آیا بدون **آموزش بلاک چین**و دانستن اینکه **بلاک چین چیست** نمی‌توان در بازار ارزهای دیجیتال خرید و فروش کرد و وارد شد؟

پس چرا دنبال این باشیم که بدانیم بلاک چین چیست؟

– چون اگر بدانیم، می‌توانیم تحلیل بهتری از وقایع، اخبار و رویدادهای دنیای کریپتو کارنسی داشته باشیم. می‌توانیم خودمان تحلیل کنیم، پروژه‌های مختلف را بشناسیم، روند تغییرات و پیشرفتشان را بسنجیم و ببینیم آیا برای سرمایه‌گذاری مناسب‌اند یا نه. درک مفهوم کلی بلاک چین برای شناخت بهتر دنیای غیرمتمرکز و [ارزهای دیجیتال](https://pooleno.ir/blog/what-is-cryptocurrency/) و [درک مفهوم NFT](https://pooleno.ir/blog/what-is-nft/) ضروری است.

بلاکچین سیستم ثبت اطلاعات است.

در ثبت تاریخ هک اطلاعات رخ میداد و سینه به سینه درست منتقل نمیشد توسط تاریخدان ها و توی جنگها کل فرهنگ با آتش زدن کتابخانه از بین میرفت و هنوز هم با سیستم های امروزی هرگونه ثبتی امکان تغییر در آنها هست. مشکل آنها متمرکز بودن است که طعمه خوبی برای سارقان است. یعنی محدود بودن دسترسی به داده و کنترل داده ها توسط ینفر یا یک قدرت مرکزی. پس جرقه ی ایجاد سیستم غیر متمرکز توسط دیوید چامز. بدنبال این بود که پول و سیستم های مالی را غیر متمرکز کرد. در سال 2009 ساتوشی ناکاماتو بلاکپین بیت کوین را راهاندازی کرد و با رمز نگاری ارز دیجیتال بیتکوین را به عنوان یک نوع پول غیر متمرکزمعرفی کرد.

بلاکچین یعنی یک زنجیره که از اتصال بلاک ها ایجاد شده.غیرمتمرکز و شفاف و امکان هک صفر بخاطر نوع ذخیره سازی. اطلاعات داخل بلاک ها قرار میگیرد و پشت سر هم قرار میگیرند و زنجیره بلوکی شکل میگیرد. پلاک هر بلاک با تابع ریاضی بنام تابع هش بدست میاد و اینقدر سخته که نیاز به دستگاهایی بنام ماینر هست برای حل آنها و مصرف برق بالا دارند. برای هش بلاک جدید از هش بلاک قبلی هم استفاده میشه و در اطلاعات خودش ثبت میکند.بنابراین بلاک جعلی اگر جایگزین کنیم کاملا قال تشخیص است. چون هش بلاک قبلی که در اولین بلاک جعلی ثبت شده نادرست است و با هش واقعی بلاکی که قبل از خودش بوده یکی نیست.

مثل جمع 2 تایی اعداد که یکی اشتباه باشه درجا میشه فهمید.

هکر همشو بخواد عوض کنه نمیشه چون هش از اولین تا آخرین بلاک روی تعدادی سیستم کامپیوتری که به آنها نود میگوییند حفط و نگهداری میشوند.برای همین غیرمتمرکز است و هر تغییری را در سیستم حودشان ثبت میکنند. حال اگر یسری از نود ها هک شوند بقیه نودها میفهمند و از ثبت این اطلاعات در شبکه بلاکپین جلوگیری میکنند تا زمانی که بیش از 50 درصد را هک نکرده باشد.

در بلاکچین بیتکوین فقط اطلاعات ثبت میشوند اما در اتریوم میتوان برنامه ها و دستور العمل های مختلف را کدنویسی کرد تا هروقت شرایطش بود بصورت خودکار اجرا شوند.

به زبان “واقعا” ساده، بلاک چین (Blockchain) یک دفتر کل/پایگاه اطلاعات توزیع شده و دیجیتال بوده که در سری‌های زمانی منظم، اطلاعاتی به آن افزوده می‌شود. در واقع بلاک چین یک سیستم ثبت اطلاعات بوده که داده‌ها را به گونه‌ای ذخیره می‌کند تا امکان تغییر و دستکاری آن‌ها وجود نداشته باشد یا به حداقل برسد.

بلاک چین ترکیب دو واژه بلاک (Block) به معنی بلوک یا قطعه و چِین (Chain) به معنی زنجیره است. از نظر لغوی، بلاک چِین معنی **زنجیره** **بلوکی**می‌دهد.

**دفتر کل (Ledger) بلاک چین عملکردی مشابه دفاتر حسابداری دارد. با این تفاوت که متمرکز و قابل تغییر نیست. یعنی همه می‌توانند به اطلاعات بده بستان‌های ثبت شده در آن دفتر حسابداری دسترسی داشته باشند.**

هر چیزی را می‌توان به هش (Hash) تبدیل کرد و رمز نگاری کرد. با الگوریتم هشینگ می‌توان داده‌های زیاد را به چند حرف و عدد تقلیل داد و به این روش، اطلاعات یک بلاک را به یک عبارت چند بیتی تبدیل کرد.

