Bitcoin

Abrahim Ladha

March 8, 2016

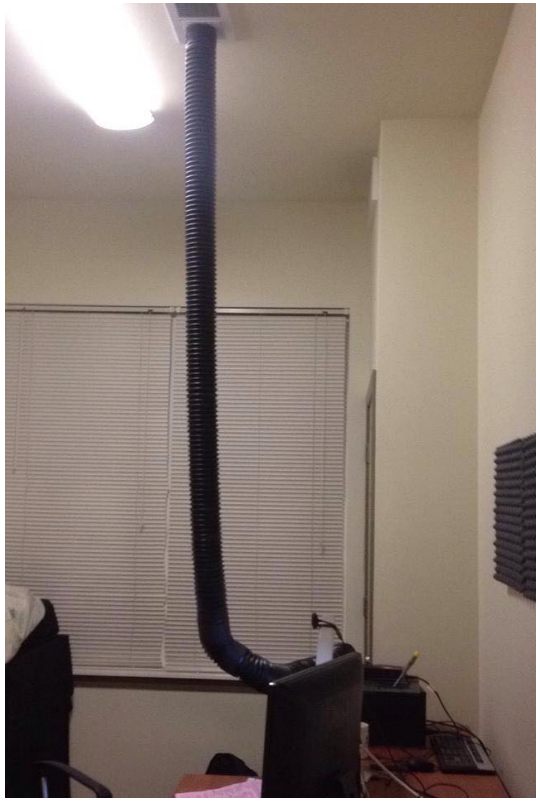
What is bitcoin?

Bitcoin is a cryptographically secured decentralized currency system.
Transactions are sent user to user without a central authority verification. Transactions between users involve units of BTC and are verified on the blockchain, which is a list of all transactions ever made by all users.
a transaction cannot be undone with out first undoing every transaction that comes after it on the blockchain.

How are coins generated and distributed?

Mining. A miner does "work" on a block of bitcoins, which is basically just bruteforcing a long SHA256 password.
Once guessed correctly the miner receives those coins.
In practice users form "pools" and work together to solve a block.
Every so often a "halvening" occurs and the block reward is halved.
There can only ever exist 21 Million BTC.


MOTHERBOARD



security?

p = probability honest node finds the next block
q = probability attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & p \leq q \\ (q/p)^z & p > q \end{cases}$$

Let $\lambda = z\frac{q}{p}$. Probability attack could catch up now is Poisson density for each amount of progress times the probability of catching up from that point: $\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \times \begin{cases} (\frac{q}{p})^{(z-k)} & k \leq z \\ 1 & k > z \end{cases}$

Security continued

Simplifying to $1 - \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!}(1 - (\frac{q}{p})^{(z-k)})$

The probability drops off exponentially with z:

q=0.3

z=0 P=1.0000000

z=5 P=0.1773523

z=10 P=0.0416605

z=15 P=0.0101008

z=20 P=0.0024804

z=25 P=0.0006132

z=30 P=0.0001522

z=35 P=0.0000379

z=40 P=0.0000095

z=45 P=0.0000024

z=50 P=0.0000006

However, if $q \geq 0.5$, an attacker has enough power to undo the blockchain. but what are the odds 51% of users are mailcious?

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf