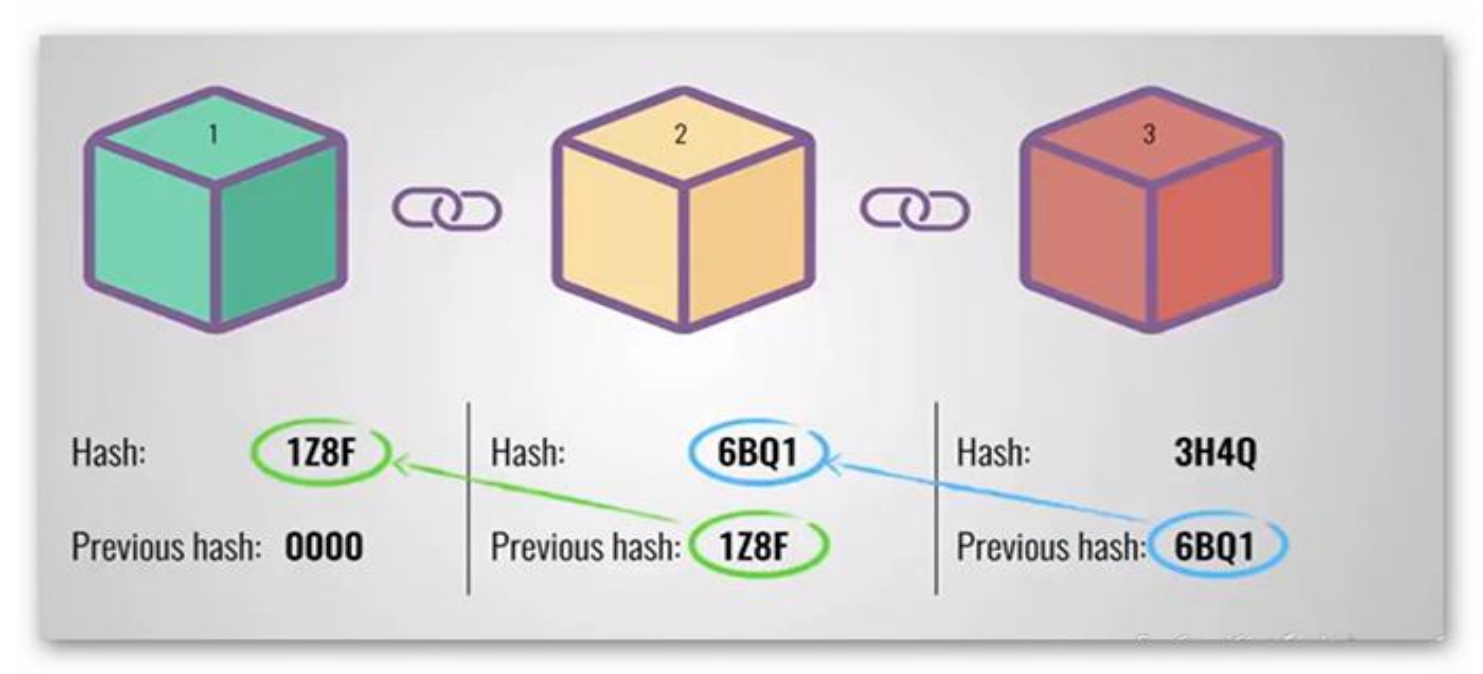
Crypto Currency

- Blockchain
- Currencies
- Token
- Wallets
- Public and private keys
- Transaction
- Algorithms
- Mining
- Trade

Blockchain

این فناوری در حقیقت زنجیره‌ای از بلوک‌هاست. به طور کلی بلاک چین یک نوع سیستم ثبت اطلاعات و گزارش است. تفاوت آن با سیستم‌های دیگر این است که اطلاعات ذخیره شده روی این نوع سیستم، میان همه اعضای شبکه به اشتراک گذاشته می‌شوند و با استفاده از رمزنگاری امکان حذف و دستکاری اطلاعات ثبت شده تقریبا غیرممکن است.

