AI, Crypto, Blockchain and Cybersecurity
A Whirlwind Introduction!

Jake van der Laan
Director Information Technology and Regulatory Informatics,
Chief Information Officer
Financial and Consumer Services Commission
New Brunswick, Canada
jake.vanderlaan@fcnb.ca

Any opinions expressed are my own and do not necessarily reflect the position or perspective of FCNB.

I do not endorse, or otherwise make any claim or statement, negative or positive, about any of the websites, companies, or products, if any, referenced in these slides or during this presentation.

Itinerary

1. Artificial intelligence 101
2. The quest for digital currency (including a blockchain explanation)
3. Cybersecurity essentials

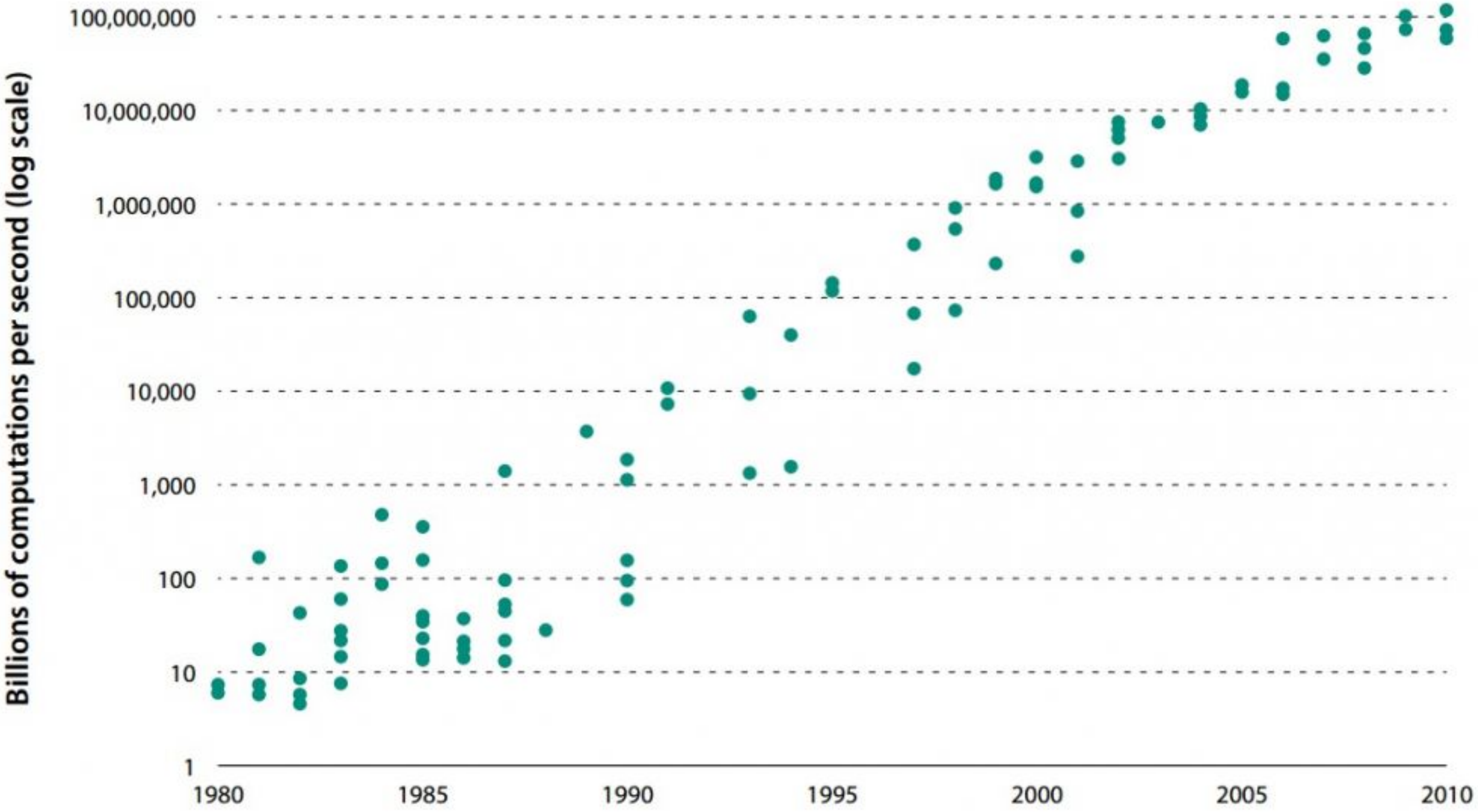
Part 1:
Artificial Intelligence 101

What is AI?

A computer based system which can do things which we traditionally attribute to the exercise of human intelligence:

planning, learning, reasoning, problem solving, knowledge representation, (spatial) perception, pruposive motion and physical manipulation, language communication, social intelligence and creativity.

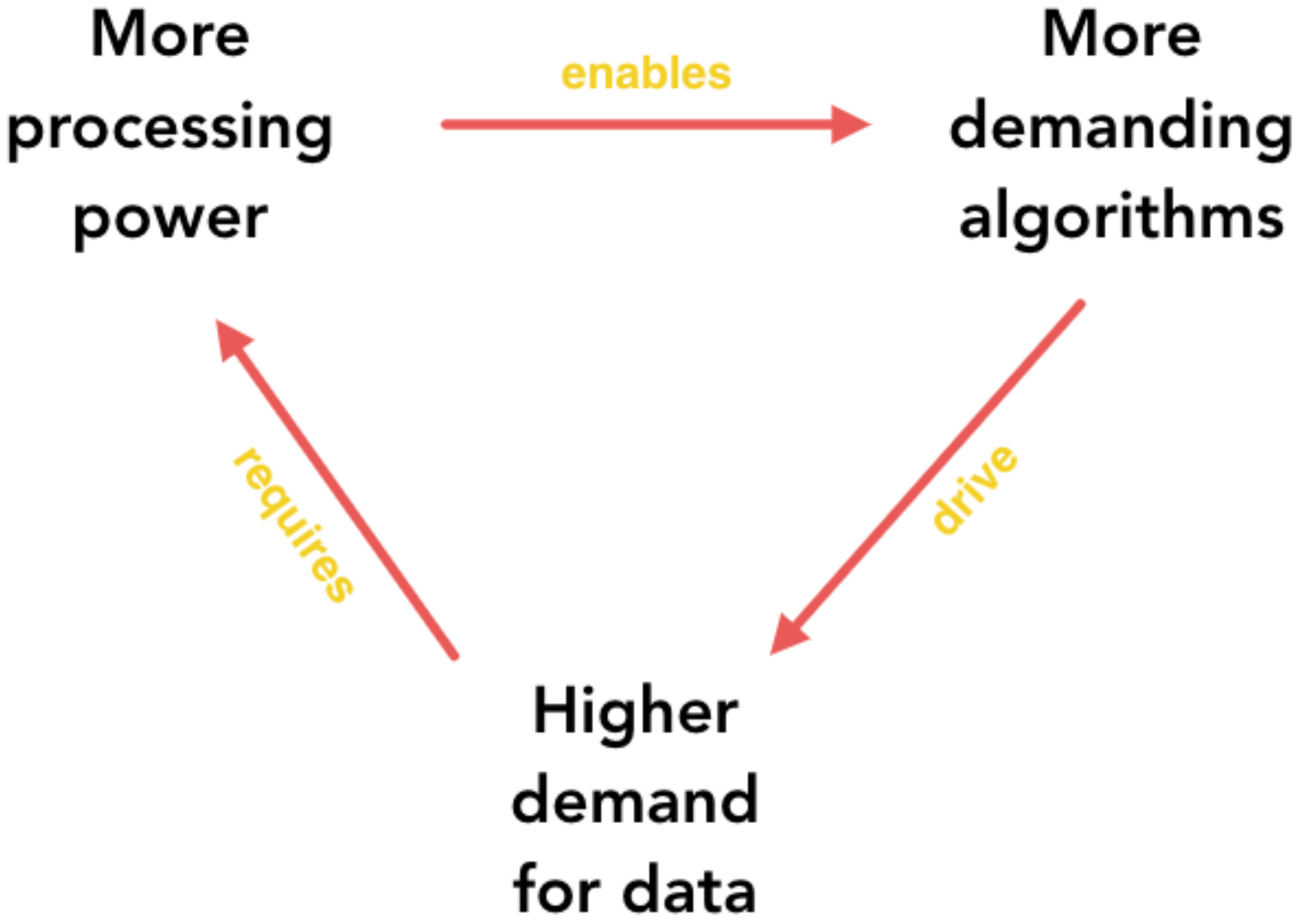
One Dollar's Worth of Computer Power, 1980–2010



Source: Nordhaus (2007); updated data through 2010 from Nordhaus, personal website, http://www.econ.yale.edu/~nordhaus/homepage/, "Two Centuries of Productivity Growth in Computing."; authors' calculations.

Note: Nordhaus (2007) defines computer power as the rate at which computers and calculators can execute certain standard mathematical tasks, measured in computations per second. The data have been adjusted for purchasing power to year 2006 dollars.

THE HAMILTON PROJECT
BROOKINGS



More processing power

enables

More demanding algorithms

drive

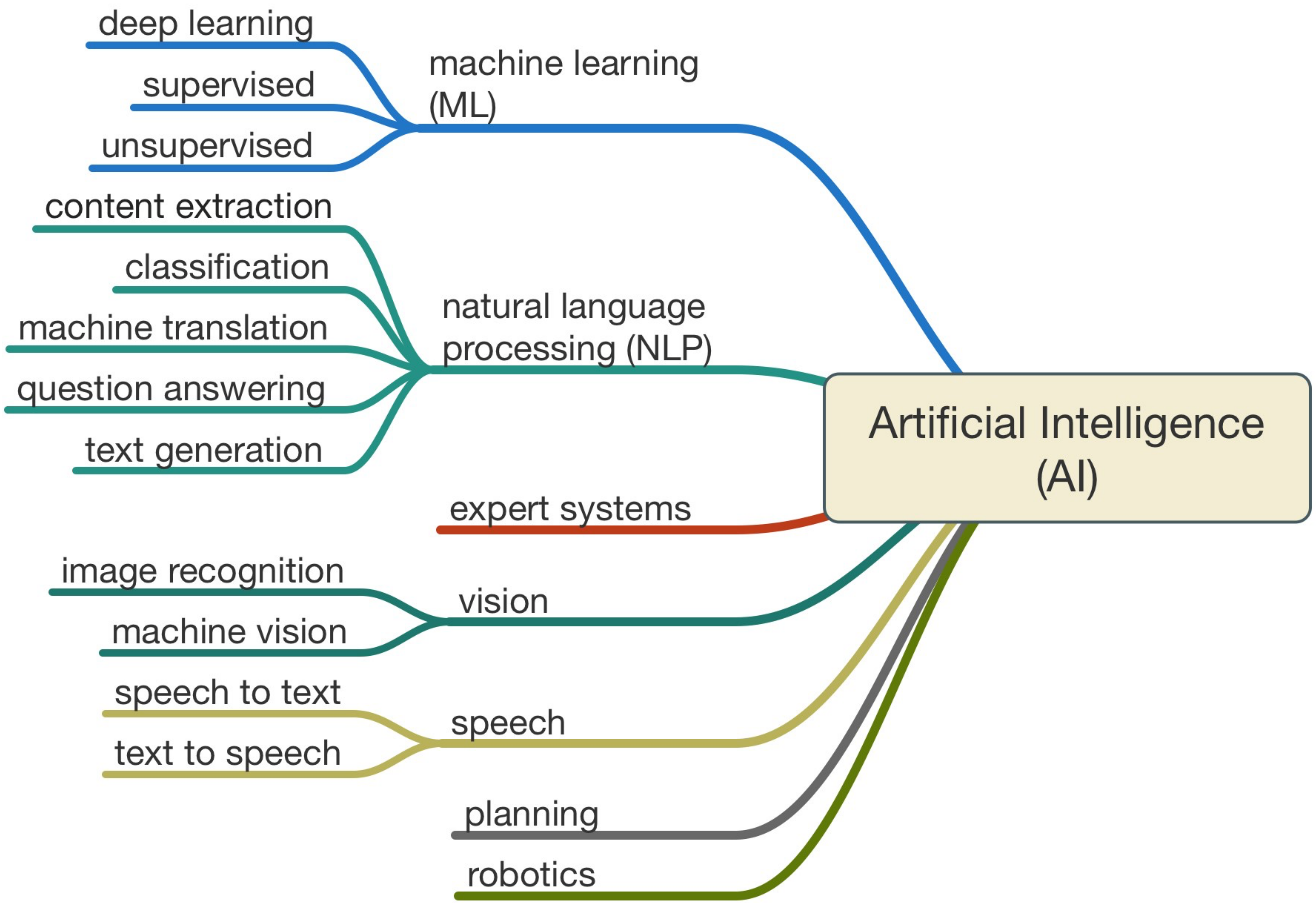
Higher demand for data

requires

Types of AI

- Narrow AI: one task (e.g. voice recognition, self driving cars)
- General AI: independent learning from any experience (e.g. Skynet)

Narrow AI implementations



“Consumer” AI

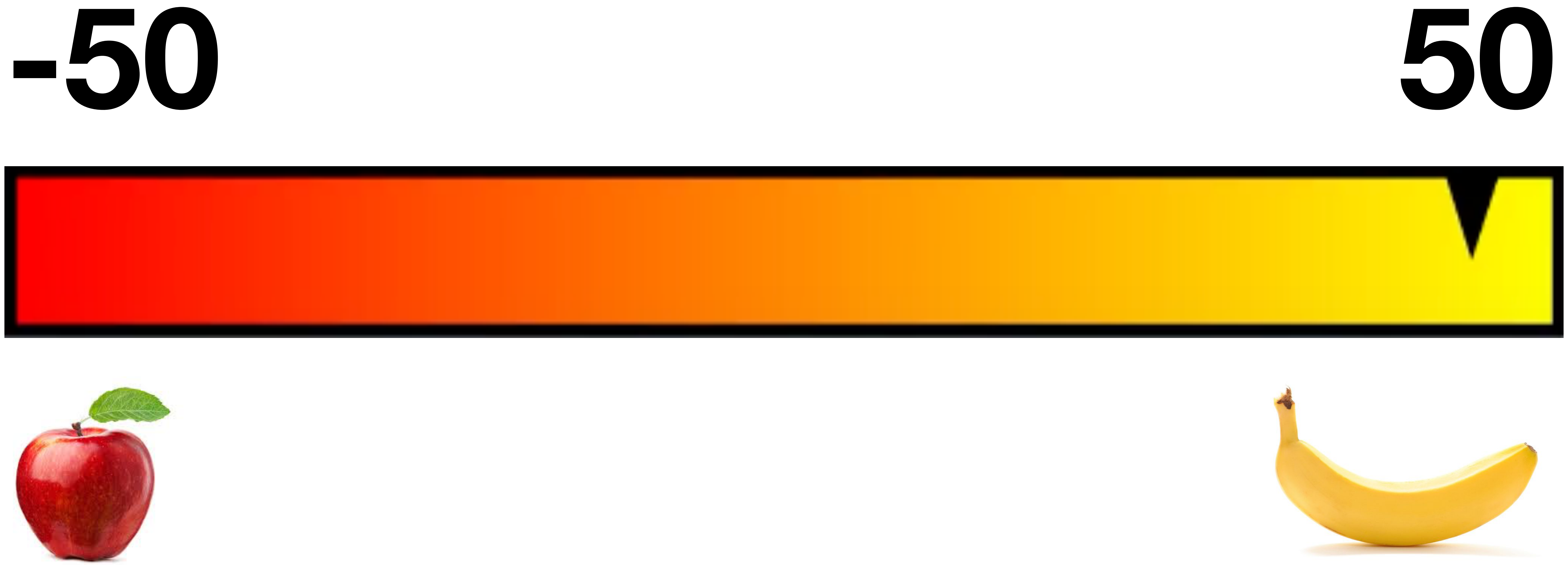
- Siri
- Automated driving
- Automated wealth management
- OCR
- Advertising

An example:
machine learning / deep learning

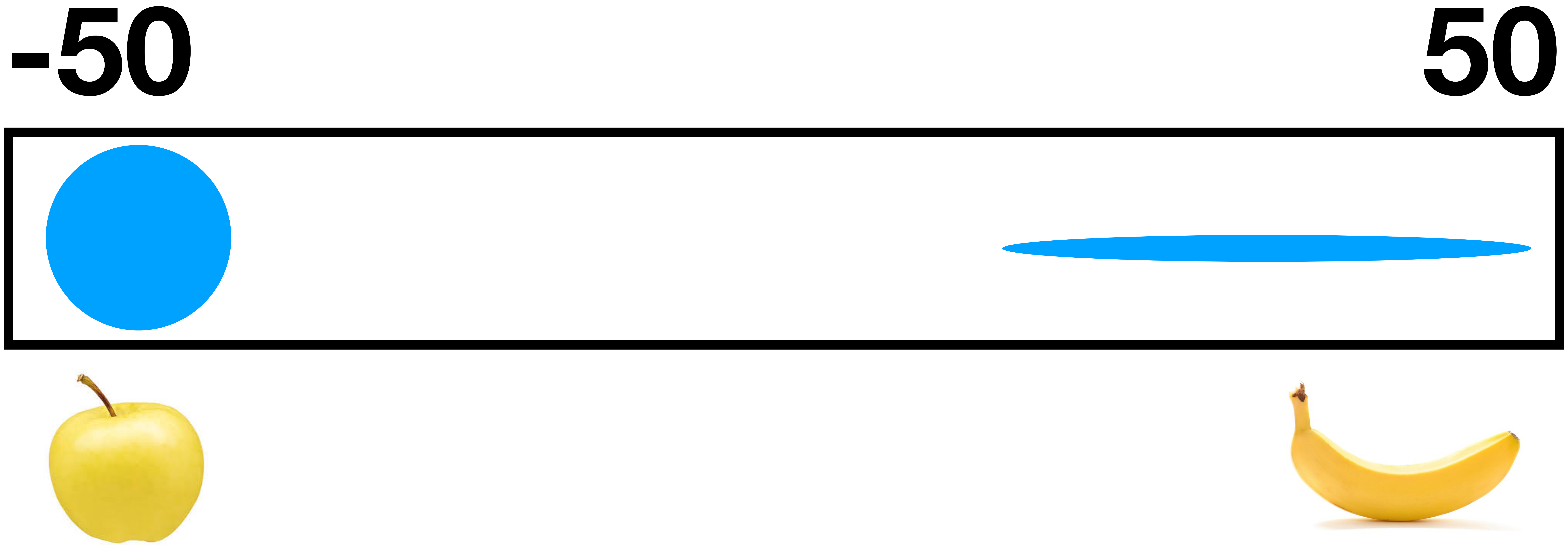
- Machine learning algorithms use computational methods to “learn” information directly from data **without relying on a predetermined equation**.
- Think “learning from experience” or “developing intuition”

- 3 turns into 9
- 4 turns into 16
- 5 turns into 25
- 6 turns into ?

