

# اصطلاحات ارز دیجیتال

Cryptocurrency's Expressions

**Kifpool**

صرافی امن و سریع کیف پول



## صفر تا صد اصطلاحات ارز دیجیتال + اصطلاحات تخصصی

### اصطلاحات ارز دیجیتال

دنیای ارزهای دیجیتال روزبه روز در حال گسترش است و آشنایی با اصطلاحات ارز دیجیتال برای افرادی که قصد سرمایه گذاری در این دنیای هیجان انگیز را دارند، امری مهم محسوب می شود. بازار ارزهای دیجیتال از سال 2009 و با ارائه بیت کوین به عنوان اولین رمزارز غیرمتمرکز کار خود را آغاز کرد و از آن زمان تا به امروز ارزهای دیجیتال رشد زیادی تجربه کرده اند؛ به طوری که امروزه هزاران ارز دیجیتال در بازار وجود دارد و با گذشت زمان به تعداد آنها نیز افزوده می شود.

رشد سریع این حوزه سبب شده تا اصطلاحات و مفاهیم جدیدی شکل بگیرند و به همین دلیل افرادی که می خواهند فعالیت خود را در این دنیا آغاز کنند، باید با این اصطلاحات آشنا باشند. در این دنیای هیجان انگیز و در چندین سال گذشته احتمالاً نام کلمه هایی نظیر ارز دیجیتال، رمز ارزها، بیت کوین، بلاک چین و غیره را شنیده اید.

برای درک بهتر و راحت تر این اصطلاحات در این مقاله از وبلاگ کیف پول من، اصطلاحات دنیای ارزهای دیجیتال به صورت ساده و قابل فهم توضیح داده شده است. پس در ادامه همراه کیف پول من باشید.

# آشنایی با اصطلاحات پایه ارزهای دیجیتال

برای درک بهتر و بیشتر اصطلاحات ارز دیجیتال، ابتدا با مفاهیم پایه و ابتدایی دنیای رمزارزها آشنا می‌شویم.

## ارز دیجیتال (Digital Currency)



ارزهای دیجیتال به شکل فیزیکی وجود ندارند و در بستر دیجیتال ایجاد می‌شوند. ارزهای دیجیتال هزینه‌های مربوط به تولید پول به صورت اسکناس و سکه را از بین برده و جابه‌جایی آن را راحت کرده‌اند. ارزهای دیجیتال با توجه به تکنولوژی و مفاهیم استفاده شده در آن به سه نوع ارز مجازی (Currency Virtual)، رمز ارز (Cryptocurrency) و ارز دیجیتال بانک مرکزی (CBDC) تقسیم می‌شوند. لازم به ذکر است که بیشتر ارزهای دیجیتال شناخته شده از نوع رمزارز هستند و به همین دلیل معمولاً این دو واژه به جای هم نیز استفاده می‌شوند.

## رمزارز (Cryptocurrency)

رمز ارزها (Cryptocurrency) دسته‌ای از ارزهای دیجیتال هستند که از تکنیک‌های رمزنگاری برای تامین امنیت اطلاعات خود استفاده می‌کنند. رمزارزها به صورت متمرکز و یا غیرمتمرکز ارائه می‌شوند که **رمزارز بیت کوین** به عنوان اولین رمزارز، از حالت غیرمتمرکز استفاده می‌کند.

رمزارزها مستقل از سیستم بانکی هستند و عدم دخالت دولت‌ها و نهادهای متمرکز در فرایند تولید، تایید و ثبت تراکنش‌ها به صورت امن، جابجایی سریع پول هم‌تا به هم‌تا و امنیت بالای اطلاعات از جمله ویژگی‌های مثبت رمزارزها است که می‌توان به آن اشاره کرد.

مطلب پیشنهادی : [معرفی ارز دیجیتال به زبان شیرین!](#)

## رمز نگاری (Cryptography)

رمزگذاری اطلاعات، رمز نگاری است و از رمزنگاری به عنوان روشی برای محافظت از اطلاعات و ارتباطات و حفظ حریم خصوصی با استفاده از کدها یاد می‌شود. در این روش فقط کسانی که به این اطلاعات دسترسی دارند، می‌توانند آنها را خوانده و پردازش کنند.

وجود رمزنگاری برای ایجاد ارتباط امن در بستر آنلاین لازم است و بدون استفاده از تکنیک‌های رمزنگاری، امکان هک اطلاعات وجود دارد. از رمزنگاری برای ایجاد **کیف پول دیجیتال**، **امضای دیجیتال** و روش‌هایی برای توافق کاربران و ماینرها شبکه استفاده می‌شود که در ادامه این اصطلاحات شرح داده شده‌اند.

# بلاک چین



یکی از اصلی‌ترین اصطلاحات ارز دیجیتال، **بلاک چین** است. بلاک چین به عنوان یک دفتر دیجیتالی برای یک رمز ارز شناخته می‌شود که در آن تمام معاملات انجام شده ثبت می‌گردند. در حقیقت بلاک چین یک سیستم ثبت اطلاعات و داده است که با استفاده از روش رمز نگاری، امکان هک و دستکاری اطلاعات را از بین می‌برد.

بلاک چین از بلاک‌های متعددی تشکیل شده و هر کدام از آن‌ها، شامل اطلاعات تراکنش‌ها هستند. این مفهوم یک فناوری غیرمتمرکز است و هیچ نسخه‌ای از آن در جایی خاص وجود ندارد و در نتیجه همه این نسخه‌ها با هم برابر هستند. لازم به ذکر است که اطلاعات بلاک چین با تمامی کاربران به اشتراک گذاشته می‌شود و به اطلاعات و داده‌های بلاک چین که به صورت عمومی در دسترس هستند، Public Blockchain می‌گویند.

### بلاکچین عمومی (Public Blockchain)

بلاکچین‌های عمومی (Public Blockchain) از شناخته شده‌ترین نوع بلاکچین‌ها هستند که در این بلاکچین‌ها به طور کامل دموکراسی برقرار است. افراد برای عضویت در این شبکه به مجوز ورود نیازی ندارند و هر شخص می‌تواند با یک سیستم کامپیوتر که به اینترنت متصل است و همراه با دانلود یک نسخه کامل از تمامی داده‌های موجود در شبکه، یکی از نودهای آن باشد.

بلاکچین عمومی یک دفتر کل توزیع شده است که از نمونه‌های آن می‌توان به **بلاکچین‌های بیت کوین**، اتریوم و سایر ارزهای دیجیتال اشاره کرد. اطلاعات تمامی تراکنش‌ها، معاملات، تبادلات و قراردادهای در بستر بلاکچین

عمومی برای تمامی افراد قابل رویت است و تمام تصمیم‌گیری‌ها در بستر این سیستم از طریق ساز و کار اجماع انجام می‌شود.

لازم به ذکر است که تمامی نودها می‌توانند در تمامی پارامترهای الگوریتم اجماع از قبیل تایید و اعتبارسنجی تراکنش‌ها و استخراج بلاک‌های جدید، بدون محدودیت شریک باشند. همچنین همه آن‌ها باید در جریان تمام فرایندهای شبکه قرار بگیرند و بدون اجازه نودها، هیچ اتفاقی در بلاکچین رخ نمی‌دهد. در حقیقت هر نود با انجام عملیات استخراج می‌تواند پاداش ماینینگ بلاک جدید را دریافت نماید.

### **بلاکچین خصوصی (Private Blockchain)**

بلاکچین خصوصی در سازمان‌های دولتی و یا شرکت‌های خصوصی برای ثبت اطلاعات استفاده می‌شود. این بلاکچین ویژگی عدم تمرکز را ندارد و ورود به این سیستم، دسترسی به اطلاعات آن و انجام فعالیت در بستر شبکه، مستلزم دریافت مجوز از سوی مسئول کنترل کننده آن است.

