Bitcoin

And other crypto currencies

Luke Herbert

Index

- Crypto currency
- Bitcoin: Background
- What is Bitcoin?
- Bitcoin: Uses
- Bitcoin: The basics
- Bitcoin: What does it look like?
- Bitcoin: Technical aspects
- Bitcoin: Differences
- Bitcoin: The technology
- Bitcoin: Problems and issues
- Conclusion: Bitcoin and beyond

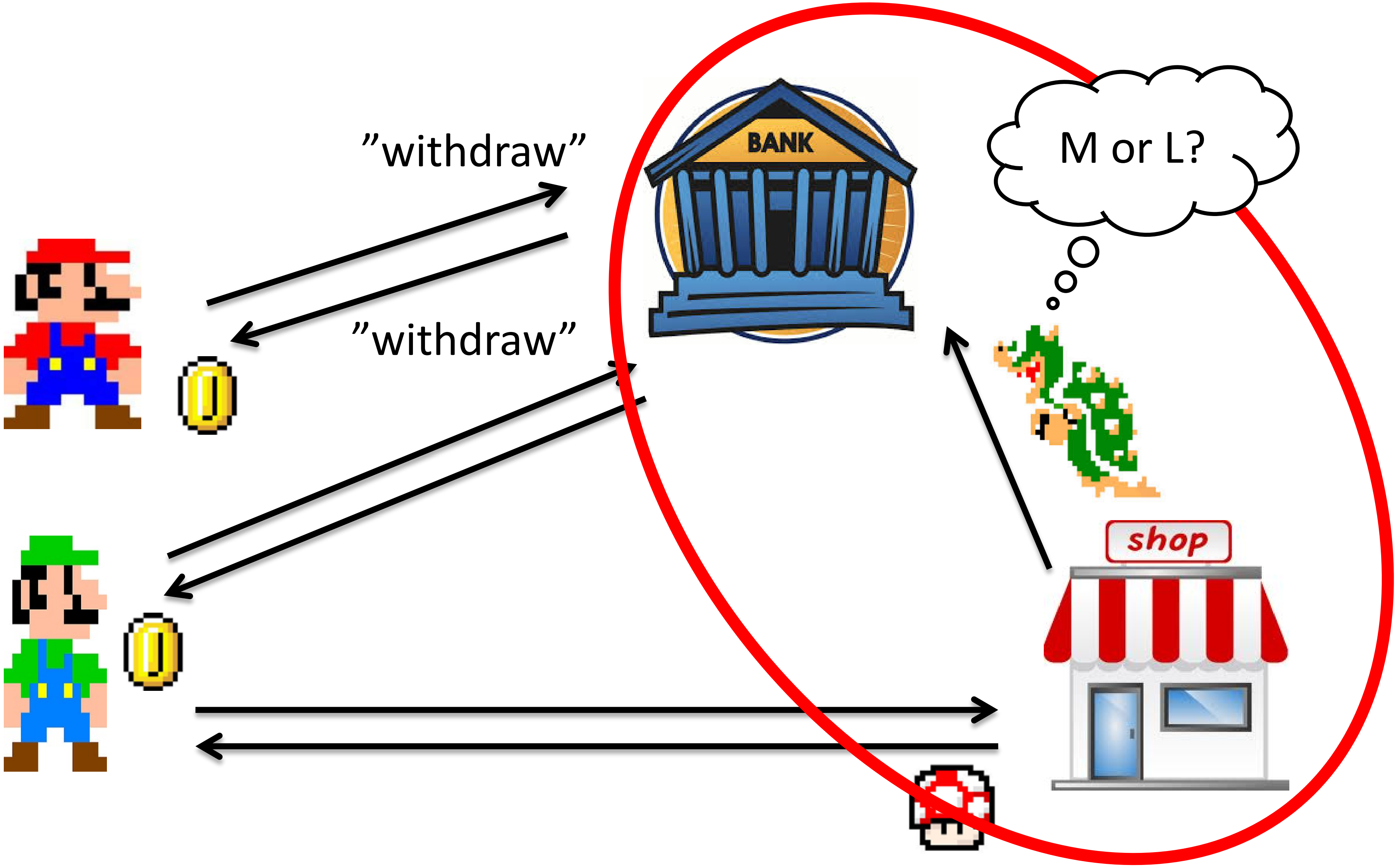
Crypto Currency

The 1990s
David Chaum and anonymous ecash

"The difference between
a bad electronic cash system
and well-developed digital cash
will determine whether
we will have a dictatorship
or a real democracy"

(attributed to Chaum)

Anonymous payments



Chaum’s **anonymous** e-cash

anonymous

secure (no double-spending)

only **transfer** (no creation/storage)

…and **bankrupted** in 1999

Alternative Coins (than Bitcoin)

MAJOR:

-BTC Bitcoin - first, strongest, most accepted, most mined, high volume market, a true currency
-LTC Litecoin - second only to BTC , faster than BTC, Smaller efficiency gap between GPUs and CPUs , ASIC-h
-NMC Namecoin merged mined with BTC, used for alternative p2p domain system
-PPC PPcoin   Proof Of Stake [very innovative, low energy] , compatibile with BTC miners

MINOR:

-TRC Terracoin based on BTC, fast difficulty adjustment, initialy flaved but corrected
-DVC Devcoin merged mined with BTC, 90% of generation goes to foundation, 10% to miners
-IXC IxCoin merged mined with BTC, premined 580k coins but still alive
-NVC NovaCoin - scrypt hashing[like LTC] , proof of stake [like PPC] , controversial start
-FRC Freicoin - back alive. 4.89% anual demurrage. for the first 3 years 80% block subsidy goes to foundatio
-FTC FeatherCoin- LTC clone with 4x more coins.

CANDIDATES:

-BTE Bytecoin- the 1:1 bitcoin copy, nothing changed. extremally high starting hype/hashrate.
-BQC BBQCoin- forgotten after 51% attack on launch, now revived and active. super fast version of LTC.
-MNC Mincoin- similar to BBQ, but very bad launch [no binaries + 25000% superblocks] giving 10% of all coins to insiders.
-CNC CHNCoin- similar to BBQ, announced on chinese forum first, very big hashrate.
-BTB BitBar- scarce version of NovaCoin. low starting diff like FTC and CNC, but quick adjustment.
-JKC Junkcoin- started as a joke, but now working ok. low starting diff and slow retarget like BTE, FTC, MNC, CNC
-YAC YACoin- Yet Another altCoin. NovaCoin fork, with modified hashing - for now CPU-ONLY
-RYC Royalcoin- Another LTC clone, starting with low diff and superblocks like MNC ...
-FRK Franko- Another faster LTC, again 0.00... starting diff. scarce.

DEAD / DYING :

-FTC Gamecoin- yes, FTC. clone so bad it was 51%'ed the first day.
-LQC Liquidcoin made to be very fast at constant difficulty, dead [pool closed, exchange closed]
-SC Solidcoin - dying (10-20% fee), designed to improove IxCoin, hard to be neutral on this one, 1.0 was a premine scam, 2.0 says BTC is pyramid scheme.

The idea is out. Even if a fatal flaw is found and exploited in Bitcoin, a better version will emerge within 24 hours . . . . probably within 1 hour.

Bitcoin: Background

History of Bitcoin

- Bitcoin is proposed as a “peer to peer electronic cash system” by an unknown software engineer, October 2008.

- First Bitcoin issued electronically, January 2009.

  Current worldwide supply = c. 12 million.

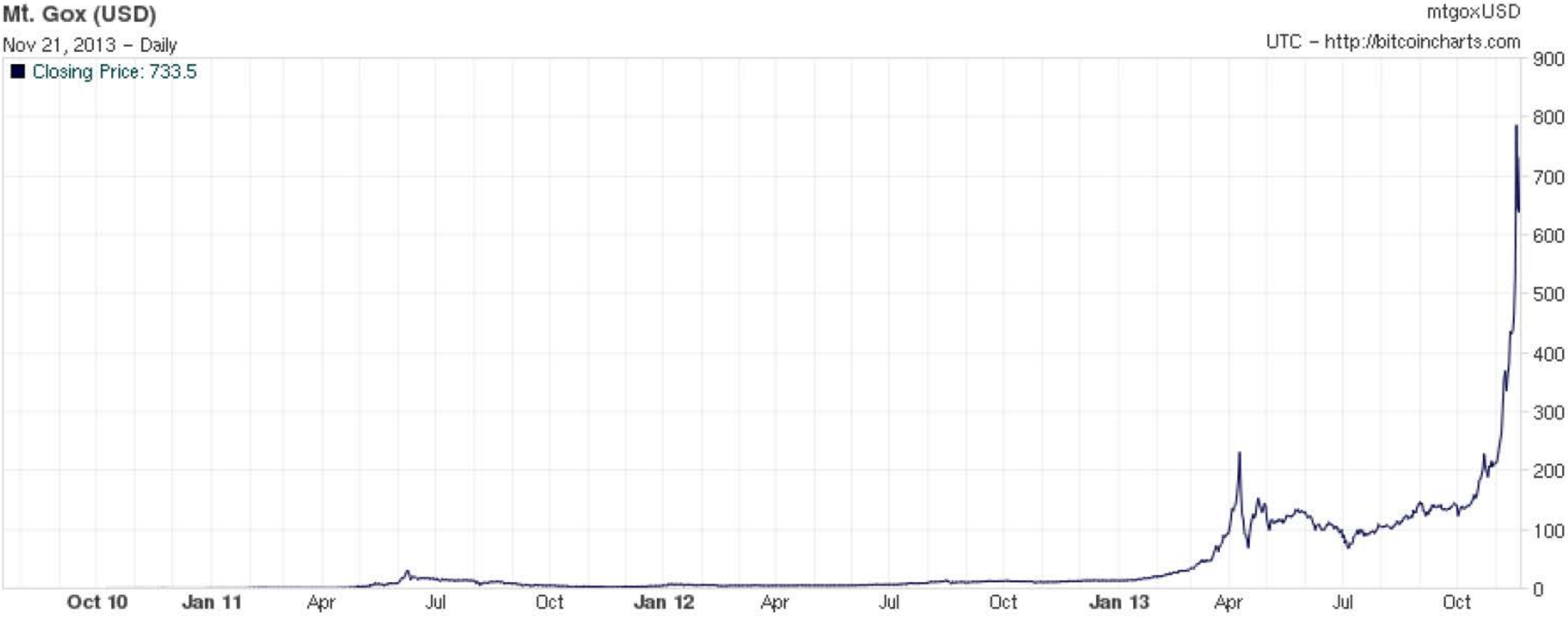
- Mt. Gox trading market opens, July 2010.

- U.S. Treasury issues first regulatory guidance for virtual currencies, March 2013.

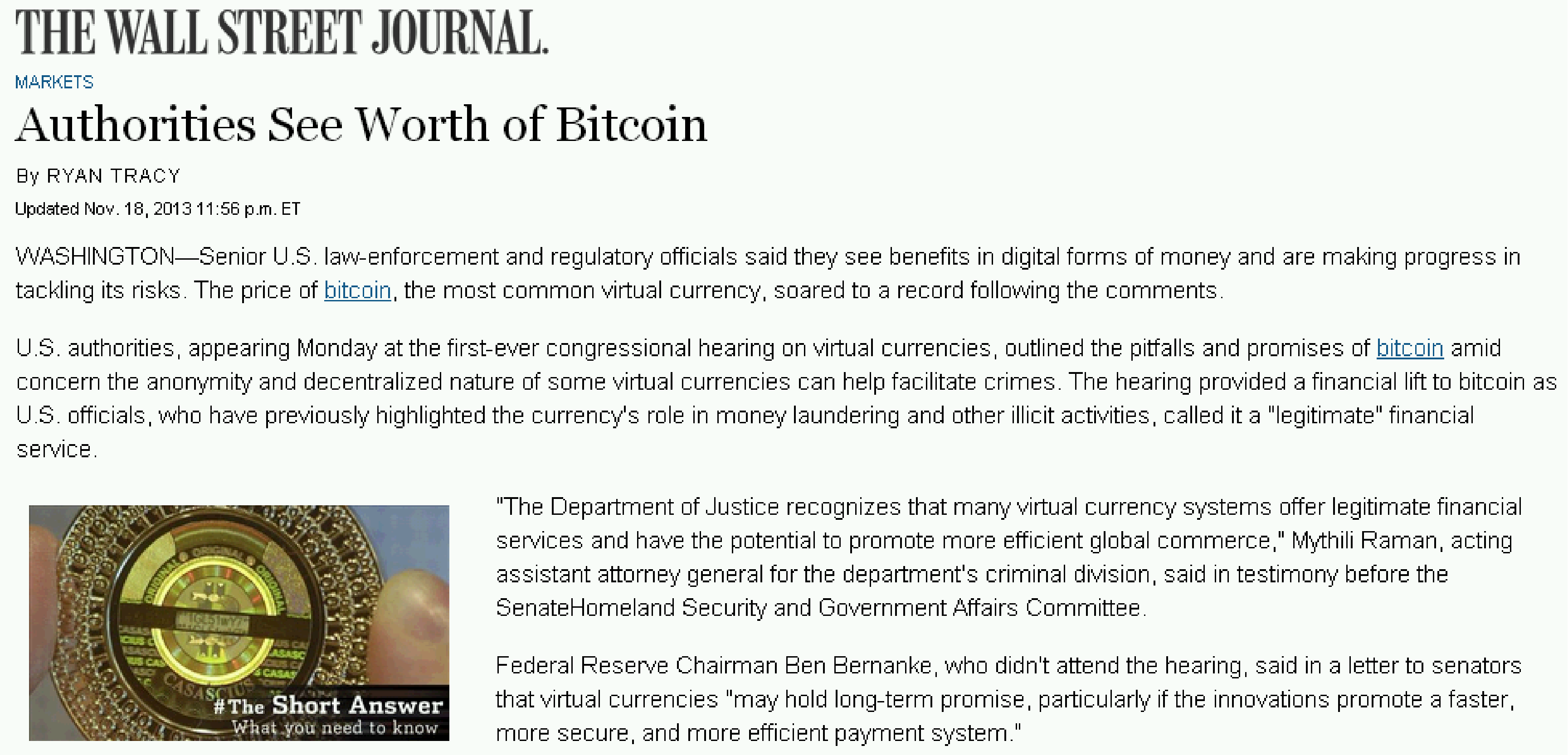
- Federal regulators, including Bernanke, comment favorably upon Bitcoin at the U.S. Senate hearing, November 2013.

What is Bitcoin?

Is Bitcoin really a currency?



David Yermack
NYU Stern School of Business
November 22, 2013



THE WALL STREET JOURNAL.

MARKETS

Authorities See Worth of Bitcoin

By RYAN TRACY

Updated Nov. 18, 2013 11:56 p.m. ET

WASHINGTON—Senior U.S. law-enforcement and regulatory officials said they see benefits in digital forms of money and are making progress in tackling its risks. The price of bitcoin, the most common virtual currency, soared to a record following the comments.

U.S. authorities, appearing Monday at the first-ever congressional hearing on virtual currencies, outlined the pitfalls and promises of bitcoin amid concern the anonymity and decentralized nature of some virtual currencies can help facilitate crimes. The hearing provided a financial lift to bitcoin as U.S. officials, who have previously highlighted the currency's role in money laundering and other illicit activities, called it a "legitimate" financial service.

"The Department of Justice recognizes that many virtual currency systems offer legitimate financial services and have the potential to promote more efficient global commerce," Mythili Raman, acting assistant attorney general for the department's criminal division, said in testimony before the SenateHomeland Security and Government Affairs Committee.

Federal Reserve Chairman Ben Bernanke, who didn't attend the hearing, said in a letter to senators that virtual currencies "may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system."

What is Bitcoin?

- A stateless , “algorithmic” currency

- That exists only in cyberspace

- Major demand is in U.S., China, and certain European countries

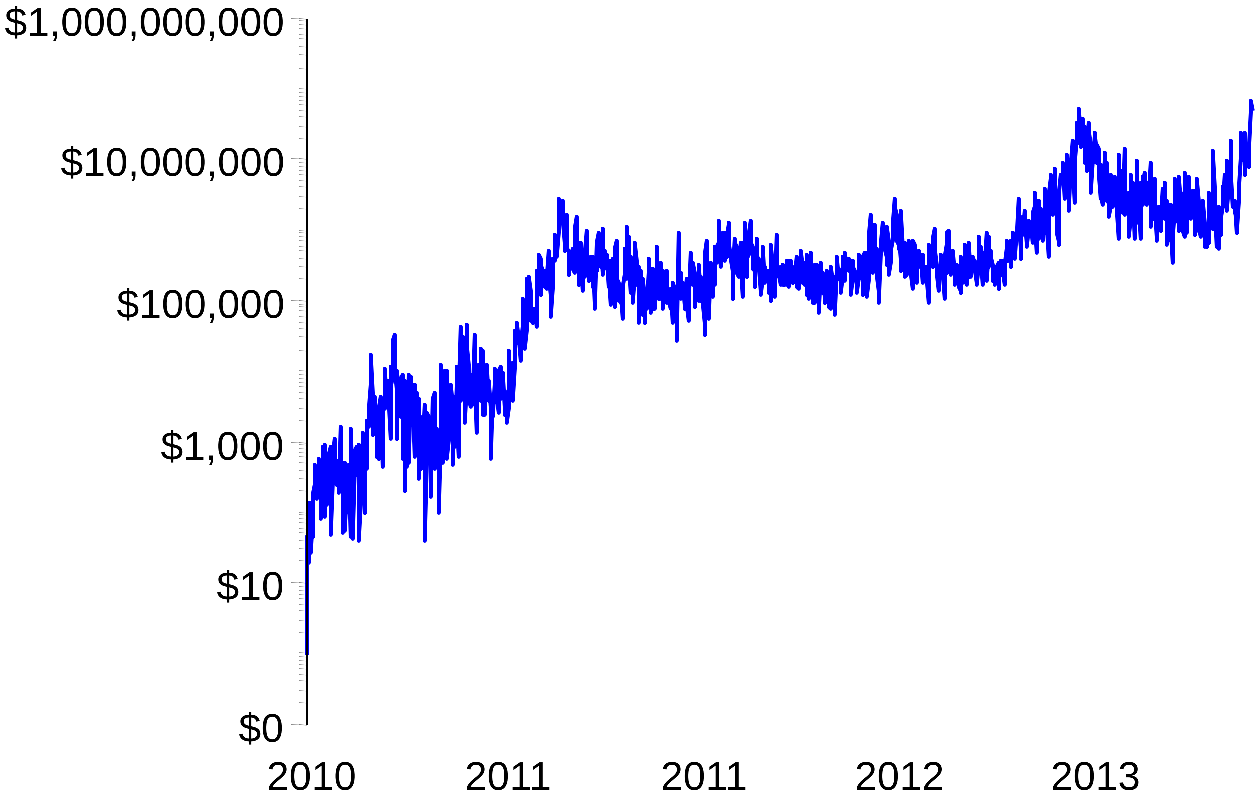
- Bitcoin / USD exchange rate:
  - July 17, 2010 1 Bitcoin = $ 0.0495
  - November 21, 2013 1 Bitcoin = $740.5948

Bitcoin’s appreciation vs. USD

- Past week 71%
- November 2013 (so far) 251%
- 2013 year to date 5,382%
- Since inception 1,495,749%

Daily trading volume

Mt. Gox exchange



Bitcoin's appeal

- Bitcoin's value cannot be debased by any government.
- The supply of Bitcoins can only grow slowly and is limited by a computer alogrithm to 21 million.
- Bitcoin attacts young, affluent users of eCommerce.
- Seigniorage revenue goes to entrepreneurs who "mine" new Bitcoins by solving math problems.