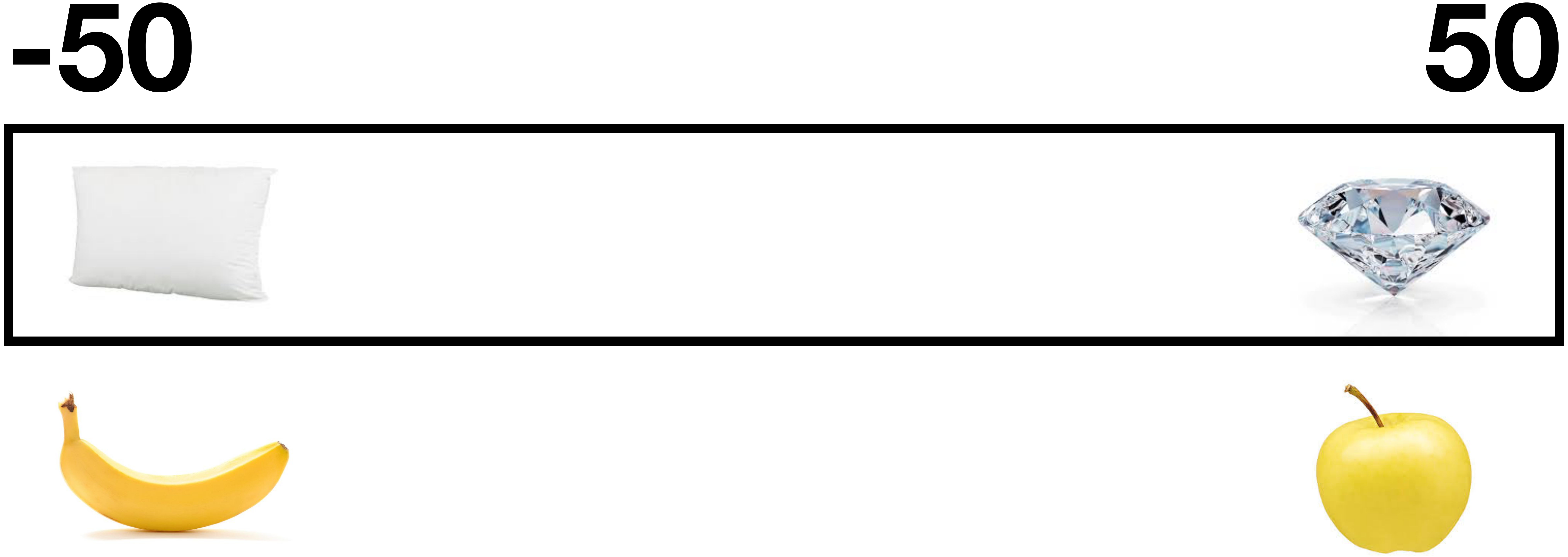
Colour



"Globe-ness”



Hardness



Label many of them

Make a training data table

Item	Colour	Globeness	Hardness	Type of fruit
1	-45	-20	44	Apple
2	-23	-33	41	Apple
3	2	36	-33	Banana
4	14	33	-31	Banana

Training

- Pick a learning algorithm suitable for the type of question you want to answer

- The algorithm goes through the table and tries to **find the weight to give to each feature** in order to correctly identify all the fruit in the table

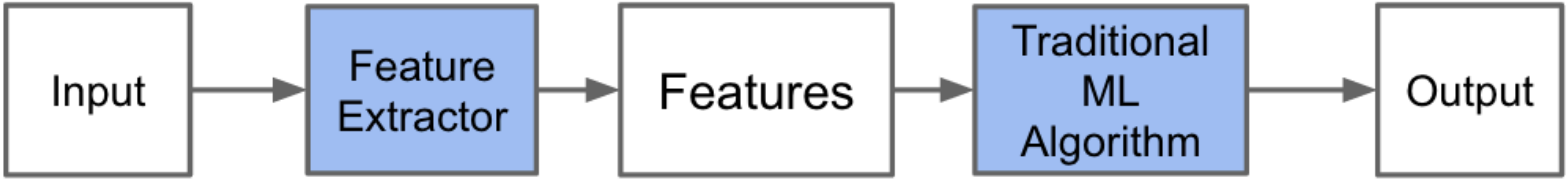
Prediction

- Show a new fruit to the “machine”

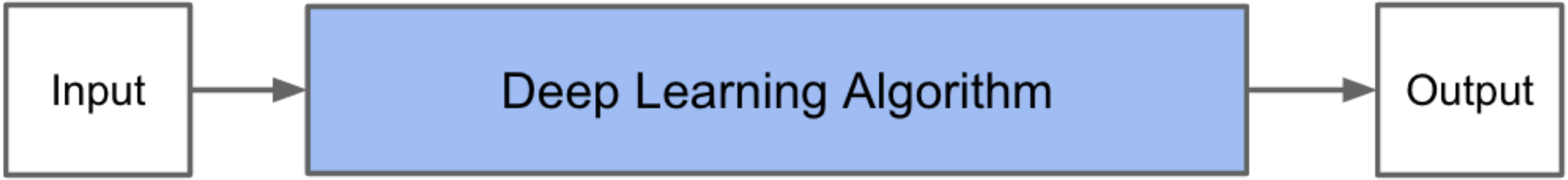
- The machine measures its features and calculates the weights based on the model

- Makes a prediction

Deep learning



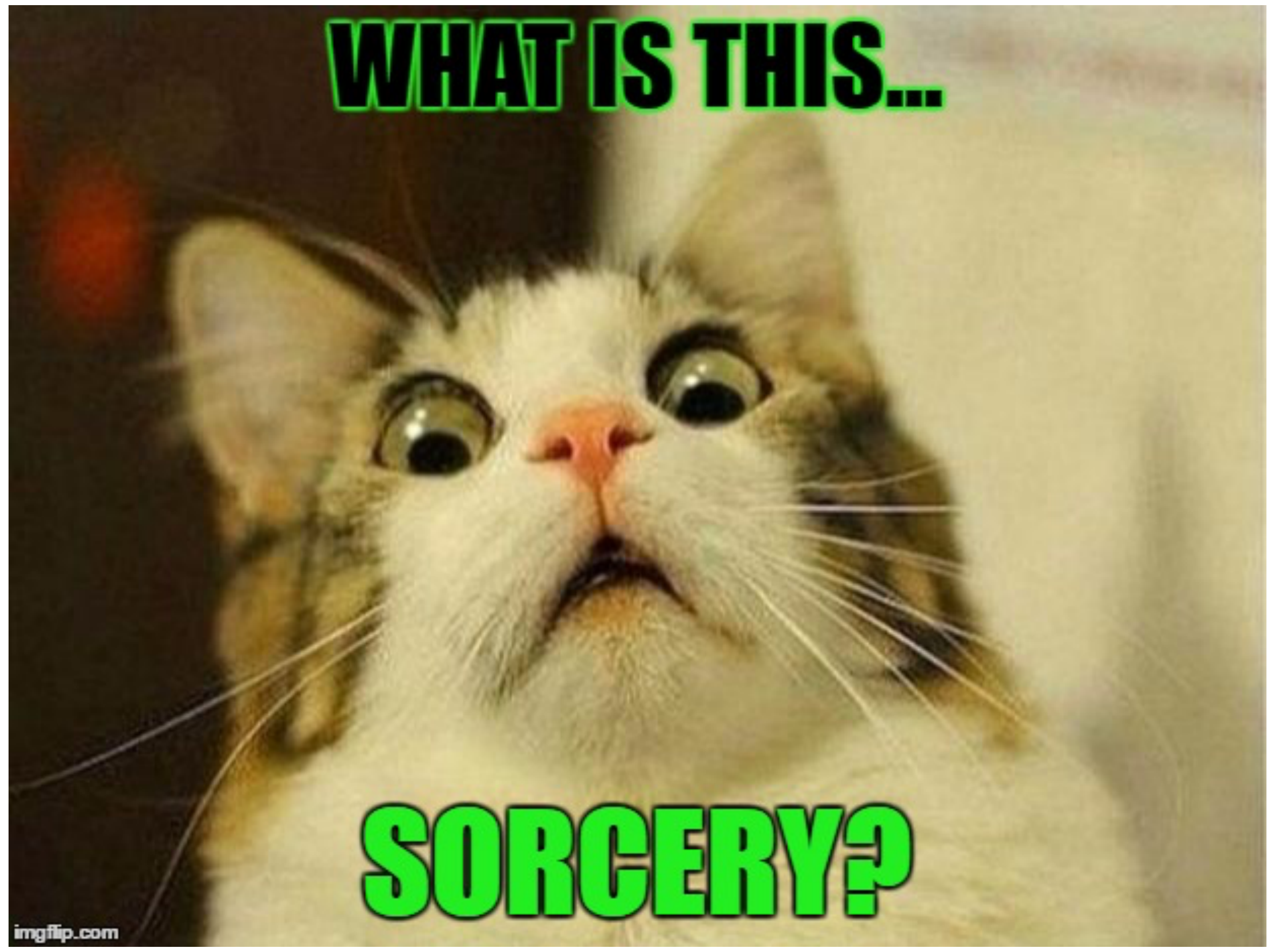
Traditional Machine Learning Flow



Deep Learning Flow

Types of deep learning

- **Supervised**: the cats and dogs are labeled before learning
- **Unsupervised**: the cats and dogs are **NOT** labeled before learning

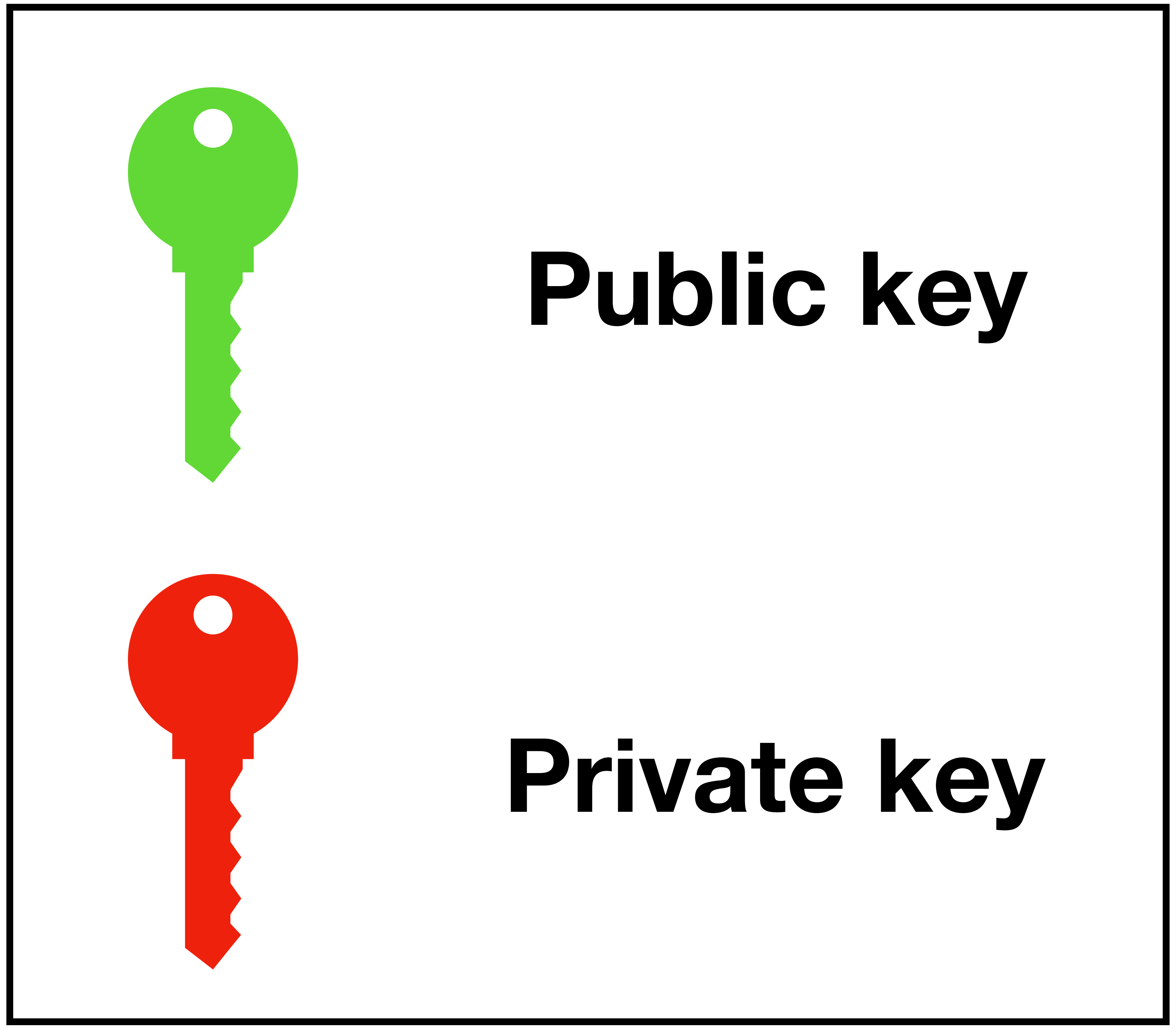


Deep learning applications

- Price and cost forecasting / optimization
- Fraud detection
- Insurance risk analysis / lifetime prediction / claims prediction and processing
- Personalized and automated marketing in all consumer areas
- Voice recognition and command / Augmented reality / Autonomous agents (cars for example)

