How to Store and Use Bitcoins

- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- Online Wallets and Exchanges
- Payment Services
- Transaction Fees
- Currency Exchange Markets

How to Store and Use Bitcoins

- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- Online Wallets and Exchanges
- Payment Services
- Transaction Fees
- Currency Exchange Markets

Spending Bitcoin

Q: I want to spend a Bitcoin, what do I need to know?!

1. Some info from the public blockchain
2. The owner's secret signing key

So, it's all about key management!

Instead of

How to Store and Use Bitcoins

the title should be

How to Store and Use Secret Keys

Goals

Availability: You can spend your coins.

Security: Nobody else can spend your coins.

Convenience

Simplest Approach

Store key in a file, on your computer or phone.

Convenience: very convenient!

Availability: just as available as your device!
device lost/wiped => key lost => coins lost!

Security: just as secure as your device!
device compromised => key leaked
=> coins stolen!

Wallet Software

Keeps track of your coins.

Provides nice user interface.

Nice trick: use a separate address/key for each coin.

1. benefits privacy (looks like separate owners)
2. wallet can do the bookkeeping, user needn't know

Encoding Addresses

Encode as text string: base58 notation

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

Encode as QR code

How to Store and Use Bitcoins

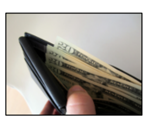
- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- Online Wallets and Exchanges
- Payment Services
- Transaction Fees
- Currency Exchange Markets

Hot Storage vs. Cold Storage

Hot storage	Cold storage
	
online	offline
convenient but risky	archival but safer

← separate keys →

Hot Storage vs. Cold Storage

Hot storage	Cold storage
	
online	offline

hot secret key(s)	payments	cold secret key(s)
cold address(es)	←→	hot address(es)

Hot Storage vs. Cold Storage

Hot storage

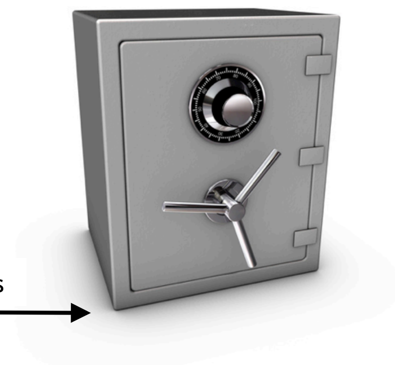
online

hot secret key(s)

cold address(es)

payments

Cold storage



offline

Dealing with Off-line Cold Wallets

Problem:

Want to use a new address (and key) for each coin sent to cold
But how can hot wallet learn new addresses if cold wallet is offline?

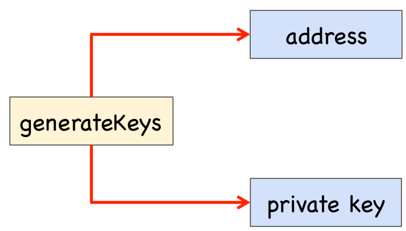
Awkward solution:

Generate a big batch of addresses/keys, transfer to hot beforehand

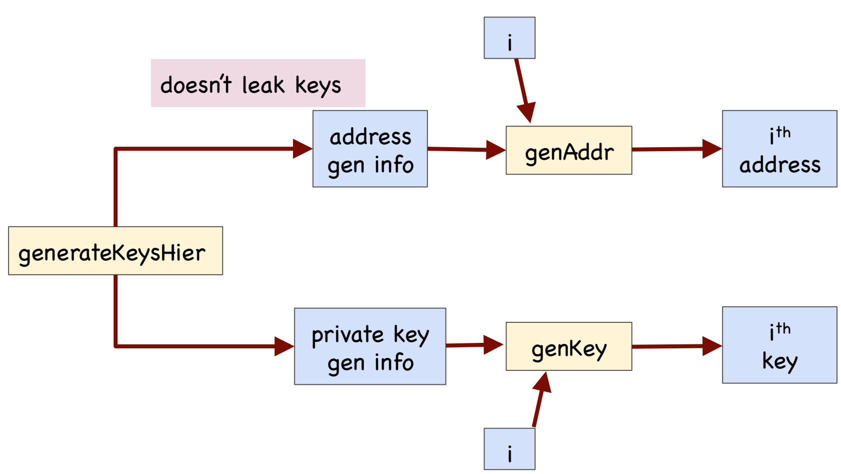
Better solution:

Hierarchical deterministic wallet

Recall: Regular Key Generation



Hierarchical Key Generation



Implementation using ECDSA

- Recall: x is private key, g^x is public key
- private key generation info (k and y are new):

  k, x, y
- i^{th} private key:

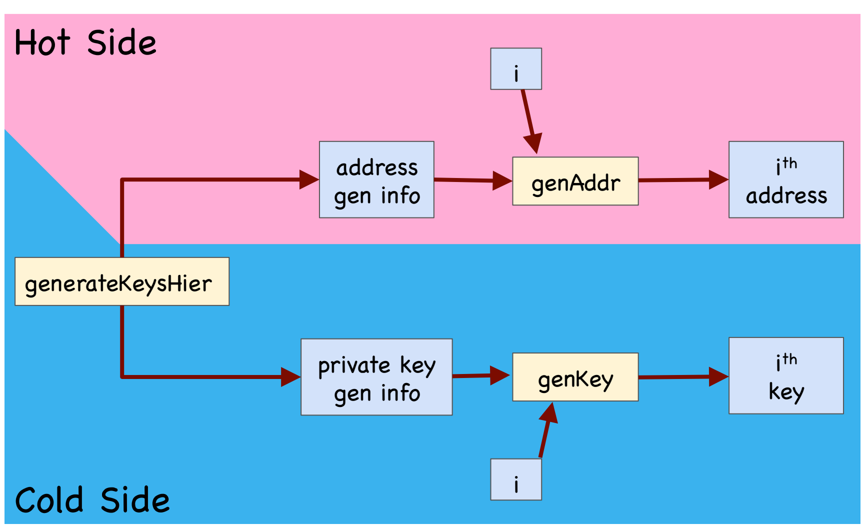
  $x_i = y + H(k \,||\, i)$
- address generation info:

  k, g^y
- i^{th} public key:

  $g^{x_i} = g^{H(k \,||\, i)} * g^y$
- i^{th} address:

  $H(g^{x_i})$

Hierarchical Key Generation



How to store Cold Info

1. Info stored in device, device locked in a safe
2. "Brain wallet"
   - encrypt info under passphrase that user remembers
3. Paper wallet
   - print info on paper,
   - lock up the paper
4. In "tamperproof" device
   - device will sign things for you, but won't divulge keys

How to Store and Use Bitcoins

- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- Online Wallets and Exchanges
- Payment Services
- Transaction Fees
- Currency Exchange Markets

Secret Sharing

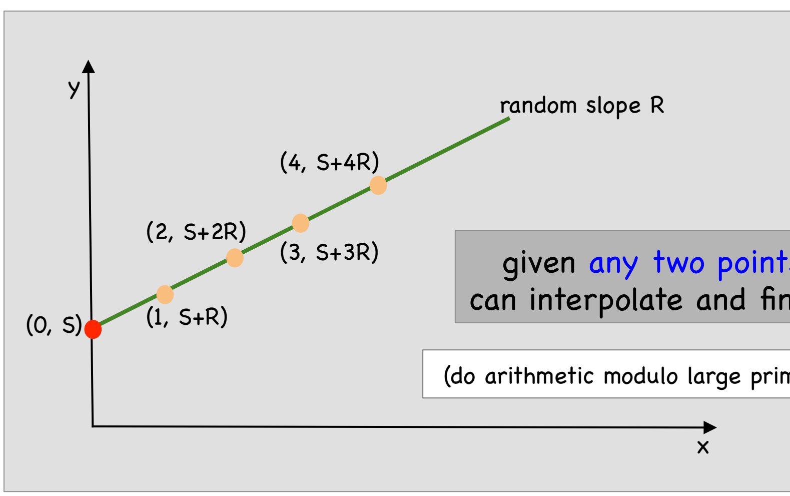
Idea: split secret into N pieces, such that
given any K pieces, can reconstruct the secret
given fewer than K pieces, don't learn anything

