Understanding Bitcoin

The fuel powering the underground economy

Trivia Question #1

Which US President moved US completely away from the Gold Standard?

Trivia Question #2

What are some of the desired attributes in a currency?

Desired attributes in a currency

- Durability
- Divisibility
- Transportable
- Difficult to counterfeit
- Limited Availability
- Acceptance
- Consistent

Need for Digital Currencies

- Non-reliance on central authorities
- Person to person transaction
- Money for the Internet based virtual world without the need for having physical money
- Not country specific
- No arbitrary limits
- Account can not be frozen by a central authority
- Lower transaction costs

What is Bitcoin?

Bitcoin is a distributed peer-to-peer payment system and digital currency introduced as open source software in 2009.

Shorthand - BTC

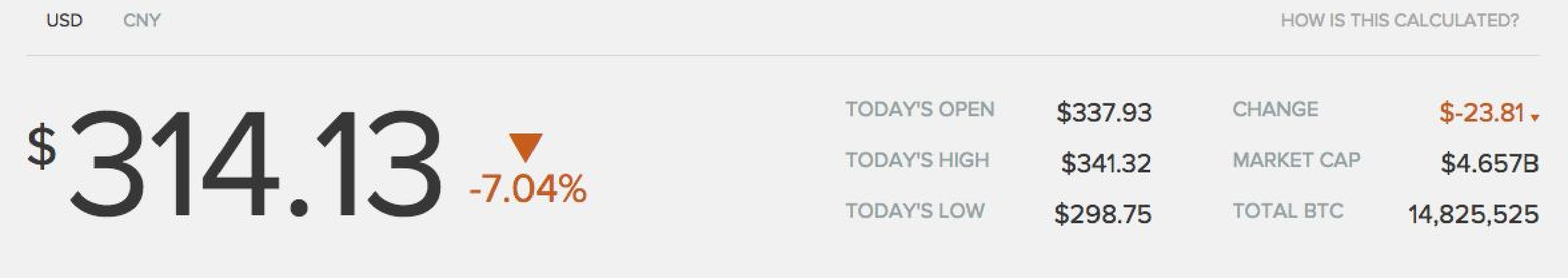
There will be only 21 million Bitcoins created or mined before 2140

Can be divided down to 8 decimal places

0.00000001 BTC (also known as Satoshi)

Bitcoin Price (as of Nov 11, 2015)

1 Bitcoin Equals



USD CNY

HOW IS THIS CALCULATED?

$314.13 ▼ -7.04%

TODAY'S OPEN	$337.93	CHANGE	$-23.81 ▾
TODAY'S HIGH	$341.32	MARKET CAP	$4.657B
TODAY'S LOW	$298.75	TOTAL BTC	14,825,525

Look at the Market Cap of all the Bitcoins in circulations

Who started this all?

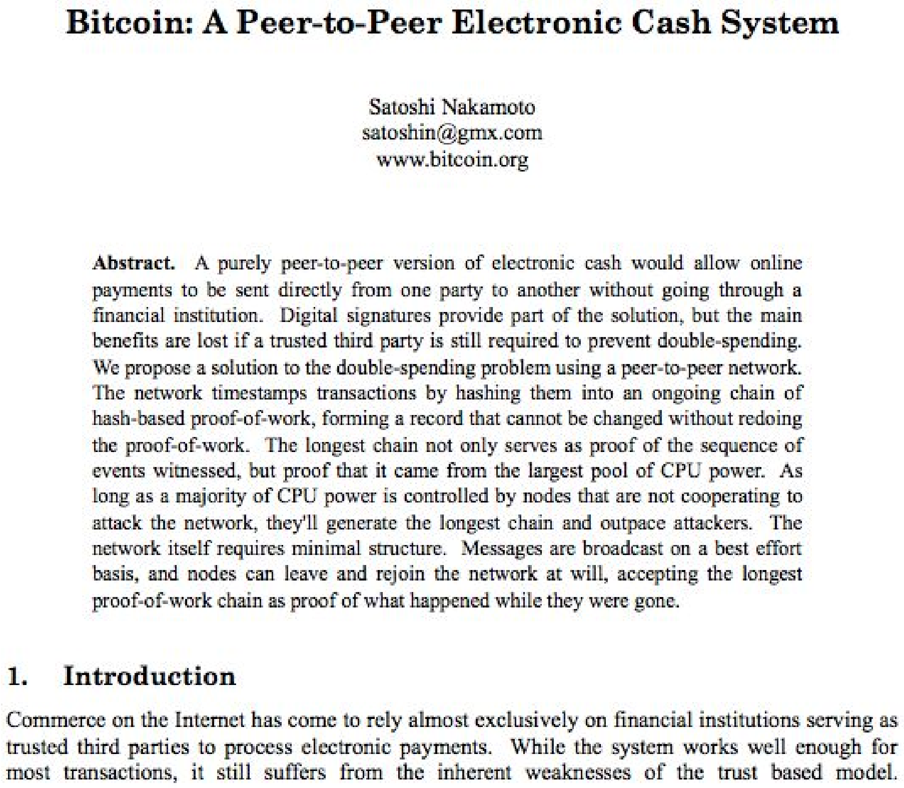
Satoshi Nakamoto (Pseudonym)

Original Bitcoin Whitepaper

Bitcoin: A Peer-to-Peer Electronic Cash System

https://bitcoin.org/bitcoin.pdf

Just a 9 page paper (including the reference page)



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

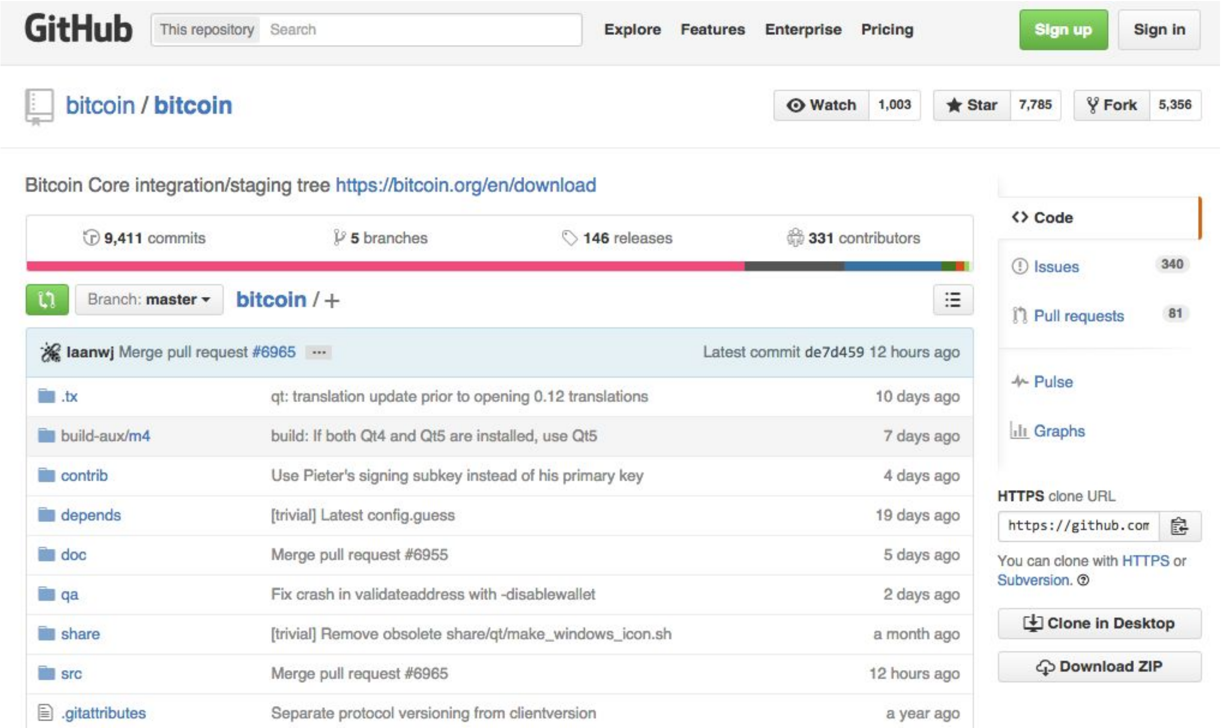
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

Bitcoin code

- Open Source (released under MIT License)
- Hosted on GitHub
- 340 Open Issues (as of Nov 11, 2015)



Bitcoin Core integration/staging tree https://bitcoin.org/en/download

laanwj Merge pull request #6965 ··· Latest commit de7d459 12 hours ago

.tx	qt: translation update prior to opening 0.12 translations	10 days ago
build-aux/m4	build: If both Qt4 and Qt5 are installed, use Qt5	7 days ago
contrib	Use Pieter's signing subkey instead of his primary key	4 days ago
depends	[trivial] Latest config.guess	19 days ago
doc	Merge pull request #6955	5 days ago
qa	Fix crash in validateaddress with -disablewallet	2 days ago
share	[trivial] Remove obsolete share/qt/make_windows_icon.sh	a month ago
src	Merge pull request #6965	12 hours ago
.gitattributes	Separate protocol versioning from clientversion	a year ago

HTTPS clone URL

https://github.com

You can clone with HTTPS or Subversion.

