

The Future of Bitcoin and Cryptocurrencies in 2018



The Future of Bitcoin and Cryptocurrencies in 2018

1. **Bitcoin and Cryptocurrency in 2017 - Year in Review**
Xmas flash crash, SegWit, SegWit2X, Bitcoin Cash, Bitcoin Gold, and more
2. **Bitcoin and Cryptocurrency lessons learned in 2017**
Crypto trends, moving averages, dormant coins, HODL, etc.
3. **Bitcoin in 2018**
Technical Chart Analysis, Deluge of Bitcoin forks (FCO - Forked Coin Offering)
4. **Other Cryptocurrencies (aka Altcoins)**
Ethereum, Litecoin, IOTA, Ripple and ICOs
5. **BONUS: My Dog Ate All my Bitcoins! Now, what do I do?**
(aka How to keep your Bitcoins and Cryptocurrencies safe)

Bitcoin and Cryptocurrency in 2017

Year in Review

BACKDROP: Civil war and infighting between **Bitcoin Core** (bitcoin.org and reddit.com/r/Bitcoin) and **Bitcoin ABC** (bitcoinabc.org and reddit.com/r/btc) had a detrimental effect on Bitcoin for years. 2017 was the year that it would stop, well almost. The NYA (the New York Agreement) was signed by developers and miners and Bitcoin Improvement Proposals (BIP) were agreed upon and set in motion the future of Bitcoin, e.g. SegWit and SegWit2X. But as Luke said,

"This is not going to go the way you think."

- **(Jul 16) Bitcoin crashed from around \$3,000 to \$1,758 (-40%)**
the last time Bitcoin was under \$2,000
- **(Jul 20) Bitcoin Improvement Proposal 91 (BIP 91) locked-in, paving the way for BIP148 UASF and Segregated Witness (SegWit) activation**
Bitcoin \$2,725: In the air there was still the threat of a split Bitcoin, e.g. Bitcoin Legacy and Bitcoin SegWit
- **(Aug 1) BIP148 SegWit activation and the birth of Bitcoin Cash (BCH)**
Bitcoin \$2,750: Finally a solution to the infighting between Bitcoin Core and Bitcoin ABC "big blockers", BUT there was still SegWit2X
- **(Aug 23) SegWit Lock-in and Enforced at block 481,824**
Bitcoin \$4,142: SegWit was required for miners to receive mining rewards
- **(Sep 4) People's Bank of China bans ICO**
Bitcoin \$4,420: Bitcoin price does not react
- **(Oct 24) Bitcoin Gold fork**
Bitcoin \$5,525: a GPU friendly Bitcoin. Weak development team, a bounty was offered to developers to implement replay protection
- **(Nov 1) The last cryptocurrency exchange in China shuts down**
Bitcoin \$6,590: Bitcoin price does not react

Bitcoin and Cryptocurrency in 2017

Year in Review

- **(Nov 8) Contentious SegWit2X fork cancelled (orig scheduled for Nov 16)**

Bitcoin \$7,435: Between Aug 1 and Nov 8th there was strong group of NYA signers against the SegWit2X hard fork since Bitcoin Cash already filled that role and because a contentious hard fork of Bitcoin would have create TWO Bitcoins with no agreement as to which one is the "real" Bitcoin.

- **(Nov 10) Wall Street support: CME and CBOE have issued Bitcoin futures**

Bitcoin \$6,577

- **(Nov 12) Bitcoin Cash Mempool attack and difficulty adjustment**

Bitcoin \$6,434 to \$5,400, Bitcoin Cash \$890 to \$2800

- **(Nov 28) CryptoKitties: The World's First Ethereum Game Launches**

Multi-day transaction delays on the Ethereum network

- **(Nov 28) Bitcoin \$10,000 ("to the moon")**

Bitcoin \$10K arrives early



To the Moon!

(to many HODLs, "the Moon" was Bitcoin \$10,000)

Bitcoin and Cryptocurrency in 2017

Year in Review

- **(Dec 16) Bitcoin rocketed past \$10,000 to \$19,900**
Bitcoin \$19,900: Bitcoin almost double in less than 3 weeks!
- **(Dec 19 - 20) 2017 Xmas flash crash - Bitcoin plunge from \$19,900 to \$10,400 (52%)**
Bitcoin \$10,400
 - Youbit South Korean exchange hack and bankruptcy
 - Coinbase Bitcoin Cash (BCH) support
 - Coinbase Bitcoin Cash (BCH) insider trading scandal
 - Charlie Lee sells all his Litecoins to avoid possible conflict of interest
- **(Dec 31) Bitcoin ends the year above estimates of Bitcoin \$10k at \$13,500**
Bitcoin \$13,500

Bitcoin and Cryptocurrency Lessons Learned in 2017

- **Do NOT sell non-performing currencies**

There is a strong trend in cryptocurrencies to be dormant for a long periods before a major breakout, e.g. Litecoin, IOTA, NEO, Ripple, etc. Remember the original reason you bought the currencies.

- **Moving-average lines crossing indicates a change in trend**

Use cryptowat.ch charts instead of GDAX charts (default moving average line seems to be better on cryptowat.ch)

- **Most cryptocurrency charts axis are linear (to give the appearance of bigger price movement at higher prices)**

*For more accurate view of percentage gain, set the chart axis to **logarithmic**, if there is an option (cryptowat.ch)*

- **Ripple (XRP)**

Just because a cryptocurrency was used only for spam protection, does not mean it could not be repurposed to increase liquidity and increase 10x! Especially if the company/cryptocurrency is supported by the banks.

- **Tron (TRX) missed a good trade**

Just because cryptocurrencies are banned in China should not stop a cryptocurrency from China from succeeding.

- **Verge (XVG) missed pump and dump**

Just because John McAfee says it is good, does not make it good.

Bitcoin in 2018

Technical Chart Analysis of Bitcoin on cryptowat.ch

- *Moving Averages*
- *Technical Analysis patterns: Symmetrical Triangle*
- *Volume*
- *MACD crossover*

Bitcoin(s) in 2018

- **Bitcoin (BTC) \$15,000** - Proof of Work - ASIC mining - difficulty adjustment every 2 week - max supply 21m
- **BITCOIN FORKS** (“Airdrop” free coins for Bitcoin holders)
 - Aug 1: **Bitcoin Cash (BCH) \$2,888** - 8meg blocks - Emergency Difficulty Adjustment (bitcoincash.org)
 - Oct 24: **Bitcoin Gold (BTG) \$245** - GPU friendly - difficulty adjustment every block (bitcoingold.org)
 - Nov 24: **Bitcoin Diamond (BCD) \$25** - hybrid Proof of Stake / Proof of Work - GPU friendly - max supply 210m (btcd.io)
 - Dec 12: **Super Bitcoin (SBTC) \$190** - Smart Contracts - Lightning - Zero-knowledge - 8meg blocks (supersmartbitcoin.com)
 - Dec 24: **Bitcoin Platinum - SCAM**
 - Dec 31: **Bitcoin Uranium** - defunct, website redirects to mvp.sonm.io
 - Jan 2: **Bitcoin Cash Plus \$???** - Emergency Difficulty Adjustment - Bigger blocks (bitcoincashplus.org)
 - **Bitcoin Silver (BTCS) \$0.0049** (NOT a Bitcoin fork coin) - tokenized Bitcoin on Ethereum - direct FIAT to Token (bitcoinsilver.io)
 - **Bitcoin Plus (XBC) \$134** (NOT a Bitcoin fork coin) - Proof of Stake - ICO in 2014
- **IMPORTANT:** DO NOT DELETE your old Bitcoin wallets, if you intend to claim your Bitcoin forked coins. Specifically, if you own Bitcoin on the date a coin is forked, you will need your wallet (empty or not) to claim your coins. **Best practice is to move all your funds to another wallet, and THEN import your empty wallet into the forked coin’s wallet, e.g. Bitcoin Cash Electron.**

Other cryptocurrencies (aka Altcoins)

- **Bitcoin Cash (BCH)** - Bitcoin's "black sheep" of the family
- **Ethereum (ETH)** and **Ethereum Classic (ETC)** - programmable Bitcoin and the thieves programmable Bitcoin
- **Litecoin (LTC)** - the better Bitcoin (faster, lower fee, non-dead creator, etc.)
- **Monero (XMR)** - the DarkWeb and Mariah Carey's preferred cryptocurrency
- **IOTA** - an experiment
- **NEO** (and **QTUM**) - Ethereum of China
- **Ripple (XRP)** - bank-supported cryptocurrency, supported by AMEX
- **Cardano (ADA)** - Ethereum of Japan?
- **Lumen Stellar (XLM)** - a 2014 fork of Ripple, but now a very different coin supported by IBM
- **Dash** - the coin formerly known as Darkcoin
- **NEM** - wat tat?

