Bitcoin 101

How to get started with the new trend in virtual currencies.

WHITE PAPER

"The timing of Bitcoin's appearance, and subsequent growth, is no accident...If one follows the relevant sentiments and trends, it's evident that society was approaching a breaking point."

Jon Matonis,
Bitcon Foundation
Board Member

What are Bitcoins (BTC)?

Although people use different mediums of digital currency through video games, Moneypak, and mobile web apps, an entirely standalone currency is revolutionizing the way we perceive money. Bitcoin is the first decentralized digital currency, and it's pushing the envelope toward a new virtual economy.

Bitcoin, a peer-to-peer online virtual currency, is leading the trend of digital currencies around the world. It is decentralized, meaning there is no central bank or hub where Bitcoins are created and it's purely digital, meaning a physical representation of the currency is not needed.

Bitcoin is designed around the idea of using cryptography to control the creation and transfer of money rather than relying on a central authority. This concept inspired its creator, only known as Satoshi Nakamoto, who created a formula that creates Bitcoins using a computer's processing power.

How does Bitcoin work?

The crux of Bitcoin is based on its block chain, or a large set of data that represents every Bitcoin transaction. All purchases are recorded in the block chain, confirming an owner's possession of Bitcoins. When you download a Bitcoin wallet, you are downloading the block chain, so every user has a copy of the entire network.

Once you've downloaded a Bitcoin wallet, the program generates an address by which you will receive Bitcoins. You're then officially ready to begin scouring the web for Bitcoins and products that can be purchased with them.

It sounds more technical in theory, but the process is easy. You simply download the wallet program and use it to purchase or receive Bitcoins.

How exactly are Bitcoins used anonymously?

Bitcoin is a crypto-currency, meaning it uses public-key cryptography. It uses cryptography to enforce the integrity of Bitcoin so malicious users can't manipulate the data. When you receive an address to receive or send Bitcoins, you're receiving a randomized hash.

You can create multiple addresses so you can choose which individuals receive which address. This is one key to Bitcoin's anonymity; since there is no single, unique address per user, you can't decipher between individuals, even if you have knowledge of the transaction history.

Since you only need to download a program to start using Bitcoins, there is no personally identifiable information (PII) attached. Bitcoin wallets are not tied to

bank accounts or any sort of identifiable information. This means that transactions can happen between users or entities without any knowledge of the transacting parties.

This does not mean that everyone who uses Bitcoin wishes to remain anonymous. Many Bitcoin users take pride in their investment and openly use their Bitcoins around the world.

"One of the traditional strengths of Bitcoin, the peer-to-peer crypto-currency, has been its decentralization. Because no one is in charge of the network, users place their trust in the security of the Bitcoin protocol rather than in any specific institution."

Timothy B Lee,
Tech Policy Reporter,
Ars Technica

How successful is Bitcoin?

The value of this digital currency depends solely on its perceived success with its users, and so far Bitcoin's solid user base believes it holds the potential to be the universal digital currency standard.

MtGox.com, the longest running Bitcoin exchange website, estimates that one Bitcoin is worth nearly $150USD as of April 2013.

In December 2012, French bank Aqoba began accepting Bitcoin accounts, backing the digital currency.

In February 2013, MegaUpload founder Kim Dotcom publically announced his affinity for Bitcoin and provided Bitcoin payment methods for his new MegaUpload site. The digital entrepreneur also expressed interest in creating a Bitcoin credit card.

Bitcoin has surged since then, jumping to more than 200 USD in April.

Many other websites are opening up to Bitcoin, either by soliciting donations or allowing purchased through the currency. The website Bitspend.net, for example, allows any user to purchase items using Bitcoins from more popular sites like eBay or amazon.com, something the two websites do not permit.

Bitcoin has become so successful, the Financial Crime Enforcement Network (FinCEN) has issued new guidelines for Bitcoin's legal status in the U.S.