Does Bitcoin have the characteristics of a currency?

A currency is . . .

1. A medium of exchange
2. A unit of account
3. A store of value

Bitcoin: Uses

Living on Bitcoin

101 days, 4 countries

Around the World in 80 Bytes | Virtual-currency bitcoin paid for travelers' global journey

Clockwise from top left: Ying Yi Chua for The Wall Street Journal; Associated Press; Ying Yi Chua for The Wall Street Journal (2); Mark Abramson for The Wall Street Journal; Bloomberg

Austin Craig and Beccy Bingham-Craig used bitcoin to buy a henna tattoo in Singapore, pizza in New York and everything in between.

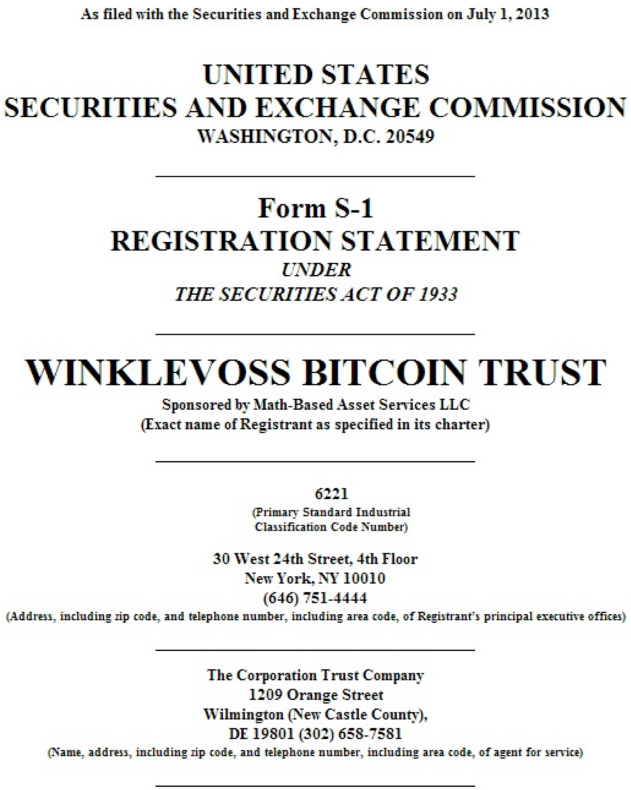
Bitcoin ATM

- Installed in a Vancouver coffee shop, October 2013

Victoria Hansen makes first-ever transaction

Bitcoin investment vehicles

- Winklevoss Twins claim to own 1% of worldwide supply, July 2013, and file for IPO of the Wilklevoss Bitcoin Trust



As filed with the Securities and Exchange Commission on July 1, 2013

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

Form S-1
REGISTRATION STATEMENT
UNDER
THE SECURITIES ACT OF 1933

WINKLEVOSS BITCOIN TRUST
Sponsored by Math-Based Asset Services LLC
(Exact name of Registrant as specified in its charter)

6221
(Primary Standard Industrial
Classification Code Number)

30 West 24th Street, 4th Floor
New York, NY 10010
(646) 751-4444
(Address, including zip code, and telephone number, including area code, of Registrant's principal executive offices)

The Corporation Trust Company
1209 Orange Street
Wilmington (New Castle County),
DE 19801 (302) 658-7581
(Name, address, including zip code, and telephone number, including area code, of agent for service)

What are the benefits?

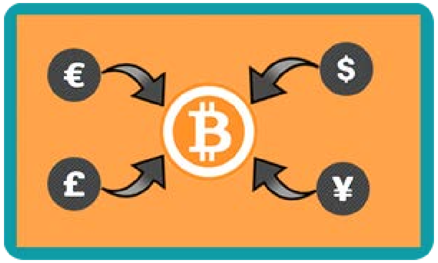
- Low or non-existent fees
- No chargebacks
- Credit card fees passed to the consumer cost $427 per household
- 55% of small businesses do not accept credit cards
- Only 27% of purchases are made with cash
- Every time a customer swipes a credit card at the grocery store, banks and credit card companies collect up to 4 percent of the total bill.
- Hedge against inflation
- Safe haven for currency collapse
  - For every Trillion dollars that enter, each bitcoin will increase $75,000
- If you have a kid in college you can give him an allowance
- You can email money
- You can send money to anyone in the world who needs quick cash
- Profit
- Can not be deflated due to printing
- Crowdsourcing

What are the Possibilities?

- End of national currencies
- End of Banks
- The end of predatory lending
- The end of the IRS
- The end of the voting booth
- A new notary system
- The end of Western Union/Money Orders
- Anyone with a cellphone is a bank

Bitcoin: The basics

How Does Bitcoin Work?

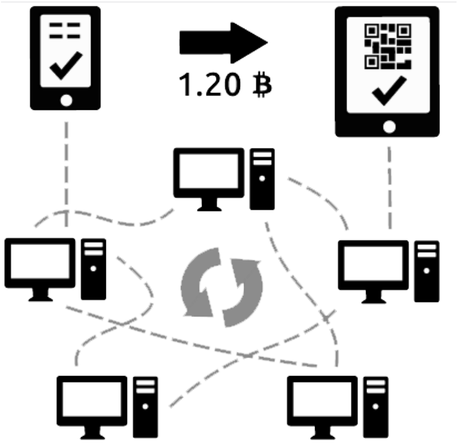


- Anyone can purchase Bitcoin from a Bitcoin exchange using dozens of different currencies and payment methods to buy and sell it. (localbitcoins.com)
- Bitcoin is sent from person to person similar to how paypal works with an email. All you need is a BTC address to send to and it will arrive instantly
- Bitcoin relies on miners who verify all transactions that are sent.
- Bitcoin is traded on the open market so there is always a real value determined

Who Uses Bitcoin?

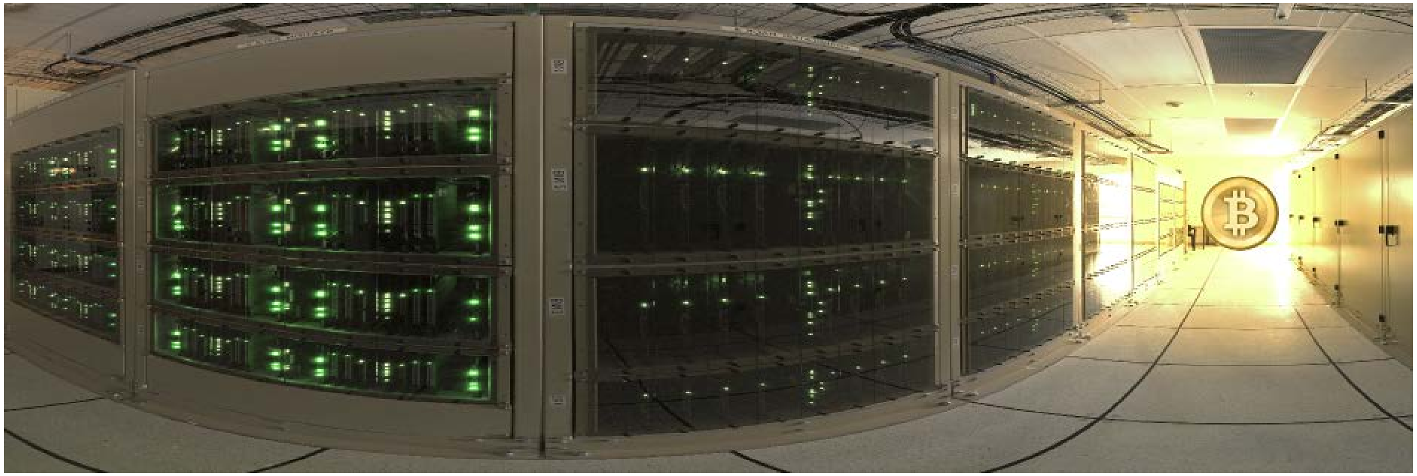
- ➢ Over 100,000 Business in the US and estimated 500,000 worldwide
- ➢ Growing fast as more merchants accept it daily (its easy to set up)
- ➢ There are no refunds, chargebacks or fees to accept bitcoin and the money is received instantly when sent (Soon it will be everywhere)

Is Bitcoin Safe?



- Yes, Bitcoin is designed with privacy and security in mind with all transactions happening anonymously so there is no personal information exchanged.
- Every transaction must be verified by the Bitcoin mining network before being validated
- Bitcoin uses 2 keys…
  - 1 Private Key (only available to owner of wallet)
  - 1 Public Key (used by miners to verify the public ledger)

What is Bitcoin Mining?



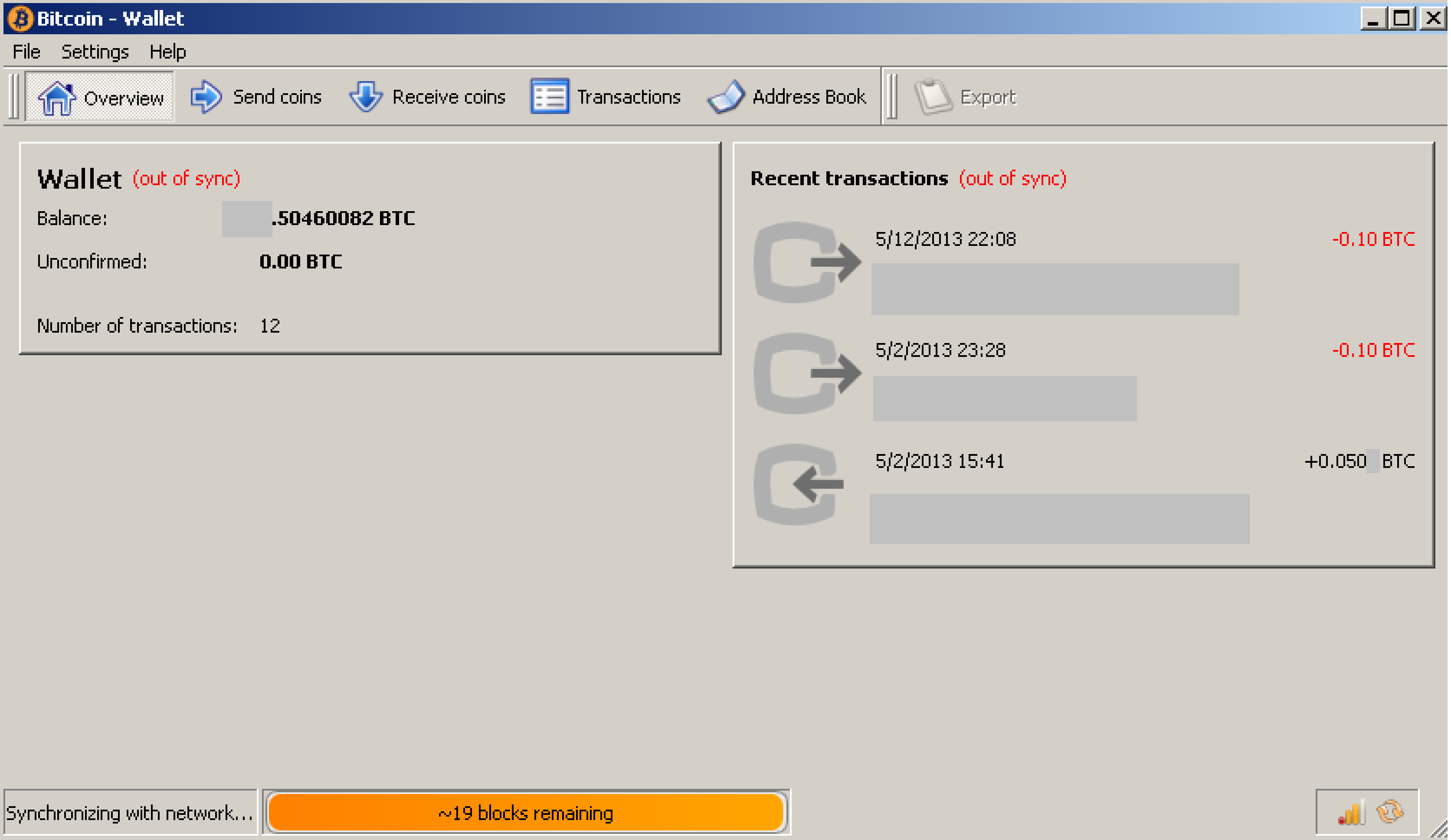
- Everyone who uses Bitcoin becomes part of the bank of Bitcoin
- Miners use special software to solve math problems that verify all transactions and they are rewarded with newly issued Bitcoin in exchange for using their computing power
- As more miners come online, the network gets more secure and the math gets harder
- Bitcoin would not work without miners

What Are Mining Pools?

- It’s nearly impossible for individuals to mine because the math is getting so hard to solve that it takes massive computing power to work
- The Solution… Mining Pools! People can share in the profits by pooling together their resources and splitting up the Bitcoin that is mined
- There are no limits or restrictions on how big a pool can get or how one is set up.

Bitcoin: What does it look like?

Bitcoin Wallet



Wallet (out of sync)

Balance: [redacted].50460082 BTC

Unconfirmed: 0.00 BTC

Number of transactions: 12

Recent transactions (out of sync)

5/12/2013 22:08 -0.10 BTC
[redacted]

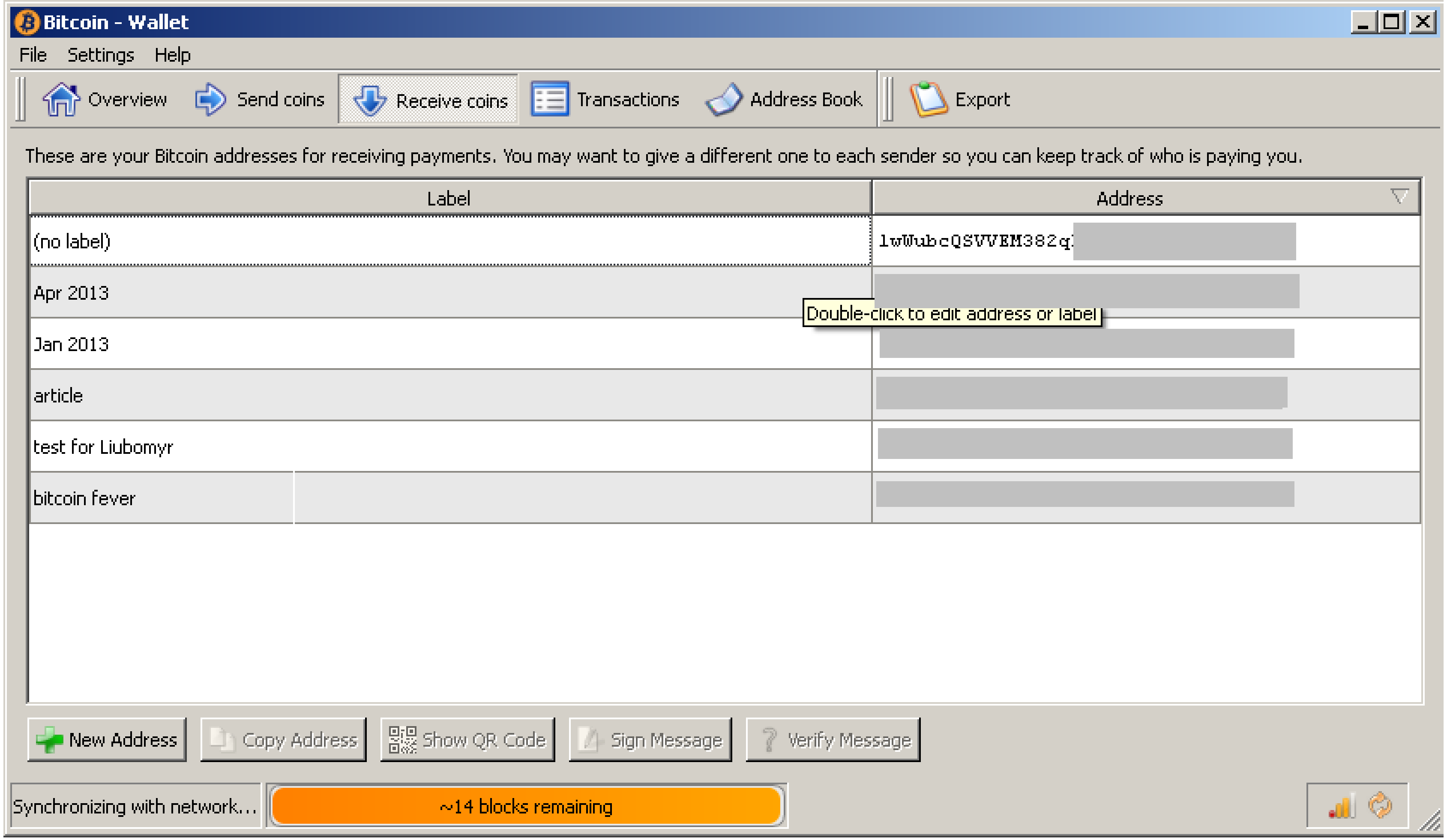
5/2/2013 23:28 -0.10 BTC
[redacted]

5/2/2013 15:41 +0.050[redacted] BTC
[redacted]

Synchronizing with network...

~19 blocks remaining

Bitcoin Wallet - receive



These are your Bitcoin addresses for receiving payments. You may want to give a different one to each sender so you can keep track of who is paying you.