* تسهیل و تسریع پرداخت‌ها و امور مالی
* ثبت اطلاعات و تاریخچه اموری مانند فعالیت‌های پزشکی
* تأیید هویت دیجیتال
* کاربرد در زنجیره تأمین
* امکان اجرای اپلیکیشن‌های غیرمتمرکز (DApps)
* پشتیبانی از بازی‌های بلاک چینی

سابقه بلاک چین به عنوان یک روش ثبت اطلاعات به قبل از ظهور بیت کوین برمی‌گردد. پیش از معرفی مفاهیمی چون[**قرارداد هوشمند**](https://pooleno.ir/blog/what-is-smart-contract/)، ایده اولیه بلاک چین را یک رمز نگار (Cryptographer) آمریکایی به نام **دیوید چام (David Chaum)** در سال ۱۹۸۲ در پایان نامه خود مطرح کرد. او برنامه‌ای برای عرضه پول نقد الکترونیکی توسعه داده بود و در سال ۱۹۹۵ شرکت دیجی کش را بر همین مبنا بنا کرد و اولین ارز دیجیتال یعنی ای کش (ecash) را ایجاد کرد. اما این پول دیجیتال، غیرمتمرکز نبود.

تراکنش‌های بیت کوین روی بلاک‌ها ثبت می‌شد. به این صورت که فرد الف به فرد ب به مقدار X بیت کوین ارسال کرد. به همین ترتیب یک بلاک ایجاد شد. در ابتدا روی هر بلاک ۳۶ مگابایت اطلاعات جای می‌گرفت، تایید می‌شد، هش آن در بلاک بعدی قرار می‌گرفت و بلاک جدید شروع می‌شد. حجم بلاک‌های بیت کوین تا الان تغییراتی داشته و هم‌اکنون ۱ مگا بایت است.

ه طور کلی، می‌توان از کلیدهای رمزنگاری (Cryptographic Keys)، شبکه‌های همتا به همتا (Peer-to-Peer Networks) و دفتر کل دیجیتال (Digital Ledegr) به عنوان ۳ جزء اصلی بلاک چین یاد کرد.

**ماینرها**کسانی هستند که ثبت می‌کنند فرد الف به فرد ب چقدر بیت کوین یا هر ازر دیجیتال دیگر داده و تایید می‌کنند که این تراکنش صحیح است. تعداد زیاد ماینرها باعث افزایش امنیت یک شبکه می‌شود چون امکان تقلب در ثبت تراکنش‌ها کاهش می‌یابد. بله! تقلب و هک، چیزی است که در بلاک چین ممکن است اتفاق بیفتد و ماینرها می‌توانند جلوی آن را بگیرند. به دلیل نقش مهم ماینرها در امنیت شبکه‌های بلاک چین، به آن‌ها پاداش داده می‌شود.

**انواع نود (Node) در شبکه بلاک چین**

**ماینینگ نود (Mining Node):** ماینینگ نودها همان تولید کنندگان بلاک در شبکه هستند و اطلاعات جدید را در شبکه پخش می‌کنند.

**فول نود (Full Node):** فول نودها یا نودهای کامل تمام اطلاعات شبکه و تاریخچه آن را را از ابتدای پیدایش شبکه ذخیره می‌کنند و می‌توانند برای شبکه تصمیم بگیرند. آن‌ها بین نودهای مختلف هماهنگی ایجاد می‌کنند و وظیفه تایید تراکنش‌ها را بر عهده دارند.

**لایت نود (Light Node):** نودهای سبک تنها بخشی از اطلاعات شبکه را در خود دارند. کیف پول‌های ارز دیجیتال نمونه‌ای از لایت نود هستند.

برای تولید بلاک‌های بیت کوین، ماینرها باید معادلات پیچیده ریاضی را حل کنند.

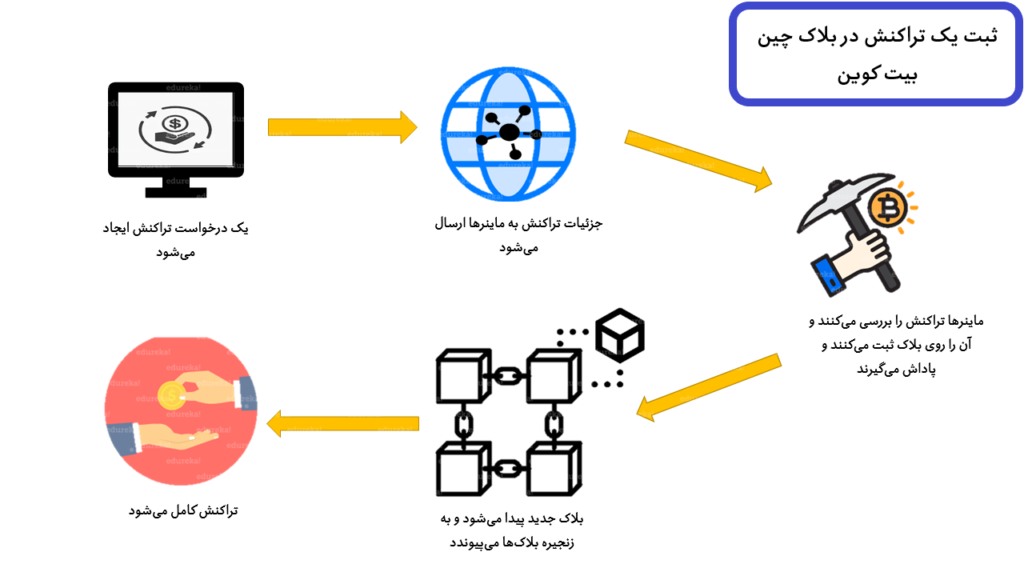
این معادلات برای این طراحی شده‌اند که هزینه ایجاد بلاک را بالا ببرند و هرکسی نتواند بلاک تقلبی یا دستکاری شده با اطلاعات ساختگی ایجاد کند. در عوض، شبکه بابت حل این معادلات پیچیده و تولید بلاک صحیح، به ماینرها بیت کوین پاداش می‌دهد.