بلاکچین خصوصی به صورت متمرکز توسط یک مسئول واحد اداره شده و تعداد کاربران در تاین بلاکچین توسط همین مسئول تعیین می‌گردد. بلاکچین خصوصی مانند بلاکچین عمومی خاصیت توزیع شدگی خود را حفظ کرده است و به این ترتیب که اعضای دارای مجوز حضور و فعالیت در سیستم، باید یک نسخه کامل از شبکه و داده‌های موجود در آن را بر روی رایانه خود ذخیره داشته باشند.

در این بلاکچین کنترل کننده مرکزی به برخی از نودها مجوز اعتبارسنجی می‌دهد و فقط آن‌ها اجازه تایید تراکنش‌ها و سایر فعالیت‌ها را دارند. همچنین به غیر از سطح دسترسی گره‌های شبکه، موارد دیگری مانند شفافیت و عدم شفافیت اطلاعات و استخراج بلاک‌ها نیز به کسب مجوز نیازمند است. قوانین بلاکچین خصوصی قبل از راه اندازی آن به طور کامل، توسط شرکت یا سازمان مربوطه تعیین و نوشته می‌شود.

### **بلاکچین کنسرسیوم (Consortium Blockchain)**

**شبکه بلاکچین کنسرسیوم** یکی از بلاک چین‌های نیمه متمرکز است که توسط سازمان‌ها مدیریت می‌شود. کاربرد این بلاکچین‌ها زمانی بسیار زیاد است که چندین سازمان یا شرکت، قصد شراکت و همکاری با یکدیگر را داشته باشند. آن‌ها می‌توانند در این بستر فضای مشترک ایجاد کنند و به راحتی اطلاعات را در امنیت کامل با یکدیگر به اشتراک بگذارند.

وظایف و قوانین الگوریتم اجماع در بلاکچین کنسرسیوم میان نودها متفاوت است و با توجه به صلاح دید رئیس‌های گروه تعیین می‌شود. این بلاک چین امنیت بالا و مقیاس‌پذیری بیشتری در مقایسه با بلاکچین عمومی دارد و کارایی آن نیز نسبت به بلاکچین عمومی بیشتر است.

### **بلاکچین هیبرید (Hybrid Blockchain)**

**بلاکچین هیبریدی** ترکیبی از بلاکچین‌های عمومی و خصوصی است که از مزایای هر دو نوع این بلاکچین‌ها بهره برده و معایب آن‌ها را به حداقل می‌رساند. در این بلاکچین اجازه عضویت با دستور مسئول کنترل کننده آن صادر می‌شود و میزان اجازه فعالیت در شبکه نیز با همین روش تعیین می‌شود.

لازم به ذکر است که ورود به این شبکه برای عموم آزاد نیست و مسئولین بلاکچین هیبرید در بازه زمانی خاص می‌توانند مشخص کنند که تراکنش‌ها و فعالیت‌های دیگر بر روی شبکه نمایش داده شود یا خیر. بلاکچین هیبریدی از حمله 51 درصدی در امان است و قوانین آن با توجه به نیازها قابل تغییر هستند. این نوع بلاکچین در مقایسه با بلاکچین عمومی مقیاس پذیری بهتری دارد و حریم خصوصی نودها در این شبکه حفظ می‌شود.

### کراس چین (Cross-Chain)

یکی از موثرترین راه حل‌ها برای تسهیل قابلیت همکاری بین شبکه‌های بلاک چین، فناوری کراس چین است. این فناوری که نوظهور است، انتقال ارزش و داده را بین دو یا چند شبکه بلاک چین تسهیل کرده و امکان تبادل داده بین چندین شبکه را فراهم می‌کند.

از طریق این پروتکل، کاربران می‌توانند بدون دخالت واسطه‌ها با یکدیگر ارتباط برقرار کنند و در نهایت بلاکچین‌هایی که شبکه‌های مشابهی را به اشتراک می‌گذارند، می‌توانند ارزش و داده را بین یکدیگر انتقال دهند. این فناوری بر اساس اصل اتمی کار کرده و امکان سازگاری مناسب بین چندین بلاکچین به هم پیوسته را فراهم می‌کند.

### مکانیسم اجماع (Consensus Process)

مکانیسم اجماع، به عنوان روشی به کار می‌رود که گروهی از افراد برای تصمیم‌گیری استفاده می‌کنند. به عنوان مثال، در شبکه بیت‌کوین نیاز است تاریخچه تراکنش‌ها در بلاک چین به طور مداوم به روزرسانی شود تا تراکنش‌های جدید و موجودی‌های کاربران را منعکس کند. این مکانیسم به گره‌هایی اطلاق می‌شود که مسئول نگهداری دفتر کل بلاک چین هستند تا بتوانند در هنگام انجام تراکنش به اجماع برسند. در مکانیسم اجماع، افرادی که کاملاً با هم غریبه هستند و آشنایی با یکدیگر ندارند، در سازوکاری که پاداش‌ها یا مجازات مالی در آن دخیل است با یکدیگر به توافق می‌رسند.

### بلاک (Block)

مجموعه‌ای از تراکنش‌ها که ماینرها آن را بررسی و تایید می‌کنند، بلاک هستند. بلاک چین از بلاک تشکیل شده است و به عنوان پایگاه داده‌ای از کلیه معاملات انجام شده شناخته می‌شود که هر بلاک آن دائمی و تغییرناپذیر هستند.

در حقیقت هر بلاک در بلاک چین به عنوان واحد ثبت اطلاعات عمل می‌کند و اطلاعات تراکنش‌ها و اطلاعات اتصال بلاک‌ها به یکدیگر را شامل می‌شود. حجم بلاک، تعداد تراکنش‌های داخل بلاک، زمان مورد نیاز برای ثبت بلاک و غیره برای بلاک چین‌های گوناگون، متفاوت هستند. رکوردهای ثبت شده در هر بلاک دائمی و تغییرناپذیر هستند و هر یک از بلاک‌ها تمامی معاملات را تا زمانی که پر نشده اند، نگهداری می‌کنند.

## ارتفاع بلاک (Block Hight)

به تعداد بلاک‌ها قبل از بلاک قبلی و موردنظر در بلاک چین، ارتفاع بلاک می‌گویند؛ برای مثال ارتفاع 0 اولین بلاک است که بلاک پیدایش نیز به آن می‌گویند.

## جستجوگر بلاک (Block Explorer)

جستجوگر بلاک، یک موتور جستجو برای پیدا کردن ارزش‌های دیجیتال است که به کاربران این امکان را می‌دهد تا اطلاعات لازم در مورد تراکنش‌ها، آدرس‌ها و دیگر موارد را پیدا کنند. در جستجوگر بلاک اطلاعات مربوط به تراکنش‌های صورت گرفته در یک بلاک چین نمایش داده می‌شود.

همچنین با استفاده از **جستجوگر بلاک**، شفافیت اطلاعات برای تمامی افراد از سرتاسر دنیا ایجاد می‌شود و تمامی تراکنش‌های کوین اصلی **شبکه بلاک چین** و توکن‌های ساخته شده بر روی آن، قابل ردیابی است. علاوه بر این عملکرد، می‌توان از جستجوگر بلاک اطلاعات زیادی در مورد آدرس‌های نگه دارنده ارز دیجیتال و وضعیت استخراج آن کسب کرد.



**وایت پیپر** یا سفید نامه گزارشی است که در آن توسعه دهندگان به بیان جزئیات طرح یا سیستم خود می‌پردازند و هر پروژه ارز دیجیتال با استفاده از آن تکنولوژی خود را برای آشنایی عموم منتشر می‌کند. اصلی‌ترین بخش Whitepaper مربوط به اهداف پروژه و مشکلی است که پروژه حل می‌کند و در این بخش، تیم پروژه با معرفی مشکل موجود و تکنولوژی خود، راه حل ارائه شده برای حل مشکل را توضیح می‌دهد.

