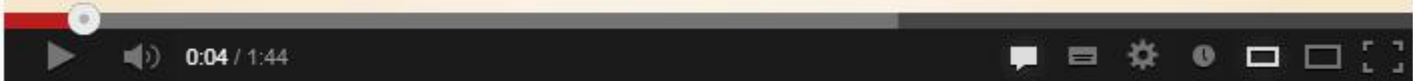




bitcoin /ˈbɪtkɔɪn/

*first decentralized
digital currency*



What is Bitcoin?



weusecoins · 1 video



Subscri...

741

1,566,005

3,055 254



Are Bitcoins and Unusual Hats the Future of Currency? | Idea Chann...



pbsideachannel · 46 videos

Subscri... 152,014

44,775

2,566 29

“ It’s a general characteristic of social systems that people need to have confidence in the future ...”

Gabe Newell: Reflections of a Video Game Maker

<http://youtu.be/t8QEObgLBQU>

Valve does not ask its users to do the hard tasks like coding: “... releasing source ... limits the ways in which people can participate and add value: its hard, right? It’s too hard for people to incrementally get into it. The way we sort of think about being a member of this economy is to think of it much more as an MMO, like you need to walk people through stepwise, here are your *Quests* ...”

Gabe Newell: Reflections of a Video Game Maker

<http://youtu.be/t8QEOBgLBQU>

“ Money needs to flow as a signaling tool in order for people to really assess whether what they are doing is valuable or not, you need currency [within virtual communities]...”

Gabe Newell: Reflections of a Video Game Maker

<http://youtu.be/t8QEOBgLBQU>

“Growing people in this economy looks an awful lot like an MMO experience...”

Gabe Newell: Reflections of a Video Game Maker

<http://youtu.be/t8QEOBgLBQU>

“We started to see things like inflation. We started to see deflation. We started to see users creating their own versions of currencies, mediums of exchange. Countries started to create regulatory structures. In Korea you actually have to create the equivalent of a W4 form for your players to account for the virtual income they get in playing your game.”

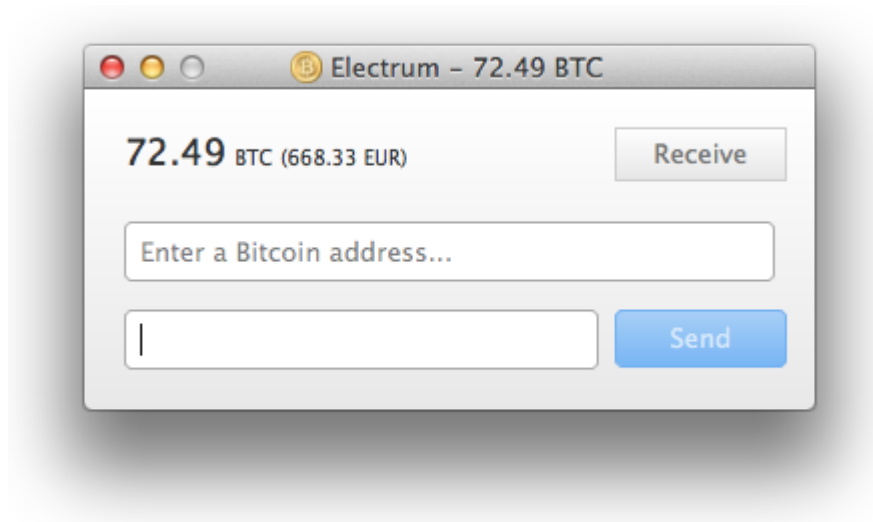
Gabe Newell: Reflections of a Video Game Maker

<http://youtu.be/t8QEOBgLBQU>

“ “The first two weeks that we did this we actually broke Paypal because they didn’t have – I don’t know what they’re worried about, maybe drug dealing – they’re, “like nothing generates cash to our userbase other than selling drugs”. We actually had to work something out with them and said “no ... they’re making hats.” ...”