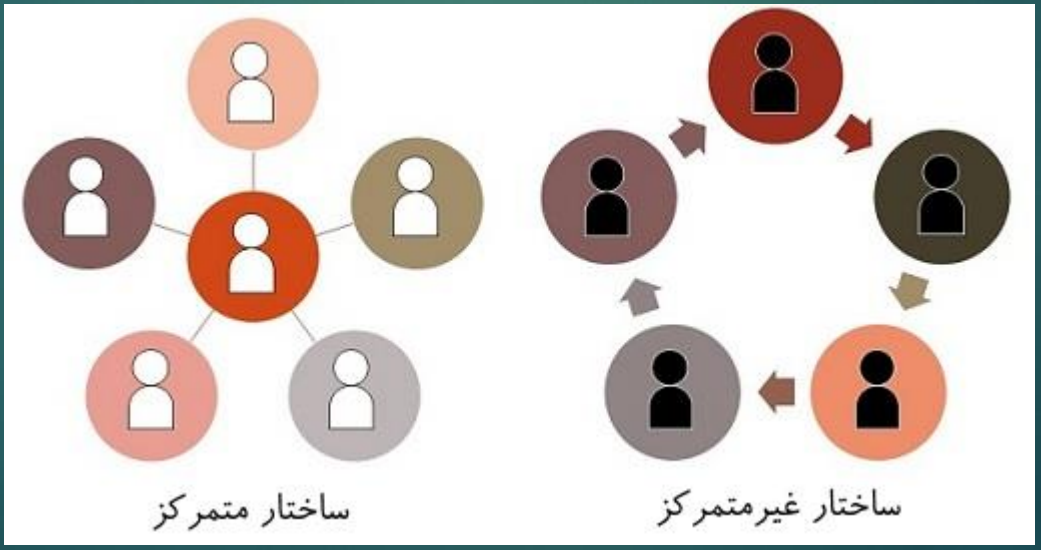
اگر بلاک چین یک سیستم عامل باشد، بیت کوین و آلت کوین ها نرم افزاری روی این سیستم عامل هستند.



Blockchain

پایگاه داده (متمرکز) فضایی است برای ذخیره اطلاعات که طبیعتا این پایگاه داده توسط یک فرد یا مرکزیتی ایجاد و کنترل می‌شود.

فناوری بلاک چین (غیر متمرکز) را می‌توان شبکه‌ای در نظر گرفت که کارکردی مانند پایگاه داده دارد اما مرکزیت خاصی ندارد و توسط نهاد یا ارگانی کنترل نمی‌شود، اطلاعاتی که در بلاک چین ذخیره می‌شوند یک سری تفاوت هایی با اطلاعات ذخیره شده در پایگاه داده ها دارد.



Blockchain

- امنیت

اطلاعات در بلاک چین رمزنگاری شده و سپس ذخیره می‌شوند، که این امر باعث افزایش امنیت اطلاعات می‌شود.

- شفافیت

نکته‌ی دیگری که جالب توجه است این است که در بلاک چین، اطلاعات برای همه‌ی اعضای آن قابل مشاهده است، بنابراین شفافیت در اوج خود قرار دارد.

- غیر قابل تغییر

قابلیت جالب دیگر بلاک چین این است که اطلاعات در بلاک چین قابل تغییر و یا حذف شدن نمی‌باشد.

- بلاک چین عمومی

به بلاک چینی گفته می‌شود که دسترسی به شبکه آن برای عموم آزاد است و همه می‌توانند یکی از اعضای آن شوند مثل بلاک چین بیت کوین، اتریوم و سایر ارزهای دیجیتالی

- بلاک چین خصوصی

در این نوع برخی از سرویس دهنده ها یا اصطلاحا گره های شبکه هستند که به سایر اعضا اعتبار می‌بخشند و شبکه در دسترس عموم قرار ندارد و سایر گره‌ها باید مورد بررسی، شناسایی و ثبت نام قرار گیرند. مثل بلاک چین های شرکتی که از طریق آن پرداخت حقوق کارمندان و امور مربوط به آنها انجام می‌شود

Currencies

Digital Currency

ارز هایی هستند که به صورت الکترونیکی ذخیره و منتقل می‌شوند و مبنای آنها صفر و یک است.

این مفهوم در مقابل واسطه‌های فیزیکی مانند پول بانکی (فیات) یا سکه مطرح می‌شود.

Cryptocurrency

رمزارز یکی از انواع ارز دیجیتال است که از فناوری رمزنگاری در طراحی آن استفاده شده و معمولا به صورت غیرمتمرکز اداره می‌شود.