همچنین وایت پیپر به مشکلاتی که توسعه دهندگان قصد دارند با رمزارز خود آن را حل کنند، اشاره دارد. در حقیقت یک وایت پیپر خوب شامل نقشه راه پروژه، اطلاعات اقتصادی مربوط به توکن یا کوین پروژه، تیم مدیریتی و سرمایه‌گذاران پروژه است و معمولاً وایت پیپر نسخه مارکتینگ پروژه نامیده می‌شود و برای جلب توجه عموم مردم به پروژه استفاده می‌گردد.

مطلب پیشنهادی : [وایت پیپر چیست؟](#)

زردنامه (Yellow Paper) نسخه فنی و علمی وایت پیپر است که در آن اطلاعات علمی پروژه به صورت کامل بررسی می‌شود. بیج پیپر (BeigePaper) نسخه ساده شده زردنامه است و برای درک آسان مباحث علمی پیچیده نوشته می‌شود. البته لازم به ذکر است که در برخی اوقات، از LitePaper نیز به عنوان نسخه آسان وایت پیپر یاد می‌شود و البته بیشتر پروژه‌های ارز دیجیتال فقط سفیدنامه و زردنامه منتشر می‌کنند.



## الگوریتم (Algorithm)

دستورالعمل‌های ریاضی کدگذاری می‌شوند و با پیاده‌سازی توسط نرم افزار کامپیوتری، نتیجه دلخواهی را ایجاد می‌کنند. اصطلاح الگوریتم را می‌توان در بسیاری از وایت پیپرها و نقاط ضعف و قدرت توکن‌ها مشاهده کرد.

### الگوریتم اثبات کار (Proof of Work)

**الگوریتم اثبات کار** نوعی مکانیسم اجماعی است که برای جلوگیری از حملات هرزنامه‌ای و وقفه در دسترسی کاربران مجاز به شبکه رایانه‌ای، به کار می‌رود. از ویژگی اصلی سیستم اثبات کار می‌توان به عدم تقارن آن اشاره کرد؛ به این معنی که فرستنده پیام برای تهیه آن به مدتی زمان نیاز دارد تا ثابت کند که کار انجام شده است. با این وجود گیرنده می‌تواند در زمان بسیار کمی تایید کند که کار توسط فرستنده انجام شده است.

### الگوریتم اثبات سهام (Proof of Stake)

الگوریتم اثبات سهام به عنوان جایگزینی برای الگوریتم اثبات کار شناخته می‌شود که ایجاد شد تا **مشکلات الگوریتم اثبات کار** را حل کند. در الگوریتم اثبات سهام به جای استفاده از استخراج، باید در سیستم مقداری سهم یا همان سکه داشته باشید؛ بنابراین اگر 10 درصد سهم یا سکه داشته باشید، احتمال استخراج بلوک بعدی توسط شما 10 درصد خواهد بود.

استخراج کردن به میزان زیادی توان پردازش برای اجرای محاسبات پیچیده رمزنگاری برای باز کردن چالش‌های پردازش نیازمند است. در الگوریتم اثبات کار این توان به معنی مصرف میزان زیاد برق، برای اثبات کار مورد نیاز است و به همین دلیل اثبات سهام برای صرفه‌جویی در برق معرفی شد.

### همتا به همتا (Peer 2 Peer)

در شبکه همتا به همتا دو یا چند کامپیوتر، خریداران و فروشندگان ارزهای دیجیتال بدون اینکه شخص سومی به عنوان واسطه مورد استفاده قرار گیرد، با یکدیگر در ارتباط هستند. در این روش دیگر نهاد واسطه متمرکز برای بررسی تراکنش‌ها و اطلاعات وجود ندارد و اطلاعات به صورت مستقیم در میان کاربران منتشر می‌شود.

در سیستم‌های متمرکز مانند بانک‌ها، هنگام انجام یک تراکنش، اطلاعات تراکنش ابتدا به سرورهای مرکزی بانک می‌رود و بانک اطلاعات حساب طرف فرستنده و گیرنده را بررسی می‌کند. در صورتی که امکان انجام تراکنش وجود داشته باشد، تراکنش تایید می‌شود و مبلغ مورد نظر به حساب گیرنده واریز می‌گردد.

در بسیاری از شبکه‌های متمرکز مانند شبکه‌های اجتماعی، انتقال داده به این شکل انجام می‌شود. لازم به ذکر است که تایید این اطلاعات توسط سیستم غیرمتمرکز از سوی کاربران در سراسر دنیا انجام می‌شود و یکی از **ویژگی‌های اصلی رمزارزها**، امکان انجام تراکنش‌های همتا به همتا با آن‌ها است.

# آشنایی با اصطلاحات عامیانه درباره ارزهای دیجیتال

در ادامه با اصطلاحات عامیانه درباره ارزهای دیجیتال آشنا می‌شویم.

## صرافی (Exchange)



صرافی بستری است که کاربران دنیای کریپتوکارنسی‌ها می‌توانند از طریق آن، به [خرید و فروش بیت کوین](#) و سایر رمزارزها مشغول شوند. در صرافی می‌توان ارزها را با یکدیگر و بین اشخاص به صورت آنلاین مبادله کرد. همچنین صرافی‌ها می‌توانند در ارائه انواع رمزارزها و کارمزد آنها، متفاوت باشند.

## صرافی غیرمتمرکز (Dex)

**صرافی‌های غیرمتمرکز ارز دیجیتال**، برنامه‌های مبتنی بر بلاک چین هستند که معاملات بزرگ دارایی‌های رمز ارزی را در میان بسیاری از کاربران هماهنگ می‌کنند. این نوع از صرافی‌ها، از طریق الگوریتم‌های خودکار این کار را انجام می‌دهند و به عنوان واسطه مالی بین خریداران و فروشندگان عمل می‌کنند.

## آربیتراژ (Arbitrage)

به [خرید ارز دیجیتال](#) از یک صرافی و کسب سود از فروش با استفاده از اختلاف قیمت آن ارز در صرافی‌های دیگر آربیتراژ گفته می‌شود. آربیتراژ فرصتی برای به دست آوردن سود با ریسک کم است و با در نظر گرفتن این که ارزهای دیجیتال در صرافی‌های گوناگونی عرضه می‌شوند و نوسان زیادی دارند، امکان آربیتراژ در دنیای ارز دیجیتال فراهم است.

## تایید شده (Confirmed)

در دنیای ارزهای دیجیتال هنگامی که یک تراکنش تایید شد، این معنی را به همراه دارد که توسط شبکه تایید شده است. در **صنعت ارز دیجیتال**، معیار تایید نشان می‌دهد که دقیقاً چند بلاک از زمان اضافه شدن یک تراکنش به یک بلاک چین سپری شده است.

## متمرکز (Centralized)

اصطلاح متمرکز به موسسه یا سازمانی گفته می‌شود که توسط فرد یا گروهی کنترل می‌گردد.

## غیرمتمرکز (Decentralized)

غیر متمرکز این معنا را دارد که در [معاملات ارزهای دیجیتال](#)، مبادلات به صورت همتا به همتا و غیرمتمرکز انجام شوند. برای مثال فروشنده و خریدار به صورت مستقیم با یکدیگر ارتباط دارند و واسطه‌ای مانند سازمان در میان آن‌ها قرار ندارد.

اما در سیستم‌های بانکداری، دولت‌ها انتقال پول از یک حساب به حساب دیگر را توسط یک واسطه به نام بانک که به اطلاعات هر دو حساب دسترسی دارند، انجام می‌شود. با عدم وجود مرجع مرکزی، رمزارزها نسبت به ارزهای فیات مثل دلار، ریال و سایر روش‌های پرداختی مزایای خاصی دارند و غیرمتمرکز بودن می‌تواند مهم‌ترین ویژگی کوین‌ها و سایر رمزارزها قلمداد شود.

## دائو (DAO)

دائو اصطلاحی آشنا در دنیای ارزهای دیجیتال است که مخفف عبارت Autonomous Decentralized Organization به سازمان‌های خود مختار غیر متمرکز گفته می‌شود. اصطلاح دائو نوعی رویکرد در اداره سازمان است که در آن هر عضوی از مجموعه فارغ از جایگاه و سمت، حقی یکسان در ایجاد تغییرات به عهده دارد. دائوها قراردادهای هوشمندی هستند که بیشتر آن‌ها بر روی بلاک چین اتریوم اجرا شده‌اند؛ اما هر بلاک چینی که از فناوری قراردادهای هوشمند پشتیبانی کند، می‌تواند میزبان یک دائو باشد.

