How to Store and Use Bitcoins

Simple Local Storage

To spend a Bitcoin, you need to know:

* some info from the public blockchain, and
* the owner’s secret signing key

So it’s all about key management.

How to Store and Use ~~Bitcoins~~ Secret Keys

Goals

availability: You can spend your coins.

security: Nobody else can spend your coins.

Convenience: Key management should be relativeloy easy.

Simplest approach: store key in a file,

on your computer or phone

Very convenient.

As available as your device.

device lost/wiped ⇒ key lost ⇒ coins lost

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.

benefits privacy (looks like separate owners)

wallet can do the bookkeeping, user needn’t know

Encoding addresses

Encode as text string: base58 notation

```
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz
```

or use QR code

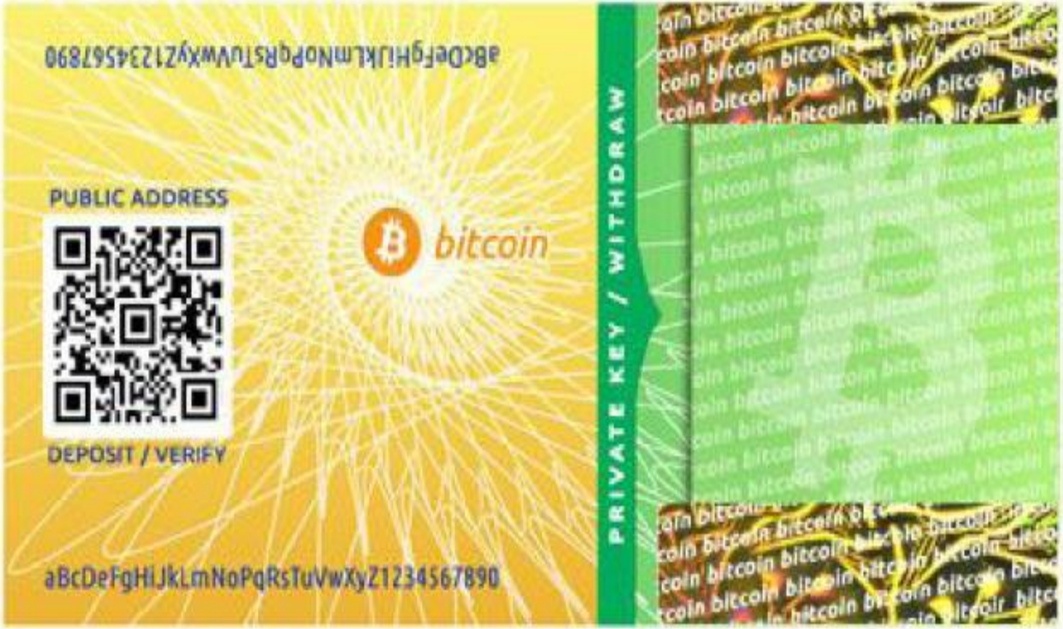

aBcDeFgHiJkLmNoPqRsTuVwXyZ1234567890
PUBLIC ADDRESS
bitcoin
DEPOSIT / VERIFY
aBcDeFgHiJkLmNoPqRsTuVwXyZ1234567890
PRIVATE KEY / WITHDRAW

Figure 4.3: A Bitcoin paper wallet with the public key encoded both as a 2D barcode and in base 58 notation. Observe that the private key is behind a tamper-evident seal.

Hot and Cold Storage

Hot storage

online

convenient but risky

Cold storage

offline

archival but safer

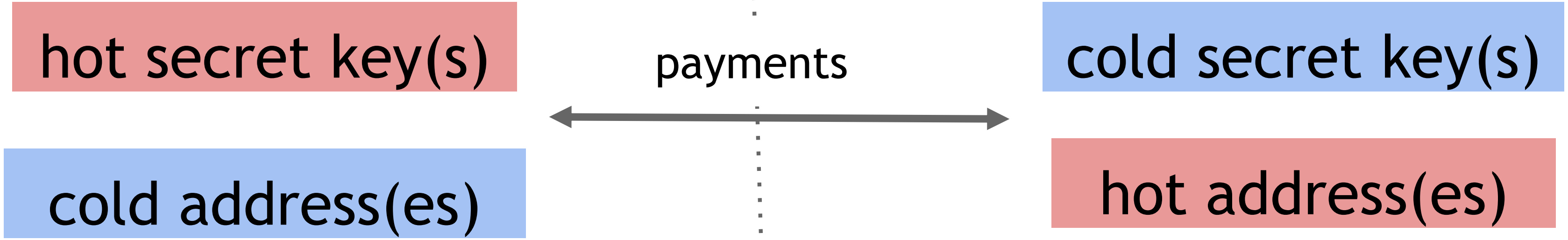
separate keys

Hot storage

online

Cold storage

offline



hot secret key(s)

cold address(es)

payments

cold secret key(s)

hot address(es)

Hot storage

online

hot secret key(s)

cold address(es)

payments

Cold storage

offline

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?

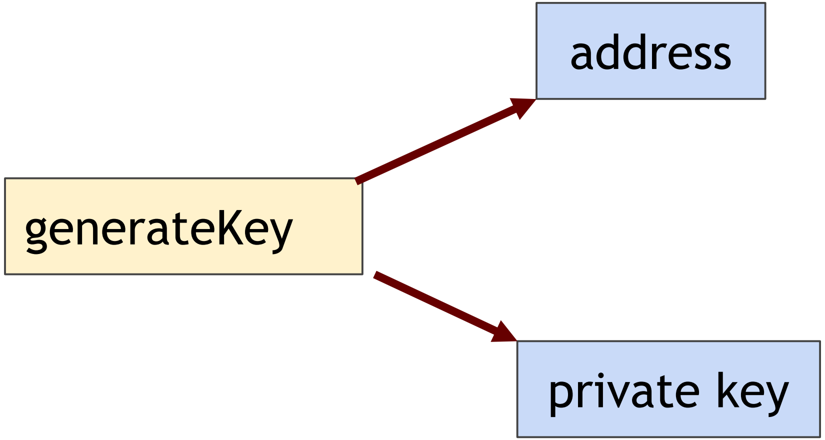
Awkward solution:

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

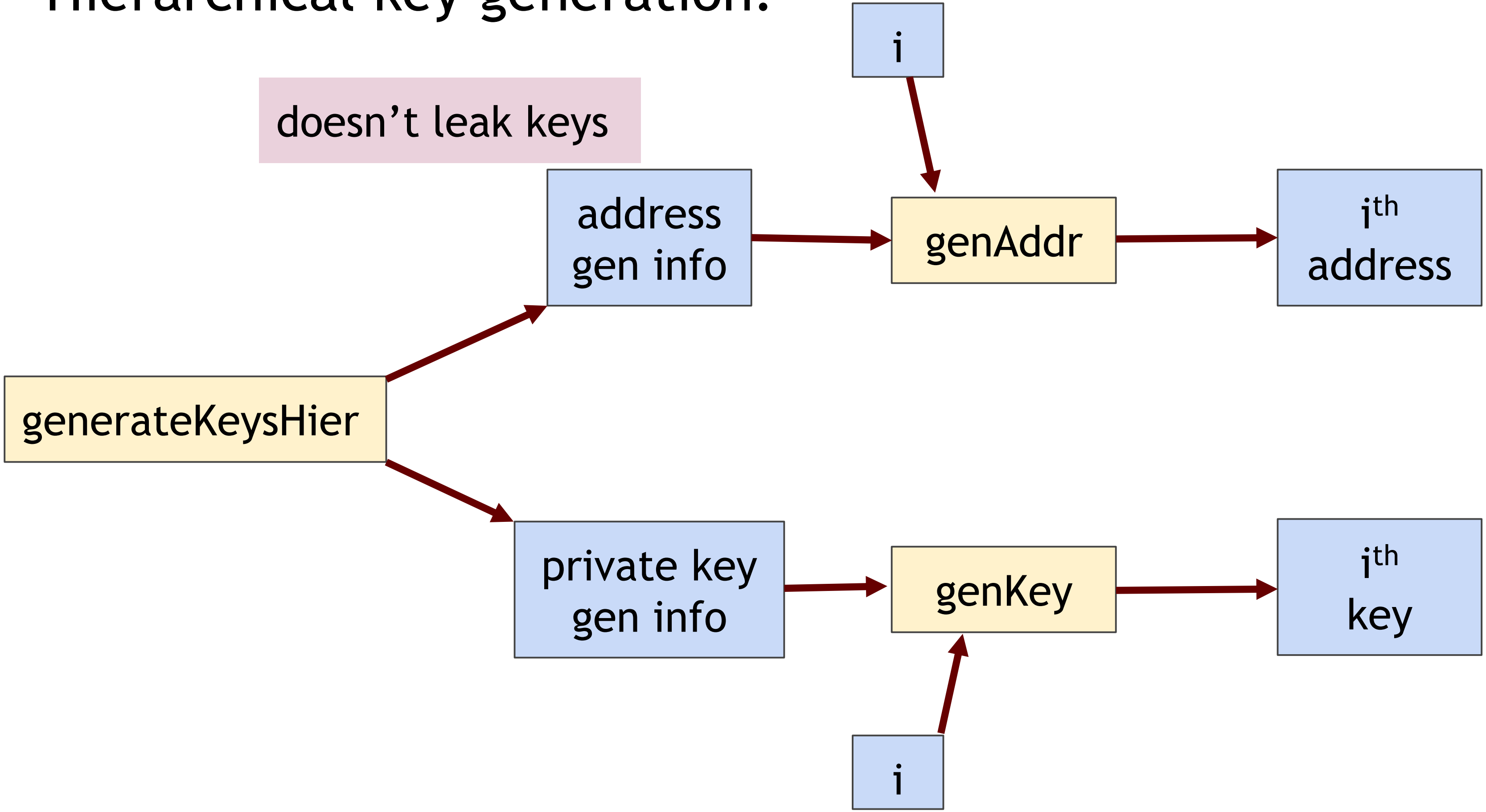
Better solution:

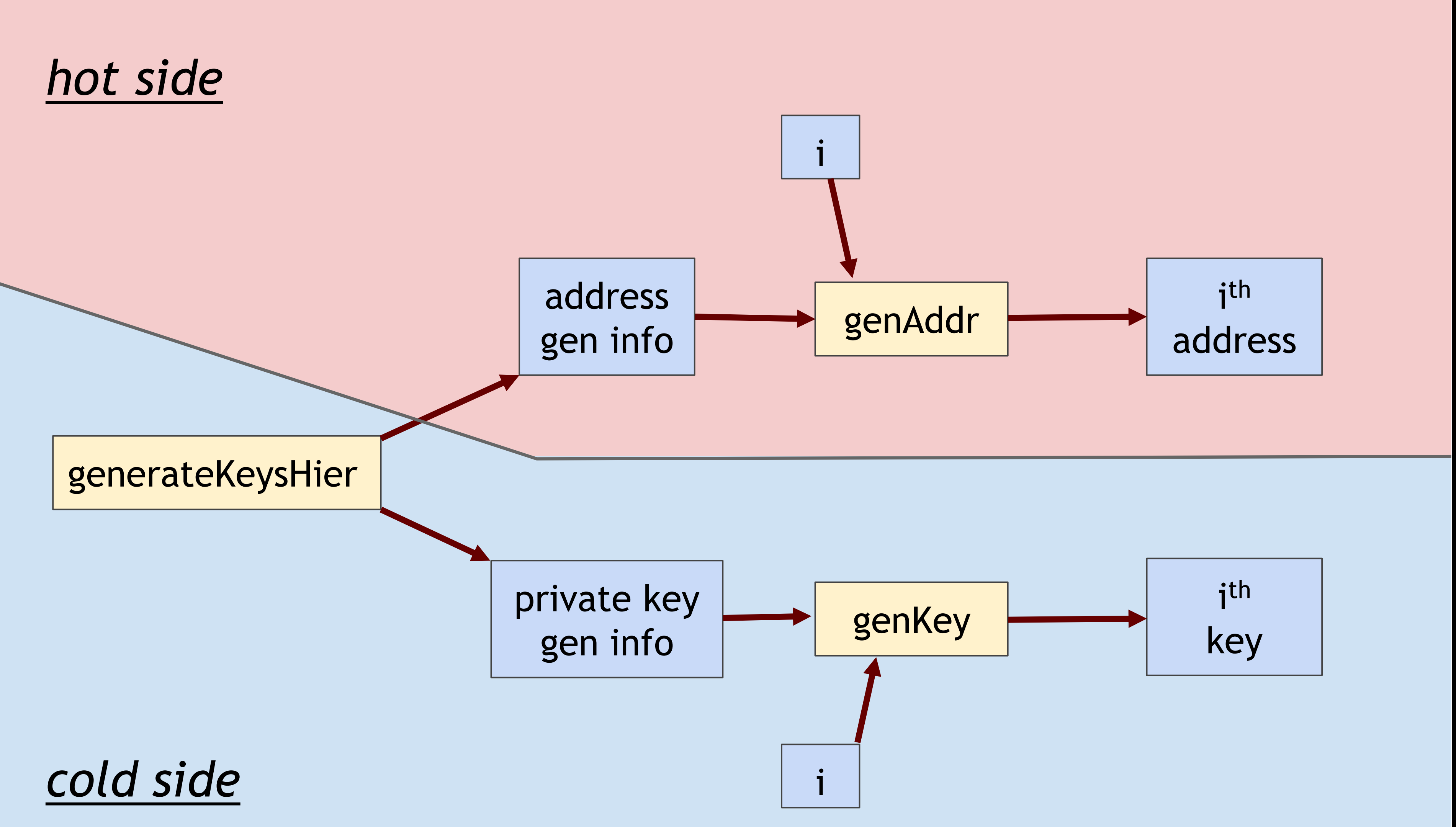
Hierarchical wallet

Regular key generation:



Hierarchical key generation:





hot side

i

address gen info

genAddr

ith address

generateKeysHier

private key gen info

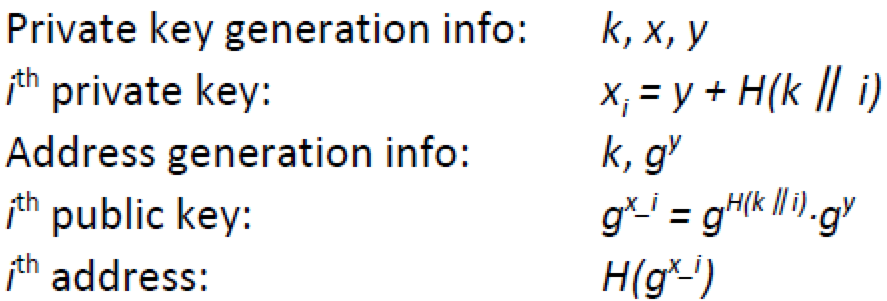
genKey

ith key

i

cold side

ECDSA hierarchical key generation Scheme



Private key generation info:	k, x, y
i^{th} private key:	$x_i = y + H(k \parallel i)$
Address generation info:	k, g^y
i^{th} public key:	$g^{x\_i} = g^{H(k \parallel i)} \cdot g^y$
i^{th} address:	$H(g^{x\_i})$

