



## کیف پول دیجیتال

### کیف پول دیجیتال چیست؟

در صورت تمایل به آموزش کیف پول دیجیتال، آموزش ایجاد حساب یا کیف پول، انتقال ارز و غیره بر روی دکمه آبی بزنید.

#### [آموزش کیف پول دیجیتال](#)

کیف پول دیجیتال چیست؟ بگذارید پیش از آنکه شروع کنیم و مستقیماً درباره‌ی کیف پول ارز های دیجیتال صحبت کنیم سوالی را بپرسیم. پول دنیای واقعی خود را چگونه نگه می‌دارید؟ آن را تمام وقت در دستانتان که نمی‌گیرید، می‌گیرید؟ احتمالاً آن را در کیف یا کیف پول چرمیتان یا حتی در قلکتان می‌گذارید!

اما اگر مقدار پولتان از حدی بیشتر شد چه؟ عاقلانه‌تر این است که پولتان را در جایی ذخیره کنید که امن باشد، مانند حساب‌های بانکی. یک کیف پول ارز دیجیتال نیز از همین اصول پیروی می‌کند.

با داشتن یک کیف پول می‌توانید ارز خود را به راحتی و با خیالی آسوده نگه دارید. علاوه بر این این امکان را خواهید داشت تا در هر لحظه‌ای ارزهای دیجیتال خود مانند [بیت کوین](#) را برای شخص دیگری بفرستید یا از شخص دیگری دریافت کنید. در حال حاضر چیزی بیش از ۱۵۰۰ ارز دیجیتال متفاوت در دنیا وجود دارد!

حال که آشنایی اولیه‌ای با کیف پول‌ها و دلیل استفاده از آن‌ها پیدا کردید، در ادامه کمی با جزئیات بیشتری به بحث درباره‌ی آن‌ها می‌پردازیم.

### یک کیف پول ارز دیجیتال چگونه کار میکند؟

در قسمت قبلی از مثالی در دنیای واقعی برای توضیح کیف پول های ارز های دیجیتال استفاده کردیم، کیف پول چرمی. اما باید گفت در دنیای دیجیتالی ارزهای دیجیتال و تکنولوژی بلاکچین شرایط کمی متفاوت است. در این دنیا، ارزهای دیجیتال نمی‌توانند در کیف پول‌های فیزیکی ذخیره شوند، چرا که خودشان نیز به صورت فیزیکی وجود ندارند. در عوض، بلاکچین تاریخچه معاملات را که به طور دقیق نشان می‌دهد کدام کلید عمومی و خصوصی سرمایه و منابع مالی را کنترل می‌کند، در خود نگه می‌دارد. برای آنکه مطمئن شویم این ساز و کار را به طور کامل درک می‌کنید، نقش هر یک از آدرس‌های کیف پول، کلید عمومی و کلید خصوصی را که با یکدیگر مرتبط نیز هستند توضیح می‌دهیم.

### آدرس کیف پول

آدرس یک کیف پول درست مانند شماره حساب بانکی است. همانطوری که می‌دانید هیچ ضرری ندارد که افراد دیگر شماره حساب شما را داشته باشند، چرا که برای انتقال پول به شما آن شماره حساب لازم است. با استفاده از همین شماره حساب ممکن است که حقوق شما پرداخته شود یا خانواده و دوستانتان برایتان پول بفرستند. در دنیای ارزهای رمزپایه نیز اگر کسی بخواهد پولی را به شما انتقال دهد باید آدرس شما را داشته باشد.

درست مانند دنیای واقعی، هیچ دو کیف پولی وجود ندارد که یک آدرس مشابه داشته باشند و در نتیجه طبیعی است که احتمال فرستادن پول برای کس دیگری جز شما صفر باشد. علاوه بر این، شما می توانید هر تعداد آدرسی که می خواهید داشته باشید و هیچ محدودیتی برای آن وجود ندارد.

## آدرس کیف پول بیت کوین

برای آنکه ببینید آدرس یک ارز مانند بیت کوین به چه شکل است، نگاهی به آدرس کیف پول زیر بیاندازید. گفته می شود این آدرس متعلق به خالق بیتکوین، ساتوشی ناکاموتو (Satoshi Nakamoto) می باشد!