## دیفای (DeFi)

کلمه DeFi مخفف کلمه Decentralized Finance به **سیستم مالی غیر متمرکز** اطلاق می‌شود که شامل دارایی‌های دیجیتال، پروتکل‌ها، قراردادهای هوشمند و نرم‌افزارهای غیرمتمرکز بر بستر بلاک چین است.

دیفای به هر ابزار مالی مانند قرارداد هوشمند یا DAO گفته می‌شود که از فناوری بلاک چین برای دور زدن موسسات واسطه استفاده می‌کند.

دیفای از فناوری پشت ارز دیجیتال بیت کوین الهام گرفته شده است و به نهادهای گوناگون اجازه می‌دهد تا نسخه‌ای از تاریخچه معاملات را نگهداری کند که این‌گونه دیگر تراکنش‌ها توسط منبع مرکزی کنترل نمی‌گردند.

### **برنامه های غیرمتمرکز (Decentralized Application (dApp**

کلمه dApp مخفف عبارت Decentralized Application نوعی برنامه نرم افزاری منبع باز توزیع شده است که در شبکه بلاک چین هم‌تا به هم‌تا (P2P) اجرا می‌شود. این برنامه‌ها به سایر برنامه‌های نرم افزاری شباهت دارند که در یک وب سایت یا دستگاه تلفن همراه به صورت P2P پشتیبانی می‌شوند.

ماهیت غیرمتمرکز بودن این برنامه یعنی زمانی که یک توسعه‌دهنده پایگاه، کد dApp را منتشر کرد، دیگران نیز می‌توانند بر روی آن بسازند. یک dApp برای ایجاد انواع برنامه‌ها، از جمله برنامه‌های مالی غیرمتمرکز، مرور وب، بازی‌ها و رسانه‌های اجتماعی توسعه می‌یابد.

### **ارزش بازار (Market Capitalization)**

رمزارها بر اساس ارزش بازار رتبه دهی می‌شوند و ارزش بازار یا مارکت کپ از ضرب قیمت فعلی ارز دیجیتال موردنظر در تعداد کل ارزهای در گردش بدست می‌آید و ارزش نقدی آن را شامل می‌شود. برای مشاهده **ارزش بازار ارز دیجیتال** مورد نظر خود، می‌توانید به سایت CoinMarketCap مراجعه کرده و جایگاه رمزارها را بررسی نمایید. به عنوان مثال در حال حاضر بیت کوین در رتبه 1 در میان سایر ارزهای دیجیتال قرار گرفته است.

# آشنایی با اصطلاحات رایج درباره کوین‌ها



احتمالا بیت کوین اولین کوینی است که پس از شنیدن کلمه ارز دیجیتال به ذهن‌تان می‌آید. اما اصطلاحات رایج درباره کوین‌ها وسیع‌تر از این حرف‌ها است که در ادامه با مفاهیم موجود در این زمینه آشنا می‌شویم.

## بیت کوین (BTC و XBT)

اولین کریپتوکارنسی که معروفیت بسیار زیادی دارد، بیت کوین است. بیت کوین به صورت غیرمتمرکز عمل کرده و هیچ کس نمی‌تواند آن را کنترل کند. این موضوع موجب ارزش او بیش از پول رسمی هر کشور است و بیشتر تامین کنندگان، بیت کوین را به عنوان نوعی پول قبول می‌کنند.

## ساتوشی (Satoshi)

ساتوشی ناکاموتو نام **خالق بیت کوین** است و ساتوشی به کوچک‌ترین واحد بیت کوین اطلاق می‌شود. هر بیت کوین را می‌توان به 100 میلیون واحد تقسیم کرد و هر ساتوشی را یک صد میلیونم بیت کوین نامید. برای دریافت اطلاعات تکمیلی شما می‌توانید مطلب [ساتوشی ناکاموتو کیست](#) را بخوانید.

## توکن (Token)

نوع دوم رمزارزها به عنوان توکن شناخته می‌شوند. توکن‌ها رمزارزهایی هستند که بلاک چین مخصوص به خود را ندارند و با استفاده از قرارداد هوشمند بر روی یک بلاک چین ساخته می‌شوند. در حقیقت توکن نام تراشه‌هایی است که با پول خریداری می‌شود و برای خرید کالا یا خدمات برای مثال خرید غذا در یک رستوران، به کار می‌روند.

در دنیای بلاکچین، این کلمه به همان معنی است، اما در معنای مجازی، توکن‌ها واحدهای با ارزشی هستند که از طریق بلاک چین به دست می‌آیند و همچنین برای خرید کالاها و خدمات استفاده می‌شوند.

## آلت کوین (Altcoin)

آلت کوین‌ها رمزارزهایی هستند که بعد از بیت کوین ایجاد شده‌اند و این اصطلاح به تمامی ارزهای دیجیتال اختراع شده بعد از بیت کوین اطلاق می‌شود. آلت کوین از دو کلمه Bitcoin Alternative یا Coin Alternative تشکیل شده است و در حال حاضر نزدیک به نه هزار آلت کوین وجود دارد. شما می‌توانید مطلب [آلت کوین چیست](#) را بخوانید تا به صورت کامل این مفهوم را متوجه شوید.

## آلت سیزن (Altseason)

آلت سیزن (Altseason) به معنای فصل آلت کوین است و به دوره‌ای گفته می‌شود که قیمت آلت کوین‌ها رشد بیشتری نسبت به بیت کوین داشته است. در حقیقت آلت سیزن دوره کوتاهی است که در آن پول از بیت کوین خارج می‌شود و باعث افزایش قابل توجه و سریع قیمت برای اکثر ارزهای دیجیتال می‌شود.

## کوین‌هایی با قیمت ثابت (StableCoin)

در دنیای رمزارزها، کوین‌هایی هستند که ارزش آن‌ها با یک دارایی ثابت مانند دلار برابر است که به این کوین‌ها، استیبل کوین گفته می‌شود؛ به عنوان مثال قیمت استیبل کوینی مانند تتر، یک دلار است. استیبل کوین‌ها با هدف کاهش نوسانات بازار ایجاد شده‌اند و برخلاف دیگر رمزارزها که قیمت پایداری ندارند، می‌توانند از سرمایه معامله‌گران محافظت کنند.

در دنیای ارز دیجیتال استیبل کوین‌های زیادی وجود دارند. برخی از استیبل کوین‌ها بر پایه طلا و جواهرات هستند، برخی بر پایه دلار و یورو و برخی از این استیبل کوین‌ها بر پایه ارز دیجیتال‌های معتبری نظیر بیت کوین هستند. پیشنهاد می‌کنیم تا قبل از سرمایه‌گذاری بر روی استیبل کوین‌ها، مطلب [استیبل کوین چیست](#) را مطالعه نمایید.

## عرضه اولیه سکه (Initial Coin Offering)

عرضه اولیه سکه یکی از روش‌هایی است که در آن شرکت، یک ارز دیجیتال جدید را برای جمع‌آوری سرمایه به فروش می‌رساند. در روش عرضه اولیه سکه، سرمایه‌گذاران می‌توانند با استفاده از دیگر رمزارزها مانند بیت‌کوین یا ارزهای فیات مانند دلار، بر روی پروژه موردنظر سرمایه‌گذاری کرده و توکن‌های مربوط به آن پروژه را از سوی شرکت مربوطه دریافت نمایند.

این مفهوم با گسترش استفاده از قراردادهای هوشمند در شبکه اتریوم در سال 2017 گسترش پیدا کرد و بسیاری از **پروژه‌های ارز دیجیتال** از عرضه اولیه برای به دست آوردن سرمایه اولیه برای ادامه پروژه استفاده کرده‌اند. عرضه اولیه سکه قبل از راه اندازی پروژه انجام می‌شود و توکن‌های پروژه به فروش می‌رسد.