SilkRoad

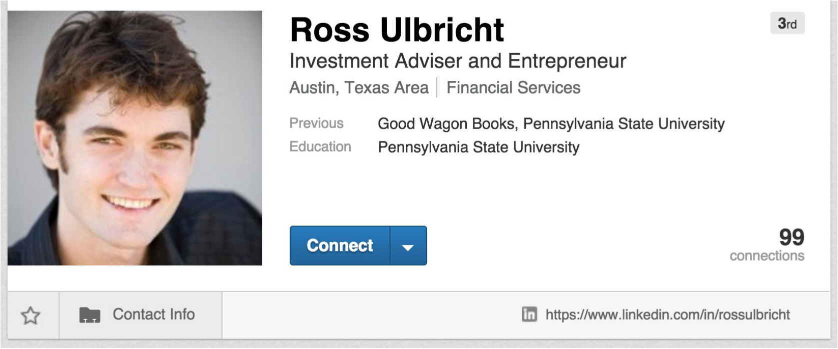
http://silkroad6ownowfk.onion

Dark Web site (accessible only via the Tor network)

Marketplace for illegal services and goods mainly drugs

Used Tor and Bitcoin as means for enabling anonymous transactions

Helped Bitcoin get popular by accepting Bitcoins as means of payment



Ross Ulbricht

3rd

Investment Adviser and Entrepreneur

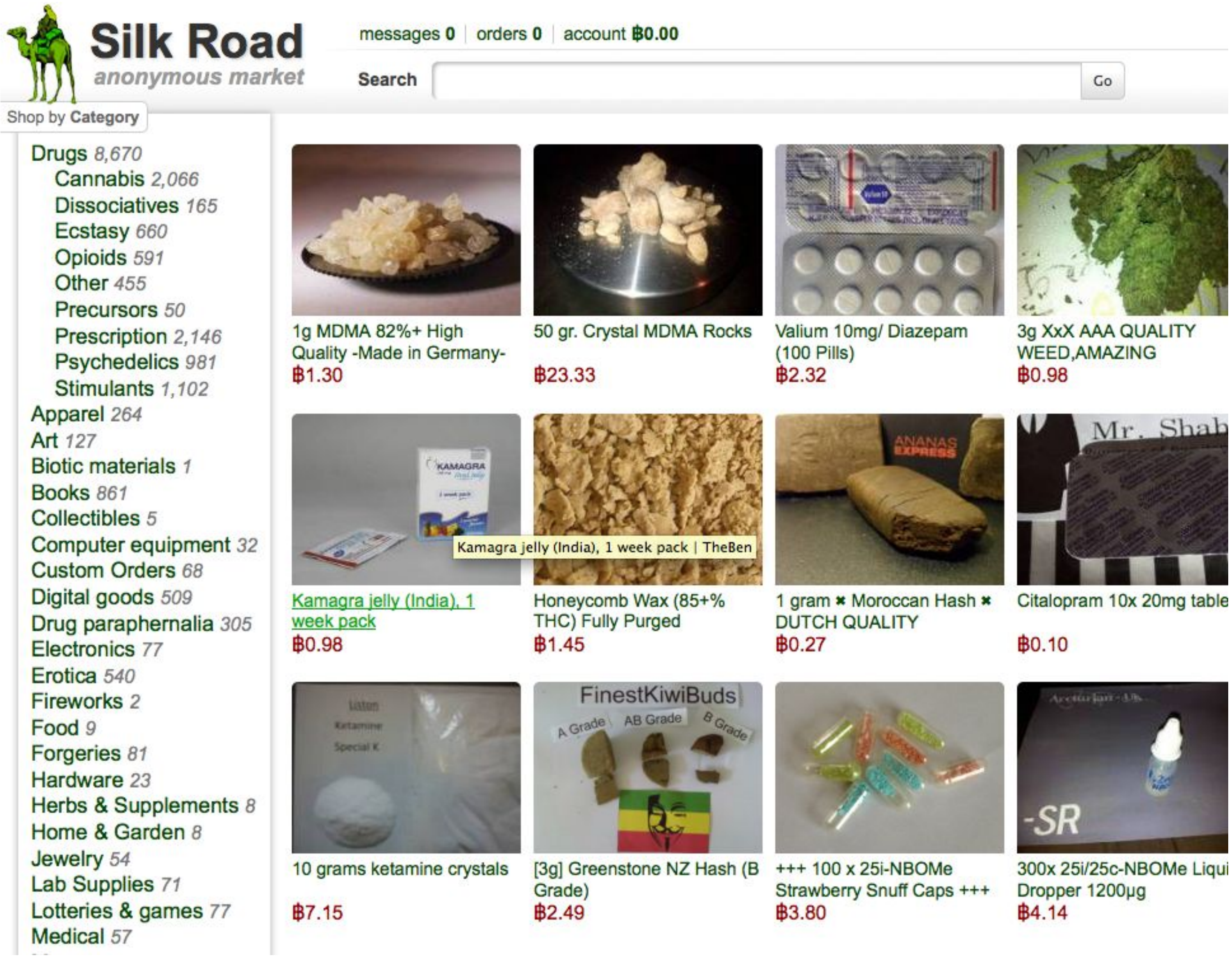
Austin, Texas Area | Financial Services

Previous Good Wagon Books, Pennsylvania State University

Education Pennsylvania State University

99 connections

https://www.linkedin.com/in/rossulbricht



Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.00

Search [ ] Go

Shop by Category

- Drugs 8,670
  - Cannabis 2,066
  - Dissociatives 165
  - Ecstasy 660
  - Opioids 591
  - Other 455
  - Precursors 50
  - Prescription 2,146
  - Psychedelics 981
  - Stimulants 1,102
- Apparel 264
- Art 127
- Biotic materials 1
- Books 861
- Collectibles 5
- Computer equipment 32
- Custom Orders 68
- Digital goods 509
- Drug paraphernalia 305
- Electronics 77
- Erotica 540
- Fireworks 2
- Food 9
- Forgeries 81
- Hardware 23
- Herbs & Supplements 8
- Home & Garden 8
- Jewelry 54
- Lab Supplies 71
- Lotteries & games 77
- Medical 57