Recent ICOs

- **My Pre-ICO experience**

- **Upfiring (UFR) - P2P file sharing token to reward file seeders**

- (origin max supply: 1,000m, burned 97%, current supply: 24m (14m float, 5m marketing, 5 developers)

- Pre-ICO 15,000 UFR = 1 ETH (\$300)*

- Day of ICO (~\$4200)*

- Week after ICO (~\$400)*

- Today (~\$5,000)**

- NOTE: Catalyst for price rise, listed on cryptopia.co.nz*

- **Enjin (ENJ) - Cross-game gaming token**

- Pre-ICO 6,000 ENJ = 1 ETH (\$300)*

- Day of ICO (~\$300)*

- Week after ICO (~\$300)*

- Today (~\$2,000)**

- **Tron (TRX) - a decentralized content sharing platform leveraging blockchain and peer-to-peer (p2p) network technology**

- Imagine a P2P YouTube with content providers reward by crypto. Created by Justin Sun is the CEO of TRON. In particular, he has been hailed as the next Jack Ma (Forbes, 2017). Justin was a former China representative for Ripple. Investors include Jihan Wu (CEO of BITMAIN)*

- **Verge (XVG)**

- A more private privacy coin, claiming to be more private than current privacy coins. Tweeted by **John McAfee** before he wisely discontinued his "Coin of the Day" tweets*

Conclusion

- 2017
 - The civil war in Bitcoin “ended” with Bitcoin supporting SegWit and the birth of Bitcoin Cash
 - The Eagle has landed, Bitcoin has reached \$10K (the Moon). Next stop Mars!
 - 2017 ended with a big shake-up in Altcoins. The kings are dead, long live the kings!
 - Bitcoin Cash failed to topple Bitcoin, but got listed on Coinbase
 - Ethereum survived 10X, only to fall to CryptoKitties
 - Litecoin’s creator Charlie Lee sold all his Litecoin to avoid conflict of interest (or may be because of a secret deal)
 - IOTA, the experiment has 10x!
 - Ripple, the bank’s spam prevention cryptocurrency has grown up and 10X!
- 2018
 - Next stop Mars! Bitcoin \$30,000 by March 1
 - After the 2017 shake-up in Altcoins, the top market cap is up in the air!
Even Bitcoin’s dominance could be threaten

BONUS: My Dog Ate All my Bitcoins!

Now, what do I do?

(aka *How to keep your Bitcoins and Cryptocurrencies safe*)

There are no Bitcoins in your Bitcoin wallet

Your Bitcoins exist on the internet on a distributed ledger, the **Bitcoin blockchain**. Your wallet *ONLY* contains the private keys to the Bitcoin addresses (that multiple addresses) that allow you to spend your Bitcoins. **Amazing Crypto-Fact:** a 24 word recovery seed is all that is needed to reconstruct all the Bitcoin addresses and private keys contained in your wallet.

- **Do NOT store your Bitcoins or altcoins for any extended period on exchanges. Transfer your coins into your private wallet as soon as convenient. Only transfer your coins to an exchange when you want to make a trade.**
Store your coins on your own personal wallet, e.g. hardware wallet, desktop wallet, mobile wallet (not recommended for large sums)
REMEMBER: Your wallet, your private keys, your money. Their wallet, their private keys, their money. (BONUS: they also get your forked coins)
- **Check and double-check** the receiving **Bitcoin address**
Recommendation: cut and paste address into a document to record the date and amount of the transaction in case anything goes wrong.
- **Check and double-check** that you are **downloading wallet software from the official website**. Many wallets are hosted at GitHub or the official website. And beware of the **Cryptoshuffler malware**.

