



## با قابلیت کیف پول های چند امضایی بیشتر آشنا شوید!

در دنیای ارزهای دیجیتال، به دلیل ارزش بالای رمزارزها، همه به دنبال امنیت بیشتر هستند. هر چه امنیت خود در دنیای ارزهای دیجیتال را بیشتر کنید، همچنان راه برای امنیت بیشتر وجود خواهد داشت.

چرا که دارایی‌های شما به صورت فیزیکی وجود ندارند و باید در دنیای مجازی مراقب دارایی‌های خود باشید. به همین دلیل توسعه دهندگان روش‌های مختلفی برای ایجاد امنیت بیشتر در دنیای ارزهای دیجیتال خلق کرده‌اند.

همان‌طور که دارایی‌های شما درون کیف پول ارز دیجیتال قرار می‌گیرد، باید به دنبال افزایش امنیت کیف پول خود باشید. به همین ترتیب می‌توان از **کیف پول چند امضایی** به جای **کیف پول تک امضایی** استفاده کرد. چنین کیف پول‌هایی امنیت بیشتری دارند و در این مطلب از کیف پول من قصد داریم تا چنین کیف پول‌هایی را بررسی کنیم.

## کیف پول چند امضایی چیست؟

برای این که با نحوه عملکرد کیف پول چند امضایی آشنا شوید، بهتر است ابتدا به نحوه کار کیف پول ارز دیجیتال آشنا باشید. کیف پول های ارز دیجیتال در ابتدای ورود از کاربران عبارات امنیتی یا یک رمز عبور را درخواست می کنند.

برای این که کاربری به دارایی های خود در دنیای ارزهای دیجیتال دسترسی داشته باشد، باید از کلید خصوصی خود استفاده کند.

در هنگام انجام تراکنش در دنیای ارزهای دیجیتال، کیف پول از طریق کلید خصوصی، یک کلید عمومی تولید می کند تا تراکنش انجام شود. به همین ترتیب کلید خصوصی نشانگر دارایی های شما در دنیای ارزهای دیجیتال است.

افرادی که **کلید خصوصی** شما را در اختیار داشته باشند، دارایی های شما را در اختیار خواهند داشت. به همین خاطر همیشه توصیه می شود تا از کلید خصوصی خود مراقبت کرده و آن را در اختیار کسی قرار ندهید.

حال حالتی را متصور شوید که مانند حساب های بانکی چند نفره، **کیف پول ارز دیجیتال** شما متعلق به چند نفر مختلف باشد. برای این که همگی افراد بتوانند به کیف پول دسترسی داشته و تراکنش را انجام دهند، باید همه افراد راضی به تراکنش باشند.

برای انجام این کار، مکانیزم متفاوتی در دنیای ارزهای دیجیتال استفاده می شود. در این حالت کیف پول های چند امضایی یا Multi-signature wallet به کار گرفته می شوند. این کیف پول ها به جای استفاده از یک کلید خصوصی، چند کلید خصوصی برای حساب شما تولید می کنند.

تعداد کلیدهای خصوصی تولید شده محدودیتی ندارد و می توانید بسته به سلیقه خود این کلیدها را در خواست کنید. باید در نظر داشته باشید که برای انجام تراکنش باید کلیدهای خصوصی را در برنامه وارد کنید.

مطلب پیشنهادی: [نحوه دسترسی به کیف پول پس از گم کردن کلید خصوصی](#)

چرا که هر کلید خصوصی برای رسیدن به کلید خصوصی نهایی ضروری خواهد بود. به همین خاطر کیف پول هایی که دارای قابلیت چند امضایی هستند، امنیت بیشتری دارند. در چنین کیف پول هایی برای هر کلید خصوصی، عبارات امنیتی تولید می شوید تا بتوانید کلید خصوصی خود را بازگردانید.