روش‌های گوناگونی برای عرضه اولیه ارزهای دیجیتال وجود دارد که از مهم‌ترین آن‌ها می‌توان به عرضه اولیه در صرافی متمرکز (IEO) و عرضه اولیه در صرافی غیرمتمرکز (IDO) اشاره کرد. لازم به ذکر است که عرضه اولیه در صرافی‌های متمرکز بزرگ به دلیل بررسی پروژه توسط مدیران صرافی اعتبار بیشتری نسبت به صرافی‌های غیرمتمرکز دارند.

## عرضه در گردش (Circulating Supply)

به کوین یا سکه‌هایی است که برای عموم قابل دسترسی است؛ عرضه در گردش یا سرمایه در گردش گفته می‌شود. البته لازم به ذکر است که این اصطلاح با عرضه کل (Total supply) یا حداکثر عرضه (Max supply) تفاوت بسیار زیادی دارد.

این اصطلاح به تعداد کوین‌ها یا توکن‌های منحصربه‌فرد یک پروژه اشاره می‌کند که در حال حاضر در دسترس عموم قرار دارند. عرضه در گردش (Supply Circulating)، به تعداد کل توکن‌هایی که به طور فعال برای تجارت در دسترس هستند و در بازار توسط عموم مردم استفاده می‌شوند، اطلاق می‌شود.

## سوزاندن سکه (Burned)

اصطلاح سوزاندن در دنیای ارزهای دیجیتال به معنی حذف دائمی تعدادی توکن در گردش است که معمولاً با انتقال توکن‌های مورد نظر به آدرس کیف پول غیر قابل بازیابی، انجام می‌شود. هنگامی که کوین‌های مد نظر خود را به آدرس مخصوص انتقال می‌دهید، دیگر آدرس خصوصی که از آن آدرس ارسال شده، وجود ندارد تا بتوانید عملیات برداشت را انجام دهید. این موضوع که کوین‌ها سوزانده می‌شوند شاید کار غیر منطقی باشد؛ اما این کار با اهداف گوناگونی انجام می‌شود.

# آشنایی با اصطلاحات رایج درباره سرمایه گذاری ارزهای دیجیتال

سرمایه گذاری در دنیای ارزهای دیجیتال در صورتی که آگاهانه انجام شود، می تواند سودمند باشد. در ادامه برخی از اصطلاحات رایج درباره سرمایه گذاری ارزهای دیجیتال را شرح می دهیم.

## پامپ و دامپ (Dump & Pump)

هنگامی که برخی از سرمایه گذاران تصمیم بگیرند قیمت رمزارزها را به صورت مصنوعی افزایش یا کاهش دهند، پامپ و دامپ رخ می دهد. گروهی از سرمایه گذاران زمانی که قیمت یک رمزارز پایین است، اقدام به خرید می کنند و سپس، با تبلیغات و اخبار دروغین باعث افزایش قیمت می شوند که این پدیده را پامپ می گویند. این سرمایه گذاران پس از افزایش قیمت به دیگران اعلام می کنند که اکنون بهترین زمان برای خرید است. بنابراین، تقاضا برای آن رمزارز زیاد می شود و سرمایه گذاران سودجو ارزهای خود در بالاترین قیمت به فروش می رسانند. بعد از مدتی که قیمت ها کاهش پیدا کرد، افراد بی تجربه بخشی از سرمایه خودشان را در این بازار از دست می دهند که به این پدیده کاهش پیدا کردن دامپ می گویند.

## نگهداری ارز دیجیتال به مدت طولانی (HODL)

هودل اولین بار برای بیت کوین به کار برده شد اما در حال حاضر این عبارت به معنی نگه داشتن و به فروش نرساندن ارزهای دیجیتال در شرایط نوسانات بازار است. این اصطلاح زمانی به وجود آمد که یکی از کاربران سایت بیت کوین تاک، پیام I AM HODLING (من در حال هودل کردن هستم) را منتشر کرد.

این کاربر به اشتباه به جای کلمه HOLD، کلمه HODL را نوشت که یک اشتباه تایپی بود. پس از مدتی، اصطلاح هودل در جامعه کریپتو رواج پیدا کرد و به نگهداری بلند مدت بیت کوین و سایر رمزارزها در جامعه جهانی کریپتو، هودل گفته شد.

## نمودار عمق بازار (Depth Chart)

نمودار عمق بازار، به عنوان ابزاری برای درک عرضه و تقاضای ارز دیجیتال در یک لحظه معین برای طیف وسیعی از قیمت ها به کار می رود. این نمودار درخواست های خرید که به پیشنهادات معروف است و درخواست های فروش را که به درخواست معروف است را بر روی نمودار نمایش می دهد. نمودار عمق بازار با دو حالت تجمعی یا همان خطی و غیر تجمعی یا همان میله ای، به معامله گران کمک می کند تا با بررسی نمای کلی سفارشات ثبت شده و حجم عرضه و تقاضا در قیمت های مختلف در نمادهای مورد نظر را بررسی کنند.

## فومو یا ترس از دست دادن (FOMO)

فومو مخفف عبارت Fear of Missing Out است و در زبان فارسی ترس از دست دادن معنا می شود. این اصطلاح به ارزهای دیجیتال اختصاص ندارد و به کسانی گفته می شود که با افزایش ارزش برخی سرمایه ها، با از دست



دادن فرصت‌های احتمالی و از روی هیجان و اقدامات احساسی، اقدام به خرید می‌کنند تا از بقیه سرمایه‌گذاران عقب‌نمانند.

هنگامی که فرد سهمی را نمی‌خرد و ارزش آن سهم بالا می‌رود، احساس جا ماندن از دیگران به او دست می‌دهد که به آن فومو می‌گویند. در حالت کلی، احساسات و هیجاناتی که باعث می‌شوند یک سهامدار در مواقع بالا بودن قیمت‌ها تصمیمات نادرستی بگیرد، فومو نام دارد.

## اوج قیمت بی سابقه (ATH)

این اصطلاح کاربرد زیادی در بازار ارزهای دیجیتال دارد و برای توصیف شرایطی به کار می‌رود که در آن ارزش دیجیتال به بالاترین قیمت خود رسیده است. این اصطلاح از عبارت all time high گرفته شده و مخفف آن ATH یکی از امیدوارکننده‌ترین اصطلاحات و به معنای افزایش قیمت ارز و رمزارزها است. اگر یکی از ارزهای دیجیتال به رکورد جدیدی در تاریخ رسیده باشد، از این اصطلاح استفاده می‌کنند.

## کمترین قیمت بی سابقه (ATL)

اصطلاح کمترین قیمت بی سابقه (ATL) مقابل اصطلاح اوج قیمت بی سابقه (ATH) قرار دارد. این اصطلاح از عبارت all time low گرفته شده است و زمانی استفاده می‌شود که ارزش ارز دیجیتال به کمترین میزان در طول تاریخ رسیده باشد.

## قیمت به اوج رسیده (TO THE MOON)

اصطلاح TO THE MOON در بیان اخبار صعود بسیار بزرگ یک دارایی استفاده می‌شود. در حقیقت این اصطلاح برای توصیف ارزش یک ارز دیجیتال در حال تجربه روند صعودی شدیدی در بازار است، به کار می‌رود. برخی از افراد عقیده دارند TO THE MOON به افزایش شدید ارزش ارزهای دیجیتال در آینده نزدیک اشاره می‌کند.

## نابود شده (Rekt)

این اصطلاح برای توصیف خسارت مالی بسیار شدید بر اثر سرمایه‌گذاری بد استفاده می‌شود و همچنین این اصطلاح برای توصیف افت شدید ارزش بازار و از دست دادن کل دارایی به کار می‌رود.

