# Cryptocurrencies
# ارزهای دیجیتالی

در این کتاب می‌خوانید:

مروری بر ارزهای دیجیتال

استانداردهای ارزهای دیجیتال

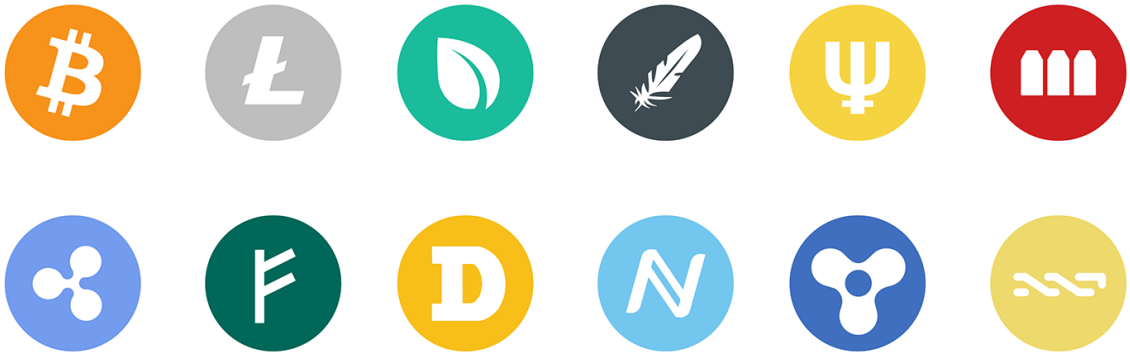
روش‌های تهیه ارزهای دیجیتال

امنیت و ارزهای دیجیتال

و بسیاری موارد ریز و درشت دیگر...

گردآوری و ترجمه توسط:
محسن صالحی

تا تاریخ نگارش این مقاله، بیش از 900 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 لیست کامل ارزهای دیجیتالی و ارزش آنها به لینک زیر بروید:

https://coinmarketcap.com/coins/views/all

تاریخچه ایجاد اولین ارز دیجیتال به سال 2009 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.

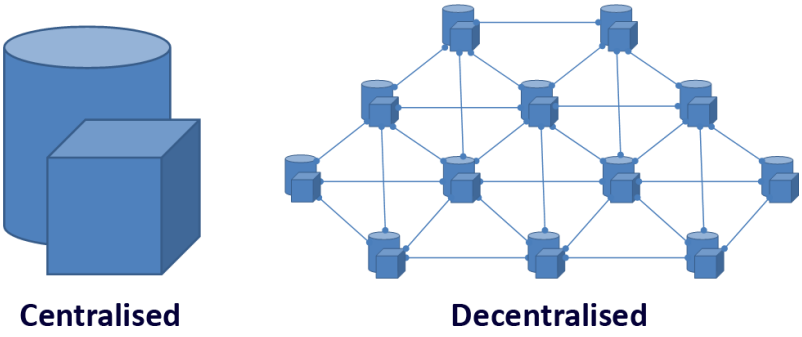
خالق Bitcoin، Satochi Nakamoto* قصد داشت ارز دیجیتالی تهیه کند که وابسته به تئوری‌های ریاضی باشد، نه به اقتصادها و بازارهای پر نوسان.

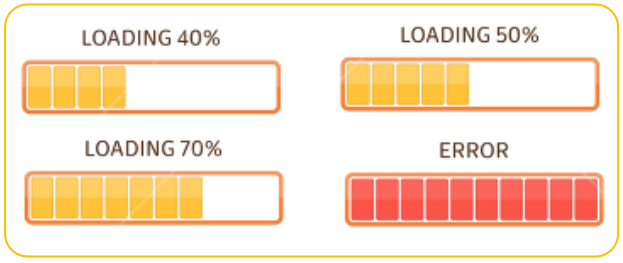
> در مورد اینکه چه کسی در واقع Bitcoin را ایجاد کرده، نظرات متفاوتی است. افراد و سازمان‌های مختلف، حتی از CIA هم به عنوان ایجاد کننده این ارز نام برده شده است.

### خواص کلی ارزهای دیجیتالی

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

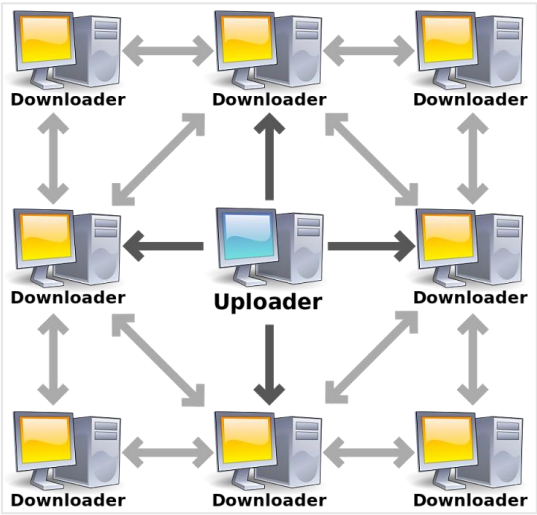
**غیر متمرکز بودن (decentralised)**، به این معنی که هیچ سازمان مالی خاصی شبکه مالی Bitcoin را مدیریت نمی‌کند و این ارز به هیچ مرکزی وابستگی ندارد. در نتیجه، مشکلات اقتصادی و خواسته‌های شخصی تأثیری در کاهش یا افزایش نرخ Bitcoin ندارد. طبق شکل زیر، در سیستم متمرکز (centralised)، هر قسمت (node) به صورت 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.




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 معنی است که فقط یک مسیر و دستگاه سرویس دانلود را در اختیار ما قرار داده و به هر دلیل مشکلی برای 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. 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:



# BLOCKCHAIN

Block Chain 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.

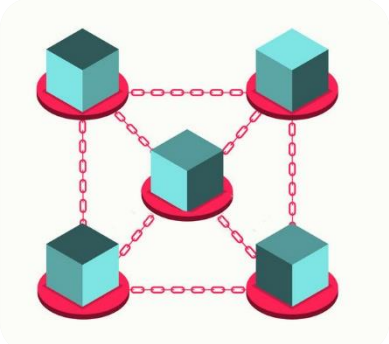
هر کامپیوتری که به شبکه Bitcoin وصل می‌شود، یک کپی از Block Chain دریافت می‌کند.


Block Chain 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 عمومی ثبت می‌کند.

معنی لغوی Block Chain برابر با "زنجیره‌ای از بلوک‌ها" است که در دنیای واقعی نیز چنین چیزی را تداعی می‌کند.

کاربران Bitcoin می‌توانند چندین حساب کاربری داشته باشند که هیچ گونه مشخصاتی از کاربر در آنها ثبت نشده باشد. برای ایجاد این حساب نیازی نیست هزینه‌ای پرداخت کنید.

### Block چیست؟



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

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

مشکل اصلی Block Chain اندازه (Size) بالای آن است.

### DAG file

این فایل در ارزهایی که بر پایه EtHash مانند Ethereum هستند 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. 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 افتاده است.

حجم فایل DAG رابطه مستقیم با GPU Memory دارد. تا تاریخ نگارش این نوشتار، حجم DAG file ارز Ether معادل 2.36GB است. به این معنی که شما دیگر نمی‌توانید با یک کارت گرافیک 2 گیگابایتی این ارز را Mine کنید.

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

https://investoon.com/tools/dag_size


### 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 Block Chain) به ازای هر Transaction یک fee در نظر می‌گیرد. این fee در نهایت به عنوان پاداش برای Miner ها 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 مختلفی هستند که در این زمینه قابلیت‌های مختلف ارائه می‌دهند و با استفاده از این سرویس‌ها 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 شماست 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.

### 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 دارید. مطرح‌ترین Online Wallet ها در فهرست زیر هستند:

https://blockchain.info/

https://www.coinbase.com

https://strongcoin.com/

https://xapo.com/

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

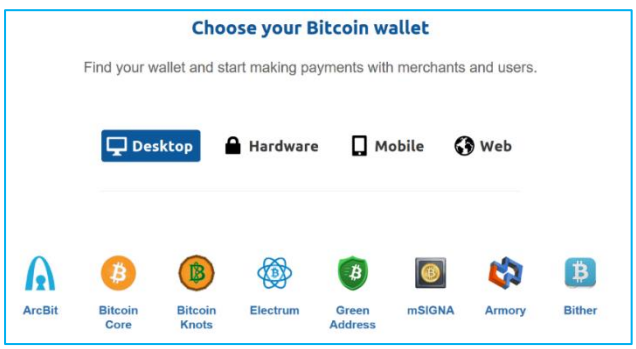
Hot Storage یا Online Wallet به معنی استفاده از فضای اینترنت جهت ذخیره کردن اطلاعات ارز دیجیتال است.

Cold Storage یا Offline Wallet به معنی نگهداری کیف پول و Private Key در محیط آفلاین است (روی کامپیوتر آفلاین یا روی کیف پول سخت افزاری). در شکل روبرو 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 به سرقت رفتن اطلاعات توسط هکرها به کلی از بین برود.

در لینک زیر، شما 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 سایت داده شده (نقاط قوت و ضعف):

https://Bitcoin.org/en/Wallets/Desktop/windows/




تصویری از ظاهر لینک بالا را در شکل روبرو می‌بینید:

Desktop Wallets: همانطور که در تصویر روبرو مشخص است، 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 آفلاین هستید، به شما قابلیت Cold-Storage هم می‌دهد.

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

https://Wallet.mycelium.com/

https://greenAddress.it/en/

https://breadapp.com/

Hardware Wallet، که همان Cold-Storage است و می‌تواند بر روی کاغذ نیز چاپ شود که به آن Paper Wallet گفته می‌شود. ماهیت Paper Wallet چون فیزیکی است، Hardware Wallet توصیف می‌شود اما به صورت کلی هنگامی که از Hardware Wallet اسم برده می‌شود، دستگاه‌های الکترونیکی ذخیره ارز دیجیتال مد نظر است. شکل زیر کیف پول سخت‌افزاری Ledger Nano S را نشان می‌دهد:

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

برای Paper Wallet، ما Private Address خود 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:

https://howsecureismypassword.net/

همچنین می‌توانید از ابزارهای Password Generator مانند زیر استفاده کنید:

https://passwordsgenerator.net/

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

> Password Vault Manager
> LastPass password manager

### تهیه نسخه پشتیبان یا Backup

از محتوا نسخه پشتیبان تهیه کنید. چه بهتر که در چند محل این کار انجام شود.

### آفلاین شدن یا Cold-Storage

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

### ایجاد Paper Wallet

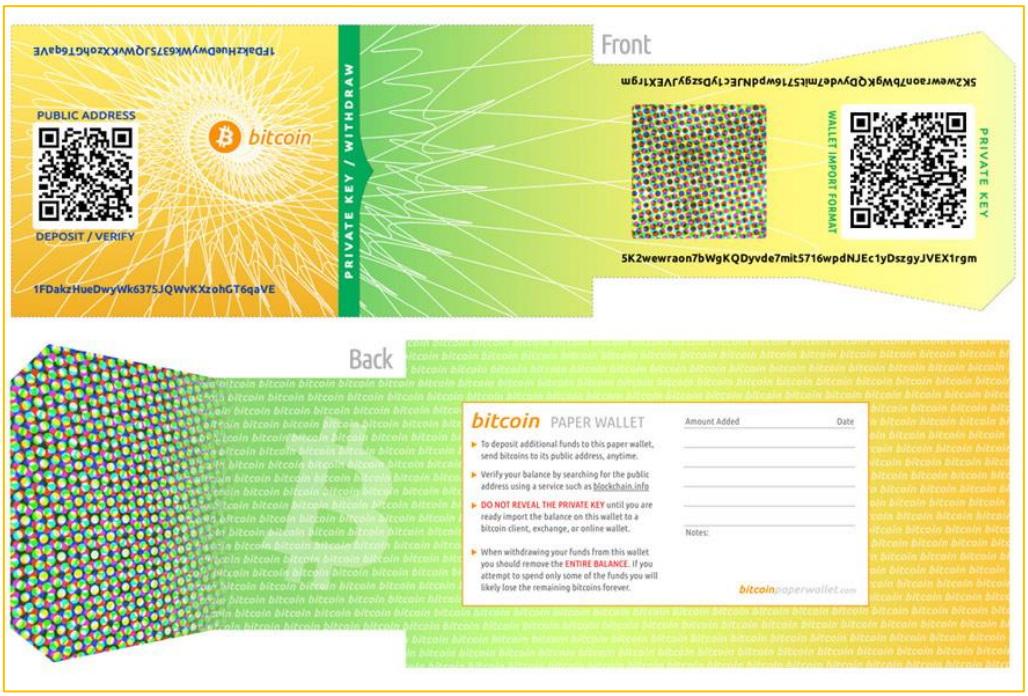
با ایجاد یک Paper Wallet، شما Public Key و Private Key شما به شکل QR Code بر روی کاغذ ذخیره شده و خطرات تحت وب به کلی از بین می‌رود. فراموش نکنید این کاغذ را لمینت کنید و از دسترس افراد حواس پرت دور نگه دارید!

### 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:

https://Bitcoinpaperwallet.com/

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 پروسه ممکن است اندکی متفاوت باشد.

### تراکنش ها چگونه انجام می‌شود؟

همه جزئیات Bitcoin ها در Block Chain 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. این تراکنش (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 ارزهای دیجیتال است. وبسایت payment24.ir یکی از وبسایت‌های معتبر داخلی برای خرید و فروش Bitcoin و ether 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 تا کنون به عنوان یک ارز مرجع شناخته شده نیست.

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، کار را ساده تر کرده است:

https://localBitcoins.com

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

http://www.coinmap.org

برخی از سایت‌های مطرح همچون Amazon.com 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 70.000 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 به صورت مفصل در مورد Mining توضیح می‌دهیم.

### چگونه ارز دیجیتال خود را بفروشیم؟

فروش ارز دیجیتال به آسانی خرید آن نیست. ما به روش‌های مختلفی 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 ارزی که انتقال می‌دهید 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 توسط شخص خریدار Exchange کنید و یا از خریدار بخواهید که کیف پول Monero ایجاد کند:

https://mymonero.com

**فروش به صورت مستقیم** یک روش 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، شما می‌توانید از وبسایت زیر برای به مزایده گذاشتن ارز دیجیتال خود و فروش آن اقدام کنید. همچنین می‌توانید فروشندگان دیگر را نیز بیابید:

http://ir-xe.com

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

https://www.coincorner.com/

https://bter.com/

https://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 معتبرتر 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 سکه‌های بیشتر گفته می‌شود و رقابتی است بین دیگر Miner ها در سراسر دنیا. مسئولیت نظارت بر Block Chain 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 می‌کنند و آن را به چیزی تبدیل کنند 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 Block Chain 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 Block Chain 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 KH/s (Kilo Hash/Second) تا رقم‌هایی مانند (TH/s) متغییر هستند.

به کلام ساده، هر چه HR شما بیشتر باشد، شما سریع‌تر معالادلات ریاضی مورد نیاز 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 ولی چیزی به دست نیاورید. 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:

https://www.multiPool.us/

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 مائل ریاضی در یک Block است.

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

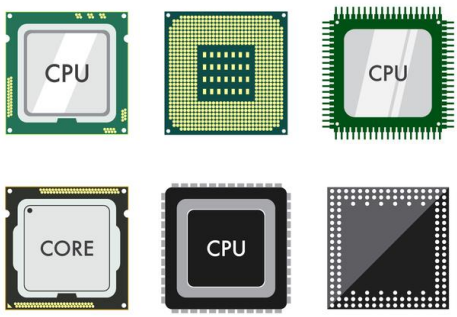
هر Mining Pool دارای یک Difficulty Rate بین 1 تا مقدار مشخص شده توسط ارز است. بسته به تعداد Miner ها این رقم نیز کاهش/افزایش پیدا می‌کند و شما نیاز به سخت‌افزار قوی‌تری برای Mining خواهید داشت.

در این میان، Share سهمی است که میان Miner های درون Pool تقسیم می‌شود و ملاکی است برای اثبات کارکرد سخت افزاری 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.

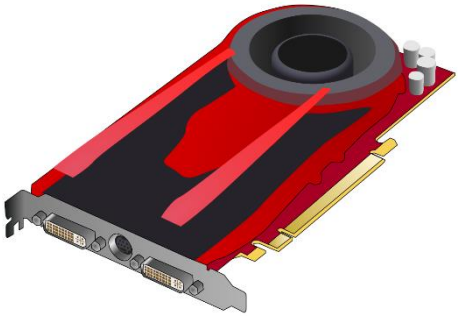
### CPU




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 کرد (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 دهنده های 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 از 100% هم فراتر رفت.

از آنجایی که در یک دوره زمانی، خریداران زیادی کارت گرافیک تهیه کردند و بازار به یک آرامش نسبی رسیده است، 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 از محدوده 5 TH تا 14 TH 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!

تا تاریخ این نوشتار، دو مدل از قدرتمندترین ASIC Miner ها را در زیر می‌بینید:

**Ant Miner S9 (13~14 TH)**

**AvalonMiner 821 (11 TH)**

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 |
|---|---|
| Kilo | 1.000 |
| Mega | $1.000^2$ |
| Giga | $1.000^3$ |
| Tera | $1.000^4$ |

### 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 در نهایت به صرفه نخواهد بود.

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

https://Miningchamp.com/

http://cryptoMining24.net/gpu-table-with-Hashrate/

https://whattoMine.com/

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

http://monerobenchmarks.info/

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 از گرم شدن و در نتیجه مصف برق بیشتر جلوگیری می‌کند (می‌توان با استفاده از Spray یا Blower این کار 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. مثلا: 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 زیر کمک بگیرید:
http://www.speedtest.net/

- 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 با نام Block Chain 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:

https://www.cryptocompare.com/Mining/calculator

https://Minergate.com/calculator/ethereum

وبسایت 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 مادامی که یک سوکت خالی است، برقی بابت آن سوکت تلف نمی‌شود.