Part 2:
The quest for digital currency

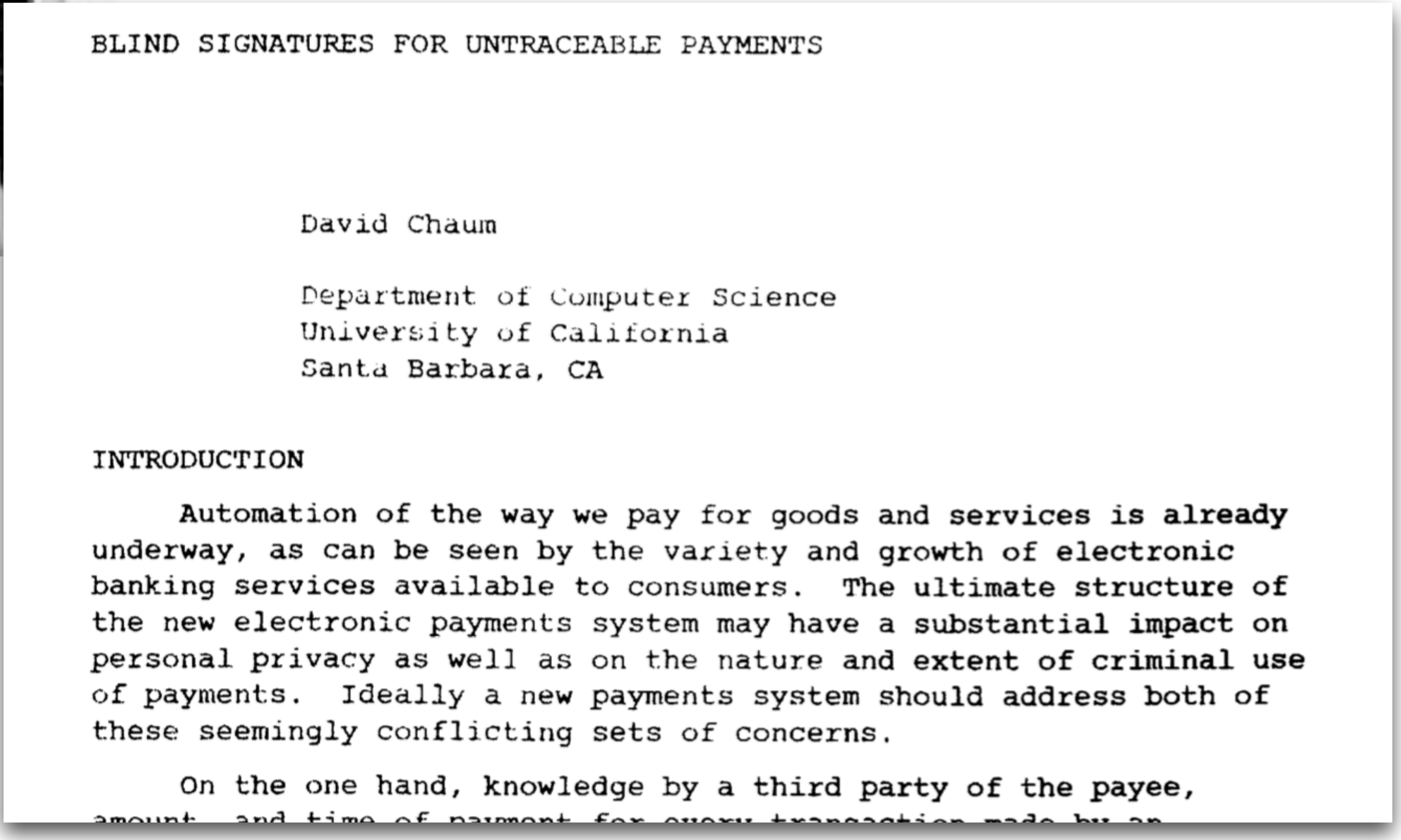
1969



Public key

Private key

1983



BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

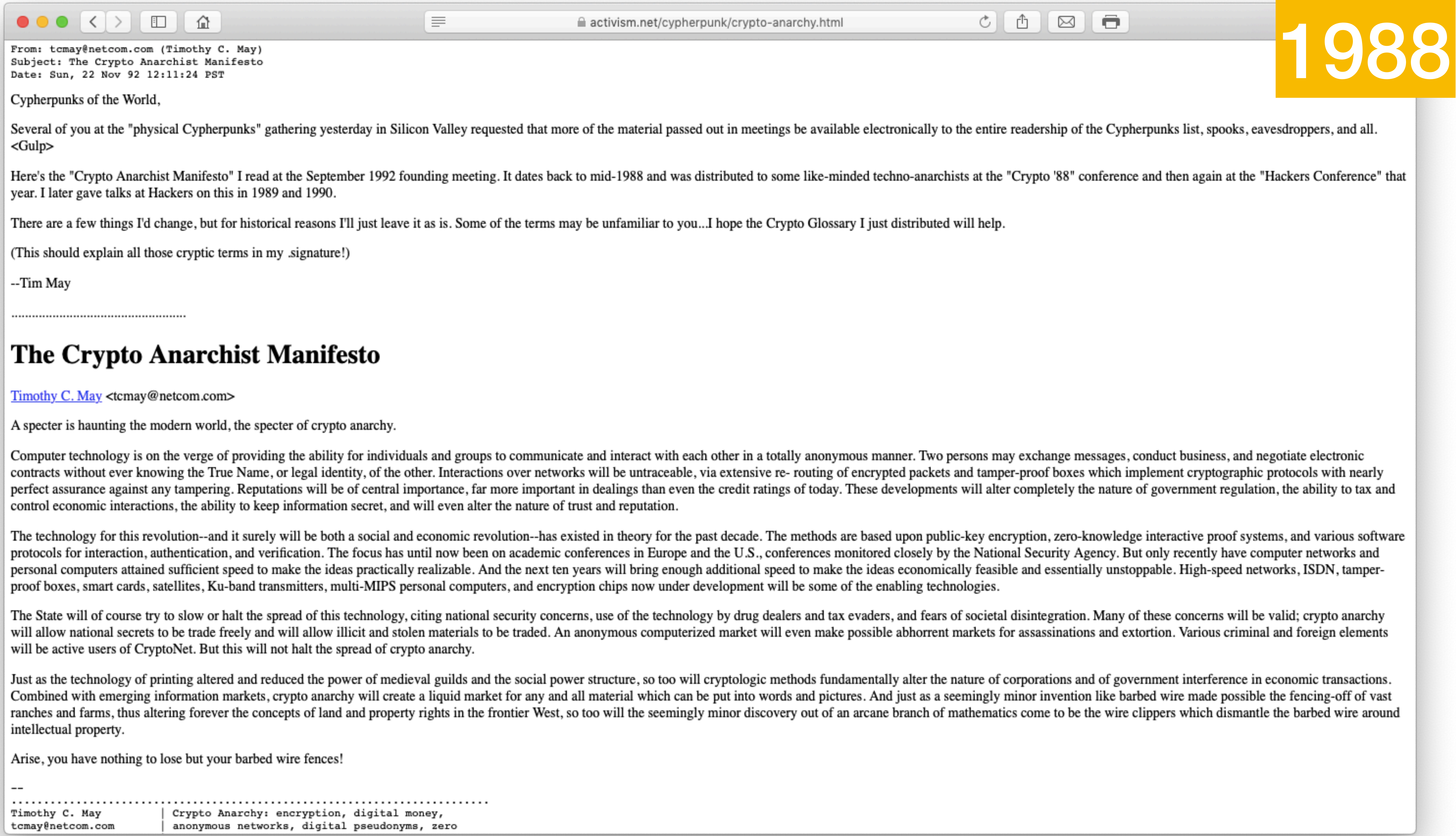
Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.

On the one hand, knowledge by a third party of the payee, amount, and time of payment for every transaction made by an

1988



From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST

Cypherpunks of the World,

Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May

....

The Crypto Anarchist Manifesto

Timothy C. May <tcmay@netcom.com>

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

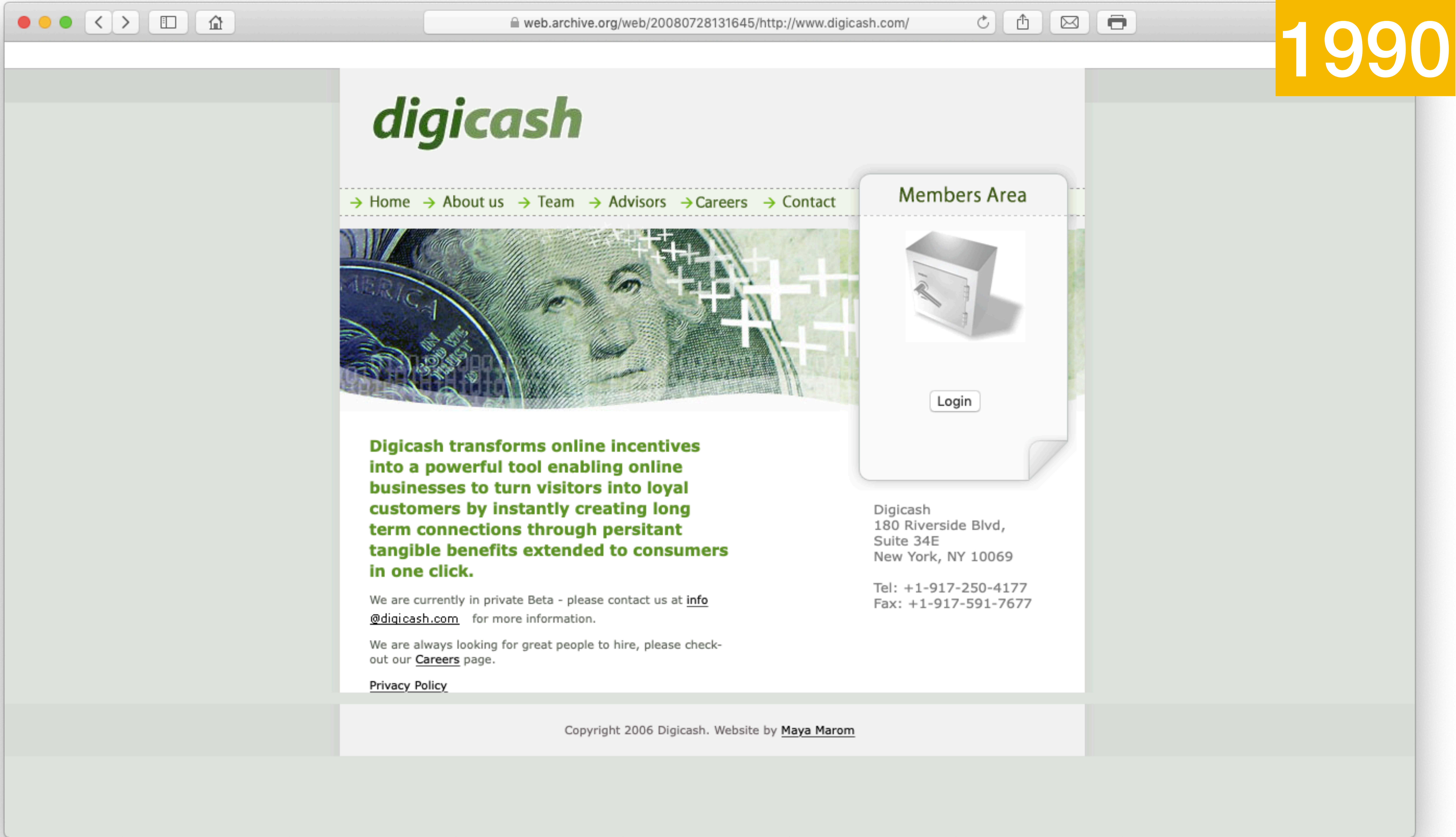
The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

```
--
..........................................................................
Timothy C. May         | Crypto Anarchy: encryption, digital money,
tcmay@netcom.com       | anonymous networks, digital pseudonyms, zero
```

1990



Digicash transforms online incentives into a powerful tool enabling online businesses to turn visitors into loyal customers by instantly creating long term connections through persitant tangible benefits extended to consumers in one click.

We are currently in private Beta - please contact us at info @digicash.com for more information.

We are always looking for great people to hire, please check-out our Careers page.

Privacy Policy

Digicash
180 Riverside Blvd,
Suite 34E
New York, NY 10069

Tel: +1-917-250-4177
Fax: +1-917-591-7677

Copyright 2006 Digicash. Website by Maya Marom

1998

web.archive.org/web/20020813012900/http://www.paypal.com/
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Shop
Sell
LOG IN
SIGN UP
Submit
Get $5 for signing up!
VISA
MasterCard
DISCOVER
reviewed by TRUSTe site privacy statement
PRIVACY BBBOnLine
SOLD

Welcome

▶ PayPal members

▶ New user?

Pay for an Auction

eBay Item Number

Seller's Email

The way to send and receive money online

Send Money
Pay anyone with an email address

Request Money
Send a personal or group bill

Over 17 million members worldwide!

Sign up for your FREE PayPal Account!

Spotlight

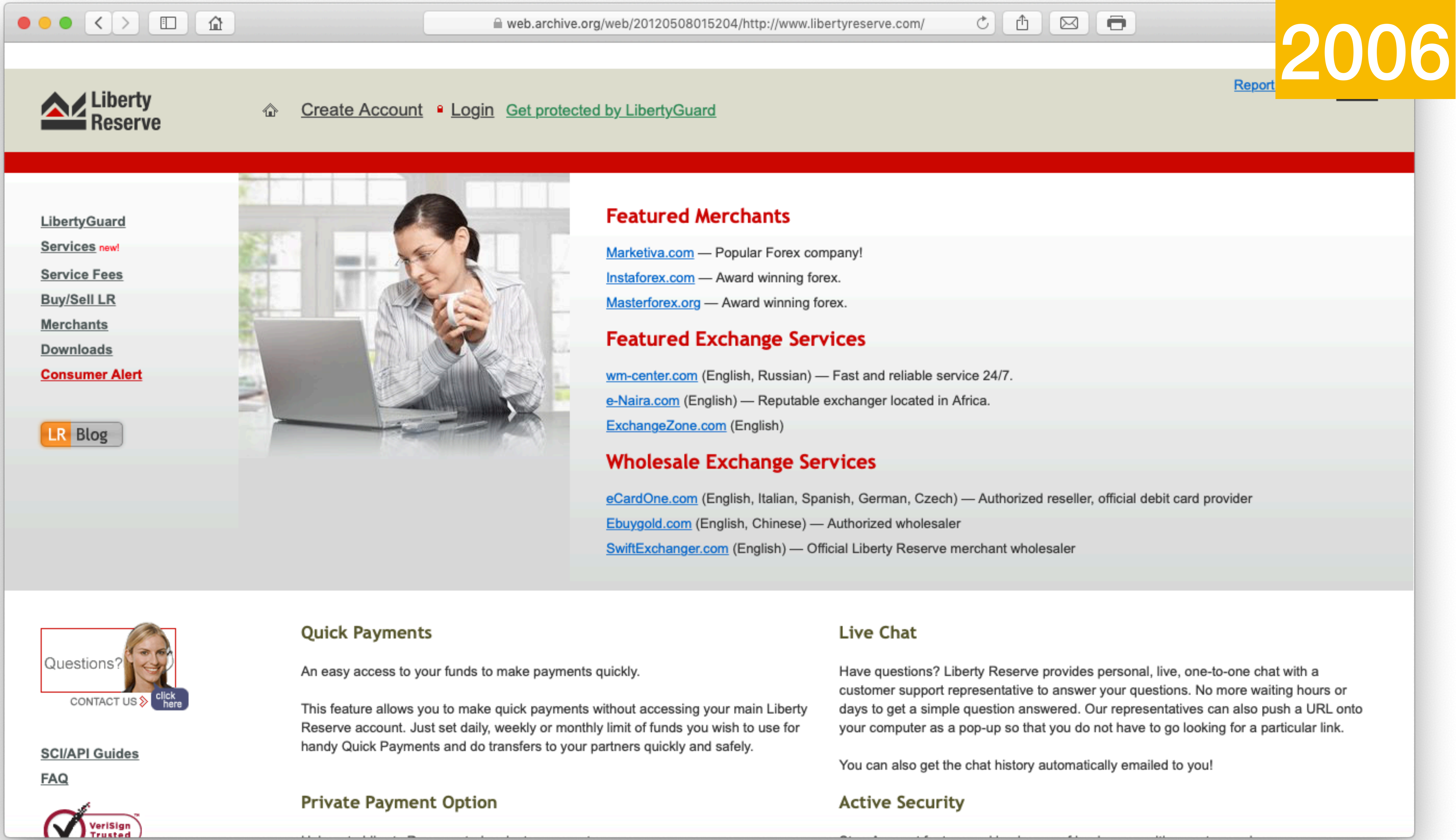
Businesses
PayPal is the easiest and cheapest way for small businesses and websites to accept payments online. Sign up now!

Auctions
#1 payment service on eBay.
Trusted on over 5 million auctions.

About Us | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Help

Copyright © 2002 PayPal. All rights reserved.
Information about FDIC pass-through insurance

2006



web.archive.org/web/20120508015204/http://www.libertyreserve.com/

Liberty Reserve

Create Account · Login · Get protected by LibertyGuard

Report

LibertyGuard
Services new!
Service Fees
Buy/Sell LR
Merchants
Downloads
Consumer Alert

LR Blog

Featured Merchants

Marketiva.com — Popular Forex company!
Instaforex.com — Award winning forex.
Masterforex.org — Award winning forex.

Featured Exchange Services

wm-center.com (English, Russian) — Fast and reliable service 24/7.
e-Naira.com (English) — Reputable exchanger located in Africa.
ExchangeZone.com (English)

Wholesale Exchange Services

eCardOne.com (English, Italian, Spanish, German, Czech) — Authorized reseller, official debit card provider
Ebuygold.com (English, Chinese) — Authorized wholesaler
SwiftExchanger.com (English) — Official Liberty Reserve merchant wholesaler

Questions?
CONTACT US click here

SCI/API Guides
FAQ

VeriSign Trusted

Quick Payments

An easy access to your funds to make payments quickly.

This feature allows you to make quick payments without accessing your main Liberty Reserve account. Just set daily, weekly or monthly limit of funds you wish to use for handy Quick Payments and do transfers to your partners quickly and safely.

Private Payment Option

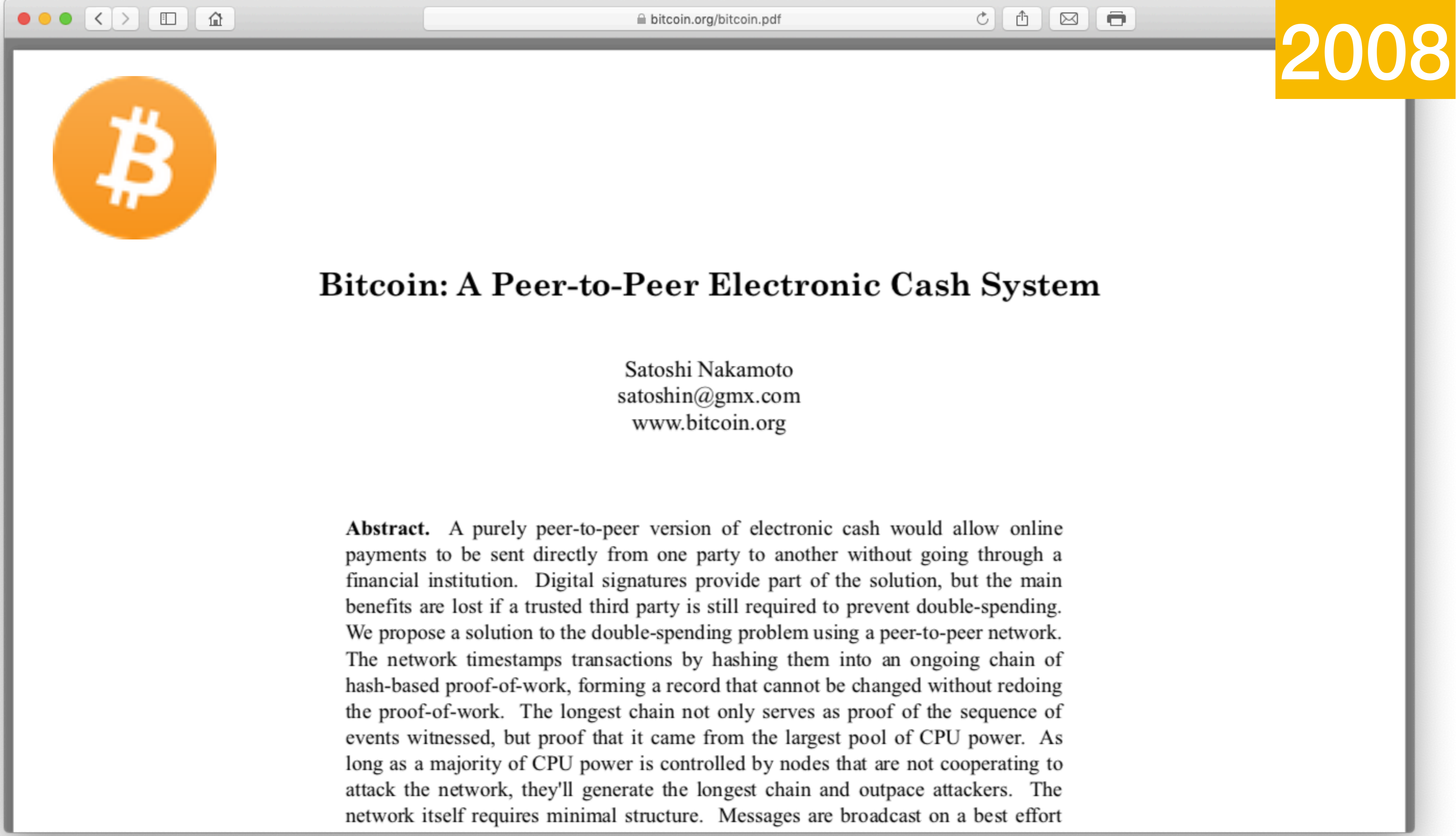
Live Chat

Have questions? Liberty Reserve provides personal, live, one-to-one chat with a customer support representative to answer your questions. No more waiting hours or days to get a simple question answered. Our representatives can also push a URL onto your computer as a pop-up so that you do not have to go looking for a particular link.

You can also get the chat history automatically emailed to you!

Active Security

2008



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

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general
Date: 2008-10-31 18:10:00 GMT

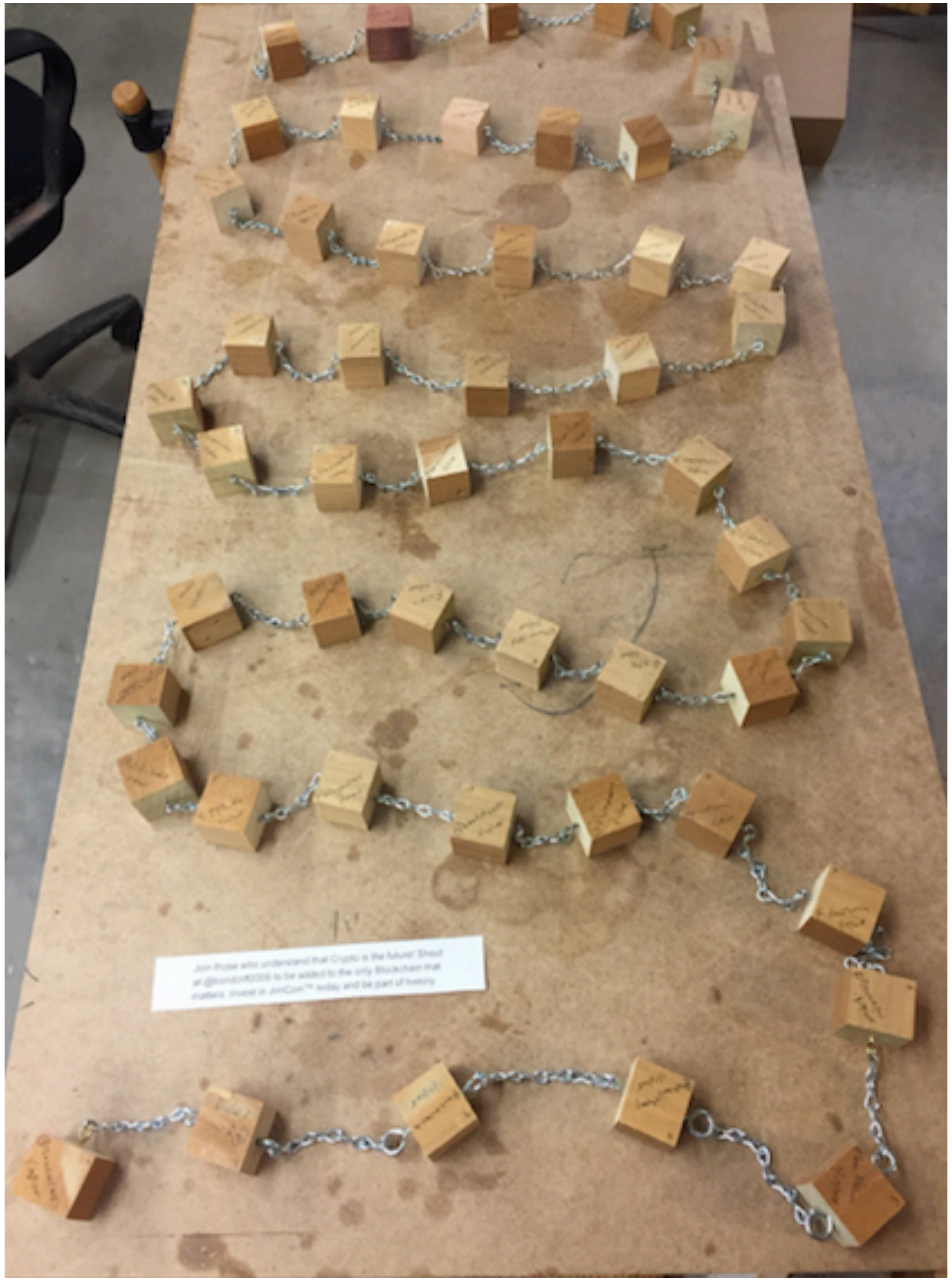
I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.
The paper is available at: http://www.bitcoin.org/bitcoin.pdf
The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the network to prevent double-spending.

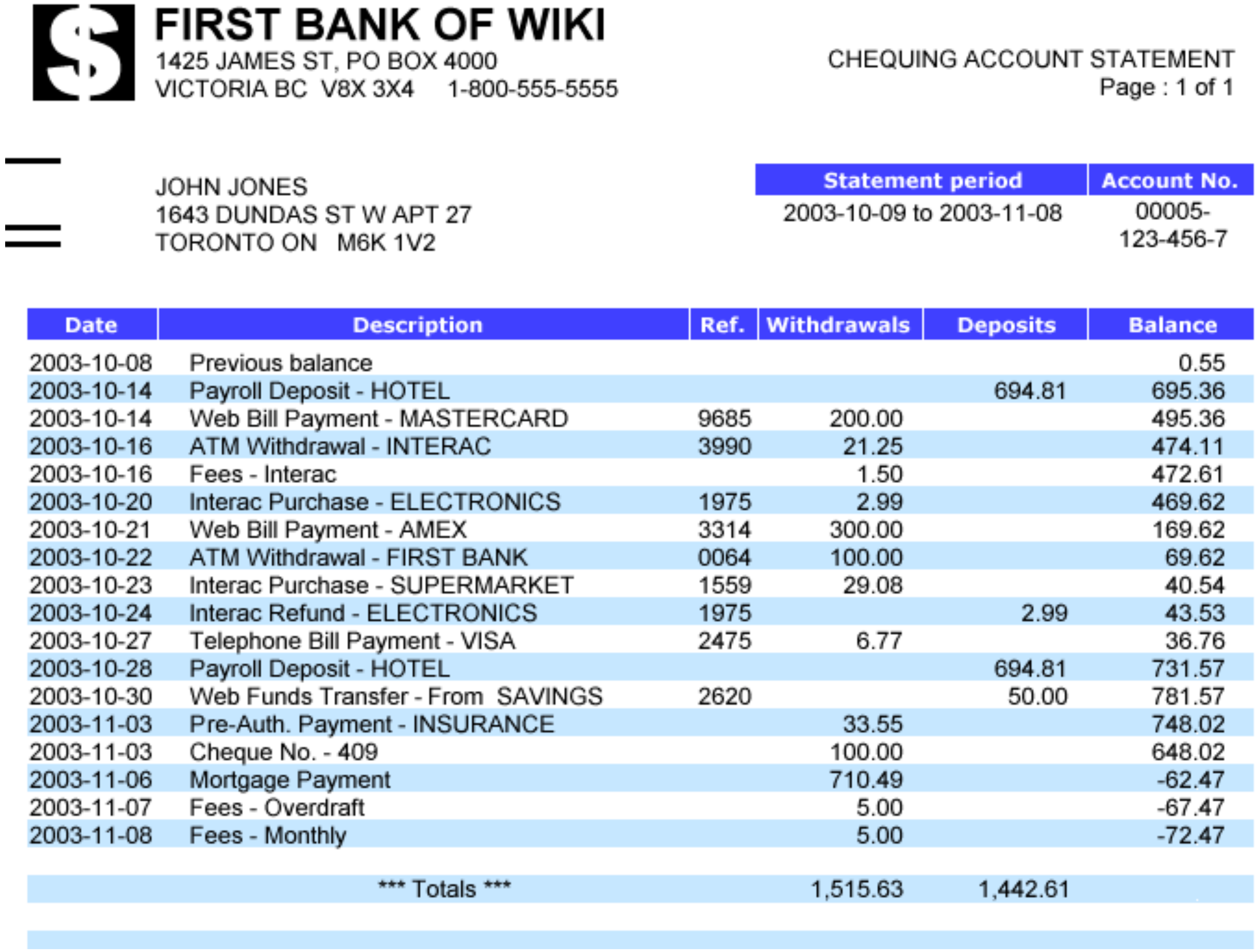
Bitcoin: A Peer-to-Peer Electronic Cash System
Abstract. A purely peer-to-peer version of electronic cash [...]

Satoshi Nakamoto

The Cryptography Mailing List

Blockchain


Join those who understand that Crypto is the future! Shout at @[illegible] to be added to the only Blockchain that matters. Invest in JimCoin™ today and be part of history.



FIRST BANK OF WIKI

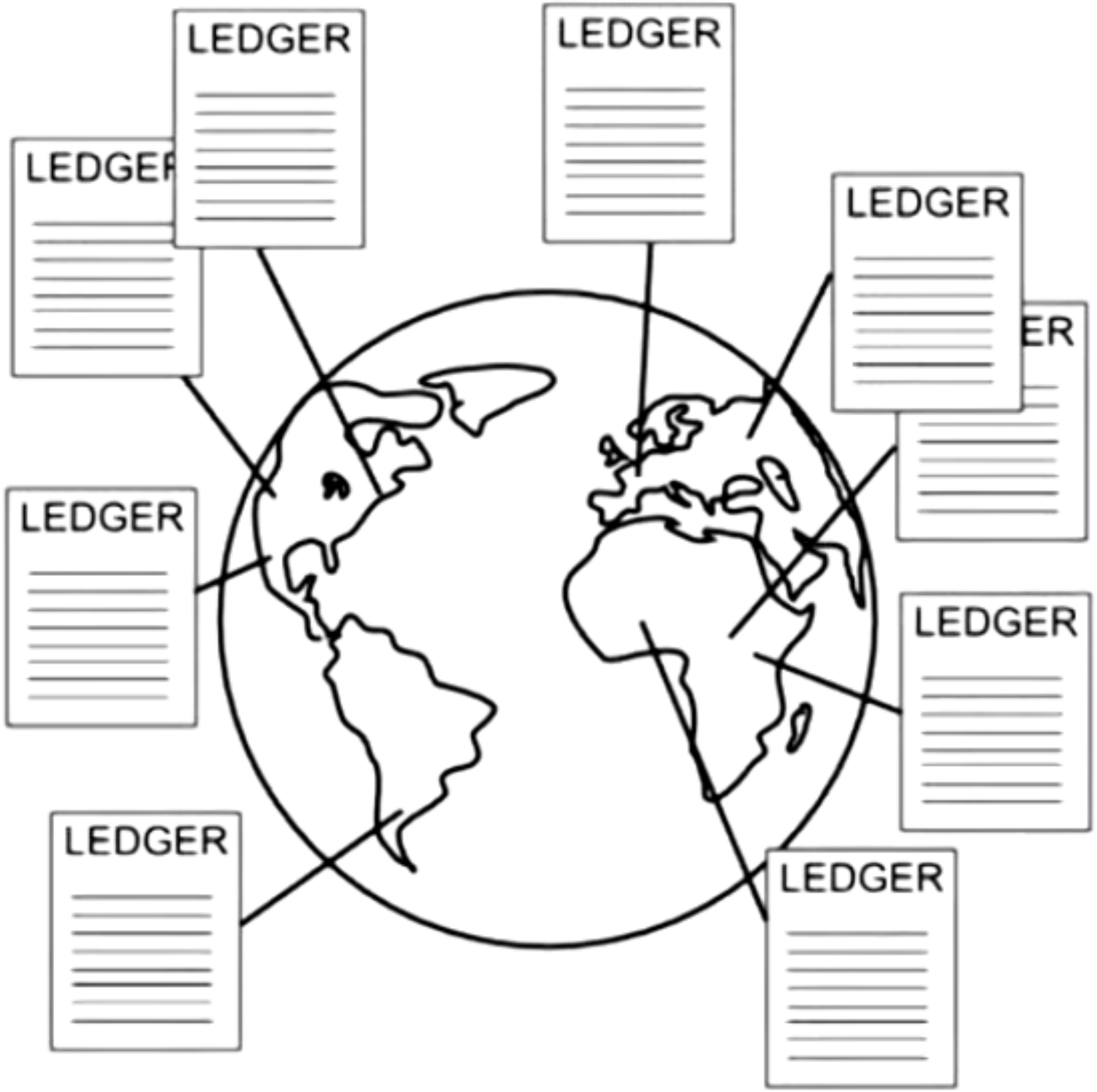
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4   1-800-555-5555

CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

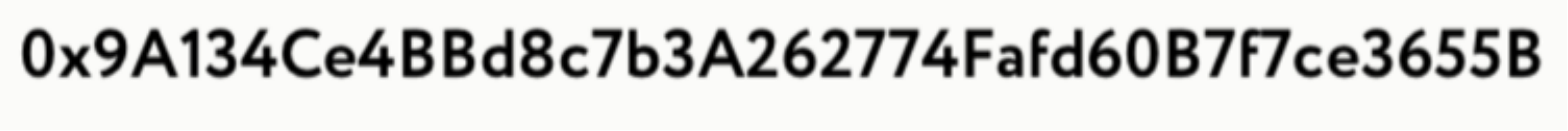
Statement period	Account No.
2003-10-09 to 2003-11-08	00005-123-456-7

Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47
	*** Totals ***		1,515.63	1,442.61	

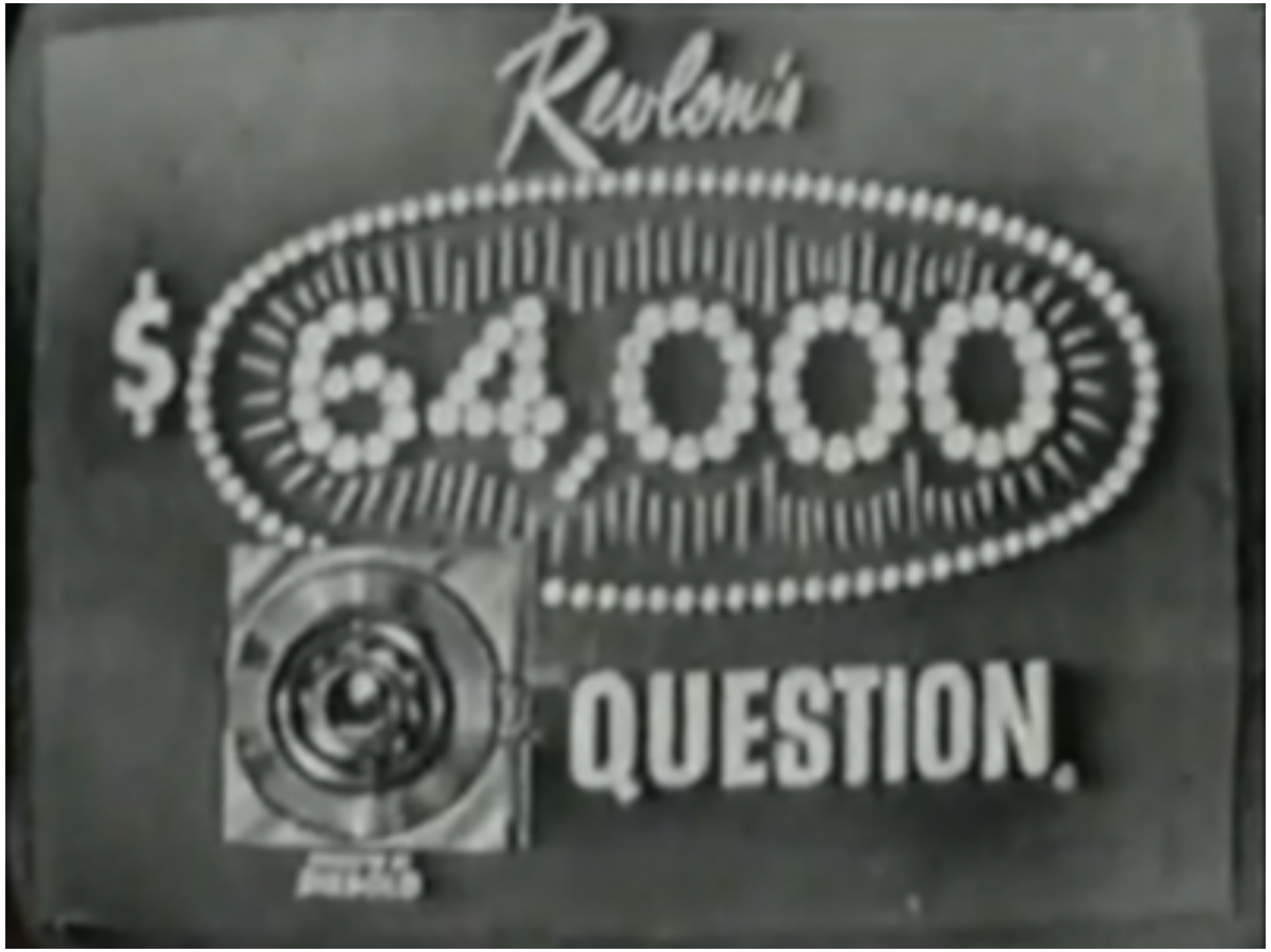

LEDGER
LEDGER
LEDGE
LEDGER
ER
LEDGER
LEDGER
LEDGER
LEDGER

Address keys, not names

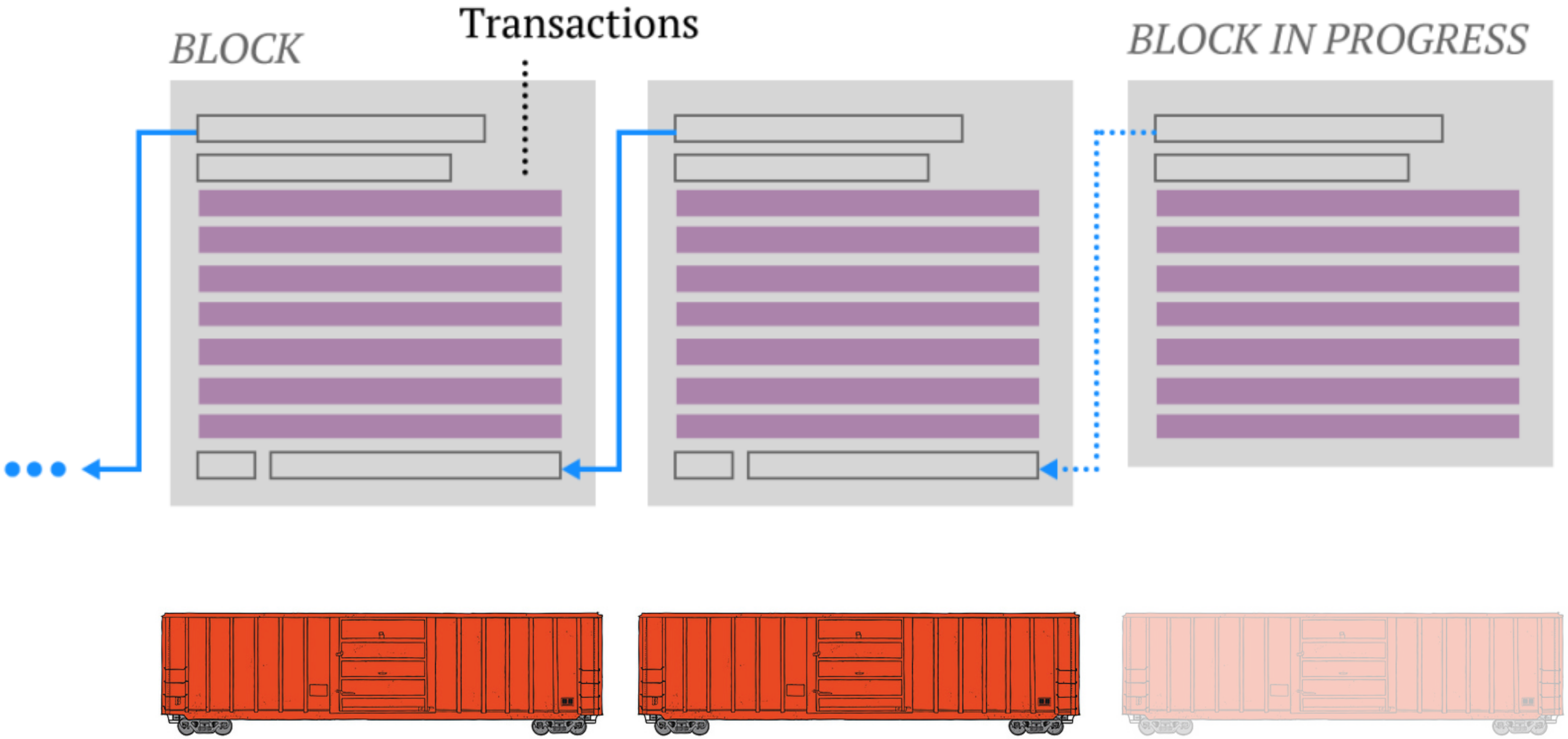
- Transactions are authorized by the owner’s **private** key (can be stored in a digital wallet)
- Ownership on the blockchain is tracked by the owner’s **public** key address



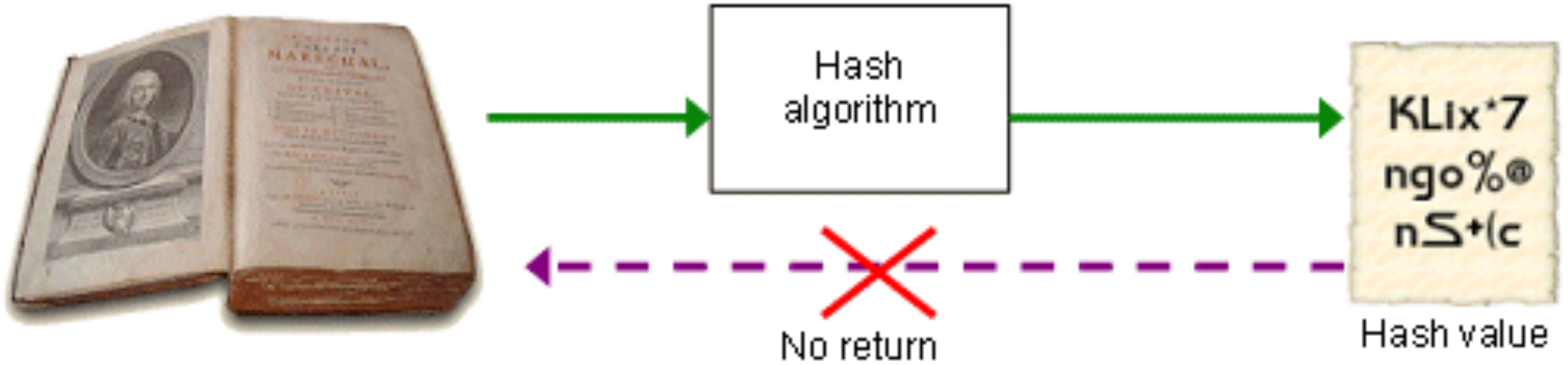
0x9A134Ce4BBd8c7b3A262774Fafd60B7f7ce3655B



How to update it?

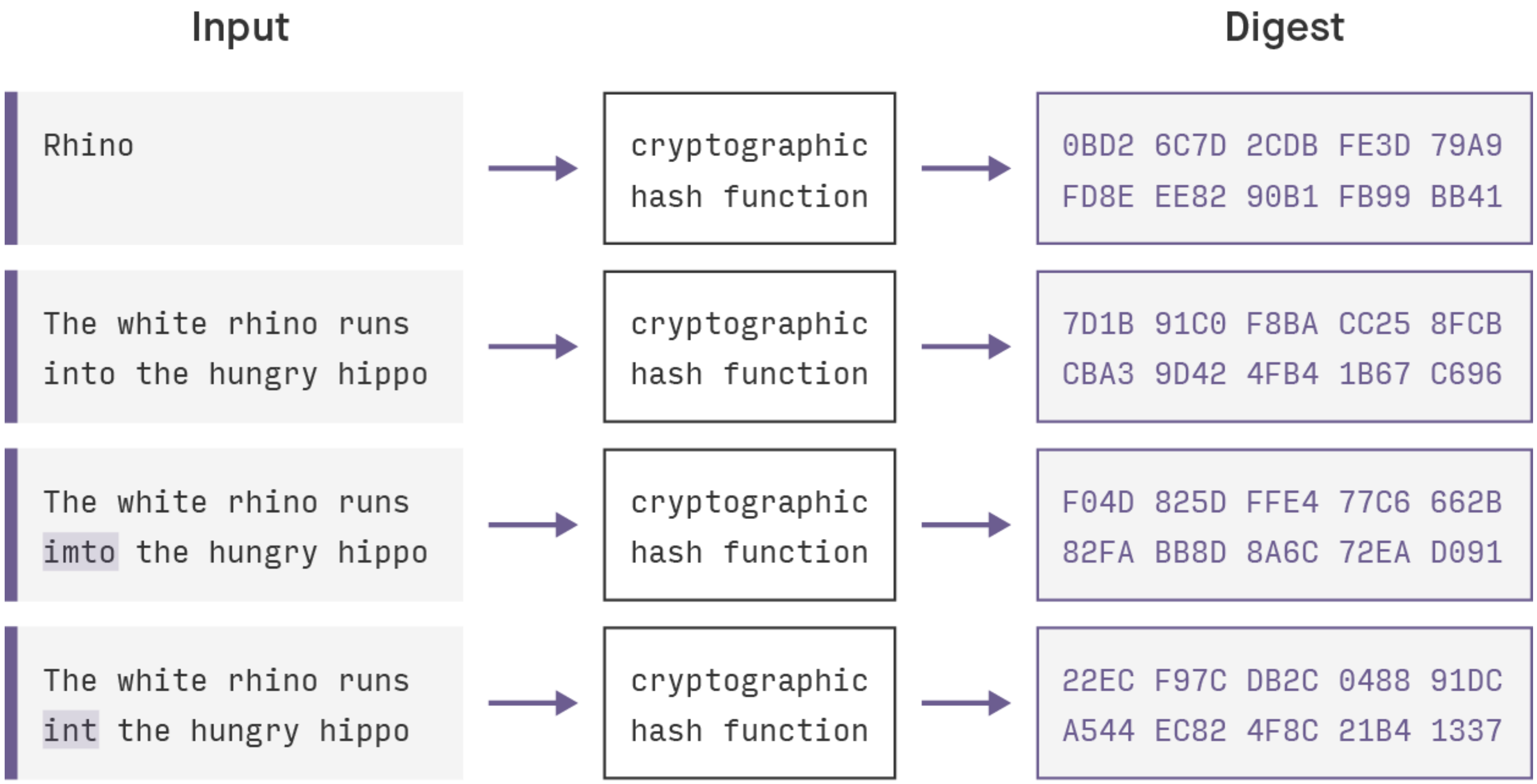

BLOCK
Transactions
BLOCK IN PROGRESS

Cryptographic hash function



Unique for structured data

Cannot be reverse engineered



Input

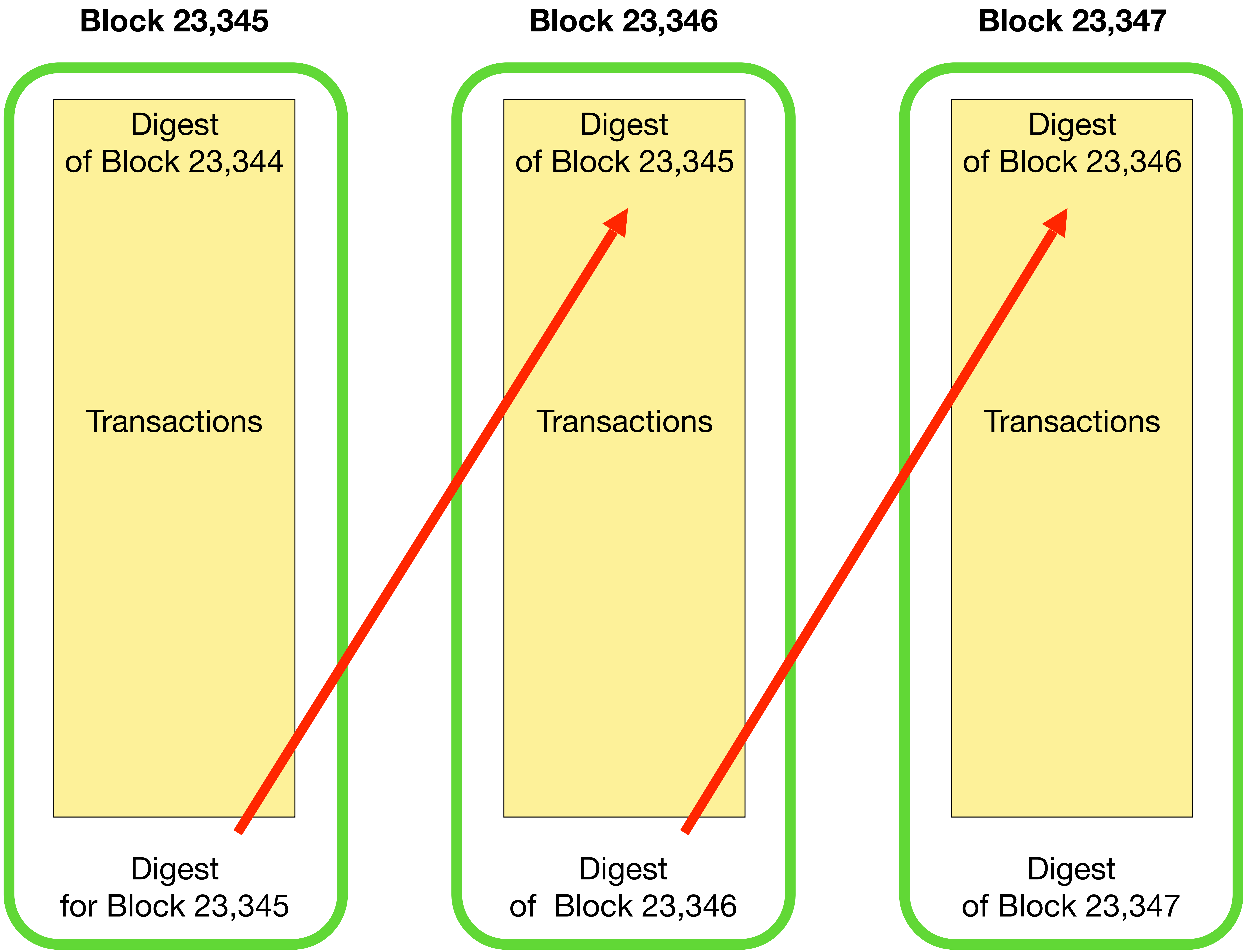
Digest

Rhino → cryptographic hash function → 0BD2 6C7D 2CDB FE3D 79A9 FD8E EE82 90B1 FB99 BB41

The white rhino runs into the hungry hippo → cryptographic hash function → 7D1B 91C0 F8BA CC25 8FCB CBA3 9D42 4FB4 1B67 C696

The white rhino runs imto the hungry hippo → cryptographic hash function → F04D 825D FFE4 77C6 662B 82FA BB8D 8A6C 72EA D091

The white rhino runs int the hungry hippo → cryptographic hash function → 22EC F97C DB2C 0488 91DC A544 EC82 4F8C 21B4 1337



Block 23,345

Digest
of Block 23,344

Transactions

Digest
for Block 23,345

Block 23,346

Digest
of Block 23,345

Transactions

Digest
of Block 23,346

Block 23,347

Digest
of Block 23,346

Transactions

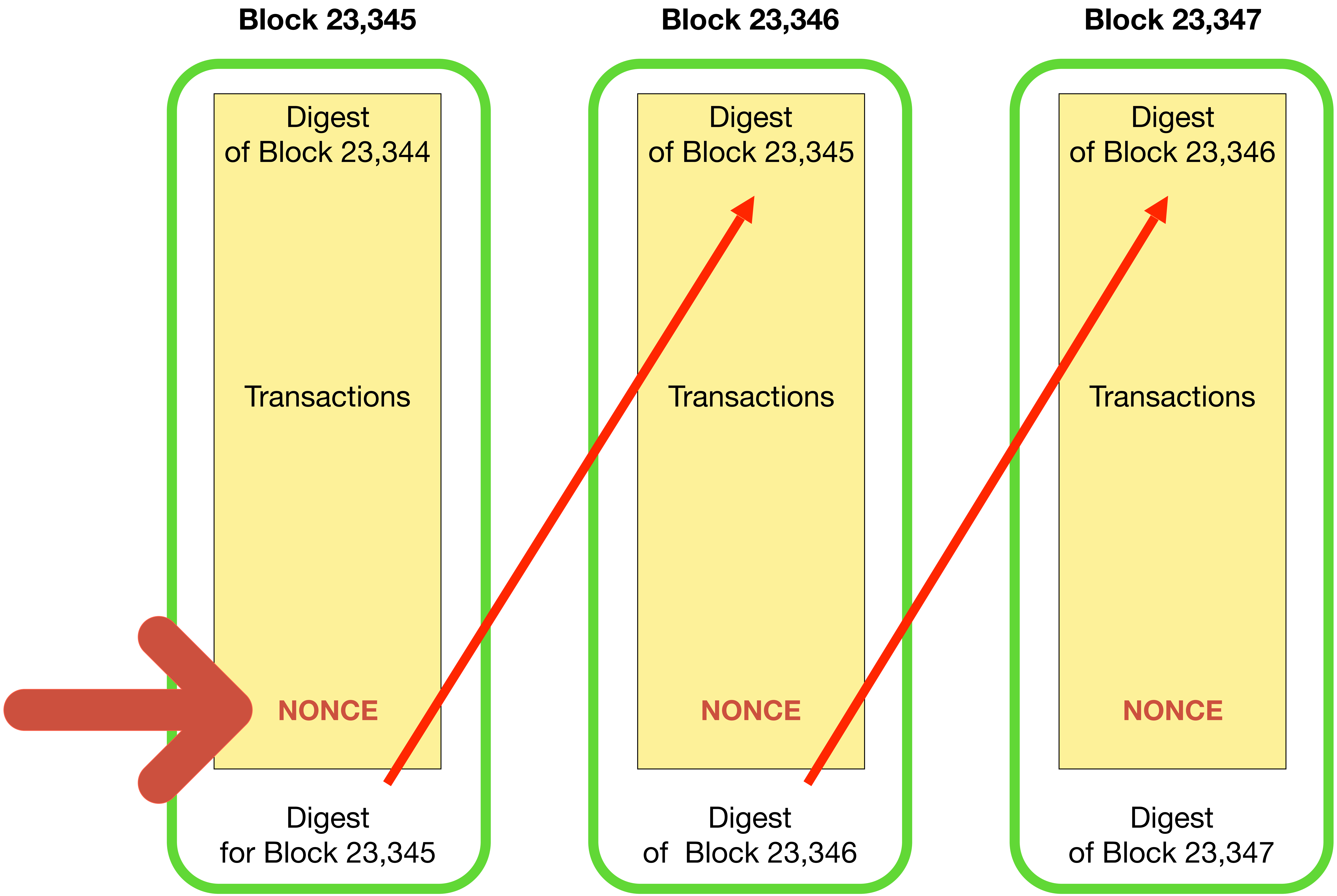
Digest
of Block 23,347

A bitcoin block hash digest:

```
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
```