Example: $N=2$, $K=2$
P = a large prime
S = secret in $[0, P)$
R = random in $[0, P)$

split:
$X_1 = (S+R) \bmod P$
$X_2 = (S+2R) \bmod P$

reconstruct:
$(2X_1 - X_2) \bmod P = S$

Secret Sharing



given any two points,
can interpolate and find S

(do arithmetic modulo large prime P)

Secret Sharing

Equation	Random parameters	Points needed to recover S
$(S + RX) \bmod P$	R	2
$(S + R_1X + R_2X^2) \bmod P$	R_1, R_2	3
$(S + R_1X + R_2X^2 + R_3X^3) \bmod P$	R_1, R_2, R_3	4

etc.

support *K*-out-of-*N* splitting, for any *K*, *N*

Secret Sharing

The Good: Store shares separately, adversary must compromise several shares to get the key.

The Bad: To sign, need to bring shares together, and reconstruct the key. This is a vulnerability.

Solution! MULTI-SIG – Lets you keep shares apart, approve transaction without reconstructing key at any point.

Secret Sharing using MULTI-SIG: Example

Andrew, Bob, Charles, and Edward are co-workers.
Their company has lots of Bitcoins.

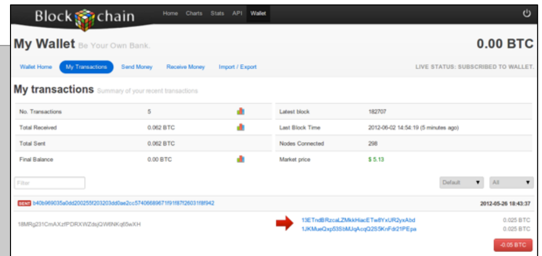
Each of the four generates a key-pair,
puts secret key in a safe, private, offline place.

The company's cold-stored coins use MULTI-SIG, so that three of the four keys must sign to release a coin.

How to Store and Use Bitcoins

- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- **Online Wallets and Exchanges**
- Payment Services
- Transaction Fees
- Currency Exchange Markets

Online Wallet



like a local wallet
but "in the cloud"

runs in your browser
site sends code
site stores keys
you log in to access wallet

Online Wallet Tradeoffs

Pros:
- convenient
- nothing to install
- works on multiple devices

Cons:
- security worries
- what if site malicious?
- what if site compromised?

Bank-like Services

You give the bank money (a "deposit").

Bank promises to pay you back later, on demand.

Bank doesn't actually keep your money in the back room.

- typically, bank invests the money
- keeps some around to meet withdrawals ("fractional reserve")

Bitcoin Exchanges

Accept deposits of Bitcoins and fiat currency ($, €, …)

Promise to pay back on demand.

Lets customers:

- Make and receive Bitcoin payments
- Buy/sell Bitcoins for fiat currency
- Typically, match up BTC buyer with BTC seller

What happens when you buy BTC

Suppose my account at Exchange holds $5000 + 3 BTC

I use Exchange to buy 2 BTC for $580 each

Result: my account holds $3840 + 5 BTC

NOTE: No BTC transaction appears on the blockchain!

Only effect: Exchange is making a different promise now.

