



# Glossary

**Address:** a long number which you can send Bitcoins to and from. Can only have coins sent from it using the matching *key*. Together they make a key pair in *public key cryptography*.

**Anarcho-capitalism:** the ideology that a complete absence of government is essential, and property rights, which are paramount, will still function without it. Bitcoin ideology shares a lot of its ideas and jargon.

**ASIC:** Application-Specific Integrated Circuit – a silicon chip to do a single specific job. In *mining*, the only power-efficient way to mine bitcoins.

**Bitcoin:** The greatest invention in the history of humanity.

**Blockchain:** The other greatest invention in the history of humanity.

**BTC:** the usual abbreviation for Bitcoin as a currency unit. Less common abbreviation: *XBT*.

**Bubble:** in economics, when an asset is hugely popular for no discernible reason. The key factor is investors buying in the hope of selling to later investors. Bubbles always pop. Bitcoin has had two major bubbles, in 2013 and 2017.

**Cold wallet:** Bitcoin private keys kept offline. Could be *wallet* software on a computer that's not online, could be keys on a USB stick, could be printed out on paper.

**Consensus model:** How you choose who gets to write the next block. Bitcoin uses *Proof of Work*, which is hugely wasteful.

**Craig Wright:** Not *Satoshi Nakamoto*.

**Crypto:** in this context, an abbreviation for *cryptocurrency* or *crypto asset*. In non-cryptocurrency use, the term is short for “cryptography.”

**Crypto asset:** the general class of cryptographic things that aren't necessarily *cryptocurrency*, but can be traded like it, *e.g.* tokens in a smart contract running on Ethereum.

**Cryptocurrency:** Bitcoin and its various copies.

**Cypherpunks:** a mailing list for cryptography enthusiasts against the forces of oppression, *i.e.* any government anywhere. Heavy on the *anarcho-capitalism*. Most of the ideas that became Bitcoin started here.

**DAO:** see *The DAO*.