1g MDMA 82%+ High Quality -Made in Germany-
฿1.30

50 gr. Crystal MDMA Rocks
฿23.33

Valium 10mg/ Diazepam (100 Pills)
฿2.32

3g XxX AAA QUALITY WEED,AMAZING
฿0.98

Kamagra jelly (India), 1 week pack | TheBen

Kamagra jelly (India), 1 week pack
฿0.98

Honeycomb Wax (85+% THC) Fully Purged
฿1.45

1 gram ✖ Moroccan Hash ✖ DUTCH QUALITY
฿0.27

Citalopram 10x 20mg table
฿0.10

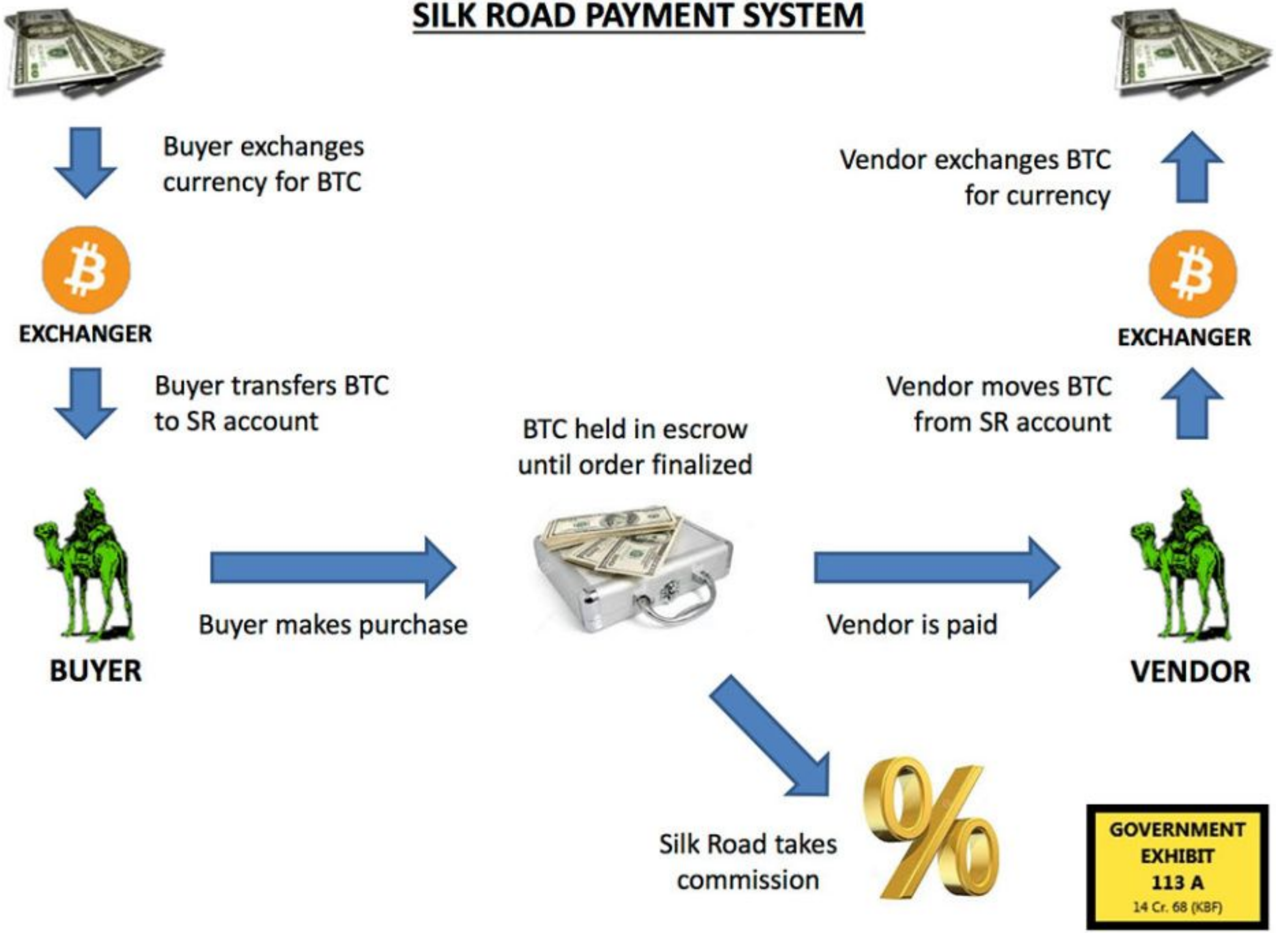
10 grams ketamine crystals
฿7.15

[3g] Greenstone NZ Hash (B Grade)
฿2.49

+++ 100 x 25i-NBOMe Strawberry Snuff Caps +++
฿3.80

300x 25i/25c-NBOMe Liqui Dropper 1200µg
฿4.14

SILK ROAD PAYMENT SYSTEM



Buyer exchanges currency for BTC

EXCHANGER

Buyer transfers BTC to SR account

BUYER

Buyer makes purchase

BTC held in escrow until order finalized

Vendor is paid

VENDOR

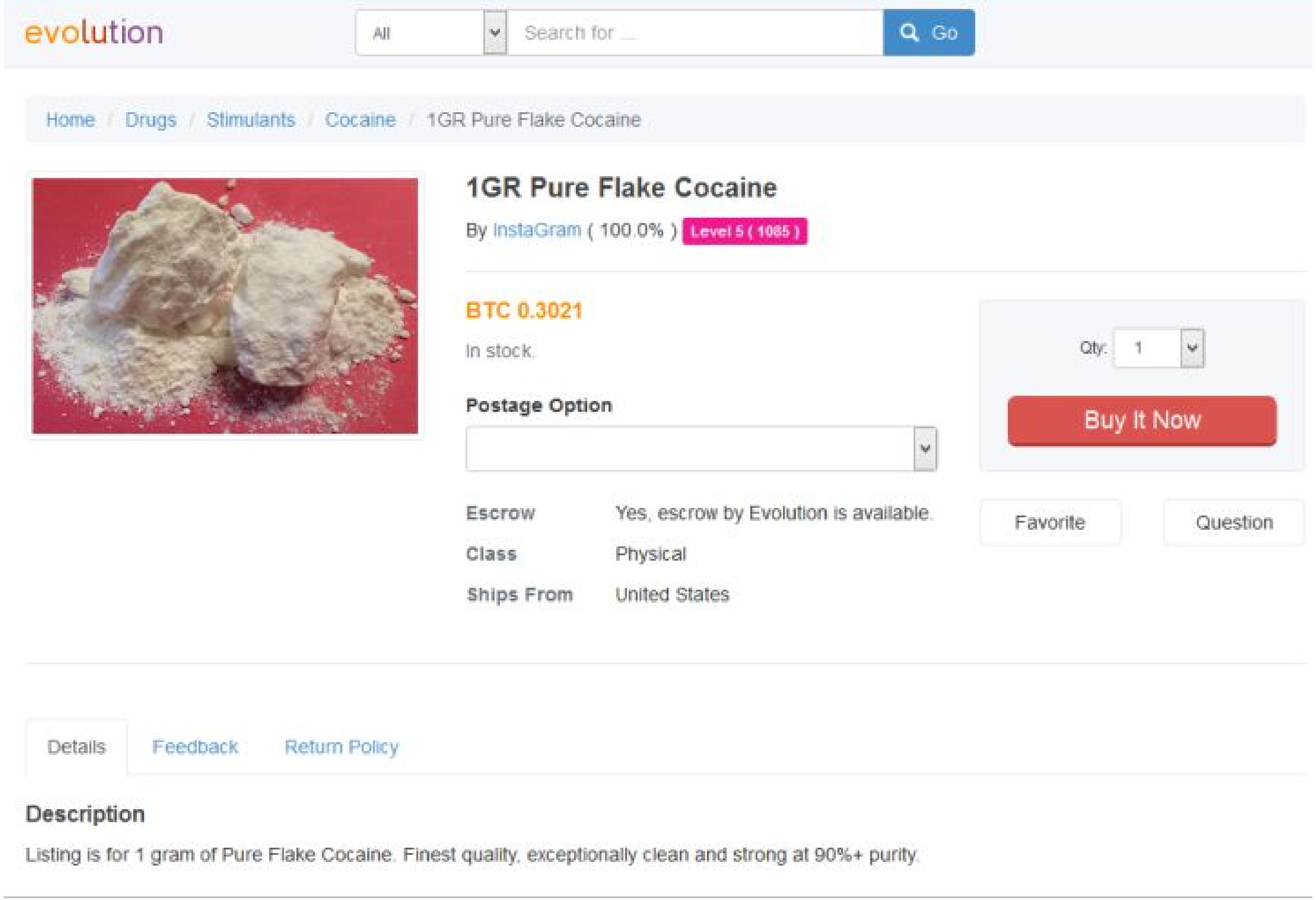
Vendor moves BTC from SR account

EXCHANGER

Vendor exchanges BTC for currency

Silk Road takes commission

GOVERNMENT EXHIBIT
113 A
14 Cr. 68 (KBF)



Home / Drugs / Stimulants / Cocaine / 1GR Pure Flake Cocaine

1GR Pure Flake Cocaine

By InstaGram (100.0%) Level 5 (1085)

BTC 0.3021

In stock.

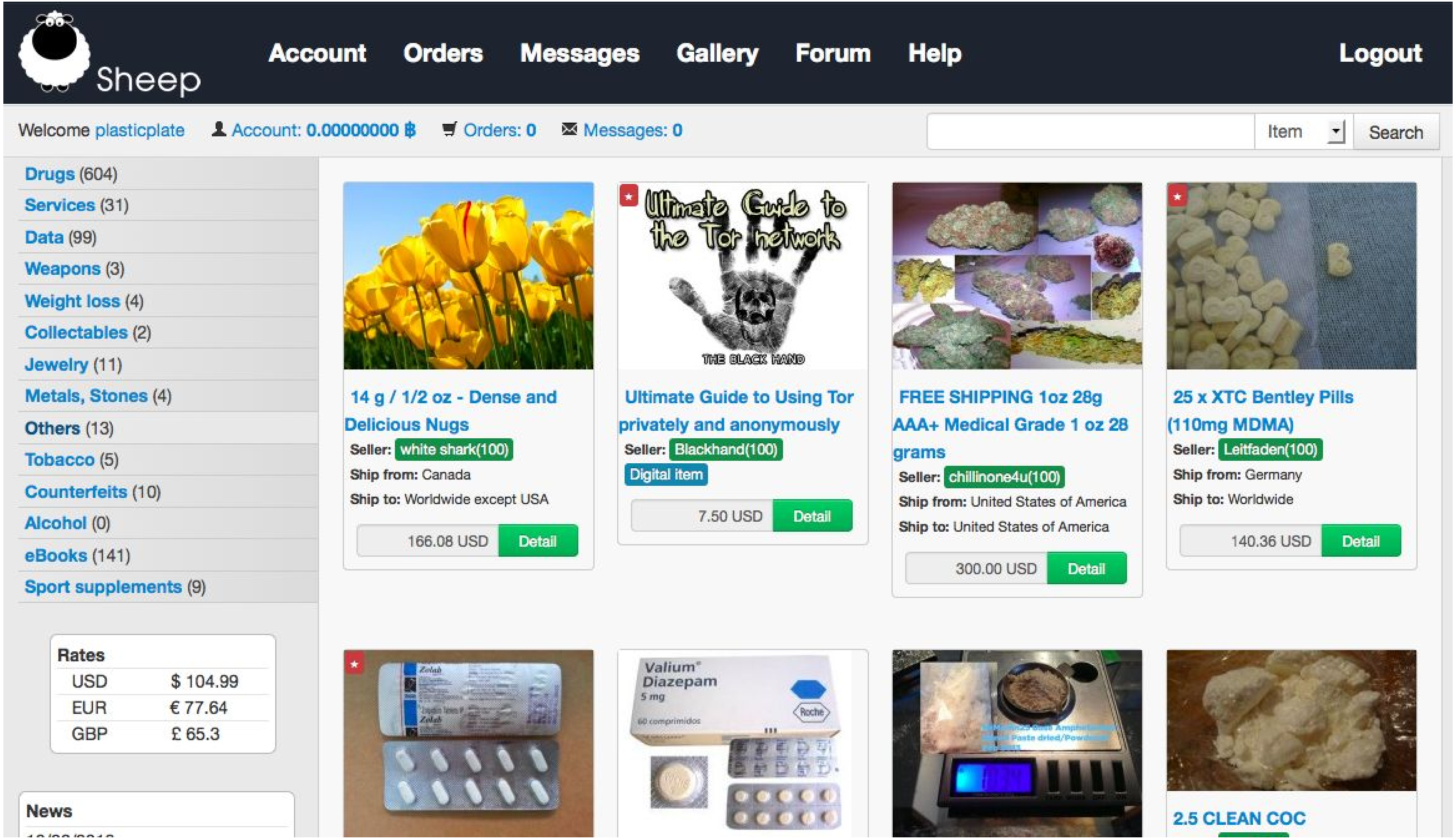
Postage Option

Qty: 1

Escrow	Yes, escrow by Evolution is available.
Class	Physical
Ships From	United States

