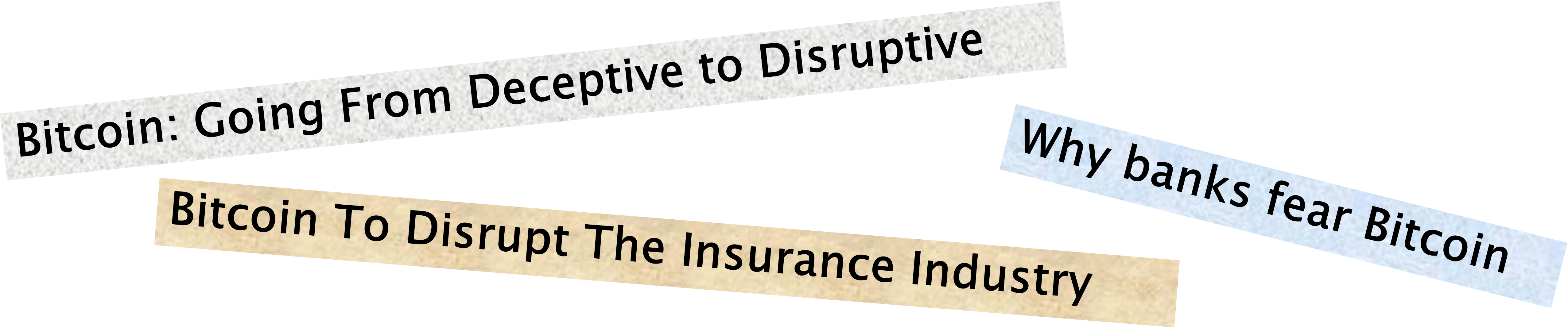
Blockchains: technology, applications & limitations