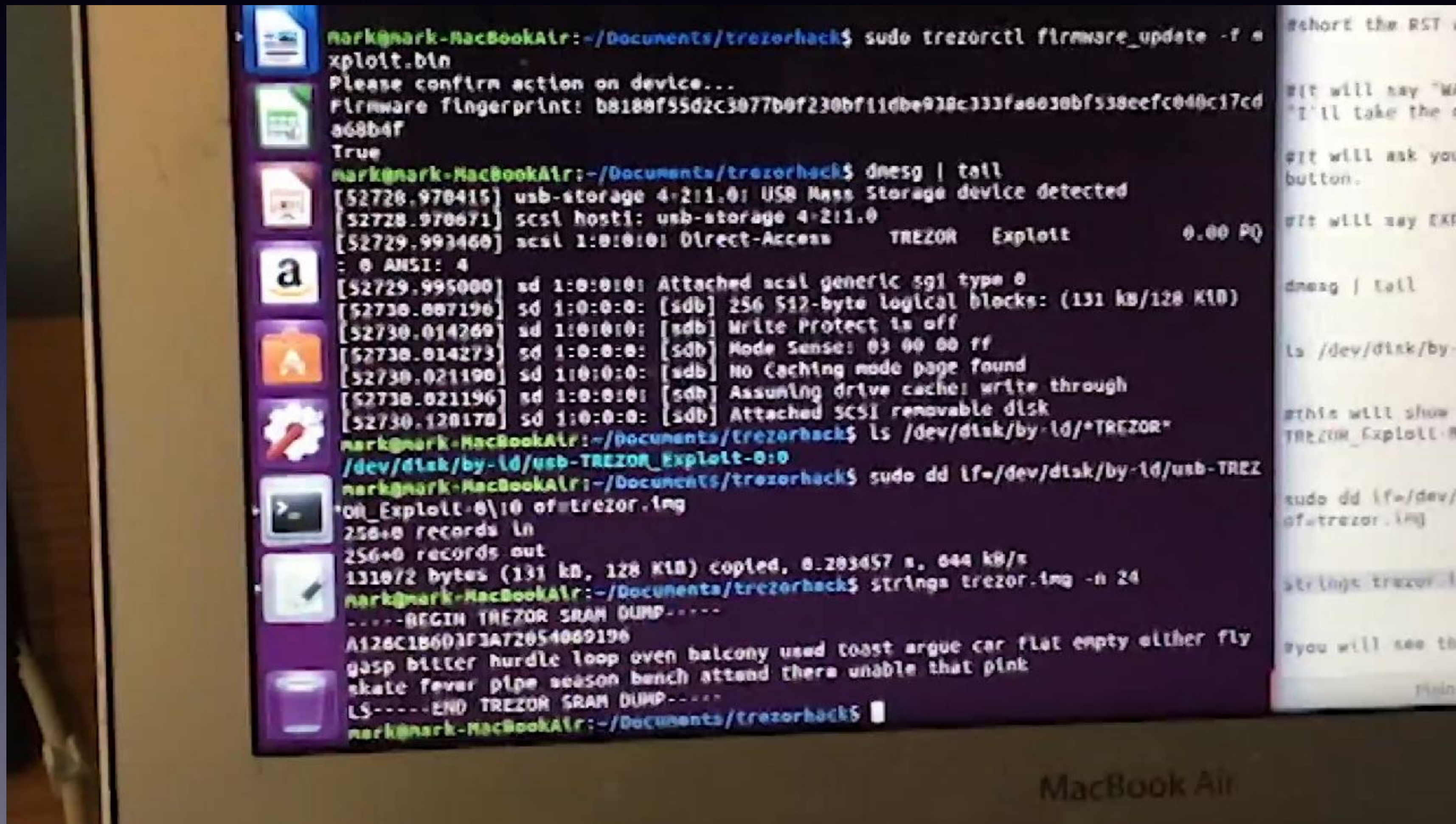
BONUS: My Dog Ate All my Bitcoins!

Now, what do I do?