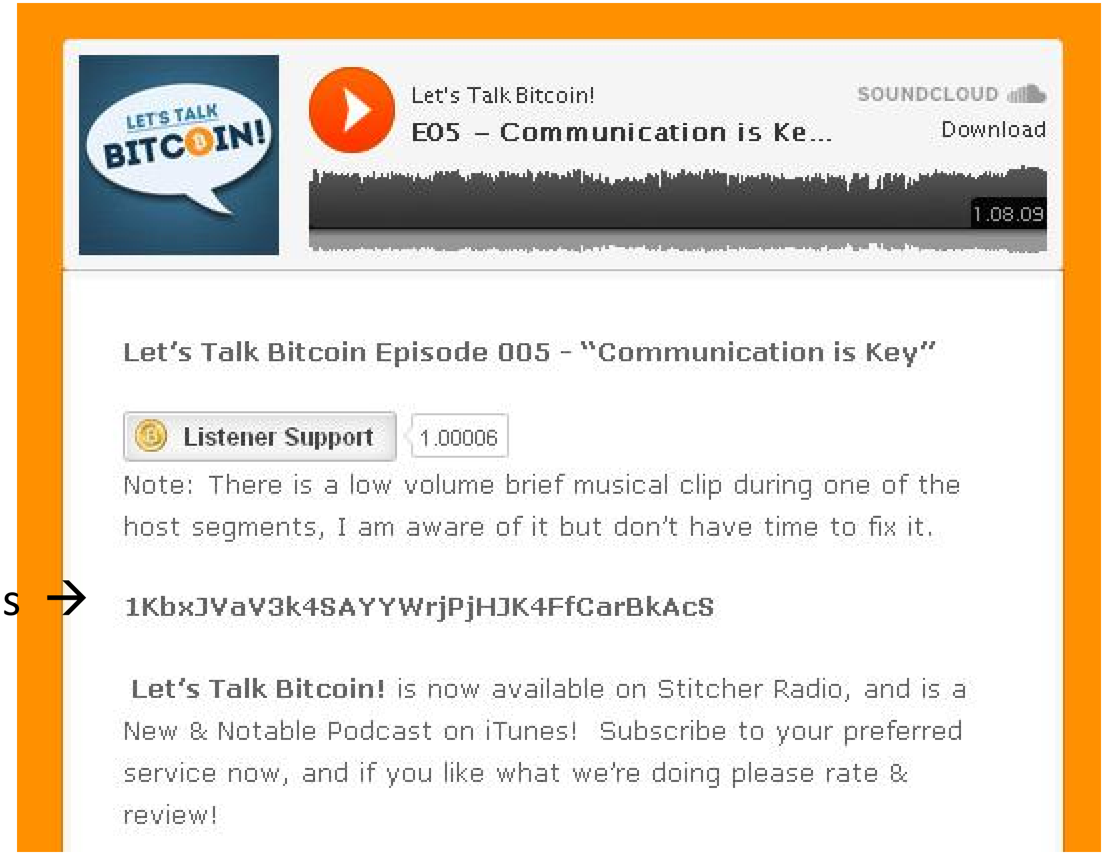
Label	Address
(no label)	1wWubcQSVVEM382q[redacted]
Apr 2013	[redacted]
Jan 2013	[redacted]
article	[redacted]
test for Liubomyr	[redacted]
bitcoin fever	[redacted]

Double-click to edit address or label

Synchronizing with network...

~14 blocks remaining

Advertising for Bitcoins →



Let’s Talk Bitcoin Episode 005 - “Communication is Key”

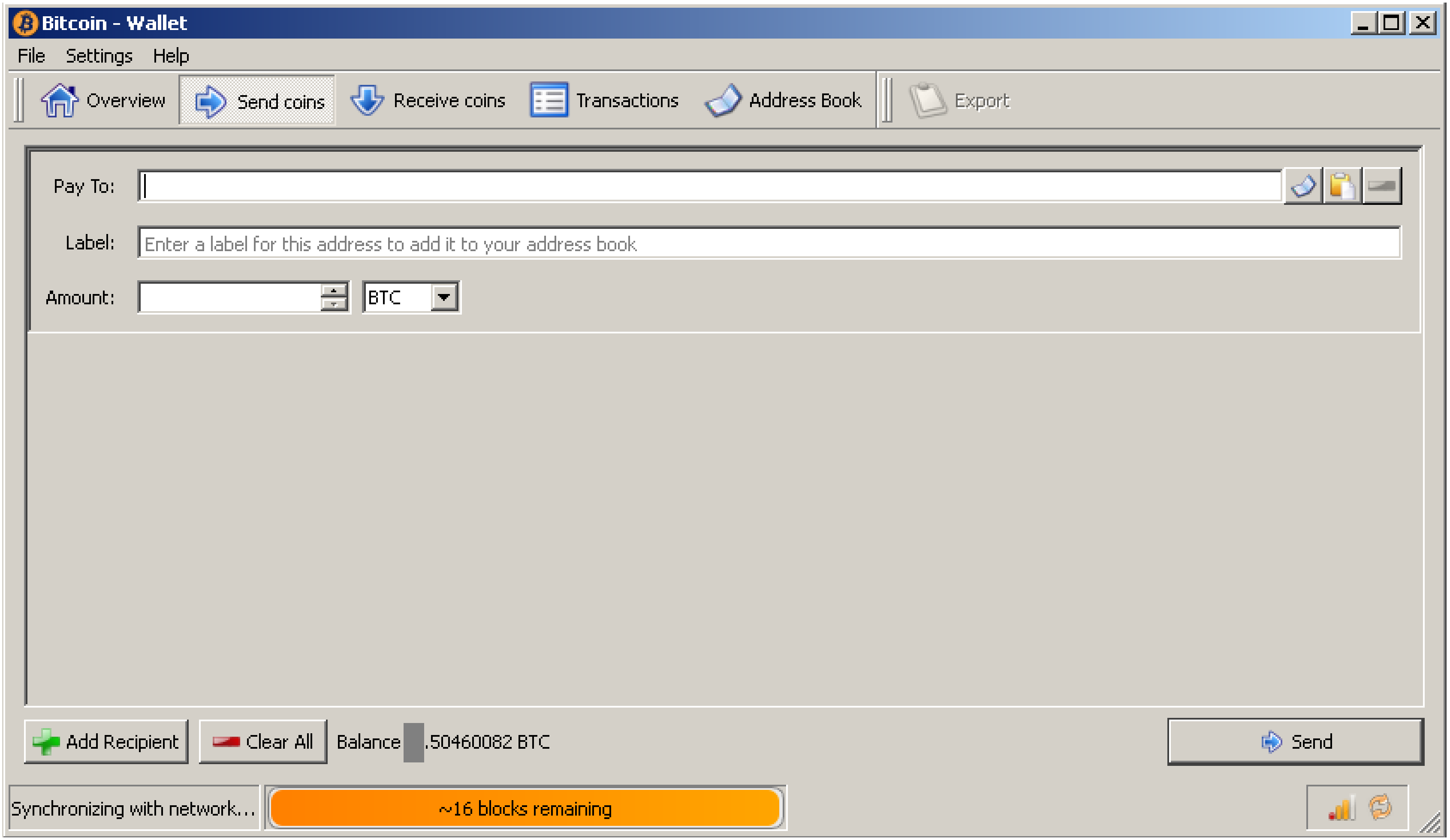
Listener Support 1.00006

Note: There is a low volume brief musical clip during one of the host segments, I am aware of it but don’t have time to fix it.

1KbxJVaV3k4SAYYWrjPjHJK4FfCarBkAcS

Let’s Talk Bitcoin! is now available on Stitcher Radio, and is a New & Notable Podcast on iTunes! Subscribe to your preferred service now, and if you like what we’re doing please rate & review!

Bitcoin Wallet - send



Pay To:

Label: Enter a label for this address to add it to your address book

Amount: BTC

Balance [redacted].50460082 BTC

Synchronizing with network...

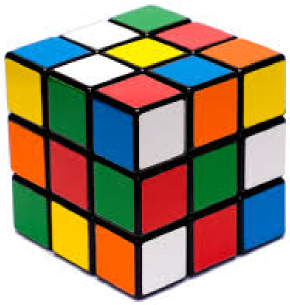
~16 blocks remaining

Bitcoin: Technical aspects

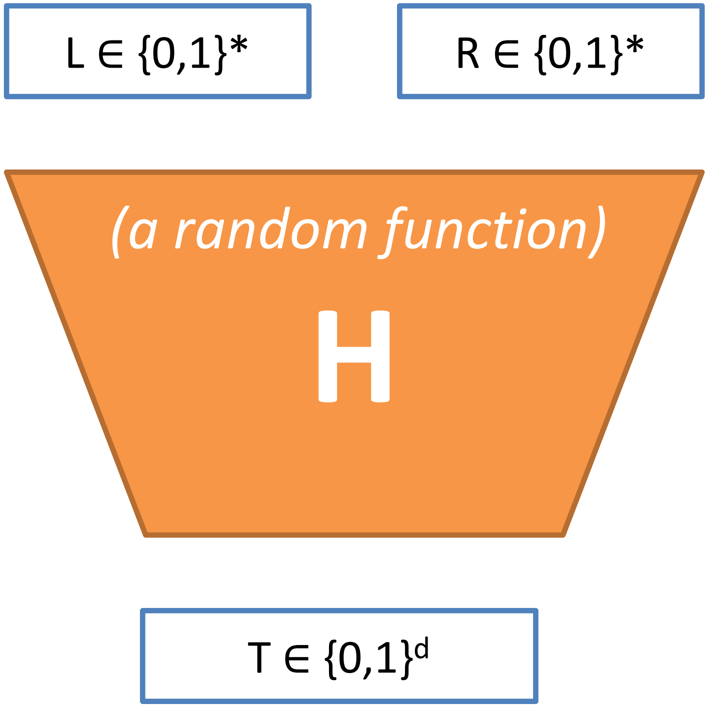
TheoryCoin:
How to create money

1. Everyone **tries to solve** a puzzle
2. The **first one** to solve the puzzle **gets 1 TC**
3. The solution of **puzzle *i* defines puzzle *i+1***

3			2	4			6	
	4						5	3
1	8	9	6	3	5	4		
				8		2		
		7	4	9	6	8		1
8	9	3	1	5		6		4
		1	9	2		5		
2			3			7	4	
9	6		5			3		2



TheoryCoin:
How to create money

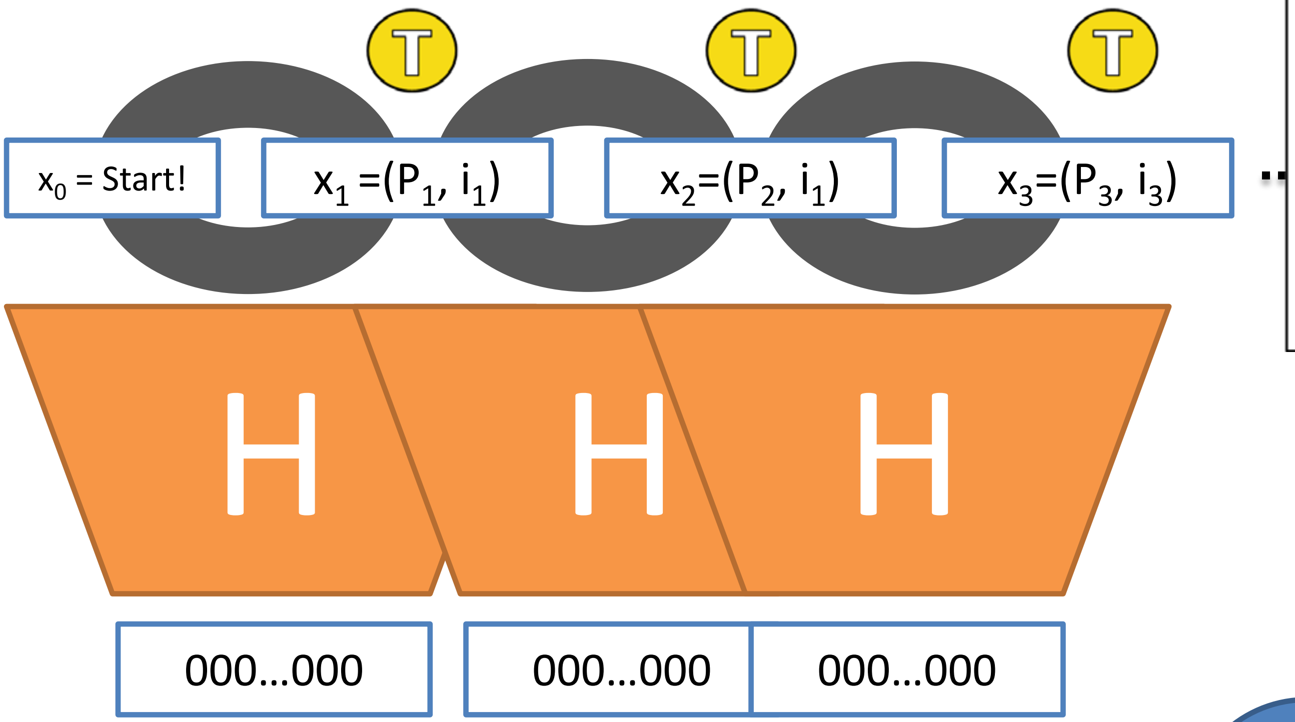


The puzzle:
given L, find R
such that $T=0^d$

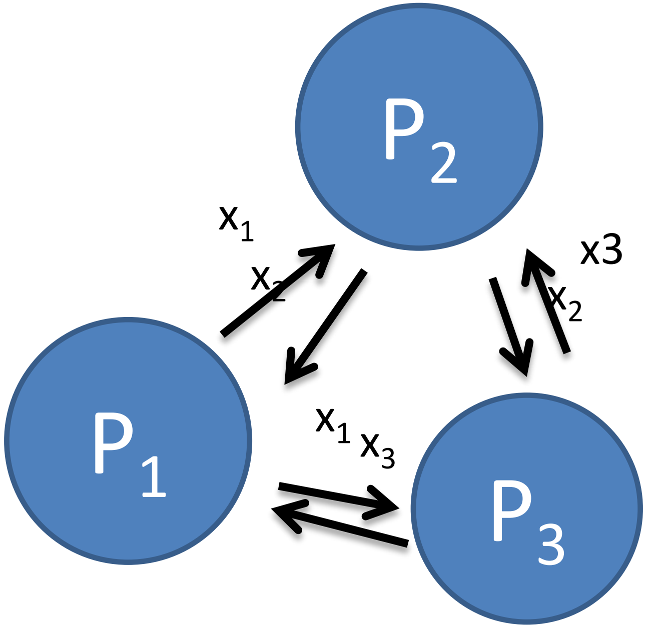
```
SolvePuzzle(L){
  repeat{
    R = my_name || i++
    T = H(L,R)
  }while(T $\neq$ $0^d$)
  return R
}
```

* *aka* ***Proof-of-Work***

TheoryCoin: (coins to ppl)
How to create money

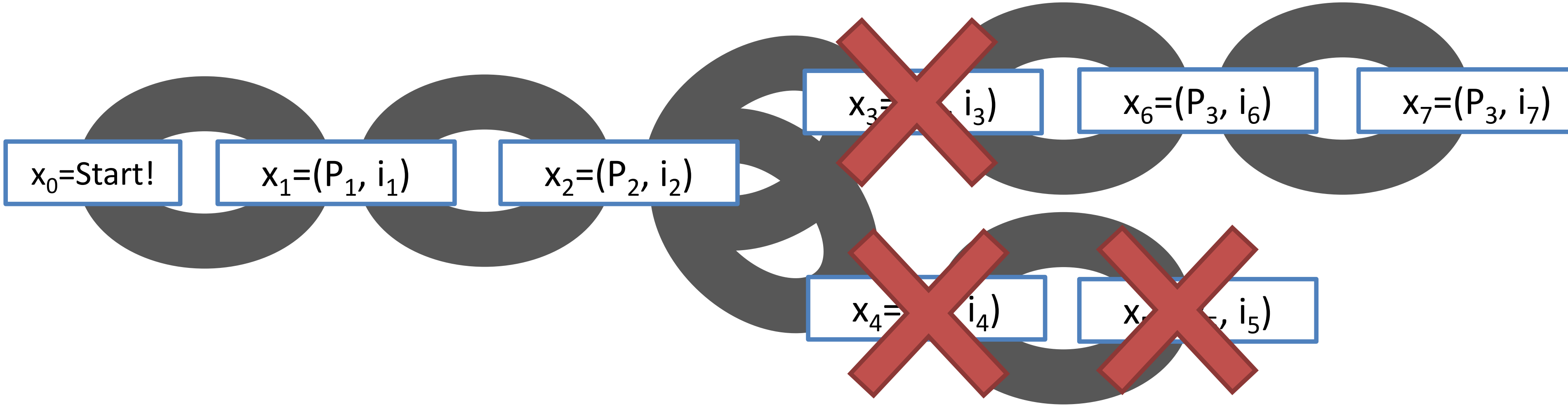


```
SolvePuzzle(L){
   repeat{
      R = my_name || i++
      T = H(L,R)
   }while(T ≠ $0^d$)
   return R
}
```



* *aka* ***the blockchain***

TheoryCoin:
How to create money



x_0=Start!

x_1=(P_1, i_1)

x_2=(P_2, i_2)

x_3= i_3)

x_6=(P_3, i_6)

x_7=(P_3, i_7)

x_4= i_4)

x , i_5)

* *aka* ***the 51% attack***

TheoryCoin:
How to create money

Recap:

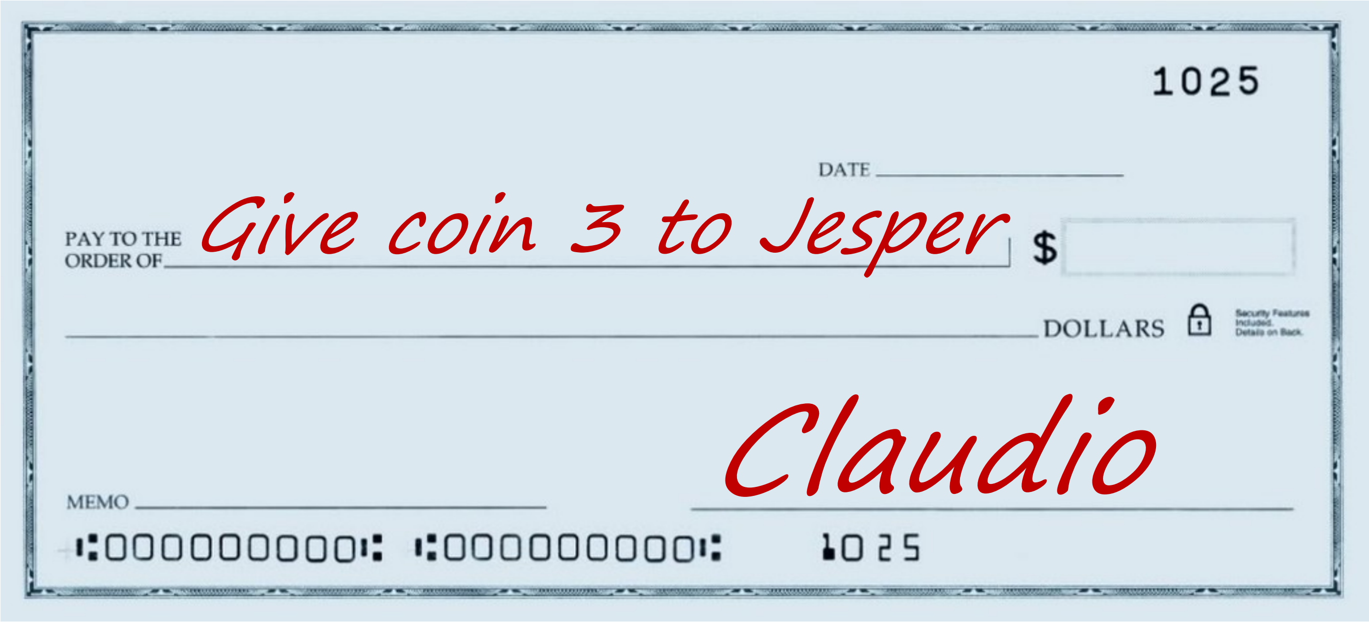
Solve the next puzzle → get a coin

- To “**solve”** puzzle i find x_i s.t $H(x_{i-1},x_i)=0^d$
- The longest chain defines “**next puzzle**”
- The name in block x_i “**gets**” coin i.