## خرس (Bear)

در میان اصطلاحات ارز دیجیتال، به افرادی که همیشه حس بدبینی نسبت به قیمت ارزها دارند و روند بازار را رو به پایین پیش‌بینی می‌کنند، خرس گفته می‌شود. این اصطلاح به شرایط نزولی بازار اشاره می‌کند و زمانی که

سرمایه گذاران به شرایط بازار اعتماد ندارند، این اصطلاح را به کار می‌برند. برای مثال بازار خرسی (Bear Market) به معنای بازار نزولی و رو به پایین است.

## تله خرسی (Bear Trap)

هنگامی که افت ارزش سهام به صورت موقتی رخ می‌دهد، برخی از سرمایه داران به اشتباه سیگنال‌هایی دریافت می‌کنند که طی آن قیمت‌های ساختگی به کاربران نشان داده می‌شود. همچنین این سیگنال‌ها نشان می‌دهند روند نزولی بازار ادامه دارد و به همین دلیل با فروش سهام خود ضرر می‌کنند. در این شرایط اصطلاح تله خرسی را برای سرمایه داری که به این وضعیت گرفتار شده است، اطلاق می‌شود.

## گاوی (BULL)

اصطلاح BULL به کاربرانی گفته می‌شود که همواره نسبت به بالا رفتن ارزش سرمایه‌های خود امید دارند و نسبت به بازار و قیمت‌ها خوشبین هستند. از واژه گاوی در حوزه اقتصاد، برای بیان موارد صعودی و افزایشی یک دارایی استفاده می‌شود؛ برای مثال بازار گاوی (Bull Market) به معنای بازار صعودی و رو به بالا است. در صورتی که بازار روند صعودی داشته باشد، سرمایه‌گذاران با اطمینان خاطر معامله انجام دهند و این امید به افزایش قیمت‌ها، بازار گاوی را ایجاد می‌کند.

## تله گاوی (Bull Trap)

تله گاوی مانند تله خرسی نیز حاصل سیگنال اشتباه است و در تحلیل تکنیکال ایجاد می‌شود. تنها تفاوت تله گاوی با تله خرسی در این است که در تله گاوی، روند نزولی بازار از دید سرمایه‌گذاران پنهان می‌ماند تا آن‌ها متقاعد شوند که بازار به حالت صعودی خود بازگشته است. به همین ترتیب، کاربران در حالی که از سیر نزولی قیمت‌ها آگاهی ندارند، به معامله‌های خود ادامه می‌دهند که در بیشتر مواقع به ضرر آنها منجر می‌شود.

## نهنگ (Whale)

اصطلاح نهنگ برای توصیف افرادی به کار می‌رود که تراکنش‌هایی با حجم بسیار بالا انجام می‌دهند که پول زیادی در بازار برای خرید مقدار زیادی رمزارز، سهام یا هر نوع دارایی دارند. نهنگ‌ها به عنوان معامله‌گران سرمایه دار، روی آینده یک ارز دیجیتال خوش بین و یا مبالغ سنگینی سرمایه گذاری می‌کنند که به آن‌ها نهنگ‌های گاوی (صعودی) نیز می‌گویند.

استراتژی‌هایی که توسط افراد نهنگ به کار می‌رود، تاثیر زیادی بر وضعیت بازار ارز دیجیتال دارد که این تاثیرات می‌توانند مثبت و یا منفی باشند. لازم به ذکر است که توانایی نهنگ‌ها برای خرید، می‌تواند نوسان‌های شدیدی در بازار را در پی داشته باشد.

# آشنایی با اصطلاحات رایج درباره کیف پول ارزهای دیجیتال



کیف پول ارز دیجیتال یکی از مهم‌ترین ابزارهای کاربران دنیای کریپتوکارنسی‌ها است و آشنایی به اصطلاحات رایج در این زمینه برای هر سرمایه‌گذاری ضرورت دارد. در ادامه با اصطلاحات رایج در این زمینه آشنا می‌شویم.

## کیف پول (Wallet)

کیف پول ارزهای دیجیتال از اصطلاحات رایج دنیای کریپتوکارنسی‌ها است که به کاربران این امکان را می‌دهد تا ارزهای دیجیتال را ذخیره کرده و معاملات خود را از این طریق انجام دهند. در کیف پول از کلیدهای عمومی و خصوصی استفاده می‌شود.

## کیف پول سرد (Cold Wallet)

کیف پول سرد یکی از انواع کیف پول ارزهای دیجیتال است که کاربران می‌توانند به صورت آفلاین به آن دسترسی داشته باشند. در این حالت امکان دسترسی آنلاین به رمزارزها از بین می‌رود و در نتیجه امنیت آن بیشتر می‌شود.

در حقیقت کیف پول‌های سرد امنیت بیشتری نسب به کیف پول‌های گرم دارند؛ چراکه هکرها برای دستیابی به کیف پول کاربران، به دسترسی فیزیکی نیازمنداند. لازم به ذکر است که **نگهداری آفلاین ارزهای دیجیتال** در کیف پول‌های سرد هزینه بیشتری در مقایسه با روش‌های گرم یا آنلاین دارد.

## کیف پول گرم (Hot Wallet)

کیف پول گرم یکی دیگر از انواع کیف پول ارزهای دیجیتال است که کاربران می‌توانند به صورت آنلاین به آن دسترسی داشته باشند. این کیف پول‌ها به اینترنت متصل هستند و می‌توانند یک برنامه تحت وب یا یک برنامه موبایل باشند.

استفاده از کیف پول‌های گرم آسان است، اما در مقایسه با سایر کیف پول‌ها مانند کیف پول سرد امنیت کمتری دارند؛ چراکه ممکن است هکرها بتوانند از طریق اینترنت به این نوع کیف پول‌ها دسترسی پیدا کنند. کیف پول‌های گرم برای مدت زمان طولانی مناسب نیستند اما برای کسانی که به صورت مداوم در حال خرید ارز هستند پیشنهاد می‌شود.

## کیف پول نرم افزاری (Software Wallet)

کیف پول‌های نرم افزاری یک شکل رایج از کیف پول هستند که در آن کلید خصوصی برای فرد در پرونده‌های نرم افزاری روی کامپیوتر ذخیره می‌شود. از کیف پول‌های نرم افزاری می‌توان به تراست ولت اشاره کرد.

## کیف پول سخت افزاری (Hardware Wallet)

کیف پول سخت افزاری وسیله‌ای فیزیکی، شبیه به USB است که اطلاعات مربوط به رمزارزها را در خود ذخیره می‌کند. لازم به ذکر است که این کیف پول‌ها امن‌ترین راه برای نگهداری رمزارزها محسوب می‌شود. از کیف پول‌های سخت افزاری می‌توان به لجر نانو اس اشاره کرد.

## کیف پول کاغذی (Paper Wallet)

ذخیره کردن رمز کیف پول (کلید خصوصی) بر روی یک سند فیزیکی، آن کیف پول را به یک کیف پول کاغذی تبدیل می‌کند.

## ذخیره سازی سرد (Cold Storage)

اصطلاح ذخیره سازی سرد، برای یک کیف پول کاغذی یا کیف پول سخت‌افزاری استفاده می‌شود. ذخیره سازی سرد روشی برای نگهداری آفلاین توکن‌های ارزهای دیجیتال است که می‌توان گفت هدف سرمایه‌گذاران ارزهای

دیجیتال برای استفاده از ذخیره‌سازی سرد، جلوگیری از دسترسی هکرها به دارایی‌های آن‌ها از طریق روش‌های سنتی است.

## آدرس کیف پول (Address)

آدرس کیف پول، رشته‌ای از حروف و اعداد را شامل می‌شود که به عنوان شماره حساب برای معاملات رمزنگاری شده مورد استفاده قرار می‌گیرند. هر کوین از یک آدرس منحصر به فرد تشکیل شده است که مشخص می‌کند روی بلاک چین قرار دارد و این آدرس‌ها می‌توانند به صورت عمومی به اشتراک گذاشته شوند.