(aka How to keep your Bitcoins and Cryptocurrencies safe)

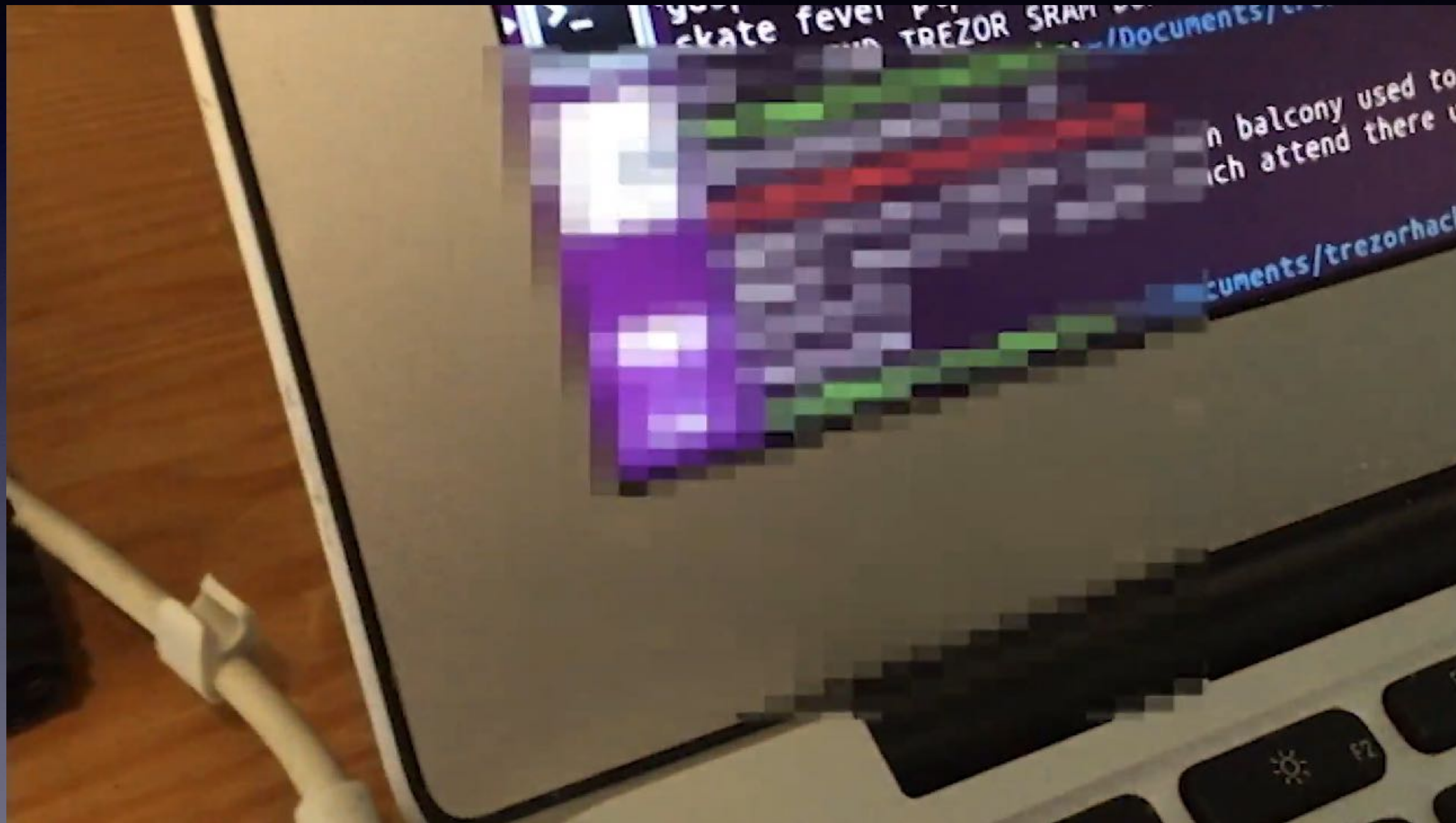
- **Use a hardware wallet (Trezor \$149/\$80, Ledger Nano S \$113/\$65)**
Advantage: your valuable private keys are never on your computer, supports multiple coins and multiple wallets
- **Trezor** supports: Bitcoin (Classic/SegWit), Litecoin, DASH, Zcash, Dogecoin, Ethers/Ethereum Classic and ERC20 Tokens via MyEtherWallet.com and recently added, Bitcoin Gold, Digibyte, Monacoin, and NEM)
- **Ledger Nano S** supports: Bitcoin, Bitcoin Cash, Bitcoin Gold, Litecoin, Ethereum/ Ethereum Classic, Dash, Zcash, Neo, Qtum, Ripple, Stellar, Vertcoin, Dogecoin, Komodo, Pivx, Ark, Expanse, Digibyte, Hcash, PoSW, Viacoin, Stealthcoin, Stratis, Ubiq
- **Protect** your wallet's **Seed/Recovery Words**, never ever disclose it
Anyone with your Seed/Recovery Words will have full access to all the funds in all the addresses in your wallet.
- **Backup** multiple copies wallet's **Seed/Recovery Words**
*Onsite backup, off-site backup (encrypted), Do **not** store your private keys on a USB thumb drive that you use daily outside your residence, since they can be easily lost, stolen or misplaced*