**ممکن است هکرها سعی کنند به شبکه نفوذ کنند و تراکنشی غیرواقعی وارد بلاک کنند. برای این کار باید توان پردازشی بیش از ۵۰ درصد ماینرها داشته باشد تا بتواند بلاک‌ها را تغییر دهد. اینجاست که اگر تعداد ماینرها و نودهای شبکه کم باشد، ممکن است حمله ۵۱ درصد رخ دهد.**

این اتفاق، برای شبکه‌هایی می‌افتد که از روش اثبات کار برای ماینینگ استفاده می‌کنند. به همین دلیل بسیاری از شبکه‌ها به روش اثبات سهام روی آورده‌اند که هم کم‌هزینه است، هم دوستدار محیط زیست.

البته در روش اثبات سهام هم احتمال [حمله ۵۱ درصد](https://pooleno.ir/blog/what-is-51-attack/) وجود دارد امّا با ظاهر دیگری! در بلاک چین‌های PoS، این حمله با نام Long Range Attack شناخته می‌شود و زمانی رخ خواهد داد که یک نفر بیش از ۵۰ درصد توکن‌های آن شبکه را در اختیار داشته باشد.

در روش اثبات سهام دیگر معادله‌ای برای حل کردن نیست و ماینرها در واقع، درستی تراکنش‌ها را بررسی می‌کنند و از کارمزد تراکنش‌ها پاداش می‌گیرند.





**مقیاس‌پذیری (Scalibility)**در یک شبکه بلاک چینی، به توانایی آن شبکه در پردازش حجم بالای تراکنش‌ها همزمان با افزایش نودهای شبکه اطلاق می‌شود. در واقع با افزایش تعداد تراکنش‌های یک زنجیره در ثانیه (TPS)، مقیاس پذیری شبکه هم افزایش می‌یابد.

## سیستم ذخیره فایل توزیع شده در بلاک چین

بدون شک سرویس‌هایی مانند Dropbox و Google Drive، از نقاط عطف دنیای تکنولوژی به حساب می‌آیند. چرا که با فراهم کردن یک فضای ابری (Cloud Storage)، به ما این اجازه را دادند تا فایل‌های خود را در فضای مشخصی نگه‌داری کنیم و تا حدی از فلش و هارد اکسترنال بی نیاز شویم!

## کیف پول در بلاک چین چیست؟

[**کیف پول بلاک چین**](https://pooleno.ir/blog/what-is-wallet/) به کاربران اجازه می دهد تا به ارسال، دریافت و ذخیره دارایی‌های خود در بلاک چین اقدام کنند. همچنین امکان مدیریت و نظارت بر دارایی‌ها را برای ما به ارمغان می‌آورد.

هر کیف پول کلید عمومی و کلید خصوصی مختص به خود را داراست و تمامی آمار یک شبکه اعم از آدرس‌های فعال، تراکنش‌ها، نهنگ‌های شبکه، مسیر یک تراکنش و… بر اساس آدرس‌های کیف پول‌ ارز دیجیتال جمع‌آوری می‌شوند.

## بلاک چین اتریوم و تفاوت آن با بلاک چین بیت کوین

حالا که معنی و مفهوم بلاک چین را درک کردیم می‌توانیم پای بلاک چین اتریوم را وسط بکشیم و ببینیم چه اتفاقی برای نسل دوم بلاک چین افتاد.

در بلاک‌های بیت کوین فقط دریافت و پرداخت‌های بیت کوین ثبت می‌شد. به این صورت:

شقایق به مهران ۱ بیت کوین ارسال کرد.

مهران به حامد ۰.۵ بیت کوین داد.

اتریوم این روش را تغییر داد.[**ویتالیک بوترین**](https://pooleno.ir/blog/who-is-vitalik-buterin/)، خالق شبکه اتریوم، چیزی به این معادله اضافه کرد. چیزی که یک تراکنش ساده را به «قرارداد هوشمند» تبدیل کرد و پایه گذار برنامه‌های غیرمتمرکز یا DApp شد.

او گفت می‌توان شروطی را برای انجام یک تراکنش در نظر گرفت. مثلا یک تراکنش انجام نشود مگر اینکه شرطی قبل از آن اجرا شده باشد. به این صورت:

شقایق به مهران ۱ بیت کوین می‌دهد اگر مهران فایل موزیک y را برای او بفرستد.

تفاوت قرارداد هوشمند با یک خرید و فروش یا قرارداد معمولی در این است که اجرا شدن قرارداد هوشمند ردخور ندارد. ممکن است در یک قرارداد عادی، یکی از طرفین به قرارداد وفادار نباشد و موجب زیان دیگری شود ولی در قرارداد هوشمند حتما مفاد قرارداد اجرا خواهند شد چون کسی قدرت کنترل بلاک چین را ندارد و حتی کد نوشته شده از سوی خود نویسنده کد نیز قابل تغییر نیست!

در هر صورت، بد نیست اگر نگاهی بیندازیک بر مزایا و معایب بلاک چین:

| **مزایا ی تکنولوژی بلاک چین** | **معایب تکنولوژی بلاک چین** |
| --- | --- |
| سهولت و نبود موانعی چون محدودیت‌های جغرافیایی | عدم پذیرش توسط برخی پلتفرم‌ها |
| تمرکززدایی | امکان تاثیرپذیری از قوانین و سیاست‌گذاری‌ها |
| حذف واسطه‌ها | مصرف انرژی (در بلاک چین‌های PoW) |
| سرعت بالای فعالیت‌ها (اغلب مواقع) |  |
| شفافیت |  |

همچنین ویژگی مهم تغییرناپذیری (Immutability) داده‌ها، از جمله مواردی است که می‌تواند مانند یک شمشیر دو لبه عمل کند و هر دو ستون جدول را پر کند! چرا که از طرفی از تغییر اطلاعات توسط هکرها جلوگیری می‌کند امّا در صورت بروز اشتباه در وارد کردن اطلاعات یک بلاک، دیگر امکان اصلاح آن نیست یا دست کم بسیار دشوار خواهد بود.

## فورک بلاک چین به چه معنی است؟

بلاک چین‌ها هم مشکلات خاص خودشان را دارند! وقتی ماینرهای یک شبکه در مورد روند شبکه و عملکرد پیاده‌سازی بلاک‌ها توافق نداشته باشند یا بخواهند متد دیگری را در پیش بگیرند یک شکاف رخ می‌دهد و فورک یا شاخه‌ای از زنجیره اصلی جدا می‌شود. یعنی برخی از اعضا و نودها، از شبکه اصلی انشعاب می‌گیرند و راه خود را می‌روند. به این اتفاق، فورک می‌گویند. فورک به معنی چنگال، شاخه یا انشعاب است. وقتی یک قانون جدید به صورت یک کد به شبکه اضافه شود، این فورک اتفاق می‌افتد. برخی نودها در ادامه قانون قبلی پیش می‌روند و برخی نودها از قانون جدید پیروی می‌کنند.

### فورک چگونه انجام می‌شود؟

فورک شدن به این شکل است که در امتداد زنجیره اصلی بلاک‌ها، یک بلاک منشعب می‌شود و ماینرها و اعضای شبکه تصمیم می‌گیرند که سر این دوراهی، به کدام سمت بروند و بلاک‌های جدید را در امتداد کدام شاخه ادامه دهند. به طور مثال دوج کوین فورکی از لایت کوین است که خود لایت کوین از بیت کوین منشعب شده (فورک شده) است.

**هارد فورک:**هارد فورک به شاخه‌ای می‌گویند که از زنجیره اصلی منشعب می‌شود و ماینرها دیگر تراکنش‌های شاخه اصلی را معتبر نمی‌دانند. مانند اتفاقی که برای اتریوم افتاد و شاخه قبلی با نام اتریوم کلاسیک به راه خود ادامه داد و اتریوم فعلی با قوانین جدید از آن منشعب شد.

**سافت فورک:**سافت فورک برای بلاک چین مانند یک آپگرید است. در سافت فورک، بلاک چین ارتقا می‌یابد و قابلیت‌های جدید به آن افزوده می‌شود و بلاک‌های قدیمی همچنان معتبر هستند. مانند سافت فورک‌هایی که بیت کوین تا کنون داشته و [آپگرید تپروت (Taproot)](https://pooleno.ir/blog/taproot-upgrade/) که به‌زودی قرار است انجام شود، یکی از آن‌هاست.

گاهی ممکن است فناوری بلاک چین با شرکت خدمات مالی ارزهای رمزنگاری شده یعنی **سایت بلاک چین (**[**Blockchain**.**com**](https://blockchain.com/)**)** اشتباه گرفته شود. این شرکت به عنوان اولین اکسپلورر بلاک چین بیت کوین در سال ۲۰۱۱ شروع به کار کرد و بعدا یک کیف پول ارز دیجیتال ایجاد کرد که ۲۸ درصد از تراکنش‌های بیت کوین را بین سال‌های ۲۰۱۲ تا ۲۰۲۰ تشکیل می‌داد. این شرکت یک صرافی ارز دیجیتال را هم اداره می‌کند.

با توجه به کاهش اطمینان افراد به سازمان‌های متمرکز، انتظار می‌رود که در آینده نه چندان دور (بلکه همین الان!)، شاهد استقبال گسترده‌تری از بلاک چین باشیم.

طبق پیش بینی شرکت تحقیقاتی Gartner، تا سال ۲۰۲۶ مجموع ارزش افزوده توسط کسب و کارهای بلاک چینی، به ۳۶۰ میلیارد دلار افزایش خواهد یافت.

همچنین به پیشبینی همین سازمان، تا سال ۲۰۳۰، این رقم به بیش از ۳.۱ تریلیون دلار خواهد رسید. یعنی حدود ۳۰۰میلیارد دلار بیشتر از ارزش بازار کمپانی اپل که باارزش‌ترین شرکت جهان محسوب می‌شود!

هک ۶۰۰ میلیون دلاری Ronin Bridge، به سرقت رفتن ۱۰۰ میلیون دلار از شبکه هارمونی و یا هک بیش از ۸ میلیون کیف پول از بلاک چین سولانا! این موارد تنها بخشی از حملاتی بودند که امنیت شبکه‌های بلاک چینی را به خطر انداخته‌اند.

شاید با خودتان تصور کنید که این اتفاقات به ندرت گریبان کاربران را می‌گیرند و یا به سال‌های آغازین ظهور **شبکه‌های بلاک چینی** محدود می‌شود. امّا بد نیست یادآور شویم که تمامی حملات مذکور در سال ۲۰۲۲ اتفاق افتاده‌اند!

فرایند تبدیل شدن به ماینر دشوار و پر هزینه خواهد بود. چرا که به تجهیزات پیشرفته‌ای برای حل مسائل بلاک چین‌ها نیاز خواهیم داشت. با این حال، اگر فرد یا گروهی موفق به تامین این تجهیزات شود و آن را گسترش دهد، می‌تواند بخش زیادی از اختیارات شبکه را به دست بگیرد.

اگر این اختیارات از ۵۰ درصد فراتر رود، آن گروه توانایی نفوذ به شبکه و برهم زدن فعالیت‌های شبکه را خواهد داشت. به این نوع از حملات اصطلاحا **حمله ۵۱ درصد** گفته می‌شود.

طی حمله رقابتی، هکر تراکنشی **تایید نشده** را به قربانی می‌فرستد و در همان حین، تراکنش دیگری را به طور موازی و همزمان در شبکه منتشر می‌کند. در این حالت، دریافت کننده تصور می‌کند که با پذیرش تراکنش، دارایی خود را دریافت خواهد کرد. امّا ای کاش اوضاع بدین شکل پیش می‌رفت!

به غیر از شخص گیرنده، دیگر تاییدکنندگان شبکه تراکنشی را می‌پذیرند که همزمان با تراکنش ابتدایی منتشر شده و در چنین موقعیتی، به احتمال زیاد پذیرنده دارایی خود را دریافت نخواهد کرد.

### حمله فیشینگ (Phishing)

 حملات فیشینگ، هکرها تلاش می‌کنند تا با ارسال پیام‌هایی، به اطلاعات کاربران از جمله عبارت **۱۲ کلمه‌ای (Seed Phrase)** دسترسی پیدا کنند. این نوع از پیام‌ها اغلب در قالب ایمیل یا دیگر شبکه‌های اجتماعی فرستاده می‌شوند.

### حمله وام فوری (Flash Loan)

احتمالا تا کنون نام **Flash Loan** یا **وام فوری** را شنیده‌اید. این وام‌ها بدون **وثیقه (Collateral)** به متقاضیان اعطا می‌شوند و افراد موظف هستند تا در زمانی کوتاه آن مبلغ را برگردانند. در غیر این صورت، مالکیت دارایی از دسترس آن‌ها خارج خواهد شد.

حمله Flash Loan زمانی رخ می‌دهد که شخص متقاضی مقدار زیادی از دارایی را در قالب وام دریافت می‌کند و پس از دستکاری قیمت‌ها در پلتفرم مالی دیگر (مثلا یک صرافی غیرمتمرکز)، وام دریافت شده را در آن صرافی به فروش برساند. این حملات معمولا در چند ثانیه صورت می‌گیرند.

## چگونه با حملات بلاک چینی مقابله کنیم؟

هنگام تامین امنیت کیف پول‌ها، نگهداری از **Seed Phrase** و **رمز عبور**، اقداماتی هستند که در بالای لیست ما قرار می‌گیرند. امّا برای در امان ماندن از حملات بلاک چین، فعالیت‌های دیگری هم هستند که باید به آن‌ها توجه داشت.

### جلوگیری از حملات Double Spending

به منظور جلوگیری از **حملات Double Spending** از جمله **حمله ۵۱ درصد**، بلاک چین‌ها از مکانیزم‌های اجماع اثبات کار (PoW) و اثبات سهام (PoS) استفاده می‌کنند.

به نوعی می‌توان گفت که به هنگام حملات Double Spending، کاربران بلاک چین از اختیارات قابل توجهی برخوردار نیستند و ایمن سازی شبکه بر عهده ماینرها و تیم فنی خواهد بود.

با استفاده از این نوع مکانیزم‌ها، **تمرکز زدایی**در شبکه افزایش می‌یابد و برای تایید هر بلاک، به رقابت بیشتری نیاز خواهد بود. از طرفی، بهتر است معاملات خود را در صرافی‌های مورد اطمینان انجام دهید تا پس از تایید هر تراکنش در کیف پول، با مشکل مواجه نشوید.

همچنین بلاک چین‌هایی مانند بیت کوین، محدودیتی را برای ماینرهای اعمال می‌کنند. به عنوان مثال، ماینری نمی‌تواند بیش از ۵۰ درصد از قدرت محاسباتی شبکه را در اختیار داشته باشد.

### مقابله با حملات Phishing

حفظ امنیت دارایی‌ها در برابر حملات فیشینگ، تا حد زیادی بر عهده کاربران خواهد بود. **بررسی دقیق ایمیل‌ها**، **عدم کلیک برروی لینک‌های ناشناس** و **نصب نسخه‌های معتبر اپلیکیشن‌ها** می‌توانند تا حد زیادی ما را از این نوع حملات مصون نگه دارند.

علاوه بر موارد گفته شده، **فعالسازی تایید ۲ مرحله‌ای**، **استفاده از رمز عبور مطمئن** و **به روز نگه داشتن اپلیکیشن‌ها**، به ما در مقابله با فیشینگ کمک خواهند کرد.

### جلوگیری از حملات وام فوری (Flash Loan)

در مقایسه با موارد قبلی، شاید بتوان گفت که برای جلوگیری از حملات مربوط به Flash Loan پروسه به نسبت آسان تری را در پیش خواهیم داشت.

* استفاده از پلتفرم‌های معتبر DeFi مانند آوه
* به کارگیری کیف پول‌های **غیر حضانتی (Non-Custodial)** مثل تراست والت و متامسک
* به روز نگه داشتن اطلاعات و آگاهی از اخبار

# استیکینگ ارز دیجیتال چیست؟

استیک یا استیکینگ (Staking) ارزهای دیجیتال یکی از مفاهیم مهم در حوزه رمز ارزها است. اهمیت شناخت این مفهوم زمانی بیشتر می‌شود که بدانیم با انجام آن می‌توانیم به درآمد خوبی برسیم؛ چون **کسب درآمد با استیک ارزهای دیجیتال** بسیار ساده است و نیاز زیادی به صرف زمان ندارد.

اگر معنی استیک در ارز دیجیتال برای شما ناآشنا است یا با شنیدن این کلمه به یاد یک نوع غذا می‌افتید، باید بدانید که واژه استیک (Stake) در ارزهای دیجیتال به معنی **قفل کردن رمز ارزها** در شبکه و دریافت سود از این کار است. دقیقا مثل زمانی که پولی را برای مدتی مشخص، در یک بانک سپرده‌گذاری می‌کنید.