Description

Listing is for 1 gram of Pure Flake Cocaine. Finest quality, exceptionally clean and strong at 90%+ purity.



Welcome plasticplate Account: 0.00000000 ฿ Orders: 0 Messages: 0

Drugs (604)
Services (31)
Data (99)
Weapons (3)
Weight loss (4)
Collectables (2)
Jewelry (11)
Metals, Stones (4)
Others (13)
Tobacco (5)
Counterfeits (10)
Alcohol (0)
eBooks (141)
Sport supplements (9)

Rates

USD	$ 104.99
EUR	€ 77.64
GBP	£ 65.3

News

14 g / 1/2 oz - Dense and Delicious Nugs
Seller: white shark(100)
Ship from: Canada
Ship to: Worldwide except USA
166.08 USD

Ultimate Guide to Using Tor privately and anonymously
Seller: Blackhand(100)
Digital item
7.50 USD

FREE SHIPPING 1oz 28g AAA+ Medical Grade 1 oz 28 grams
Seller: chillinone4u(100)
Ship from: United States of America
Ship to: United States of America
300.00 USD

25 x XTC Bentley Pills (110mg MDMA)
Seller: Leitfaden(100)
Ship from: Germany
Ship to: Worldwide
140.36 USD

2.5 CLEAN COC

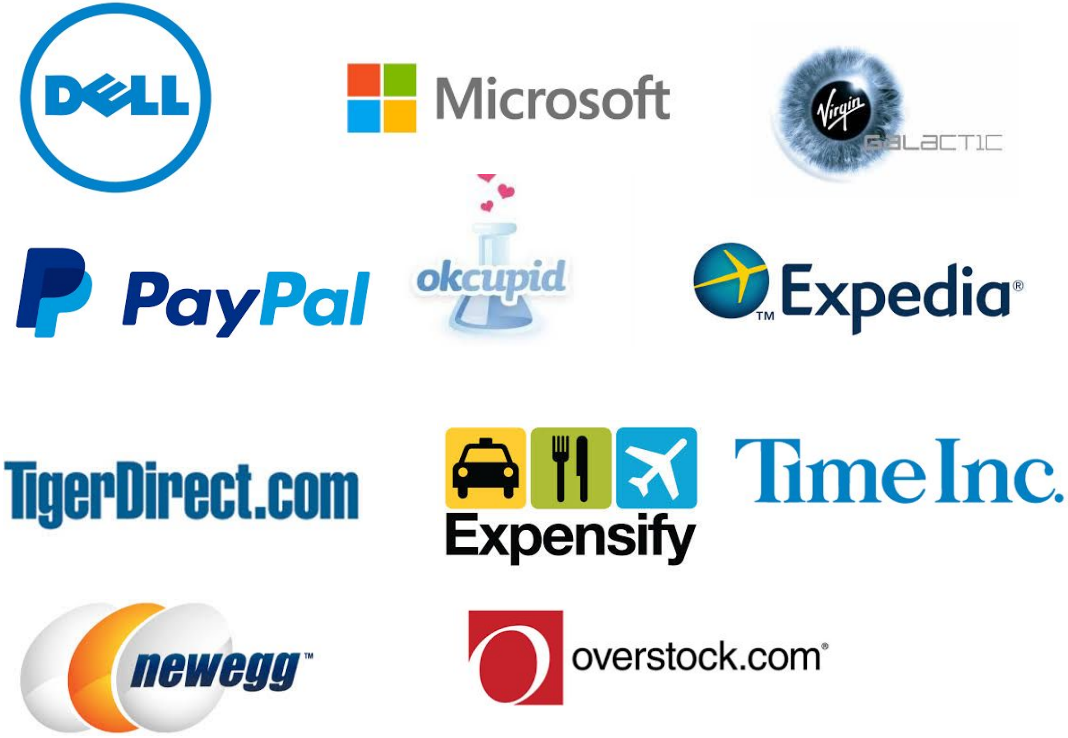
First purchase using Bitcoins

User "laszlo" made the first real-world transaction using Bitcoins in Feb 2010.

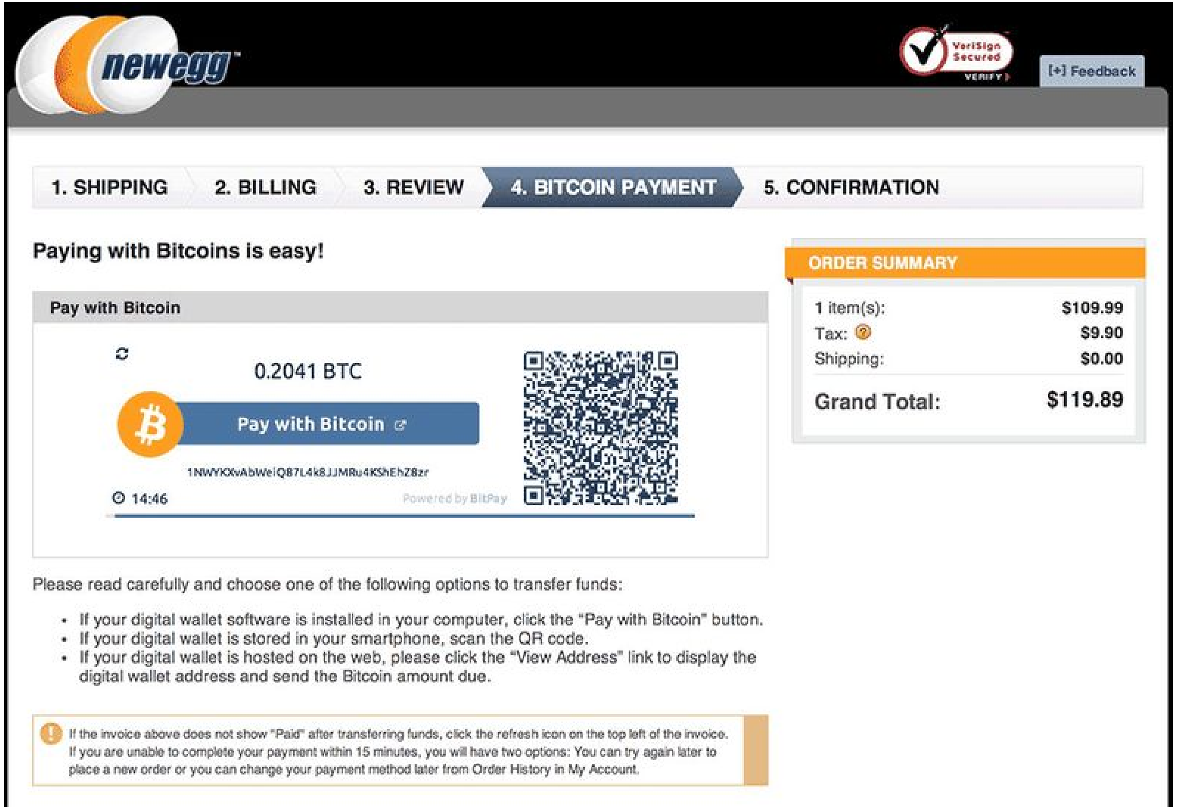
Bought 2 pizzas for 10,000 BTC

Who is accepting Bitcoins?

In most cases, the companies don’t directly accept bitcoins but use a bitcoin processing partner who accepts Bitcoins.



Paying with Bitcoins - Shopping Cart View



Paying with Bitcoins is easy!

Pay with Bitcoin

0.2041 BTC

1NWYKXvAbWeiQ87L4k8JJMRu4KShEhZ8zr

14:46

ORDER SUMMARY

1 item(s):	$109.99
Tax:	$9.90
Shipping:	$0.00
Grand Total:	$119.89

Please read carefully and choose one of the following options to transfer funds:

- If your digital wallet software is installed in your computer, click the "Pay with Bitcoin" button.
- If your digital wallet is stored in your smartphone, scan the QR code.
- If your digital wallet is hosted on the web, please click the "View Address" link to display the digital wallet address and send the Bitcoin amount due.