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

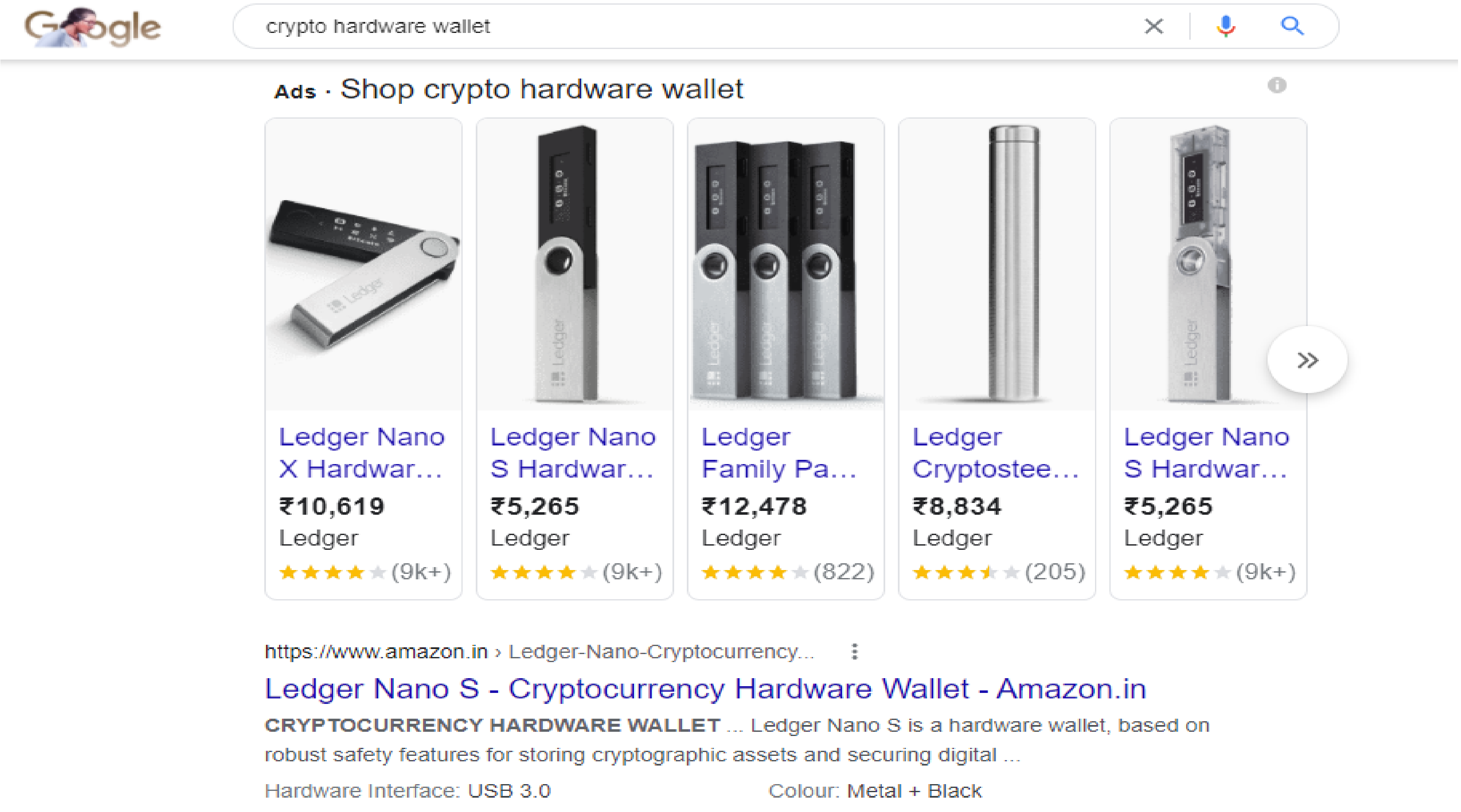
(3) Paper wallet

print info on paper,

lock up the paper

(4) In “tamperproof” device

device will sign things for you, but won’t divulge keys



Ads · Shop crypto hardware wallet

Product	Price	Seller	Rating
Ledger Nano X Hardwar…	₹10,619	Ledger	★★★★☆ (9k+)
Ledger Nano S Hardwar…	₹5,265	Ledger	★★★★☆ (9k+)
Ledger Family Pa…	₹12,478	Ledger	★★★★☆ (822)
Ledger Cryptostee…	₹8,834	Ledger	★★★½☆ (205)
Ledger Nano S Hardwar…	₹5,265	Ledger	★★★★☆ (9k+)

https://www.amazon.in › Ledger-Nano-Cryptocurrency...

Ledger Nano S - Cryptocurrency Hardware Wallet - Amazon.in

CRYPTOCURRENCY HARDWARE WALLET ... Ledger Nano S is a hardware wallet, based on robust safety features for storing cryptographic assets and securing digital ...

Hardware Interface: USB 3.0 Colour: Metal + Black

Splitting and Sharing Keys

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)

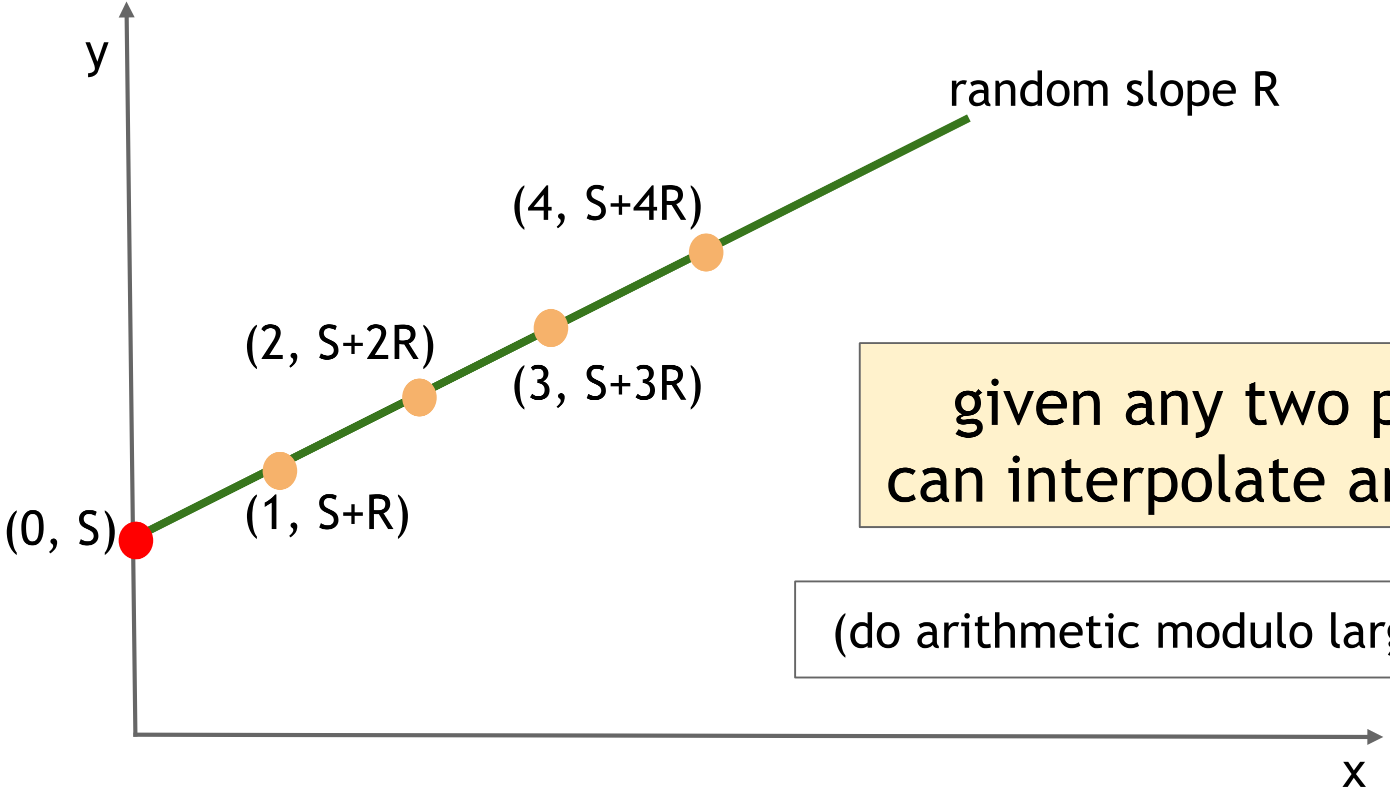
R = random in [0, P)

split:

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

reconstruct:

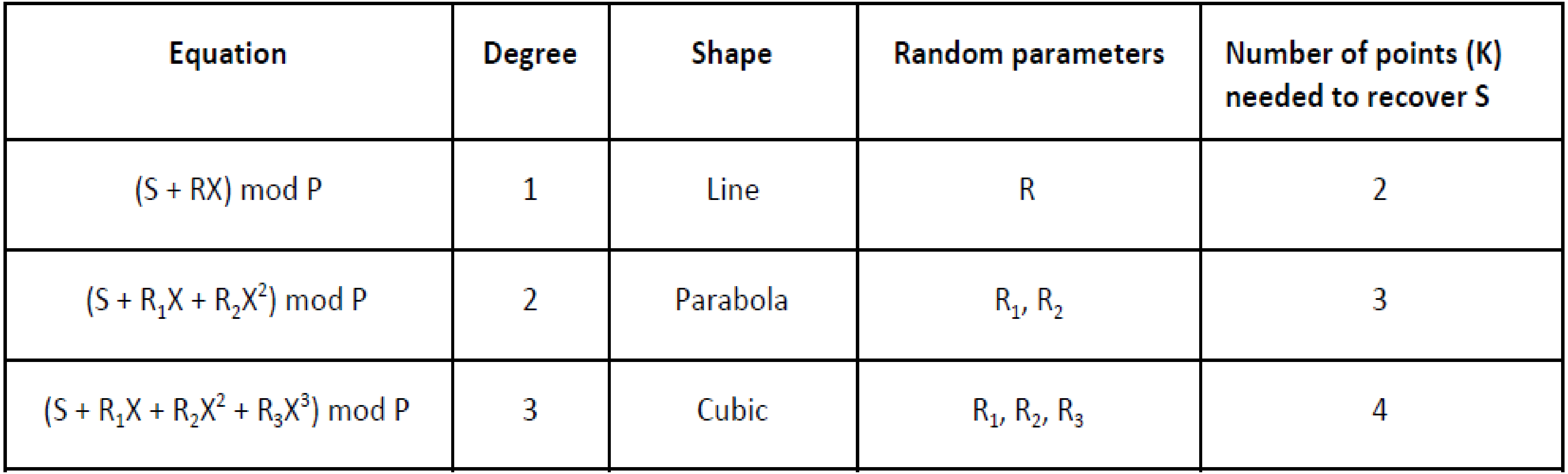
$(2X_1 - X_2) \bmod P = S$



given any two points,
can interpolate and find S

(do arithmetic modulo large prime P)

Secret sharing



Equation	Degree	Shape	Random parameters	Number of points (K) needed to recover S
$(S + RX) \bmod P$	1	Line	R	2
$(S + R_1X + R_2X^2) \bmod P$	2	Parabola	R_1, R_2	3
$(S + R_1X + R_2X^2 + R_3X^3) \bmod P$	3	Cubic	R_1, R_2, R_3	4

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

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

Bad: To sign, need to bring shares together, reconstruct the key. $\Leftarrow$ vulnerable

Multi-sig

Recall multi-sig.

Lets you keep shares apart, approve transaction without reconstructing key at any point.

Example

Andrew, Arvind, Ed, and Joseph 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.

Online Wallets and Exchanges

Online wallet

2015 Popular Wallet: Coinbase and Blockchain.info

like a local wallet

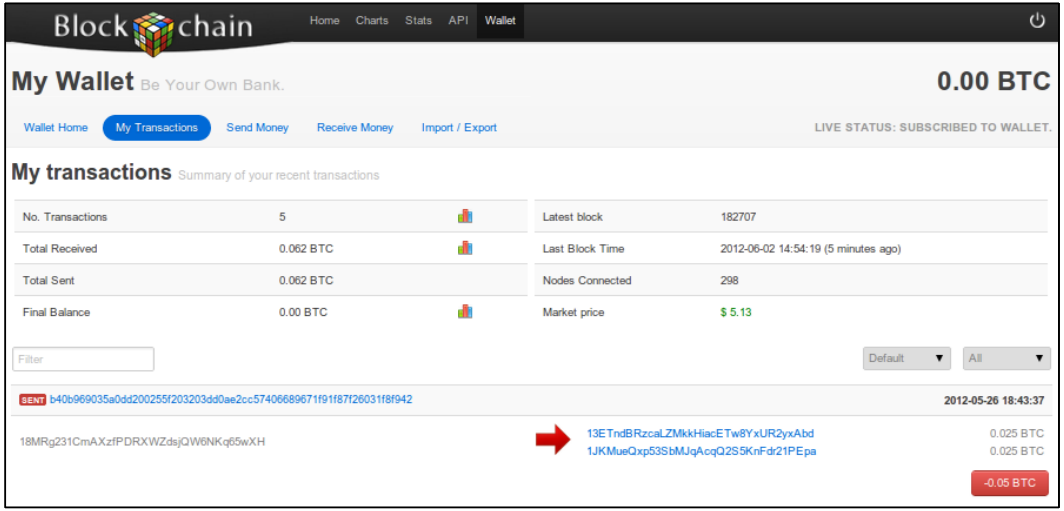
but “in the cloud”

runs in your browser

site sends code

site stores keys

you log in to access wallet



My Wallet Be Your Own Bank. 0.00 BTC

LIVE STATUS: SUBSCRIBED TO WALLET.

My transactions Summary of your recent transactions

No. Transactions	5	Latest block	182707
Total Received	0.062 BTC	Last Block Time	2012-06-02 14:54:19 (5 minutes ago)
Total Sent	0.062 BTC	Nodes Connected	298
Final Balance	0.00 BTC	Market price	$ 5.13

SENT b40b969035a0dd200255f203203dd0ae2cc57406689671f91f87f26031f8f942 2012-05-26 18:43:37

18MRg231CmAXzfPDRXWZdsjQW6NKq65wXH → 13ETndBRzcaLZMkkHiacETw8YxUR2yxAbd 0.025 BTC
1JKMueQxp53SbMJqAcqQ2S5KnFdr21PEpa 0.025 BTC

