحظه ممکن است در معرض خطر قرار گیرد. بدافزارها همیشه در کمین هستند و جوانب احتیاط همیشه باید در نظر گرفته شود. استفاده از یک ضد ویروس معتبر تا حد بسیار زیادی امنیت ما را تأمین می‌کند. مهم نیست که از کدام یک از ابزارها برای مبارزه با بدافزارها استفاده می‌کنید، مهم این است که "حتماً" از یکی استفاده کنید. برخی از ضد ویروس‌های مطرح شامل:

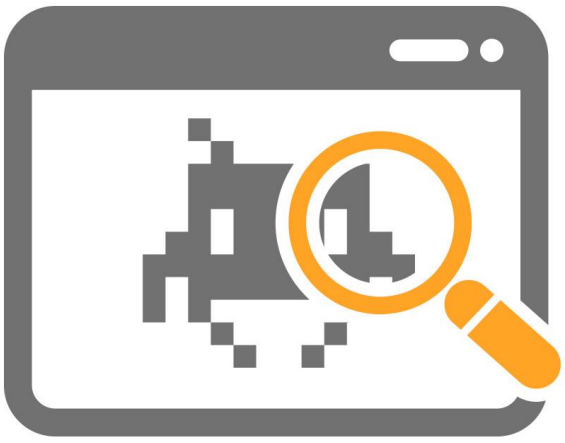
ESET Internet Security

Bitdefender

Kaspersky

Avira

تکیه به ابزار ضد ویروس Defender ویندوز به هیچ عنوان توصیه نمی‌شود و در صورتی که از Windows 10 استفاده می‌کنید، حتما ضد ویروس پیش فرض آن را با نصب یک ویروس‌کش معتبر جایگزین کنید.



ایجاد Paper Wallet

با ایجاد یک Paper Wallet، Public Key و Private Key شما به شکل QR Code بر روی کاغذ ذخیره خواهد شد و خطرات تحت وب به کلی از بین می‌رود. فراموش نکنید این کاغذ را لمینت کنید و از دسترس افراد حواس پرت دور نگه دارید!

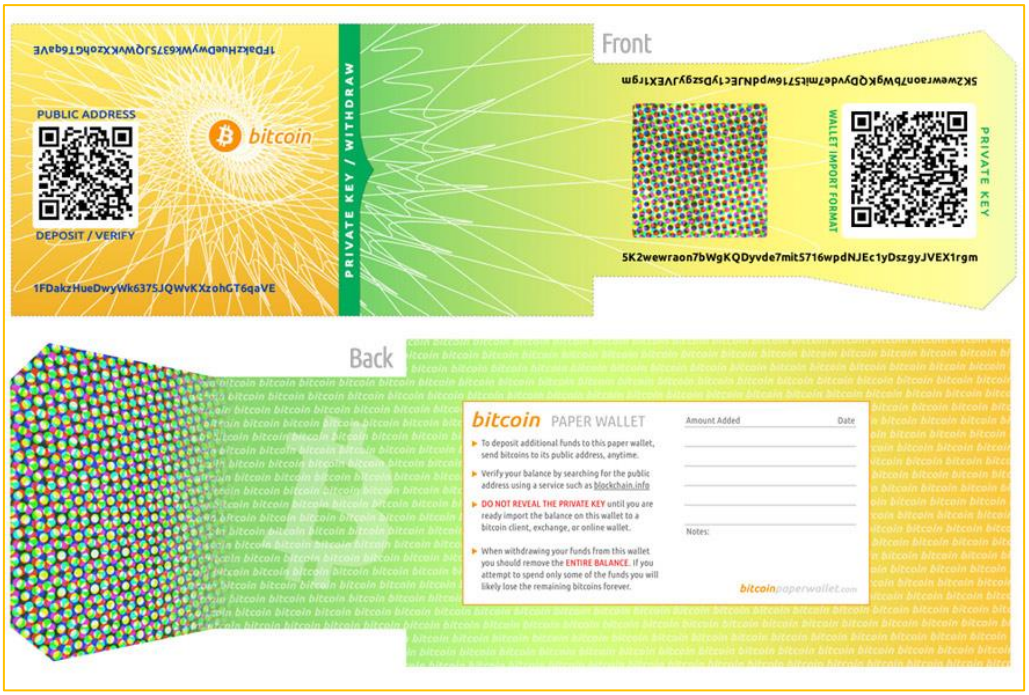
نحوه ساخت یک Paper Wallet (کیف پول کاغذی)

برای ایجاد یک Paper Wallet می‌توانید از bitaddress.org استفاده کنید. همچین وبسایت زیر سرویس ایجاد Paper Wallet را به خوبی به شما ارائه می‌دهد:

bitcoinpaperwallet.com

همچنین نحوه چاپ کردن Paper Wallet توسط این وبسایت، در این لینک در حدود ۹۰ ثانیه نشان داده شده است.

یک نمونه از Paper Wallet ایجاد شده توسط وبسایت BitcoinPaperWallet.com:



برای حفظ ایمنی Paper Wallet، آن را از دید دیگران مخفی نگه دارید و از دستگاهی آن را پرینت کنید که به شبکه یا کامپیوتر دیگری متصل نباشد.

انواع مختلف ارزهای دیجیتال می‌توانند بر روی Paper Wallet ذخیره شوند، البته این فرآیند برای ارزهای مختلف ممکن است اندکی متفاوت باشد.

چگونه از Paper Wallet چاپ شده استفاده کنیم؟

برای این منظور، نرم‌افزار Wallet خود را (که ممکن است Cold یا Hot) باشد را باز کنید و موجودی را به Public Address چاپ شده روی Paper Wallet ارسال کنید. بعد از این کار، از طریق وبسایت blockchain.info و در کادر جستجو، Public Key خود را وارد کنید و Enter بزنید. روند پیشرفت تراکنش در حال انجام به شما نشان داده خواهد شد.

چگونه پول‌های درون Paper Wallet را خرج کنیم؟

برای این منظور، باید از یک کیف پول Online (مثلاً trezor.io یا mycelium.com) یا Exchange Service (مثلاً coinbase.com) استفاده کنیم.

Wallet ها عموماً گزینه‌هایی مانند Import Private Key یا Spend یا Spend from Cold Storage دارند. این گزینه‌ها، به شما اجازه می‌دهد که Private Key مخفی شده در Paper Wallet را وارد کنید.

> توصیه می‌شود که همیشه کل موجودی Paper Wallet را جابجا یا خرج کنید و نه بخشی از آن را، چرا که به دلیل سیستم ایجاد Change Address (آدرسی که باقیمانده ارز در آنجا قرار می‌گیرد) این مقدار در حالت Offline و در Paper Wallet قابل دسترسی نیست. برای مثال، اگر 5BTC داشته باشیم، و 1BTC برای یک شخص ارسال کنیم، دیگر 4BTC در Paper Wallet ما نخواهد بود چرا که به یک Change Address جدید منتقل شده است.

تراکنش ها چگونه انجام می‌شود؟

همه جزئیات Bitcoin ها در Blockchain ذخیره شده است و مادامی که کلیدهای اختصاصی شما (Private Keys) ایمن باشند، جای نگرانی نخواهد بود. اگر قصد داشتید که به شخصی Bitcoin بفروشید، از کلید اختصاصی خود برای ارسال Bitcoin به کلید عمومی یا Public Address شخص مد نظر استفاده می‌کنید.

میزبانی همه این تراکنش‌ها (Transaction) توسط Miner ها انجام می‌شود.

روش‌های تهیه ارز دیجیتال

ساده‌ترین روش تهیه ارزهای دیجیتال مانند Bitcoin مراجعه به صرافی‌ها یا خرید مستقیم از فروشنده‌های مختص این ارزها است. وبسایت ir-xe.com یکی از وبسایت‌های معتبر داخلی برای خرید و فروش این ارزها است.