If the invoice above does not show "Paid" after transferring funds, click the refresh icon on the top left of the invoice. If you are unable to complete your payment within 15 minutes, you will have two options: You can try again later to place a new order or you can change your payment method later from Order History in My Account.

How to get Bitcoins?

- Mine it
- Exchange with regular currency e.g. at Exchanges, at a Bitcoin ATM or from a person
- Get it as payment for goods/services

How are Bitcoins generated?

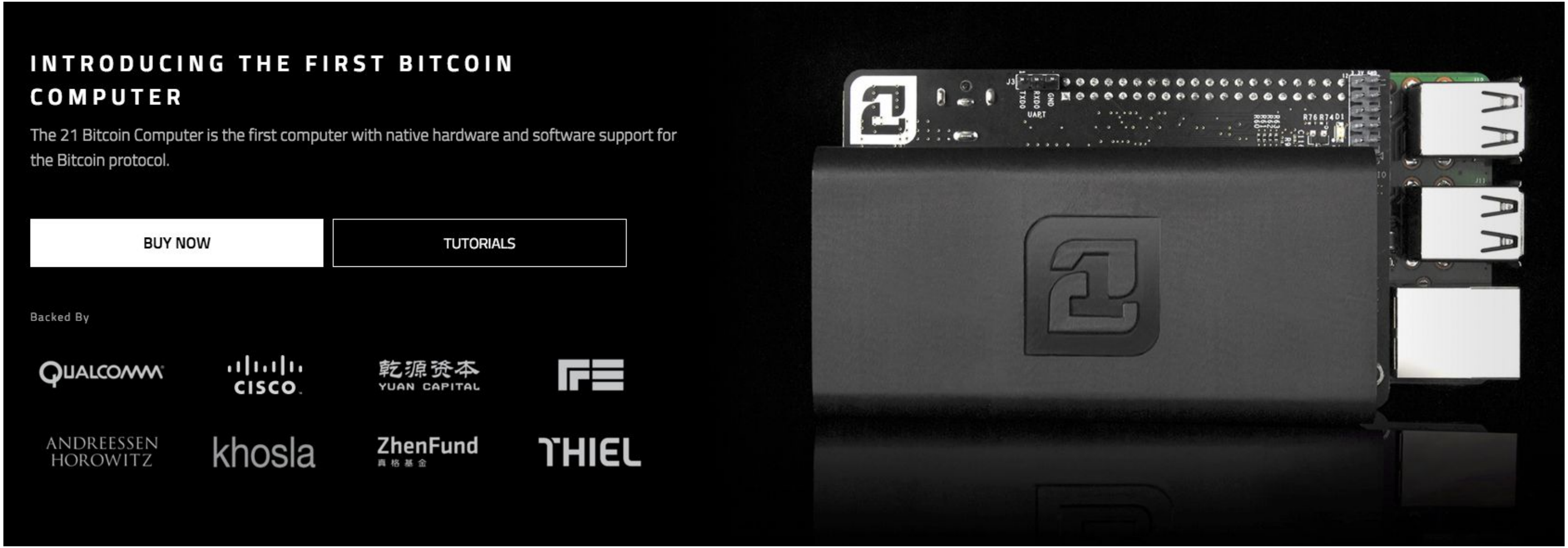
Initially, it was just basic computers

GPU - Graphic Processing Unit

ASIC (Application Specific Integrated Circuit)

The complexity of mining coins increases as more coins are generated

21 Inc.

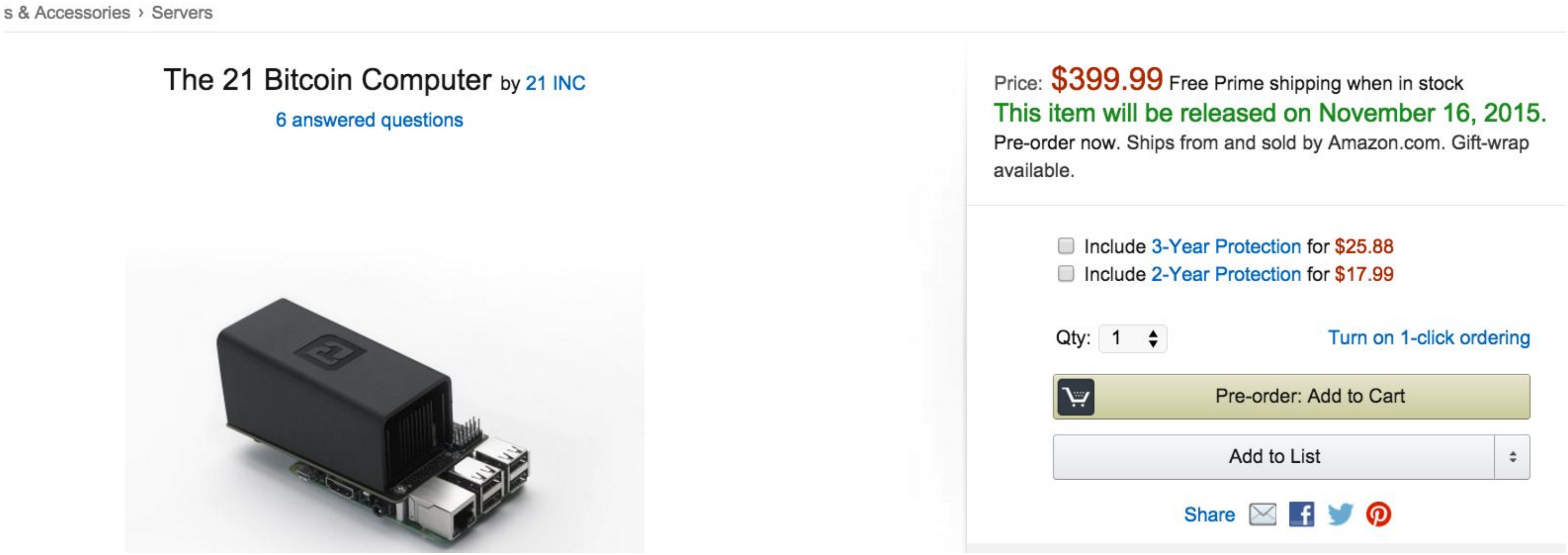


INTRODUCING THE FIRST BITCOIN COMPUTER

The 21 Bitcoin Computer is the first computer with native hardware and software support for the Bitcoin protocol.

Look at the backers of this company

You can buy it on Amazon.com



s & Accessories › Servers

The 21 Bitcoin Computer by 21 INC

6 answered questions

Price: $399.99 Free Prime shipping when in stock

This item will be released on November 16, 2015.

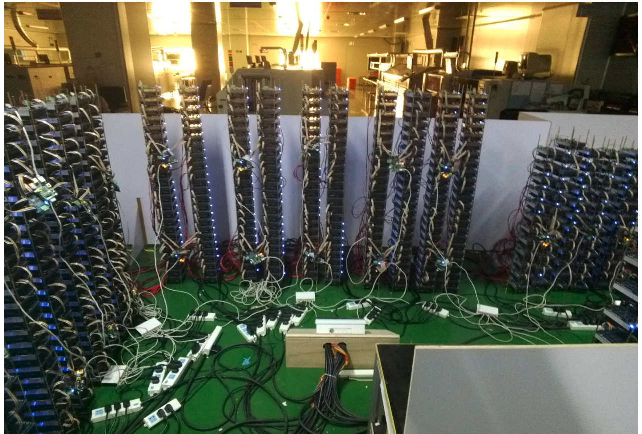
Pre-order now. Ships from and sold by Amazon.com. Gift-wrap available.