Exchanges: Pros and Cons

Pros:

- connect BTC economy to fiat currency economy
- easy to transfer value back and forth

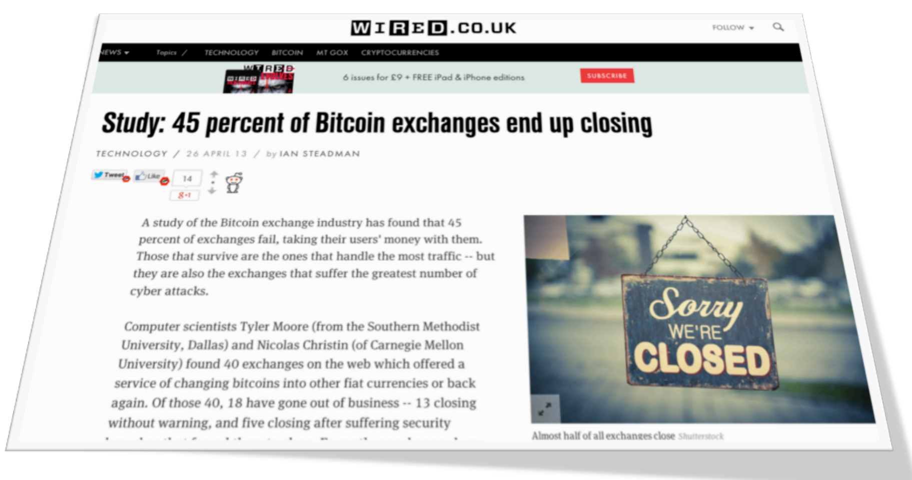
Cons:

- risk!
- same kinds of risks as banks

Exchanges and their Risks

Charles Ponzi

In fact . . .



WIRED.CO.UK

NEWS Topics / TECHNOLOGY BITCOIN MT GOX CRYPTOCURRENCIES

6 issues for £9 + FREE iPad & iPhone editions SUBSCRIBE

Study: 45 percent of Bitcoin exchanges end up closing

TECHNOLOGY / 26 APRIL 13 / by IAN STEADMAN

A study of the Bitcoin exchange industry has found that 45 percent of exchanges fail, taking their users' money with them. Those that survive are the ones that handle the most traffic -- but they are also the exchanges that suffer the greatest number of cyber attacks.

Computer scientists Tyler Moore (from the Southern Methodist University, Dallas) and Nicolas Christin (of Carnegie Mellon University) found 40 exchanges on the web which offered a service of changing bitcoins into other fiat currencies or back again. Of those 40, 18 have gone out of business -- 13 closing without warning, and five closing after suffering security

Almost half of all exchanges close Shutterstock

Bank Regulation

For traditional banks, government typically:

- Imposes **minimum reserve requirements**
  - Must hold some fraction of deposits in reserve
- **Regulates** behavior, investments
  - Insures depositors against losses
- Acts as **lender of last resort**

Bitcoin is not regulated like this!

Proof-of-Reserve Problem

Bitcoin exchanges can prove a lower bound on fractional reserve by providing:

1. Lower bound for reserves
2. Upper bound for liabilities

Proof of Reserve

Q: How to **prove** how much reserve you are holding?

1. Publish a valid **payment-to-self** of claimed amount.
2. Sign **challenge string** with same private key.

Now the hard part . . .

Proof of Liabilities

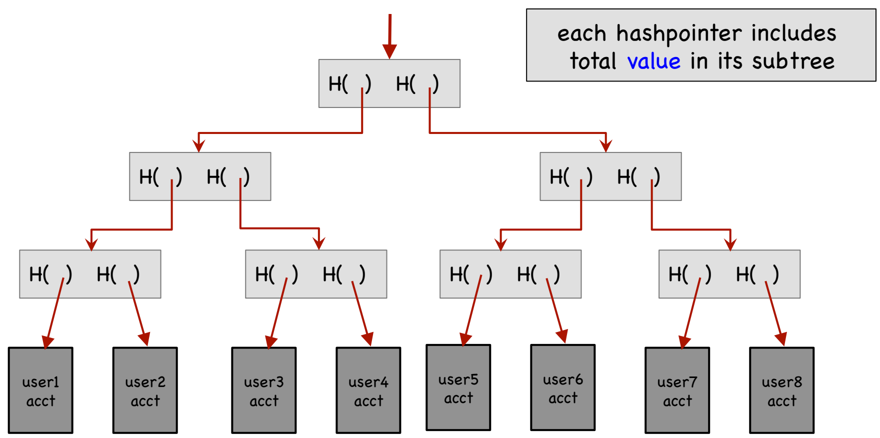
Vanilla approach:
Publish list of amounts and usernames of all accounts!