پرداخت‌ها جهت خرید Bitcoin عمدتاً از طریق کارت‌های اعتباری یا حساب‌های الکترونیکی همانند PayPal انجام می‌شود. مشکلی که اینجا وجود دارد، این است که در حین مبادله کالایی به صورت فیزیکی مبادله نمی‌شود، پس در صورت بروز اختلاف، اثبات وجود تراکنش مشکل خواهد بود. هر چند، این مشکل اکنون توسط سرویس‌های مختلف حل شده و برای تراکنش‌ها رسید دریافت می‌کنید.

هم اکنون در برخی کشورها (همانند بریتانیا و آمریکا) ATM های مخصوص ارزهای دیجیتال و Bitcoin وجود دارد:

بر خلاف قوانین بانک‌ها، تراکنش‌ها و تبادلات Bitcoin مشتمل قوانین مالی نیست. هیچ سازمان خاصی وجود ندارد که شما را از سرقت Bitcoin یا ارز دیجیتالی که دارید محفوظ کند، چرا که هنوز ارزهای دیجیتال تاکنون به عنوان یک ارز مرجع شناخته نشده‌اند.

برای تبادل Bitcoin، بهترین راه ملاقات حضوری شخص خریدار یا فروشنده است. هر چند این امر که کاملاً اینترنتی انجام می‌شود شاید ضروری به نظر نرسد، اما وبسایت زیر با پیدا کردن نزدیکترین صرافی ارز دیجیتال در کشورها (شامل ایران)، کار را ساده تر کرده است:

localbitcoins.com

همچنین این وبسایت نزدیکترین مرکز تبادل ارز دیجیتال را بر روی نقشه به ما نشان می‌دهد:

coinmap.org

برخی از شرکت‌های مطرح نیز همچون Microsoft، Amazon، Steam و Dell، ارز Bitcoin را برای تبادل قبول می‌کنند.

> اکثر بانک‌ها رشد ارزهای دیجیتال را یک تهدید برای تجارت خود می‌دانند، اما تا کنون بیش از صدها هزار فروشگاه در سر تا سر دنیا از Bitcoin برای تبادل استفاده می‌کنند.

شما می‌توانید ارز مد نظر خود را نیز Mine کنید. در بخش‌های بعدی در مورد Mining توضیح می‌دهیم.

چگونه ارز دیجیتال خود را بفروشیم؟

فروش ارز دیجیتال به آسانی خرید آن نیست. ما به روش‌های مختلف و به صورت آنلاین می‌توانیم Bitcoin خود را بفروشیم.
دقت داشته باشید، برای انتقال یک ارز دیجیتال به کیف پول شخص خریدار می‌بایست کیف پول دو طرف از ارز انتقالی پشتیبانی کند. برای مثال شما نمی‌توانید ارز Monero را به شخصی که در blockchain.info کیف پول ایجاد کرده بفرستید. برای این کار لازم است ابتدا ارز خود را به یکی از ارزهای پشتیبانی شده Exchange کنید و یا از خریدار بخواهید که کیف پول Monero ایجاد کند:

https://mymonero.com

> Blockchain Wallet تنها از ارزهای Bitcoin (BTC)، Bitcoin Cash (BCH)، Ether (ETH) و Stellar (XLM) پشتیبانی می‌کند.

فروش به صورت مستقیم روشی است که مستلزم تأیید هویت شخص فروشنده است. این تأیید هویت با ارائه اسکن یا عکس مدارکی همچون کارت شناسایی ملی، عکس شناسنامه، گواهینامه رانندگی، قبض (برق یا تلفن یا ...) صورت می‌گیرد.

در ایران، همانطور که پیش تر نیز گفته بودیم، می‌توانید از وبسایت زیر برای به مزایده گذاشتن ارز دیجیتال خود و فروش آن اقدام کنید. همچنین می‌توانید فروشندگان دیگر را نیز بیابید:

ir-xe.com

همچنین برای Exchange کردن یا تبدیل نوع ارز دیجیتال می‌توانید از سرویس‌های بین‌المللی زیر استفاده کنید:

coincorner.com | changelly.com

ممکن است این سوال پیش بیاید که چرا باید ارز دیجیتال خود را تبدیل کنیم؟ به دلیل نوسانات بازار ارزهای دیجیتال و ناپایداری ارزش برخی ارزها، بهتر است ارز دیجیتالی که در اختیار داریم را به یکی از ارزهای معتبر تر مانند Bitcoin تبدیل کنیم. به این ترتیب، نقل و انتقالات و تراکنش‌ها نیز برای ما ساده تر می‌شود.

اگر در این امر مبتدی هستید، بهتر است اولین تراکنش خود را به صورت حضوری انجام دهید.

سعی کنید مرتباً اطلاعات خود را در زمینه ارزهای دیجیتال به روز کنید. سخت افزارهای جدید، ارزهای جدید، نرخ ها، فرصت‌ها و تهدیدات جدید روز به روز با پیشرفت این حوزه بیشتر پدیدار می‌شوند.

Mining

Mining به پروسه "کشف" یا Discover کردن سکه‌ها یا ارزهای دیجیتال گفته می‌شود و رقابتی است بین دیگر Miner ها در سراسر دنیا. مسئولیت نظارت بر Blockchain و صحت و ثبت تراکنش‌هایی که روزانه انجام می‌شود نیز بر عهده Miner ها است.

هنگامی که یک Block برای تراکنش‌ها ایجاد می‌شود، Miner ها یکسری فرمول‌های ریاضی بر روی آن اعمال و آن را به چیزی تبدیل می‌کنند که به عنوان Hash شناخته می‌شود. Hash، یک سلسله از حروف و اعداد است که در آن Block ذخیره شده‌اند.

Miner ها از آخرین Block ذخیره شده در Blockchain برای تأیید قانونی بودن Chain استفاده می‌کنند. بدین ترتیب، اگر یک Hash دستکاری شده باشد، پس Block هم تحت تأثیر قرار می‌گیرد و تغییر می‌کند و این Hash دستکاری شده در Block بعد نیز در Blockchain نمایان خواهد بود.

کار Miner ها این هست که اگر چنین دستکاری در Hash انجام شده باشند، خبردار شوند و آن را به عنوان یک Hash جعلی شناسایی کنند. در نتیجه، ایجاد و تزریق یک تراکنش جعلی به Chain غیر ممکن است چرا که منجر به تغییر Hash می‌شود.

Miner ها بابت مهر و موم کردن Block ها به این طریق، درصدی از ارزی که آن را Mine کرده‌اند به عنوان پاداش یا Reward دریافت می‌کنند.

فرمول دریافت Reward یا پاداش به صورت زیر است:

```
Reward = ((Hashrate * Block_Reward) / Current_Difficulty) * (1 - Pool_fee) * 3600
```

اکثر ارزهای دیجیتال که قابل Mine شدن هستند، برای جلوگیری از جعل Hashing، از پروتکلی تحت عنوان POW (مخفف Proof of Work) استفاده می‌کنند که مشخص کننده زمانی است که یک دستگاه برای Mining اختصاص داده و آن را در محاسبه Reward مد نظر قرار می‌هند.

Hash Rate (HR) چیست؟

رقم HR در Mining بسیار مهم است. HR مشخص کننده تعداد محاسباتی است که سخت‌افزار شما می‌تواند در هر ثانیه انجام دهد.

HR از (Kilo Hash/Second) KH/s تا رقم‌هایی مانند (TH/s) متغییر هستند.

به کلام ساده، هر چه HR شما بیشتر باشد، سریع‌تر معادلات ریاضی مورد نیاز را برای تکمیل تراکنش یک Block انجام می‌دهید و سود بیشتری نصیبتان می‌شود.