-0.05 BTC

Online wallet tradeoffs

convenient: nothing to install, works on multiple devices

but security worries

vulnerable if site is malicious or compromised

ideally, site is run by security professionals

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

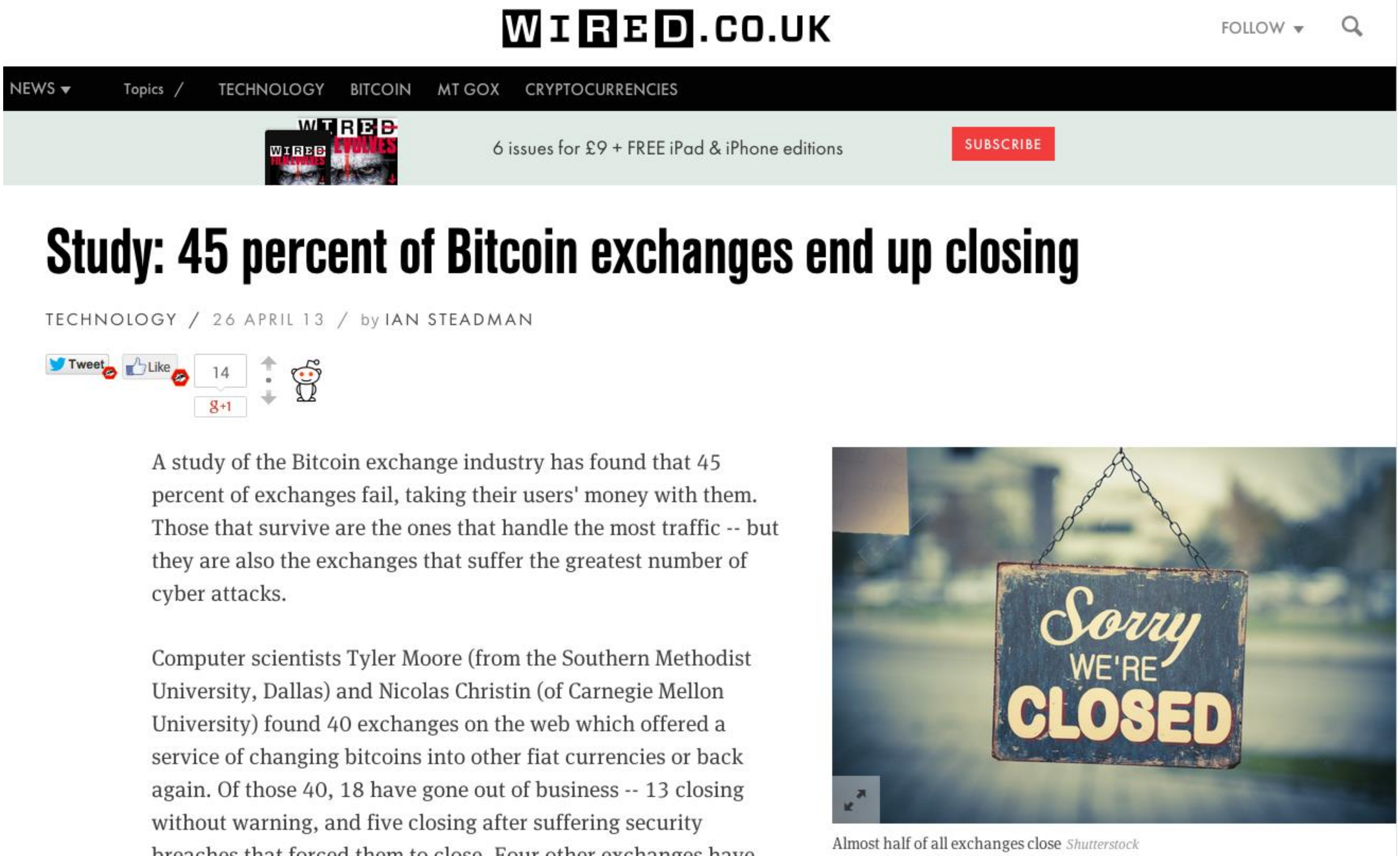
Exchanges: Pros and Cons

pro: connects BTC economy to fiat currency economy

- easy to transfer value back and forth

con: risk

- same kinds of risks as banks
  - Risk of Bank Run
  - Bank Owner running Fraud Scheme
  - Security Attack- Hacking the stored secrets



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 breaches that forced them to close. Four other exchanges have

Almost half of all exchanges close *Shutterstock*

東京でMT.GOXのデモ
へ参加してください。
東京都渋谷区渋谷
2丁目１１−５
MTGox
WHERE IS
OUR MONEY

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

Proof of Reserve

Bitcoin exchange can prove it has fractional reserve.

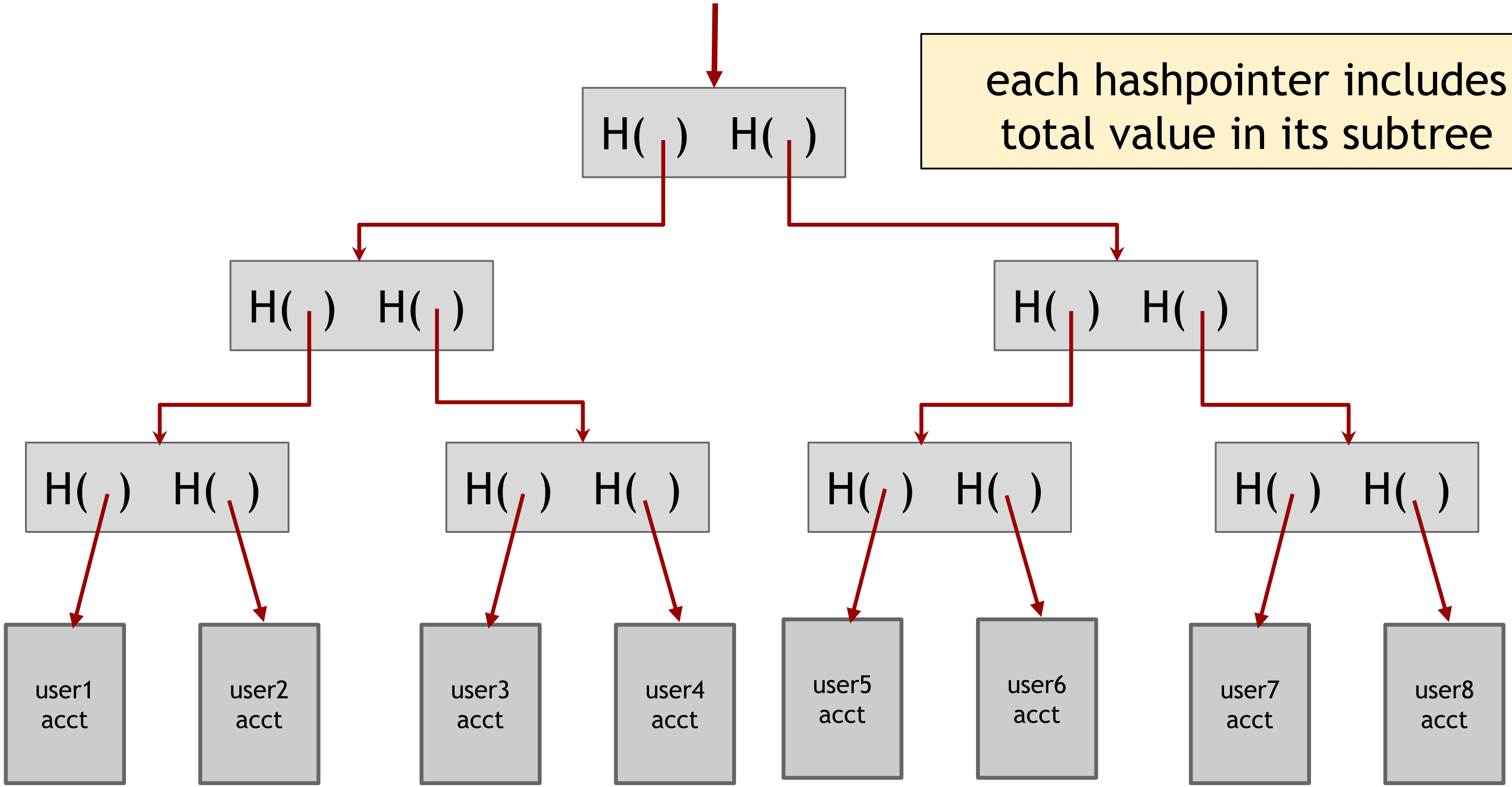
- fraction can be 100%

Prove how much reserve you're holding:

- publish valid payment-to-self of that amount
- sign a challenge string with the same private key

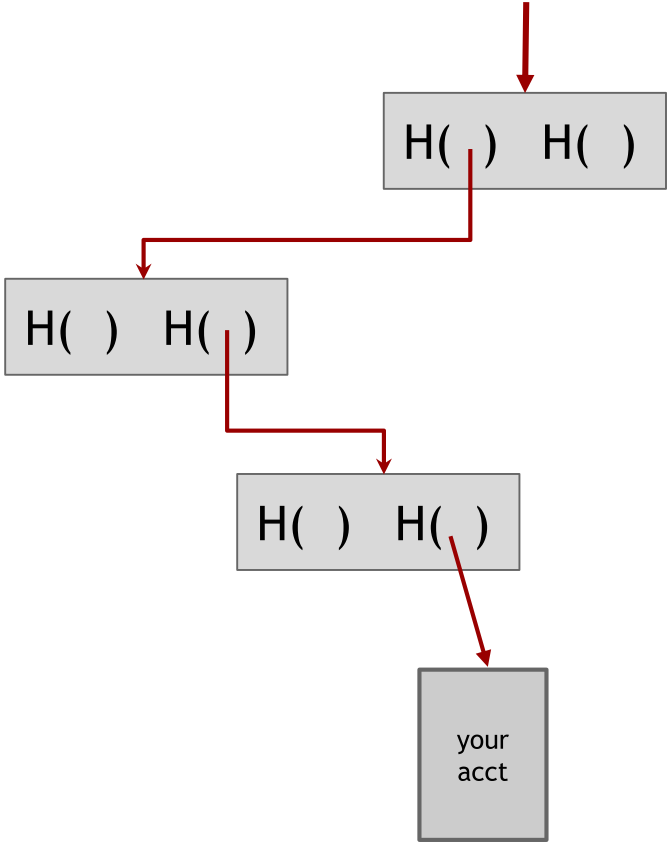
Prove how many demand deposits you hold: …