Users can complain if their accounts are missing or amounts are wrong.

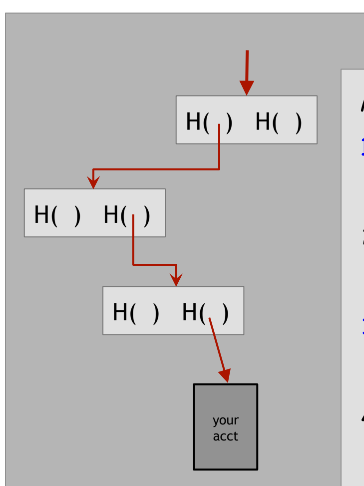
Exchange can create fake users, but this only overstates liabilities.

Problem: What about customer privacy?!!

Approach II: Merkle Tree with Subtree Totals



Are you in the Tree?



As customer you can verify that:

1. Root hash pointer and root value are what exchange published.
2. Hash pointers are consistent all the way down.
3. Leaf contains correct information (customer no. and amount)
4. Each value is sum of the values of subtrees beneath it.
5. Neither of values is negative number.

Proof of Reserve

Exchange proves that it has at least X amount of reserve currency.

Exchange proves that customers have at most Y amount deposited.

So, reserve fraction $\geq X / Y$

How to Store and Use Bitcoins

- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- Online Wallets and Exchanges
- Payment Services
- Transaction Fees
- Currency Exchange Markets

Scenario: Merchant accepts BTC

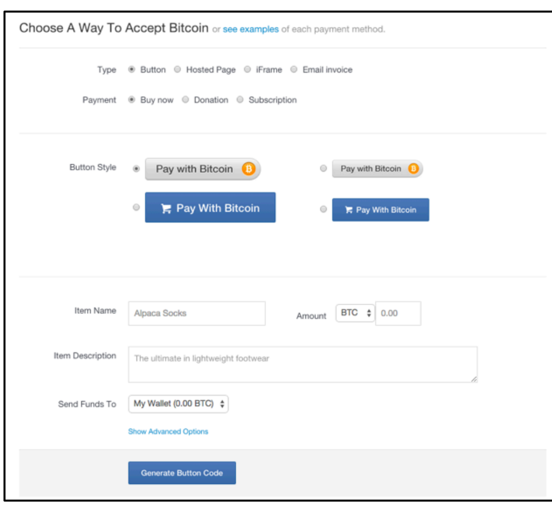
Customer objectives:

- to pay in Bitcoin

Merchant objectives:

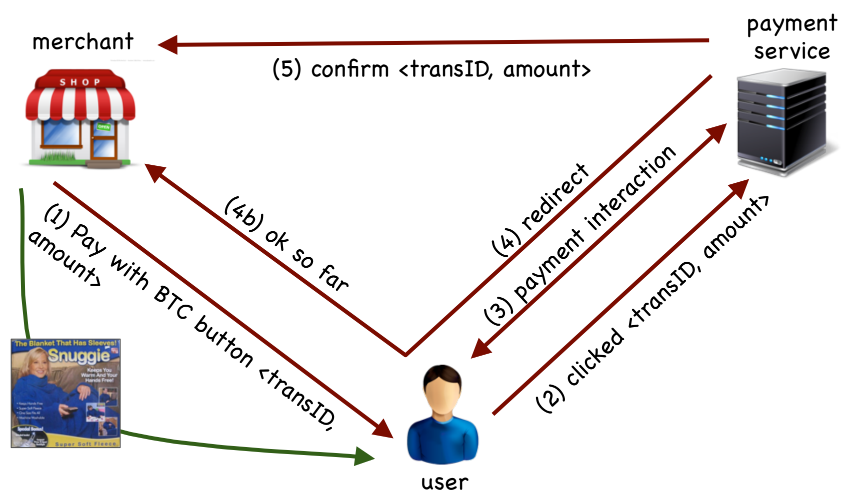
- to receive dollars
- simple deployment
- low risk (tech, security, exchange rate)