Gabe Newell: Reflections of a Video Game Maker

<http://youtu.be/t8QEOBgLBQU>



“**Bitcoin** (sign: **BTC**) is a [decentralized digital currency](#) based on an [open-source protocol](#) that was created by a [pseudonymous developer](#) named [Satoshi Nakamoto](#).^{[7][1]} One bitcoin is divided into 100-million smaller units called satoshis. ^[3] There is a hard limit of 21-million bitcoins in total, which are released at a scheduled rate until the year [2140](#)”



‘Bitcoin is one of the first implementations of a concept called *crypto-currency* which was first described in 1998 by Wei Dai on the cypherpunks mailing list. Building upon the notion that money is any object, or any sort of record, accepted as payment for goods and services and repayment of debts in a given country or socio-economic context, Bitcoin is designed around the idea of using cryptography to control the creation and transfer of money, rather than relying on central authorities.’”

Q. What is Bitcoin?

A. Bitcoin is a peer-to-peer currency. Peer-to-peer means that no central authority issues new money or tracks transactions. These tasks are managed collectively by the [network](#).



Bitcoin P2P Digital Currency

Bitcoin is an experimental new digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: managing transactions and issuing money are carried out **collectively by the network**. Bitcoin is also the name of the open source software which enables the use of this currency.

The **software** is a community-driven open source project, released under the **MIT license**.

[Learn how to use Bitcoin »](#)

[Learn more about Bitcoin »](#)

Download

Latest Bitcoin-Qt version: 0.7.2

[\(see all Bitcoin clients\)](#)

-  Windows (zip) ~13MB
-  Windows (exe) ~9MB
-  Ubuntu PPA
-  Linux (tgz, 32/64-bit) ~12MB
-  Mac OS X ~13MB
- [Source code \(GitHub\)](#)



Bitcoin P2P Digital Currency

Bitcoin is an experimental new digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: managing transactions and issuing money are carried out **collectively by the network**. Bitcoin is also the name of the open source software which enables the use of this currency.

The **software** is a community-driven open source project, released under the **MIT license**.

[Learn how to use Bitcoin »](#)

[Learn more about Bitcoin »](#)

Download

Latest Bitcoin-Qt version: 0.7.2

(see all Bitcoin clients)

-  Windows (zip) ~13MB
-  Windows (exe) ~9MB
-  Ubuntu PPA
-  Linux (tgz, 32/64-bit) ~12MB
-  Mac OS X ~13MB
- Source code (GitHub)

Resources

- [We Use Coins. Start here!](#)
- [Bitcoin clients](#)
- [Bitcoin Wiki](#)
 - [FAQ](#)
 - [Sites That Accept Bitcoin](#)
 - [Merchant Howto](#)
- [Bitcoin Charts / Markets](#)

Developers

- Satoshi Nakamoto
- Gavin Andresen - gavinandresen@gmail.com (PGP)
- Pieter Wuille - pieter.wuille@gmail.com (PGP)
- Nils Schneider - [nils.schneider@gmail.com](mailto:nil.s.schneider@gmail.com) (PGP)
- Jeff Garzik - jgarzik@exmulti.com (PGP)
- Wladimir J. van der Laan - laanwj@gmail.com (PGP)
- Gregory Maxwell - gmaxwell@gmail.com (PGP)

Press mailing list for presentation and interview requests:
bitcoin-press@lists.sourceforge.net

