

Forum:[Hack Forums](#)

Thread: [Bitcoin - Decentralized P2P Currency](#)

NathanKBarrows - December 22, 2010, 9:21 am

[Bitcoin](#) <-link

Bitcoin is a peer-to-peer digital currency. Peer-to-peer (P2P) means that there is no central authority to issue new money or keep track of transactions.

Instead, these tasks are managed collectively by the nodes of the network.

How does Bitcoin work?

Bitcoin utilizes public/private key digital signatures (ECDSA). A coin has its owner's public key on it. When a coin is transferred from user A to user B, A adds B's public key to the coin and signs it with his own private key. Now B owns the coin and can transfer it further. To prevent A from transferring the already used coin to another user C, a public list of all the previous transactions is collectively maintained by the network of Bitcoin nodes, and before each transaction the coin's unusedness will be checked.

Where does the value of Bitcoin stem from? What backs up Bitcoin?

Bitcoins have value if they are accepted as payment by many.

When we say that a currency is backed up by gold, we mean that there's a promise in place that you can exchange the currency for gold. In a sense, you could say that Bitcoin is "backed up" by the price tags of merchants – a price tag is a promise to exchange goods for a specified amount of currency.

It's a common misconception that Bitcoins gain their value from the cost of electricity required to generate them. Cost doesn't equal value – hiring 1,000 men to shovel a big hole in the ground may be costly, but not valuable. Also, even though scarcity is a critical requirement for a useful currency, it alone doesn't make anything valuable. For example, your fingerprints are scarce, but that doesn't mean they have any exchange value.

How are new Bitcoins created?

New coins are generated by a network node each time it finds the solution to a certain calculational problem (i.e. creates a new block), for which an average solution time can be calculated. The difficulty of the problem is adjusted so that in the first 4 years of the Bitcoin network, 10,500,000 coins will be created. The amount is halved each 4 years, so it will be 5,250,000 in years 4-8, 2,625,000 in years 8-12 and so on. Thus the total number of coins will approach 21,000,000 over time.

What is a "block"?

A block is a unit which contains the information of the transactions made after the previous block, plus a transaction which assigns a new coin to the creator of the block. Blocks form a chain from the first block to the latest block. To create a new block you need to spend CPU time, which acts as an unbribable timestamp for the previous transactions. The average rate of block creation in the whole

system is 6 / hour.

The block chain length is shown in the status bar of the Bitcoin main window. The number increases rapidly while your Bitcoin client is downloading the block chain from other nodes. After the downloading is finished, your node can start generating new blocks.

So your wealth is determined by the amount of CPU power you have?

No. There's a constant average rate of new Bitcoins created, and that amount is divided among the nodes by the CPU power they supply. The competition for coin creation will drive the price of electricity needed for generating a coin close to the value of the coin, so the profit margin won't be that huge. The easier way to gain a lot of wealth would be trading goods.

At the moment, though, you can generate new coins quite profitably, if you expect them to have real value in the future. If you choose to, be aware that Bitcoin is still experimental software.

Are my Bitcoins safe?

As long as you make backups of your Bitcoin wallet, protect it with a strong password and keep keyloggers away from your computer. You need to make a backup of your wallet after each transaction, as the old wallet backup will be partially or completely invalid.

If you lose your wallet or if some unknown attacker gets it and manages to break your password, there's no way to get your coins back. On the other hand, that is usually also the case if you lose your physical wallet.

WI3-FM?(What is in it for me)

Untrackable! Generate a new address for each transaction.

Unstoppable! The power of the peers.

Unregulated! There is not even an agreement.

Disclaimer: I posted this since it is a great opportunity for all hackers worldwide. You may donate for my info anytime @

12En1W4DUMUTtrqBFU9zAfgQPSC5RAjRdK if you find it useful. I considered this was the best forum to post it in, if it wasn't feel free to move it. I

invite everyone to try it. There is a lot to win. If you consider this isn't secure enough, I invite you to attempt to exploit it; it is open-source.

You may exchange Bitcoins for other currencies @ [Bitcoin Exchange](#)

[BitcoinFX](#)

[Bitcoin Market](#)

[Bitcoin4Cash](#)

[Bitcoin2Cash](#)

[BitLex](#)

[Mt Gox](#)

[BTCex](#)

[#bitcoin-otc](#)

[Nanaimo-gold](#)

[Bitcoin2CC](#)

[Bitcoin Gateway](#)

[Bitcoin Morpheus](#)

[EuroBTC](#)

Did I mention there are practically no fees? Have a nice day, will ya??

Please at least offer the option to pay with Bitcoins, even if it is overpriced vs the USDs.

EDIT: Hey, I forgot to mention I want to hear your experiences with Bitcoin.
Was it easy to use? Do you offer a product with Bitcoins as payment option?

Are you going to use it now on as payment option? Why or why not?

Vendetta_ - July 9, 2011, 6:06 am

That is a very nice guide. Cleared some stuff up and it was nicely explained.

Krawk - July 9, 2011, 7:11 am

Nice guide! Im getting into bitcoin mining now and putting my investment in, hopefully its worth it.
looking for some people who had experience with mining opinons

Henry Chinaski - May 3, 2024, 11:53 pm

this is the oldest post on bitcoin in this forum and its pretty impressive.....I wonder what happened to NathankBarrows

Henry Chinaski - May 4, 2024, 2:07 am

(May 4, 2024 01:52 AM)Antonio Wrote: [\[CITE\]](#) It is an extremely interesting post, thank you for the bump

Can't believe it, people thought it was overpriced even back in 2011
Its absolutely insane to think that the USD was stronger then but its all different now

Eran - May 4, 2024, 4:40 am

(May 3, 2024 11:53 PM)Henry Chinaski Wrote: [\[CITE\]](#) this is the oldest post on bitcoin in this forum and its pretty impressive.....I wonder what happened to NathankBarrows
Oh boy, actually a very useful gravedigging bump. Nice.