این آدرس، نوعی موقعیت مکانی است که در آن داده‌ها ذخیره شده و هر گونه تغییر در آن به ثبت می‌رسد. برای [خرید و فروش بیت کوین](#) و سایر رمزارزها، تنها موردی که باید در اختیار دیگران قرار بگیرد، همین آدرس کیف پول است. البته لازم به ذکر است که اگر بخواهید تراکنشی در شبکه انجام دهید، می‌توانید از یک آدرس منحصر به فرد و جدید استفاده کنید.

## کلید عمومی (Public Key)

کلید عمومی به عنوان یک آدرس کیف پول منحصر به فرد شناخته می‌شود که شامل رشته‌ای از اعداد و حروف است. عملکرد کلید عمومی به شماره حساب بانکی شباهت دارد و برای دریافت رمزارز استفاده می‌شود.

## کلید خصوصی (Private key)

اصطلاح کلید خصوصی به رشته‌ای از اعداد و حروف که برای دسترسی به کیف پول کاربران اطلاق می‌شود. کلید خصوصی، رمز عبور کیف پول ارزها است که کاربران باید از آن مراقبت کنند. هنگام فروش یا برداشت رمزارزها به این کلید نیاز است؛ چراکه این کار به عنوان امضای دیجیتالی محسوب می‌شود.

## امضا (Signature)

هنگامی انجام یک معامله در شبکه بلاک چین، معامله با کلید خصوصی خود کاربر امضا شود. این امضای رمزنگاری شده، به کاربران اجازه می‌دهد تا مالکیت خود را اثبات کنند. امضای دیجیتال مقداری رمزنگاری است که از داده‌ها و یک کلید مخفی که فقط امضا کننده آن را می‌شناسد، محاسبه می‌شود. در دنیای واقعی، گیرنده پیام به اطمینان نیاز دارد که پیام متعلق به فرستنده باشد و او نباید بتواند منشأ آن پیام را انکار کند.

# آشنایی با اصطلاحات رایج درباره استخراج ارزهای دیجیتال



[استخراج ارز دیجیتال](#) یکی از روش‌های کسب درآمد در دنیای کریپتوکارنسی‌ها قلمداد می‌شود. در ادامه با اصطلاحات ارزهای دیجیتال در زمینه استخراج آشنا می‌شویم.

## ماینر (Miner)

ماینر به کامپیوتر یا تجهیزاتی گفته می‌شود که بر اساس توان محاسباتی خود، یک رمز ارز خاصی را استخراج می‌کند.

مطلب پیشنهادی : [دستگاه‌های استخراج ارز دیجیتال چگونه کار می‌کنند؟](#)

## استخراج (Mining)

ماینینگ به فرایندی گفته می‌شود که تایید تراکنش‌ها با استفاده از کامپیوترها و بر اساس حل مسائل ریاضی به صورت رمز نگاری شده انجام شده، صورت می‌گیرند. البته لازم به ذکر است در مرحله آخر پس از تایید صحت تراکنش، بلاک جدیدی به زنجیره بلاک‌های قبلی افزوده می‌شود.

## مزرعه استخراج (Mining Farm)

فرایند استخراج یا ماینینگ توسط سخت افزارهایی با توان ویژه انجام می‌شود که مصرف برق زیادی دارند. برخی افراد تعداد بسیاری از این دستگاه‌ها را خارج از شهر در یک سوله قرار داده و فرایند استخراج را آغاز می‌کنند. به محوطه‌ای که این دستگاه‌ها در آن قرار می‌گیرند؛ مزرعه استخراج گفته می‌شود که اگر در این محوطه‌ها بیت کوین مورد استخراج قرار بگیرد، به آن Bitcoin Farm می‌گویند.

مطلب پیشنهادی : [فارم ماینینگ \(مزرعه استخراج رمزارز\) چیست؟](#)

## ریگ استخراج (Mining Rig)

ریگ استخراج یا ماینینگ ریگ به تجهیزات لازم برای استخراج رمزارزها گفته می‌شود. امکان دارد ریگ‌های به کار رفته در فرایند استخراج تخصصی باشند و یا به کامپیوتر شخصی اختصاص بیابند.

## استخراج ابری (Cloud Mining)

از اصطلاح استخراج ابری زمانی استفاده می‌شود که شخصی بدون داشتن تجهیزات شخصی برای استخراج، مبلغی را به صورت ماهیانه به یک شرکت استخراج کننده ارزهای دیجیتال پرداخت می‌کند تا به جای این شخص فرایند ماینینگ را انجام دهند. سود حاصل از استخراج ابری یا کلود ماینینگ در مقایسه با استخراج مستقیم کمتر است و امکان ضرر دهی وجود دارد. البته لازم به ذکر است که هزینه‌های مربوط به تجهیزات، نگهداری، برق، محوطه و غیره با این روش حذف می‌شوند.

## استخر استخراج (Mining Pool)

هنگامی که تعدادی از ماینرها قدرت محاسباتی خود را در کنار هم جمع کرده و تلاش کنند تا بمعاملات مورد نیاز برای شروع یک بلوک جدید در زنجیره را تکمیل نمایند، در واقع در یک استخر استخراج قرار می‌گیرند. پاداش این ماینرها بر اساس میزان مشارکت آن‌ها، میان کسانی که در استخر قرار دارند، تقسیم می‌شود. هدف اصلی این است که حضور در یک استخر استخراج ارزش دیجیتال، شانس بیشتری برای داشتن هش‌های موفق فراهم می‌کند.

## پاداش بلاک (Block Reward)

ماینرها تراکنش هر بلاک را تایید کرده و باعث می‌شوند بلاک بسته شود و به زنجیره بلاک‌های قبلی اضافه گردد. این ماینرها به ازای کاری که در شبکه بلاک چین انجام می‌دهند، رمزارز پاداش می‌گیرند.

## گواه اثبات کار (Proof of work)

گواه اثبات کار یکی از اصطلاحات دنیای ارزهای دیجیتال است که در طی آن ماینرها ثابت می‌کنند روی حل یک مسئله ریاضی در شبکه کار کرده‌اند. هر ماینری که بتواند مسئله موردنظر را حل کند، می‌تواند بلاک جدید را به بلاک چین اضافه نماید.

## گواه اثبات سهام (Proof of Stake)

گواه اثبات سهام نوعی مکانیزم اجماع است که ماینرها بر اساس تعداد رمزارزهایی که در اختیار دارند، انتخاب می‌شوند. به این صورت که هر چه دارایی یا سهام ماینر بیشتر باشد، شانس بیشتری برای تایید بلاک‌های جدید خواهد داشت.

## آشنایی با اصطلاحات رایج درباره تراکنش ارزهای دیجیتال

تراکنش‌های ارز دیجیتال، هسته اصلی این دنیای هیجان انگیز را در بر دارند. در ادامه با اصطلاحات رایج درباره تراکنش ارزهای دیجیتال آشنا می‌شویم:

### تایید (Confirmation)

هر بار که تراکنش جدیدی در شبکه انجام می‌شود، ماینرها اعتبار و صحت تراکنش را بررسی و تأیید می‌کنند. برای اینکه تراکنش کاربران صورت بگیرد، باید تاییدیه‌های موردنیاز از شبکه دریافت شوند.

### کارمزد تراکنش (Transaction Fees)

برای انجام تراکنش در شبکه رمزارزها، کاربران باید هزینه‌ای بابت تایید تراکنش پرداخت کنند. این هزینه‌ها با توجه به وضعیت شبکه و ترافیک آن، متغیر است و اگر بخواهند تراکنش خود سریع‌تر تایید شود، باید کارمزد بیشتری پرداخت کنند.

### عبارت بازیابی (Recovery Phrase)

عبارت بازیابی 24 کلمه دارد و کاربران باید آن را به دور از دسترس دیگران قرار دهند. از این عبارت می‌توان برای انتقال رمزارزها از یک کیف پول دیجیتال به کیف پولی دیگر استفاده کرد.