This is really a number between 1 and 2^256 (in hexadecimal format)

Adding a cost for each block: “proof of work”



Block 23,345

Digest
of Block 23,344

Transactions

NONCE

Digest
for Block 23,345

Block 23,346

Digest
of Block 23,345

Transactions

NONCE

Digest
of Block 23,346

Block 23,347

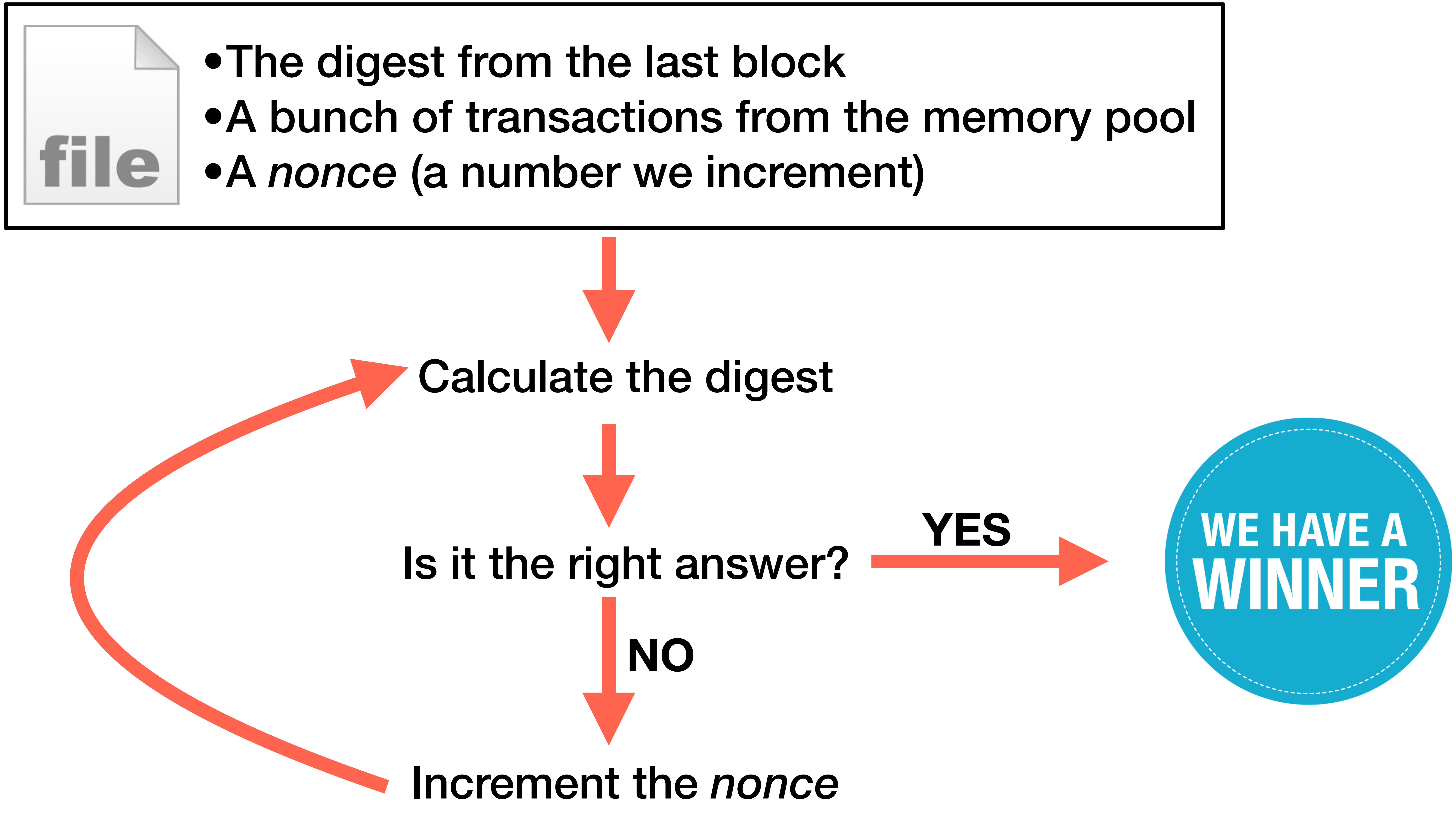
Digest
of Block 23,346

Transactions

NONCE

Digest
of Block 23,347

“mining”



- The digest from the last block
- A bunch of transactions from the memory pool
- A *nonce* (a number we increment)

Calculate the digest

Is it the right answer?

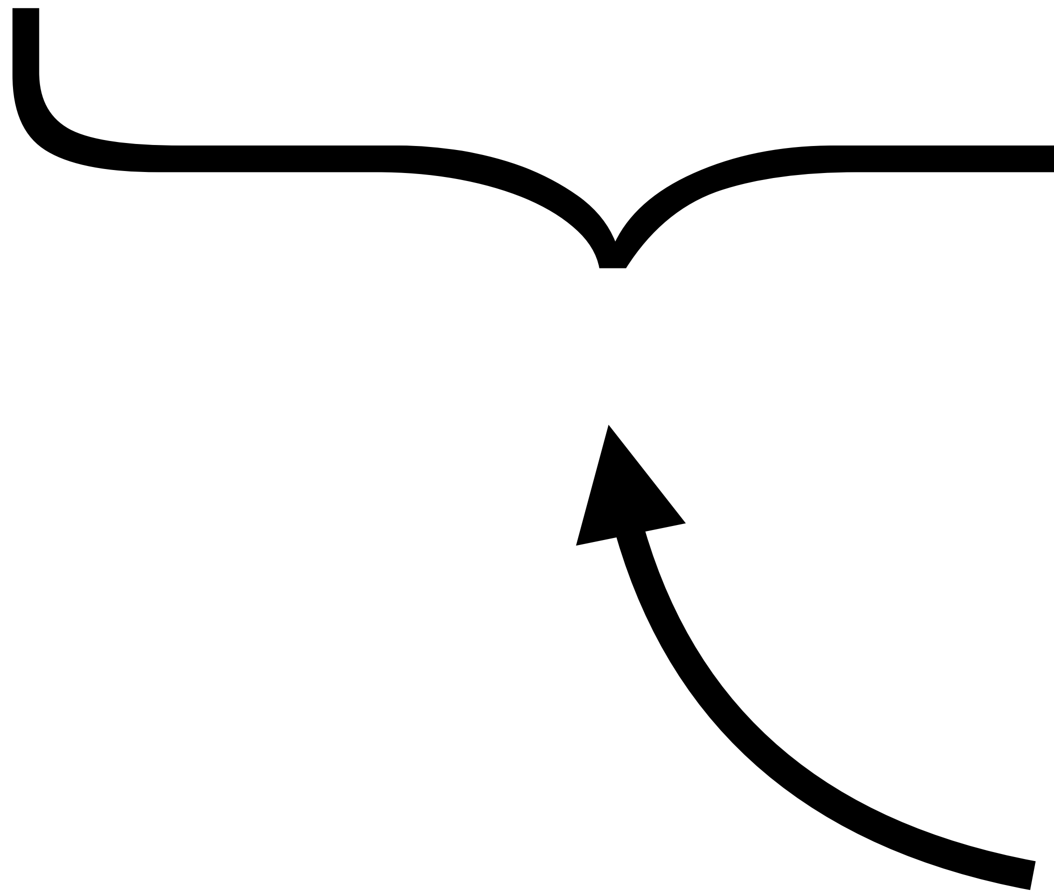
YES

NO

Increment the *nonce*

Example of a winning hash:

```
0000000000000000b42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
```



Make this shorter to increase the difficulty of “winning”

When a winner is found:

1. The winning node messages all other nodes: winner!
2. Other nodes verify and if OK accept the block
3. Once **51% of nodes** have accepted the block, the block is “confirmed”
4. **The winning node gets 12.5 bitcoin (plus any fees added by users)**

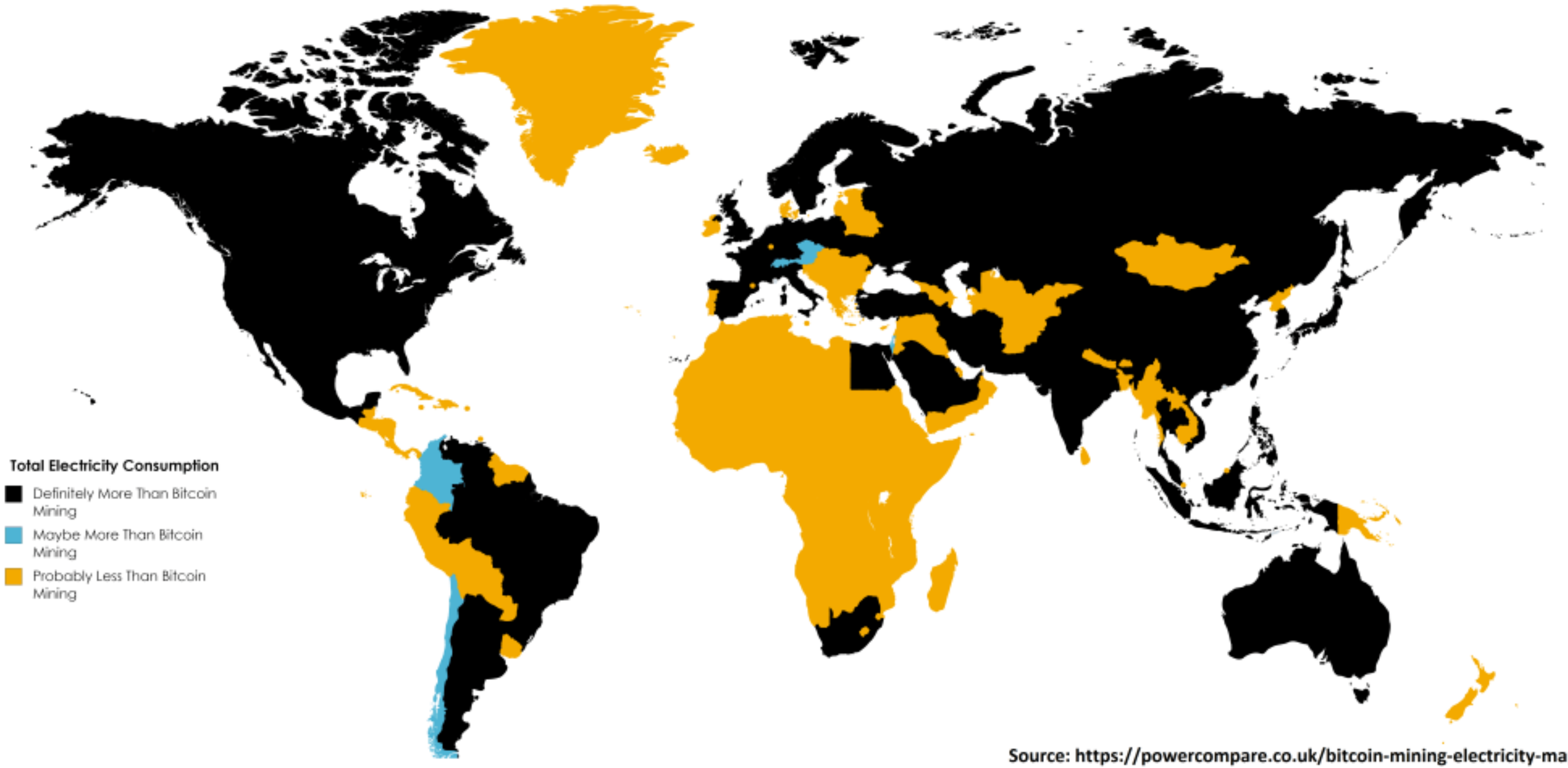
… and we start all over again

So …

a blockchain is really nothing more than an “**append only**” **transaction log** with useless work added to make it unchangeable?

Yes.

Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018


Total Electricity Consumption
■ Definitely More Than Bitcoin Mining
■ Maybe More Than Bitcoin Mining
■ Probably Less Than Bitcoin Mining

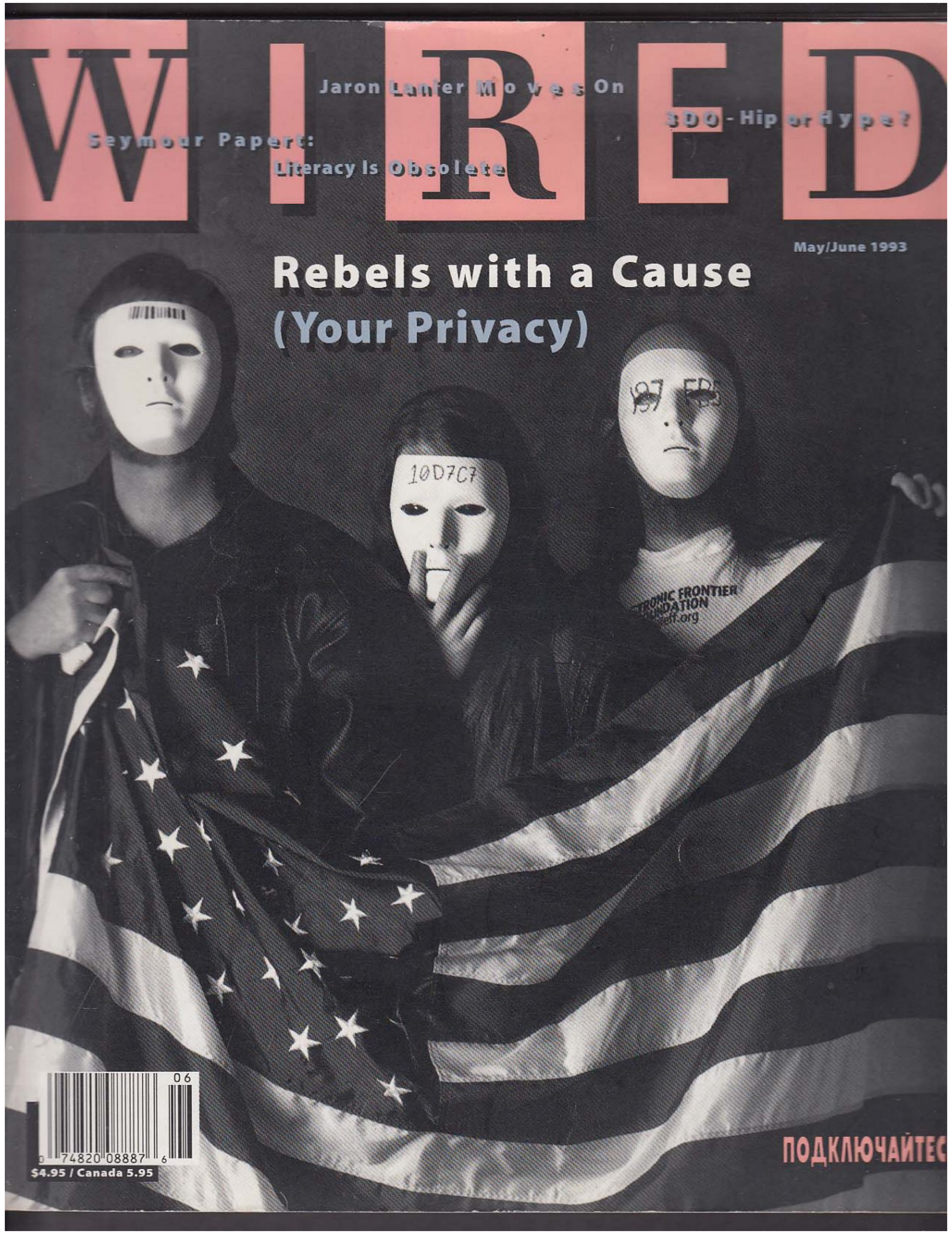
Source: https://powercompare.co.uk/bitcoin-mining-electricity-map/

Other consensus mechanisms

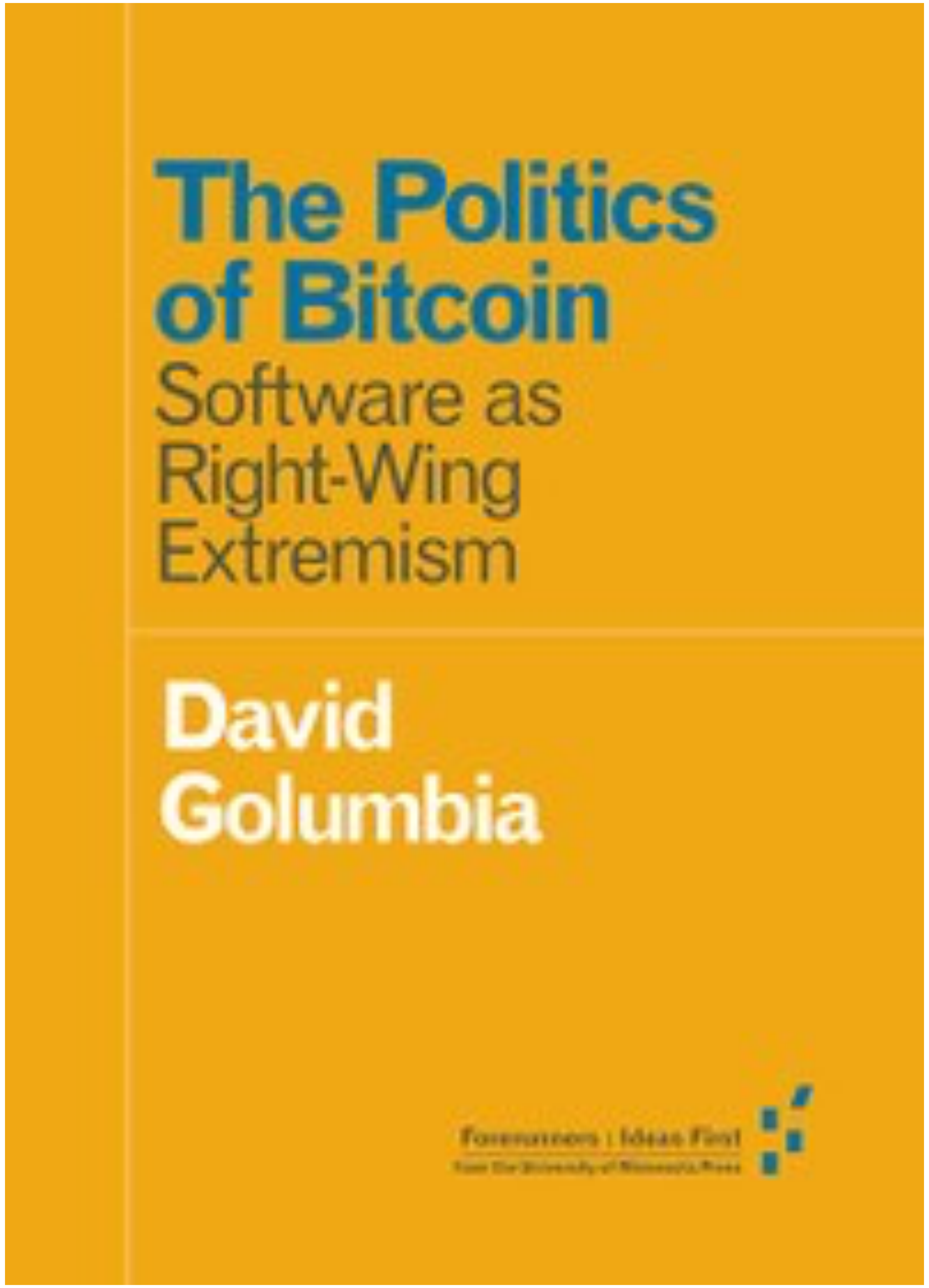
- Proof of Stake and Delegated Proof of Stake
- Proof of Authority
- Proof of Weight
- Byzantine Fault Tolerance approaches
- Directed Acyclic Graph approaches