Community

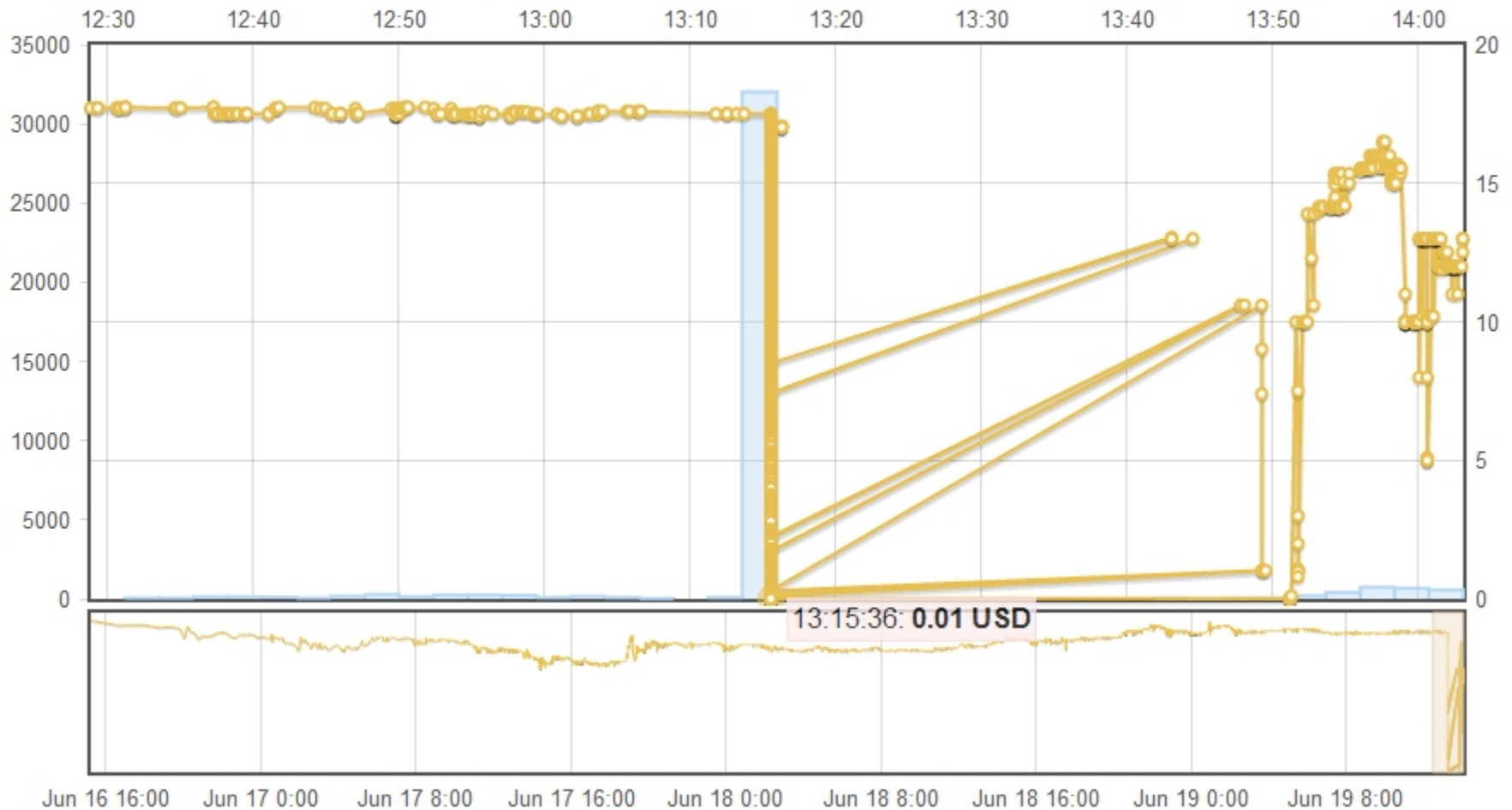
- [Bitcoin StackExchange \(Q&A\)](#)
- Visit the unofficial [Bitcoin Forums](#)
- Join the project's lively IRC channels on the [FreeNode](#) network or use the [FreeNode Web IRC](#).
 - [#bitcoin](#) (General Bitcoin-related)
 - [#bitcoin-dev](#) (Development and technical)
 - [#bitcoin-otc](#) (Over The Counter exchange)
 - [#bitcoin-market](#) (Live quotes from markets)
 - [#bitcoin-mining](#) (GPU mining related)
- [Twitter Search](#)
- [Facebook Page](#)

Hashcash

From Wikipedia, the free encyclopedia

Hashcash is a [proof-of-work system](#) designed to limit [email spam](#) and [denial-of-service attacks](#). It is also used as the proof-of-work protocol in [Bitcoin](#). Hashcash was proposed in March 1997 by [Adam Back](#).^[1]

Last trades



“Over the last few weeks the currency's value rose 30-fold to more than \$30 before falling back to \$10 and rising again to \$20 late last week. But Bitcoin [prices fell to pennies](#) this weekend following a security breach that allowed as much as \$8.75M worth of Bitcoins (at pre-crash prices) to be (temporarily?) stolen.”