## شناسه تراکنش ارز دیجیتال (Tx ID)

تراکنش رمزارز به فرایندی گفته می‌شود که در طی آن کاربران رمزارز جدید دریافت کرده و یا به شخص دیگری ارسال می‌کنند. هر یک از تراکنش‌هایی که در معاملات ارزهای دیجیتال انجام می‌شوند، دارای یک شناسه هستند. شناسه هر تراکنش منحصر به فرد است و با دیگر تراکنش‌ها تفاوت دارد که البته از این شناسه‌ها برای پیگیری و بررسی وضعیت تراکنش‌ها استفاده می‌شود.

## استاپ لیمیت (Stop Limit)

استاپ لیمیت یا Stop Limit یکی از اصطلاحاتی است که در صرافی‌های ارز دیجیتال با آن روبه‌رو می‌شوید. استاپ لیمیت این امکان را فراهم می‌کند تا هر کاربری میزان سود و زیان خود در بازار را مشخص کند.

# آشنایی با اصطلاحات تخصصی ارزهای دیجیتال

## آشنایی با اصطلاحات تخصصی ارزهای دیجیتال



در این بخش به شرح اصطلاحات تخصصی ارزهای دیجیتال می‌پردازیم:

### هش (Hash)

هش به نوعی خروجی گفته می‌شود که از اطلاعات ورودی بدست می‌آید. الگوریتم هش، اطلاعات ورودی را در هر اندازه‌ای که باشند دریافت می‌کند و به تولید یک خروجی با اندازه ثابت می‌پردازد. هش را می‌توان اثر انگشت دیجیتالی نیز عنوان کرد که از طریق پردازش اطلاعات توسط تابع هش ایجاد می‌شود. این فرایند به صورت خطی و یکطرفه صورت می‌گیرد و از طریق هش ایجاد شده، نمی‌توان به داده‌های اصلی یا همان اطلاعات ورودی دست پیدا کرد. لازم به ذکر است که هش بیت کوین 64 رقمی بوده و با صفر شروع می‌شود.

### نرخ هش (Hash Rate)

نرخ هش نشان می‌دهد که کامپیوتر کاربران تا چه اندازه‌ای توان تولید دارد و سرعت انجام عملیات استخراج و عملکرد آن چقدر است. یکی از مهم‌ترین فاکتورهای انتخاب دستگاه استخراج نرخ هش محسوب می‌شود.

## هارد فورک (Hard Fork)

هارد فورک به تغییرات اساسی در پروتکل رمزارز اطلاق می‌شود که در حقیقت آن را به 2 ارز متفاوت تبدیل می‌کند. در هارد فورک، نسخه جدید با نسخه‌های قبلی سازگار نیست؛ برای مثال بیت کوین کش (فورک بیت کوین) که یکی از تغییرات اعمال شده در آن نسبت به بیت کوین، افزایش حجم بلاک‌ها است. هارد فورک زمانی ایجاد می‌شود که برخی از ماینرها تصمیم می‌گیرند قوانین جدیدی را برای رمزارز موردنظر ایجاد کنند. افرادی که با این تغییرات مشکلی ندارند، به فورک جدید می‌پیوندند. افرادی هم که مخالف تغییرات جدید هستند، می‌توانند از همان نسخه قبلی استفاده نمایند.

مطلب پیشنهادی: [ایردراپ چیست؟ و نحوه دریافت ارز دیجیتال رایگان](#)

## سافت فورک (Soft Fork)

در سافت فورک، یک تغییر جزئی در پروتکل رمزارز موردنظر ایجاد می‌شود که این تغییر در مقایسه با نسخه‌های قبلی سازگار است.

## دفتر کل مرکزی (Central Ledger)

دفتر کل مرکزی به سازمانی گفته می‌شود که داده‌های مربوط به تراکنش‌ها و سایر موارد شبیه به آن را به صورت سازماندهی شده نگهداری می‌کند.

## دفتر کل توزیع شده (Distributed Ledger)

دفتر کل توزیع شده سیستمی است که در آن تمام اطلاعات مربوط به تراکنش‌ها و مقدار سرمایه‌ها به صورت گسترده ثبت می‌شوند. در حقیقت دفتر کل توزیع شده، دفتر کل ثبت تراکنش‌ها است که نسخه‌ای از آن به صورت مشترک در دست همه کاربران قرار دارد و همه کاربران می‌توانند با استفاده از آن امنیت اطلاعات را تامین کنند. روش توزیع اطلاعات در دفتر کل توزیع شده باعث افزایش امنیت اطلاعات و کاهش خطر هک شدن آنها شده است. دستکاری اطلاعات و یا از بین بردن آنها در این تکنولوژی بسیار سخت است و در دفتر کل توزیع شده با ایجاد یک شبکه غیرمتمرکز از تاییدکنندگان تراکنش، می‌توان به یک سیستم توزیع شده بدون نیاز به حضور نهاد واسطه دسترسی پیدا کرد.

## دو بار خرج کردن (Double spending)

اگر کاربران تلاش کند که به صورت همزمان، یک رمزارز را در 2 بخش مختلف خرج کند، از اصطلاح دوبار خرج کردن یا خرج کردن مضاعف استفاده می‌کنند. دوبار خرج کردن به عنوان خطری شناخته می‌شود که یک ارز دیجیتال می‌تواند دو بار یا بیشتر مورد استفاده قرار بگیرد.

البته اگر شرایط خاصی رعایت شود، اطلاعات تراکنش در یک بلاک چین قابل تغییر است. این شرایط به بلوک‌های اصلاح شده اجازه می‌دهد تا وارد بلاک چین شوند و اگر این اتفاق بیفتد، شخصی که تغییر را آغاز کرده است می‌تواند سکه‌های مصرف شده را دوباره پس بگیرد.

## حمله 51 درصدی (Attack ۵۱%)

در بلاک چین برای دسترسی به اجماع و تایید و ثبت تراکنش‌ها، حداقل باید 51 درصد از کاربران شبکه، تراکنش مورد نظر را تایید کنند. در صورتی که شخص یا گروهی بتوانند قدرت 51 درصد شبکه را به دست آورند، می‌توانند با استفاده از قدرت خود تراکنش‌های مورد نیاز خود را در شبکه ایجاد کرده و اطلاعات قبلی ایجاد شده را دستکاری کنند. در شبکه‌های با الگوریتم اثبات کار، برای این کار باید 51 درصد توان پردازشی شبکه جمع‌آوری شود؛ اما در شبکه‌های اثبات سهام به داشتن 51 درصد توکن‌های بلاک چین نیاز است.

## احراز شناخت مشتری (KYC)

اصطلاح احراز شناخت مشتری (Know Your Customer) برای توصیف قوانینی به کار می‌رود که طبق آن‌ها، فروشنده باید اطلاعات کاملی از هویت خریدار داشته باشد. لازم به ذکر است که این اطلاعات برای تایید و احراز هویت کاربران استفاده می‌شود و در تراکنش‌های با حجم زیاد ضروری است.

## شناخت اصطلاحات رایج ارزهای دیجیتال؛ گامی موثر برای ورود به دنیای کریپتوکارنسی

برای سرمایه‌گذاری و ورود به هر بازاری کسب اطلاعات در آن زمینه و آشنایی با اصطلاحات مرتبط گامی ضروری و موثر است. بازار ارزهای دیجیتال چندین وجه دارد و در صورتی که کاربران دنیای ارزهای دیجیتال دانش و آگاهی کافی در این زمینه داشته باشند، می‌توانند بازار پر سود و روبه‌رشدی را از نزدیک مشاهده کنند. در این مقاله از وبلاگ کیف پول من به معرفی 65 اصطلاح رایج در دنیای رمزارزها پرداختیم. پیشنهاد می‌شود قبل از آغاز فعالیت در دنیای کریپتوکارنسی‌ها حتماً با این اصطلاحات آشنا شوید تا پیش زمینه‌ای مناسب کسب کنید. صرافی کیف پول من به عنوان اولین سامانه نگهداری ارزهای دیجیتال پیشگام کشور همراه شماست تا معاملات خود را به عالی‌ترین شکل ممکن انجام دهید.