## استیکینگ چیست؟

**استیکینگ (Staking)** ارز دیجیتال فرایندی است که طی آن، دارندگان ارزهای دیجیتال به صورت داوطلبانه، بخشی از دارایی‌ کریپتویی خود را در یک شبکه قفل می‌کنند تا در پروسه **تایید**و **اعتبارسنجی** **(Validation)** تراکنش‌ها مشارکت داشته باشند. در قبال کمک به تایید بلاک‌های زنجیره، استیک‌کنندگان یا ولیدیتورها پاداشی را دریافت خواهند کرد.

با سپرده‌گذاری، می‌توانید دارایی‌های دیجیتال خود را به کار انداخته و بدون فروش آن‌ها **درآمد غیرفعال (Passive Income)** کسب کنید.

## استیکینگ چگونه کار می‌کند؟

از برخی جهات، استیکینگ شبیه به واریز وجه نقد در یک حساب پس انداز با بازده بالا است. بانک‌ها سپرده‌های شما را قرض می‌دهند و یا صرف فعالیت‌های سودآور و مولّد می‌کنند و شما سود موجودی حساب خود را دریافت می‌کنید.

این فرایند تنها برای رمز ارزهایی با [الگوریتم اجماع اثبات سهام (POS)](https://pooleno.ir/blog/what-is-proof-of-stake/) انجام می‌شود‌. بنابراین ارزهایی مثل بیت کوین یا دوج کوین که از [الگوریتم اجماع اثبات کار (POW)](https://pooleno.ir/blog/what-is-proof-of-work/) استفاده می‌کنند، قابلیت استیکینگ را ندارند.

شرکت در تصمیم‌گیری‌های یک بلاک چین به‌همین سادگی‌ها هم نیست، دست همه ما برای تبدیل شدن به یک نود باز است؛ اما هر نود (اعضای کامپیوتری شبکه که کارشان ثبت داده‌ها در بلاک‌های جدید است) باید طبق روش‌ و الگوریتمی مشخص، معتمد‌بودن خود را به شبکه ثابت کند. درحال حاضر دو نوع کلی برای این الگوریتم‌ها وجود دارند، که باعث اعتماد شبکه و اعضای دیگر به هر نود می‌شوند.

روش اول، **الگوریتم اجماع اثبات کار (Proof of Work)** نام دارد. در این روش هر عضو باید از قطعات سخت‌افزاری بسیار گران و پیشرفته‌ای که مصرف برق بالایی هم دارد، استفاده کند، بلکه بتواند از پس حل مسائل سخت ریاضی بربیاید. نودها با حل این مسائل می‌توانند بلاک‌های اطلاعاتی جدیدی در شبکه ثبت کرده و با این کار ارز دیجیتال کسب کنند.

روش **اجماع اثبات سهام (Proof Of Stake)** نوع دیگری از الگوریتم‌های اجماع است. در این روش داوطلبانی که می‌خواهند تبدیل به یک **ولیدیتور (Validator – اعتبارسنج)** شوند، مجبور به صرف هزینه‌های کلان برای تامین سخت‌افزارهای گران‌ نیستند. یکی از مهم ترین ارکان فرایند استیکینگ، چیزی نیست جز [قرارداد هوشمند](https://pooleno.ir/blog/what-is-smart-contract/) یا Smart Contract.

در اثبات سهام داوطلبان نیازی به حل مسائل پیچیده ندارند. بیشترین هزینه‌ای که یک ولیدیتور (اعتبارسنج شبکه) باید در یک شبکه POS بپردازد همان هزینه ارزهای دیجیتال استیک شده اوست. نودها با سرمایه‌گذاری و قفل‌کردن ارزهای دیجیتال، اعتبار و درستکاری خود را به سیستم و دیگر اعضا اثبات می‌کنند. در سیستم اثبات سهام هم ولیدیتورها با ثبت هر بلاک در شبکه، مقداری ارز دیجیتال بومی شبکه را پاداش می‌گیرند.

ه جز سود حتما باید به اعتبار و [تحلیل فاندامنتال](https://pooleno.ir/blog/what-is-fundamental-analysis/) ارز دیجیتال مورد نظر، موقعیت تکنیکال آن در بلند مدت و همچنین به امنیت و امکانات پلتفرمی که به وسیله آن این ارز را استیک می‌کنیم، دقت داشته باشیم.

## آیا می‌شود استیبل کوین‌های مبتنی بر دلار را هم استیک کرد؟

البته که می‌شود. خبر خوبی است؛ چون استیبل کوین‌ها (Stablecoins) ارزهای دیجیتالی هستند که ارزش ثابتی دارند. استیبل‌کوین‌هایی مثل تتر، دای و USDN برای این ساخته شدند که همیشه ارزشی تقریبا معادل یک دلار داشته باشند.

گاهی قیمت آنها دچار نوساناتی می‌شود و اختلاف کمی نسبت به قیمت دلار پیدا می‌کند،  اما معمولا تغییر قیمت در این نوسانات، ناچیز است. داشتن ارزش ثابت، یعنی خیالمان راحت‌تر است و احتمال کاهش ارزش دلاری دارایی استیک‌شده، کم می‌شود. بنابراین استیبل کوین‌هایی مانند BUSD، به دارایی محبوبی برای استیک‌کنندگان تبدیل گشته است.

