

Bitcoin for Beginners - Cheat Sheet - Dec 2017

Byron Yee - byronsyee@yahoo.com

Suggested reading:

Digital Gold by Nathaniel Popper Why? It will give you the history lesson of Bitcoin through 2014 and help you understand in non technical terms what bitcoin and the blockchain are about.

Suggested videos:

Anything with **Andreas Antonopolous** in YouTube. Why? He is the most ethical guy out there and is a true evangelist. He will explain Bitcoin in such a way that you can then describe it to your friends.

Terminology and Acronyms

KYC (Know Your Customer) and **AML** (Anti Money Laundering)

BIP - Bitcoin Improvement Proposal

BTC - Bitcoin in its most popular fork - (small block)

BCH - Bitcoin Cash - a fork of BTC - (big block)

ETH - Ethereum, the second most popular Alt Coin for the moment

LTC - Litecoin, third most popular Alt Coin, used to be second

HD Wallet - Hierarchical Deterministic Wallet - should be BIP 32 and BIP 39 compliant.

ICO - Initial Coin Offering - BUYER BEWARE - Like going to Vegas

Altcoins - Anything other than Bitcoin - BUYER BEWARE

2FA - Two Factor Authentication

HODL or **HODLers** - Inside Bitcoin joke from many years ago, it means someone that holds bitcoin for a long time.

FUD - Fear, Uncertainty, and Doubt

FOMO - Fear of Missing Out

Where can I buy Bitcoin?

Exchanges such as **Coinbase** (SF based, you also get **GDAX** account for trading), **Gemini** (Winklevoss Twins), **Bittrex** and many others. DO YOUR DUE DILIGENCE. Low to no transaction fee. Must comply with KYC/AML laws. Will take some time to setup and to jump through all the hoops. Lots of people are opening accounts so you have to be patient.

From someone local with cash - **LocalBitcoins** - reputation based.

From a **Bitcoin ATM**, usually in a smoke or vape shop - high transaction fees.

Where you buy will be a tradeoff between price/convenience/anonymity. Determine what's most important to you.

How do I store Bitcoin?

If you keep your bitcoin on an exchange, **YOU ARE NOT TRULY IN CONTROL OF YOUR BITCOIN**. Only keep enough money or bitcoin on an exchange if you are actively trading.

Transfer to a wallet - you will pay a transaction fee. Online, mobile or web wallets only if you are doing transactions (not likely)

Online/Mobile Wallet - Convenient, security risks. What happens if you lose your phone? Use secure passwords, always be careful of keylogging and malware.

Paper wallet (also known as cold storage) BUT you have to balance risk and security.

Hardware Wallet that is HD 32/39 compatible. Recommend **Ledger Nano S**, also **Trezor**, **Keepkey**, **Digital Bitbox**, others. The wallet will give you 24 words from a list of 2048 words. As long as this list of 24 words is not compromised, then you truly are in control of your bitcoin.

Before you buy bitcoin and put it on a hardware wallet, **YOU MUST THINK ABOUT SECURITY**. You must make decisions based upon your own tolerance of risk.

STEP 1: USE A PASSWORD MANAGER. LastPass seems to be popular. Norton Identity Safe is another. There are others. DO YOUR DUE DILIGENCE. And use a random password generator of at least 12 characters, uppercase, lowercase, a number, and a symbol

STEP 2: USE 2FA (TWO FACTOR AUTHENTICATION). Google Authenticator or Authy.

STEP 3: SETUP A PROTONMAIL.COM (OR .CH) ACCOUNT FOR EMAIL. Free encrypted email that is OUTSIDE of government snooping - for now.

NEVER, EVER, EVER, EVER, (WHEN? NEVER) STORE YOUR BITCOIN HD WALLET SEED DIGITALLY OR AT THE VERY LEAST UNENCRYPTED.

Assume that you are hacked and have been keylogged at any time.

Initially write down your seed but ask yourself the following questions:

WHAT HAPPENS IF I WRITE DOWN MY SEED AND LOSE THE PAPER. WHAT IF THERE IS AN EARTHQUAKE/FIRE/ETC?

WHAT IF I GET HIT BY A BUS? HOW DO I TRANSFER MY BTC TO SOMEONE THAT I WANT TO HAVE IT.

EVEN IF YOU TRUST SOMEONE ELSE, THEY CAN BE COMPROMISED.

There are ways to do this electronically, a concept called "Security by Obscurity" but I will only explain verbally.

Remember the first rule of **Fight Club**? That applies to your own bitcoin security.