TheoryCoin:
How to transfer money

(Digital) Signatures

- Only you can sign
- Everyone can verify
- You cannot deny



1025

DATE

PAY TO THE ORDER OF *Give coin 3 to Jesper* $

DOLLARS

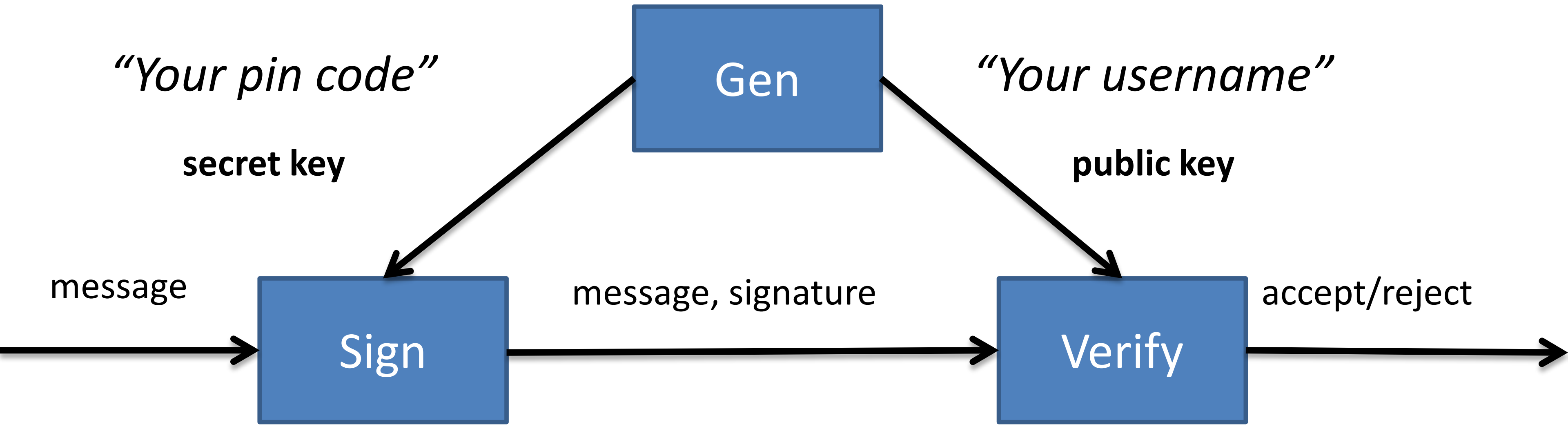
Security Features Included. Details on Back.

MEMO

Claudio

⑆000000000⑆ ⑆000000000⑆ 1025

TheoryCoin:
How to transfer money



“Your pin code”

secret key

Gen

“Your username”

public key

message

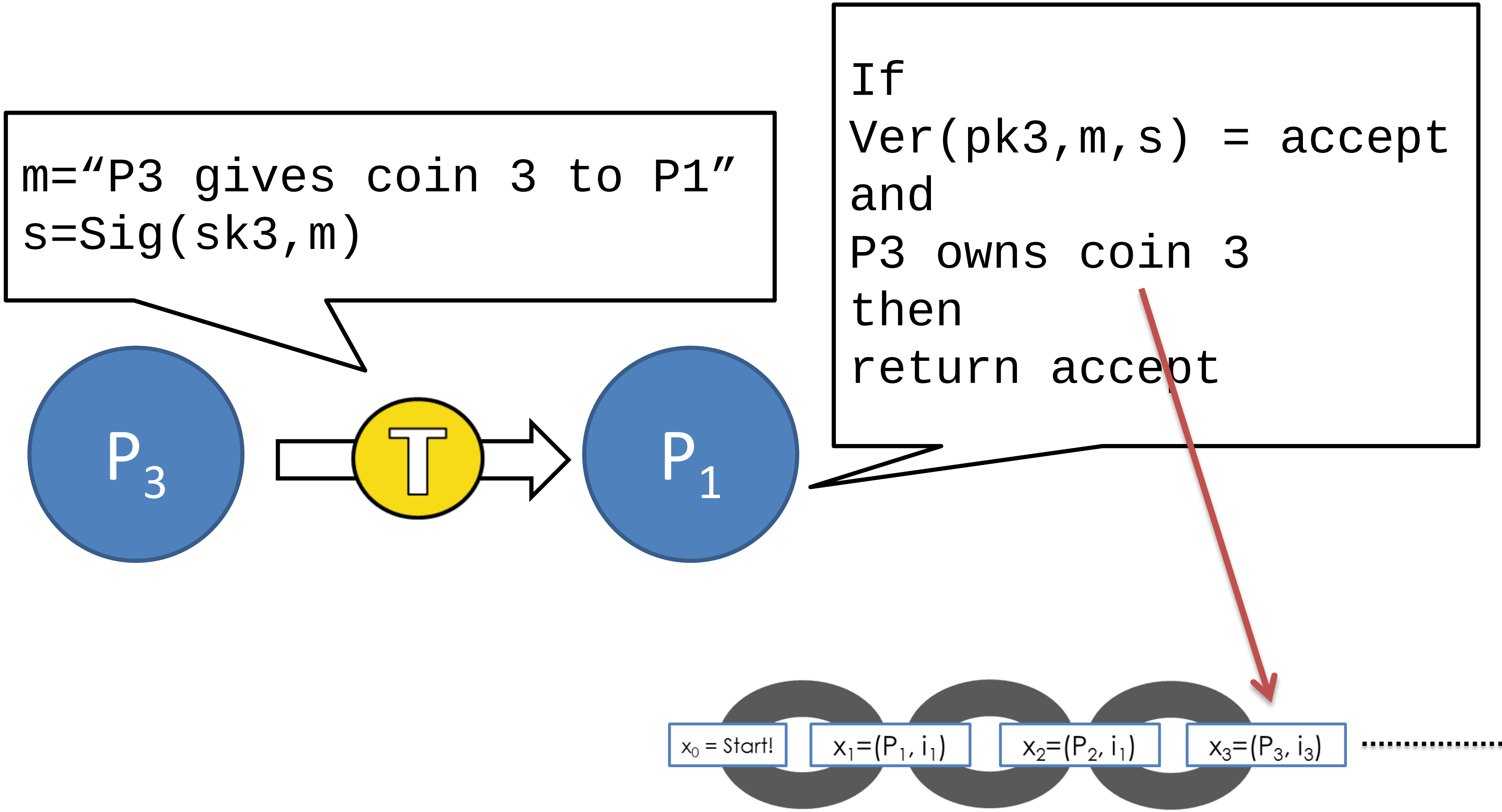
Sign

message, signature

Verify

accept/reject

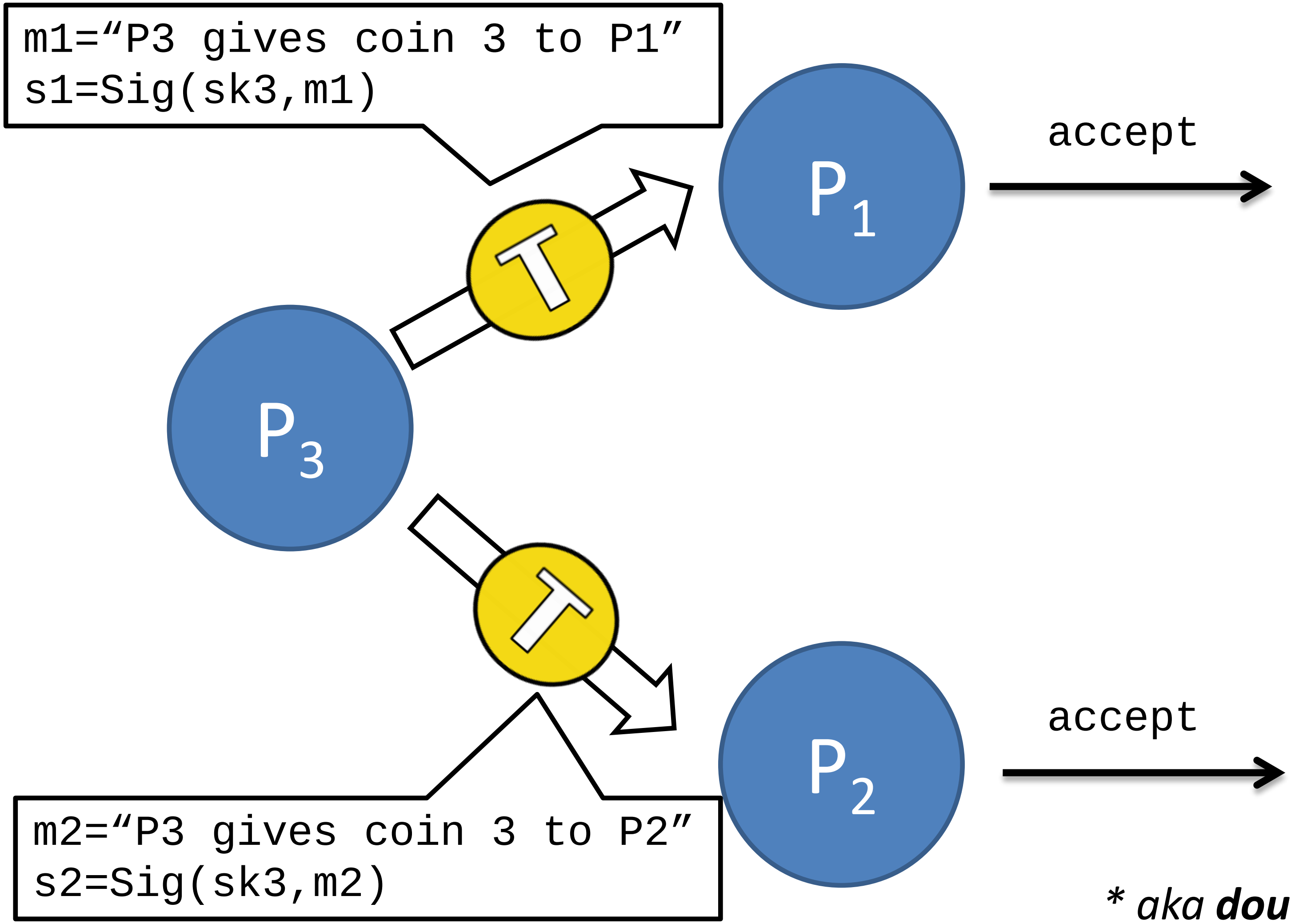
TheoryCoin:
How to transfer money



```
m=“P3 gives coin 3 to P1”
s=Sig(sk3,m)
```

```
If
Ver(pk3,m,s) = accept
and
P3 owns coin 3
then
return accept
```

TheoryCoin:
How to transfer money

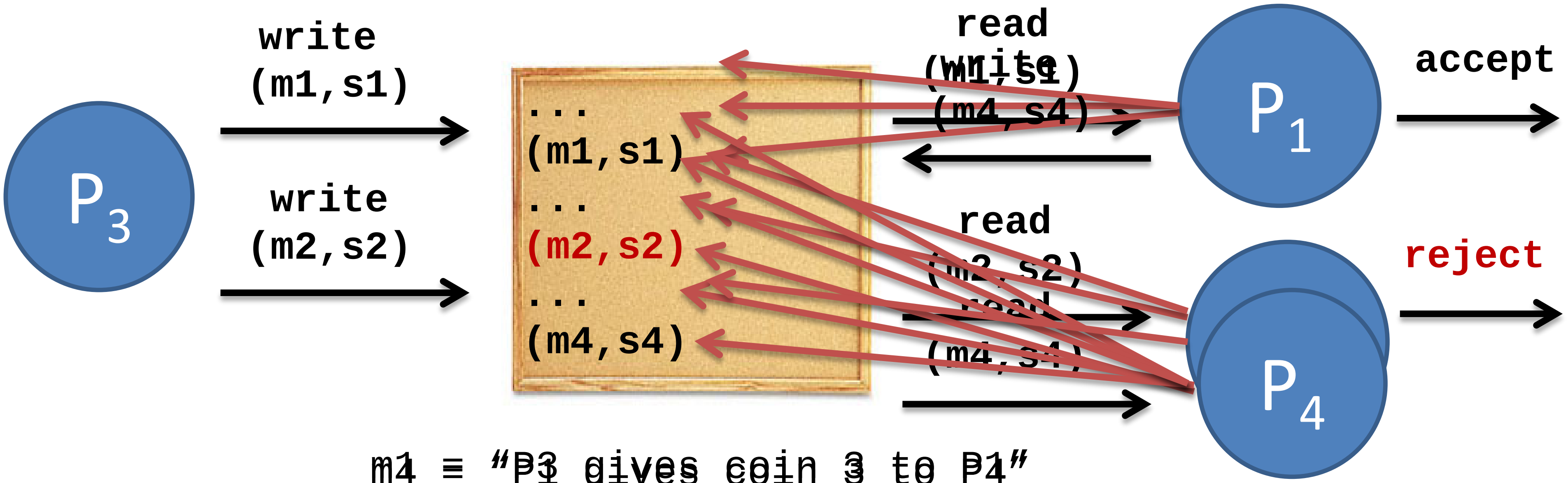


```
m1=“P3 gives coin 3 to P1”
s1=Sig(sk3,m1)
```

```
m2=“P3 gives coin 3 to P2”
s2=Sig(sk3,m2)
```

** aka* ***double spending***

TheoryCoin:
How to transfer money



m1 = “P3 gives coin 3 to P1”
s1 = Sig(sk3,m1)

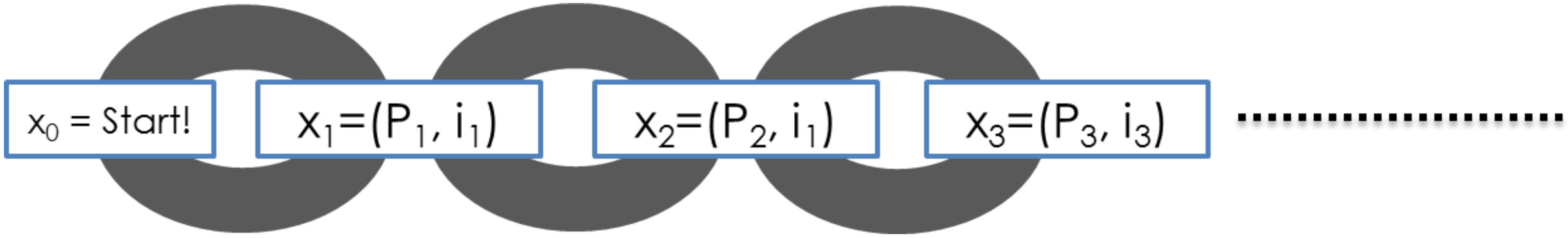
m4 = “P1 gives coin 3 to P4”
s4 = Sig(sk1,m4)

m2 = “P3 gives coin 3 to P2”
s2 = Sig(sk3,m2)

TheoryCoin:
How to store money

Main Idea:

Record **transfers** in the **blockchain**



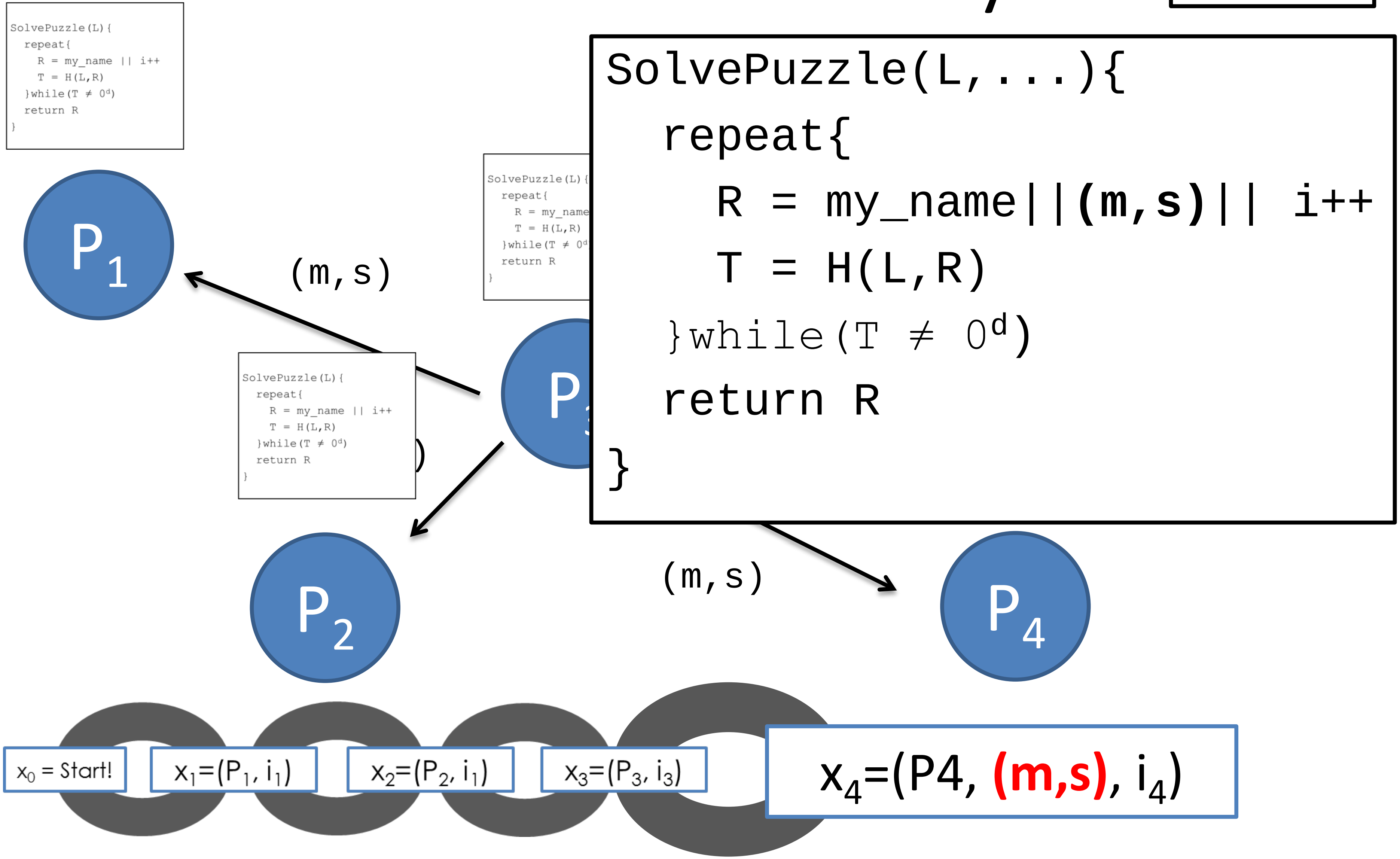
x_0 = Start!