## کیف پول چند امضایی چگونه کار می‌کند؟



### کیف پول چند امضایی چگونه کار می‌کند؟



نحوه کار کیف پول‌های چند امضایی پیچیده نیست و در حقیقت همه می‌توانند از آنها استفاده کنند. این کیف پول‌ها به جای تولید یک کلید خصوصی، چند کلید خصوصی دیگر نیز تولید می‌کنند.

این کیف پول‌ها می‌توانند برای کارهای شراکتی یا برای کارهای تکی به دلیل افزایش امنیت مورد استفاده قرار بگیرند. در هر حالتی که قابلیت چند امضایی را فعال کنید، با روند مشابهی مواجه خواهید بود.

گاو صندوقی را تصور کنید که درون آن دارایی‌هایی متعلق به چند نفر مختلف وجود دارد. برای این که به محتوای درون گاو صندوق دسترسی داشته باشید، باید همه افراد از کلیدهای خود استفاده کنند تا در گاو صندوق باز شود.

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

حال همین حالت را می‌توان برای کیف پول ارز دیجیتال استفاده کرد. در این حالت یک کیف پول می‌تواند چند کلید خصوصی داشته باشد. هر کلید خصوصی به همراه یک عبارت امنیتی تولید می‌شود تا بتوانید با استفاده از آن کلید خصوصی را بازیابی کنید.

برای این که کیف پول باز شود، باید تمامی کلیدهای خصوصی را در برنامه وارد کنید. پس از آن می‌توانید به دارایی‌ها دسترسی پیدا کرده و به تراکنش بپردازید.

در نظر داشته باشید که تایید تراکنش‌ها در این حالت نیاز به وارد کردن کلیدهای خصوصی یا امضاها دارد. برای این که انجام تراکنش‌ها درون تیم‌های شراکتی راحت‌تر شود، می‌توان شرایط خاصی را برای انجام تراکنش در نظر گرفت.

به همین خاطر برخی کیف پول‌ها امکان انجام تراکنش با در دست داشتن 2 کلید از 3 کلید را فراهم می‌کنند. این برای حالت‌های دیگر نیز قابل تعریف است. البته شما می‌توانید ضرورت وارد کردن 3 کلید خصوصی از 3 کلید را نیز برای کیف پول تعریف کنید تا به امنیت بیشتری برسید.

در حالتی که 3 امضا برای کیف پول خود ساخته باشید، 2 کلید خصوصی را نیاز است تا وارد کنید. با وارد کردن 2 کلید خصوصی، به کلید خصوصی سوم دسترسی خواهید داشت.

در این حالت نیز می‌توانید با آن کلید خصوصی، کلید عمومی تولید کنید. کیف پول‌هایی که دارای قابلیت چند امضایی هستند، با روش‌های مختلفی قابلیت چند امضایی را در اختیار کاربران قرار می‌دهند. این قابلیت می‌تواند به صورت 2 از 3 (روشی که گفته شد)، 3 از 4 یا غیره باشد که فرایندی مشابه به فرایند 2 از 3 دارد.

## مزایای کیف پول چند امضایی

**امنیت بیشتر** همچنان در صدر اهداف دنیای **بلاک چین** و ارزهای دیجیتال قرار دارد و به همین خاطر کیف پول‌های چند امضایی به وجود آمده‌اند. قابلیت چند امضایی مزایای زیادی دارد که امنیت را برای کاربران افزایش می‌دهد. از مزایای کیف پول چند امضایی می‌توان به موارد زیر اشاره کرد.

زمانی که از قابلیت چند امضایی استفاده می‌کنید، می‌توانید حالت‌های 2 از 3 یا 3 از 4 را تعریف نمایید. در این حالت حتی زمانی که یکی از کلیدهای خصوصی را از نداشته باشید، می‌توانید تراکنش‌های خود را انجام دهید.

در حقیقت مسئولیت کیف پول بین چند نفر مختلف تقسیم می‌شود و با از دست رفتن یک کلید خصوصی نیز کیف پول به کار خود ادامه می‌دهد. البته این در شرایطی است که چنین حالتی فعال شده باشد.