2009

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.ÃˆŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

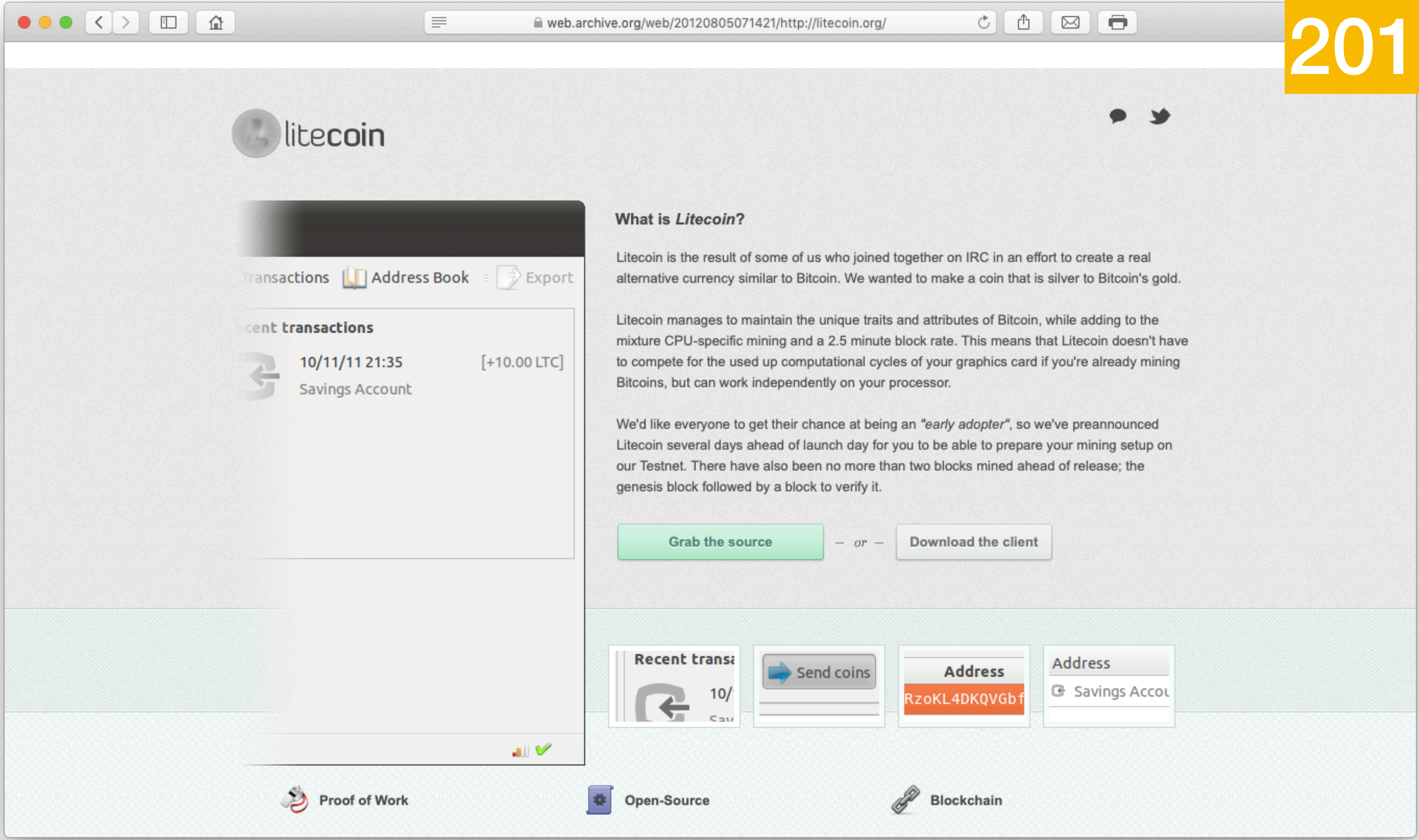


https://www.wired.com/1993/02/crypto-rebels/



https://www.upress.umn.edu/book-division/books/the-politics-of-bitcoin

2011



What is *Litecoin*?

Litecoin is the result of some of us who joined together on IRC in an effort to create a real alternative currency similar to Bitcoin. We wanted to make a coin that is silver to Bitcoin's gold.

Litecoin manages to maintain the unique traits and attributes of Bitcoin, while adding to the mixture CPU-specific mining and a 2.5 minute block rate. This means that Litecoin doesn't have to compete for the used up computational cycles of your graphics card if you're already mining Bitcoins, but can work independently on your processor.

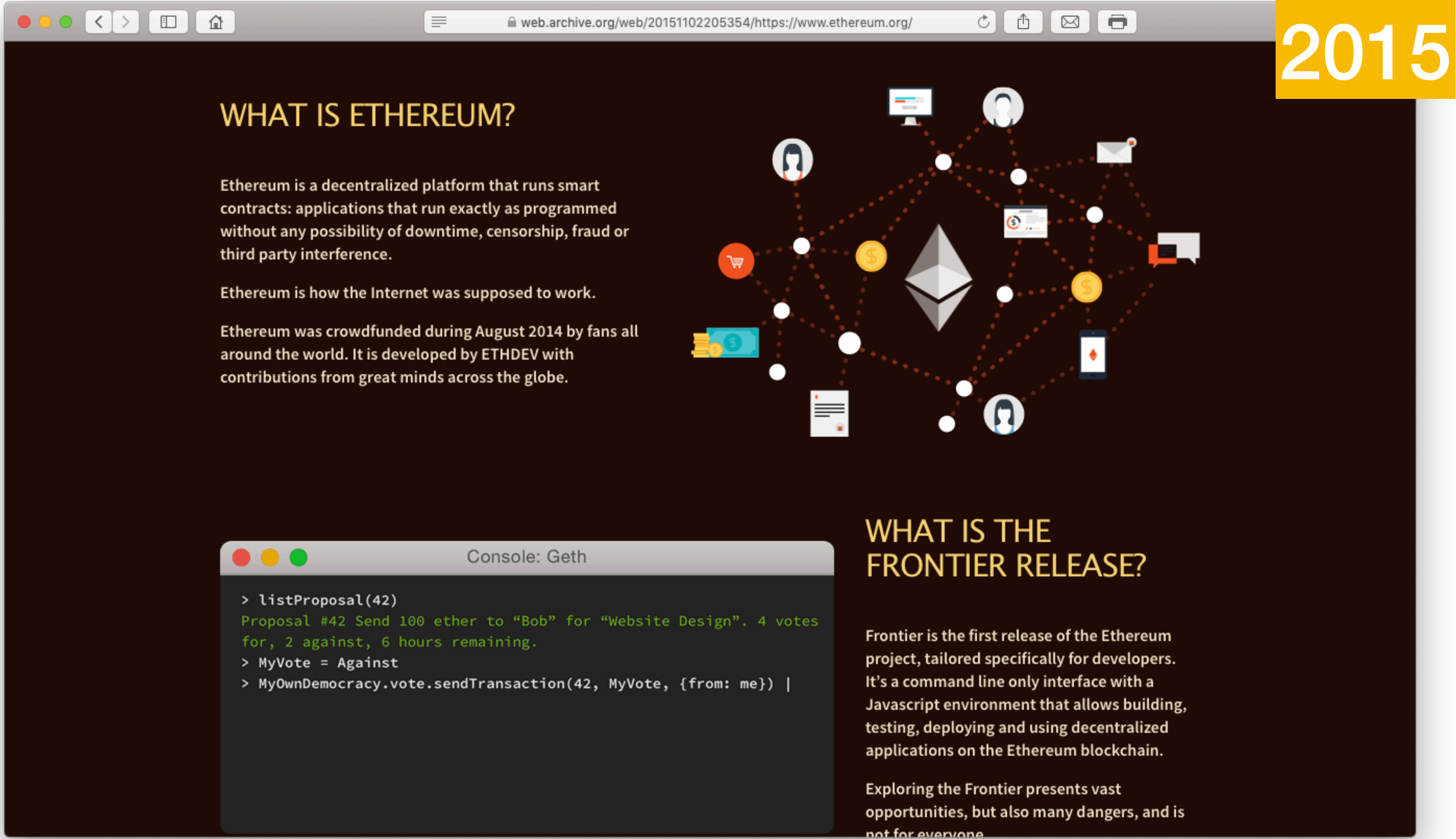
We'd like everyone to get their chance at being an *"early adopter"*, so we've preannounced Litecoin several days ahead of launch day for you to be able to prepare your mining setup on our Testnet. There have also been no more than two blocks mined ahead of release; the genesis block followed by a block to verify it.

Proof of Work

Open-Source

Blockchain

2015


web.archive.org/web/20151102205354/https://www.ethereum.org/

WHAT IS ETHEREUM?

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

Ethereum is how the Internet was supposed to work.

Ethereum was crowdfunded during August 2014 by fans all around the world. It is developed by ETHDEV with contributions from great minds across the globe.

Console: Geth

```
> listProposal(42)
Proposal #42 Send 100 ether to “Bob” for “Website Design”. 4 votes
for, 2 against, 6 hours remaining.
> MyVote = Against
> MyOwnDemocracy.vote.sendTransaction(42, MyVote, {from: me}) |
```

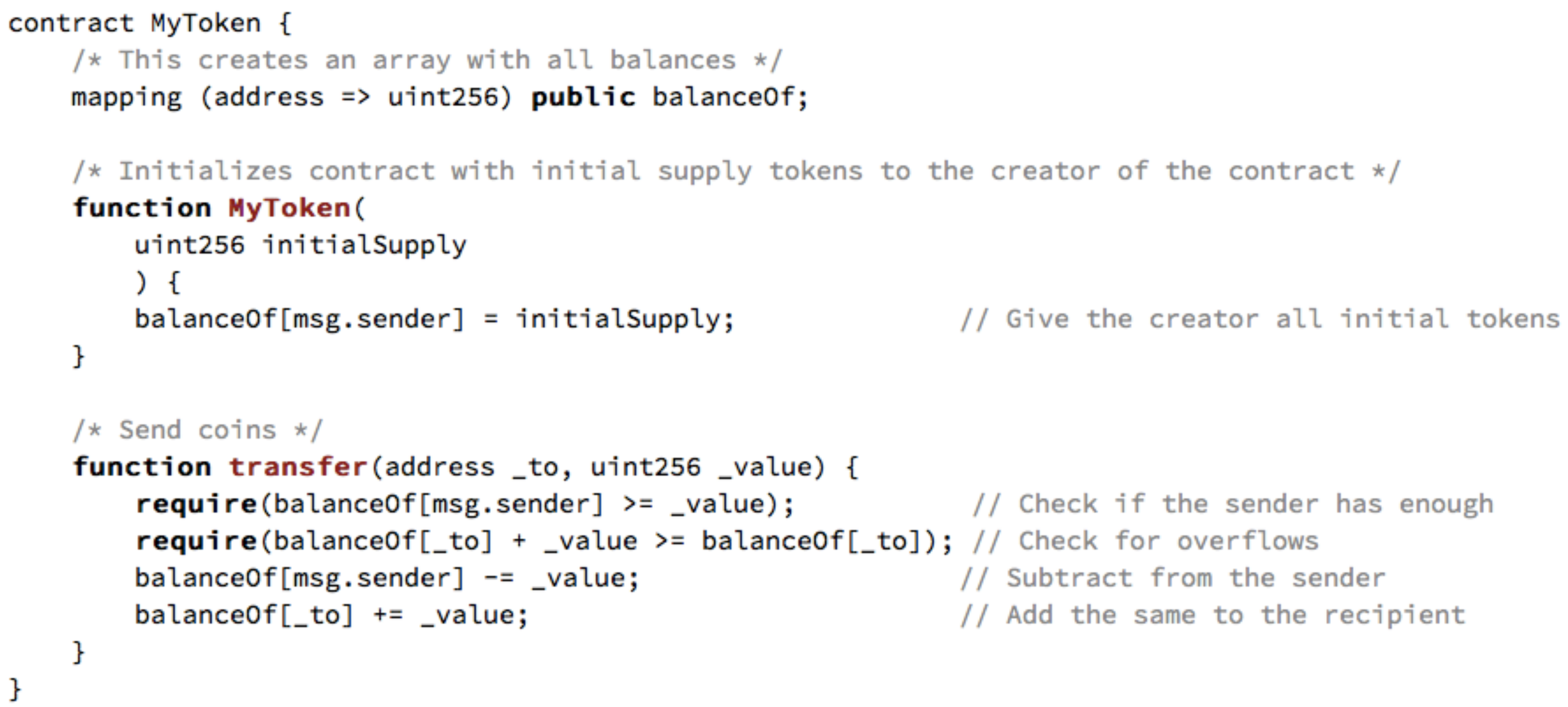
WHAT IS THE FRONTIER RELEASE?

Frontier is the first release of the Ethereum project, tailored specifically for developers. It’s a command line only interface with a Javascript environment that allows building, testing, deploying and using decentralized applications on the Ethereum blockchain.

Exploring the Frontier presents vast opportunities, but also many dangers, and is not for everyone