□ Include 3-Year Protection for $25.88

□ Include 2-Year Protection for $17.99

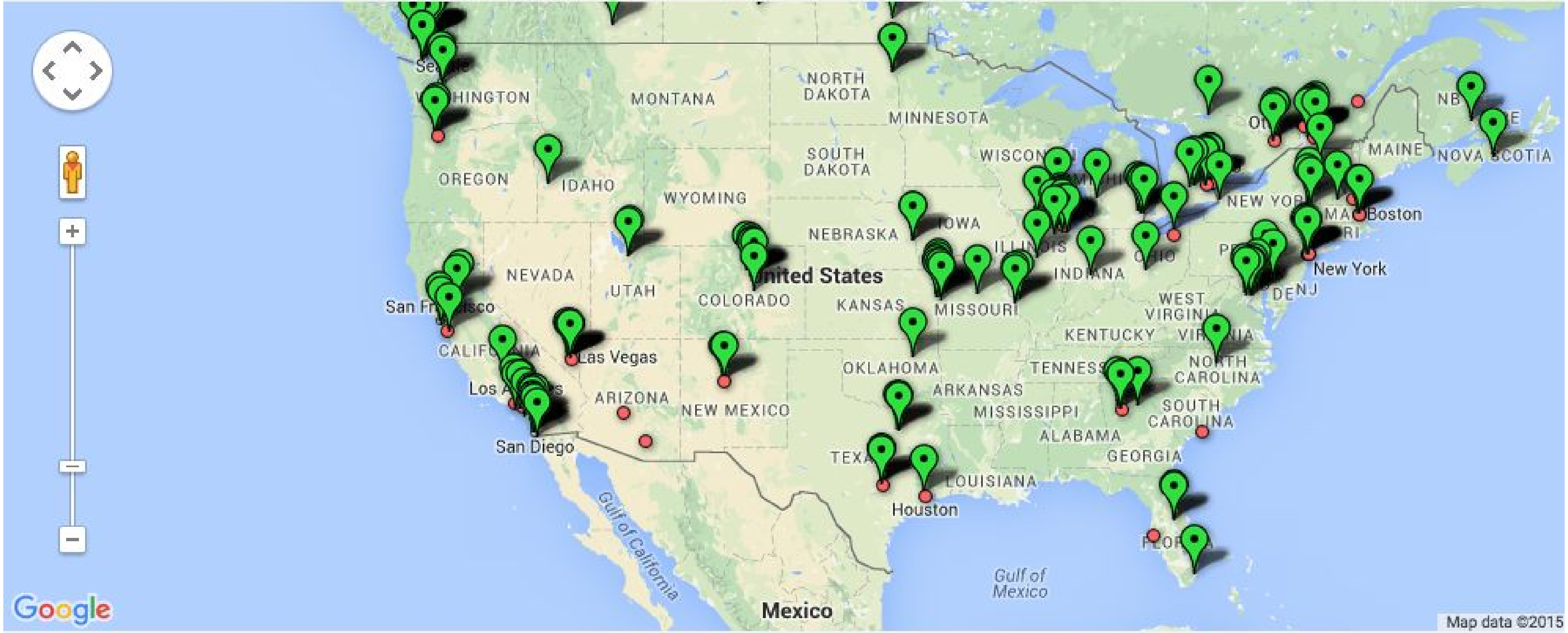
Qty: 1

Bitcoin Farms



Bitcoin ATM’s

Bitcoin ATM Map



Bitcoin ATM in San Francisco

2415 Mission St

San Francisco

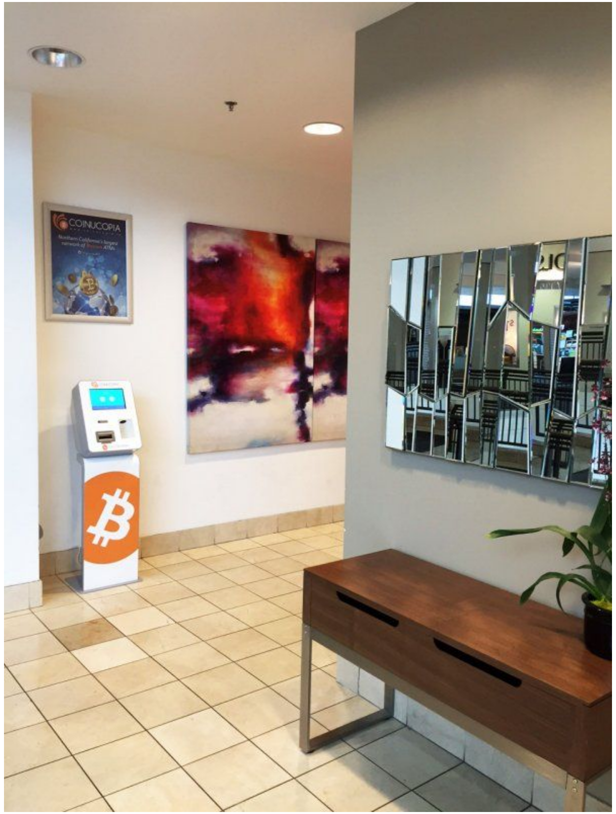
http://nakamotos.io/

Bitcoin ATM in Santa Clara

Westfield Valley Fair Mall

2855 Stevens Creek Boulevard

Santa Clara

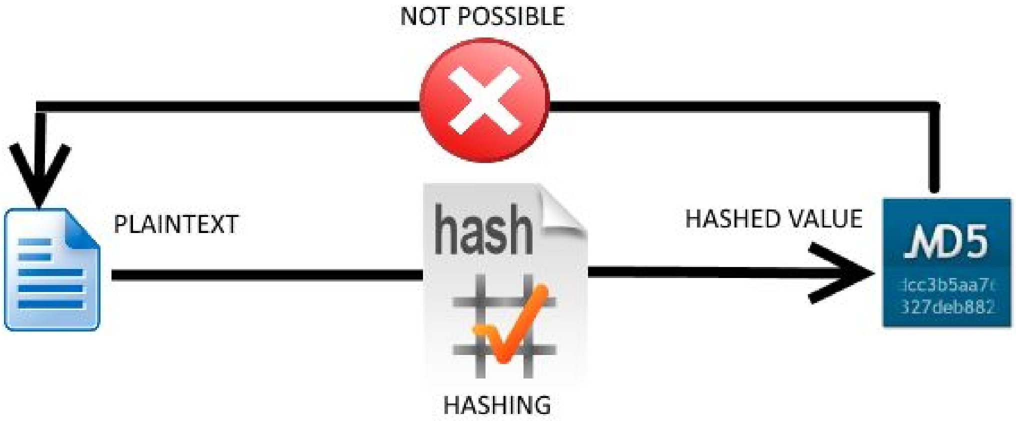


Trivia Question #3

What are hash functions or what is hashing?

Hash Functions

Hash functions are "one way" mathematical functions that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called **hash values**, **hash codes**, **hash sums**, or simply **hashes**. Bitcoin uses SHA-256.

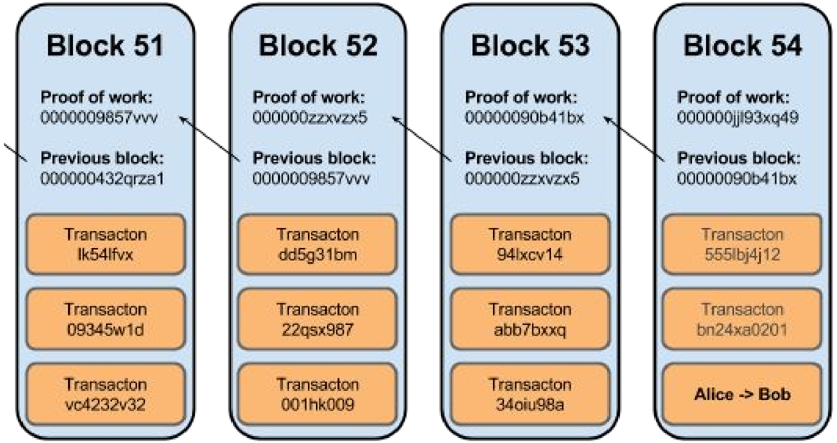


How are Bitcoins generated?

- Mining
- Hashing
- Block
- Proof of Work
- Coinbase

Blockchain

- Blockchain is the Bitcoin transaction log/ledger of past transactions.
- Contains every transaction ever conducted through the Bitcoin network. Shared record of which wallets owns which bitcoins
- Shared by everyone on the Bitcoin network.



Block 51

Proof of work:
0000009857vvv

Previous block:
000000432qrza1

Transacton
lk54lfvx

Transacton
09345w1d

Transacton
vc4232v32

Block 52

Proof of work:
000000zzxvzx5

Previous block:
0000009857vvv

Transacton
dd5g31bm

Transacton
22qsx987

Transacton
001hk009

Block 53

Proof of work:
00000090b41bx

Previous block:
000000zzxvzx5

Transacton
94lxcv14

Transacton
abb7bxxq

Transacton
34oiu98a

Block 54

Proof of work:
000000jjl93xq49

Previous block:
00000090b41bx

Transacton
555lbj4j12

Transacton
bn24xa0201

Alice -> Bob

Blockchain

- Transactions are not recognized until added to the blockchain
- Pending transactions are cleared and added to the block chain only after a majority vote approves them
- Currently about 40 transactions per minute happen on the Bitcoin network (Visa handles about 200,000 transactions per minute) which get added to the block chain every 10 minutes.

Mining

Process of adding record of transactions to Bitcoin's Public Ledger of past transactions (Blockchain)

Currently the Bitcoin network allows approximately 10 Bitcoins to be mined every 10 minutes. This number halves every 4 years.