رمز ارز از نمونه ارزهای دیجیتال محسوب میشود اما هر ارز دیجیتالی ارز رمزارز نیست

مثال رمز ارز: بیت کوین – اتریوم - ریپل - مونرو ...

Fiat currency

پول یا ارز فیات Fiatچیست ؟ پول فیات به واحد پولی گفته میشود که دولت‌ها آن را منتشر می کنند

Token

- COINS

A coin is a cryptocurrency that has its own blockchain, such as Bitcoin, Ethereum, Litecoin, Ripple.

- TOKEN

A token is a cryptocurrency that is built on another blockchain, such as a dApp that runs on Ethereum's blockchain.

Wallet

والت ارز رمزپایه : نرم افزاریست که کلید های عمومی و خصوصی را ذخیره و در تعامل با انواعی از زنجیره بلوکیست. تا کاربران بتوانند پول دیجیتال فرستاده یا دریافت کنند و موجودی خود را مدیریت کنند.

Wallet

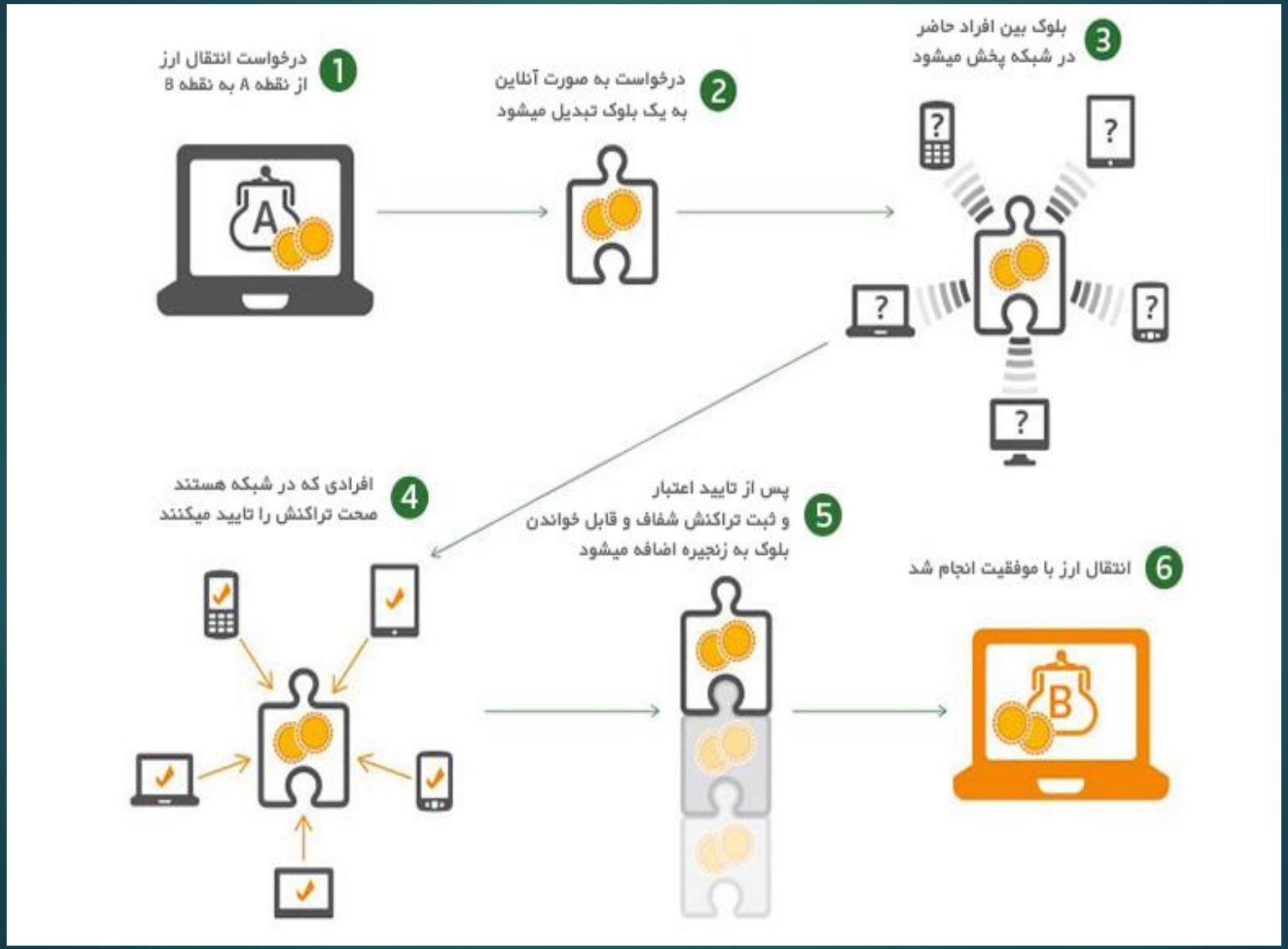
software (hot)