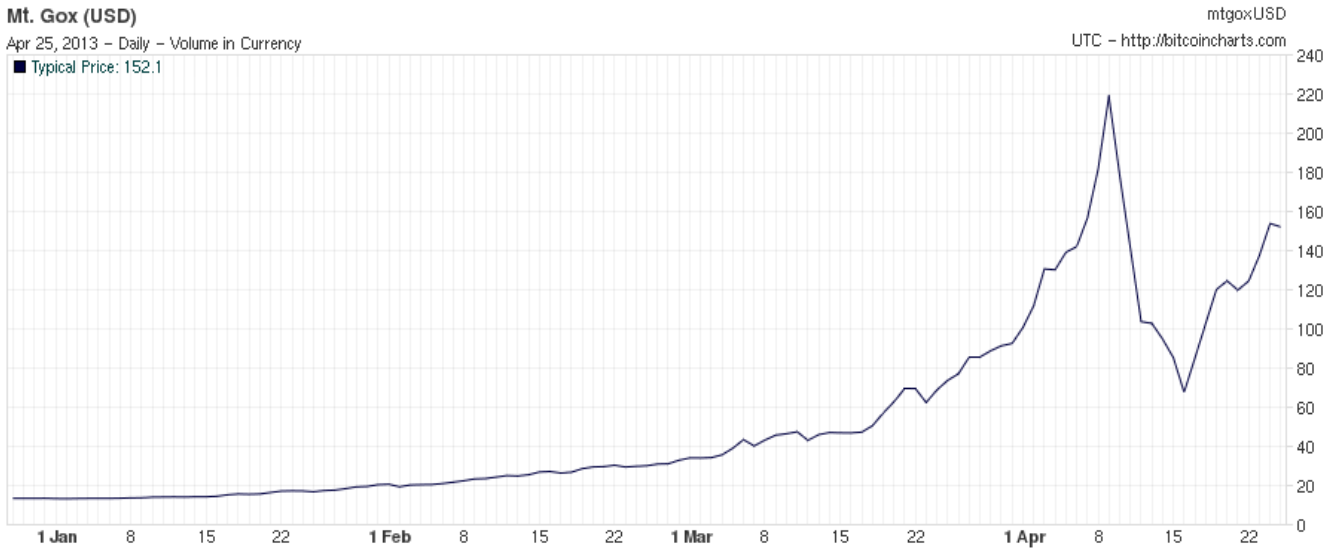
How are Bitcoins created?

The creation of Bitcoins began in 2009 by a man allegedly named Satoshi Nakamoto. Satoshi created a formula so sophisticated that when it is solved (using computer processing power), it creates a "block" of data which contains Bitcoins. There is a maximum amount of Bitcoins that will exist, and there is diminishing returns built into the system. For example, users were formerly able to create 50 Bitcoins in one block, but since the end of 2012, the amount created reduced to 25.

Bitcoin is also unique in its creation; anyone can create their own Bitcoins. This process is called mining and requires an excessive amount of computer power in order to do efficiently.

Since mining requires so much computing power, users will frequently collaborate and create 'mining pools' to collectively create new blocks and split the newly-created Bitcoins. Virtual currency entrepreneurs have also created hardware with a sole purpose of efficiently mining Bitcoins.

An interesting note is Satoshi's identity, or lack thereof. Satoshi is an unknown figure. He allegedly helped with the first Bitcoin transactions in 2010, but soon disappeared.



Price of Bitcoins relative to USD. Courtesy of Bitcoincharts.com

How can I purchase Bitcoins?

There is a plethora of ways to purchase Bitcoins. Usually, it's accomplished through a currency exchange. MtGox.com remains the most popular exchange site for USD, being both the oldest and largest exchange center for Bitcoins. MtGox.com lists pricing data for both buyers and sellers of Bitcoins. It then matches up two interested exchangers and arranges the transaction.

Users can also exchange various gift cards to trade for Bitcoins instead of using cash. Moneypak gift cards are commonly traded as an alternate. Users can also contact Bitcoin miners and make a direct exchange.

Exploitation

Since a Bitcoin wallet is simply data on a computer, theft or manipulation of a users' wallet could occur if the user does not take necessary precautions to protect their Bitcoins. This makes security of a users' wallet imperative.

On June 27th, Synaptic released an article about a Bitcoin Trojan. The program would email the victim's wallet back to the attacker, literally stealing the victim's virtual wallet.

Attacking a users' wallet is not the only vulnerability. In June 2011, a user hacked into MtGox.com and transferred 25,000 BTC from 478 different accounts. At the time it was priced to around 8.75 million USD. This attack was also two-pronged, because the value of Bitcoins dropped dramatically after the hack. The price dropped from $19 USD to $.01 USD within a matter of hours.

These attacks have demonstrated to the digital currency community that security is just as important, and entrepreneurs like Bitcoin have since increased their security parameters to prepare themselves against attacks.

Should I invest in Bitcoins?

Since the price in Bitcoins has increased by nearly 1000% since 2011, there's certainly reason to pay attention. Although many skeptics fear the bubble bursting, entrepreneurs and investors alike appear enthusiastic to the thought of a decentralized digital currency.

ABOUT THE AUTHOR

Katherine Sagona-Stophel, Government Analyst, Thomson Reuters, Mclean, VA

Focused on open source collection, Katherine specializes in understanding the power of crowd sourcing through social media applications, gaming, and mobile technologies in order to solve intelligence problems. She managed to get away with an International Relations degree from American University while building computers and playing video games in her spare time.