Protect your wallet's **Seed/Recovery Words**, never ever disclose it (especially, do **not** post a video of it on the internet and especially if you are Mark Frauenfelder, **Director of Blockchain Technology**)



source: 'I Forgot My Pin': An Epic Tale Of Losing \$30,000 In Bitcoin @ Wired

Protect your wallet's **Seed/Recovery Words**, never ever disclose it
(blurred out Trezor PIN number, with Recovery Seed Words clearly visible)



source: 'I Forgot My Pin': An Epic Tale Of Losing \$30,000 In Bitcoin @ Wired

Mark's 24 Word BIP39 Recovery Seed

gasp bitter hurdle loop oven balcony
used toast argue car flat empty
either fly skate fever pipe season
bench attend there unable that pink

BONUS: My Dog Ate All my Bitcoins!

Now, what do I do?

(aka *How to keep your Bitcoins and Cryptocurrencies safe*)

- **Do NOT store your coins on cryptocurrency exchanges** (store your coins on your own personal wallet)
 - Mt. Gox - 850,000 bitcoins missing and likely stolen, since then 200,000 bitcoins have since been "found". It turns out that Bitcoins were being stolen from Mt. Gox's Bitcoin hot wallet undetected for years.
 - BTC-e.com - seized by the US Government and the CEO indicted for money laundering
 - Youbit - a South Korean crypto-exchange filed for bankruptcy after it was hacked and lost 17% of their funds (Dec 20)
- Fake Altcoin Wallets and **Fake Forked coin wallets** may steal coins from your other wallets
I have not seen this IRL, but Bitcoin Gold hosted a FAKE wallet on their official website before they took it down.
- Claiming Forked coins that do **not** have **transaction replay protection** implemented
e.g. if you claimed **Bitcoin Gold** before transaction replay protection was implemented, a bad actor could replay a **Bitcoin Gold (BTG)** transaction on the **Bitcoin (BTC)** network (by definition forked coin copies the original parent's blockchain) and get your Bitcoins also! *This is why you should MOVE ALL YOUR COINS TO ANOTHER WALLET before collecting forked coins*
- **Cryptoshuffler malware**
Bitcoin addresses are long and hard to remember, just about everyone cut and paste the address when they want to transfer their Bitcoins. The Cryptoshuffler malware is ingeniously simple. It changes the sending address on clipboard to the Bitcoin address of the thief.

Since the Bitcoin blockchain is public, you can monitor how many Bitcoins has been stolen by Cryptoshuffler. So far about 23 Bitcoins or \$345,000 to date.

<https://blockchain.info/address/1v9UCfygQf3toN1vA5xvr7LhKmv9QWcwZ>

BONUS: My Dog Ate All my Bitcoins!

Now, what do I do?

(aka How to keep your Bitcoins and Cryptocurrencies safe)

Other ways you can lose your money in cryptocurrencies:

- **Bitcoin.org** is the official Bitcoin website, **NOT** Bitcoin.com
- Beware of **CoinHive** Javascript-based web mining malware
- Beware of **BitConnect** ponzi scheme
- Beware of 95% of ICO (Initial Coin Offering) will fail
- Beware of Altcoin Pump and Dumps
- Beware of scam / phishing site and emails
- I Wrote Down a Wallet Recovery Seed Word Incorrectly. What Can I Do?
Most wallets will allow display the Recovery Seed Word after entering the wallet password

Thank You

Thank you for coming and/or joining on Facebook Live!

If you want to be part of the **Bitcoin 101 Google Hangout group**, signup at the front or email me.

Please clean up after yourself and
throw away any trash into the trash bin

Slides will be available online at www.YBU.com
email: mike@ybu.com