“... rather than rely on a central monetary authority to monitor, verify and approve transactions, and manage the money supply, Bitcoin is underwritten by a peer-to-peer network akin to file-sharing services like BitTorrent. ”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“The easiest way to store Bitcoins is to sign up to an online wallet service through which all transactions are carried out. This, of course, means trusting the provider of that service not to cheat, or go out of business, taking clients' savings with it. Warier users can install a personal digital wallet on their own computers. They must then, however, keep it safe from viruses or physical damage. If a laptop went up in smoke, so would the virtual coins stored on its hard drive. (Keeping back-up copies would do the trick.)”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“All transactions are secured using public-key encryption, a technique which underpins many online dealings. It works by generating two mathematically related keys in such a way that the encrypting key cannot be used to decrypt a message and vice versa. One of these, the private key, is retained by a single individual. The other key is made public. In the case of Bitcoin transactions, the intended recipient's public key is used to encode payments, which can then only be retrieved with the help of the associated private key. The payer, meanwhile, uses his own private key to approve any transfers to a recipient's account.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“This provides a degree of security against theft. But it does not prevent an owner of Bitcoins from spending his Bitcoins twice—the virtual analogue of counterfeiting. In a centralised system, this is done by clearing all transactions through a single database. A transaction in which the same user tries to spend the same money a second time (without having first got it back through another transaction) can then be rejected as invalid.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“The whole premise of Bitcoin is to do away with a centralised system. But tracking transactions in a sprawling, dispersed network is tricky. Indeed, many software developers long thought it was impossible. It is the problem that plagued earlier attempts to establish virtual currencies; the only way to prevent double spending was to create a central authority. And if that is needed, people might as well stick with the government devil they know.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“A hashing algorithm converts a message into a number called a hash value, or a digest. If this number is big enough, it provides a unique representation of the original (since the same algorithm could not conceivably yield identical hash values for different messages). Moreover, it is impossible to reconstruct the original on the basis of the digest alone. Nor is it possible to predict what the digest would be for even a slightly tweaked version of the original message; fiddling with a single letter will produce a completely different digest. In that regard, digests appear to be generated at random. As a result, hashing is what computer scientists call an irreversible process.”