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

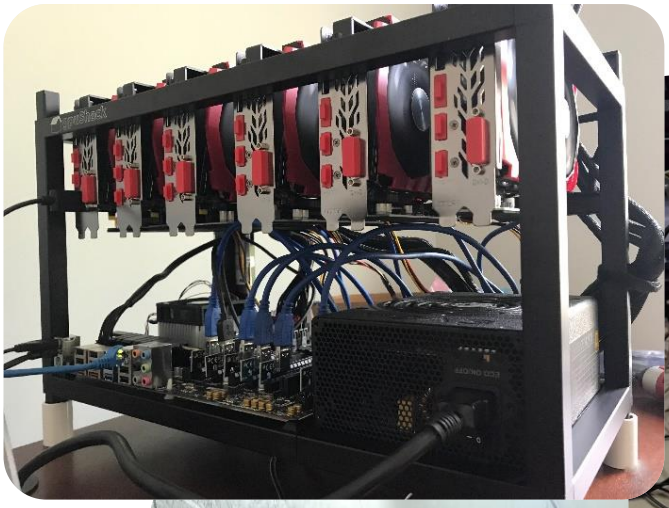
**Terotec BX11**

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

**Mining Rig**

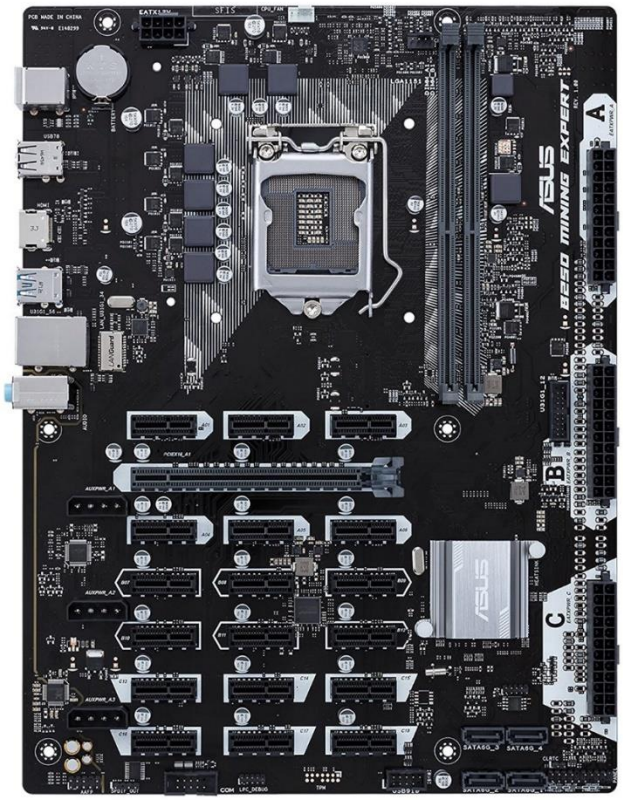
با سرمایه‌گزاری بالایی که اکثر مردم بر روی Mining انجام دادن، شرکت‌های تولید کننده سخت‌افزار به فکر طراحی ابزارهای جانبی متنوعی برای راحت تر کردن کار Miner ها شدند تا توانایی محاسباتی برای کامپیوترهای خانگی قابل افزایش باشد.

از آنجایی که Case های معمولی و اندازه‌ای که دارند جوابگوی تعداد زیاد کارت گرافیک نیست، فریم‌هایی 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:

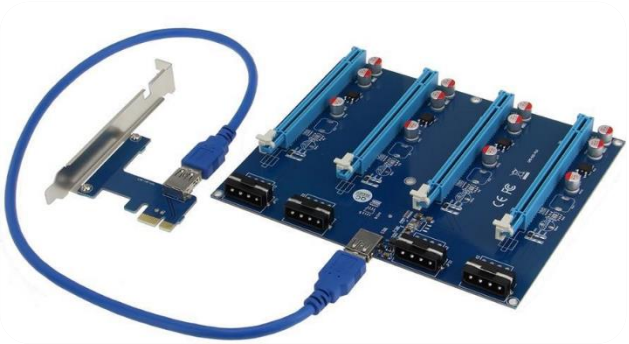
ASUS B250



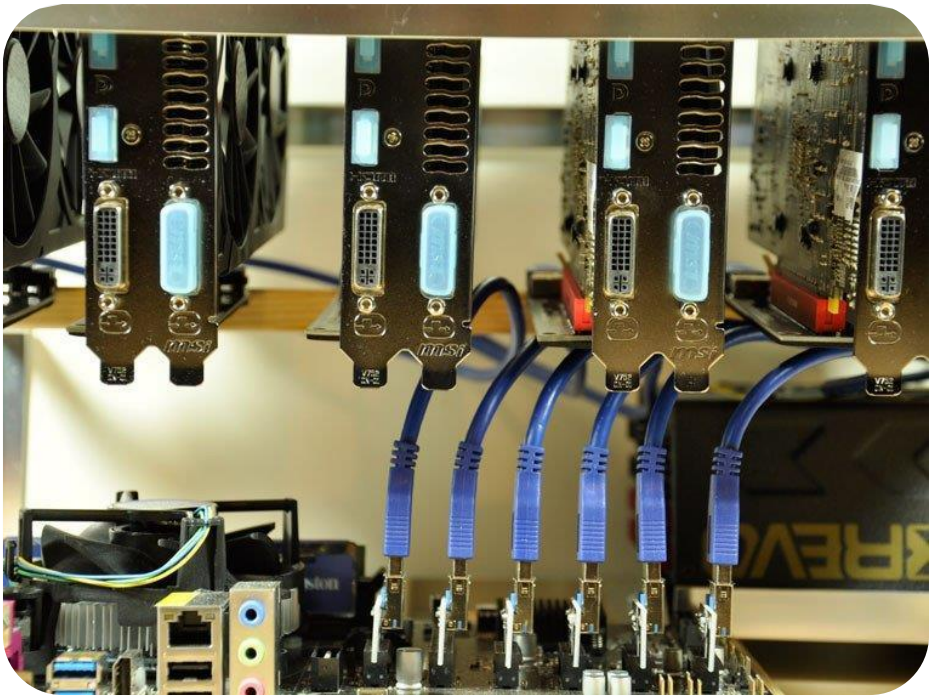

همانطور که می‌بینید، سه درگاه برای اتصال سه عدد Power به این Motherboard تعبیه شده است. همچنین 18 عدد شکاف PCIe x1 و 1 عدد PCIe x16 برای آن تعبیه شده که حداکثر اجازه نصب 19 عدد کارت گرافیک را به ما می‌دهد.