Arvind Narayanan
Princeton University

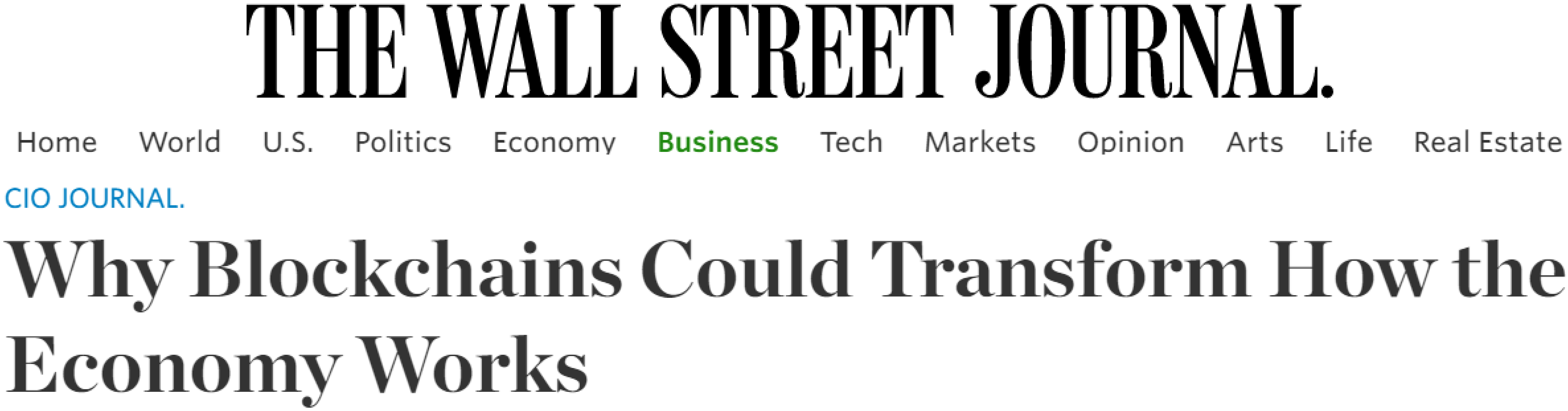
@random_walker



Bitcoin: Going From Deceptive to Disruptive

Why banks fear Bitcoin

Bitcoin To Disrupt The Insurance Industry

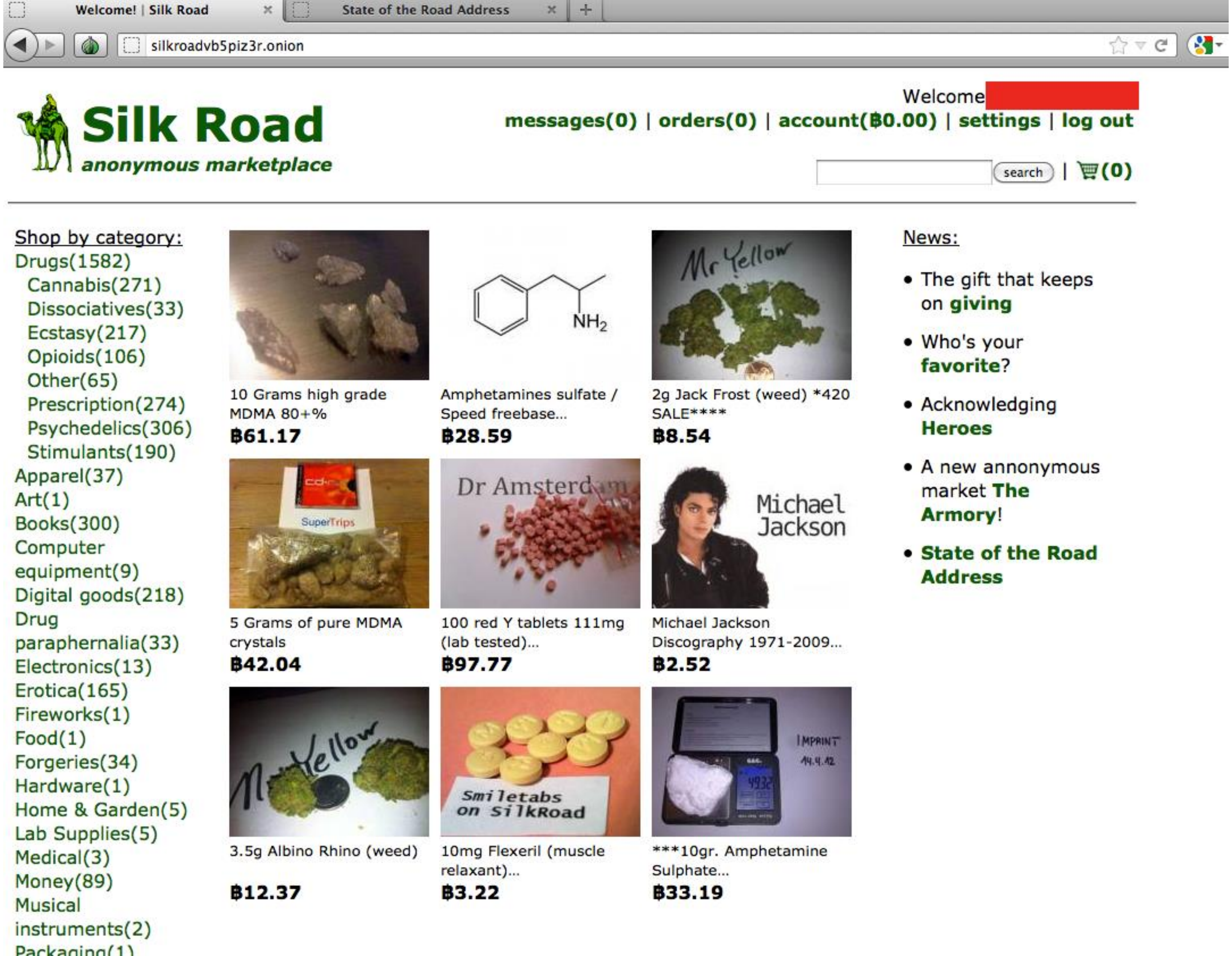


THE WALL STREET JOURNAL.

Home World U.S. Politics Economy **Business** Tech Markets Opinion Arts Life Real Estate

CIO JOURNAL.

Why Blockchains Could Transform How the Economy Works



Silk Road

anonymous marketplace

Welcome [redacted]

messages(0) | orders(0) | account(฿0.00) | settings | log out

search | (0)

Shop by category:

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)
- Erotica(165)
- Fireworks(1)
- Food(1)
- Forgeries(34)
- Hardware(1)
- Home & Garden(5)
- Lab Supplies(5)
- Medical(3)
- Money(89)
- Musical instruments(2)
- Packaging(1)

10 Grams high grade MDMA 80+%
฿61.17

Amphetamines sulfate / Speed freebase...
฿28.59

2g Jack Frost (weed) *420 SALE****
฿8.54

5 Grams of pure MDMA crystals
฿42.04

100 red Y tablets 111mg (lab tested)...
฿97.77

Michael Jackson Discography 1971-2009...
฿2.52

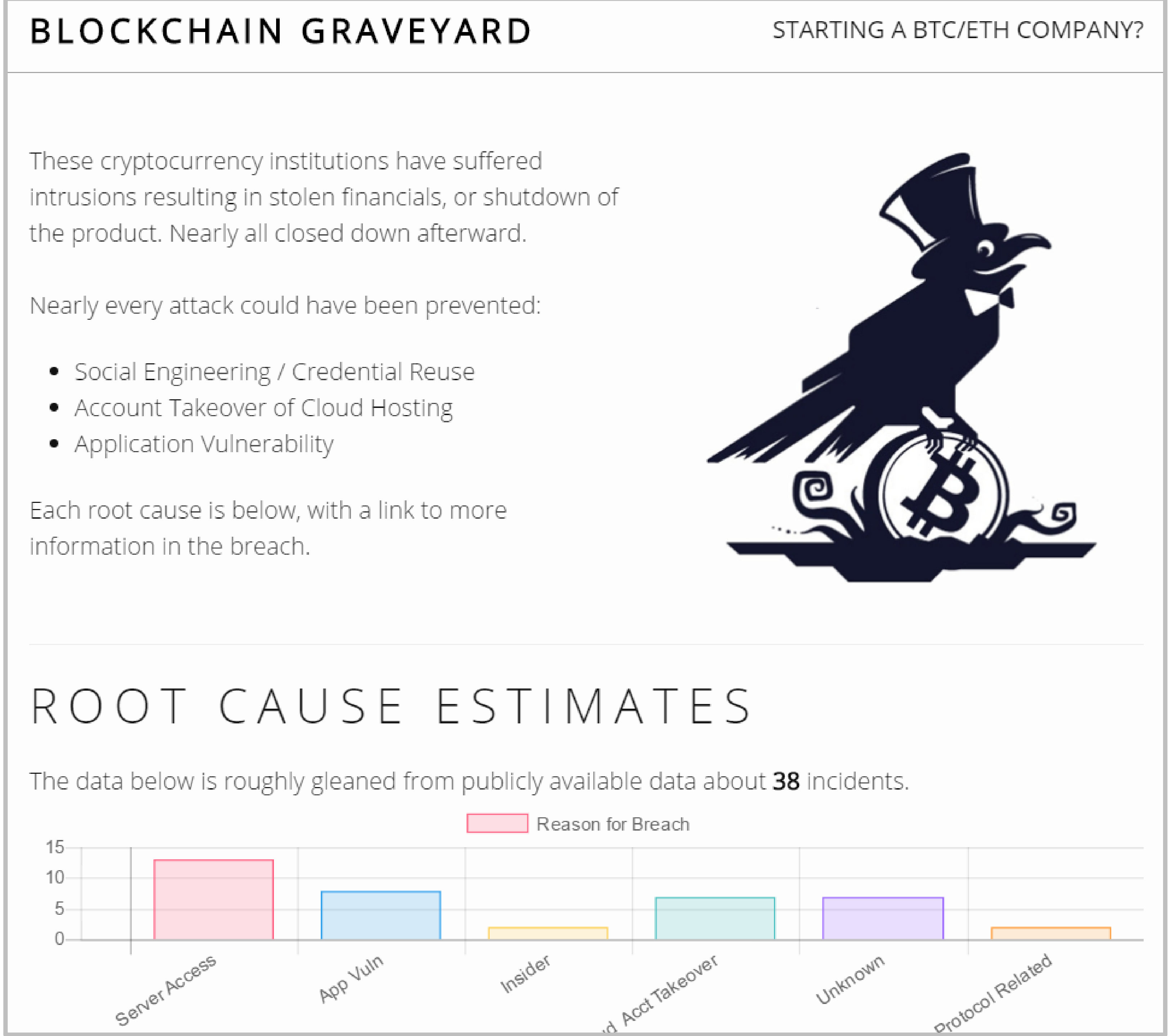
3.5g Albino Rhino (weed)
฿12.37

10mg Flexeril (muscle relaxant)...
฿3.22

***10gr. Amphetamine Sulphate...
฿33.19

News:

- The gift that keeps on **giving**
- Who's your **favorite**?
- Acknowledging **Heroes**
- A new annonymous market **The Armory**!
- **State of the Road Address**



BLOCKCHAIN GRAVEYARD

STARTING A BTC/ETH COMPANY?

These cryptocurrency institutions have suffered intrusions resulting in stolen financials, or shutdown of the product. Nearly all closed down afterward.

Nearly every attack could have been prevented:

- Social Engineering / Credential Reuse
- Account Takeover of Cloud Hosting
- Application Vulnerability

Each root cause is below, with a link to more information in the breach.

ROOT CAUSE ESTIMATES

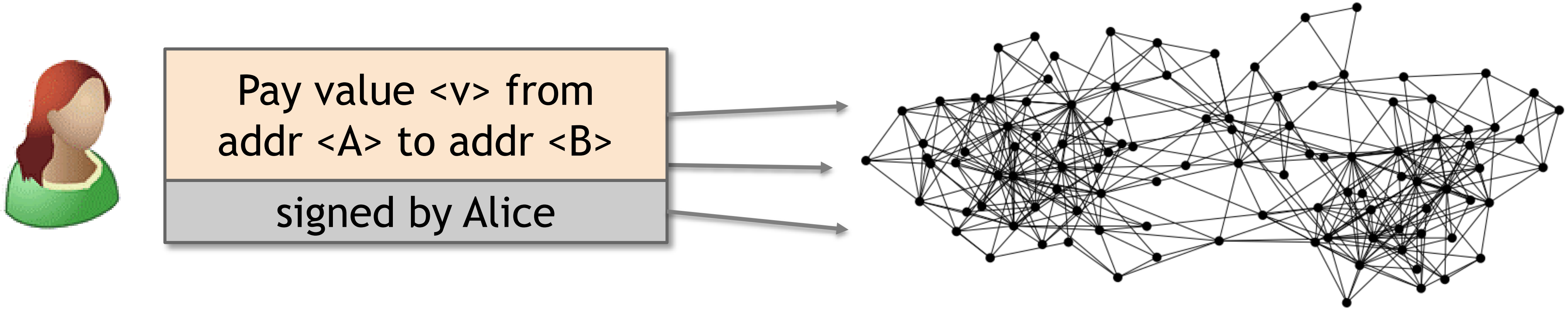
The data below is roughly gleaned from publicly available data about **38** incidents.

MTGOX
WHERE IS
OUR MONEY

MtGox
Are you
solvent?
MTGOX
WHERE IS OUR
MONEY?
© AP

Bitcoin is a peer–to–peer system

When Alice wants to pay Bob:
she broadcasts the transaction to all Bitcoin nodes



Pay value <v> from addr <A> to addr <B>

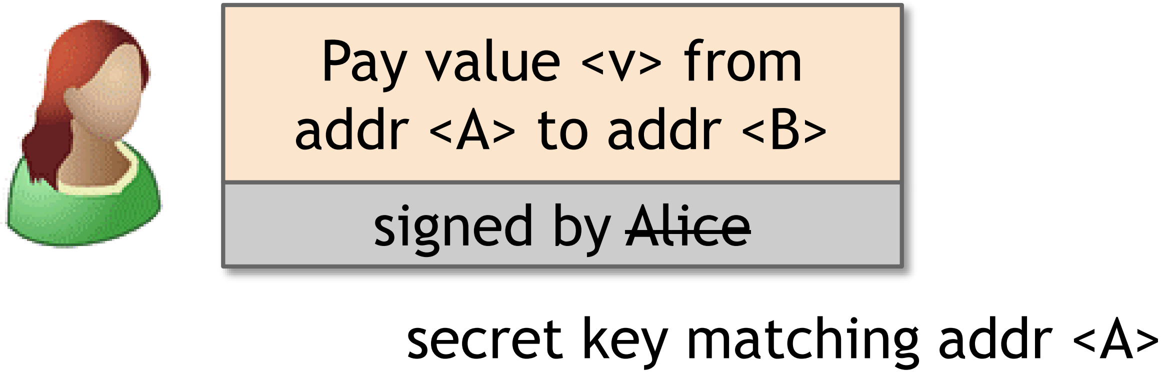
signed by Alice

Note: Bob's computer is not in the picture

Signing messages in Bitcoin

To "speak for" an address,
    you must know matching secret key

Message *msg* signed by secret key will be interpreted as:
    owner of *<addr>* says *<msg>*.



Pay value <v> from addr <A> to addr <B>

signed by ~~Alice~~

secret key matching addr <A>

Decentralized identity management

Addresses are the only identities in Bitcoin

Anybody can make a new identity at any time
    make as many as you want!

No central point of coordination

Goal of the Bitcoin protocol

Tinkerbell effect

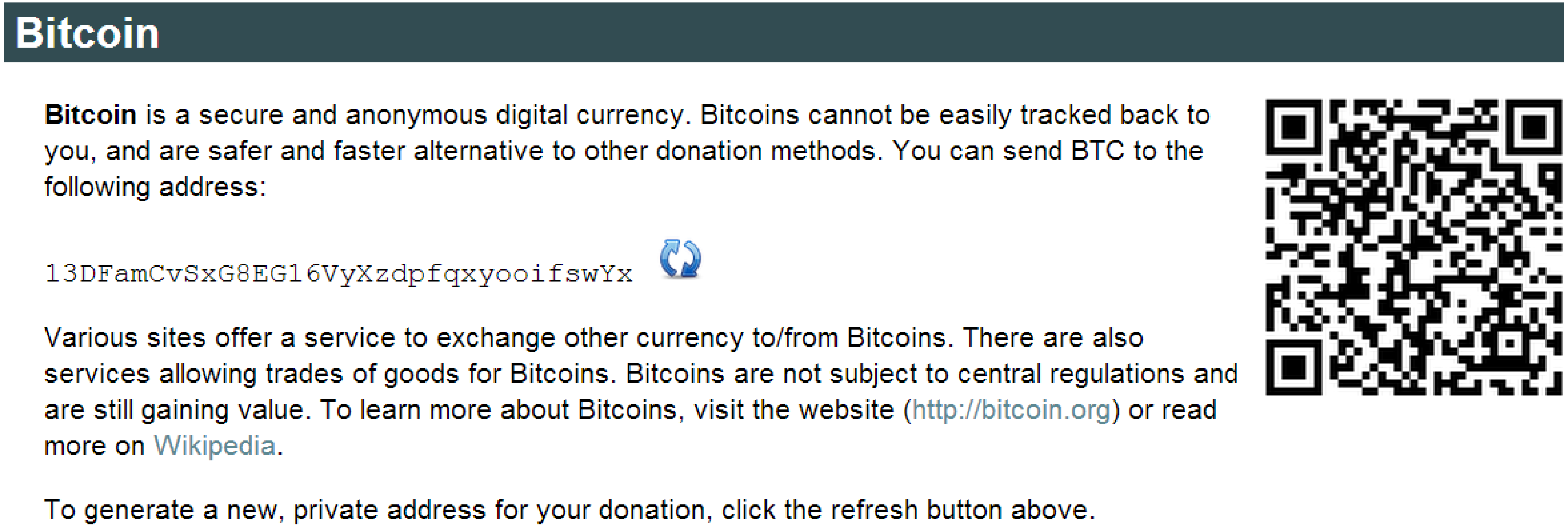
Record transfers of value between addresses in a global ledger

From	To	Value	Signature
1JLinwE…	1NcZ3pw…	0.1	H3QWJA…
336Ka4r…	18nE2xQ…	2.4	fWRMtB…
…	…	…	

How to keep the ledger secure?

What about people and companies?

Wikileaks donation page



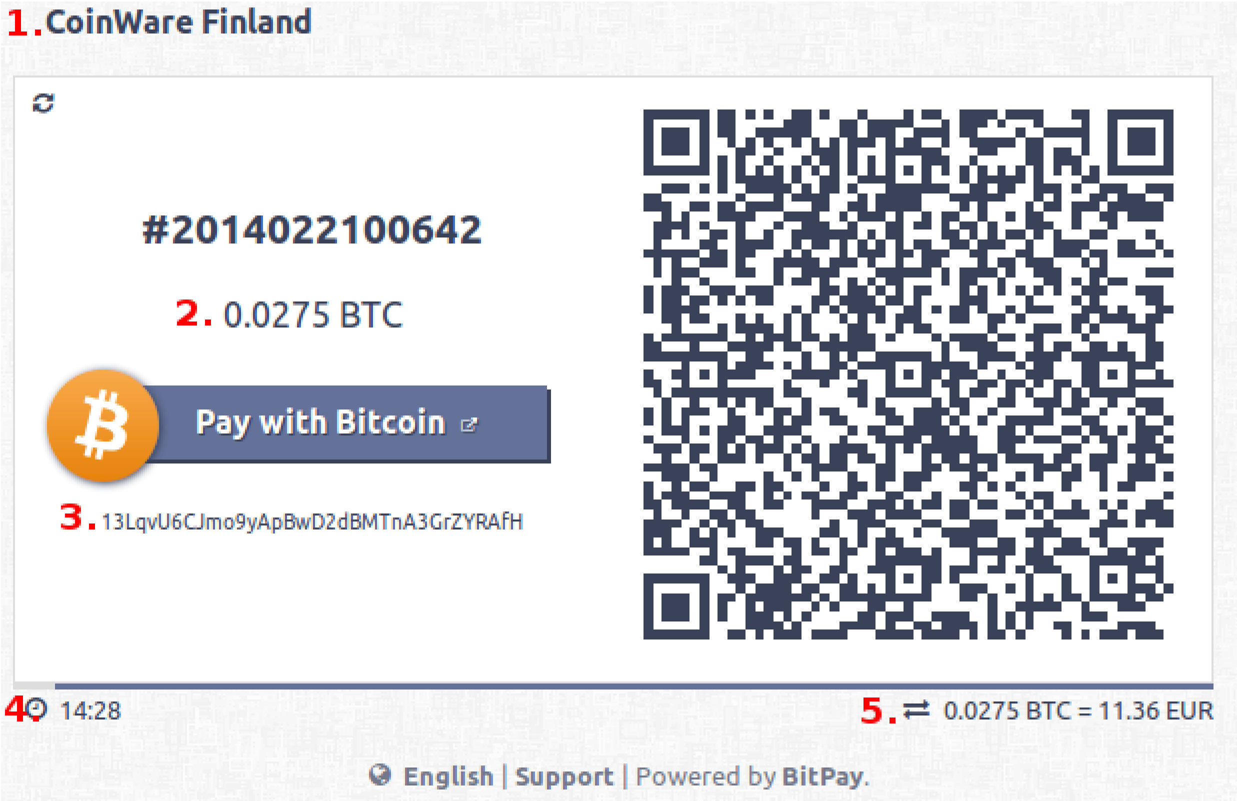
Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

`13DFamCvSxG8EG16VyXzdpfqxyooifswYx`

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (http://bitcoin.org) or read more on Wikipedia.

To generate a new, private address for your donation, click the refresh button above.



1. CoinWare Finland

#2014022100642

2. 0.0275 BTC

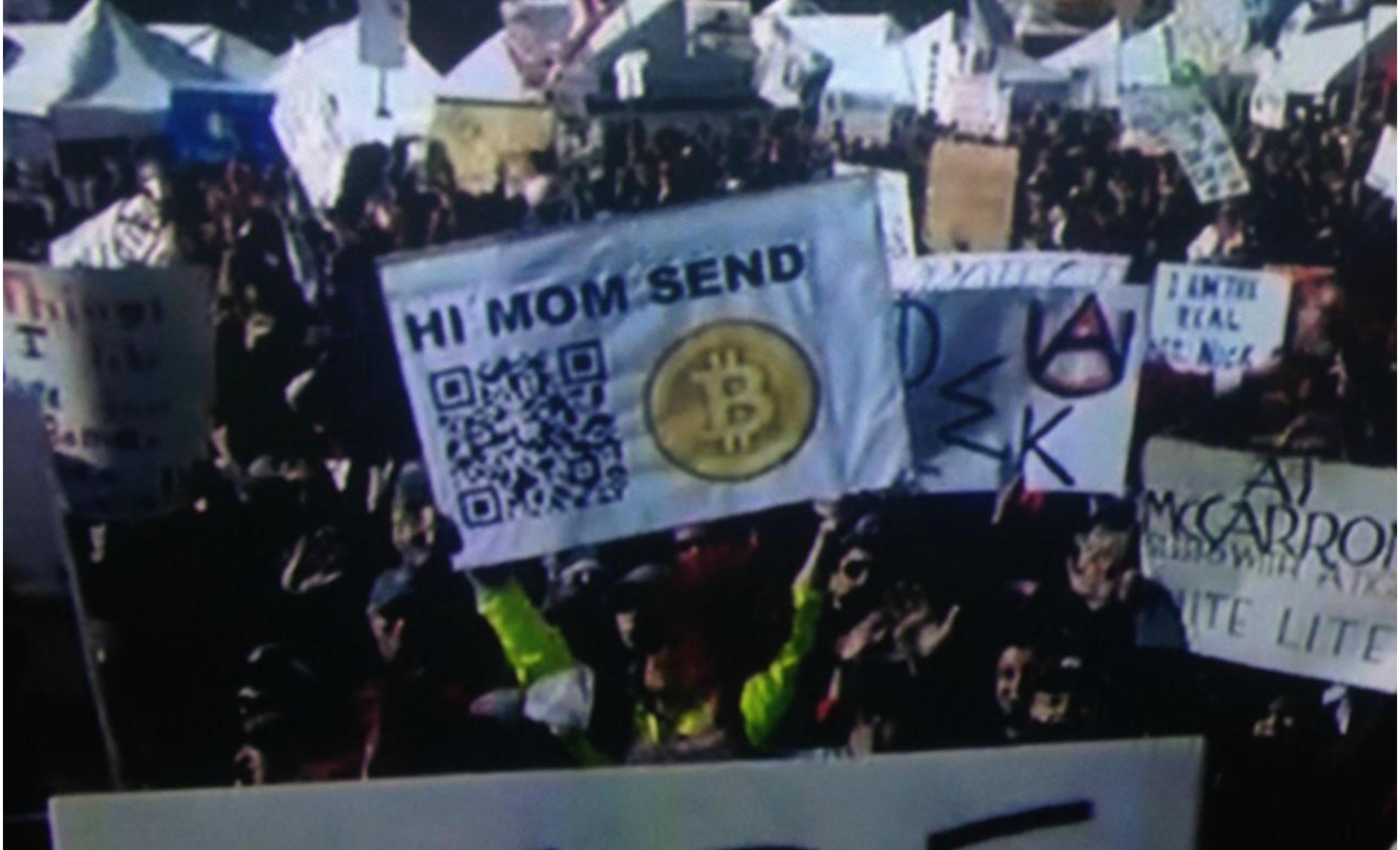
3. 13LqvU6CJmo9yApBwD2dBMTnA3GrZYRAfH

4 14:28

5. ⇄ 0.0275 BTC = 11.36 EUR

English | Support | Powered by BitPay.

Clicking the button opens the Bitcoin app on your computer or smartphone


HI MOM SEND
I AM THE
REAL
AJ
McCARRON
ITE LITE

Users in Bitcoin

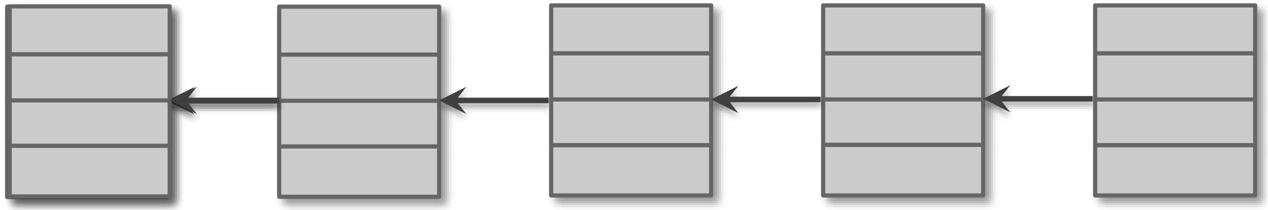
- Exchange addresses
- Issue signed statements to Bitcoin network authorizing transfers of value

Blockchain:

global, public, immutable ledger

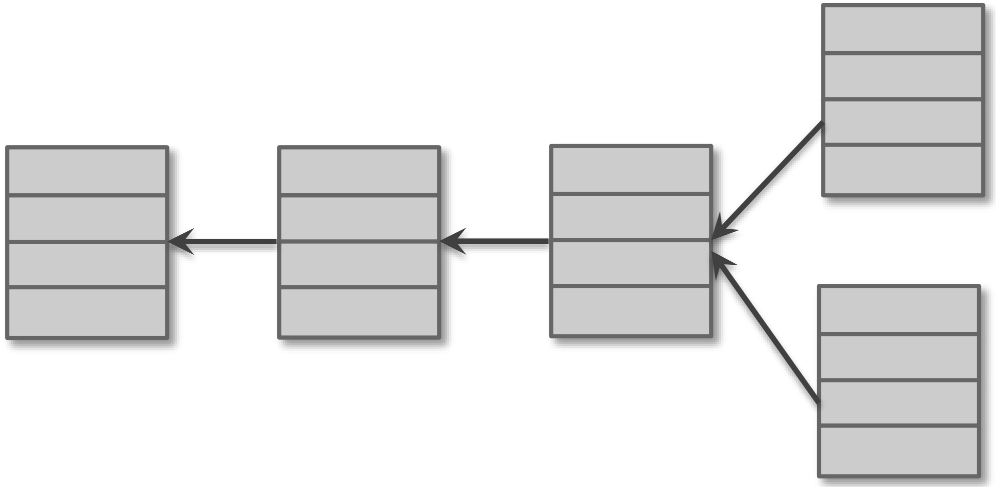
Blockchain: immutable ledger

- Collect transactions into blocks
- Each block links to previous block



- Each block has a cryptographic digest of prev. block

How to resolve inevitable disagreements?



“One CPU one vote”

Miners’ say in decision-making is proportional to computing power

Evolution of mining

CPU

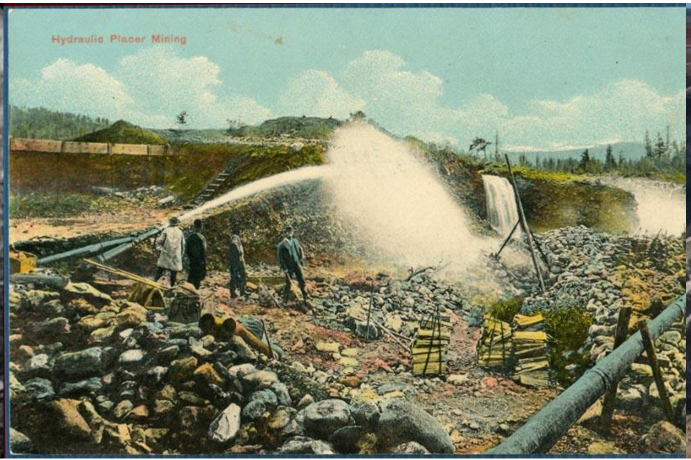
GPU

FPGA

ASIC

gold pan

sluice box



placer

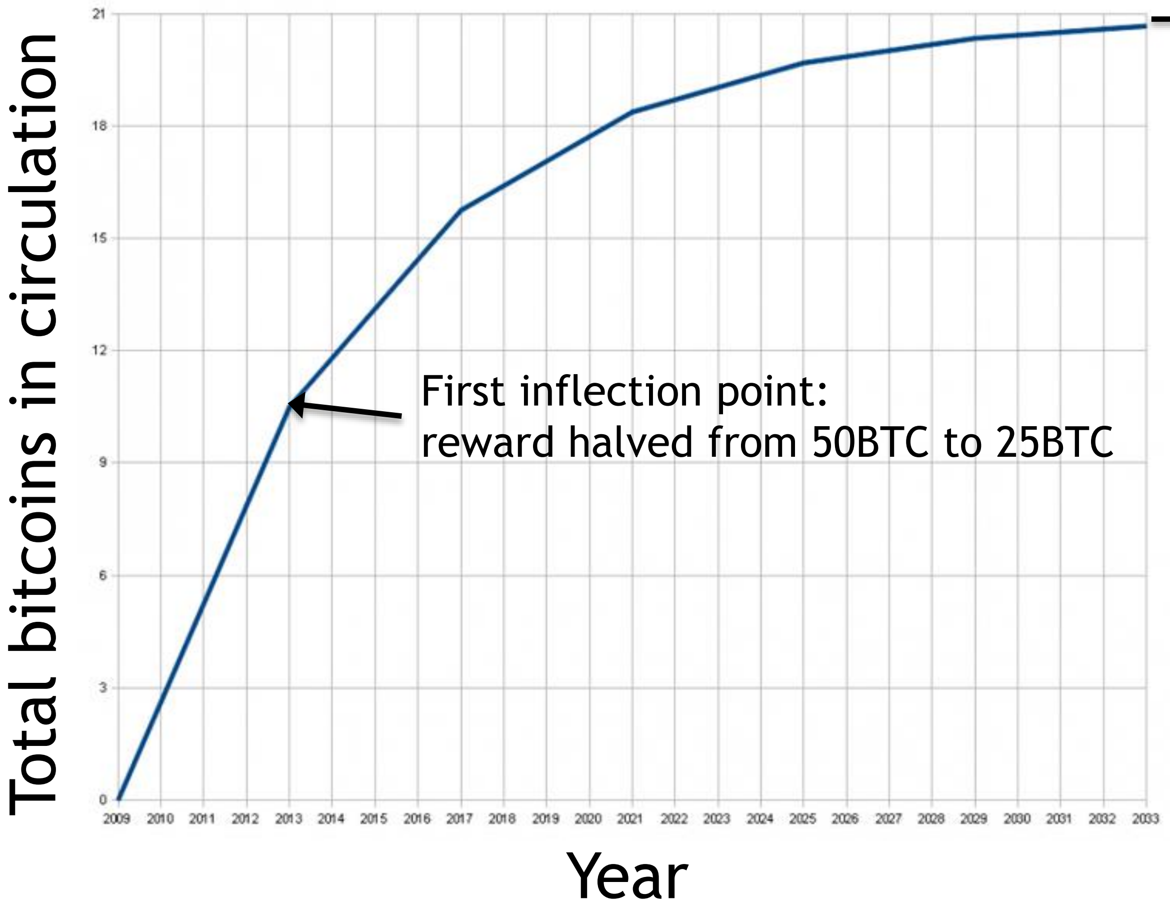
pit

Miners in Bitcoin

- Collect transactions from users
- Assemble them into blocks
- Contribute blocks to ledger by solving computationally hard puzzle
- Collect reward

Currently about a *trillion trillion* operations every 10 minutes

There’s a finite supply of bitcoins



First inflection point:
reward halved from 50BTC to 25BTC

Total supply: 21 million

- Block reward is how new bitcoins are created
- Will run out eventually

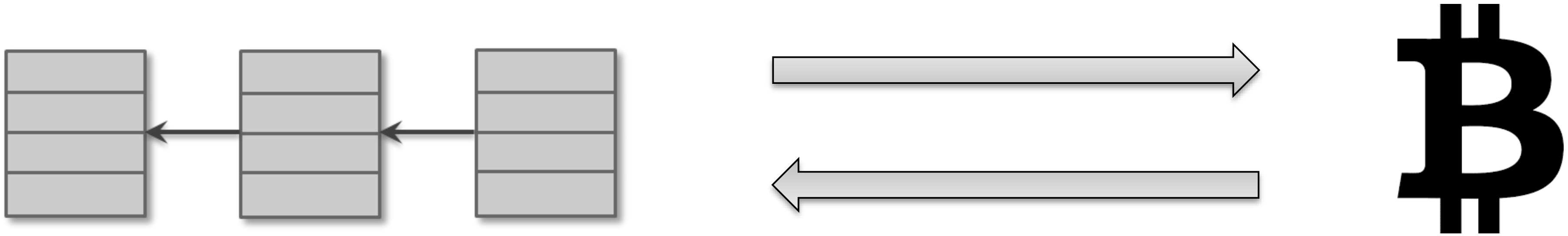
Summary of technical system

- **Overall system**: Record transfers of value between addresses in a global ledger (blockchain)

- **Users**: exchange addresses, issue signed statements to Bitcoin network authorizing transfers of value

- **Miners**: assemble user transactions into blocks, use computing power to get them into ledger, gain reward

The blockchain needs a currency



The blockchain enables the currency to function
by recording transactions

The currency motivates miners to secure the blockchain

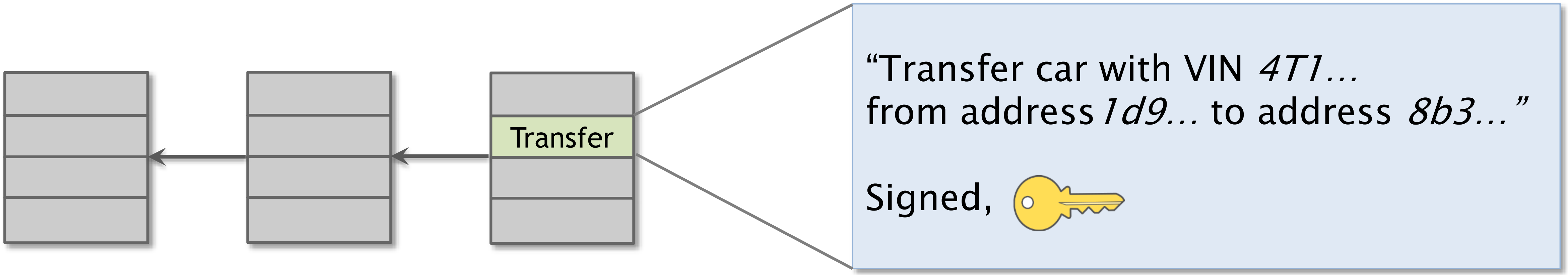
What else can we put on the blockchain?

- Stocks, derivatives, securities
- Supply chain tracking
- Personal identity
- Property titles
- …

Globally shared, immutable database of transactions

Sell your car? Register it on the blockchain

Each car is associated with a blockchain address

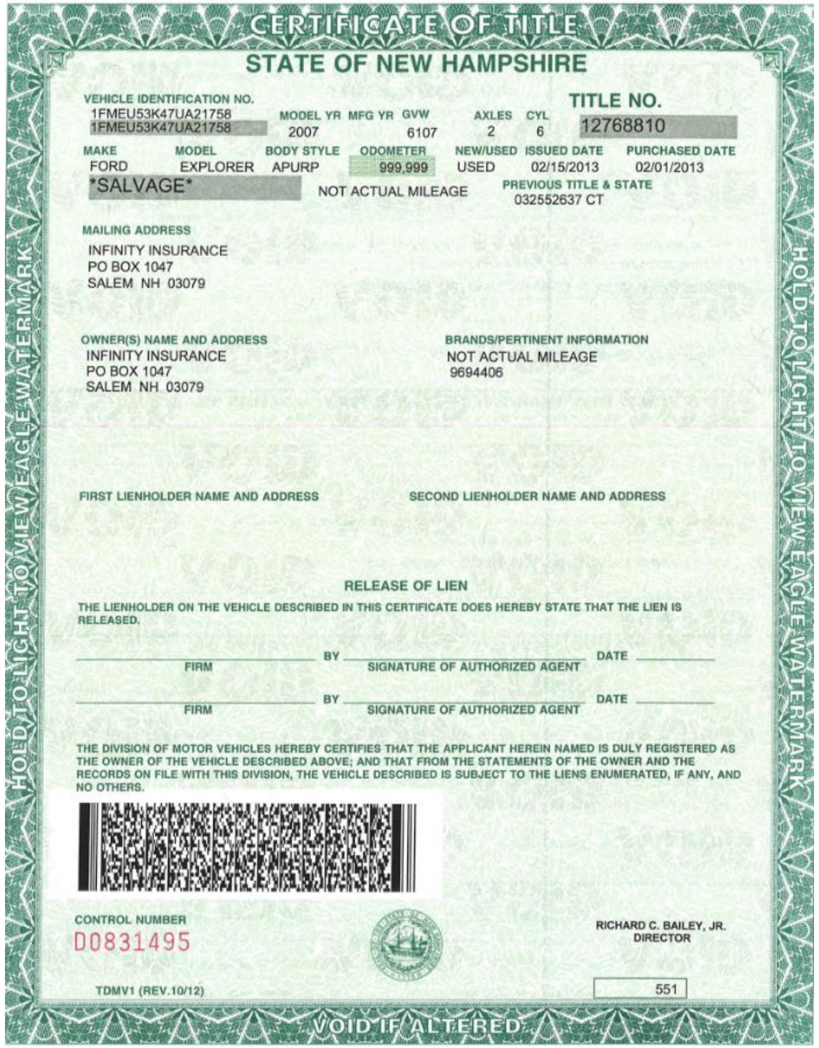


"Transfer car with VIN *4T1…*
from address *1d9…* to address *8b3…*"

Signed, 🔑

Validity of transfers can be cryptographically verified!

Decentralized property ownership



CERTIFICATE OF TITLE

STATE OF NEW HAMPSHIRE

VEHICLE IDENTIFICATION NO.	MODEL YR	MFG YR	GVW	AXLES	CYL	TITLE NO.
1FMEU53K47UA21758 1FMEU53K47UA21758	2007		6107	2	6	12768810

MAKE	MODEL	BODY STYLE	ODOMETER	NEW/USED	ISSUED DATE	PURCHASED DATE
FORD	EXPLORER	APURP	999,999	USED	02/15/2013	02/01/2013

SALVAGE

NOT ACTUAL MILEAGE

PREVIOUS TITLE & STATE
032552637 CT

MAILING ADDRESS
INFINITY INSURANCE
PO BOX 1047
SALEM NH 03079

OWNER(S) NAME AND ADDRESS
INFINITY INSURANCE
PO BOX 1047
SALEM NH 03079

BRANDS/PERTINENT INFORMATION
NOT ACTUAL MILEAGE
9694406

FIRST LIENHOLDER NAME AND ADDRESS

SECOND LIENHOLDER NAME AND ADDRESS

RELEASE OF LIEN

THE LIENHOLDER ON THE VEHICLE DESCRIBED IN THIS CERTIFICATE DOES HEREBY STATE THAT THE LIEN IS RELEASED.

_______________ BY _______________ DATE ________
FIRM SIGNATURE OF AUTHORIZED AGENT

_______________ BY _______________ DATE ________
FIRM SIGNATURE OF AUTHORIZED AGENT

THE DIVISION OF MOTOR VEHICLES HEREBY CERTIFIES THAT THE APPLICANT HEREIN NAMED IS DULY REGISTERED AS THE OWNER OF THE VEHICLE DESCRIBED ABOVE; AND THAT FROM THE STATEMENTS OF THE OWNER AND THE RECORDS ON FILE WITH THIS DIVISION, THE VEHICLE DESCRIBED IS SUBJECT TO THE LIENS ENUMERATED, IF ANY, AND NO OTHERS.