Generate pay-with-Bitcoin Button



HTML for payment button

Payment Process



End Result

Customer: pays Bitcoins

Merchant: gets dollars, minus a small percentage

Payment service:

-gets Bitcoins

-pays dollars (keeps small percentage)

-absorbs risk: security, exchange rate

-needs to exchange Bitcoins for dollars, in volume

How to Store and Use Bitcoins

- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- Online Wallets and Exchanges
- Payment Services
- Transaction Fees
- Currency Exchange Markets

Transaction Fees

It costs resources for
- Peers to relay your transaction
- Miners to record your transaction

Transaction fee compensates for (some of) these costs.

Generally, higher fee means transaction will be forwarded and recorded faster.

Consensus Fees

Current Consensus Fee

- **No fee** if
  1. tx less than 1000B in size
  2. all outputs are 0.01 BTC or larger; and
  3. priority is large enough
- Otherwise fee is **0.0001 BTC per 1000B**

Priority = (sum of inputAge * inputValue) / (tx size)

Approx tx size : $148\ N_{inputs} + 34\ N_{outputs} + 10$

Transaction Fee

Most miners enforce the consensus fee structure.

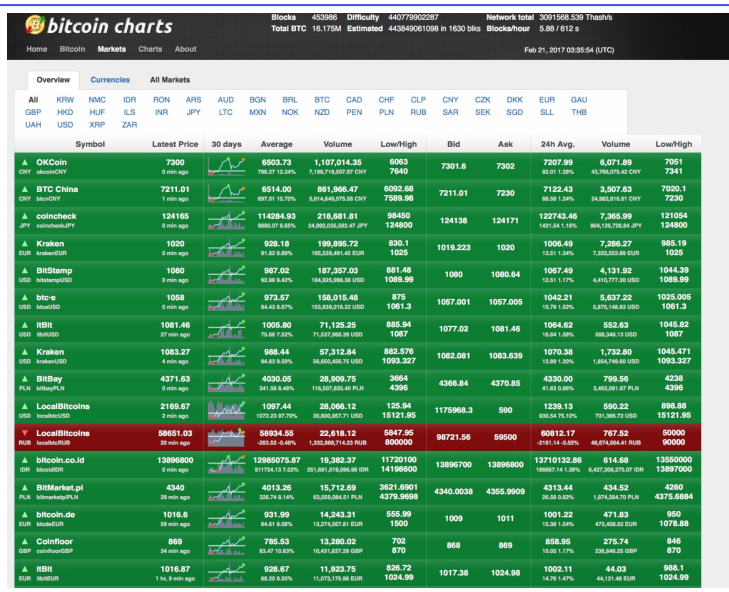
If you don't pay the consensus fee, your transaction will take longer to be recorded.

Miners prioritize transactions based on fees and the priority formula.