How to Store Bitcoins - Bitcoin Wallet

- Bitcoins are stored in what is called a “Wallet”
- A wallet has two components - a “public key” and a “private key”
- Private key allows access to your Bitcoins

How to Store Bitcoins - Bitcoin Wallet

Paper Wallet

Hardware Wallet

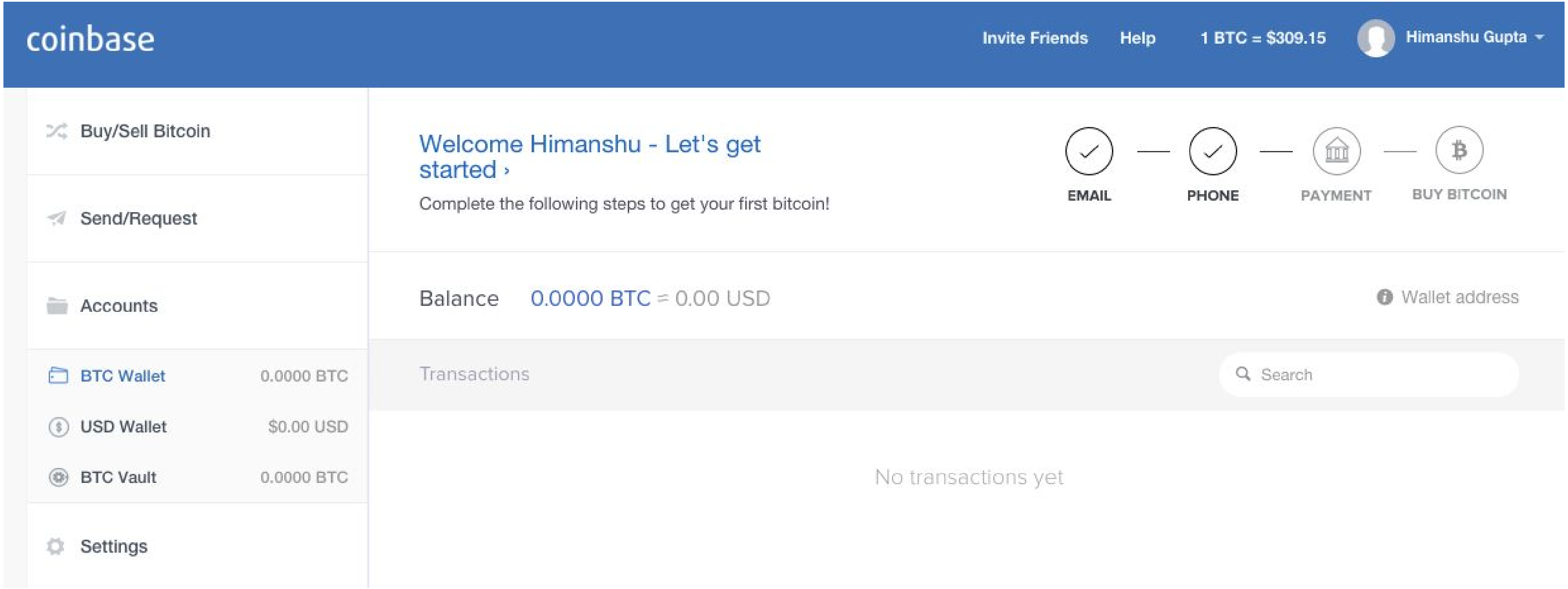
Digital Copy

- Online Wallets
- Personal Digital Wallet
- USB/CD

bitcoin
PUBLIC ADDRESS / DEPOSIT
1DeSignGw8mxzTkoGzFsaQbTMiWThRk93S

Hardware Bitcoin Wallet

Online Digital Wallet



coinbase

Invite Friends Help 1 BTC = $309.15 Himanshu Gupta

Buy/Sell Bitcoin

Send/Request

Accounts

BTC Wallet	0.0000 BTC
USD Wallet	$0.00 USD
BTC Vault	0.0000 BTC

Settings

Welcome Himanshu - Let's get started ›

Complete the following steps to get your first bitcoin!

EMAIL — PHONE — PAYMENT — BUY BITCOIN

Balance 0.0000 BTC = 0.00 USD

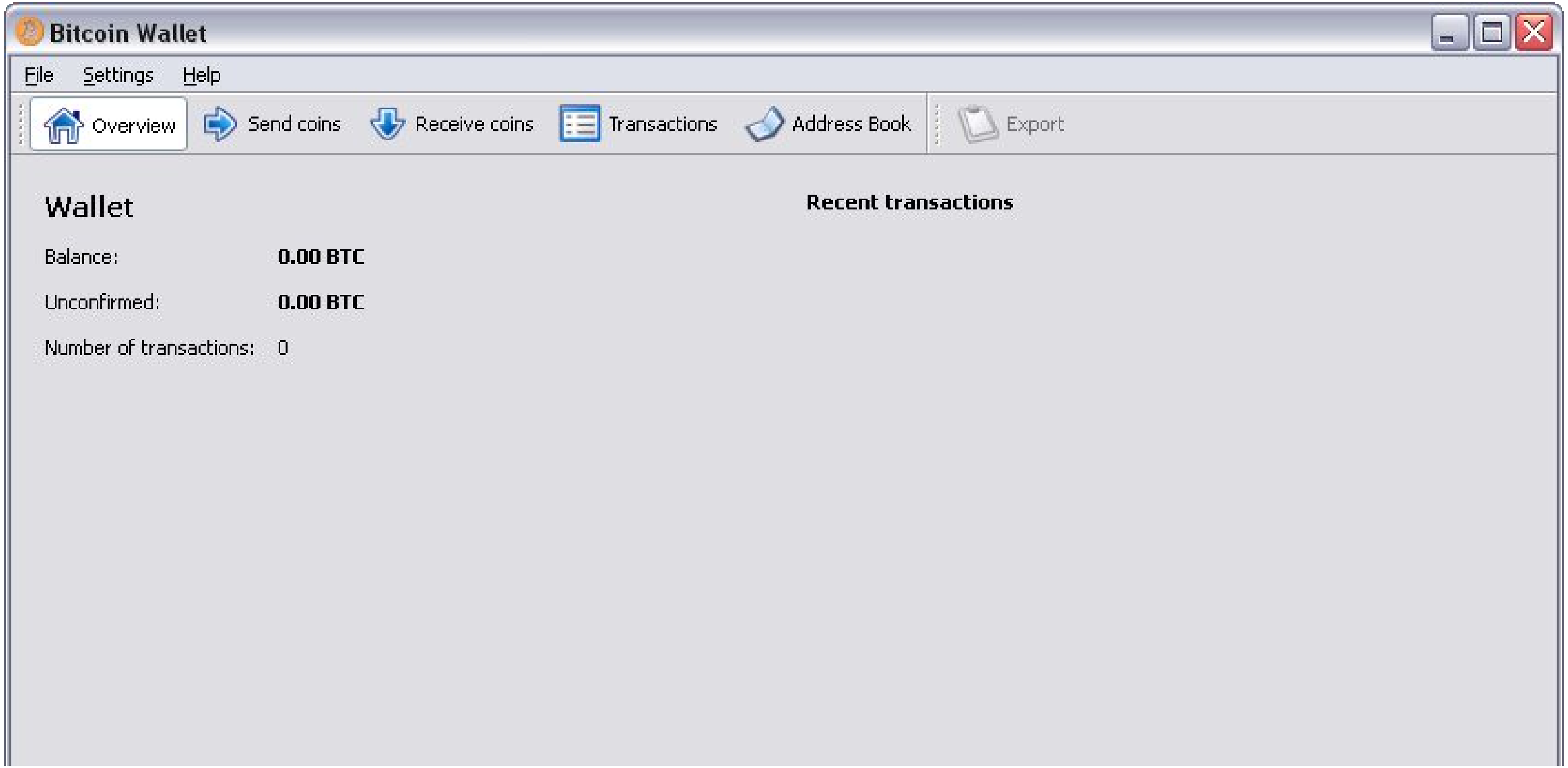
Wallet address

Transactions

Search

No transactions yet

Personal Digital Wallet



Wallet

Balance: 0.00 BTC

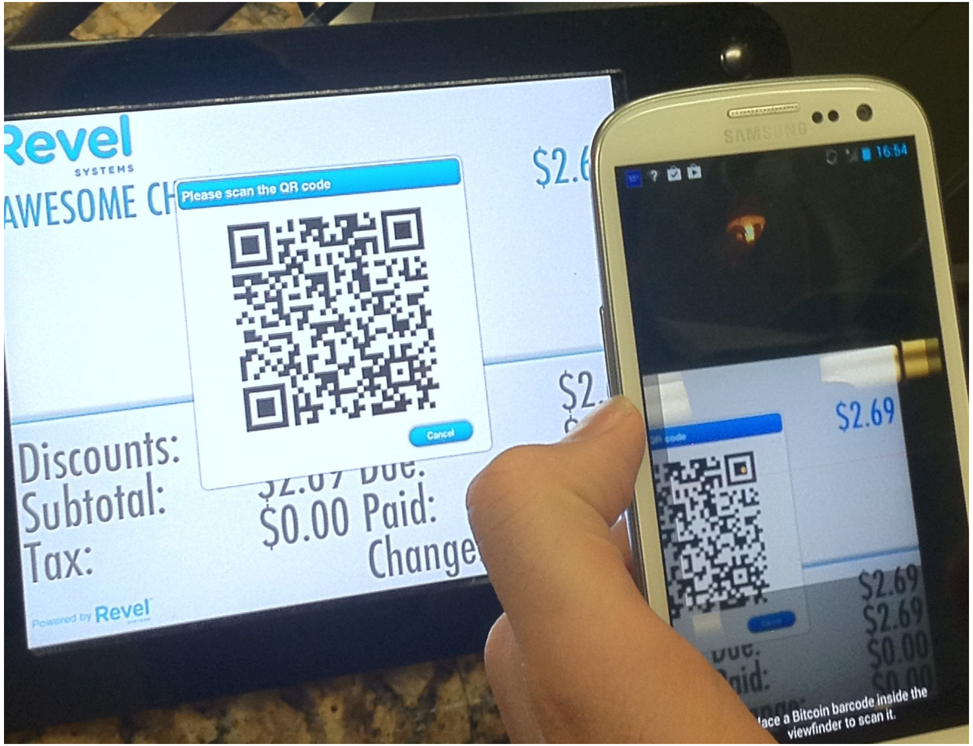
Unconfirmed: 0.00 BTC

Number of transactions: 0

Recent transactions

How to send Bitcoins?

