

کیف پول

در ارزهای دیجیتال

علیرضا زجاجی



بلاکچین

یک دفتر دیجیتال جهانی خطاناپذیر است که برای ذخیره سازی هر نوع تراکنش‌هایی که برای انسان مهم است، به کار می‌رود.

Blockchain ➡

زنجیره‌ی بلاک‌ها ➡

زنجیره‌ی بسته‌ها ➡

دفاتر کل عمومی ➡



ارز دیجیتال

ارزی است که معمولاً مبتنی بر بلاکچین یا سیستم‌های عمومی پیشرفته‌تر است و تراکنش‌های آن در یک دفتر کل عمومی ثبت می‌شود.



انواع دسترسی به بلاکچین

دسترسی عمومی: قابلیت رؤیت تراکنش‌های یک حساب ➡

دسترسی اختصاصی: قابلیت ثبت تراکنش از یک حساب ➡



انواع کلید

👉 کلید عمومی:

کلید یک حساب که در
اختیار همه قرار می‌گیرد

👉 کلید اختصاصی:

کلید یک حساب که فقط
در اختیار صاحب حساب
قرار می‌گیرد



و اما کلید ...



کاربرد کلید

رمز کردن و از رمز در آوردن اطلاعات جهت مبادله در یک فضای
عمومی

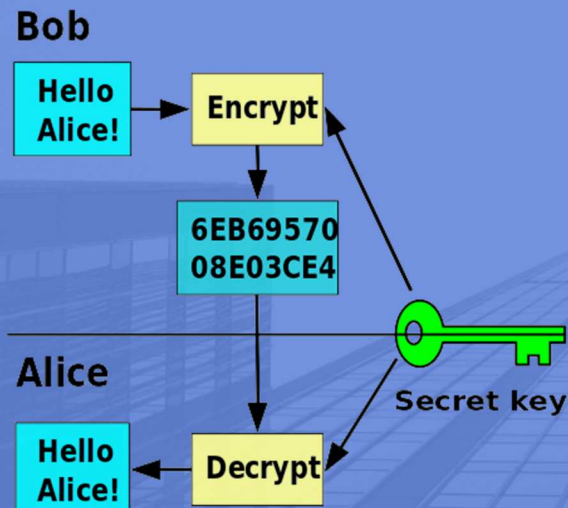




انواع رمز نگاری با کلید

👉 رمز نگاری با کلید متقارن: یک کلید برای رمز کردن و از رمز در آوردن استفاده می‌شود.

👉 مشکلات: چگونه در یک فضای عمومی کلید را به طرف مقابل منتقل کنیم؟

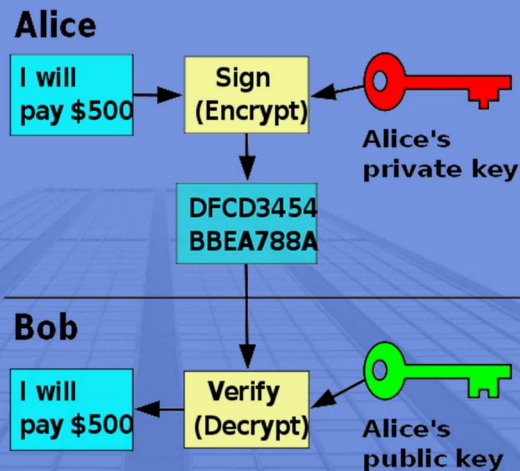
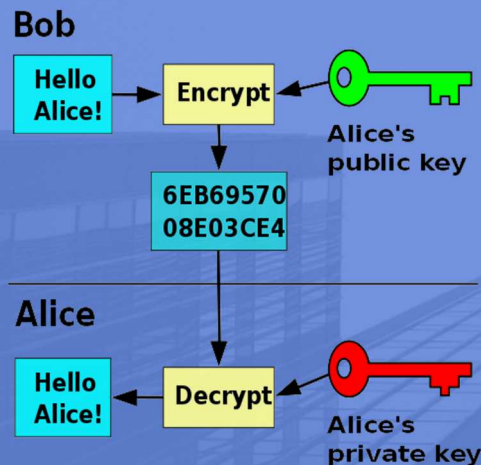


Symmetric Cryptography



انواع رمز نگاری با کلید

👉 رمز نگاری با کلید نامتقارن: از یک زوج کلید، یکی برای رمز کردن و دیگری برای از رمز در آوردن استفاده می‌شود.
👉 کلید عمومی و کلید اختصاصی



Asymmetric
Cryptography



نقش کلیدها در کیف پول دیجیتال

کلید اختصاصی:

در ثبت هر تراکنش علاوه بر
محتوای تراکنش آن محتوا با کلید
اختصاصی فرد ارسال کننده نیز
رمز می شود

کلید عمومی:

برای بررسی صحت تراکنش رمز
ارسال شده با کلید عمومی فرد
ارسال کننده باز می شود و با
محتوای تراکنش مقایسه می شود



امنیت در کیف پول دیجیتال

👉 کلید اختصاصی کیف پول در اختیار صاحب کیف باشد

👉 کلید اختصاصی در اختیار هیچ فرد دیگری نباشد

👉 در صورت از بین رفتن کیف پول، کلید اختصاصی قابل بازیابی باشد



وظایف کیف پول دیجیتال

👉 ذخیره سازی کلید اختصاصی

👉 محافظت از کلید اختصاصی

👉 امضا کردن تراکنش‌ها با کلید اختصاصی

👉 دسترسی به بلاکچین و خواندن تراکنش‌های حساب

👉 مدیریت حساب‌های فرعی و اتصال به حساب اصلی



زوج کلیدهای فرعی در HD Wallet

➡ برای هر زوج کلید عمومی و اختصاصی هر کیف پول می‌توان برای
ارزهای مختلف زوج کلید ساخت

➡ زوج کلید فرعی: برای هر ارز می‌توان تعداد بیشماری زوج کلید
ساخت

➡ کاربرد زوج کلیدهای فرعی



کیف پول‌های چند امضایی

➡ برای امضا کردن تراکنش‌ها از ترکیب چند زوج کلید استفاده می‌شود.

➡ برای تأیید تراکنش‌ها امضای تمام صاحبان امضا لازم است.

➡ قراردادهای هوشمند به عنوان کیف پول چند امضایی



انواع

کیف پول دیجیتال

فول نود ➡

کیف پول تحت وب ➡

کیف پول نرم افزاری ➡

کیف پول سخت افزاری ➡

کیف پول کاغذی ➡



فول نود

یک کامپیوتر در شبکه‌ی بلاکچین که نقش یکی از سرورهای شبکه را بازی می‌کند

👉 کیف پول نیز روی همان کامپیوتر قرار دارد و این کامپیوتر فقط برای پرداخت ارز اینترنتی روشن می‌شود و به اینترنت وصل می‌شود

👉 امنیت بسیار بالا

👉 حجم اطلاعات بسیار بالا



کیف پول تحت وب

مانند سایت www.blockchain.info

➡ کلید اختصاصی شما علاوه بر شما در اختیار سایت نیز هست

➡ هک شدن سایت

➡ بسته شدن سایت یا بلاک شدن کاربران

کیف پول نرم افزاری

یک نرم افزار روی کامپیوتر یا موبایل شما که نقش رمز کردن تراکنش و مدیریت آن را بر عهده می گیرد

مانند Exodus روی کامپیوتر و Jaxx و Coinomi برای موبایل

- 👉 باید رمز اختصاصی شما قابل بازیابی باشد
- 👉 از عدم مبادله‌ی کلید توسط نرم افزار مطمئن باشیم
- 👉 ترجیحا اپن سورس (متن باز) باشد
- 👉 توسط ارائه کننده‌ی ارز مورد نظر تأیید شده باشد



کیف پول سخت افزاری

یک وسیله که به کامپیوتر شما وصل می‌شود و بدون مبادله‌ی کلید اختصاصی نقش رمز کردن داده را بر عهده می‌گیرد

مانند Ledger Nano S و Trezor

👉 باید رمز آن را در هنگام نصب ریست کنیم

👉 از پشتیبانی ارز مورد نظر مطمئن باشیم

👉 بالاترین امنیت

کیف پول سخت افزاری

کیف پول سخت افزاری ایرانی

دُرَج



👉 کی کیف پول ترزور



کیف پول کاغذی

کلید اختصاصی مستقیماً یا به شکل رمز ۱۲ کلمه‌ای یا رمز ۲۴ کلمه‌ای یا به شکل QR Code روی یک کاغذ نوشته یا چاپ می‌شود تا در زمان بازیابی مورد استفاده قرار گیرد.

www.BitAddress.org

👉 حتماً باید کنار یک سیستم کیف پول دیگر مورد استفاده قرار گیرد

👉 از امنیت کاغذ پشتیبان مطمئن باشیم



تولید کلید

روش‌های زیادی برای تولید کلید وجود دارد اما یکی از روش‌های خوب استفاده از سایت بیت آدرس است:

www.BitAddress.org



رمزهای معادل
کلید اختصاصی

رمز ۱۲ کلمه‌ای

رمز ۲۴ کلمه‌ای



روش انتخاب کیف پول مناسب برای هر ارز

➡ باید به سایت اصلی ارز مورد نظر مراجعه کنیم و کیف پول توصیه شده برای آن را ببینیم

➡ برای پیدا کردن سایت اصلی ارز مورد نظر به سایت زیر مراجعه می‌کنیم:

www.CoinMarketCap.com



به امید موفقیت شما عزیزان...

علیرضا زجاجی

@AlirezaZojaji