> در برخی ارزها به جای Hash Rate از Solution استفاده و به اینصورت Sol/s نشان داده می‌شود.

Mining Pool

شما می‌توانید به تنهایی اقدام به Mine کردن کنید یا به یک Pool یا استخر متصل شوید. Mine کردن به تنهایی ممکن است حتی یکسال طول بکشد و حتی چیزی به دست نیاورید.

در این میان، نرم افزار Minergate GUI به صورت خودکار شما را به یکی از Pool ها متصل می‌کند. اما اگر از نرم‌افزارهای Console Miner استفاده می‌کنید لازم است به صورت دستی Pool را تعریف کنید:

multipool.us

در وبسایت بالا، شما به صورت لحظه‌ای می‌توانید سودآورترین ارزها را برای Mining بیابید (که البته این امر رابطه مستقیم با حجم Pool ارائه شده توسط این وبسایت نیز دارد).

هنگامی که وارد یک Pool می‌شوید، بخشی از مقدار Mine شده به عنوان Pool Fee یا کمیسون از شما کسر می‌شود. این مقدار بستگی به Input یا ورودی دیگر کاربران به Block دارد.

در بخش‌های بعد مرور کوتاهی بر نرم‌افزارهای Mining خواهیم داشت.

Difficulty

مورد دیگر که در هنگام Mining با آن برخورد می‌کنیم، Difficulty است. این فاکتور مشخص کننده درجه سختی حل مسائل ریاضی در یک Block است.

Mining پروسه حل مشکلات الگوریتمی است و هر ارز، سطح سختی مختص خود را دارد.

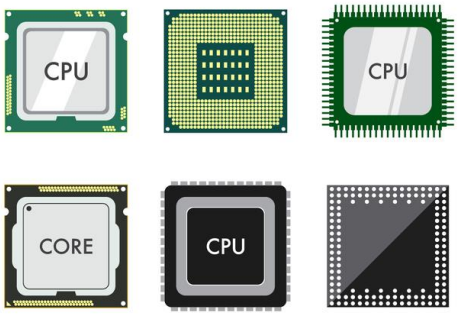
هر Mining Pool دارای یک Difficulty Rate بین ۱ تا مقدار مشخص شده توسط ارز است. بسته به تعداد Miner ها این رقم نیز کاهش/افزایش پیدا می‌کند و با افزایش این رقم، شما نیاز به سخت‌افزار قوی‌تری برای Mining خواهید داشت.

در این میان، Share سهمی است که میان Miner های درون Pool تقسیم می‌شود و ملاکی است برای اثبات کارکرد سخت‌افزاری کاربر (POW => Proof of Work).

سخت افزارهای مورد نیاز برای Mining

به طور کلی ما با سه نوع سخت افزار می‌توانیم ارزهای دیجیتال را Mine کنیم. هر چند، برخی ارزهای دیجیتال که جدیداً معرفی شده‌اند یا مربوط به سازمان‌های خاص هستند ممکن است قابل Mine کردن نباشند. البته همه ارزهای مطرح را می‌توان با سخت افزار مناسب Mine کرد.

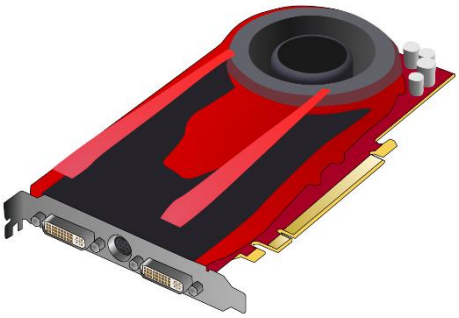
CPU یا پردازنده مرکزی



بسته به نوع ارز دیجیتال و الگوریتم آن، شما می‌توانید برخی از آنها را با CPU به تنهایی Mine کنید. برخی ارزها را فقط با CPU می‌توان Mine کردو برخی هم با CPU به خوبی Mine می‌شوند (برای مثال AEON Coin). سرعت پردازش Mining با CPU بسیار کمتر از سخت‌افزارهایی همچون کارت گرافیک و ASIC Miner است.

برای Mining در ابتدا از CPU استفاده می‌شد، اما توسعه دهنده‌های ارزهای دیجیتال بعداً متوجه شدند که کارت‌های گرافیکی قدرت پردازش چند برابری در حل محاسبات ریاضی ارزهای دیجیتال ارائه می‌دهند.

GPU یا کارت گرافیک



بهترین گزینه برای Mining در حال حاضر، کارت‌های گرافیک هستند. هم از لحاظ قیمت و هم از لحاظ قدرت پردازشی که ارائه می‌دهند می‌توان آنها را گزینه مناسبی برای Mining دانست.

هر چند، در سال گذشته به دلیل سرمایه گذاری بسیاری از افراد در سرتاسر دنیا برای Mining، قیمت کارت گرافیک درصد زیادی افزایش پیدا کرد. این افزایش نرخ در ایران در برخی مدل‌های کارت گرافیک چندین برابر بود.

از آنجایی که در یک دوره زمانی، خریداران زیادی کارت گرافیک تهیه کردند و می‌توان گفت بازار به یک آرامش نسبی رسیده است، و همچنین با ورود موج جدیدی از مدل‌های رده بالا و متنوع کارت گرافیک، قیمت‌ها کم کم در حال کاهش پیدا کردن هستند. همچنین کارت گرافیک‌های دست دوم رده بالای زیادی در مدت کوتاه موجود خواهد بود که خود این امر باعث کاهش تقاضا و قیمت نهایی کارت‌های گرافیک خواهد شد.

ASIC Miner

مدال طلای المپیک Mining را باید به ASIC Miner داد. ASIC مخفف Application Specific Integrated Circuits است و فقط برای یک هدف طراحی شده‌اند: Mine کردن Bitcoin و Litecoin با بالاترین سرعت. هر دوی این ارزها از یک الگوریتم مشابه استفاده می‌کنند بنابراین این دستگاه محدود به Mine کردن ارزهای دیجیتالی است که از الگوریتم Bitcoin تبعیت می‌کنند.

قیمت این دستگاه‌ها بالا است، اما اگر به دنبال سودآوری در بلند مدت هستید، ASIC Miner بهترین گزینه است.

سرعتی که ASIC Miner ها می‌توانند ارائه دهند تا تاریخ این نوشتار از محدوده 5TH تا 44TH متغییر است. لازم به ذکر است که این دستگاه‌ها سر و صدای زیادی تولید می‌کنند، بنابراین استفاده از آنها در منزل ممکن است باعث سلب آسایش شود!

در زیر، سه مدل ASIC Miner از مدل‌های پر طرفدار در بازار را می‌بینید:

Ant Miner S9 (13~14TH)

AvalonMiner 821 (11TH)

DragonMint (16TH)

TH مخفف Tera Hash است. به این معنی که در هر ثانیه چه مقدار Hash پردازش می‌شود. برای درک بهتر این موضوع جدول زیر را ببینید:

معرف	مقدار
Hash	1
KiloHash	1.000
MegaHash	1.000^2
GigaHash	1.000^3
TeraHash	1.000^4

نکاتی در رابطه با سخت‌افزارهای Mining

در حال حاضر کارت گرافیک عمومی‌ترین سخت‌افزار برای Mining به شمار می‌رود چرا که تهیه و راه اندازی آن ساده است و محدود به استخراج سکه (ارز) خاصی نیست. شما در هر زمان می‌توانید هر سکه‌ای که مد نظرتان بود را Mine کنید.

در نظر داشته باشید که تنها کارت گرافیک‌های رده بالا برای Mining مناسب و به صرفه هستند. شما با یک یا دو کارت گرافیک، سود بسیار کمی به دست خواهید آورد و این اقدام در نهایت به صرفه نخواهد بود.

