Bitcoin Foundation

Introduction to Bitcoin

Education Committee of the Bitcoin Foundation

What is Bitcoin and why should I care?

When most people first hear about Bitcoin, the first question they ask is "What is it?" This guide provides a concise answer to that question and explains a few of the terms that one usually hears in connection with Bitcoin.

For most practical purposes, Bitcoin can be thought of as just two things: (1) A payment network and (2) a currency that is used in the Bitcoin payment network. We often refer to the currency as BTC, such as "please pay me 3.1 BTC".

But why does the world need another currency and another payment network? To answer that question, we need to see how bitcoin differs from existing currencies and how Bitcoin differs from existing payment networks.

The **bitcoin currency** is exclusively digital. It is not issued or backed by a government, organization or company. There will never be more than 21 million bitcoins, and the money supply increases with a predefined and diminishing rate until their limit is reached. Those characteristics are almost completely antithetical compared to those of local currencies. For example, the US dollar has a physical form (the dollar bills), although it is commonly used in electronic form through trusted intermediaries. It is issued and backed by the central bank of the United States, there is no limit to how many US dollars will ever exist, and the rate of generation, or "printing," of US dollars is unknown.

The **Bitcoin network** is a decentralized, peer-to-peer computer network, in which computers can exchange information with each other without the mediation of a central server. The Bitcoin network is therefore neutral because no central computer can forbid another computer to be part of the network. The security of messages exchanged in the Bitcoin network is guaranteed by the use of public-key cryptography, and the validity of the transactions is guaranteed by hard mathematical calculations that the network computers have to perform in a process called "mining." Finally, transaction costs in the Bitcoin network are either free or extremely low.

Let's now compare the Bitcoin network with SWIFT, the payment network used by many banks in the world. The SWIFT network depends on a select number of computer servers and it's a centralized network. Similarly to the Bitcoin network, the messages in the SWIFT network are secured by cryptography, but transactions are validated by a central database. Finally, transactions in the SWIFT network can be quite costly.

Now you know that :

- The bitcoin currency is exclusively digital, independent of any central issuing authority, borderless, with a money supply that is limited and predetermined.
- The Bitcoin network is a decentralized, neutral, peer-to-peer computer network which is secured by cryptography and charges zero or tiny fees.

Now, let's consider a few cases where bitcoin and the Bitcoin network is superior to existing currencies and payment networks.

- If you are one of the 2.5 billion people in this world who do not have a bank account or if you have friends and family who live in other countries, you can use the Bitcoin network to exchange bitcoin with people from all over the world immediately for no or for a very small cost.
- If you have savings and you are worried that your government might confiscate some of it, like the government of Cyprus did in March of 2013, you could transfer a portion of your savings into bitcoin to protect it.
- Using the Bitcoin network you can exchange bitcoins with people you have never met while being absolutely sure that your bitcoins will end up with the rightful owner. And all that without the need for a bank to act as an intermediary.
- Remittances, payments usually sent by a family member living in another country back to family in the home country, can have large transaction costs. Bitcoin allows such payments with much lower fees.

Finally, keep in mind that Bitcoin is a new technology that may have many new applications in the future. Similar to the way that the Internet in the early 1990s was considered almost synonymous to email, Bitcoin today is considered, by most, synonymous to the Bitcoin payment network and

the bitcoin currency. But the same way that the Internet today is not just email but also the World Wide Web, Internet video and telephony, Bitcoin tomorrow will be more than it is today.

So prepare for the future by learning more about Bitcoin. You can start by learning the meaning of a few important terms that are included in the frequently asked questions below:

What is a Bitcoin Address?

A Bitcoin address is similar to the account numbers in a bank. You can send money bitcoins to any address, just like you can send cash to any bank account if you know its number, and you can only spend bitcoins from an address that you control. You control your Bitcoin address by a secret key, called the private key. Unlike an account in a bank though, you can easily have as many Bitcoin addresses as you wish.

What is a Bitcoin Wallet?

A Bitcoin wallet is a very general term meaning a piece of software running on the Web, a Mac or PC, IOS or Adroid, which enables transactions with the Bitcoin protocal. The software typically shows the balance of all bitcoins that exist related to the Bitcoin addresses it holds. Beyond that general statement, wallets vary widely. They may or may not provide you with your own private keys, for example.

What is Wallet security? You should protect your wallet with a strong password and make sure nobody else has access to it. This is very important and it has to be repeated: You should never give out the private key associated with a Bitcoin address! If you let someone else get hold of a private key, they will be allowed to spend your Bitcoins from your bitcoin address. It's a little scary to realize this, but once you do it's no big deal; just protect the keys by encrypting them, something that your wallet makes convenient.

What's the deal with cryptography and security?

You might read a lot of descriptions about Bitcoin that mention cryptography, hash functions, public and private keys and all sorts of very geeky sounding terms. For starters the only thing you really need to understand is that Bitcoin works and your bitcoins are secure because of complicated mathematics. This complicated mathematics allows you to conduct business and exchange money with people on the Internet who you don't know and who you don't necessarily trust. And that is a really cool thing!