CSU Bakersfield REVS UP Research Experience Vitalizing Science University Program

bitcoin [1]

And The SHA-256 Hashing Function

Taylor Redden, Chelsea Dalton, Jordan Lacava, Remy Verduzco, Austin Burgeis

Advisor: Dr. Charles Lam Assistant: Frank Madrid

CSU Bakersfield Research Experience Vitalizing Science — University Program

Chevron

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

What is Bitcoin?

Bitcoin is a form of cryptocurrency created in 2009 by an unknown person who went by the alias Satoshi Nakamoto. It is basically internet money, but instead of being controlled by an organization like Paypal, Bitcoin does not have any middlemen.[9]

Obtaining a Bitcoin

Bitcoins may be obtained by buying, exchanging, selling, or earn them through mining. Mining is the process that allows for Bitcoins to be brought into the market, where they may then be sold. They can be purchased through Bitcoin ATMs or from other sellers. [11]

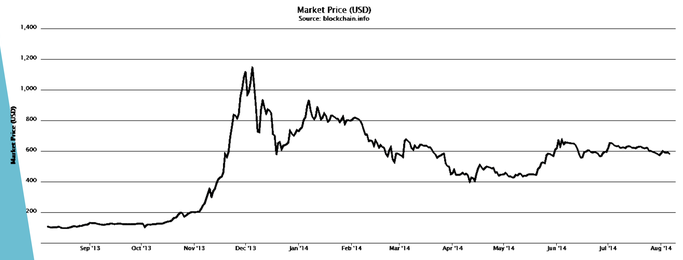
Bitcoin Benefits

- Mobile payments made easy
- Security and control over your money
- Works everywhere, anytime
- Fast international payments
- Zero or low fees
- Protect your identity [7]

Bitcoin Drawbacks

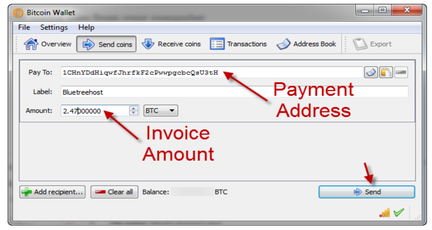
- Securing your wallet
- Bitcoin price is volatile
- Bitcoin payments are irreversible
- Bitcoin is anonymous
- Instant transactions are less secure
- Bitcoin is still experimental
- Government taxes and regulations [8]

Worth



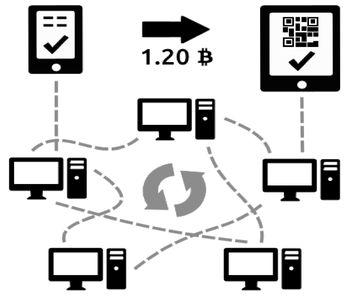
In the beginning, Bitcoin was only worth a few cents, but since then, it has peaked at $1,100 and currently sits at about $580. [6]

Transactions



Bitcoin Wallet [5]

When you make a transaction, the data is sent to every node in the network where it updates the transaction tree, which basically verifies that you have enough Bitcoins to spend. Everyone can see everyone else's account balance and transactions, so there is no discrepancy with exchanges.



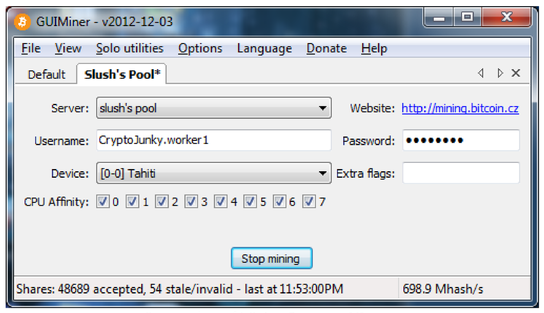
Example of a Bitcoin Transaction [2]

These transactions are then ordered in the block chain. Each of the blocks contain information on the inputs and outputs of a transaction and also the name of the previous block in order to link all the blocks. The blocks of the block chain are created through a process called mining.

Mining

Mining is used to expand the block chain as well as bring new Bitcoins to the market. When a user creates a new block, they receive a mining reward as well as any transaction fees. Anyone on the network can propose a new block, but it must meet special conditions. The SHA-256 hashing function is used to meet these conditions.

For better results, experienced miners invest in higher computing power found in more cutting-edge technology. But even with the most high tech gear, the competition is too stiff for any one person to profit from, so people join mining pools. [10]



Screen shot of Mining Program [4]

Into the SHA-256 Function

Bitcoin transactions are secured by SHA-256. This security system is used to encrypt transactions, addresses, wallets, etc, which allow the main user to be the only one that can read the information. SHA stands for "Secure Hash Algorithm" and the 256-bit model was created by the NSA to protect their information. [12]

When you run the hashing function it will return a 64 character string. The hash for the word 'hello' is:

2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

Changing a single character in the original string will yield a completely different string. The hash for the word 'jello' is:

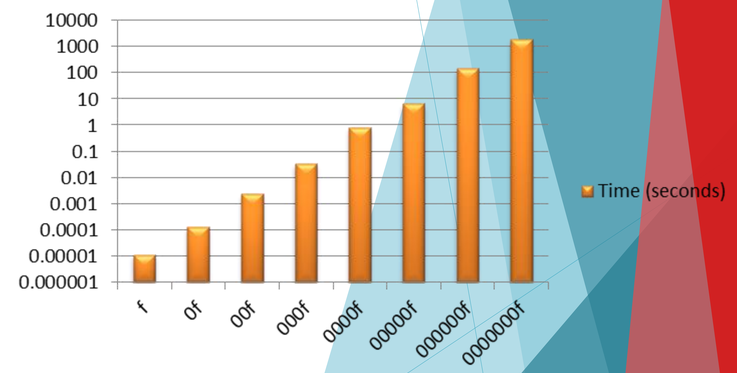
187c9bceeb919e1b3e6d20fa50ecabf7d9d50b5343e8f9a3d912abb13929102e

To solve a block, the hash output needs to start with a certain number of zeros. The hash of the number '2036798186' is:

00000d624810aaeb4aa6edf3e91290c25419391631e380a14461e8cc204d86

To find this hash we pick random numbers until the hash is correct. Below shows the time it took to find a hash beginning with the specified number of zeros.

Time to Find Hash



Using the data we were able to create the formula: time = $10^{1.1866x - 6.164}$ (where x is the number of zeros). This can be used to find the time that it may take a computer to solve different hash functions. Using this formula , we predict that at 7 zeros, it takes about 33 minutes to find an appropriate answer. The current mining difficulty has 16 zeros. Based on this formula it would take our system about 210,000 years to find an answer.

[1] http://logonoid.com/images/bitcoin-logo.png
[2] https://bitcoin.org/en/how-it-works
[3] http://earn-bitcoins.com/downloads.html
[4] http://cryptojunky.com/blog/wp-content/uploads/2013/03/BitcoinMining.png
[5] https://www.bluetreehost.com/media/bitcoin-send-payment.png
[6] https://blockchain.info/charts/market-price?timespan=1year&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=
[7] https://bitcoin.org/en/bitcoin-for-individuals
[8] https://bitcoin.org/en/you-need-to-know
[9] https://bitcoin.org/en/faq
[10] https://www.youtube.com/watch?v=j7opJ5-32hw
[11] https://bitcoin.org/bitcoin.pdf
[12] http://thehackernews.com/2013/09/NSA-backdoor-bitcoin-encryption-sha256-snowden.html