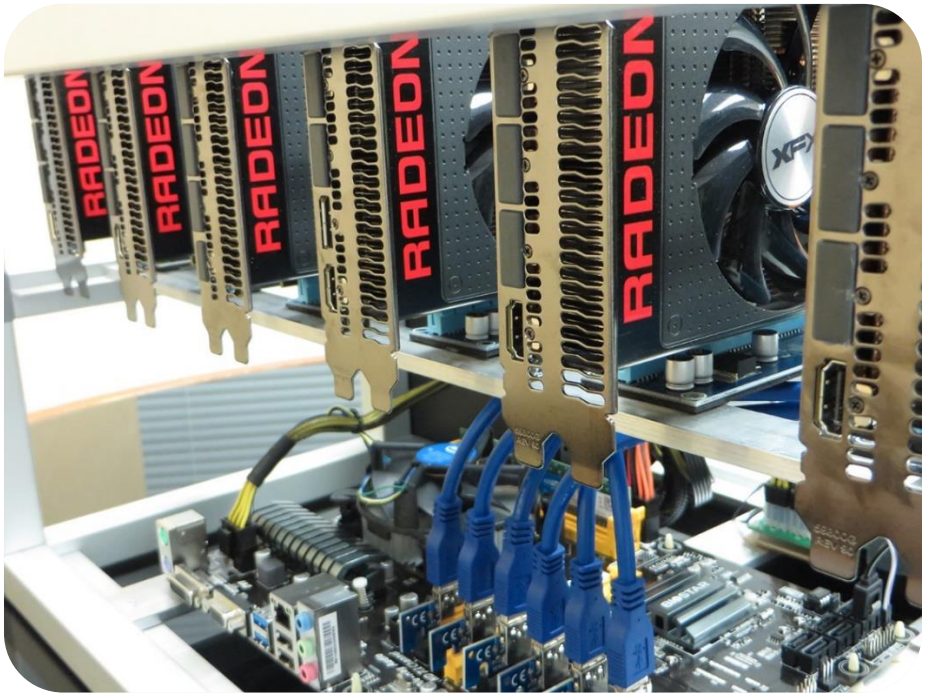
بین شکاف‌های PCIe 1x و PCIe x16 در کارت گرافیک‌های رده بالا تفاوت محاسباتی ناچیزی (تقریباً 0) وجود دارد.

این سوال پیش می‌آید که چگونه می‌توان 19 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 بورد خروجی متصل می‌شود. این بورد خروجی به ما اجازه نصب کارت گرافیک‌های اضافی را می‌دهد. نمونه استفاده از این کارت را در شکل 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 ملیون قیمت داشته باشد، توان پردازشی مناسب برای Mining ارائه نمی‌دهند و سیستم خنک کنندگی آنها 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 دیگر بسیار کند عمل می‌کند.

### 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.

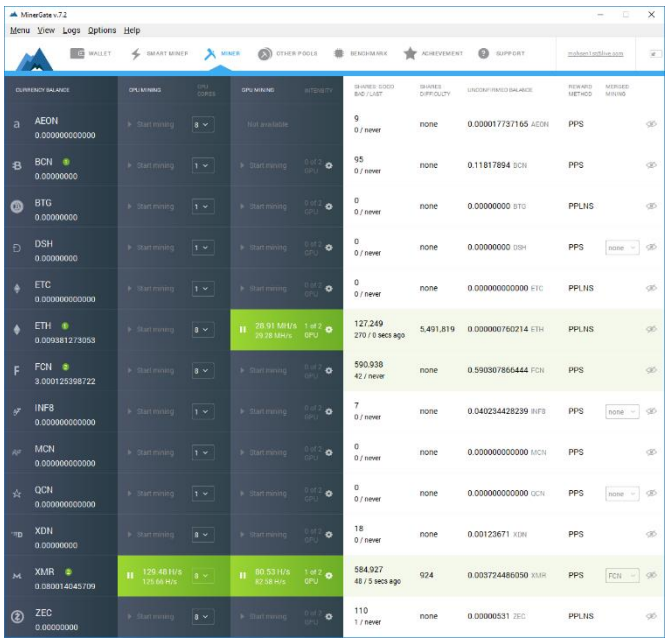
نرم‌افزارهای GUI رابط کاربری ساده‌ای را در اختیار ما قرار می‌دهند و ما با چند کلیک ساده آنها را راه‌اندازی می‌کنیم.

نرم‌افزارهای Console از یک رابط 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 اینجا ما چند مورد از این نرم‌افزارها را معرفی می‌کنیم:

### Minergate

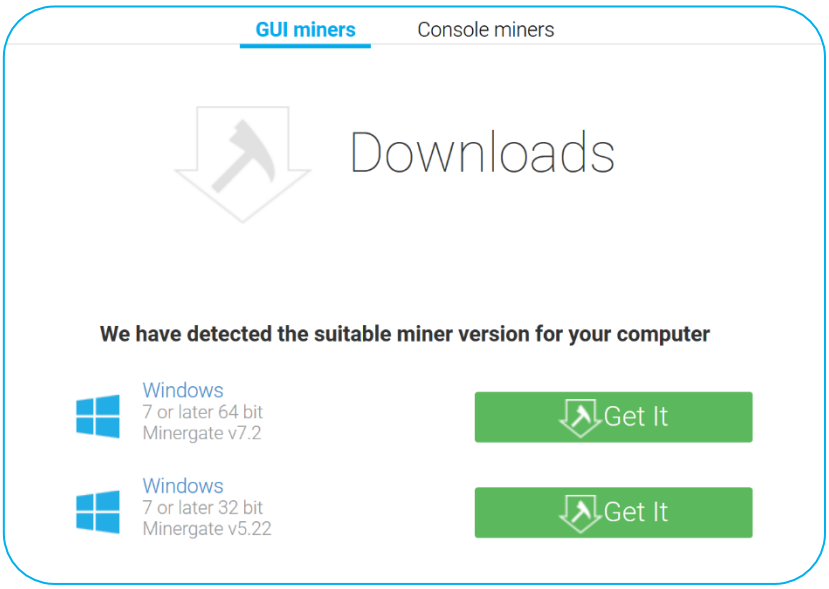



این نرم‌افزار که بر روی سیستم عامل‌های مختلف قابل نصب است به ما اجازه می‌دهد که بدون هیچ گونه تنظیمات خاصی مستقیماً Mining ارز مد نظرمان را از 13 ارزی که این ابزار پشتیبانی می‌کند انجام دهیم.

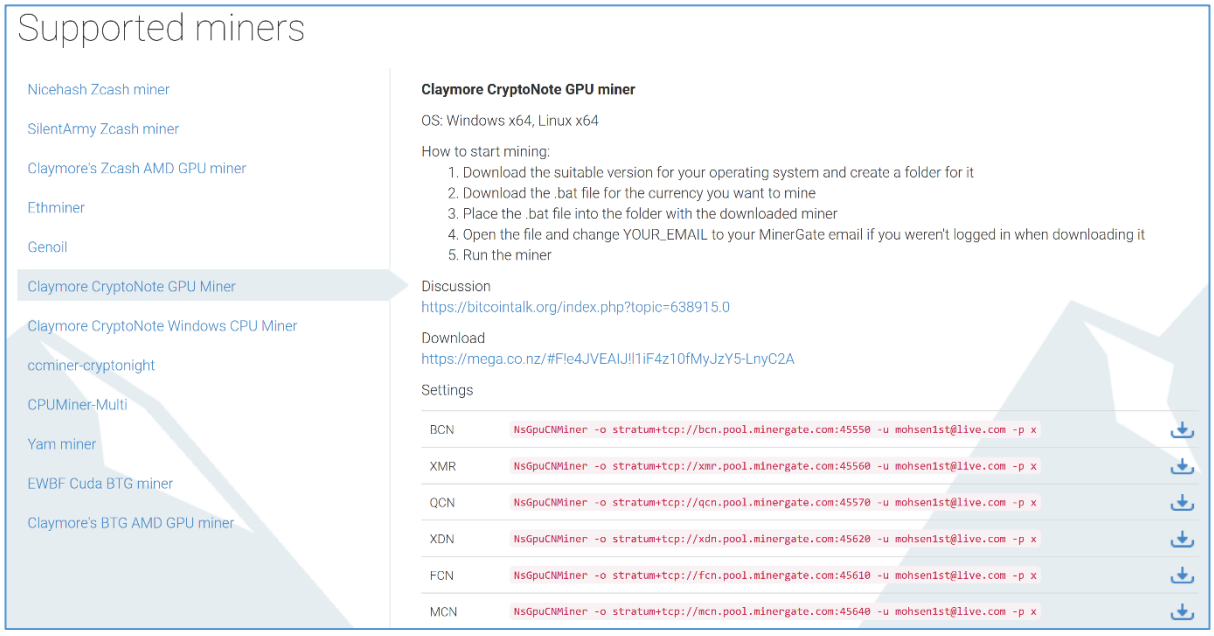
برای اینکه با این نرم‌افزار شروع به استخراج ارز کنید، ابتدا لازم است در وبسایت Minergate.com یک حساب کاربری ایجاد کنید. سپس نرم‌افزار Minergate مخصوص سیستم عاملی که دارید را از لینک زیر دانلود و Login کنید، سپس با کلیک بر روی Smart Miner می‌توانید به صورت خودکار ارزی که بیشترین نرخ تبادل را داشته است، Mine کنید:

https://Minergate.com/downloads/gui

با کلیک بر روی این لینک صفحه زیر را می‌بینید:




در صفحه بالا، با کلیک بر روی سربرگ Console Miners و در انتهای صفحه کلیک بر روی لینک Alternative Miners فهرستی از ابزارهای اختصاصی برای Mining به شما نشان داده می‌شود:




در سمت چپ، فهرستی از Console Miner ها را می‌بینید. این ابزارها از ابزارهای گرافیکی اندکی سریعتر هستند و شما می‌توانید با دانلود و اندکی تنظیمات، شروع به Mine کردن کنید.

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 (مانند شکل بالا) برای شما به صورت خودکار پر شده است و تنها کافیست با کلیک بر روی دکمه آبی رنگ دانلود مربوط به ارز مورد نظر (دکمه دانلود روبروی سطر قرمز رنگ)، فایلی که دانلود کردید را در کنار نرم‌افزار Console Miner قرار دهید.

نرم‌افزار Claymore از ابزارهای محبوب Miner ها است.

توضیحات جزئی تنظیمات ابزارها در این مقاله نمی‌گنجد. منابعی در انتهای مقاله جهت سهولت خوانندگان آورده شده است.

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

### امنیت

ارزهای دیجیتال، سرمایه ارزشمندی هستند. 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 درصد 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% |

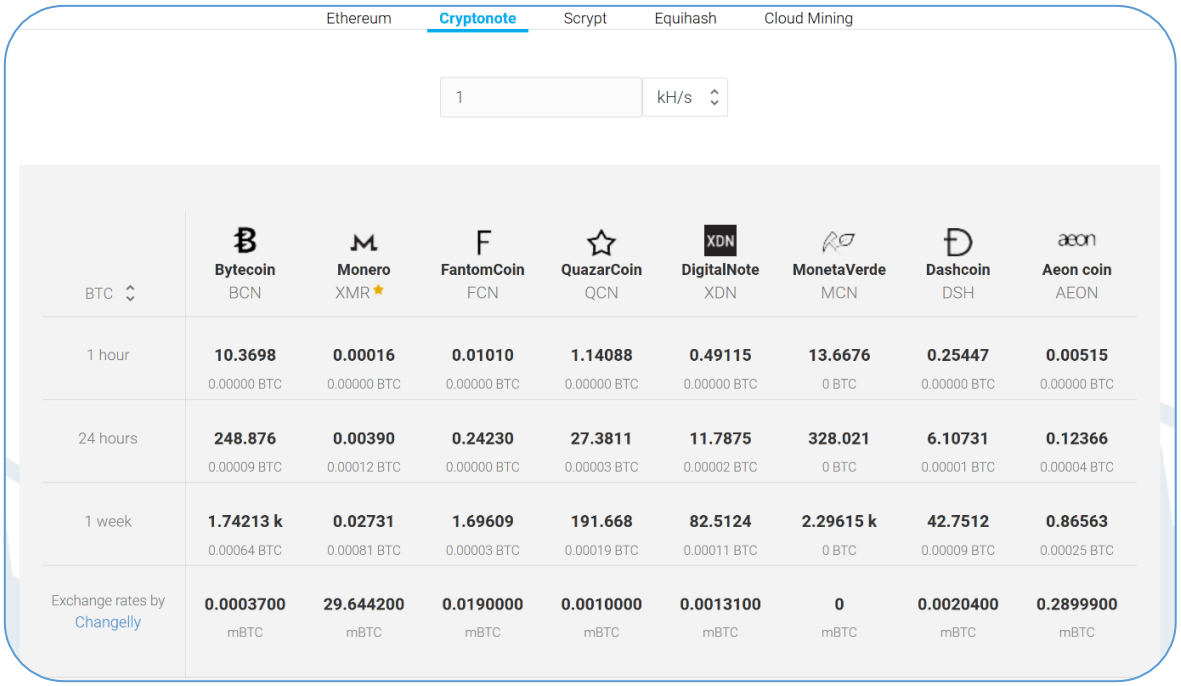
لازم به ذکر است که ویروس‌کش‌ها در به روز رسانی های خود تقریباً این مشکل را رفع کرده‌اند و شما با خیال راحت می‌توانید وبگردی کنید.

## الگوریتم‌ها

هر ارز دیجیتال از یک الگوریتم مادر سرچشمه می‌گیرد. در لینک زیر 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:

https://Minergate.com/calculator/ethereum

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




| BTC | Bytecoin BCN | Monero XMR | FantomCoin FCN | QuazarCoin QCN | DigitalNote XDN | MonetaVerde MCN | Dashcoin DSH | Aeon coin AEON |
|---|---|---|---|---|---|---|---|---|
| 1 hour | 10.3698<br>0.00000 BTC | 0.00016<br>0.00000 BTC | 0.01010<br>0.00000 BTC | 1.14088<br>0.00000 BTC | 0.49115<br>0.00000 BTC | 13.6676<br>0 BTC | 0.25447<br>0.00000 BTC | 0.00515<br>0.00000 BTC |
| 24 hours | 248.876<br>0.00009 BTC | 0.00390<br>0.00012 BTC | 0.24230<br>0.00000 BTC | 27.3811<br>0.00003 BTC | 11.7875<br>0.00002 BTC | 328.021<br>0 BTC | 6.10731<br>0.00001 BTC | 0.12366<br>0.00004 BTC |
| 1 week | 1.74213 k<br>0.00064 BTC | 0.02731<br>0.00081 BTC | 1.69609<br>0.00003 BTC | 191.668<br>0.00019 BTC | 82.5124<br>0.00011 BTC | 2.29615 k<br>0 BTC | 42.7512<br>0.00009 BTC | 0.86563<br>0.00025 BTC |
| Exchange rates by Changelly | 0.0003700<br>mBTC | 29.644200<br>mBTC | 0.0190000<br>mBTC | 0.0010000<br>mBTC | 0.0013100<br>mBTC | 0<br>mBTC | 0.0020400<br>mBTC | 0.2899900<br>mBTC |

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.

موفق و پیروز باشید.

2018-03-12

ارتباط با نویسنده:


+98 930 072 0204


mohsen1st@gmail.com

.