مدل‌های مختلف کارت گرافیک، HR های متفاوتی ارائه می‌دهند. برای دیدن فهرستی از HR کارت گرافیک‌ها می‌توانید به لینک‌های زیر بروید:

miningchamp.com | cryptomining24.net | whattomine.com

همچنین در این وبسایت HR مربوط به ارز Monero را در سخت‌افزارهای مختلف می‌بینید:

monerobenchmarks.info

> به جز ارزهایی که بر اساس الگوریتم Ethash هستند، دیگر ارزها دارای DAG file نیستند.
>
> ارزهایی که DAG file دارند، قابل Mine شدن با ASIC Miner نیستند.

بسته به نوع سیستم عامل و قدرت دیگر سخت‌افزارهای جانبی مانند RAM و CPU، سرعت HR ممکن است درصدی متفاوت باشد. روش‌های مختلفی برای بالابردن عدد HR وجود دارد که شامل:

- تأمین دمای مناسب با کنترل سرعت Fan کارت گرافیک و نصب خنک کننده‌های جانبی

- گردگیری و تمیز نگه داشتن قطعات الکترونیکی، از گرم شدن و در نتیجه مصرف برق بیشتر جلوگیری می‌کند (می‌توان با استفاده از Spray یا Blower گردگیری را انجام داد)
- Over Clock کردن کارت گرافیک و افزایش فرکانس مرجع در افزایش بازدهی تأثیر دارد*.

کارت‌های گرافیکی که از Over Clock پشتیبانی می‌کنند معمولاً در انتهای نام آنها دو حرف OC به معنی Over Clocked می‌بینید. مثلاً: GTX 1060 6GT OCV2

- به روز کردن BIOS مادربورد (Motherboard) برای ارتقاء بهره وری قطعات نصب شده بر روی آن
- استفاده از اینترنت با اتصال پایدار و Latency پایین*

برای بررسی میزان سرعت و Latency سرویس دهنده اینترنت خود می‌توانید از وبسایت speedtest.net کمک بگیرید.

- استفاده از نرم‌افزار مناسب Mining
- استفاده از جدیدترین درایورهای منتشر شده کارت گرافیک*

شرکت‌های تولید کننده GPU (AMD و Nvidia) در به روزترین نسخه از درایورهایی که ارائه داده‌اند، قابلیت‌هایی برای بهینه‌سازی Mining به درایورها و ابزارهای جانبی همراه آنها اضافه کرده‌اند. نسخه مجزای درایور AMD تحت عنوان Blockchain Driver و با نام Adrenalin Driver نیز منتشر شده است.

مصرف برق دستگاه‌های Mining را فراموش نکنید! از آنجایی که از حداکثر توان کارت‌های گرافیکی یا ASIC Miner ها استفاده می‌شود، بهتر است قبل از تهیه هر گونه سخت‌افزار Mining، ابتدا قدرت پردازشی یا Hash Rate آن را به دست بیاورید، سپس با استفاده از لینک‌های زیر میزان سود یا ضرر را در روز، هفته، ماه و سال محاسبه کنید:

cryptocompare.com

minergate.com

در وبسایت cryptocompare.com و این لینک نیز فهرستی از تجهیزات و میزان قدرت و مدت زمان بازگشت سرمایه را می‌بینید.

وبسایت‌های بالا بر اساس نرخ روز یکسری از ارزهای مطرح، برای شما کار محاسبه سود یا زیان را راحت کرده است.

همچنین برای Mining Rig که با کارت گرافیک ایجاد شده است، حتماً از Power های مرغوب Modular با ظرفیت بالا استفاده کنید. نمونه یک Modular Power:

GREEN GP1200B-OC

از مزیت‌های Power های Modular این است که اتصالات برای هر قطعه به صورت جدا وصل می‌شوند و به ما امکان چیدمان مناسب کابل‌ها را می‌دهد.

همچنین می‌توانید از دستگاه‌های نمایش میزان مصرف برق و محافظ برق استفاده کنید که میزان مصرفی را به شما نشان دهد:

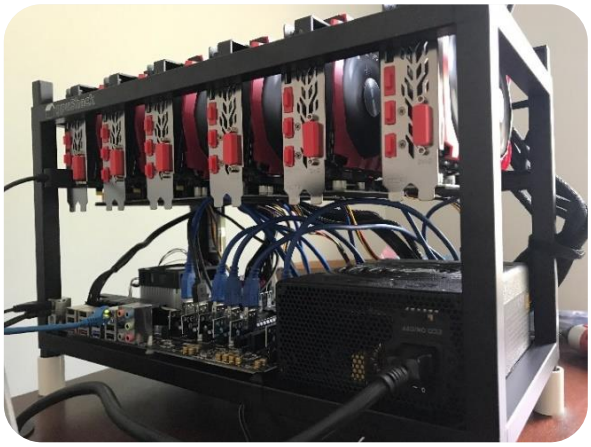
Terotec BX11

استفاده از UPS را جهت روشن نگه داشتن تمام وقت Mining Rig خود فراموش نکنید!

Mining Rig

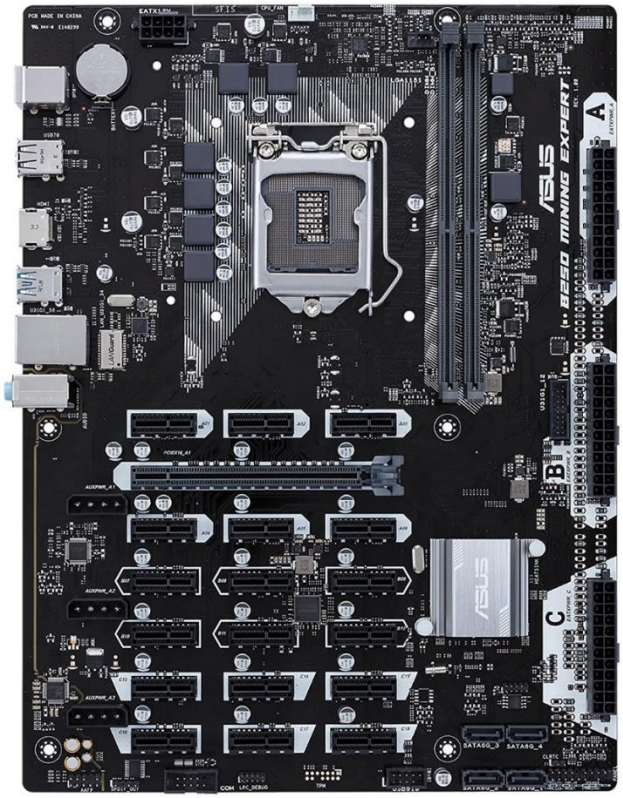
با سرمایه‌گزاری بالایی که اکثر مردم بر روی Mining انجام دادن، شرکت‌های تولید کننده سخت‌افزار به فکر طراحی ابزارهای جانبی متنوعی برای راحت تر کردن کار Miner ها شدند تا توانایی محاسباتی برای کامپیوترهای خانگی قابل افزایش باشد.