How to Store and Use Bitcoins

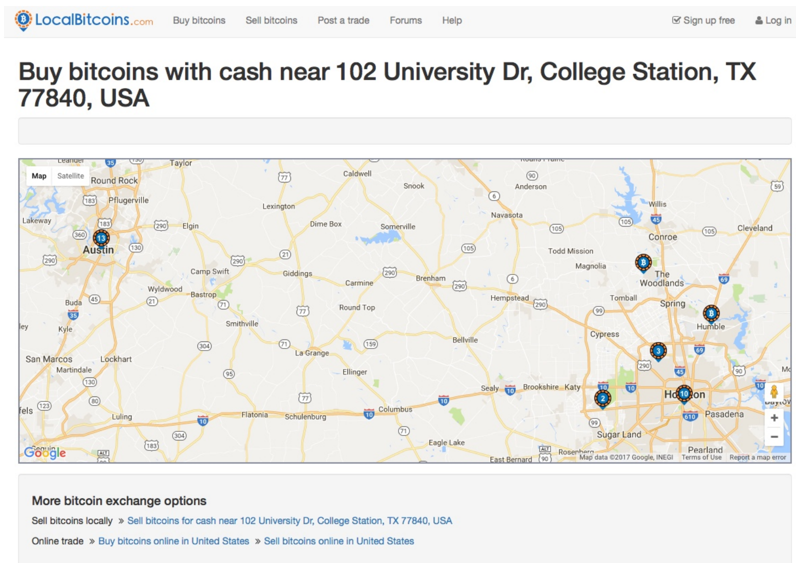
- Simple Local Storage
- Hot and Cold Storage
- Splitting and Sharing Keys
- Online Wallets and Exchanges
- Payment Services
- Transaction Fees
- Currency Exchange Markets

Markets: Examples



Symbol	Latest Price	30 days	Average	Volume	Low/High	Bid	Ask	24h Avg.	Volume	Low/High
▲ OKCoin CNY okcoinCNY	7300 0 min ago		6503.73 796.27 12.24%	1,107,014.35 7,199,719,507.97 CNY	6063 7640	7301.6	7302	7207.99 92.01 1.28%	6,071.89 43,766,075.42 CNY	7051 7341
▲ BTC China CNY btcnCNY	7211.01 1 min ago		6514.00 697.01 10.70%	861,966.47 5,614,849,575.58 CNY	6092.68 7589.98	7211.01	7230	7122.43 88.58 1.24%	3,507.63 24,982,816.81 CNY	7020.1 7230
▲ coincheck JPY coincheckJPY	124165 0 min ago		114284.93 9880.07 8.65%	218,681.81 24,992,035,582.47 JPY	98450 124800	124138	124171	122743.46 1421.54 1.16%	7,365.99 904,126,728.84 JPY	121054 124800
▲ Kraken EUR krakenEUR	1020 0 min ago		928.18 91.82 9.89%	199,895.72 185,539,491.45 EUR	830.1 1025	1019.223	1020	1006.49 13.51 1.34%	7,286.27 7,333,553.89 EUR	985.19 1025
▲ BitStamp USD bitstampUSD	1080 0 min ago		987.02 92.98 9.42%	187,357.03 184,925,998.38 USD	881.48 1089.99	1080	1080.64	1067.49 12.51 1.17%	4,131.92 4,410,777.30 USD	1044.39 1089.99
▲ btc-e USD btceUSD	1058 0 min ago		973.57 84.43 8.67%	158,015.48 153,839,218.22 USD	875 1061.3	1057.001	1057.005	1042.21 15.79 1.52%	5,637.22 5,875,148.83 USD	1025.005 1061.3
▲ itBit USD itbitUSD	1081.46 27 min ago		1005.80 75.66 7.52%	71,125.25 71,537,988.39 USD	885.94 1087	1077.02	1081.46	1064.62 16.84 1.58%	552.63 588,346.13 USD	1045.82 1087
▲ Kraken USD krakenUSD	1083.27 4 min ago		988.44 94.83 9.59%	57,312.84 56,650,456.75 USD	882.576 1093.327	1082.081	1083.639	1070.38 12.89 1.20%	1,732.80 1,854,749.60 USD	1045.471 1093.327
▲ BitBay PLN bitbayPLN	4371.63 0 min ago		4030.05 341.58 8.48%	28,909.75 116,507,835.40 PLN	3664 4396	4366.84	4370.85	4330.00 41.63 0.96%	799.56 3,462,081.67 PLN	4238 4396
▲ LocalBitcoins USD localbtcUSD	2169.67 2 min ago		1097.44 1072.23 97.70%	28,066.12 30,800,957.71 USD	125.94 15121.95	1175968.3	590	1239.13 930.54 75.10%	590.22 731,366.72 USD	898.88 15121.95
▼ LocalBitcoins RUB localbtcRUB	58651.03 20 min ago		58934.55 -283.52 -0.48%	22,618.12 1,332,988,714.23 RUB	5847.95 800000	98721.56	59500	60812.17 -2161.14 -3.55%	767.52 46,674,564.41 RUB	50000 90000
▲ bitcoin.co.id IDR btcoidIDR	13896800 0 min ago		12985075.87 911724.13 7.02%	19,382.37 251,681,519,096.98 IDR	11720100 14198600	13896700	13896800	13710132.86 186667.14 1.36%	614.68 8,427,308,275.07 IDR	13550000 13897000
▲ BitMarket.pl PLN bitmarketplPLN	4340 29 min ago		4013.26 326.74 8.14%	15,712.69 63,059,084.51 PLN	3621.6901 4379.9698	4340.0038	4355.9909	4313.44 26.56 0.62%	434.52 1,874,284.70 PLN	4260 4375.6884
▲ bitcoin.de EUR btcdeEUR	1016.6 59 min ago		931.99 84.61 9.08%	14,243.31 13,274,567.81 EUR	555.99 1500	1009	1011	1001.22 15.38 1.54%	471.83 472,408.50 EUR	950 1078.88
▲ Coinfloor GBP coinfloorGBP	869 34 min ago		785.53 83.47 10.63%	13,280.02 10,431,837.29 GBP	702 870	868	869	858.95 10.05 1.17%	275.74 236,846.25 GBP	846 870
▲ itBit EUR itbitEUR	1016.87 1 hr, 9 min ago		928.67 88.20 9.50%	11,923.75 11,073,175.96 EUR	826.72 1024.99	1017.38	1024.98	1002.11 14.76 1.47%	44.03 44,121.48 EUR	988.1 1024.99