Sending Bitcoins to someone is as simple as scanning the QR code of the receiver's public key (bitcoin address) with your smartphone.



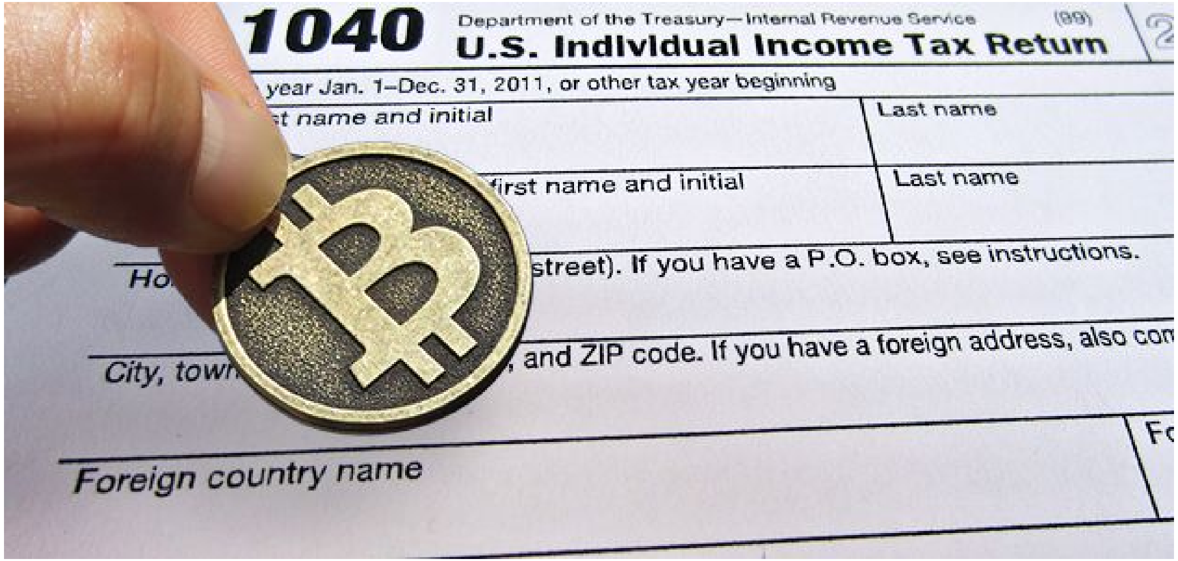
Bitcoin Alternatives

Dogecoin

Bitcoin Taxation

IRS has ruled Bitcoins as “property” not currency

If you buy and then sell Bitcoins you will have to report capital gain/loss


1040
Department of the Treasury—Internal Revenue Service
(99)
U.S. Individual Income Tax Return
year Jan. 1–Dec. 31, 2011, or other tax year beginning
st name and initial
Last name
first name and initial
Last name
Ho
street). If you have a P.O. box, see instructions.
City, town
, and ZIP code. If you have a foreign address, also com
Foreign country name
Fo

Risks with Bitcoins

- Bitcoin's value is not backed by any single government or organization.
- Like other currencies, it is worth something partly because people are willing to trade it for goods and services.
- Bitcoin exchange rate fluctuates continuously, and sometimes wildly.
- If a company kept the Bitcoins from a sale and the value dropped the revenue from bitcoin sales would drop as well.
- Bitcoin lacks wide acceptance and is vulnerable to manipulation by parties with modest funding.
- Security incidents such as website and account compromise may trigger major sell-offs.
- If a Bitcoin user loses his wallet, his money is gone forever, unless he finds it again. Those Bitcoins go completely out of circulation, rendered utterly inaccessible to anyone

The case of Mt Gox

- Bitcoin Exchange founded in 2010
- Declared bankruptcy in 2014
- Around 850,000 bitcoins belonging to customers and the company were missing and likely stolen.
- 200,000 bitcoins have since been found

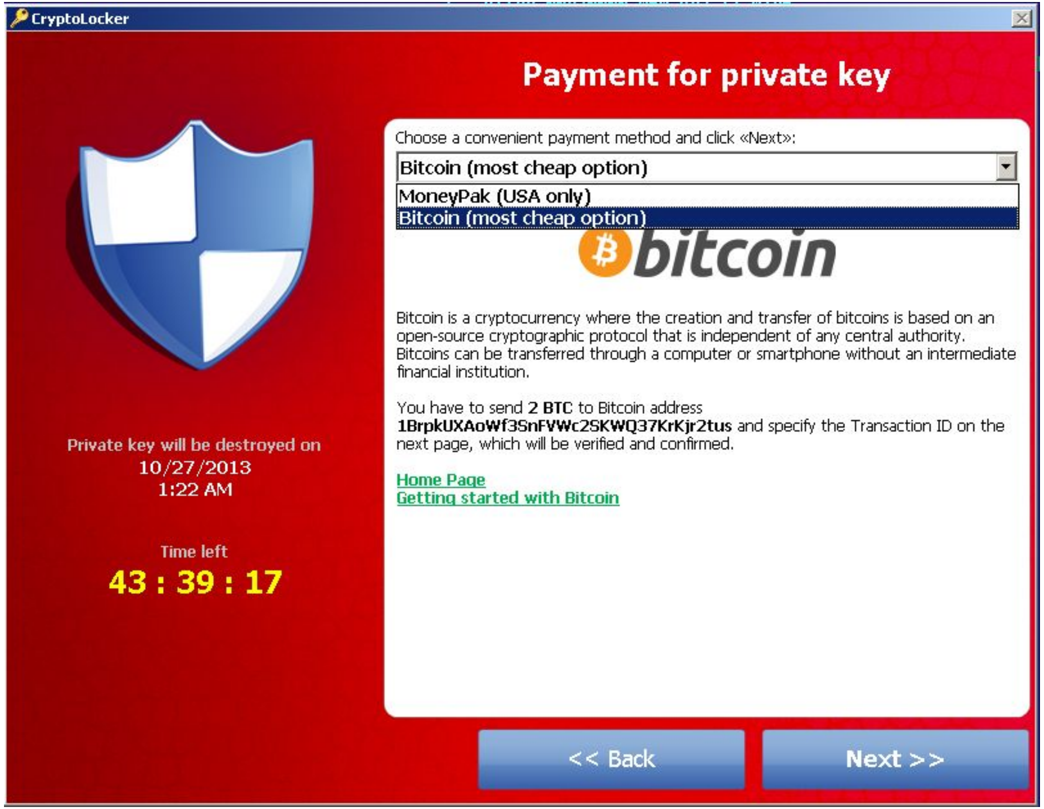
Concerns around Bitcoin - Money Laundering

Concerns around Bitcoin - Drug Trafficking

Concerns around Bitcoin - Terrorism

Concerns around Bitcoin - Consumer Protection

Concerns around Bitcoin - Ransom Payments



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

MoneyPak (USA only)
Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address **1BrpkUXAoWf3SnFVWc2SKWQ37KrKjr2tus** and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Private key will be destroyed on
10/27/2013
1:22 AM

Time left
43 : 39 : 17

Contact Information

Contact me at

Personal Email - “tohimanshu@gmail.com

Cell - 816-210-2710

Company Email - anshu.gupta@hellosign.com

LinkedIn - https://www.linkedin.com/in/anshuguptapmp

Twitter - fromanshu

Abstract

As new digital crypto currencies like BitCoin have come forth, so have been use cases where they have been used to fund and fuel criminal enterprises. This presentation “Understanding BitCoin - The fuel powering the underground economy” is intended as a technical primer for security and compliance professionals to understand the internals of “BitCoin” and be aware of the security issues in the use of digital currencies and be prepared to address any security and compliance challenges as businesses adopt the use of the digital currencies as means of payment for goods and services.

This presentation will also delve into some of the recent high profile security issues around BitCoin that have been covered in the media including Mt. Gox, Silk Road, CoinCut, BitStamp among others.

Anshu Gupta Bio

Anshu Gupta is the Director of Information Security at HelloSign, a leading eSignature company. Anshu is a long time security practitioner, having served as a trusted advisor on information security issues to Fortune 500 companies at Ernst & Young and KPMG and recently in senior security roles at Esurance and Coupa. Anshu holds the CISM, CISA, PMP and CIPP certifications.