## انواع روش‌های استیکینگ

* **استیک برای تبدیل شدن به ولیدیتور**: در این روش، نیاز داریم تا دارایی خود را مستقیماً به پلتفرم مقصد اختصاص دهیم و یک کامپیوتر که به صورت شبانه‌روز به اینترنت متصل باشد را در اختیار داشته باشیم. ولیدیتورها وظیفه تأیید بلاک‌ها را عهد‌دار هستند و این کار مستلزم دانش فنی بالایی از تکنولوژی بلاک چین خواهد بود. اغلب به سرمایه بالایی نیاز دارد (همانند استیک ETH).
* **استیک نمایندگی شده (Delegated Staking)**: ساز و کاری مشابه روش قبلی را داراست با این تفاوت که نیازی به اجرای مستقیم Node نبوده و دارایی خود را در اختیار یک شخص ثالث می‌گذاریم تا این کار را برای ما انجام دهد. در مقایسه با روش قبل، از پاداش کمتری برخوردار خواهیم بود.
* **استخرهای نقدینگی**: در این روش، نیازی به صرف زمان و منابع مورد نیاز برای تبدیل شدن به یک ولیدیتور نبوده و کافیست دارایی‌های خود را به استخرهای نقدینگی مخصوص اختصاص دهیم تا با تامین نقدینگی استخر و به کار انداختن آن ارز، سودی را دریافت کنیم.
* **استیک بدون محدودیت** **(Soft Staking)**: در پلتفرم‌هایی چون [**Lido**](https://pooleno.ir/blog/what-is-lido-dao/)، ما دارایی خودمان را در شبکه استیک می‌کنیم امّا همچنان می‌توانیم به آن دسترسی داشته باشیم و در پلتفرم‌های دیگر، با آن فعالیت کنیم. به عبارتی، زمانی که توکن اوّلیه خودمان را استیک می‌کنیم، یک توکن هم‌ارز با پیشوند st از شبکه دریافت می‌کنیم که نسبتی برابر با دارایی اوّلیه دارد. در آخر پس از برداشت دارایی، این توکن هم سوزانده می‌شود.
* **استیک در صرافی‌های متمرکز**: این روش هم مورد استقبال طیف کثیری از کاربران قرار گرفته است و بسیاری دارایی‌های خود را در صرافی‌هایی چون بایننس و کوین بیس استیک می‌کنند. البته که به دلیل رویکرد متمرکز این پلتفرم‌ها، این فرایند با واسطه بوده و صرافی‌ها می‌توانند بر توکن‌های ما کنترل داشته باشند.

البته که این میزان ارز همیشه هم چندان ناچیز نبوده و گاهی اوقات به مقادیر بالایی از دارایی‌ها نیاز داریم. به عنوان مثال برای تبدیل شدن به ولیدیتور در اتریوم PoS، نیاز داریم تا مضرب صحیحی از **۳۲ اتر(ETH)** را در شبکه قفل کنیم.

**سود استیک ارزهای دیجیتال** مختلف به چند عامل بستگی دارد. این عوامل شامل مواردی مثل نوع ارز دیجیتال، تعداد ارزهای استیک‌شده استیک کننده، تعداد کل ارزهای استیک شده در آن بلاک چین و مدت زمانی است که می‌خواهیم این رمزارزها را استیک‌ کنیم. به‌اضافه این‌ها هنگام استیک یک ارز دیجیتال، ممکن است در سایت‌ها و قراردادهای هوشمند مختلف، با درصد سود متفاوتی روبرو شویم.

در‌کل هرچه زمان استیک طولانی‌تر باشد یا تعداد ارزهای بیشتری را استیک کرده باشید، مقدار سود دریافتی شما هم بالاتر می‌رود. درست مثل بازکردن حساب سپرده مدت‌دار در بانک است؛ سودی که برای سپرده شش‌ماهه بانکی دریافت می‌کنید بیشتر از سود سپرده سه‌ماهه است.

درصد **سود سالانه استیکینگ** اغلب با APR یعنی نرخ درصدی سالیانه (Annual Percentage Rate) بیان می‌شود. APR معادل سود ساده سالانه است. هر شخصی که برای ۳۶۵ روز رمزارزهای خود را استیک کند، از این سود سالانه بهره‌مند خواهد شد.

عبارت دیگری که احتمال دارد گاهی با آن مواجه شوید APY است. **APY سود مرکب سالانه** را نشان می‌دهد. سود مرکب یعنی شما نه تنها از اصل سرمایه استیک‌شده، بلکه از سود آن هم پاداش دریافت می‌کنید.

ارزهای دیجیتال معروف‌تر که سرمایه‌های بیشتر و با ارزش‌تری در شبکه آنها استیک‌شده (TVL یا ارزش کل قفل‌شده بیشتری دارند)، شامل نرخ سود سالانه متعادل‌تری هستند. اما ارزهای تازه وارد و کم‌تر شناخته‌شده‌ معمولا برای جذب سرمایه، APR بیشتری به استیک کنندگان خود می‌پردازند. سود استیکینگ سالانه برخی از این ارزها بالای ۱۰۰% است.

در **ماشین حساب استیکینگ تراست والت** که در سایت این کیف پول قرار دارد، می‌توانید به‌راحتی، سود استیک سالانه ارزهایی مانند ترون، بایننس کوین، تزوس و کاوا را حساب کنید؛ برای این کار کافی است تا تعداد و نوع ارز دیجیتال را مشخص کنید.

<https://www.stakingrewards.com/>

* استیکینگ روش خوبی برای **مقابله با تورم** است. با اضافه‌شدن هر بلوک جدید به یک  شبکه اثبات سهام، تعدادی ارز دیجیتال جدید تولید می‌شوند. این ارزهای جدید باعث بالا‌رفتن تعداد کل کوین‌های بومیِ شبکه می‌شوند، در نتیجه با گذشت زمان، شاهد ایجاد تورم و کاهش ارزش هر واحد از آن ارز خواهیم بود.

رمزارزهایی که ثابت و بی‌استفاده نگهداری می‌شوند نیز با بالا رفتن **تعداد کل عرضه (Total Supply)**، ارزش کمتری نسبت به**ارزش بازار (Market Cap)**خود پیدا می‌کنند. اما با روش استیک ارزهای دیجیتال، با قفل‌کردن دارایی سود دریافت می‌کنیم؛ پس به دلیل این پاداشی که می‌گیریم، تا حدی می‌توانیم با تورمی که در شبکه رمزارز پدید می‌آید، مقابله کنیم.

### ریسک‌ها و خطرات استیکینگ ارزهای دیجیتال

* شاید بزرگ‌ترین ریسک استیکینگ، قفل شدن ارزهای دیجیتال تا **پایان بازه استیک** باشد. چون تا زمان به پایان رسیدن استیکینگ، نمی‌توانیم به ارزهای استیک شده دست بزنیم. اگر قیمت ارز دیجیتال تا آخر این دوره کم و کم‌تر شد، ما نمی‌توانیم با فروش این ارزها جلوی کاهش سرمایه را بگیریم. اگر قیمت این ارزها رشد خوبی هم کرد باز توانایی فروش و کسب سود را نداریم.
* اگر یک اعتبارسنج‌ وظایف خود را کامل و درست انجام ندهد، جریمه می‌شود. به‌عنوان مجازات ممکن است همه یا بخشی از ارزهایی که در شبکه استیک کرده‌ را از دست بدهد.

**جریمه اعتبارسنج‌ها** ممکن است، دامن‌گیر استیکرهایی که دارایی خود را به آنها سپرده‌اند هم بشود. در نتیجه باید زمان انتخاب نماینده یا ولیدیتور، گزینه‌های خوش‌سابقه و معتبر را انتخاب کنید.

* این خطر مربوط به استیک کنندکان استیبل کوین‌ها می‌شود. این احتمال وجود دارد که در طی زمان، استیبل کوین‌هایی مانند تتر که قیمتشان حدود یک دلار است، همبستگی ارزش خود را با دلار از دست بدهند.
* زمانی که در یک پلتفرم آنلاین عمل استیکینگ را انجام می‌دهیم، باید ریسک هک‌شدن آن را هم درنظر بگیریم. احتمال هک‌شدن، حتی برای صرافی بزرگی مثل بایننس، هرچند که بسیار کم است اما صفر نیست.

### تراست ولت

کار با کیف پول موبایلی [تراست والت](https://pooleno.ir/blog/install-trust-wallet/) بسیار راحت است؛ به‌همین‌علت یکی از رایج‌ترین کیف پول‌ها بین فعالان بازار کریپتو کارنسی به‌شمار می‌رود.

### بایننس

صرافی بایننس، بزرگترین صرافی حال حاضر مارکت، از استیکینگ ارزهای دیجیتال زیادی پشتیبانی می‌کند. استیکینگ در صرافی بایننس به دو صورت **استیکینگ در کیف پول صرافی** و استیک در پروژه‌های مالی دیگر دیفای، به‌واسطه صرافی انجام می‌شود،

### استیکینگ در صرافی کوینکس

صرافی کوینکس در ایران کاربران زیادی دارد. این اکسچنج امکان استیک چندین ارز مختلف را برای اعضای خود فراهم کرده است. سود سپرده‌گذاری و استیکینگ ارز دیجیتال در کوینکس به‌صورت APY (سود مرکب) محاسبه می‌شود.

## تفاوت هولد و استیک در چیست؟

هودل (HODL) یا همان هولد، از محبوب ترین و کم‌ریسک ترین استراتژی‌های موجود در بازار کریپتو و سهام به حساب می‌آید. چرا که ما تنها بخشی از دارایی خودمان را صرف خرید سهام یا رمزارز کرده و آن را نزد خودمان نگهداری می‌کنیم.

به عبارتی، با دید بلندمدت قدم به بازار می‌گذاریم و دیگر نیازی نیست تا نمودارهای قیمتی را به صورت شبانه‌روزی رصد کنیم! همین موضوع، ریسک ما را کاهش می‌دهد. با این حال، در تمامی بازارها یک قانون نانوشته وجود دارد:  
ریسک بیشتر= پاداش بیشتر!

**استیکینگ چیست؟**

**استیکینگ (Staking)** ارز دیجیتال فرایندی است که طی آن، هولدرها به صورت داوطلبانه، بخشی از دارایی‌ کریپتویی خود را در یک شبکه قفل می‌کنند تا در **اعتبارسنجی** **(Validation)** تراکنش‌ها مشارکت کنند. در قبال کمک به تایید بلاک‌های زنجیره و یا تامین نقدینگی، استیک‌کنندگان پاداشی را دریافت می‌کنند.

**انواع استیکینگ چیست؟**

استیک برای تبدیل شدن به ولیدیتور،استیک نمایندگی شده (Delegated Staking)، استیک در استخرهای نقدینگی، استیک بدون محدودیت (Soft Staking) و استیک در صرافی‌های متمرکز، از جمله روش‌های استیکینگ به شمار می‌آیند.

<https://pooleno.ir/blog/blockchain-use-cases-in-real-world/>

<https://pooleno.ir/blog/what-is-blockchain-trilemma/>

<https://pooleno.ir/blog/what-is-etc/>

<https://pooleno.ir/blog/what-is-aave-protocol/>

<https://pooleno.ir/blog/what-is-tether-usdt/>

<https://pooleno.ir/blog/who-is-satoshi-nakamoto/>

<https://pooleno.ir/blog/what-is-lido-dao/>

tron