Merkle tree with subtree totals

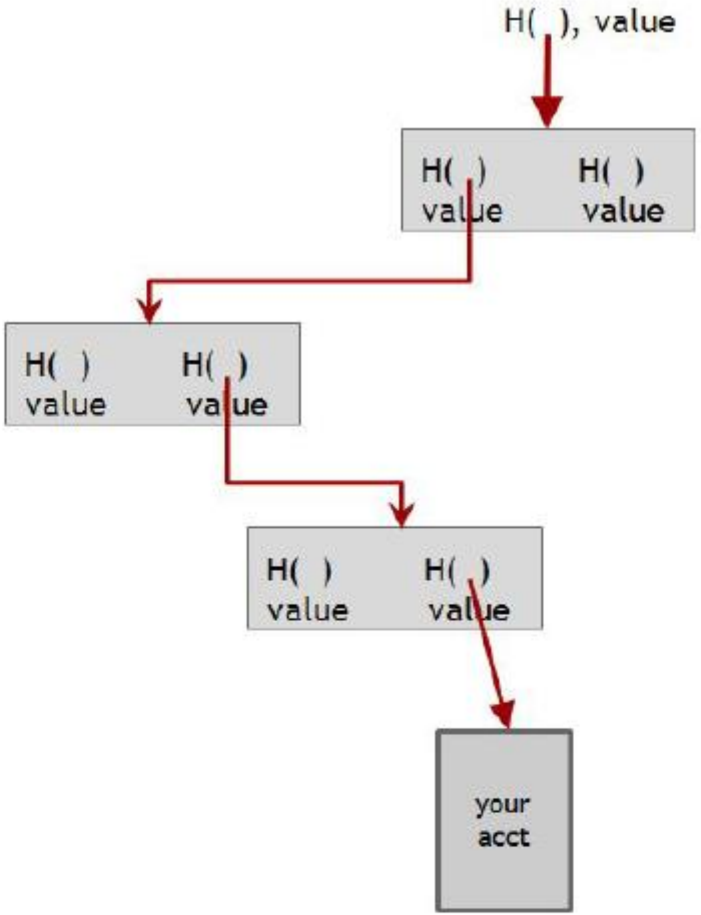


each hashpointer includes total value in its subtree

Checking that you're represented in the tree



show O(log n) items


H( ), value
H( )
value
H( )
value
H( )
value
H( )
value
H( )
value
H( )
value
your
acct

Proof of Reserve

Prove that you have at least X amount of reserve currency

Prove that customers have at most Y amount deposited

So reserve fraction ≥ X / Y

Payment Services

Scenario: merchant accepts BTC

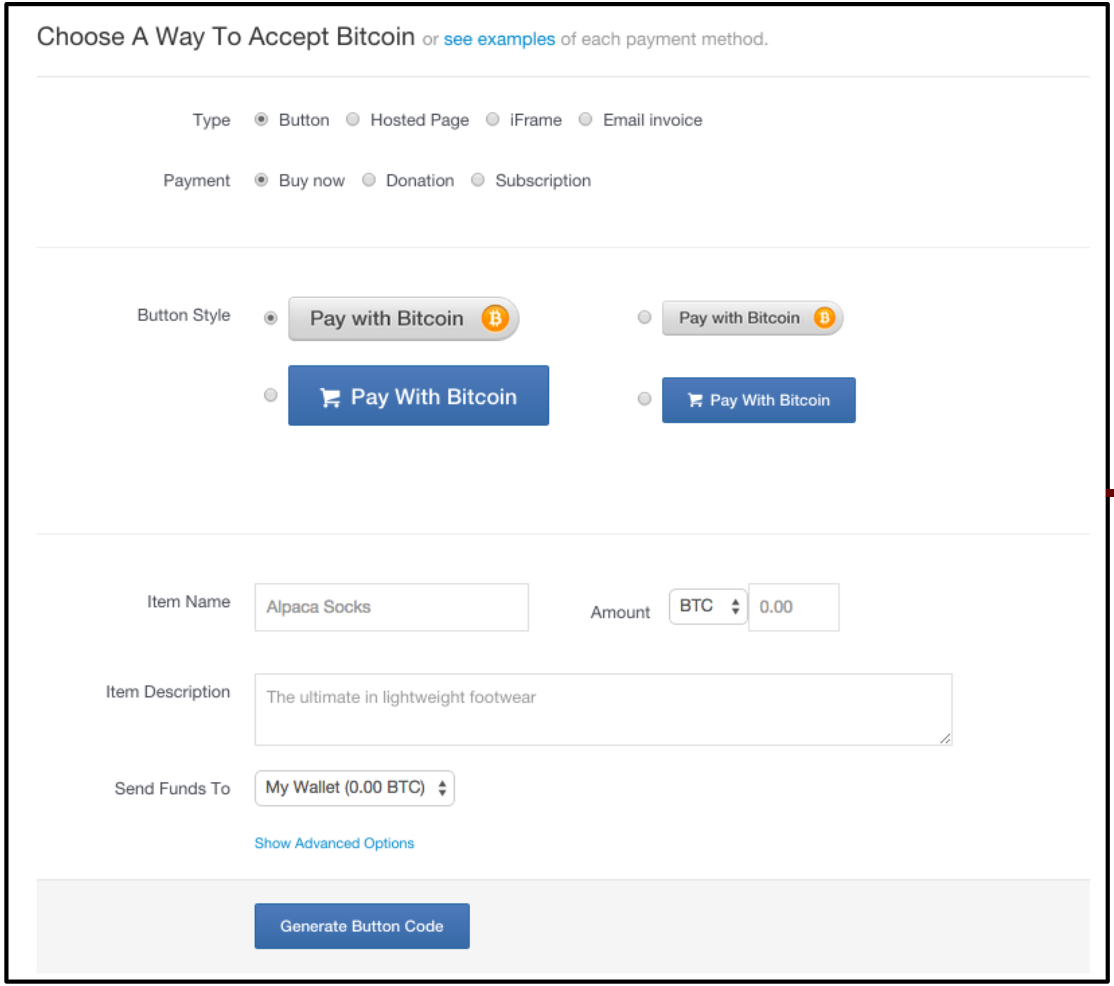
customer wants: to pay with Bitcoin

merchant wants:

* to receive dollars

* simple deployment

* low risk (tech risk, security risk, exchange rate risk)



Choose A Way To Accept Bitcoin or see examples of each payment method.

Type ● Button ○ Hosted Page ○ iFrame ○ Email invoice

Payment ● Buy now ○ Donation ○ Subscription

Button Style ● Pay with Bitcoin ○ Pay with Bitcoin ○ Pay With Bitcoin ○ Pay With Bitcoin