Virtual currency

Bits and bob



“With Bitcoin, all new transactions are automatically broadcast across the entire network and analysed in portions, called blocks. Besides any new as-yet-unconfirmed transactions, each block contains the digest for the last block to have got the nod from the network. That last block will always come from tip of the longest chain of blocks currently on the network. This chain is, in effect, the official log—confirmation that all the previous blocks tot up.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“To prevent acceptance of bogus logs, giving it a seal of approval has to be prohibitively costly to any individual user, but relatively cheap for the network as a whole. This is done by making it into a forced-work task, which involves using the valid blocks and the new transactions to generate a digest consisting of 256 bits (ie, any number between 0 and 2^{256}). The task is complete when the system's algorithm spits out a hash value below a preset target (like 11 in the example above).”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“The target is set so that the puzzle is solved by someone on the network, and a new block approved, every 10 minutes. To keep this rate constant as the network's ranks swell and its combined computing power grows, the target is lowered in order to make generating a value below it harder.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“The system can thus rely on users to police it. As a reward for giving up some computing power to that end, the first user to crack the forced-work task gets 50 coins for the effort.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“This is also how Bitcoin niftily gets around the problem of increasing the money supply without a central mint. Since blocks are created at a constant average rate, and there is a set number of coins minted per block, the total money supply, too, increases at a steady clip.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“The idea is to mimic the extraction of [minerals](#) (the transaction-validating software is called the Bitcoin miner). As the most readily accessible resources are exhausted, the supply dwindles.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“In theory, then, the system ought to keep a lid on inflation—making it attractive to critics of interventionist monetary policy of the sort practised since 2008 by America's Federal Reserve under the label quantitative easing. (The mineral analogy, in particular, appeals to proponents of a return to a gold standard.) It offers other apparent benefits, too. The currency can be used by anyone (unlike credit cards, for instance), anywhere.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“Transaction costs are also likely to be lower than those for traditional payment systems, though these are not in fact zero. Some are reflected in the hardware and energy used to police the system. Some surely creep in whenever those who have no wish to mine Bitcoins themselves purchase them for dollars, euros and several other currencies at specialised sites like [Mt. Gox.](#)”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“Legally, Bitcoin exchanges are subject to the same regulations as ones trading commodities. For example, an exchange must report any transaction above \$15,000, a policy meant to stem money laundering. For the purposes of taxation, meanwhile, reimbursing somebody for a product or service in BitCoins is treated as barter. The tax code makes provisions for such practices, though, admittedly, they can be tough to enforce.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“... the open-source nature of the project is also a bulwark against hackers or malware. Indeed, as cybercrime goes, Bitcoin may be safer than traditional financial institutions, which are often on the receiving end of such attacks.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE



“... established fiat currencies—ones where the bills and coins, or their digital versions, get their value by dint of regulation or law—are underwritten by the state which is, in principle at least, answerable to its citizens. Bitcoin, on the other hand, is a community currency. It requires self-policing on the part of its users. To some, this is a feature, not a bug. But, in the grand scheme of things, the necessary open-source engagement remains a niche pursuit. Most people would rather devolve this sort of responsibility to the authorities. Until this mindset changes, Bitcoin will be no rival to real-world dosh.”

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G.T. | MELBOURNE

”Bitcoin developers owe their dedication to the project's intellectual yieldings more than to those of a monetary nature. Bitcoin is still taking its first baby steps; it may go on to do great things but right now it only has something to offer those chasing conceptually interesting projects or bleeding edge technology.”

https://en.bitcoin.it/wiki/FAQ#How_can_I_get_bitcoins.3F

Author Topic: [new ppl should read]Goxxing: the art based on fail that create spikes (Read 540 times)

myself
Hero Member
★★★★★

Posts: 705



atm advisor for bitfinex.com



Ignore

[new ppl should read]Goxxing: the art based on fail that create spikes #1
January 08, 2013, 12:40:07 AM

Mtgox decided to support multiple currencies under same order book, so instead of having one order book for USD, one for EUR, and another for every single currency they support, mtgox calculates the order book prices based on pair crosses against the USD and a certain percentage on top of that.

where you can see the order book of fail
<http://mtgoxlive.com/orders?dark;currency=EUR>
<http://mtgoxlive.com/orders?dark;currency=CAD>
<http://mtgoxlive.com/orders?dark;currency=GBP>
.....

or you can go to mtgox live and look on the help/option and select a currency

Q /so where is the art on this ?
A / a 400BTC buy on the EUR market can spike the USD market 12 cents upwards

Q /can there be also crash ?
A / yep is the other way around

Logged

@myselfbtc.if any post made by me are useful you can tip here 1GazXbr5ARdr152eYbjtAcKd5Yk1tD3WQu.Using speech to text software and sometimes this fail.my post are my personal view and have nothing to do with <https://bitfinex.com> views

Advertisement: **BitMillions.com** Win more than \$ 1,400 Instantly with only \$ 0.01 **Play Now!**



Photo Hour's photostream

[Photostream](#) | [Sets](#) | [Favorites](#) | [Galleries](#) | [Profile](#) | [More](#) ▾

Do you wish to direct a Photo session?

Current auction is here!

www.bitmit.net/en/item/12200-photo-hour-mission-6-special...