از آنجایی که Case های معمولی و اندازهٔ آنها جوابگوی کارت گرافیک به تعداد زیاد نیست، Frame هایی به عنوان Mining Rig معرفی شدند که در واقع چیزی جز یک چارچوب فلزی یا چوبی نیست. ساختار آن مشابه یک Case بدون درب و با مقیاس بزرگتر جهت متصل کردن تعداد بالای کارت گرافیک و Power است. چند نمونه Rig را در شکل‌های زیر می‌بینید:



قطعاتی که برای راه اندازی Rig ها معرفی شدند شامل Motherboard هایی با تعداد زیاد شکاف (Slot) های PCIe برای نصب کارت گرافیک هستند. شکل زیر یکی نمونه از این Motherboard ها را نشان می‌دهد:

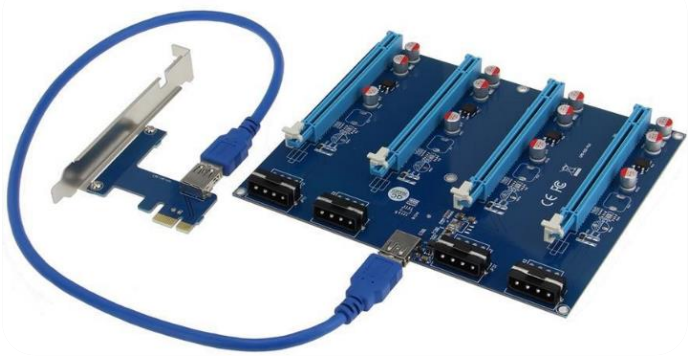
ASUS B250



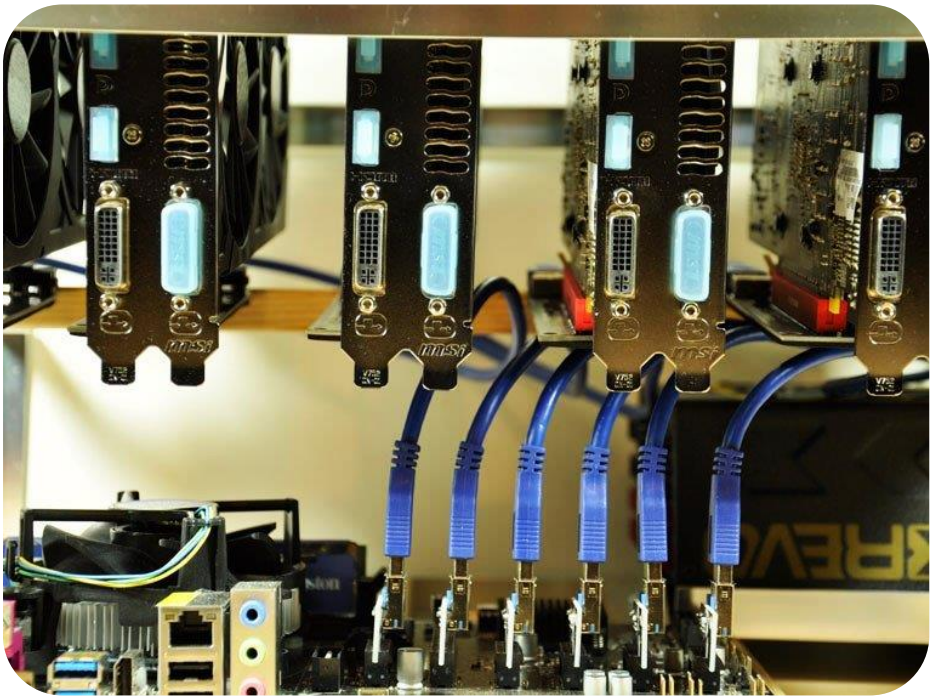
همانطور که می‌بینید، سه درگاه برای اتصال سه عدد Power به این Motherboard تعبیه شده است. همچنین ۱۸ عدد شکاف PCIe x1 و ۱ عدد PCIe x16 برای آن تعبیه شده که حداکثر اجازه نصب ۱۹ عدد کارت گرافیک را به ما می‌دهد.

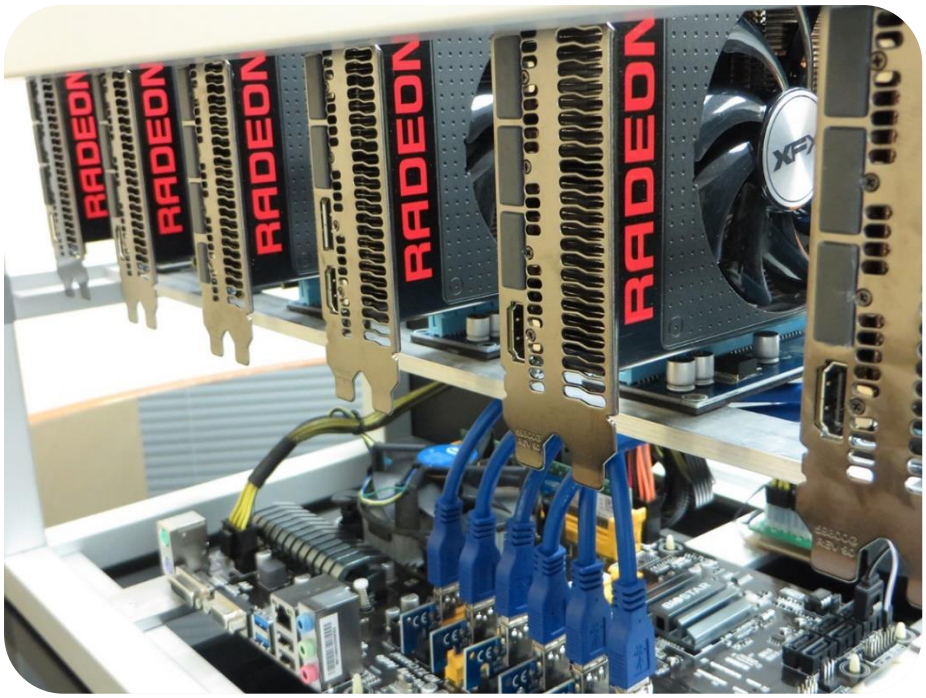
بین شکاف‌های PCIe 1x و PCIe x16 در کارت گرافیک‌های رده بالا تفاوت محاسباتی ناچیزی (تقریباً ۰) وجود دارد.

این سوال پیش می‌آید که چگونه می‌توان ۱۹ کارت گرافیک را به این Mainboard وصل کرد؟ اینجاست که پای قطعه‌ای به نام PCIe x1 Riser به میان میاید:



همانطور که در شکل‌های بالا می‌بینید، Riser Card درون شکاف PCIe 1x مادربورد قرار می‌گیرد و با استفاده از یک کابل USB 3.0 به Board خروجی Riser متصل می‌شود. این Board خروجی به ما اجازه نصب کارت گرافیک‌های اضافی را می‌دهد. نمونه استفاده از این کارت را در شکل‌های زیر می‌بینید:





نبایدها در سخت‌افزار و Mining

هیچگاه از دستگاهی مانند Laptop برای Mining استفاده نکنید. از دستگاه‌هایی که توان پردازشی پایین دارند نیز برای این کار استفاده نکنید.

دستگاهی مثل Laptop حتی اگر چند میلیون قیمت داشته باشد، توان پردازشی مناسب برای Mining را ارائه نمی‌دهد و سیستم خنک کنندگی آن نیز جوابگوی Mining نیست. این کار ممکن است منجر به آسیب رساندن به دستگاه یا مستهلک شدن آن شود.

هنگامی که Mining با یک دستگاه (یک کامپیوتر برای مثال) شروع می‌شود، شما عملاً هیچ کار دیگری نمی‌توانید انجام دهید چرا که تمام توان سخت‌افزاری سیستم برای امر Mining صرف می‌شود. شکل زیر درصد استفاده از CPU و GPU را در یک سیستم با دو کارت گرافیک در حال Mining ارز Monero (XMR) نشان می‌دهد:

Name	100% CPU	18% Memory	0% Disk	21% Network	54% GPU
minergate	85.5%	175.9 MB	0.1 MB/s	0 Mbps	0%

همانطور که می‌بینید CPU به طور کامل (100%) در حال استفاده است و همچنین کارت گرافیک 54% مشغول کار است. در این حالت، عملاً سیستم برای انجام هر کار دیگری بسیار کند عمل می‌کند.

این نکته جای تعجب دارد که برخی از توسعه دهنده‌های نرم‌افزارهای Mining، برای موبایل‌ها هم نسخه‌ای ارائه داده‌اند. Mining با دستگاه ضعیفی مانند موبایل فقط می‌تواند آسیب رسان باشد و هیچ سودی ندارد.

بنابر این می‌توان گفت زمانی که گوشی یا لپ تاپ شما بدون اجازه در حال Mining باشد، فقط یک دلیل وجود دارد، و آن این است که به بد افزار آلوده شده باشید.

نرم‌افزارهای Mining

ما علاوه بر سخت‌افزار، به نرم‌افزار مناسب جهت Mining نیز احتیاج داریم. نرم‌افزارهای Mining بر روی سیستم عامل‌های مختلف قابل اجرا هستند و نسخه‌های مناسب برای هر سیستم عامل را می‌توانید از سایت‌های مربوطه دانلود کنید. کار با این نرم‌افزارها بسیار ساده است.

این نرم‌افزارها در دو نوع GUI (Graphical User Interface) و Console Miner توسعه یافته‌اند.

نرم‌افزارهای GUI رابط کاربری ساده‌ای را در اختیار ما قرار می‌دهند و ما با چند کلیک ساده آنها را راه‌اندازی می‌کنیم.

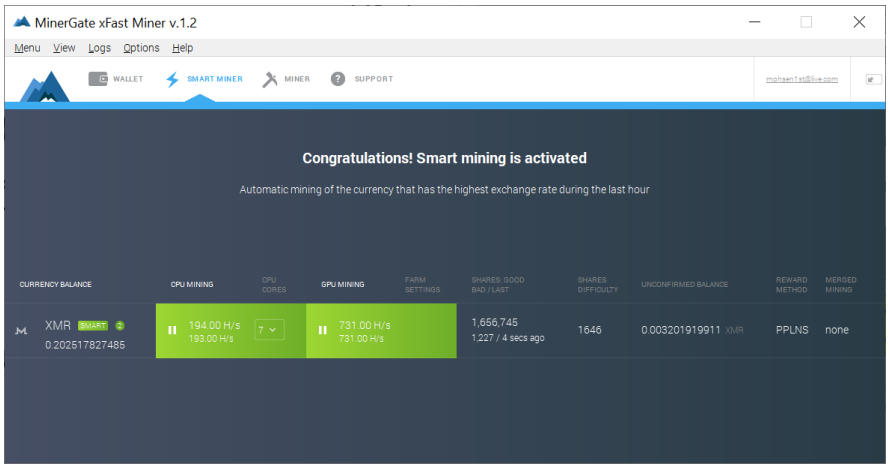
نرم‌افزارهای Console از یک رابط فقط نوشتاری مانند CMD ویندوز استفاده می‌کنند که ما باید دستورات مد نظر را تایپ کنیم و یکسری تنظیمات خاص را در فایل‌های مربوطه انجام دهیم.

راه‌اندازی نرم‌افزارهای Miner در وبسایت مرجع آنها به طور کامل شرح داده شده است.

در ادامه ما چند نرم‌افزار مطرح برای Mining معرفی می‌کنیم.

Minergate xFast

این نرم‌افزار که بر روی سیستم عامل‌های مختلف قابل نصب است به ما اجازه می‌دهد که بدون هیچ گونه تنظیمات خاصی مستقیماً Mining ارز مد نظرمان را از ۸ ارزی که این ابزار پشتیبانی می‌کند انجام دهیم. تصویری از محیط این نرم‌افزار را در شکل زیر می‌بینید:



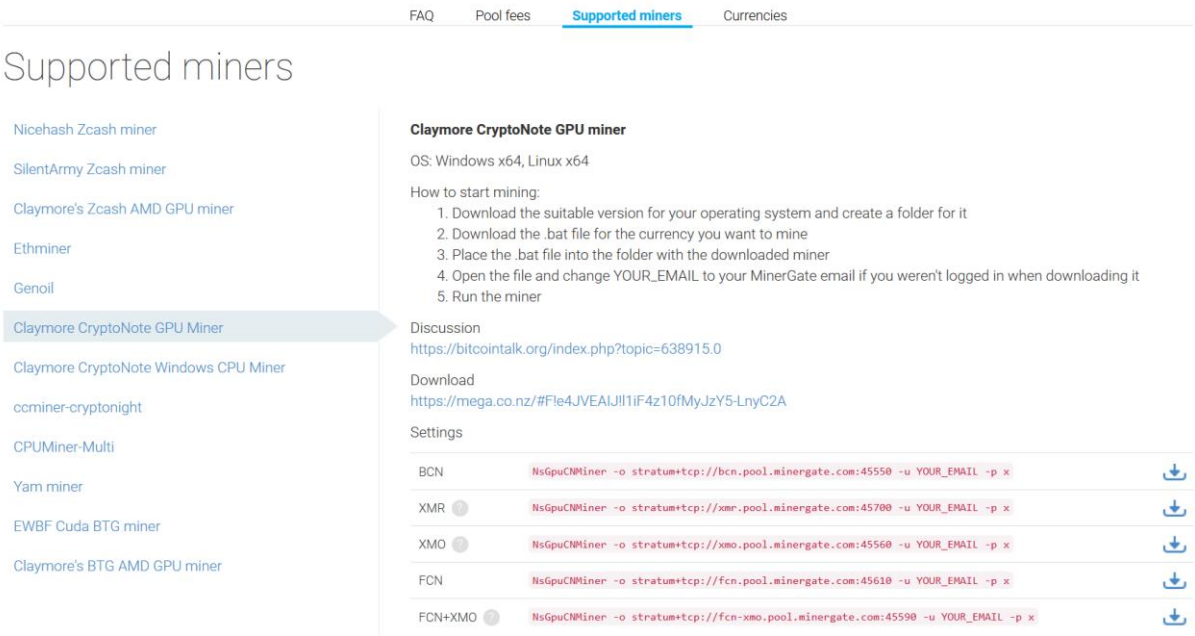
برای اینکه با این نرم‌افزار شروع به استخراج ارز کنید، ابتدا لازم است در وبسایت minergate.com یک حساب کاربری داشته باشید که در واقع کیف پول شما نیز خواهد بود. سپس نرم‌افزار Minergate مخصوص سیستم عاملی که دارید را از همان وبسایت دانلود و Login کنید، سپس با کلیک بر روی Smart Miner می‌توانید به صورت خودکار ارزی که بیشترین نرخ تبادل را داشته است، Mine کنید.

در بخش Downloads وبسایت minergate.com نسخه‌های قدیمی تر این ابزار به همراه چندین Console Miner جهت دانلود وجود دارد.

~~Console Miner ها از GUI Miner ها سریعتر هستند~~؛ این گفته کاملاً اشتباه است و حتی اکثر افرادی که برای مدت‌ها Miner هستند اعتقاد دارند که ابزارهای گرافیکی برای Mining کند عمل می‌کنند.

هیچ اختلافی در سرعت Mining با این ابزارها وجود ندارد، تنها مواردی که باید در نظر گرفت این است که ما برای ارز مد نظر از Miner، استخر و تنظیمات مناسب استفاده کنیم و نه هر نرم‌افزاری که قابلیت Mine کردن به ما می‌دهد. از آنجایی که اکثر ابزارهای Mining به صورت Console Miner ارائه شده‌اند، این تفکر که Console Miner ها بهتر هستند شکل گرفته است.