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

همانطوری که می بینید این آدرس هم عدد و هم حروف بزرگ و کوچک دارد. از آنجایی که بلاکچین شفاف است، به راحتی می توانید اطلاعات آن را داشته باشید. بفهمید چه مقدار پول در آن نگهداری می شود یا چه تراکنش هایی پیش از این با آن انجام شده. البته باید گفت که آدرس کیف پول، نام و هویت اصلی صاحب آن در دنیای واقعی را فاش نمی کند. بخاطر همین موضوع از بلاکچین با عنوان «تخلص» یا «نام مستعار» (pseudonymous) یاد می شود.

## کلیدهای عمومی و خصوصی چگونه به آدرس کیف پول مربوط می شوند؟

حالا که می دانید آدرس یک کیف پول شباهت زیادی با یک شماره حساب بانکی دارد به سراغ آن می رویم که چگونه یک شخص می تواند کنترل پول و حساب خودش را داشته باشد. معمولاً افراد فکر می کنند که کلید عمومی یک کیف پول همان آدرس آن است، در صورتی که اینگونه نیست.

## کلید خصوصی

اساساً هر آدرس کیف پول ارز دیجیتال (به یاد داشته باشید که آدرس های کیف پول یکتا هستند و هیچ دو کیف پولی نمی توانند آدرس یکسانی داشته باشند) یک کلید عمومی و یک کلید خصوصی دارد. کلید خصوصی به صاحب آن اجازه می دهد که کنترل پول و حساب خود را در دست داشته باشد.

برای مثال در دنیای واقعی، برای انتقال پولی از حساب بانکی خود به حسابی دیگر لازم است از رمز شخصیتان استفاده کنید. هیچ کس دیگری نیست که این رمز را بداند، حتی بانکی که پولتان را در آن نگه میدارید. بدیهی است اگر کسی این رمز را بداند می تواند پول را از حساب شما به جایی دیر منتقل کند!

## کلید عمومی

یک کلید خصوصی نیز کاربردی مشابه دارد و به طور خاص به یک آدرس کیف پول منحصر به فرد تعلق دارد. اما کاربرد کلید عمومی چیست؟ یک کلید عمومی از طریق یک فرمول ریاضی (تابعی یک طرفه) به آدرس کیف پول مربوط می شود. این کلید یک «نسخه ی هش شده» است که در زیر توضیح داده می شود.

تابع هش (hash function) تابعی است که یک توالی یا سری از اعداد و حروف را (به نام ورودی) دریافت کرده و یک توالی یا سری جدید از اعداد و حروف را (به نام خروجی) تحویل می دهد. به این صورت، برای هر آدرس کیف پولی دیجیتالی یک کد عمومی وجود دارد که اگر آن را به تابع هش بدهیم آدرس کیف پول مد نظر را دریافت می کنیم. این تابع یک طرفه است، به این معنا که تابع معکوس ندارد و نمی توانیم آدرس را به کلید عمومی آن تبدیل کنیم. چنین کاری باعث امنیت کیف پول ها شده و به شما اطمینان می دهد که کیف پولتان نمیتواند هک شود. در زیر مثالی ساده آورده می شود.

**Private**

**Key:**

**03bf350d2821375158a608b51e3e898e507fe47f2d2e8c774de4a9a7edecf74eda**

**Public Key: 99b1ebcfc11a13df5161aba8160460fe1601d541**

به چشم انسان این دو کلید کاملاً دو چیز متفاوت و بی ربط با یکدیگر هستند. اما تکنولوژی این دو کلید را کاملاً مرتبط با یکدیگر شناخته و اثبات می کند شما صاحب این حساب هستید! در نتیجه می توانید کنترل پولتان را به دست بگیرید.

نکته قابل ذکر این است که توضیحات بالا توضیحاتی تکنیکی هستند و لازم نیست این کارها را خودتان انجام دهید. خود نرم افزار همه ی این کارها را انجام می دهد. درست مانند فرستادن ایمیل با استفاده از اینترنت. لزومی ندارد که بدانید تکنولوژی که این ایمیل را منتقل می کند چگونه کار میکند. خود جی میل همه ی کارها را برای شما انجام خواهد داد، درست مانند کیف پول دیجیتالی که تراکنش های شما را انجام می دهد!

## انواع مختلف کیف پول ارز های دیجیتال

در حال بازار، انواع متفاوتی از کیف پول ها در بازار وجود دارد و این به شما بستگی دارد که کدام یک از آن ها را انتخاب کنید. اساساً کیف پول های مختلف ویژگی های متفاوتی مانند امنیت بیشتر، راحتی یا کاربر پسندتر بودن را ارائه می کنند. در ادامه معروف ترین انواع کیف پول ها را معرفی خواهیم کرد.