Mission #6 is also Special lomo mission #1

PhotoHour was donated a few rolls of vintage porta 160 120-film, stored since 2005. I was also given a lomography 6x6, 6x9, 6x12 belair camera. To celebrate this i will host 3 special lomography missions. Mission #6 will be the lomo mission for 6x6, mission #9 6x9 and mission #12 ofcourse 6x12. Since its vintage film I cant give any guarantee that it has aged with pleasure or that it even usefull at all. However there is a chance it will generate great lomo effects, fingers crossed. Thus, i will shoot digital on these missions as well.

This is Photo Hour - a bitcoin art project. The goal of photo hour is to document the interests and maybe even the lives of people around the world and publish it right here. About once a week, i will auction off one or more hours of my time for whatever nickel people think it is worth to decide what and where i will shoot next. You may ask me to come to you, send me stuff shoot or send me off on a wierd mission. You can even use me as a very cheap regular photo service, shooting your wedding or car or mining rigg and the pictures will be yours to use freely, as long as they can be part of the project too.

The pictures i take will be sent to you as digital pictures and you will be granted (non exclusive) rights to do whatever you want with them, even sell them if you can. At least one picture from every mission will be incorporated in the photo hour art project.

I am an experienced photographer and I have DSLR and middle format gear to cover most kinds of photography. Photography is, however, not my main trade and photo hour is an art project i do mostly for my own amusement, so I don't expect people to pay that much for the services. What i really want the winners to do, is to contribute to photo hour by letting your ideas or even your lives become part of the project.

Name: Photo Hour a bitcoin art project

Joined: November 2011

Currently: Stockholm, Sweden

I am: Other and Open

Email: roos [at] roos.tc

IT'S ALL ABOUT THE BITCOINS


Vending Machine Art Project Converts Euros Into Bitcoins

It's not quite a candy machine, but it'll do.


By Jessica Roy 7/16/12 10:47am

 Twitter 23

 Facebook 17

 Reddit

 LinkedIn

 Email

 Print



(Photo: Max F. Albrecht)

For his summer exhibition at Bauhaus University, German art student Max F. Albrecht [turned](#) an old vending machine into a Bitcoin vending machine. You feed Euro coins into the machine and it prints out a box with an easywallet.org link in it. Navigate to that link and you'll see your bitcoin, which you can then send to whoever you want. Mr. Albrecht helpfully offers the case of Wikileaks as a worthy Bitcoin recipient.

On a [Bitcoin forum](#), Mr. Albrecht writes:

My dream project would be a electronic version 2.0 with the ability to also withdrawal cash for BTC. My initial research shows this would be possible using a mixture of open source software and hardware and some proprietary modules to deal with the physical money.

Silk Road Objects

Brad Troemel

“Troemel has been collecting, replicating, and growing artifacts purchased from this anonymous online black market since 2011.

For this exhibition the artist has placed objects obtained from the Silk Road in conversation with modes of display that reflect the aestheticization of rebellion, creating a feedback loop between direct action as a sincere gesture and the inevitably fetishized forms those cultures of rebellion take on in a marketplace.”

<http://bradtroemel.com/index.php/project/silk-road-objects/>



Silk Road Objects
Brad Troemel

*Anonymous Beavis and Butthead T-Shirt
from eBay with Northern Lights Leaves
(2012)*

1/1, 20x24"



Silk Road Objects
Brad Troemel

*Bleached Tie Dye T-Shirt with Third Generation
Bump Keys Dipped and Pressed
(2012)*



1st century CE Silk Road map

Silk Road transmission of art

- [1 Scythian art](#)
- [2 Hellenistic art](#)
- [3 Greco-Buddhist art](#)
 - [3.1 Buddha](#)
 - [4 Chinese art](#)



Recent Sends

Other Sites:

[Bitcoin.org](#)

[WeUseCoins](#)

[Bitcoin Monitor](#)

Faucet Closed

The Faucet is being fixed; please come back in an hour or three.

What are Bitcoins?

Bitcoins are a new kind of money. They aren't created or controlled by a government (like dollars or euros), they're created and controlled by anybody who wants to be part of the Bitcoin payment network. Visit the [Bitcoin.org](#) website for all the details.