وارد بخش Downloads در وبسایت minergate.com شدیم، در انتهای صفحه بر روی Alternative Miners کلیک می‌کنیم و به صفحه زیر هدایت می‌شویم:



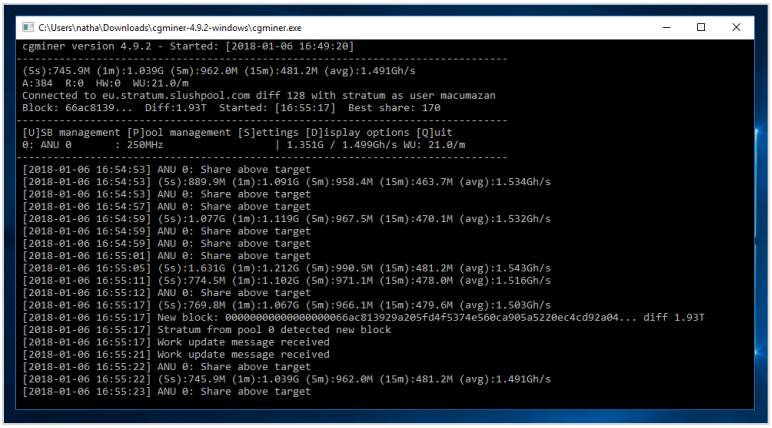
در تصویر بالا و در قسمت قرمز رنگ، تنظیماتی را می‌بینید که باید به صورت دستی وارد شود، اما اگر در minergate.com وارد حساب کاربری خود شده باشید، بخش Email این تنظیمات برای شما به صورت خودکار پر شده است و تنها کافیست با کلیک بر روی دکمه آبی رنگ دانلود در جلوی ارز مد نظر (دکمه دانلود روبروی سطر قرمز رنگ)، فایلی که دانلود کردید را در کنار نرم‌افزار Console Miner قرار دهید.

نرم‌افزارهای Claymore، EasyMiner و BFGMiner نیز از ابزارهای محبوب Miner ها است. توضیحات جزئی تنظیمات ابزارها در این مقاله نمی‌گنجد، لذا منابعی در انتهای مقاله جهت سهولت خواننده مطلب آورده شده است.

فراموش نکنید که اینترنت پایدار برای Mining الزامی است. سرعت اینترنت مهم نیست، مصرف اینترنت نیز برای Mining بالا نیست، تنها یک ارتباط پایدار مورد نیاز است.

CGMiner

این ابزار یکی از Miner های مطرح است که تقریباً بر روی همه سیستم عامل‌ها اجرا می‌شود. از مزایای آن این است که تا حد بسیاری قابل خصوصی سازی است و حتی جزئی‌ترین تنظیمات سخت افزاری را می‌توان تغییر داد. هر چند، راه اندازی این Miner مقداری پیچیده تر از انواع GUI است. در تصویر زیر نمایی از این Miner می‌بینید:

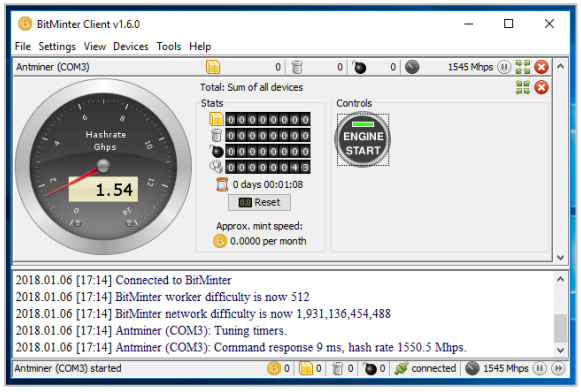


برای دانلود CGMiner از لینک زیر اقدام کنید:

ck.kolivas.org

Bitminter

این نرم‌افزار از یک شمایل GUI برای Mining بهره می‌برد و تنظیمات آن ساده است. همانند Minergate، ابتدا لازم است که از طریق وبسایت این ابزار اقدام به ایجاد حساب کاربری و شروع به Mine کردن کنید. Mining فقط از طریق Pool های این وبسایت امکان پذیر است. تصویری از محیط این ابزار در شکل زیر می‌بینید:



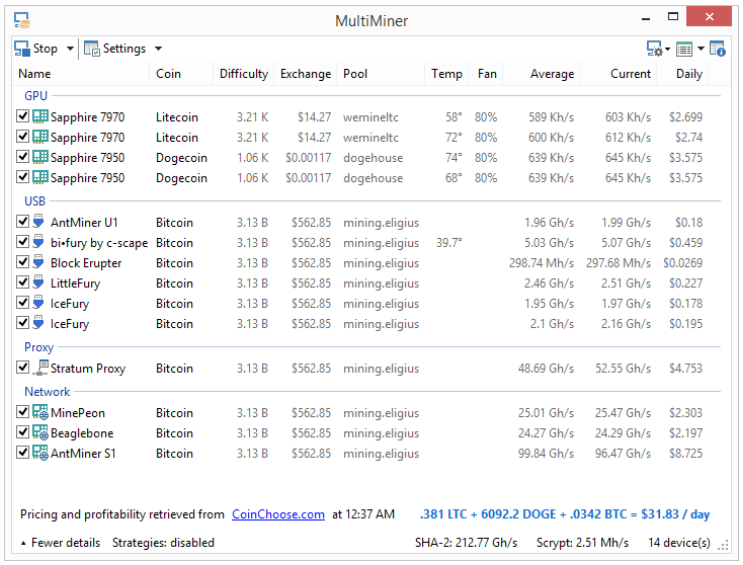
برای دانلود و ایجاد حساب کاربری در این ابزار به وبسایت زیر مراجعه کنید:

bitminter.com

MultiMiner

این ابزار نیز یکی از ابزارهای گرافیکی و قدرتمند برای Mining است. راهنمای متنی برای لغات نا آشنا توسط Tooltip ها، مراحل راه اندازی قدم به قدم و مدیریت چندین دستگاه Mining از توانمندی‌های این ابزار است. این ابزار پس از نصب، به سادگی به شما این امکان را می‌دهد که دستگاه‌های Miner را جستجو کنید و مشخصات Pool ها را بیابید.

تصویری از محیط این ابزار را در شکل زیر می‌بینید:



برای دانلود این ابزار و اطلاعات بیشتر به وبسایت زیر مراجعه کنید:

multiminerapp.com

امنیت

ارز دیجیتال، سرمایه و کالای ارزشمندی است. بنابراین، تهدیدات و روش‌های سرقت روز به روز به شکل‌های مختلف برای به دست آوردن سرمایه دیگران توسط افراد خرابکار صورت می‌گیرد.

علاوه بر رعایت مسائل کلی امنیتی همچون:

- استفاده از یک ویروس کش معتبر و به روز نگه داشتن آن
- عدم باز کردن لینک‌های ناشناس و اجرای فایل‌های ناشناس در هر محیطی (مثلاً Telegram یا در محیط Email)
- عدم به اشتراک گذاری اطلاعات مهم از طریق اینترنت
- استفاده از رمزهای پیچیده

یکی از روش‌هایی که با توسعه ارزهای دیجیتال نیز همه گیر شده است، Cryptojacking نام دارد. این روش، از منابع سخت افزاری سیستم شما بدون اینکه اطلاع داشته باشید برای Mine کردن ارز دیجیتال استفاده می‌کند.

عمومی‌ترین حالت Cryptojacking زمانی است که شما در مرورگر خود مشغول تماشای یک وبسایت هستید، ممکن است متوجه شوید که سرعت سیستم افت پیدا کرده و صدای Fan های درون Case شنیده می‌شود.

برای اینکه از این موضوع مطمئن شویم، با اجرای Task Manager ویندوز و مشاهده Process ها، می‌توانیم بفهمیم که چه نرم‌افزاری منابع بیشتری را اشغال کرده است.

