



## پس از گم شدن کلید خصوصی چگونه به کیف پول دیجیتال خود دسترسی پیدا کنیم؟

در دنیای ارزهای دیجیتال، کیف پول دیجیتال مانند کارت بانکی و گاوصندوق شما است. این نوع از کیف پول مانند کیف پول معمولی بوده و وظیفه نگه داری ارزهای دیجیتال شما را بر عهده دارد. در دنیای مجازی برای این که افراد امنیت داشته باشند، مکانیزم‌های مختلفی به کار گرفته می‌شود.

استفاده از **کلید** در کیف پول یکی از راه‌های برقراری امنیت است. هر کیف پول دیجیتال می‌تواند دارای دو نوع کلید باشد. **کلید عمومی** و **خصوصی** از مشخصات هر کیف پول هستند که کاربرد جداگانه‌ای دارند. زمانی که **کلید خصوصی کیف پول دیجیتال** خود را گم کنید، با خطر از دست دادن سرمایه مواجه خواهید شد. به همین دلیل در این مطلب از کیف پول من می‌خواهیم راهکارهایی برای دسترسی به کیف پول دیجیتال پس از **گم شدن کلید خصوصی** را معرفی کنیم.

# کیف پول دیجیتال در دنیای ارزهای دیجیتال

زمانی که وارد فعالیت در دنیای ارزهای دیجیتال می‌شود، اولین قدم در اکثر مواقع ثبت نام در یک صرافی و خرید مقداری ارز دیجیتال است. ارزهای دیجیتالی که از طریق صرافی‌ها خریداری می‌کنید در کیف پول شما درون خود صرافی ذخیره می‌شود.

با استفاده از این کیف پول می‌توانید ارزهای دیجیتال خود را به افراد مختلف انتقال داده یا معامله کنید. اگر قصد دارید خارج از محیط یک صرافی ایرانی یا خارجی فعالیت کنید، می‌توانید از کیف پول دیجیتال استفاده کنید. کیف پول دیجیتال فضای مشابهی به صرافی‌های ارز دیجیتال دارد.

در حال حاضر کیف پول‌های مختلفی به وجود آمده‌اند که می‌توانند دارایی‌های دیجیتال شما را نگه داری کنند. برخی از این کیف پول‌ها تنها برای یک بلاک چین ساخته شده‌اند یا تنها می‌توانند ارز دیجیتال درون خود نگه دارند.

در حالی که کیف پول‌های پیشرفته‌تر را می‌توان برای دیگر کارهای دنیای وب 3 استفاده کرد. [ثبت نام در متاورس](#)، پلتفرم‌های بلاک چینی و نگه داری از دارایی‌های ان اف تی جزوی از کاربردهای کیف پول دیجیتال است.

البته لازم به ذکر است که برخی از کیف پول‌های دیجیتالی متعلق به صرافی‌های ارز دیجیتال هستند. به طور مثال کیف پول تراست ولت توسط صرافی بایننس خریداری شده و از طریق این کیف پول می‌توانید به برخی از بخش‌های صرافی ارز دیجیتال بایننس دسترسی داشته باشید.

زمانی که از یک کیف پول برای خرید و فروش ارزهای دیجیتال استفاده می‌کنید، دو نوع کلید دریافت می‌کنید. برخی کیف پول‌های دیجیتال در ابتدای ورود به شما یک **کلید اختصاصی** می‌دهند و برخی از آنها در ادامه استفاده از برنامه این کلید را مشخص می‌کنند. به هر حال در هنگام استفاده از یک کیف پول دیجیتال، شما دارای دو نوع کلید خواهید بود.

## کلید خصوصی چیست؟

همان طور که گفتیم، هر کیف پول دارای دو کلید است. شما یک **کلید خصوصی** و یک **کلید عمومی** خواهید داشت. در هنگام معامله در دنیای ارزهای دیجیتال، در دست داشتن هر دو کلید عمومی و خصوصی ضروری است.

چرا که این دو کلید در کنار هم می‌توانند باعث انجام یک معامله و دسترسی به دارایی‌های دیجیتال شوند. در نگاه اول شاید کلیدهای عمومی تصادفی به نظر برسند، در صورتی که این کلیدها به طور کامل رمزنگاری شده هستند. کلید عمومی یک کلید اطلاعاتی هست که دارای داده‌های خاصی هست و این کار با استفاده از پروتکل‌های رمزنگاری انجام می‌شود.