$x_1=(P_1, i_1)$

$x_2=(P_2, i_1)$

$x_3=(P_3, i_3)$

TheoryCoin:
How to store money



```
SolvePuzzle(L){
  repeat{
    R = my_name || i++
    T = H(L,R)
  }while(T ≠ $0^d$)
  return R
}
```

```
SolvePuzzle(L){
  repeat{
    R = my_name
    T = H(L,R)
  }while(T ≠ $0^d$
  return R
}
```

```
SolvePuzzle(L,...){
  repeat{
    R = my_name||(m,s)|| i++
    T = H(L,R)
  }while(T ≠ $0^d$)
  return R
}
```

```
SolvePuzzle(L){
  repeat{
    R = my_name || i++
    T = H(L,R)
  }while(T ≠ $0^d$)
  return R
}
```

P_1

(m,s)

P_3

P_2

(m,s)

P_4

x_0 = Start!

x_1=(P_1, i_1)

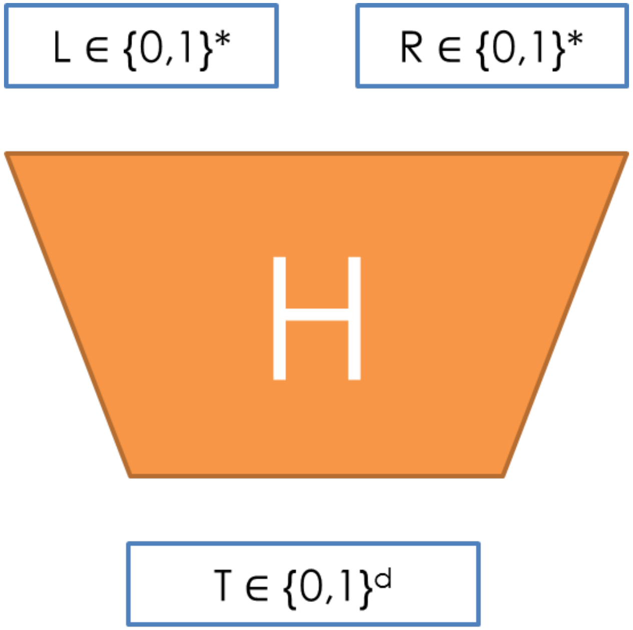
x_2=(P_2, i_1)

x_3=(P_3, i_3)

x_4=(P4, **(m,s)**, i_4)

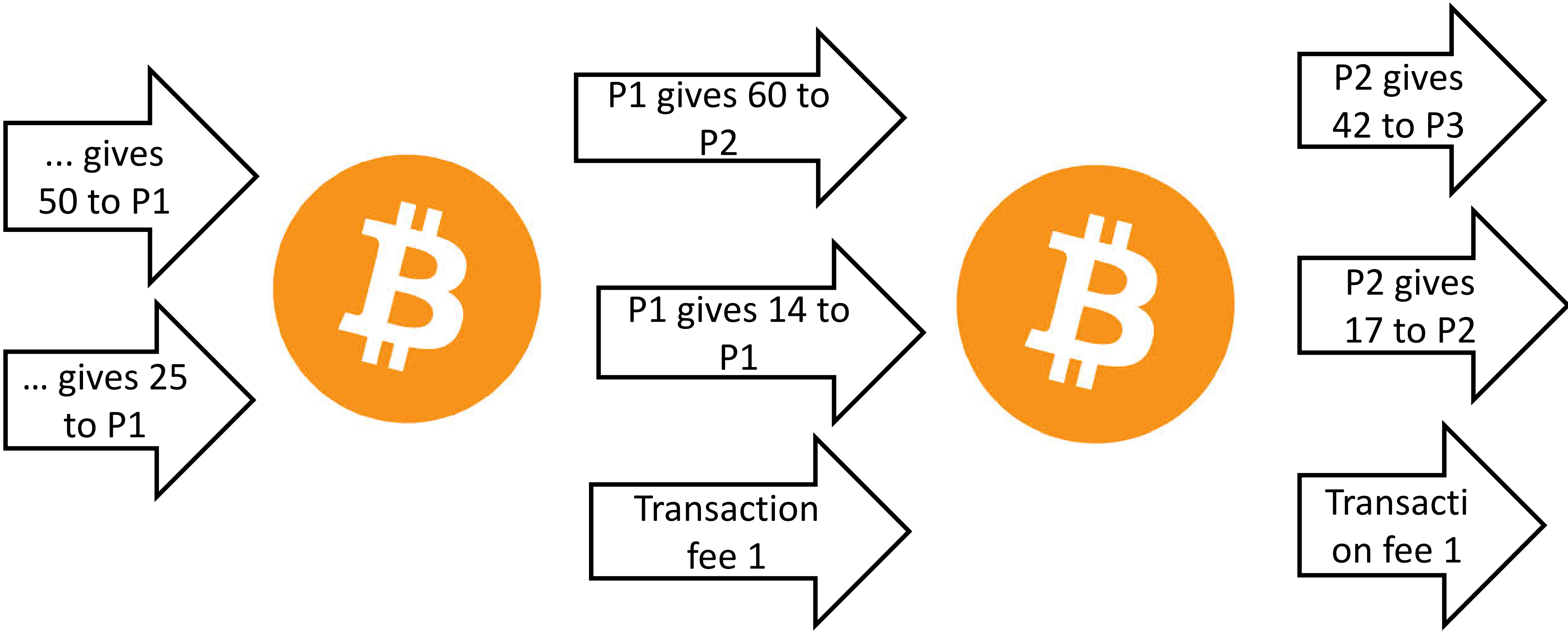
How is money created in Bitcoin?

- New block **every ~10 mins**
  - **d** adjusted every ~2000 blocks
- H = **2-SHA2**
- Initial reward: **50 BTC**
  - Halved every ~4 years (now **25 BTC**)



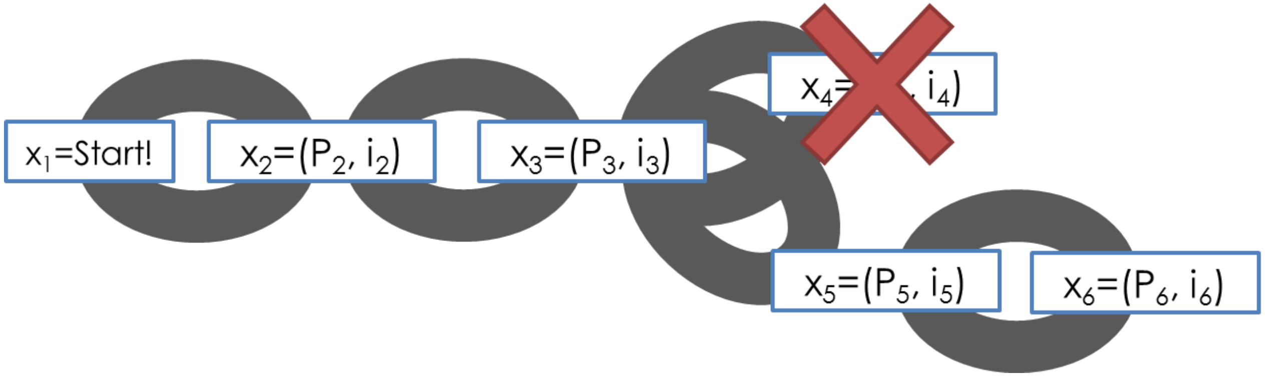
How is money transferred in Bitcoin?

Example: P1 wants to give 60 to P2



How is money stored in Bitcoin?

- Transaction in **orphaned blocks** are invalid
  - **Wait 6 blocks** (~1 hour) before accepting transaction.
  - **Checkpoints** to prevent complete history rollback.



- **All transaction** are stored in the blockchain
  - (Currently ~14 GB)

Bitcoin: The technology

The Technology Behind BTC

- Hashing (double-SHA256, RIPEMD-160)
- Proof-of-work (hashcash proof)
- Dual key encryption (Elliptical Curve Digital Signature Algorithm, Merkle Trees)
- Peer-To-Peer Networking (similar to IRC Internet Relay Chat)

Hashing

- Hashing is applying an algorithm to find a short number (digest) of a block of data
- A checksum is an example hashing algorithm
- Every time you apply a hash to some data, you get the same hash number
- Hashes are one-way. If you have the data, you can find the hash. But, if you have the hash, you can’t figure out the data.
- Hashes are useful for verifying data

Checksum (type of hash)

- Add up numbers
- Take the least significant digits
- Example:

$$\begin{array}{r} 7\\ 7\\ 3\\ 4\\ 2\\ 5\\ 9\\ 0\\ 0\\ \underline{6}\\ 4\boxed{3} \end{array}$$

Checksum as Hash

- Checksums are a bad (but easy to do) hash
- SHA256 is a “secure hashing algorithm” that produces 256 bits of output (equivalent to a 78-digit number)
- A checksum doesn’t care about the order of the numbers
- With SHA256, any tiny change to the data being hashed will completely change the output hash value

Proof-of-Work

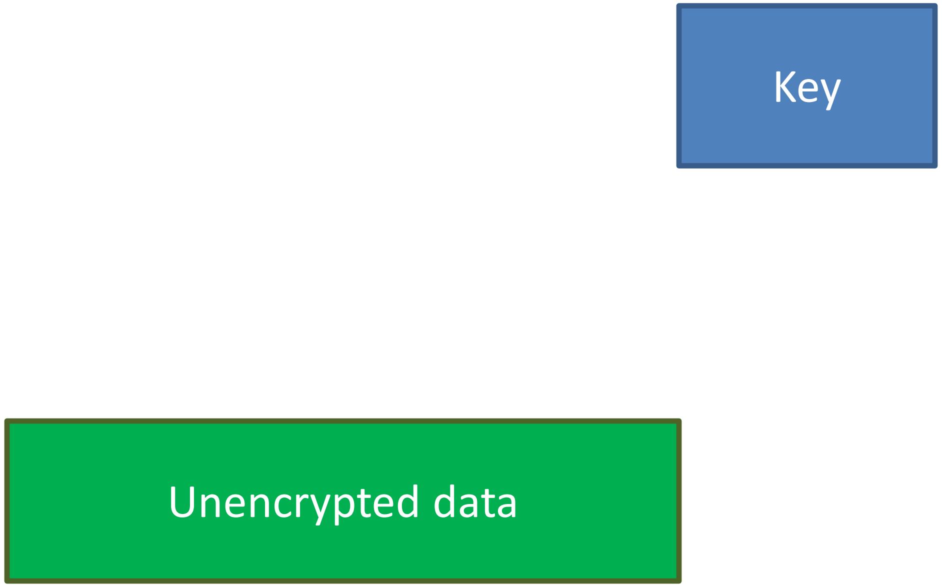
- Hashcash algorithm designed to prevent spam
- A hash is an apparently random set of 256 bits
- Every time you change something being hashed (for example, with a nonce) the hash completely changes
- There is a 50% chance the first bit might be 0
- If you change the thing-to-be-hashed a little bit, you could try a few times and get one with the first bit of 0
- First 2 bits: 25%
- First 10 bits: 0.0977%
- Find a hash with the first 63 bits as 0 (0.000000000000000001%), and you can publish a block and win 25 Bitcoins

Dual-key Encryption

- Fundamental to understanding virtual currencies
- Encrypting with a password is single-key
- Dual-key encryption uses two keys
- If one key is used to encrypt, the other key can be used to decrypt
- And vice-versa
- The key that encrypted CANNOT decrypt

Single Key Encryption

- A key (like a password) can encrypt data

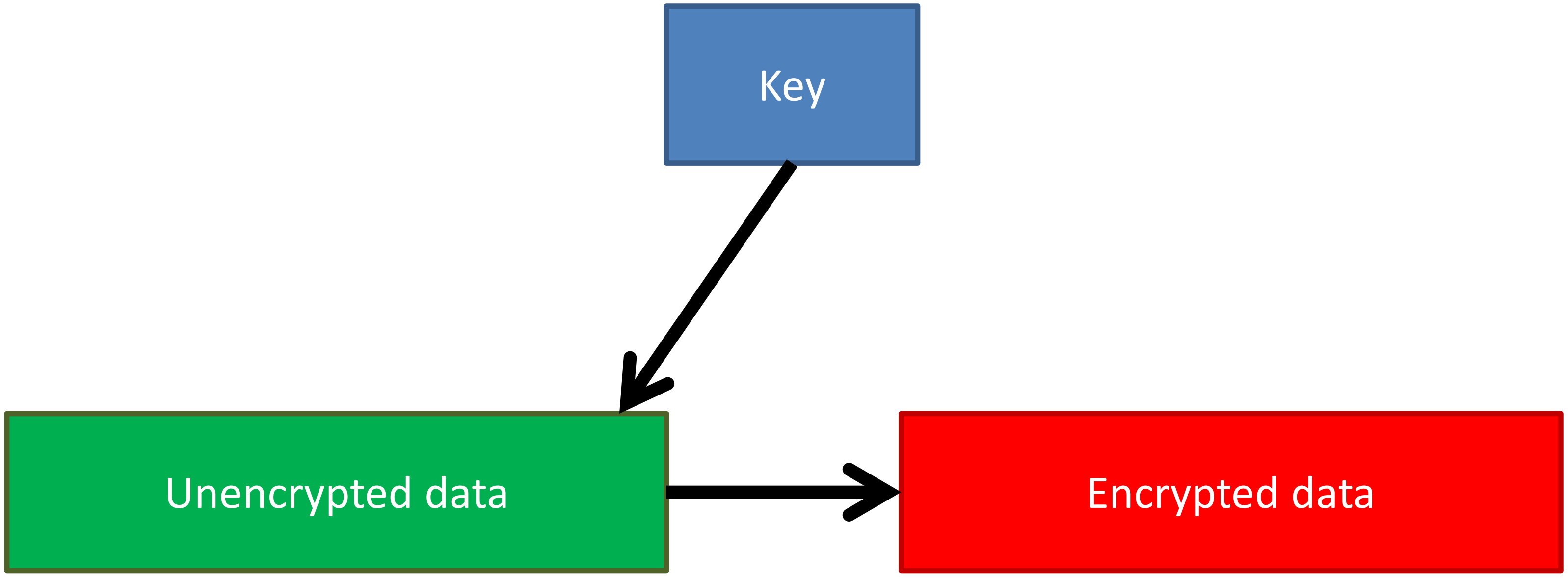


Key

Unencrypted data

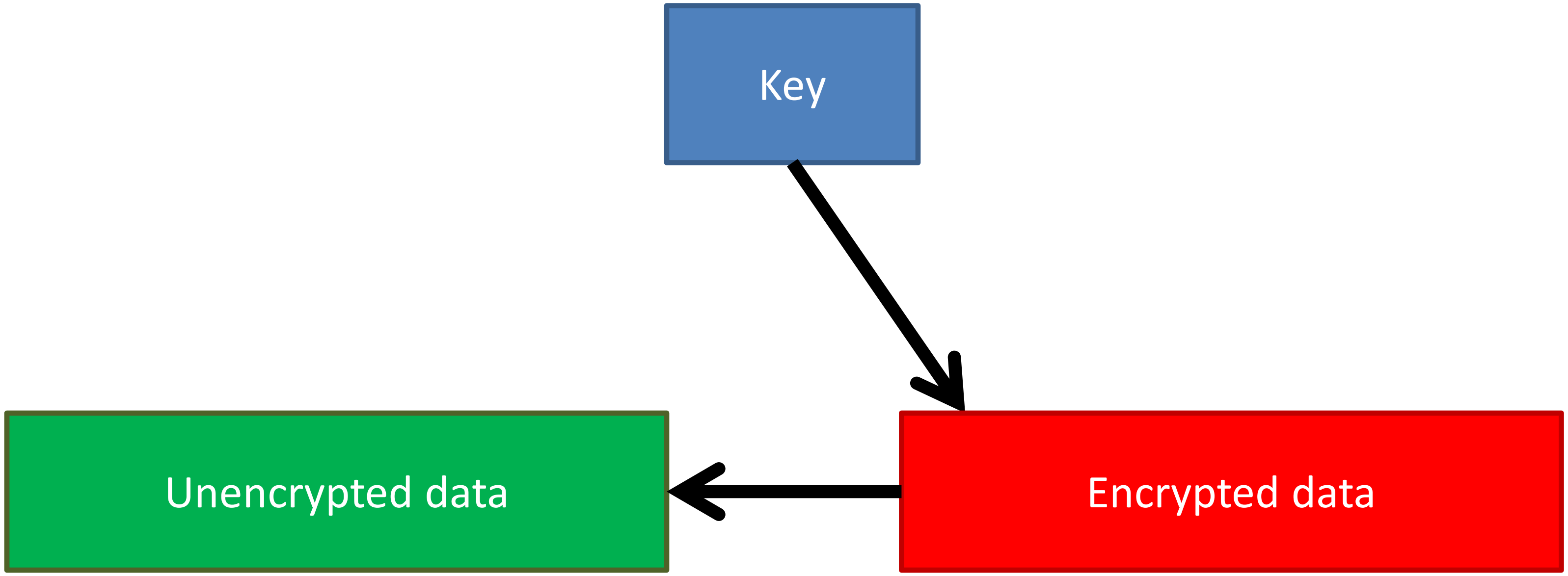
Single Key Encryption

- Use the key to encrypt some data



Single Key Encryption

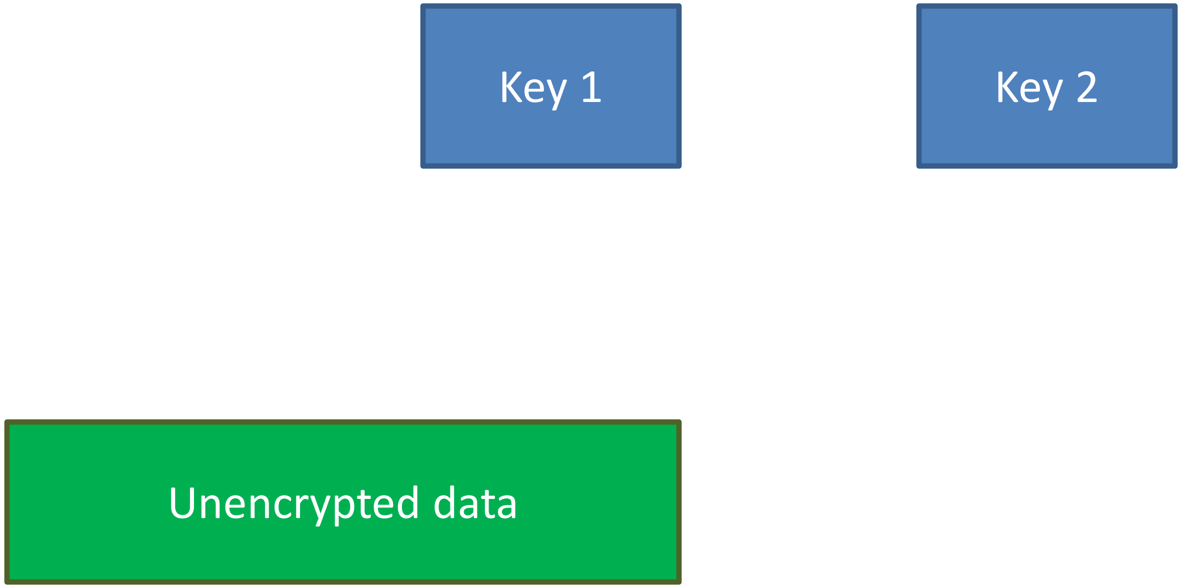
- Use the same key to unencrypt



- But, I have to give away the key
- And, I have to transmit that key

Dual-key Encryption

- There are two keys (like special passwords)



Key 1

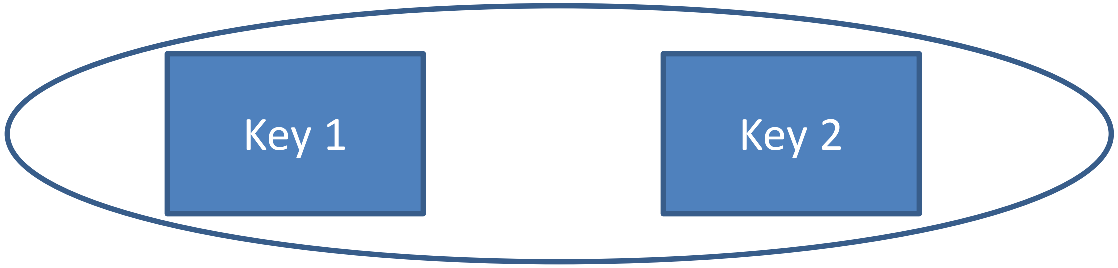
Key 2

These keys are big numbers

Unencrypted data

Dual-key Encryption

- Keys are generated in pairs. They go together



Key 1

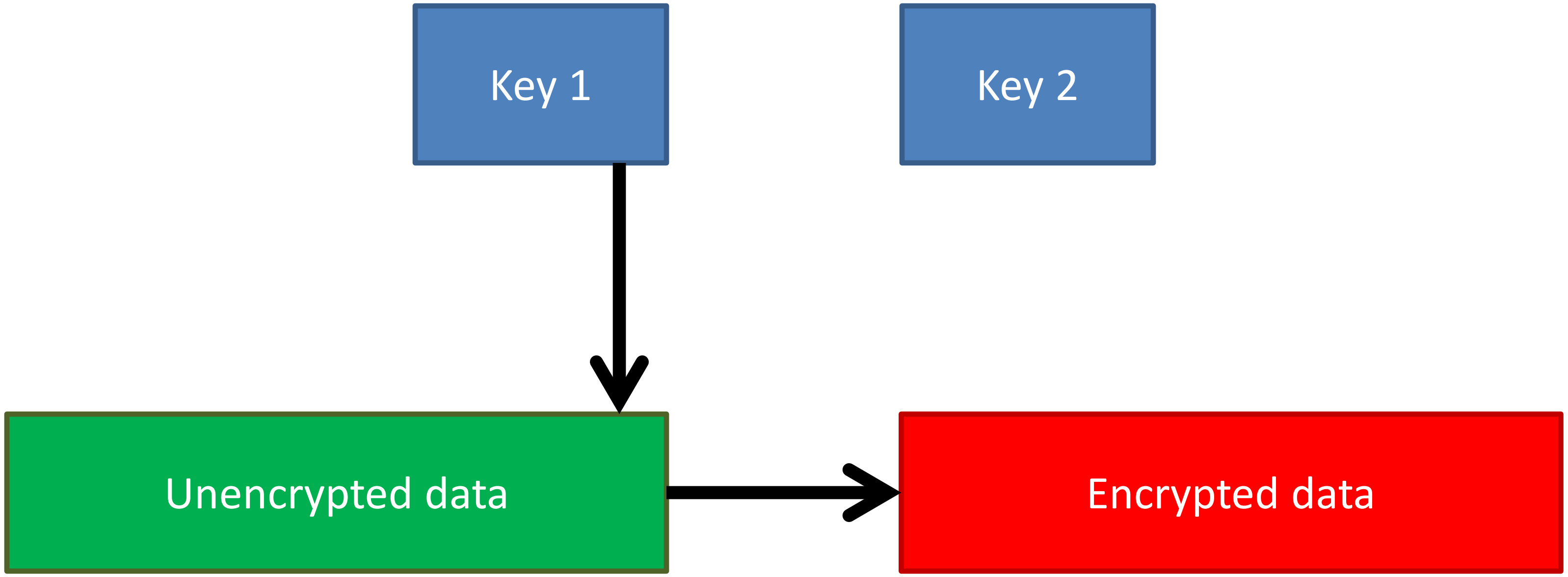
Key 2

Unencrypted data

- One key can’t be used to find the other

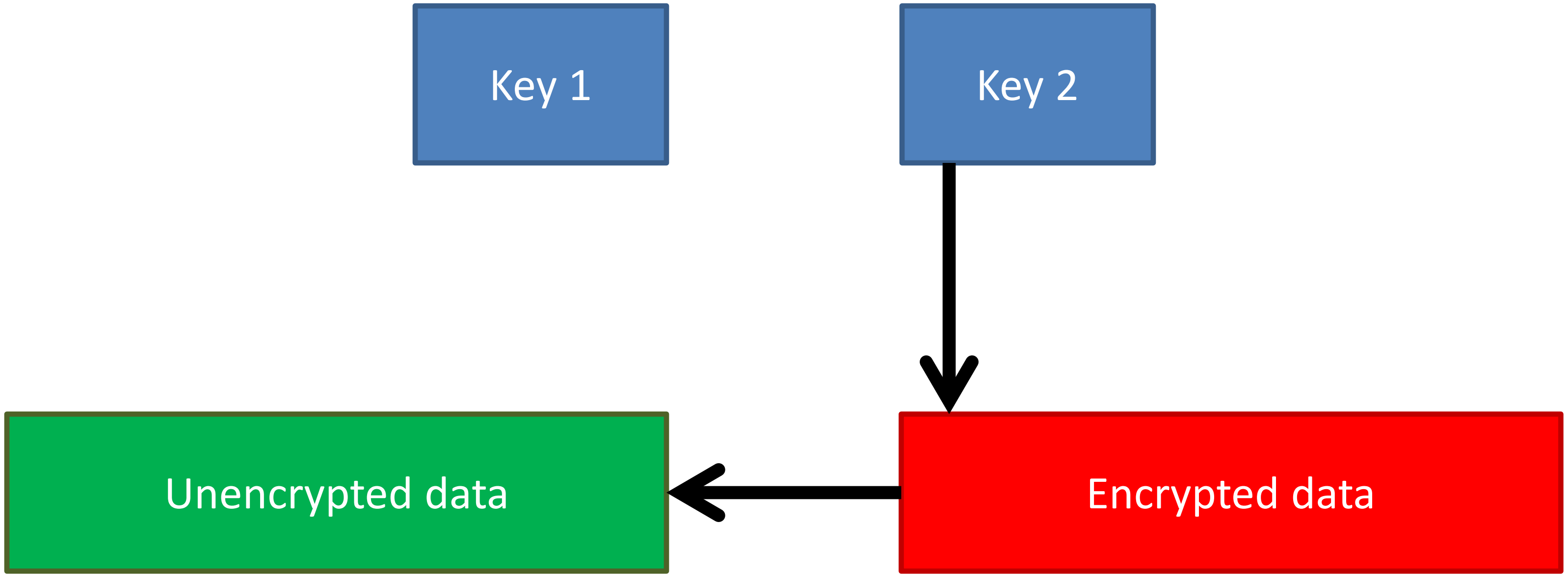
Dual-key Encryption

- Encrypt with Key 1



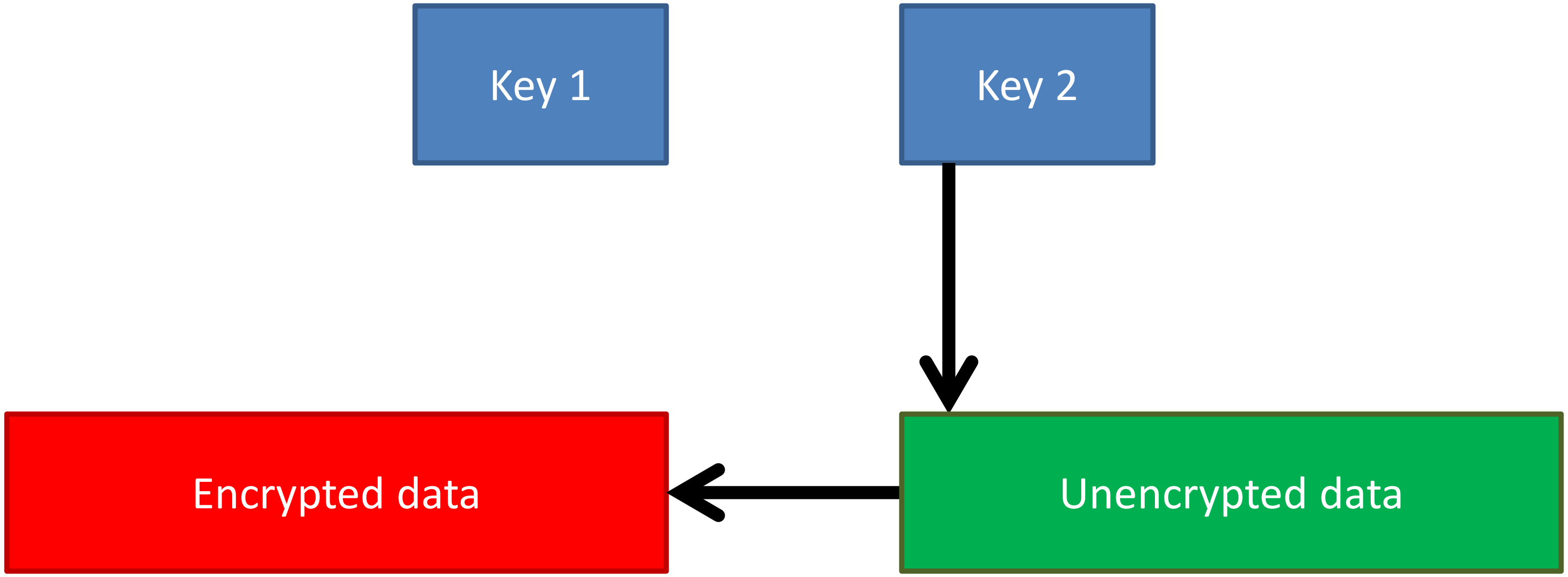
Dual-key Encryption

- Decrypt with Key 2



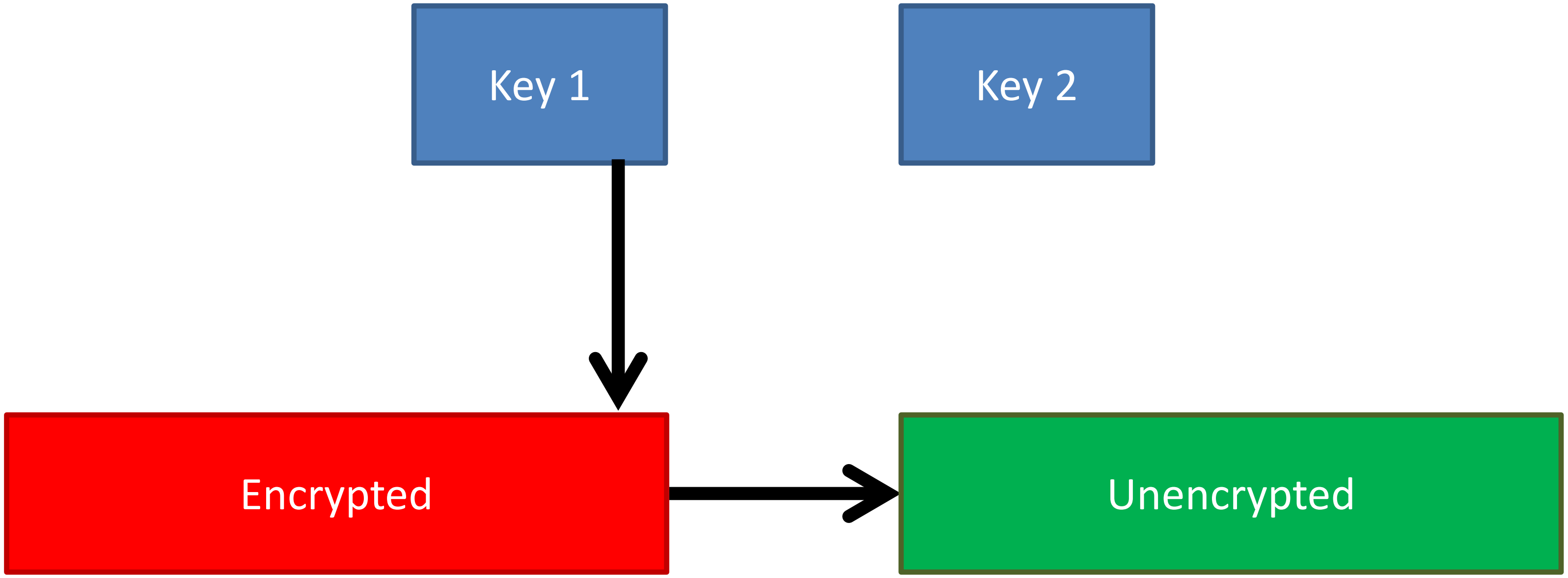
Dual-key Encryption

- Encrypt with Key 2



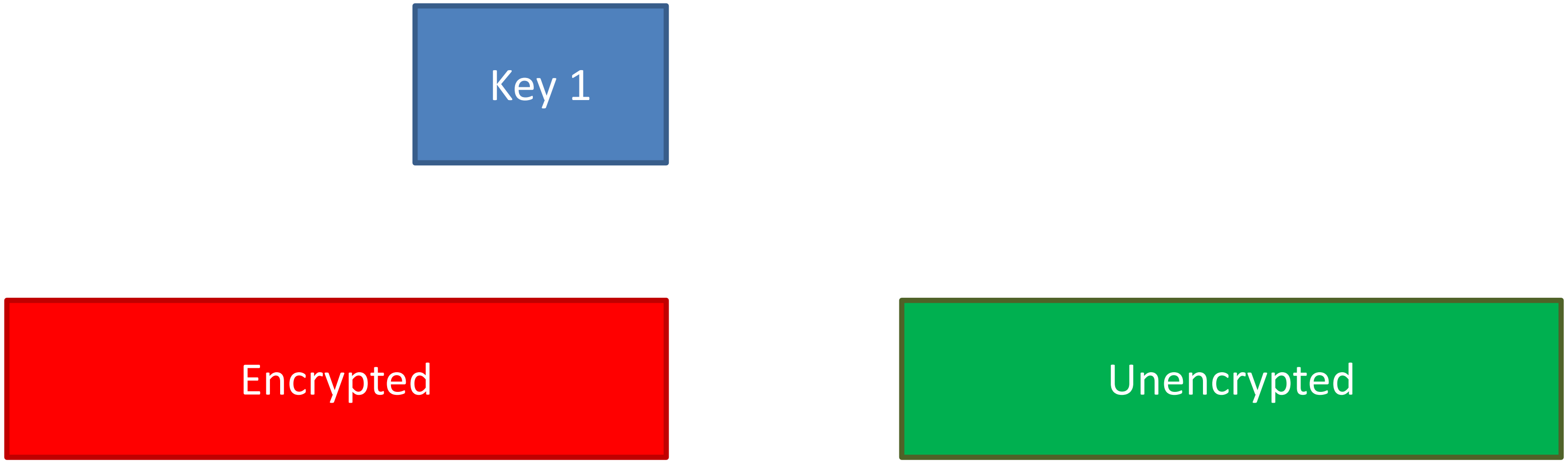
Dual-key Encryption

- Decrypt with Key 1



Dual-key Encryption

- If you only have one key, you can’t unencrypt your own data.



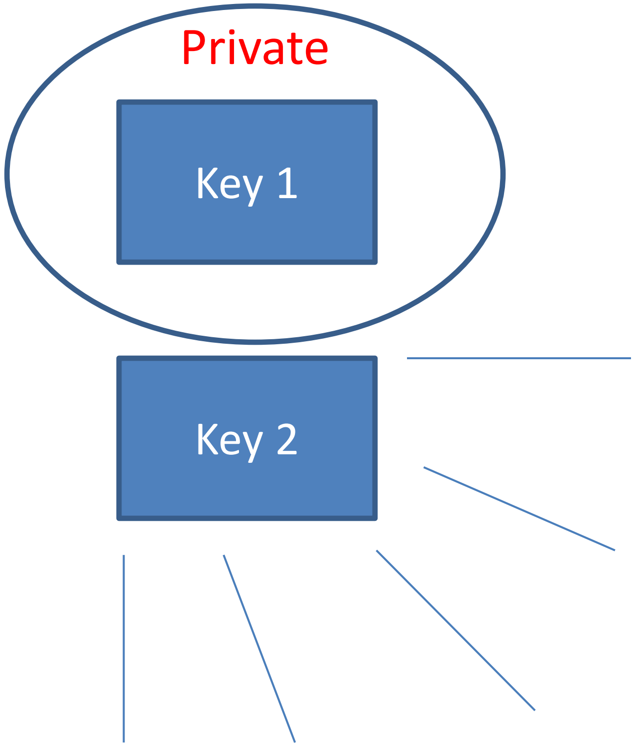
Key 1

Encrypted

Unencrypted

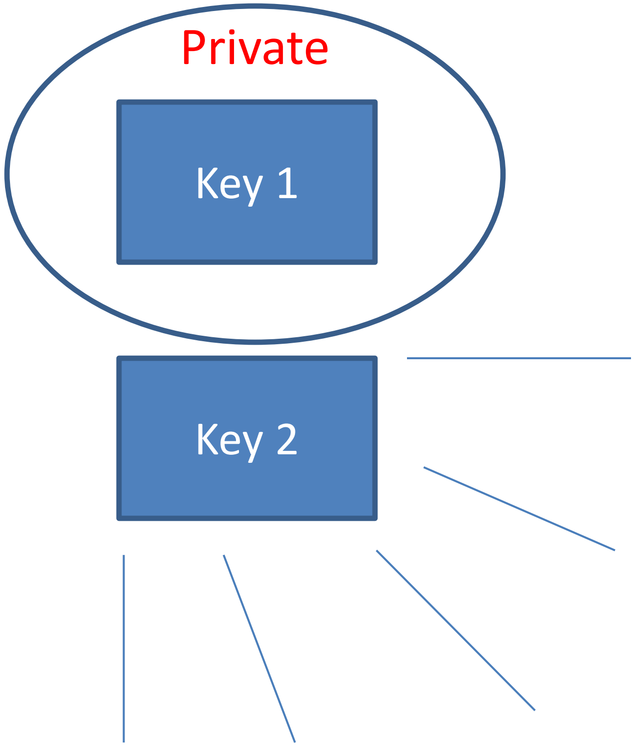
Private and Public Keys

- Although keys are symmetrical, usually one key is kept private, while the other one is considered public.



Private and Public Keys

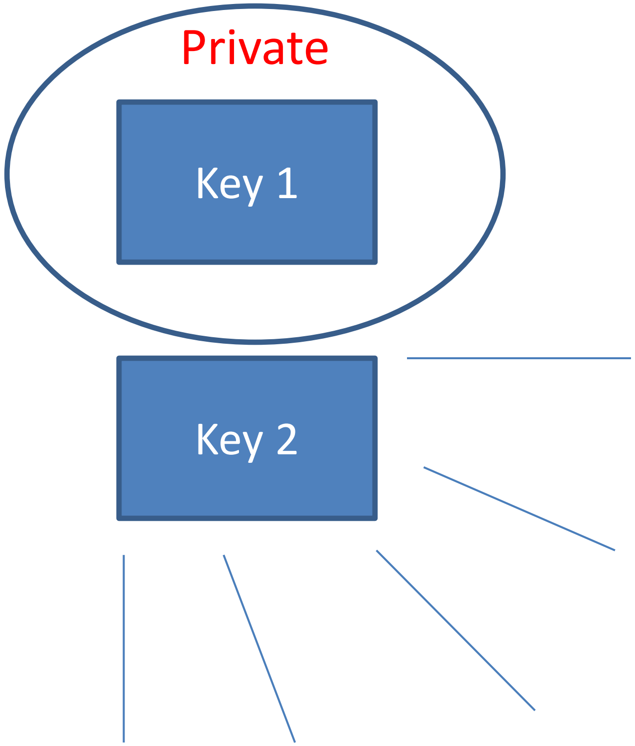
- If you want someone to sent you an encrypted file, tell them to use your public key to encrypt it.



- That way, nobody (not even the person who encrypted it) can read the encrypted data, except you.

Private and Public Keys

- And, if you want to send someone a file so only they can read it, you can just use their public key. It's probably on their website even.



Digital Signing

- Digital signatures prove that data came from the person with the private key
- For me to sign some text
  - Do a hash of the text
  - Encrypt the hash with my private key
  - Send the encrypted hash with the text
- To prove that I signed it
  - Do a hash of the text (same as I did)
  - Unencrypt the encrypted hash with my public key
  - Check that it matches the calculated value

What If I Lose My Key?

- The blockchain will store your address forever in case you later find it
- Ask Buddha for help
- The real number of Bitcoins will be less than 21 million because some of them are already lost

Peer-to-Peer

- Bitcoin originally used Internet Relay Chat
- When a peer starts up, they get a list of other peers and go looking for a few peers who aren’t so busy
- Peers share information about recent transactions and historical blocks
- Blocks are verified with Merkle tree signature

Bitcoin: Problems and issues

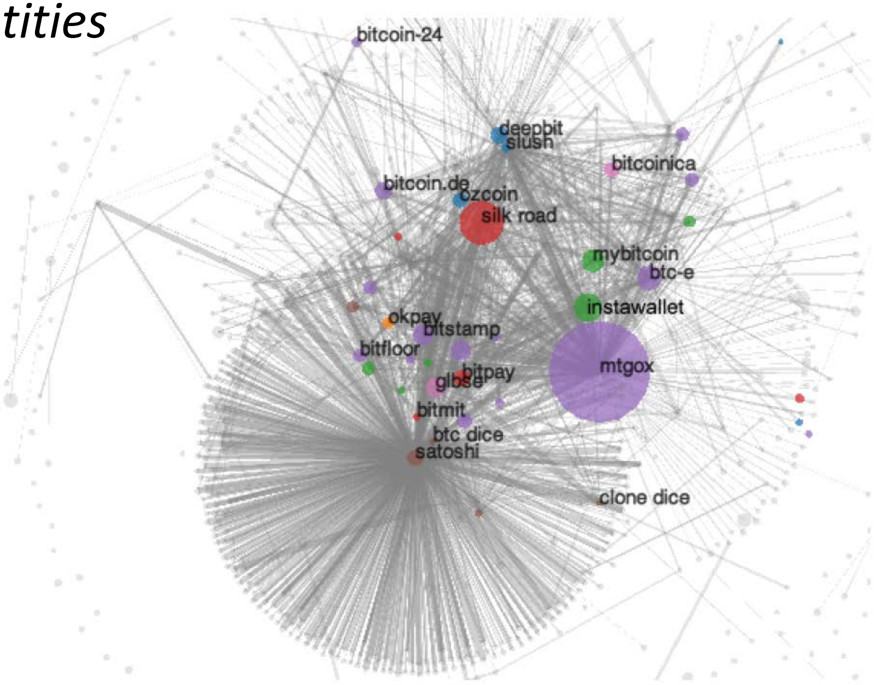
Anonymity (1/2)

- Bitcoin provides some anonymity (pseudonymity)
- Bitcoin addresses are like numbered bank accounts with a password
- The flow of money from address to address is completely public
- You can try to deny that you “have” BTC
- You can try to deny knowing where BTC went
- There are ways to increase anonymity

Anonymity (2/2)

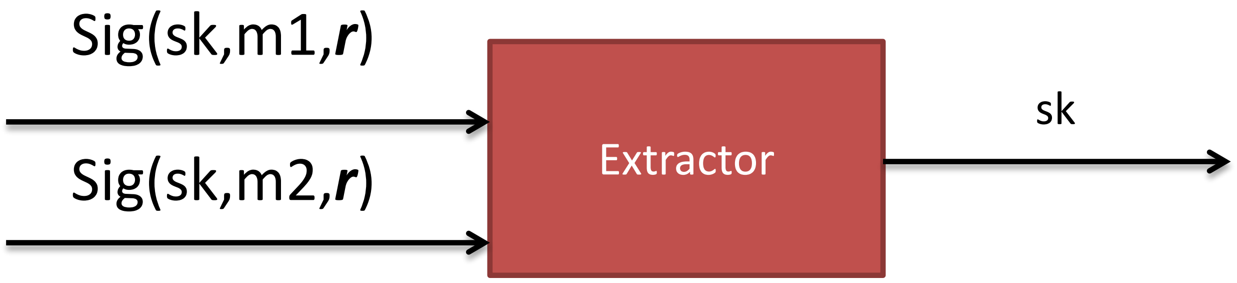
- **Problem**:
  - Every transaction ever made is **recorded forever**
- **Solution**?
  - *Use **new identity** for each transaction*
- **But**:
  - *Heuristics allow to **cluster** identities*

- **Anonymous alternatives:**
  - *Zerocoin, Zerocash…*



Users?
(and their devices)

- Unfortunate property of DSA



- This address

`1HKywxiL4JziqXrzLKhmB6a74ma6kxbSDj`

probably stole ~250000kr this way

(due to bug in Android Java based random generator)

Programmable money?

*“Bitcoin uses a **scripting system** for transactions. Forth-like, Script is simple, stack-based, and processed from left to right. **It is purposefully not Turing-complete, with no loops**.”*

E.g., “P1 gives 1 BTC to P2 if at least
2 out of (P1,P2,P3) sign this transaction”

Functionality: more than money?

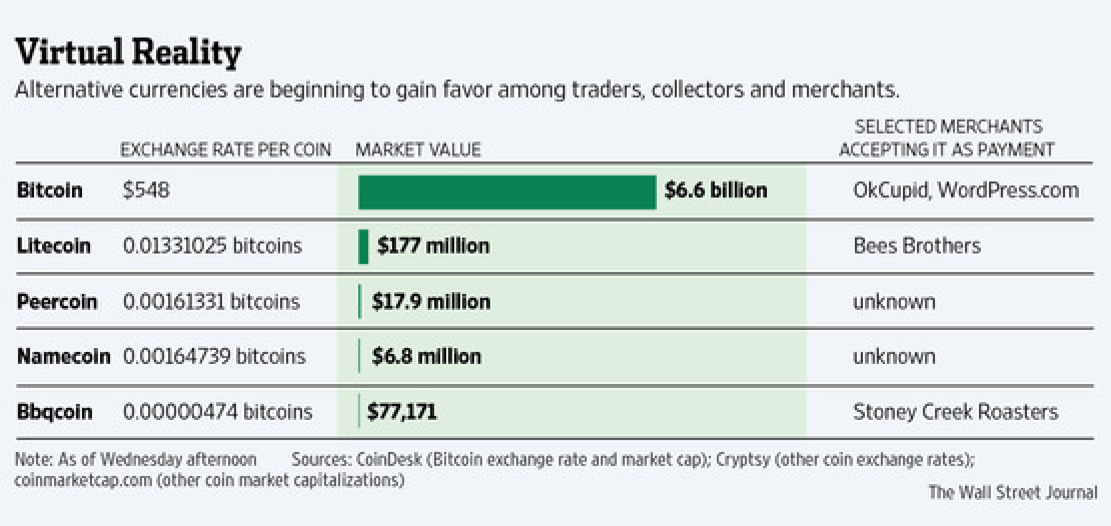
Security: malware payments?

Mining pools

- **Solving puzzles (mining) is hard!**
  - Miners join pools and share work/reward
- **How to optimally split work?**
- **Mechanism design?**
  - rational miner?
  - how to allocate reward?

Bitcoin’s greatest vulnerability

Market entry by competitors



Virtual Reality

Alternative currencies are beginning to gain favor among traders, collectors and merchants.

	EXCHANGE RATE PER COIN	MARKET VALUE	SELECTED MERCHANTS ACCEPTING IT AS PAYMENT
Bitcoin	$548	**$6.6 billion**	OkCupid, WordPress.com
Litecoin	0.01331025 bitcoins	**$177 million**	Bees Brothers
Peercoin	0.00161331 bitcoins	**$17.9 million**	unknown
Namecoin	0.00164739 bitcoins	**$6.8 million**	unknown
Bbqcoin	0.00000474 bitcoins	**$77,171**	Stoney Creek Roasters

Note: As of Wednesday afternoon Sources: CoinDesk (Bitcoin exchange rate and market cap); Cryptsy (other coin exchange rates); coinmarketcap.com (other coin market capitalizations)

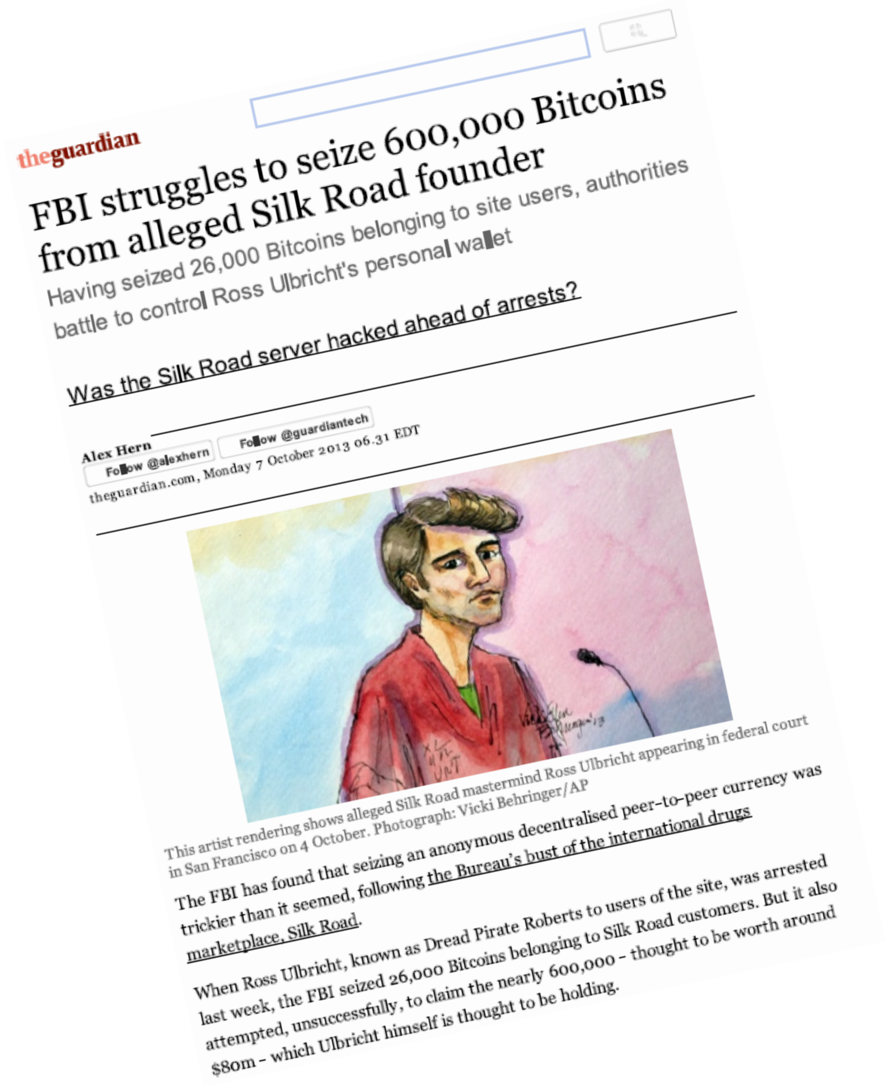
The Wall Street Journal

Silk Road Website

- A black market website that began on the TOR network starting in February of 2011
- Bitcoin predates Silk Road
- Transactions are paid for with Bitcoin
- Uses an escrow system to reduce abuse
- Looks like eBay, but most things are illegal—most notably, drugs
- Shut down by the FBI on 10/2/2013 and a suspected leader (Dread Pirate Roberts) was arrested
- Many millions of dollars worth of BTC were confiscated from people all over the world, even if they broke no laws
- On 11/6/2013 the website re-opened as 2.0, apparently with new management, but he calls himself DPR
- Silk Road is only the most successful marketplace for black market goods. There are others

Does Bitcoin have a stigma?

Silk Road online drug market



theguardian

FBI struggles to seize 600,000 Bitcoins from alleged Silk Road founder

Having seized 26,000 Bitcoins belonging to site users, authorities battle to control Ross Ulbricht's personal wallet

Was the Silk Road server hacked ahead of arrests?

Alex Hern

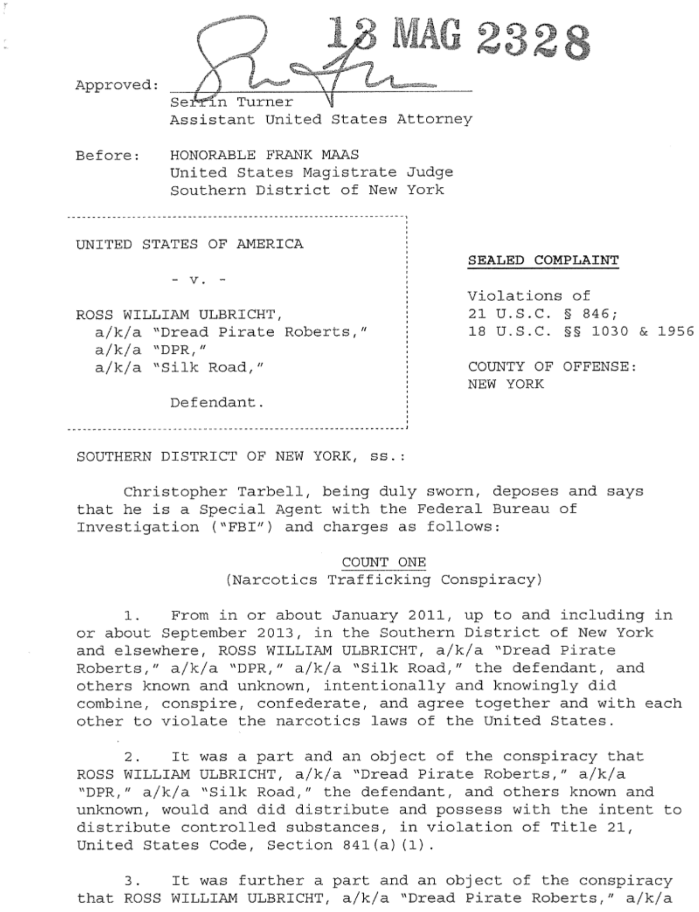
Follow @alexhern Follow @guardiantech

theguardian.com, Monday 7 October 2013 06.31 EDT

This artist rendering shows alleged Silk Road mastermind Ross Ulbricht appearing in federal court in San Francisco on 4 October. Photograph: Vicki Behringer/AP

The FBI has found that seizing an anonymous decentralised peer-to-peer currency was trickier than it seemed, following the Bureau's bust of the international drugs marketplace, Silk Road.

When Ross Ulbricht, known as Dread Pirate Roberts to users of the site, was arrested last week, the FBI seized 26,000 Bitcoins belonging to Silk Road customers. But it also attempted, unsuccessfully, to claim the nearly 600,000 - thought to be worth around $80m - which Ulbricht himself is thought to be holding.



13 MAG 2328

Approved: Serrin Turner
Assistant United States Attorney

Before: HONORABLE FRANK MAAS
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA

- v. -

ROSS WILLIAM ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

SEALED COMPLAINT

Violations of
21 U.S.C. § 846;
18 U.S.C. §§ 1030 & 1956

COUNTY OF OFFENSE:
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

Christopher Tarbell, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Narcotics Trafficking Conspiracy)

1. From in or about January 2011, up to and including in or about September 2013, in the Southern District of New York and elsewhere, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to violate the narcotics laws of the United States.

2. It was a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, would and did distribute and possess with the intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841(a)(1).