در حالتی که قابلیت چند امضایی تعریف شود، هرکس به سختی می‌توانند به دارایی‌های شما دسترسی داشته باشند. چرا که یک کلید خصوصی برای هک کردن کیف پول کافی نخواهد بود.

به دست آوردن کلیدهای خصوصی موجود در افراد دیگر نیز سخت است و بعید است افراد بتوانند از این روش برای دستیابی به دارایی‌های شما استفاده کنند. امکان دزدی از طریق فیشینگ در این حالت به صفر می‌رسد. در بلاگ کیف پول من مطلبی در خصوص **نحوه فیشینگ ارز دیجیتال** داریم که پیشنهاد می‌کنیم مطالعه بفرمایید.

به طور معمول کیف پول‌هایی که قابلیت چند امضایی دارند، برای اکثر پلتفرم‌ها و دستگاه‌ها عرضه شده‌اند. به همین ترتیب نیاز نیست تا شرکای دیگر منتظر یک فرد باشند. این افراد می‌توانند با استفاده از کلید خصوصی خود از هر دستگاهی به کیف پول متصل شده و کارهای خود را انجام دهند.

بازیابی کلید خصوصی با استفاده از عبارات امنیتی امکان پذیر است. این کار می‌تواند در اکثر مواقع امنیت شما را به خطر بیندازد. چرا که هکرها با در دست داشتن این عبارات می‌توانند کلید خصوصی شما را به دست آورند.

این امر در مورد کیف پول‌های چند امضایی وجود ندارد. چرا که برای به دست آوردن کلید خصوصی از طریق عبارات امنیتی، بقیه افراد نیز باید عبارات امنیتی خود را وارد کیف پول کنند.

## معایب کیف پول چند امضایی



همیشه می‌توان انتظار چند عیب از تکنولوژی و فناوری‌های جدید را داشت. این مورد برای کیف پول‌هایی با قابلیت چند امضایی نیز صادق است. به همین ترتیب کیف پول‌های چند امضایی چند عیب عمده دارند که باعث محدودیت آنها شده است.

در ابتدا باید این نکته را متذکر شد که استفاده و ساخت یک کیف پول چند امضایی برای همه افراد امکان پذیر نیست. انجام چنین کاری نیاز به دانش خوب در زمینه ارزهای دیجیتال و بلاک چین دارد. به همین خاطر برای استفاده از قابلیت چند امضایی باید از افراد متخصص این حوزه استفاده کنید.

مطلب پیشنهادی: [امنیت شبکه بلاک چین چگونه است؟](#)

عیب دیگر چنین کیف پول‌هایی، عدم وجود قوانین مشخص و واضح برای چنین کیف پول‌هایی است. در صورتی که کیف پول ارز دیجیتال با قابلیت چند امضایی بین شریکان خود داشته به مشکل برخورد، نمی‌توانید از مراجع قانونی کمک بگیرید.

چرا که همچنان قوانین مشخصی برای چنین مواردی به وجود نیامده و باید به تنهایی برای خارج کردن دارایی‌های خود از کیف پول تلاش کنید. زمانی که قصد داشته باشید با این کیف پول ارز دیجیتال به خرید یا معامله بپردازید، باید صبور باشید.

چرا که کار کردن این کیف پول‌ها **کند** بوده و وابسته به سرعت وارد کردن کلیدهای خصوصی دارد. شریکان و همکاران شما باید انجام هر تراکنش را با استفاده از کلید خصوصی تایید کنند.

به همین دلیل انجام معامله با کیف پول چند امضایی زمان‌بر خواهد بود. برای مثال شما اگر قصد **خرید** را داشته باشید بایستی زمانی را برای تایید کردن تراکنش توسط شریکان ولت ارز دیجیتال تان بگذرانید.

از طرف دیگر، همان‌طور که گفتیم مزیت برگرداندن کلید خصوصی با استفاده از عبارات امنیتی در این حالت می‌تواند دردسرساز شود. برای این کار نیاز است تا همه افراد کلیدهای خصوصی خود را وارد کنند.