Created by Gavin Andresen | Design: [www.yomena.de](#) | Photo: [mira66](#) | CC:Attribution

<http://freebitcoins.appspot.com/>

DWOLLA

Log in

Sign up

The best way to move money.

No percentages. No hidden fees. Just **25¢ per transaction** or **free** for transactions \$10 and less.



Download for iOS



Download for Android



Last price:\$27.23154

High:\$27.59690

Low:\$25.82100

Volume:81118 BTC

Weighted Avg:\$26.82511

USD



or [Sign up](#)



Trade with confidence on the world's largest Bitcoin exchange!

Mt.Gox is the world's most established Bitcoin exchange. You can quickly and securely trade bitcoins with other people around the world with your local currency!

[SIGN UP NOW](#)



“As of July 2011, Mt. Gox handles over 80% of all Bitcoin trade”

WIKIPEDIA
The Free Encyclopedia

Payments made easy.

NEW GENERATION ASIC Bitcoin Miner

30
GH/s

\$649

ORDER NOW



Mint work rate:

1.53Thps

Live updates: [Live Stats](#)



RSS



Google+



Facebook



Twitter

[Log in](#)

[HOME](#)

[JOIN](#)

[LOG IN](#)

[COMMUNITY](#) ▾

[TOOLS](#) ▾

[STATISTICS](#) ▾

[CONTACT](#)

ON YOUR MARK, GET SET, GO!

BITMINTER

Try out our Gauge Metered mining software.



What is BitMinter?

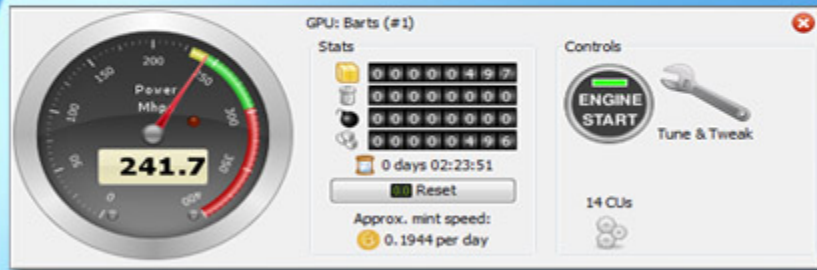
BitMinter aims to make the minting of bitcoins easy and accessible for everyone. BitMinter is a "mining pool" where the efforts of all active members are put together to make bitcoins faster. Mining alone, even with a powerful equipment, can take months without seeing any bitcoins.



What are Bitcoins?

The bitcoin is a digital currency. You can use bitcoins to pay for goods and services (where accepted) and there are exchanges where you can buy and sell bitcoins. Anyone with a computer can also make bitcoins. Watch this video for an introduction:

BitMinter Client



Tune and tweak each individual GPU.

2012.01.14 [15:31] BitMinter Client v1.1.0 started

2012.01.14 [15:31] Hint: Use performance mode for max speed (bottom right button)

2012.01.14 [15:31] Found 2 OpenCL-compatible GPUs

2012.01.14 [15:31] Starting long polling

2012.01.14 [15:31] Difficulty is now 1250758

Barts (#1) started 0 974 0 0 connected 6 482.7 Mhps

Easy to view detailed information.

Improving the way we mine, one step at a time.

“Merged mining: Through a technique called merged mining we are now making name coins in addition to bitcoins, with no additional effort. You can read more about namecoins at dot-bit.org.”



Put your graphics card to work...

Make bitcoins - the digital currency

Reward System

Whenever we are successful in making a block, the bitcoins are split between the users who were working recently.

PPLNS with shifts: Work is split in [shifts](#).

Minted bitcoins are split proportional to your share of work in the last 10 shifts.



*What is
Bitcoin?*

*Getting
Started*

*Questions
& Answers*

*Bitcoin For
Merchants*

your portal into the world of bitcoin



FREE GROUND SHIPPING
on all orders over \$50



SAME-DAY SHIPPING
if you order by 4pm PST



NEED HELP NOW?
Chat with Us Live!