Buy/Sell Bitcoins



Or . . .

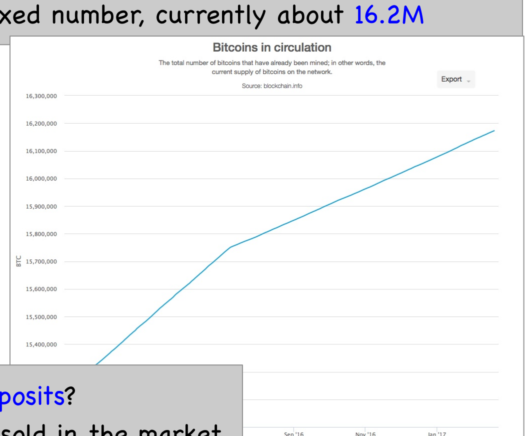
Basic Market Dynamics

- Market matches buyer and seller
- Large, liquid market reaches a consensus price
- Price set by supply (of BTC) and demand (for BTC)

Supply of Bitcoins

supply = coins in circulation (+ demand deposits?)

coins in circulation: fixed number, currently about 16.2M



When to include demand deposits?
When they can actually be sold in the market.

Demand for Bitcoins

BTC demanded to mediate fiat-currency transactions

1. Alice buys BTC for $
2. Alice sends BTC to Bob
3. Bob sells BTC for $

BTC "out of circulation" during this time

BTC demanded as an investment

if the market thinks demand will go up in future

Simple Model of Transaction-Demand

T = total transaction value mediated via BTC ($ / sec)

D = duration that BTC is needed by a transaction (sec)

S = supply of BTC (not including BTC held as long-term investments)

$\frac{S}{D}$ Bitcoins become available per second

$\frac{T}{P}$ Bitcoins needed per second

Equilibrium:

$P = \frac{TD}{S}$