هر دو کلید عمومی و خصوصی متشکل از حروف و اعداد انگلیسی هستند. زمانی که می‌خواهید در دنیای ارز دیجیتال ارزی را دریافت کنید، باید کلید عمومی خود را در اختیار فرد دیگر قرار دهید. به کلید عمومی می‌توانند مانند آدرس ایمیل نگاه کرد.

کلید خصوصی همان طور که از نامش پیداست، ماهیت خصوصی دارد و به هیچ وجه نباید آن را در اختیار افراد دیگر قرار داد. کلید خصوصی نیز برای دسترسی به دارایی‌های شما در دنیای بلاک چین استفاده می‌شود. به همین خاطر کلید خصوصی را می‌توان یک نوع رمز عبور برای ورود به ایمیل دانست.

مطلب پیشنهادی: [آموزش پیدا کردن آدرس کیف پول](#)

در مفهومی عملی‌تر و پیچیده‌تر، کلید عمومی دارایی‌های شما در دنیای ارز دیجیتال را رمزگذاری می‌کند و رمزگشایی این دارایی‌ها به عهده کلید خصوصی است. هر فردی که کلید خصوصی شما در اختیار بگیرد، به دارایی‌های شما دسترسی خواهد داشت. برای انتقال و دریافت رمزارز، مجبور به استفاده از کلید عمومی هستید. در صورتی که کلید خصوصی تنها برای دسترسی به دارایی‌های قبلی استفاده می‌شود.

## دلیل اهمیت کلید خصوصی چیست؟



دلیل اهمیت کلید  
خصوصی چیست؟



کلید خصوصی دقیقا همان چیزی است که برای دسترسی به دارایی‌های خود نیاز خواهید داشت. زمانی که این کلید از دست برود، تمام دارایی‌های شما نیز از بین می‌رود. برای آشنایی با اهمیت کلید خصوصی بهتر است کمی با ساز و کار ارزهای دیجیتال آشنا شوید.

ارزهای دیجیتالی مانند بیت کوین و اتریوم، ارزهایی کاملا غیرمتمرکز هستند. یعنی هیچ نوع بانک و سازمانی نیست که این ارزها را درون خود ذخیره کند. پس دارایی شما بین شبکه‌ای از کامپیوترهای مختلف پخش شده که به آن بلاک چین گفته می‌شود. یکی از اصلی‌ترین ویژگی‌های بلاک چین شفافیت آن است. یعنی همه می‌توانند تراکنش‌های انجام شده را مشاهده کنند.

براساس یک سری فرمول‌های پیشرفته ریاضی، کلید خصوصی شما یک کلید عمومی تولید می‌کند. به همین دلیل این دو کلید را می‌توان یک زوج کلید دانست. هرچند موقع دریافت و انتقال ارز دیجیتال، همه می‌توانند انتقال وجوه را مشاهده کنند، اما آنها از هویت شما مطلع نخواهند بود.

چرا که تنها کلید عمومی قابل مشاهده است. اما برای این که به ارزهای دیجیتال دسترسی پیدا کنید، مجبورید که از کلید خصوصی استفاده کنید. بدون داشتن کلید خصوصی، دسترسی به دارایی‌های دیجیتال تقریباً غیرممکن به نظر می‌رسد. البته برخی راه‌ها برای این کار نیز به وجود آمده‌اند که در ادامه به بررسی آنها می‌پردازیم.

## ریکاوری اطلاعات پاک شده هارد



## ریکاوری اطلاعات پاک شده هارد

تمام داده‌هایی که درون کامپیوتر مشاهده می‌شوند، به نحوی درون هارد ذخیره سازی شده‌اند. در دنیای ارزهای دیجیتال گم کردن کلید خصوصی و از دست دادن دارایی چیز جدیدی نیست. در حقیقت تا به حال ماینرهای زیادی سرمایه خود را از دست داده‌اند.

از زمان شروع به کار بیت کوین که ارزش بسیار کمی داشت، ماینرها بدون توجه به رشد قیمت بیت کوین، برنامه‌های مربوط به استخراج را گم کرده و باعث از دست رفتن سرمایه‌های کلان شده‌اند. پیش بینی می‌شود تا

1 میلیون عدد بیت کوین در دنیای این ارز دیجیتال گم شده باشد و هیچ راهی برای دسترسی به این ارزهای گم شده وجود ندارد.