در شکل زیر، چند وبسایت با مرورگر Firefox باز شده است که می‌بینیم یکی از وبسایت ها 2.7% از کارت گرافیک را به خود مشغول کرده است! این وبسایت، در حال Mining از سیستم به صورت مخفیانه است:

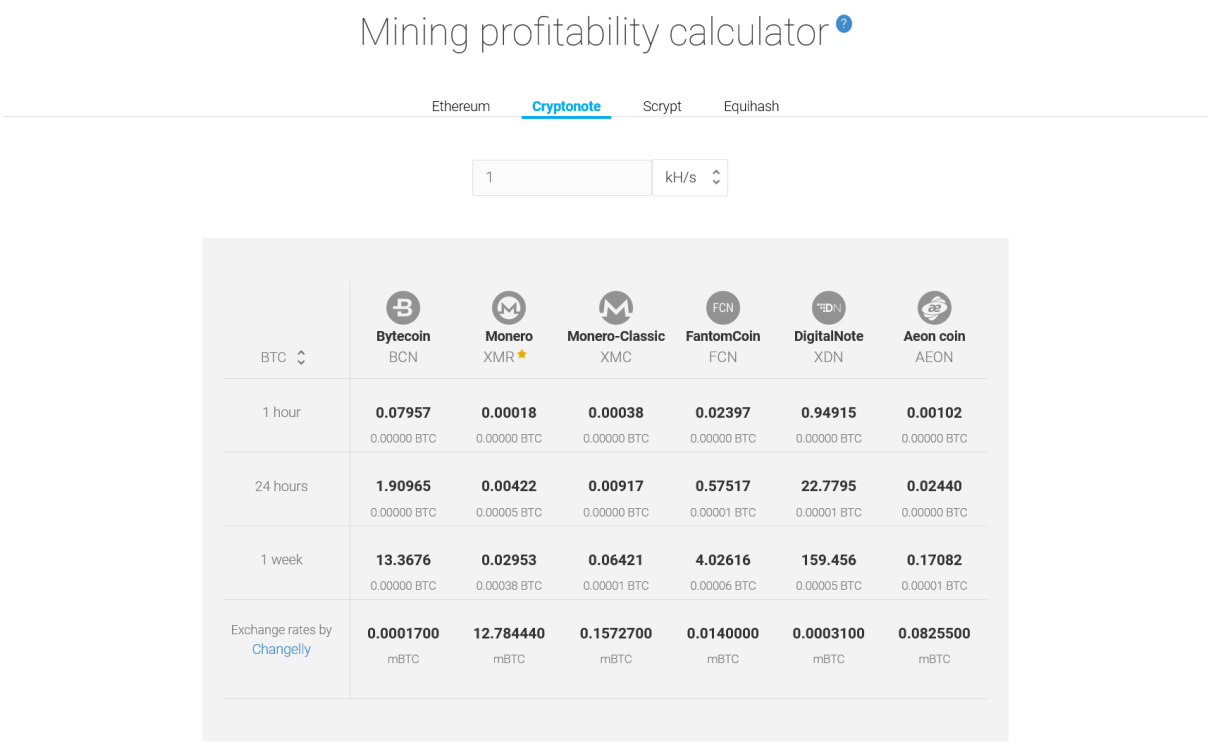
Name	11% CPU	31% Memory	0% Disk	0% Network	5% GPU
Firefox (7)	6.3%	2,693.7 MB	0.2 MB/s	0.7 Mbps	2.7%
Firefox	2.1%	548.9 MB	0 MB/s	0 Mbps	0%
Firefox	2.0%	362.0 MB	0.2 MB/s	0.7 Mbps	0%
Firefox	0.7%	432.8 MB	0 MB/s	0 Mbps	0%
Firefox	0.6%	112.7 MB	0 MB/s	0 Mbps	2.7%
Firefox	0.6%	491.3 MB	0 MB/s	0 Mbps	0%
Firefox	0.3%	424.9 MB	0 MB/s	0 Mbps	0%
Firefox	0.1%	321.1 MB	0 MB/s	0 Mbps	0%

لازم به ذکر است که ویروس‌کش‌ها در به روز رسانی‌های خود تقریباً این مشکل را رفع کرده‌اند و شما با خیال راحت می‌توانید وبگردی کنید.

الگوریتم‌ها

هر ارز دیجیتال از یک الگوریتم مادر سرچشمه می‌گیرد. در این لینک که برای محاسبه سودآوردی استخراج ارز نیز کاربرد دارد، هر سربرگ معادل یک الگوریتم مطرح در ارزهای دیجیتال است و با کلیک بر روی آن سربرگ، می‌توانید سکه‌ها یا ارزهای مربوط به آن الگوریتم خاص را مشاهده کنید.

در شکل زیر، ما بر روی الگوریتم Cryptonote کلیک کردیم و می‌بینید که فهرستی از سکه‌های مطرح (مثل Monero و Aeon) از این الگوریتم استفاده می‌کنند:



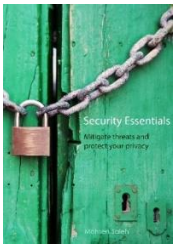
موارد و نکات مربوط به دنیای Mining و Cryptocurrency بسیار زیاد است و این نوشتار تنها بخش اندکی از این علم را پوشش داده است.

با جستجوی عمیق تر در دنیای وب، از تازه ترین و به روز ترین اطلاعات در رابطه با این علم با خبر شوید.

نظرات سازنده خود را می‌توانید در رابطه با نویسنده و به صورت بی نام در لینک زیر بنویسید:

mohsen1st.sarahah.com

فهرست کامل کتاب‌های این نویسنده به همراه لینک دانلود



نام کتاب: Security Essentials
توضیحات: مروری بر نکات و ابزارهای امنیتی و راهکارهای دفع حملات اینترنتی
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: اول
تعداد صفحات: ۲۴ صفحه
حجم: ۳٫۶ مگابایت
⇩دانلود

نام کتاب: Cryptocurrencies
توضیحات: ارزهای دیجیتال، ابزارها، نکات و دانستنی‌های این علم
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: سوم
تعداد صفحات: ۴۷ صفحه
حجم: ۵٫۳ مگابایت
⇩دانلود

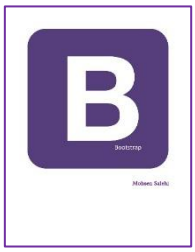
نام کتاب: SEO
توضیحات: کلیه موارد ضروری و ابزارهای مورد نیاز در رابطه با ارتقاء و بهینه سازی وبسایت و اعمال استانداردهای SEO
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: سوم
تعداد صفحات: ۵۴ صفحه
حجم: ۷٫۷ مگابایت
⇩دانلود

نام کتاب: PHP
توضیحات: آشنایی پایه‌ای با زبان برنامه نویسی PHP و الزامات آن
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: اول
تعداد صفحات: ۱۰۳ صفحه
حجم: ۱۱٫۶ مگابایت
⇩دانلود

نام کتاب: HTML
توضیحات: آشنایی مقدماتی به زبان بسیار ساده با ساختار برنامه نویسی HTML
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: اول
تعداد صفحات: ۲۱ صفحه
حجم: ۳ مگابایت
⇩دانلود

نام کتاب: CSS
توضیحات: آشنایی مقدماتی به همراه مثال‌ها و معرفی تکنیک‌های مختلف جهت طراحی ظاهری وبسایت با CSS
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: اول
تعداد صفحات: ۶۶ صفحه
حجم: ۷ مگابایت
⇩دانلود

نام کتاب: JS
توضیحات: آشنایی مقدماتی با زبان برنامه نویسی JavaScript
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: اول
تعداد صفحات: ۱۲ صفحه
حجم: ۱٫۶ مگابایت
⇩دانلود



نام کتاب: Bootstrap
توضیحات: آشنایی با ساختار Bootstrap به همراه مثال‌های متنوع و ساخت ۳ نمونه قالب
تاریخ آخرین به روز رسانی: 2019-01-25
ویرایش: اول
تعداد صفحات: ۶۳ صفحه
حجم: ۵٫۹ مگابایت
⇩دانلود