CONTROL NUMBER
D0831495

RICHARD C. BAILEY, JR.
DIRECTOR

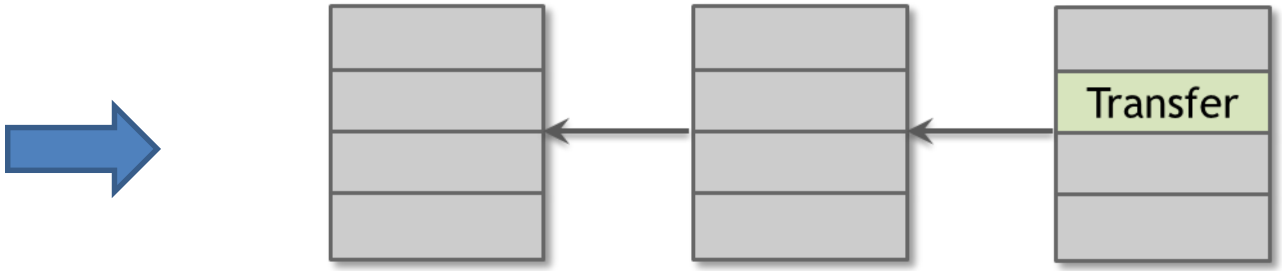
TDMV1 (REV.10/12)

551

HOLD TO LIGHT TO VIEW EAGLE WATERMARK

HOLD TO LIGHT TO VIEW EAGLE WATERMARK

VOID IF ALTERED



Limitations of blockchains

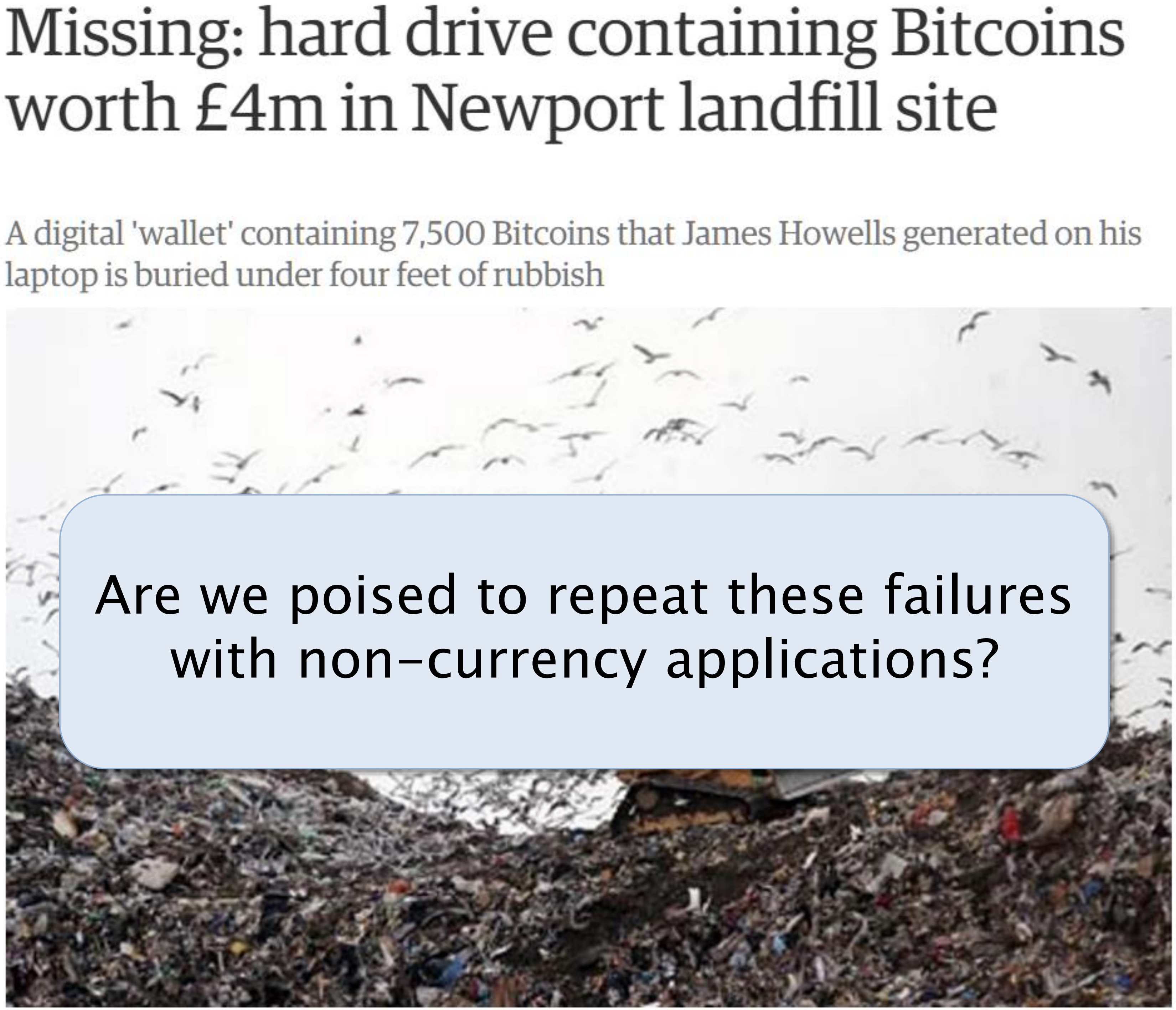
What are the problems with car ownership and trade?

- Security (theft)
- Disputes about sale terms

How does the blockchain address these problems?

(It doesn’t)

It introduces new problems: what if you lose your key?



Missing: hard drive containing Bitcoins worth £4m in Newport landfill site

A digital 'wallet' containing 7,500 Bitcoins that James Howells generated on his laptop is buried under four feet of rubbish

Are we poised to repeat these failures with non-currency applications?

Take-home messages

- Public blockchain technology is novel and sound

- Yet it has sharp edges:
  e.g., tricky to handle crypto keys!

- Can’t solve social problems using technology
  Integrate into existing institutions: long, hard work