اگر به هارد دیسک دستگاه خود دسترسی دارید، می‌توانید از فرایند [بازیابی اطلاعات](#) استفاده کنید. اطلاعات پاک شده زمانی می‌توانند بازیابی شوند که اطلاعات دیگری روی هارد اضافه نشده باشد. زمانی که داده‌های جدیدی روی بخش ذخیره شده داده‌های شما قرار بگیرد، اطلاعات قبلی از بین می‌روند. اگر خوش شانس باشید، می‌توانید با انواع نرم افزارهای مختلف اطلاعات هارد دیسک خود را استخراج کرده و به کلید خصوصی خود دسترسی داشته باشید.

### اثبات با دانش صفر یا Zero Knowledge Proof

این روش که اولین بار در سال 1980 ابداع شده بود، امروزه در دنیای ارزهای دیجیتال مورد استفاده قرار می‌گیرد. به دلیل ارزش بالای ارزهای دیجیتال و حجم زیاد ارزهای گم شده، استفاده از **روش اثبات با دانش صفر** راه مناسبی برای بازپس گیری دارایی‌ها است. این روش از دسترسی به اطلاعات بارها در طول سالیان توسط ریاضی دان‌های مختلف توسعه پیدا کرده و در نهایت در سال 2016 توسط تعدادی از پروژه‌های ارز دیجیتال این مکانیزم را به کار گرفتند.

در این روش دو نوع کد به نام تایید کننده و ثابت کننده وجود دارد. کد ثابت کننده سعی می‌کند تا به تایید کننده‌ها ثابت کند که اطلاعات مشخص شده را می‌دانید. تایید کننده‌ها نیز پس از اثبات این ادعا، به ثابت کننده دسترسی می‌دهند.

مشابه این فرایند امروزه در دنیای ارزهای دیجیتال برای بازگشت ارزهای دیجیتال استفاده می‌شود. اگر بتوانید به سیستم ثابت کنید، می‌توانید به کیف پول ارز دیجیتال خود دسترسی پیدا کرده و دارایی‌های خود را در اختیار بگیرید.

### خدمات شرکت والت ریکاوری (Wallet Recovery)

در فرایند **تولید کلید عمومی** از طریق **کلید خصوصی**، یک مسیر یک طرفه را شاهد هستیم. یعنی نمی‌توان از طریق **کیف پول عمومی** به کلید خصوصی دست پیدا کرد. حداقل این ادعایی است که برای اکثر افراد صادق است.

تنها راهی که برای شما باقی می‌ماند، حدس زدن کلید خصوصی از طریق کلید عمومی است. اگر به اندازه کلیدهای خصوصی و عمومی نگاه کنید، متوجه می‌شوید که این کار سال‌ها طول خواهد کشید. ترکیب حرف و عدد در ساخت کلیدهای عمومی و خصوصی کار را برای حدس زدن کلیدها سخت‌تر می‌کند.

شرکت والت ریکاوری با استفاده از روش‌های جدید تصمیم گرفته تا این کار را به صورت پیشرفته‌تری انجام دهد که درصد موفقیت بالایی دارد. در این روش شرکت والت ریکاوری، باید آخرین تراکنش‌های کیف پول شما شناسایی شود.

سپس از طریق این تراکنش‌ها، والت ریکاوری سعی می‌کند تا کلید خصوصی را حدس بزند. زمانی که یک کلید خصوصی با تراکنش‌های انجام شده منطبق باشد، به معنای موفقیت فرایند حدس زدن خواهد بود. به این ترتیب می‌توان گفت که آن کلید، کلید خصوصی شما است.

## FinderOuter

برنامه نویسان همیشه سعی می‌کنند روش‌های مختلفی برای بازیابی اطلاعات و حدس کلیدهای خصوصی ایجاد کنند. برنامه فایندر آوتر یا FinderOuter یکی از بهترین برنامه‌هایی است که برای **بازیابی کلید خصوصی ارز دیجیتال** ایجاد شده و اکثر افراد می‌توانند از آن استفاده کنند. در این حالت شما می‌توانید اطلاعاتی که از کلید خصوصی خود در اختیار دارید را به برنامه بدهید.

بهتر است برنامه FinderOuter را تنها از سایت‌ها و پلتفرم‌های معتبر دریافت کنید. پس از دانلود و نصب یک سری اطلاعات از شما درخواست می‌شود. برنامه پس از دریافت اطلاعات سعی می‌کند تا کلید خصوصی را حدس زده و به شما اطلاع دهد. ساده بودن رابط کاربری این برنامه باعث شده تا کاربران زیادی از آن استفاده کنند.