Altcoins

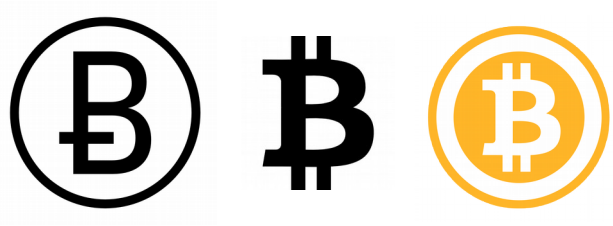
Competition is healthy, and alternatives to Bitcoin are cropping up almost every day. In terms of market capital, Ethereum comes in at number 2 with around $17 Billion. Ethereum offers more features such as programmable smart contracts, where you can send money only when certain conditions are satisfied. DASH is another good alt coin, offering a private ledger for anonymous transactions as well as a voting system for deciding on network-wide changes. The list goes on and on, with intended special use cases varying from humourous Dogecoin, to ultra-fast Litecoin, to dank PotCoin. There is a coin for everyone!

Chris Grimmett
Bitcoin Enthusiast
chris@grimtech.net

How do I use Bitcoin? Contd.

Having a Bitcoin wallet on your phone is often called a "hot wallet," meaning it's not the most secure way of storing Bitcoin. You could potentially lose your phone, along with your private keys, which means you wouldn't be able to spend your Bitcoin anymore.

Because of the nature of hot wallets, it is important to create a backup of your private keys in case your device is lost or stolen. This feature is available in all Bitcoin wallets worth their salt. Remember, your wallet doesn't hold the Bitcoin, it only holds the keys which allow you to spend your Bitcoin. As long as you have your private keys, you can recover your ability to spend your Bitcoin even if your device is lost.



What is Bitcoin?

Forget about the "coin" in Bitcoin for a moment. Bitcoin is a worldwide database with records that cannot be changed. New records can be added, but it is impossible to alter old records. Anyone can run software on any computer or smartphone and access this database, to read any records that have ever been written to the database.

Because it is not possible to mutate these database records, it's only natural that the first application of Bitcoin is currency. The database history, or **blockchain**, holds records telling who owns what. Charlie owns 3 Bitcoin. Sara owns 0.5 Bitcoin. George owns 0.0003 Bitcoin.

Who owns Bitcoin?

Bitcoin is not a company; Bitcoin is a protocol. You may have heard of TCP/IP, a computer protocol which powers much of the internet. Just like TCP/IP, Bitcoin the protocol is not owned by anyone, it is simply a tool which anyone can use to securely prove ownership of resources.

What is Bitcoin mining?

Bitcoin mining is a process which prevents users from cheating the ledger. Miners use the ledger of all past transactions, and ensure that spenders are rightful owners of the funds that they claim to be spending. This process is done using software on high performance computers, and mining is what makes the Bitcoin network so secure. Because of the mining process, Charlie can't spend 5 Bitcoin when he only owns 3.

How is Bitcoin used?

Bitcoin's most popular use is as digital cash for the internet. Using Bitcoin, Sara can pay Charlie directly for goods or services, in the same way as when she pays in-person using physical cash. Bitcoin liberates users from the fees, political censorship, middlemen, and gatekeepers which are inherent in payment methods such as VISA, MASTERCARD, and Paypal.

What do I need to participate?

Anyone can participate in the Bitcoin network. Unlike traditional money, with Bitcoin you don't need to ask permission or rely on a central authority.

How do I use Bitcoin?

Bitcoin is traded between two parties similar to how a bank transfer works. When Charlie sends 1 Bitcoin to George, the Bitcoin isn't actually going anywhere. All that is happening is that the global Bitcoin ledger (blockchain) is being updated to show that George now owns 1 more Bitcoin, and Charlie owns 1 less Bitcoin. Charlie is able to spend the Bitcoin in his account because Charlie owns the **private key** which unlocks the Bitcoin he owns. In Bitcoin, private keys equal ownership. Without that private key, Charlie can't spend the Bitcoin in his account.

The easiest way to use Bitcoin is to install "Bitcoin wallet" software on your smartphone. Using a popular Bitcoin wallet such as Mycelium, you can generate public and private keys which you can use for receiving and sending Bitcoin.