علاوه بر این مطالب می توانید از محتوای ارائه شده توسط وبسایت ارز دیجیتال [arzdigital.com](http://arzdigital.com) در این زمینه نیز استفاده کنید. ارز دیجیتال علاوه بر معرفی انواع کیف پول ها و صحبت درباره ی ویژگی ها و تفاوت های آن ها، چگونه ثبت نام و ایجاد یک کیف پول را نیز به طور کامل توضیح داده است. از آنجایی که توضیحات این سایت جامع و کامل می باشد توصیه می شود که سری به این سایت نیز بزنید.



## کیف پول دسکتاپ

کیف پول‌های دسکتاپ بر روی یک لپ تاپ یا کامپیوتر دانلود و نصب شده و تنها از طریق همان لپ تاپ یا کامپیوتر می‌توان به آن کیف پول دسترسی داشت. به طور کلی این نوع کیف پول‌ها امنیت و راحتی مناسبی را به کاربران ارائه میکنند. اما باید به یاد داشت که اگر هکری از راه دور کنترل لپ‌تاپ یا کامپیوتر دستگاه شما را در دسترس بگیرد یا کسی رمز دستگاه شما را داشته باشد می‌تواند به کیف پولتان دسترسی پیدا کند. چند کیف پول معروف دسکتاپ:

Coinomi •

Electrum •



## کیف پول موبایلی

این نوع شباهت زیادی به کیف پول دستکتاپ دارد، به این صورت که باید نرم افزار آن را بر روی گوشی‌تان نصب کنید. در برخی کشورها مانند ژاپن افراد می‌توانند در فروشگاه‌ها از طریق اسکن کردن QR code پول خود را خرج کنند! چند کیف پول معروف موبایلی:

Bread wallet •

TronLink •

coinomi •



## کیف پول تحت وب

درست است که کار کردن با این نوع کیف پول از همه کیف پول‌ها راحت‌تر است اما امنیت آن از همه پایین‌تر است. این موضوع به این خاطر است که کثی که این کیف پول را در اختیار شما قرار می‌دهد کنترل کامل آن را نیز در دست دارد. توصیه می‌شود که مقداری کمی از ارز خود را در این نوع از کیف پول نگه‌داری کنید. چند کیف پول معروف تحت وب:

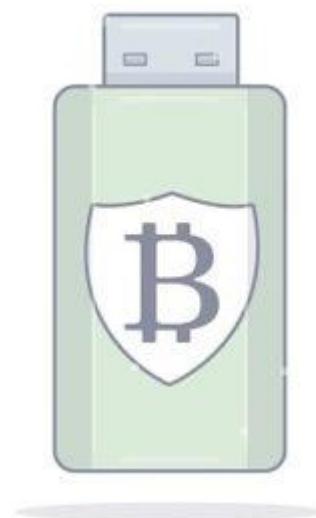
TronLink •

Tronscan •



## کیف پول کاغذی

کیف پول‌های کاغذی کیف پول‌هایی هستند که ارزششان واقعا دست کم گرفته می‌شود. تمام کاری که نیاز است انجام دهید چاپ کردن کلید عمومی و خصوصیتان بر روی یک تکه کاغذ است، همین، پولتان امن خواهد ماند! در این روش کلیدهای شما به هیچ سروری متصل نیستند، در نتیجه هکر ها تنها از طریق دزدیدن آن کاغذ فیزیکی می‌توانند شما را هک کنند! زمانی که نیاز داشتید پولتان را انتقال دهید، می‌توانید به سادگی به یک نرم افزار یا کیف پول تحت وب متصل شده یا حتی QR code چاپ شده را اسکن کنید.



## کیف پول سخت افزاری

اگر به دنبال امنیت هستید، هیچ کیف پولی امن‌تر از کیف پول سخت افزاری نیست. این کیف‌پول یک دستگاه فیزیکی است که تنها هدفش، نگه داری از کلیدهای دیجیتال عمومی و خصوصیتان می‌باشد. این دستگاه هیچ‌گاه به اینترنت متصل نمی‌شود، مگر این‌که بخواهید پولتان را انتقال دهید. هر چند در همین حالت نیز رمزتان را مستقیماً به خود دستگاه می‌دهید و به این صورت احتمال هک شدنتان توسط یک هکر را تقریباً به صفر می‌رسانید. چند کیف پول معروف سخت افزاری:

## آیا کیف پول‌های ارز دیجیتال امن هستند؟

حال که با انواع مختلف کیف پول‌ها با درجه راحتی‌های متفاوت آشنا شدید بیایید درباره امنیت آن‌ها صحبت کنیم. به طور کلی فارغ از اینکه از چه نوع کیف پولی استفاده می‌کنید، اگر کسی به کلید خصوصی شما دسترسی داشته باشد به راحتی می‌تواند کنترل پولتان را در دست گرفته و از حسابتان به حساب‌های دیگر پول منتقل کند. سوالی که وجود دارد آن است که برای جلوگیری از این اتفاق چه ساز و کارهایی طراحی شده است.

هر نوع کیف پولی که با اینترنت در ارتباط باشد در خطر هک شدن نیز قرار دارد. به یاد داشته باشید که با اینکه هکرها انسان‌هایی بی اخلاق هستند اما از هوش و نبوغ بالایی نیز برخوردارند. آن‌ها همواره در حال خلق راه‌های جدیدی برای دسترسی به اطلاعات انسان‌ها هستند. بنابراین این خود شما هستید که باید مراقب کلید خصوصیتان باشید. معمولاً هکرها از یکی از این روش‌ها برای دسترسی به اطلاعات شما استفاده می‌کنند:

- بد افزار (Malware)
- ویروس (Virus)
- کی لاگر (Key logger)
- دسترسی از راه دور به دستگاه شما (Remote access to your device)
- فیشینگ (Phishing)

برای حفاظت از حساب خود در برابر روش‌های بالا راه‌هایی نیز وجود دارد. در ابتدای اطمینان حاصل کنید که از آخرین نسخه نرم افزار، چه دستکتاپ و چه موبایل، استفاده می‌کنید. با این کار همواره بروزترین سطح از امنیت را خواهید داشت. علاوه بر این همواره می‌توانید از لایه‌های امنیتی بیشتر استفاده کنید. در بسیاری از کیف پول‌های ارز دیجیتال می‌توانید از روش احراز هویت دو مرحله‌ای (two-factor authentication) استفاده کنید، به این معنا که برای مثال برای ورود به اپ موبایل کیف پول، حتماً باید به کدی که به آن تلفن ارسال می‌شود دسترسی داشت.

در آخر استفاده از کیف پول‌هایی که به چندین امضا نیاز دارند نیز می‌تواند کمک کند. این کیف پول‌ها multi-signatures wallets نام دارند و برای انتقال پول توسط آن‌ها نیاز است تا فرد آن انتقال را از طریق چند دستگاه تایید کند، مثلاً هم با کامپیوتر شخصی‌اش در خانه، هم با موبایل و هم با لپ‌تاپ. اینگونه اگر یکی از آن دستگاه‌ها گم شود یا دزدیده شود یا حتی هک شود، باز هم کسی نمی‌تواند به کیف پول او دسترسی داشته باشد.

با رعایت کردن چنین مواردی می‌توانید مطمئن باشید که کیف پول شما از دست هرکس در امان است.

## آیا می توان همه ی ارزشهای دیجیتال خود را در یک کیف پول مشابه نگه داشت؟

این سوال یکی از متداول ترین سوالات درباره ی کیف پول ها است و جواب آن، بستگی دارد است. گاهی اوقات با توجه به نوع خاص ارزی که دارید می توانید این کار را بکنید. برای مثال، اگر فقط بیت کوین دارید تنها لازم است از کیف پولی که برای بیت کوین مناسب است استفاده کنید، اما اگر هم بیتکوین داشتید و هم لایتکون چه؟

با وجود آنکه هر کدام از ارزشهای بیت کوین و لایت کوین کیف پول مخصوص به خود را دارند اما این امکان که از یک کیف پول چند کاربرده نیز استفاده کرد وجود دارد. این نوع کیف پول ها به شما این امکان را می دهند تا انواع مختلفی از ارزشهای دیجیتال را در یک کیف پول ذخیره کنید که طبیعتاً از داشتن یک کیف پول برای هر ارز راحت تر است. البته باید گفت که این کیف پول ها ممکن است از هر ارزی پشتیبانی نکنند. توجه داشته باشید که اگر یک کیف پول متناسب با یک ارز خاص نباشد و شما آن ارز را به آن کیف پول انتقال دهید، پولتان را از دست خواهید داد! بنابراین همیشه پیش از انجام کاری ویژگی های کیف پولتان را بررسی کنید.