Type product name, sku, brand, category



Like

647 people like this. Be the first of your friends.

TRANSCEIVER

MEMORY

HARDWARE

CABLES

Shop By

CATEGORY

[Transceiver \(90\)](#)

PRICE

[\\$0.00 - \\$10,000.00 \(2037\)](#)

[\\$30,000.00 - \\$40,000.00](#)

[\(1\)](#)

CONDITION

[new \(1779\)](#)

[used \(177\)](#)

You are here: [Home](#) > [10 Casascius Bitcoin \(1 Troy Ounce Silver Round w/Gold Plated Bitcoin Logo\)](#)



10 Casascius Bitcoin (1 Troy Ounce Silver Round w/Gold Plated Bitcoin Logo)

Availability: **Out of stock**

\$245.78

Add to Wishlist

Review this Product

Add to Compare

Email to a Friend

Facebook Tweet

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJLybLCWrfDpN.



Bob creates a new Bitcoin address for Alice to send her payment to.

CREATING A NEW ADDRESS



Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

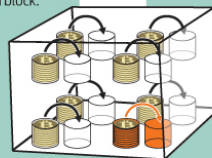


Gary, Garth, and Glenn are Bitcoin miners.

VERIFYING THE TRANSACTION

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.



Private key

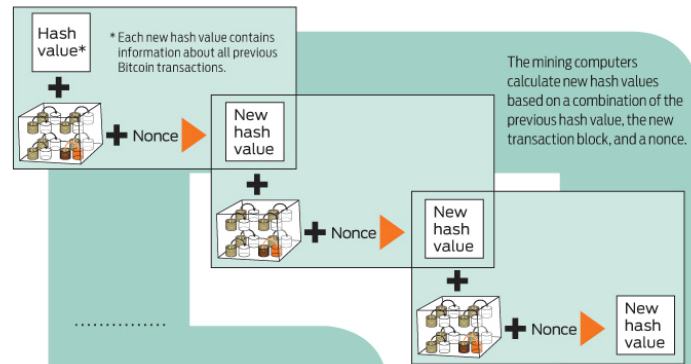


Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Public key



Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.



Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

- The root of all evil → 6d0a 1899 086a... (56 more characters)
- The root of all evil → 486c 6be4 6dde...
- The root of all evil → b8db 7ee9 8392...

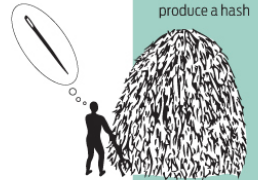
Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ??? → 0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash



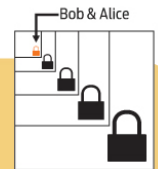
value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

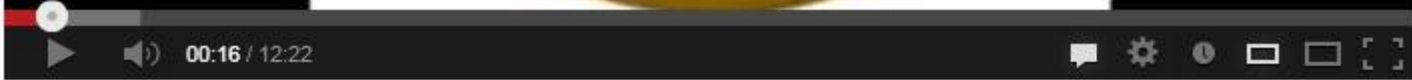
Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.



TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.





Introduction to Bitcoin



“On 21 February 2007, Sotheby's auction house in London auctioned three works, reaching the highest ever price for a Banksy work at auction: over £102,000 for his *Bombing Middle England*. Two of his other graffiti works, *Balloon Girl* and *Bomb Hugger*, sold for £37,200 and £31,200 respectively, which were well above their estimated prices.^[32] The following day's auction saw a further three Banksy works reach soaring prices:*Ballerina with Action Man Parts* reached £96,000; *Glory* sold for £72,000; *Untitled (2004)* sold for £33,600; all significantly above estimated values.^[33] To coincide with the second day of auctions, Banksy updated his website with a new image of an auction house scene showing people bidding on a picture that said, "I Can't Believe You Morons Actually Buy This Shit.””

<http://en.wikipedia.org/wiki/Banksy>

I Can't Believe You Morons Actually Buy This Shit.

Banksy

(2007)