این نوع از والت ها بر روی فضای ذخیره مجازی (Cloud)فعالیت میکنند و از طریق هر دستگاه کامپیوتری از هر مکانی قابل دسترسی اند. با اینکه این نوع از والت، آسانترین نوع دسترسی را داراست، والت های آنلاین کلیدهای خصوصی شما را بصورت آنلاین ذخیره میکنند و توسط یک شخص یا شرکت ثالث کنترل میشوند، پس در برابر هک شدن و حملات، آسیب پذیر هستند.

Hardware (cold)

والت های سخت افزاری از این لحاظ با والت نرم افزاری متفاوتند که کلید خصوصی یک کاربر را بر یک سخت افزار، مانند یک USBذخیره میکنند. با اینکه والت های سخت افزاری تراکنش ها را آنلاین انجام میدهند، اما به صورت آفلاین ذخیره شده اند که باعث امنیت بیشتر میشود.

Transaction



Transaction

Let’s assume A wants to send B 1 BTC.

B sends his Bitcoin address (what’s known as a “hashed public key”) to A.

It looks something like this:
3D94LKmtQuVG8JFB3F7cB7gwj614yG4CPg

A enters the address in his cryptocurrency exchange or wallet along with the Bitcoin (BTC) amount (1BTC) and presses send.

B receives the BTC minus a small fee.

these fees can range anywhere between $0.05 to be delivered within the next hour or $0.58 within ten minutes.

It doesn’t matter if Alex sent 1BTC or 1000BTC - the fees would still be the same.

Transaction

From the moment A submits his transaction to the blockchain, every node in the Bitcoin network receives the transaction request. Every node makes sure that:

1-A is actually who he is claiming to be. The nodes verify A's identity through his private key — a private key identifies your source of funds. Anyone who has access to this private key has access to your money. This is why it's paramount to make sure to keep your private key secure.

2-A actually has the 1BTC to send to B. Since the nodes have a copy of the entire ledger of transactions, they can easily check to see if Alex has the money.

If at least 51% of the nodes come to a consensus on the two above elements, the transaction goes through and the nodes update the ledger with the new transaction.

Algorithms (Proof of work)

- SHA-256 بیت کوین، بیت کوین کش
- Scrypt لایت کوین، دوج کوین، نئو
- Ethash اتریوم، اتریوم کلاسیک
- Equihash- زی کش، زن کش و بیت کوین گلد
- Blake, Blake2, and Blake2b- سیاکوین و دکرد
- Keccak- اسمارت کش، مکس کوین
- CryptoNight- مونرو، بایت کوین
- X11- دش
- Verge و کوین های چند الگوریتمی Myriad

Algorithms (Proof of stake)

Mining (hardware)

این نوع ماینینگ مربوط به شبکه هایی است که بر مبنای گواه اثبات کار (POW) کار می‌کنند؛ مانند بیت کوین، اتریوم و...

- ASIC

- GPU

Mining (software)

این نوع ماینینگ نیاز به استفاده از سخت افزارهای قدرتمند ندارد، بلکه بیشتر میزان دارایی فرد ماینر است که در فرآیند ماینینگ دخیل و موثر است. شبکه‌هایی که ماینینگ آنها به این صورت است، با ساختار مبنی بر گواه اثبات کار (POW) متفاوت است و شبکه‌ی آنها بر مبنای روش‌هایی مانند گواه اثبات سهام (POS) و DPOSو... کار می‌کند. شبکه‌ی کوین ها و توکن هایی مانند لیسک، استیم، ویوز و... اینگونه کار می‌کند. ماینر در این شبکه با گرو گذاشتن مقدار مشخصی از توکن خود در شبکه مورد نظر، شروع به فرآیند ماینینگ می‌کند..