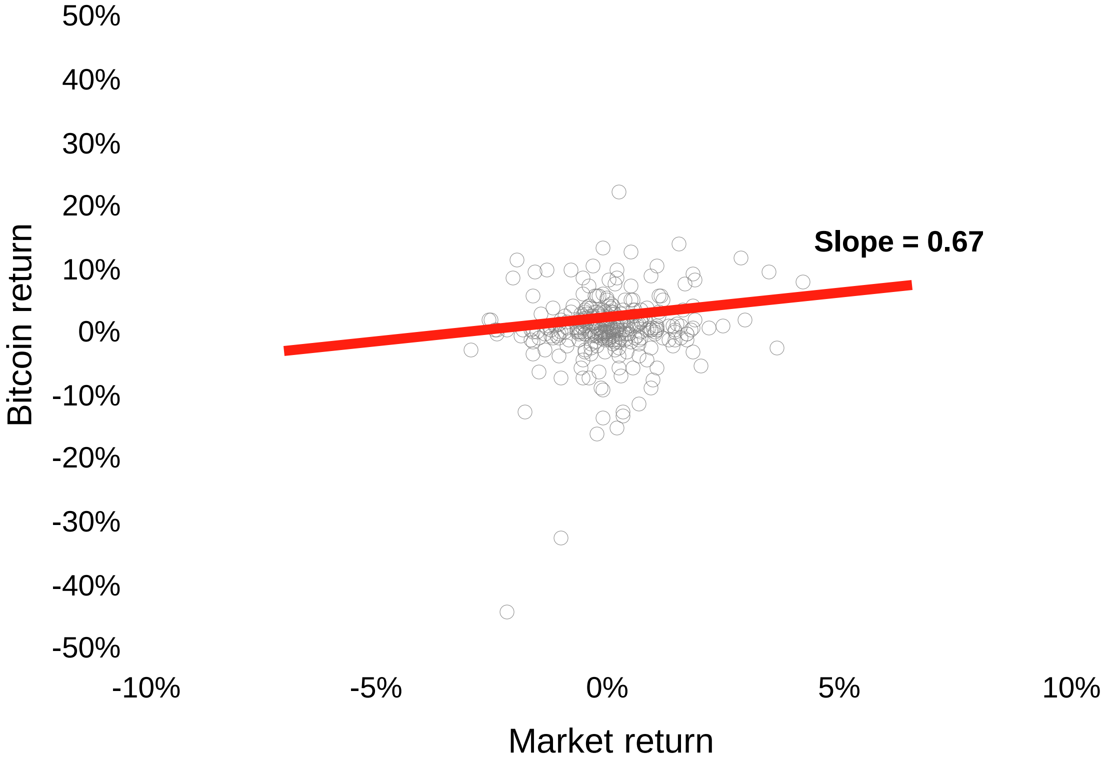
3. It was further a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a

Bitcoin and other currencies

Seems to be worthless for hedging

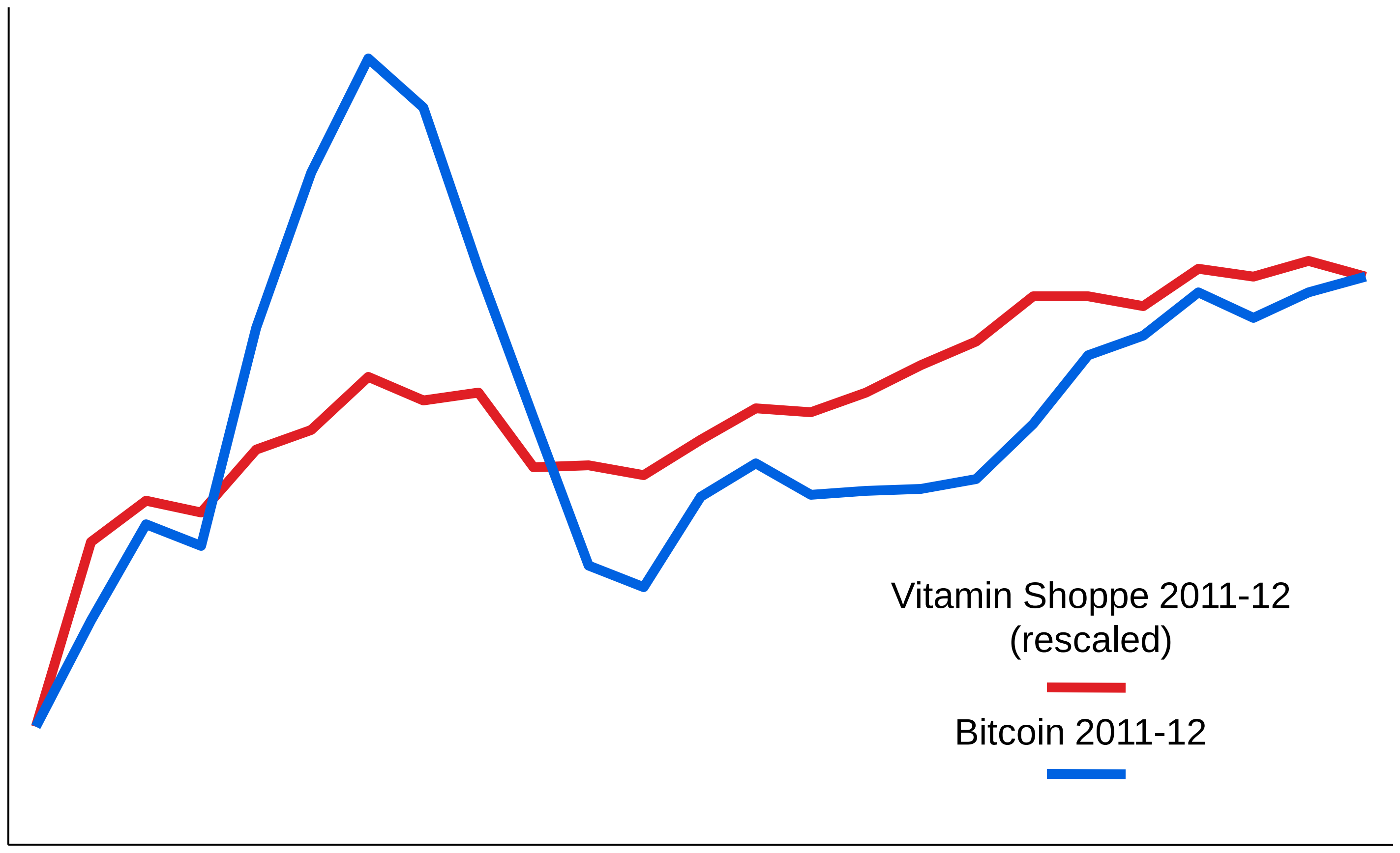
	EUR	JPY	CHR	GBP	Bitcoin
EUR	1.00	-0.19	-0.60	-0.65	0.05
JPY		1.00	0.33	0.22	0.01
CHF			1.00	0.42	-0.04
GBP				1.00	-0.02
Bitcoin					1.00

Bitcoin’s beta



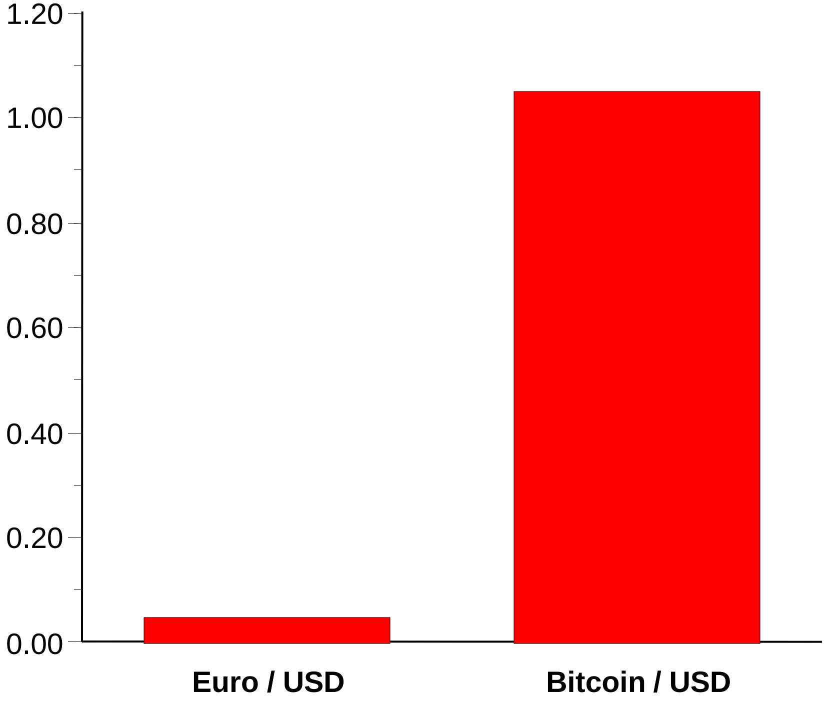
What’s the best hedge for Bitcoin?

Growth stocks like Vitamin Shoppe (NYSE VSI): *ρ* = 0.607



Bitcoin’s volatility

2013 to date



What can you *not* do with Bitcoin?

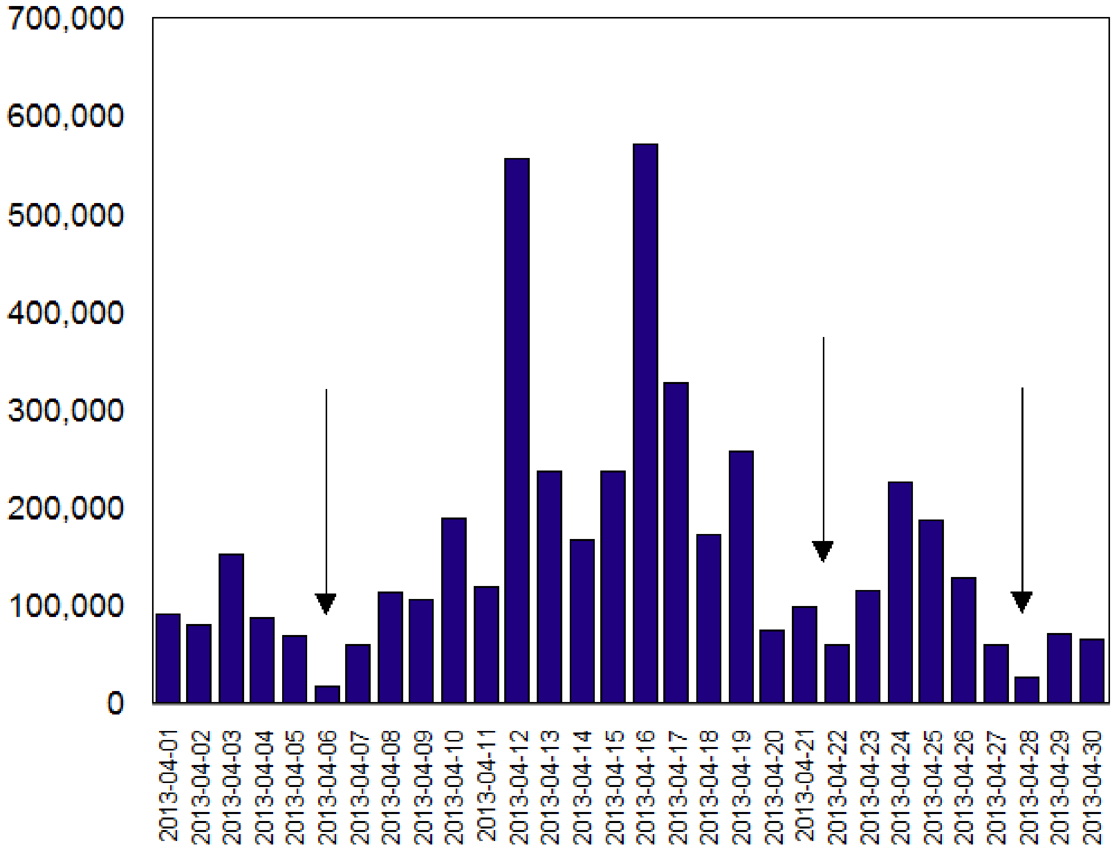
- Store it in a real bank that has deposit insurance

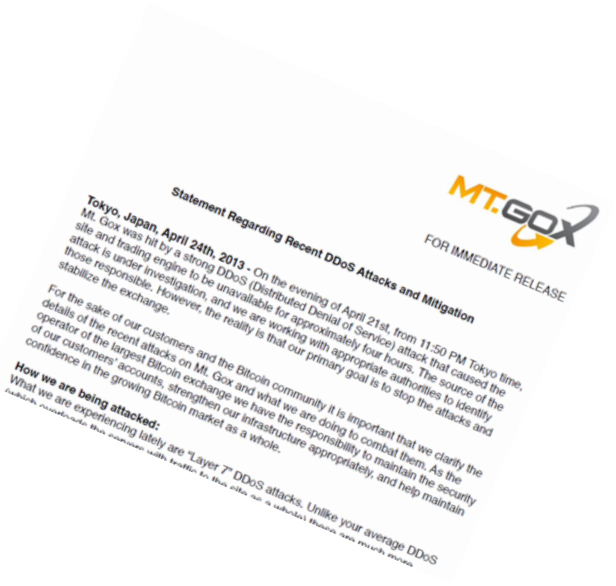
- Spend it anonymously

- Sell it short

Bitcoin’s security risks

Denial-of-service attacks depress Mt. Gox trading volume, April 2013





MT.GOX

FOR IMMEDIATE RELEASE

Statement Regarding Recent DDoS Attacks and Mitigation

Tokyo, Japan, April 24th, 2013 - On the evening of April 21st, from 11:50 PM Tokyo time, Mt. Gox was hit by a strong DDoS (Distributed Denial of Service) attack that caused the site and trading engine to be unavailable for approximately four hours. The source of the attack is under investigation, and we are working with appropriate authorities to identify those responsible. However, the reality is that our primary goal is to stop the attacks and stabilize the exchange.

For the sake of our customers and the Bitcoin community it is important that we clarify the details of the recent attacks on Mt. Gox and what we are doing to combat them. As the operator of the largest Bitcoin exchange we have the responsibility to maintain the security of our customers' accounts, strengthen our infrastructure appropriately, and help maintain confidence in the growing Bitcoin market as a whole.

How we are being attacked:

What we are experiencing lately are “Layer 7” DDoS attacks. Unlike your average DDoS (which overloads the servers with traffic to the site as a whole) these are much more

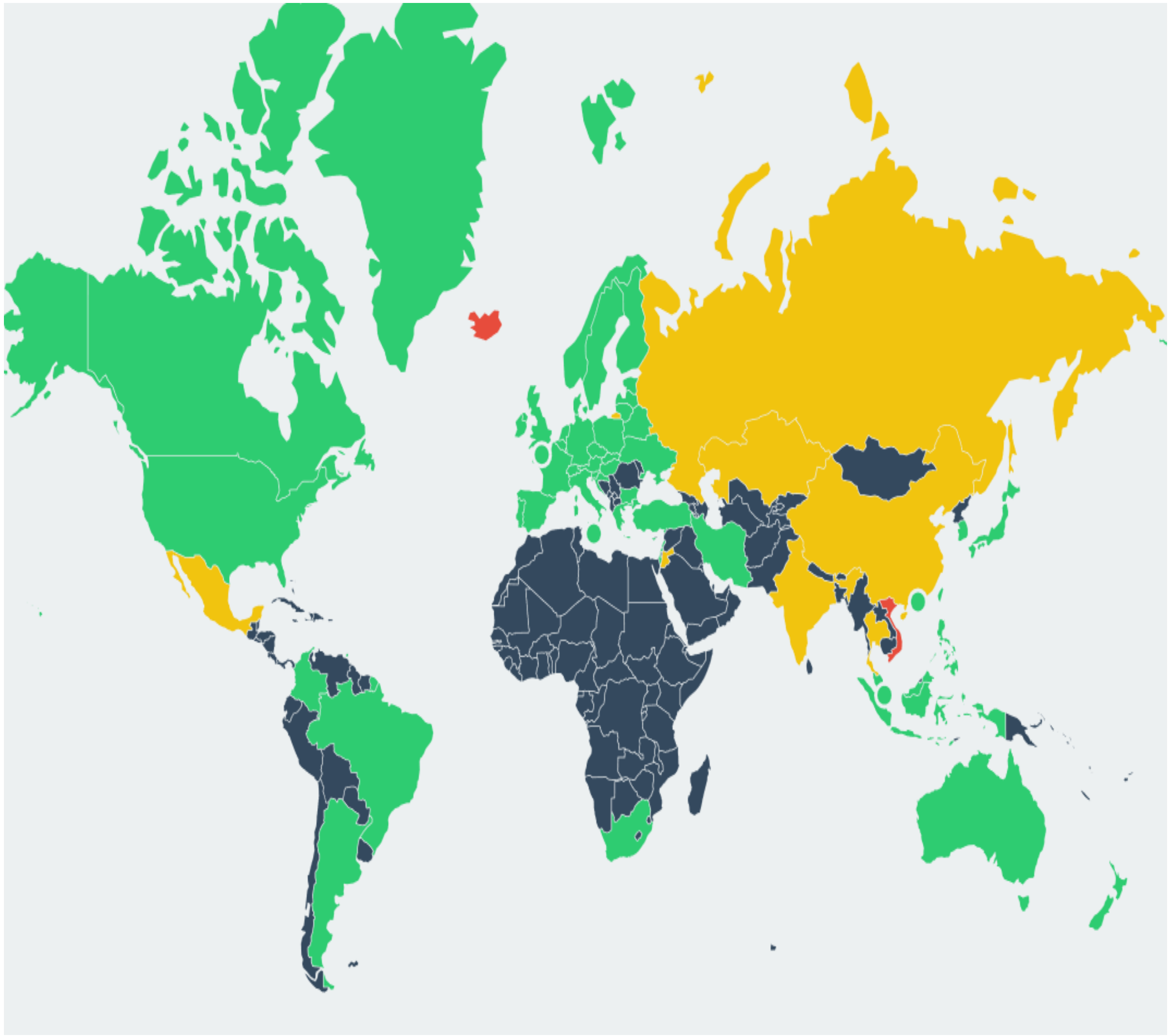
Risks

- Theft
- Lost keys
- Lost memory
- EMP Bomb
- Exchange Collapse
- Value collapse
- Hacking

How does the government feel about Bitcoin?

- Bitcoin precludes monetary policy
- Bitcoin precludes money laundering and tax evasion too

Legality of Bitcoin by country



- PERMISSIV E
- CONTENTI OUS
- HOSTILE
- UNKNOWN

Source: bitlegal.io

Threats to Bitcoin

- Competing currencies (Network effects)
- Blockchain forking due to philosophical conflicts
- Government attacks
- Denial of service attacks (Probably temporary)
- Hackers stealing currency
- Unrecoverable bug in the protocol
- Cryptography breakthrough (quantum computers?)
- Loss of confidence due to volatility
- Early adopters dumping
- Redlisting
- Processing power takeover
- Pressure from Visa/MasterCard
- Pressure from Internet providers
- Crushing increase in volume
- Selfish Miners problem
- Mutable transactions
- Byzantine Generals Problem
- Maybe lack of regulation really is bad
- Maybe free markets/capitalism just don’t work

Bitcoin is hard to regulate because it is:

- Decentralized
- Global
- Flexible
- Popular

Conclusion: Bitcoin and beyond

Conclusion

ADVANTAGES

- It is easy to set up and it is fast
- Low and irreversible transaction fees
- Without central authority???

(possible disadvantage)

DISADVANTAGES

- New and uninvestigated financial product
- History is full of illegal and questionable activity
- Absence of relevant theoretical background
- Highly volatile value and an unknown issuer
- Undefined legal status
- Unregulated commodity and absence of consumer protection
- Anonymity and blurry taxation status
- Illegal or undefined in most countries of the world

A final word…

Distributed currencies:

for the **good guys** or the **bad guys**?

- Crime is bad! Tax evasion is bad!
- But sometimes governments are bad too!