Item Name: Alpaca Socks

Amount: BTC 0.00

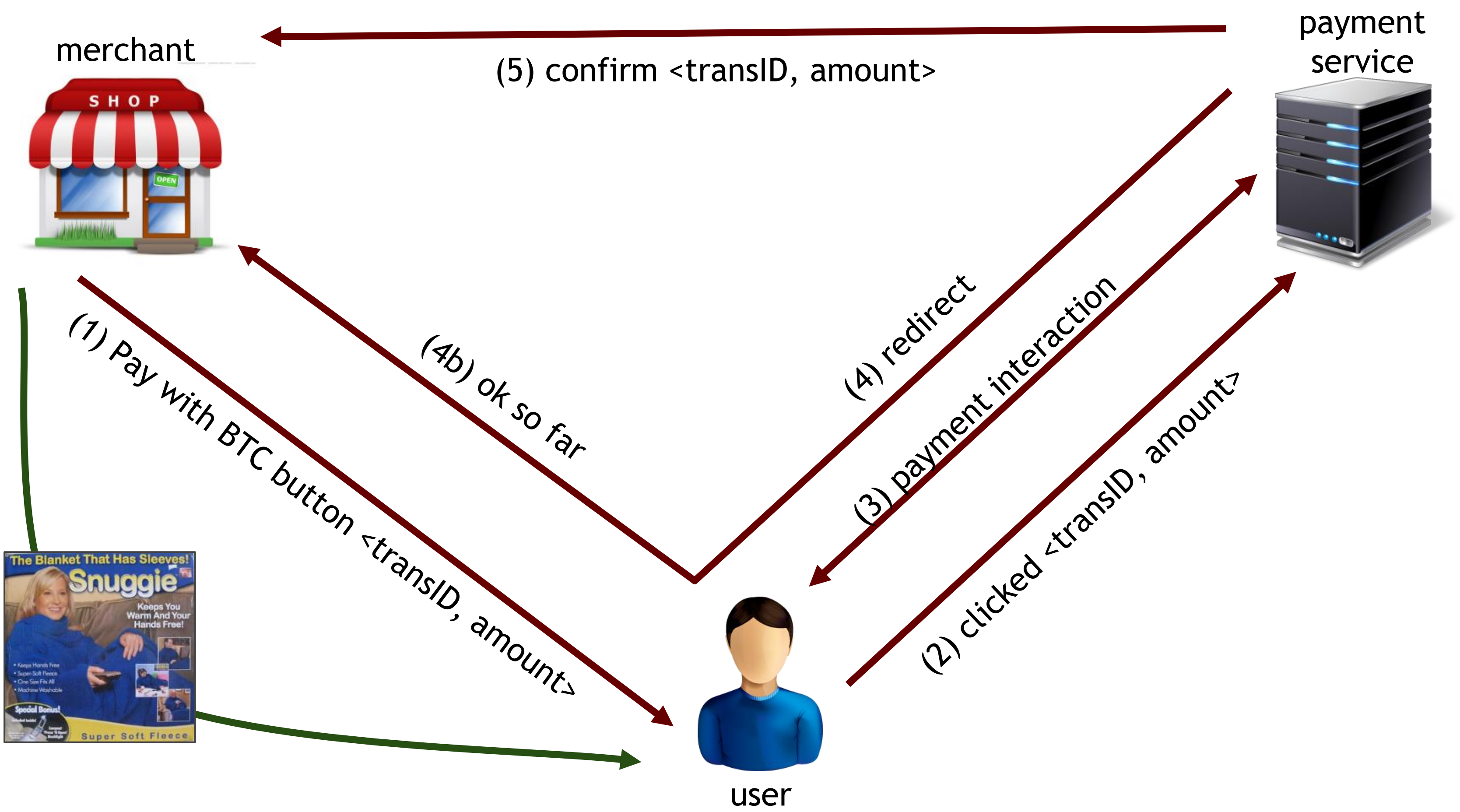
Item Description: The ultimate in lightweight footwear

Send Funds To: My Wallet (0.00 BTC)

Show Advanced Options

Generate Button Code

HTML for payment button



merchant

payment service

user

(1) Pay with BTC button <transID, amount>

(2) clicked <transID, amount>

(3) payment interaction

(4) redirect

(4b) ok so far

(5) confirm <transID, amount>

SHOP
OPEN
The Blanket That Has Sleeves!
Snuggie
Keeps You Warm And Your Hands Free!
Special Bonus!
Super Soft Fleece

End result

customer: pays Bitcoins

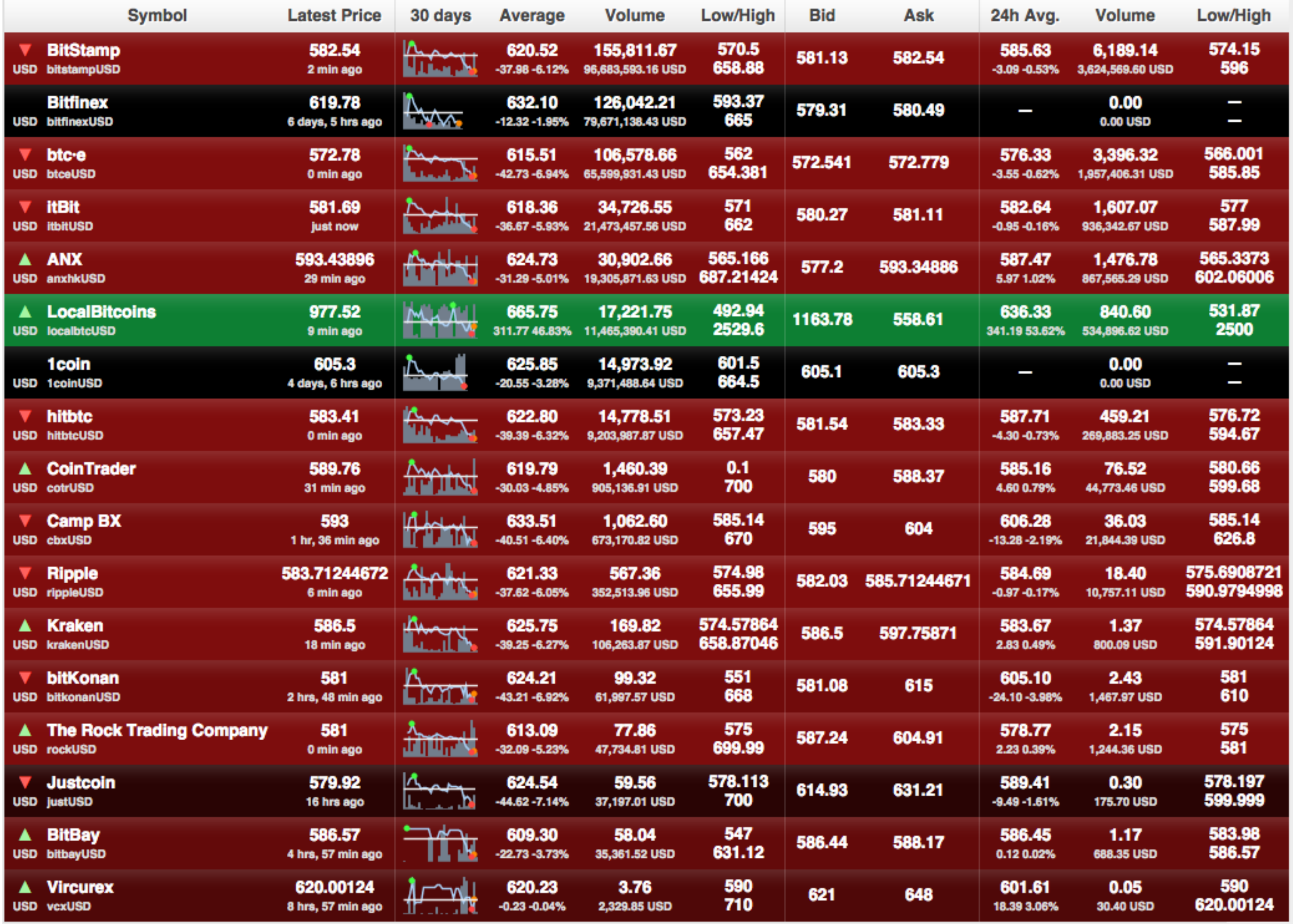
merchant: gets dollars, minus a small percentage

payment service:

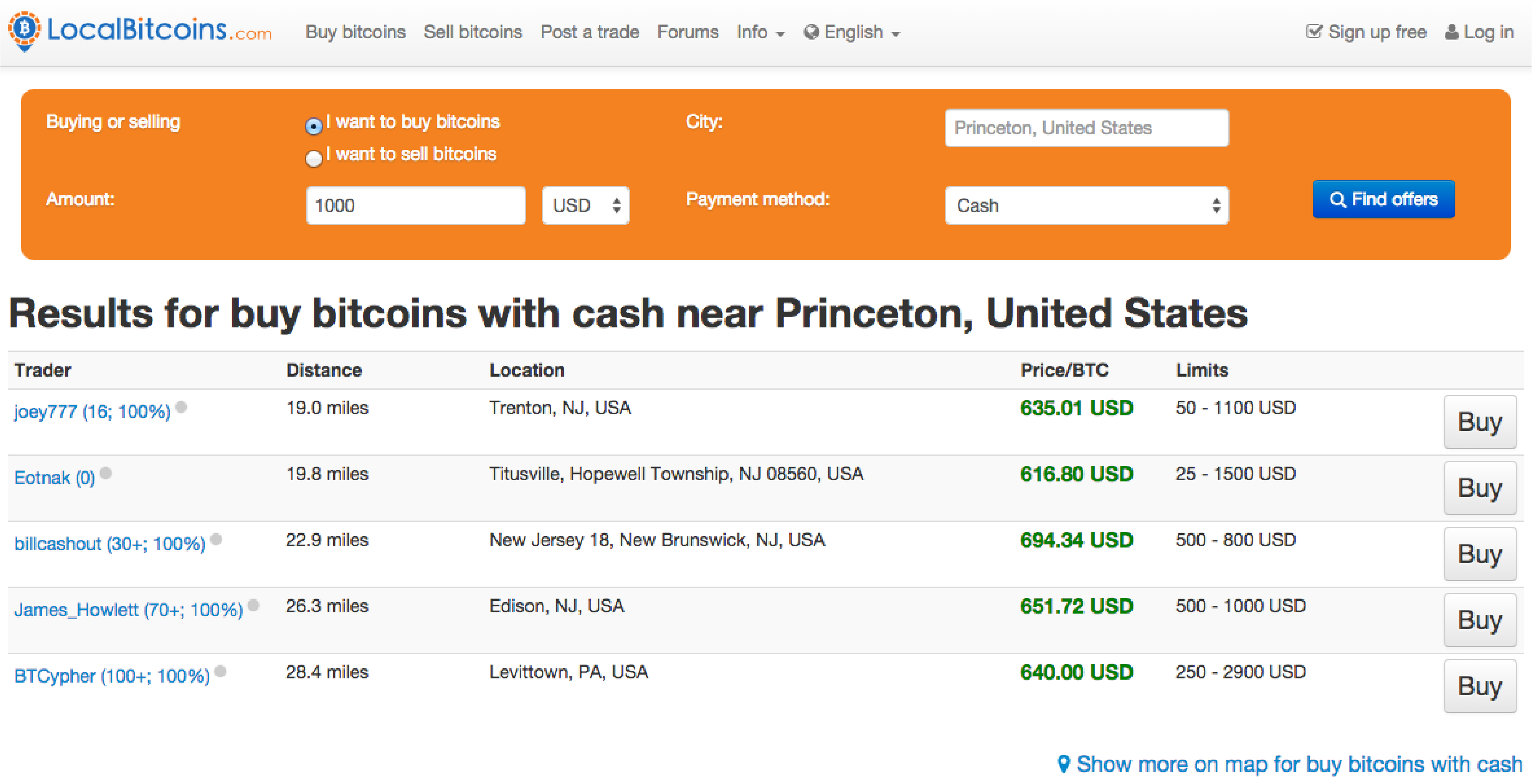
- gets Bitcoins
- pays dollars (keeps small percentage)
- absorbs risk: security, exchange rate
- needs to exchange Bitcoins for dollars, in volume

Currency Exchange Markets

http://bitcoincharts.com/markets



Symbol	Latest Price	30 days	Average	Volume	Low/High	Bid	Ask	24h Avg.	Volume	Low/High
▼ BitStamp USD bitstampUSD	582.54 2 min ago		620.52 -37.98 -6.12%	155,811.67 96,683,593.16 USD	570.5 658.88	581.13	582.54	585.63 -3.09 -0.53%	6,189.14 3,624,569.60 USD	574.15 596
Bitfinex USD bitfinexUSD	619.78 6 days, 5 hrs ago		632.10 -12.32 -1.95%	126,042.21 79,671,138.43 USD	593.37 665	579.31	580.49	—	0.00 0.00 USD	— —
▼ btc·e USD btceUSD	572.78 0 min ago		615.51 -42.73 -6.94%	106,578.66 65,599,931.43 USD	562 654.381	572.541	572.779	576.33 -3.55 -0.62%	3,396.32 1,957,406.31 USD	566.001 585.85
▼ itBit USD itbitUSD	581.69 just now		618.36 -36.67 -5.93%	34,726.55 21,473,457.56 USD	571 662	580.27	581.11	582.64 -0.95 -0.16%	1,607.07 936,342.67 USD	577 587.99
▲ ANX USD anxhkUSD	593.43896 29 min ago		624.73 -31.29 -5.01%	30,902.66 19,305,871.63 USD	565.166 687.21424	577.2	593.34886	587.47 5.97 1.02%	1,476.78 867,565.29 USD	565.3373 602.06006
▲ LocalBitcoins USD localbtcUSD	977.52 9 min ago		665.75 311.77 46.83%	17,221.75 11,465,390.41 USD	492.94 2529.6	1163.78	558.61	636.33 341.19 53.62%	840.60 534,896.62 USD	531.87 2500
1coin USD 1coinUSD	605.3 4 days, 6 hrs ago		625.85 -20.55 -3.28%	14,973.92 9,371,488.64 USD	601.5 664.5	605.1	605.3	—	0.00 0.00 USD	— —
▼ hitbtc USD hitbtcUSD	583.41 0 min ago		622.80 -39.39 -6.32%	14,778.51 9,203,987.87 USD	573.23 657.47	581.54	583.33	587.71 -4.30 -0.73%	459.21 269,883.25 USD	576.72 594.67
▲ CoinTrader USD cotrUSD	589.76 31 min ago		619.79 -30.03 -4.85%	1,460.39 905,136.91 USD	0.1 700	580	588.37	585.16 4.60 0.79%	76.52 44,773.46 USD	580.66 599.68
▼ Camp BX USD cbxUSD	593 1 hr, 36 min ago		633.51 -40.51 -6.40%	1,062.60 673,170.82 USD	585.14 670	595	604	606.28 -13.28 -2.19%	36.03 21,844.39 USD	585.14 626.8
▼ Ripple USD rippleUSD	583.71244672 6 min ago		621.33 -37.62 -6.05%	567.36 352,513.96 USD	574.98 655.99	582.03	585.71244671	584.69 -0.97 -0.17%	18.40 10,757.11 USD	575.6908721 590.9794998
▲ Kraken USD krakenUSD	586.5 18 min ago		625.75 -39.25 -6.27%	169.82 106,263.87 USD	574.57864 658.87046	586.5	597.75871	583.67 2.83 0.49%	1.37 800.09 USD	574.57864 591.90124
▼ bitKonan USD bitkonanUSD	581 2 hrs, 48 min ago		624.21 -43.21 -6.92%	99.32 61,997.57 USD	551 668	581.08	615	605.10 -24.10 -3.98%	2.43 1,467.97 USD	581 610
▲ The Rock Trading Company USD rockUSD	581 0 min ago		613.09 -32.09 -5.23%	77.86 47,734.81 USD	575 699.99	587.24	604.91	578.77 2.23 0.39%	2.15 1,244.36 USD	575 581
▼ Justcoin USD justUSD	579.92 16 hrs ago		624.54 -44.62 -7.14%	59.56 37,197.01 USD	578.113 700	614.93	631.21	589.41 -9.49 -1.61%	0.30 175.70 USD	578.197 599.999
▲ BitBay USD bitbayUSD	586.57 4 hrs, 57 min ago		609.30 -22.73 -3.73%	58.04 35,361.52 USD	547 631.12	586.44	588.17	586.45 0.12 0.02%	1.17 688.35 USD	583.98 586.57
▲ Vircurex USD vcxUSD	620.00124 8 hrs, 57 min ago		620.23 -0.23 -0.04%	3.76 2,329.85 USD	590 710	621	648	601.61 18.39 3.06%	0.05 30.40 USD	590 620.00124



Buying or selling ● I want to buy bitcoins ○ I want to sell bitcoins

City: Princeton, United States

Amount: 1000 USD

Payment method: Cash

Results for buy bitcoins with cash near Princeton, United States

Trader	Distance	Location	Price/BTC	Limits	
joey777 (16; 100%) ●	19.0 miles	Trenton, NJ, USA	**635.01 USD**	50 - 1100 USD	Buy
Eotnak (0) ●	19.8 miles	Titusville, Hopewell Township, NJ 08560, USA	**616.80 USD**	25 - 1500 USD	Buy
billcashout (30+; 100%) ●	22.9 miles	New Jersey 18, New Brunswick, NJ, USA	**694.34 USD**	500 - 800 USD	Buy
James_Howlett (70+; 100%) ●	26.3 miles	Edison, NJ, USA	**651.72 USD**	500 - 1000 USD	Buy
BTCypher (100+; 100%) ●	28.4 miles	Levittown, PA, USA	**640.00 USD**	250 - 2900 USD	Buy

Show more on map for buy bitcoins with cash

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 ~18.77 million

When to include demand deposits?

When they can actually be sold in the market.

Demand for Bitcoins

BTC demanded to mediate fiat-currency transactions

- Alice buys BTC for $
- Alice sends BTC to Bob
- 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:

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