“Smart” contracts

- A computer program that “lives” on the (Ethereum) blockchain
- Anyone can add one, for a small fee
- Takes action based on inputs and conditions
- Running a smart contract costs “gas”, which is a small bit of “ether”
- Has its own balance of funds and can send and receive money
- Can create and track “value” by the way of “tokens”
- Other users can send and receive messages from the smart contract



```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

Baked!
Lay's
Fritos
Gardetto's
Cheetos
HERSHEY'S
0.00

Make a selection

- Machine keeps the coin
- You receive candy

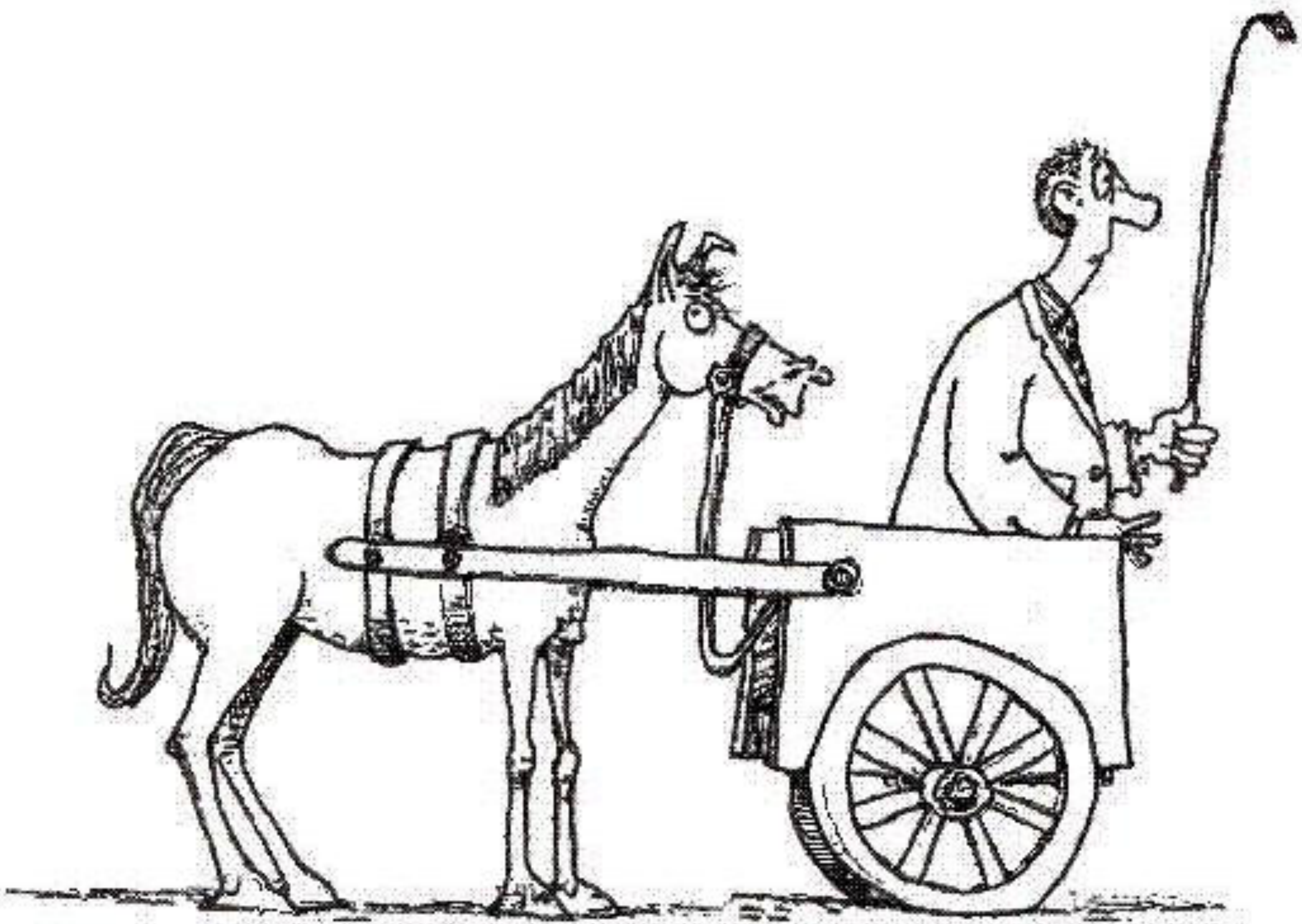
Don’t make a selection

- Machine keeps the candy
- You receive the coin back

(Touted) applications

- Escrow services
- Transactional instruments (e.g. mortgage, deed, etc.)
- Supply chain management
- Securities transactions
- **ICO's**

The Initial Coin Offering



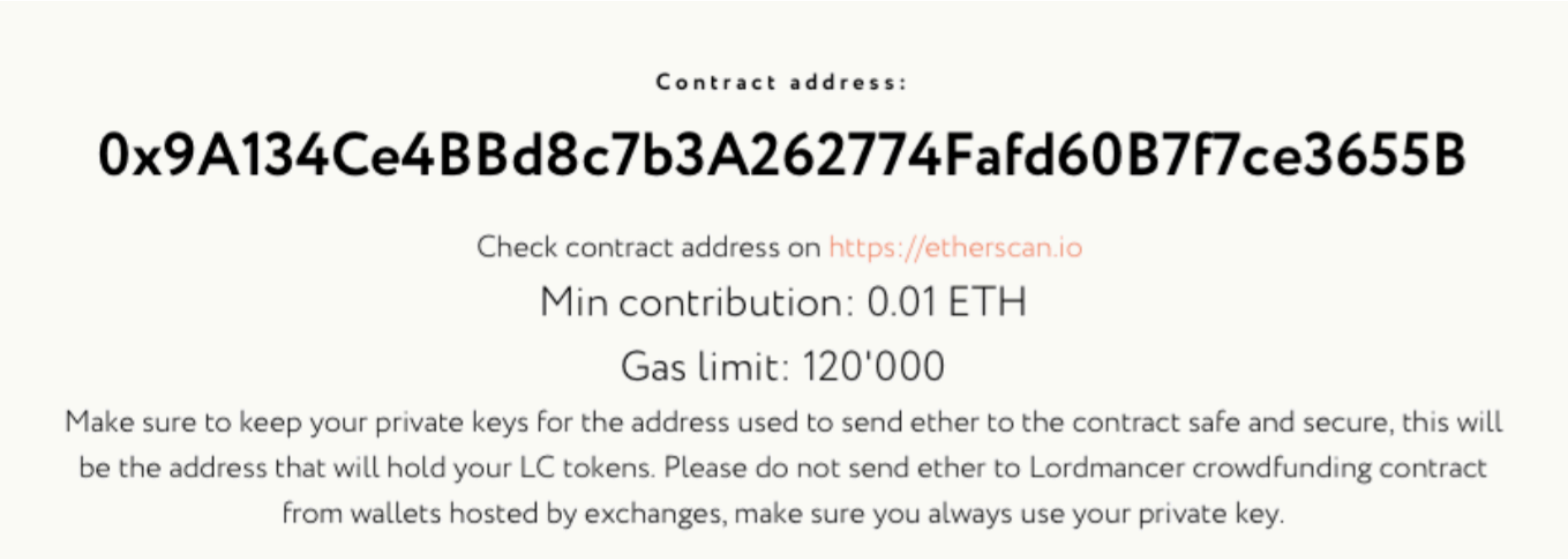
The three stages of an ICO

1. New project sells tokens in exchange for usually Bitcoin or Ether

2. Promoters then sell the Bitcoin or Ether for cash to fund their project

3. After the ICO, tokens can usually be traded on an exchange

Buying into an ICO is easy



Contract address:

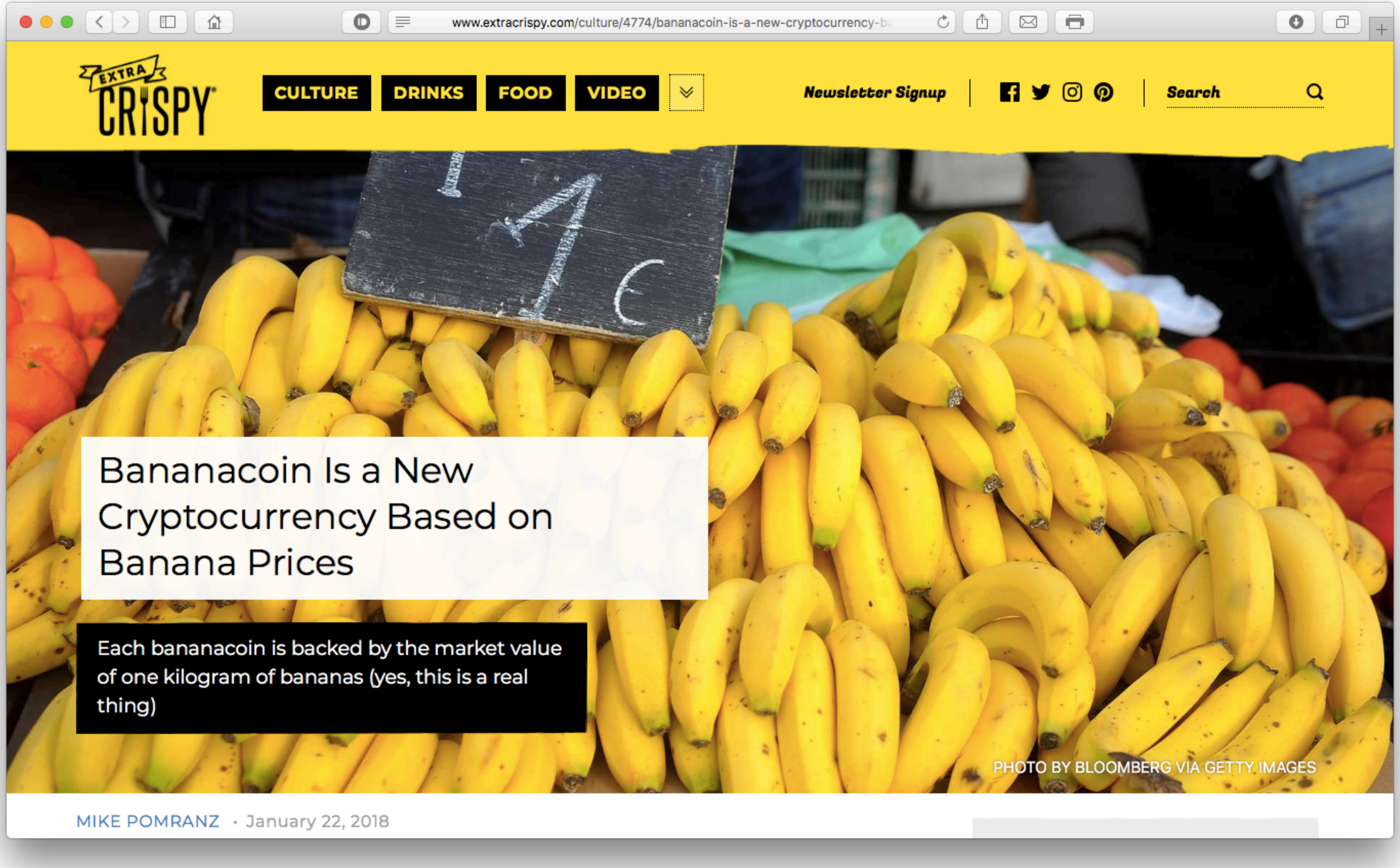
0x9A134Ce4BBd8c7b3A262774Fafd60B7f7ce3655B

Check contract address on https://etherscan.io

Min contribution: 0.01 ETH

Gas limit: 120'000

Make sure to keep your private keys for the address used to send ether to the contract safe and secure, this will be the address that will hold your LC tokens. Please do not send ether to Lordmancer crowdfunding contract from wallets hosted by exchanges, make sure you always use your private key.

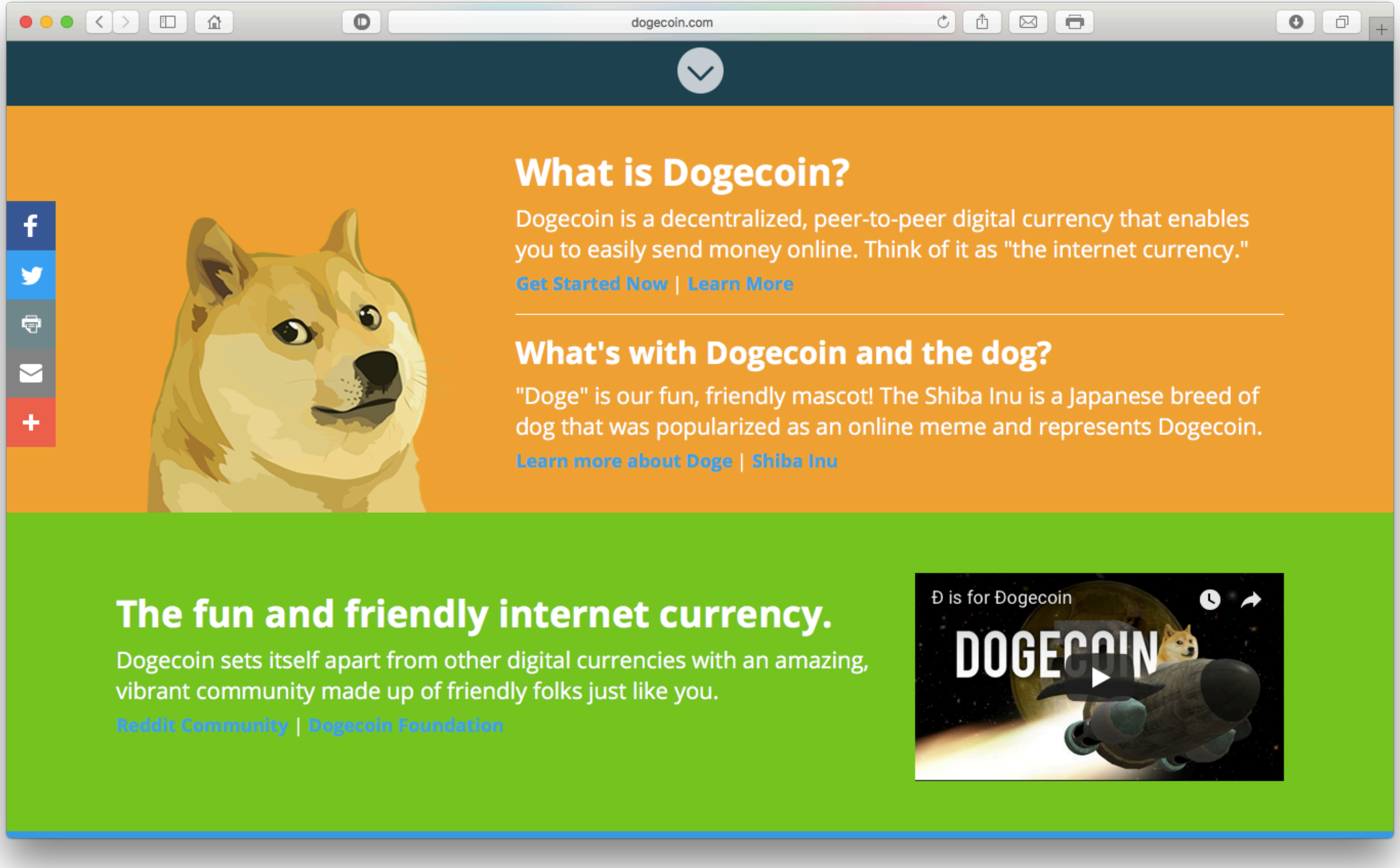

www.extracrispy.com/culture/4774/bananacoin-is-a-new-cryptocurrency-b
EXTRA CRISPY
CULTURE
DRINKS
FOOD
VIDEO
Newsletter Signup
Search
1 €

Bananacoin Is a New Cryptocurrency Based on Banana Prices

Each bananacoin is backed by the market value of one kilogram of bananas (yes, this is a real thing)

PHOTO BY BLOOMBERG VIA GETTY IMAGES

MIKE POMRANZ · January 22, 2018



What is Dogecoin?

Dogecoin is a decentralized, peer-to-peer digital currency that enables you to easily send money online. Think of it as "the internet currency."

Get Started Now | Learn More

What's with Dogecoin and the dog?

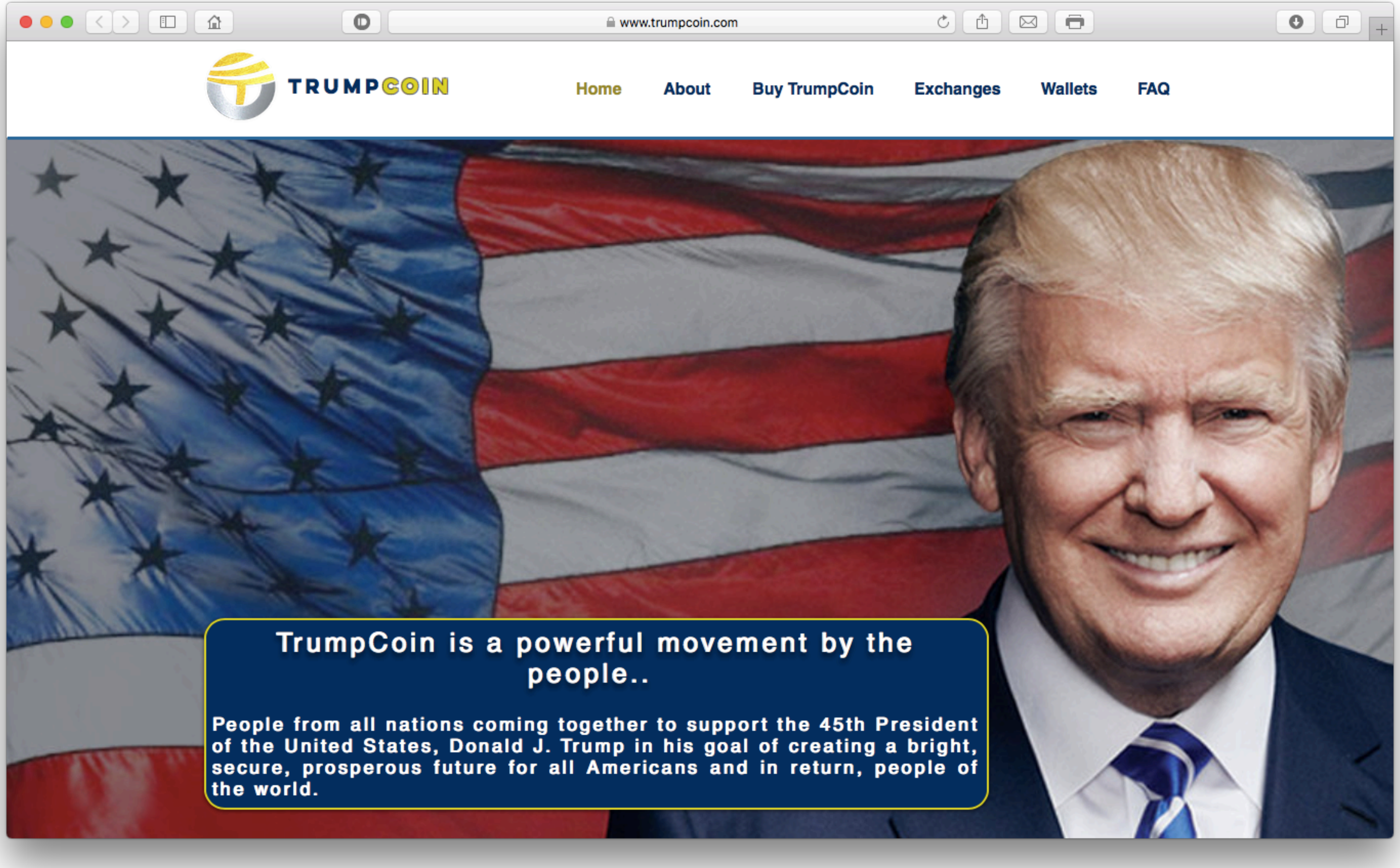
"Doge" is our fun, friendly mascot! The Shiba Inu is a Japanese breed of dog that was popularized as an online meme and represents Dogecoin.

Learn more about Doge | Shiba Inu

The fun and friendly internet currency.

Dogecoin sets itself apart from other digital currencies with an amazing, vibrant community made up of friendly folks just like you.

Reddit Community | Dogecoin Foundation



TrumpCoin is a powerful movement by the people..

People from all nations coming together to support the 45th President of the United States, Donald J. Trump in his goal of creating a bright, secure, prosperous future for all Americans and in return, people of the world.

Token Sales, Jan14-Aug18

Total Raised:
$307,160,995

elementus
?
The DAO $168m
Ethereum $19m
Europe
North America
Asia
Middle East
Stateless/Unknown
13 JAN 17
Monthly Total ($)
01 JAN 14
01 JAN 15
01 JAN 16
01 JAN 17
01 JAN 18

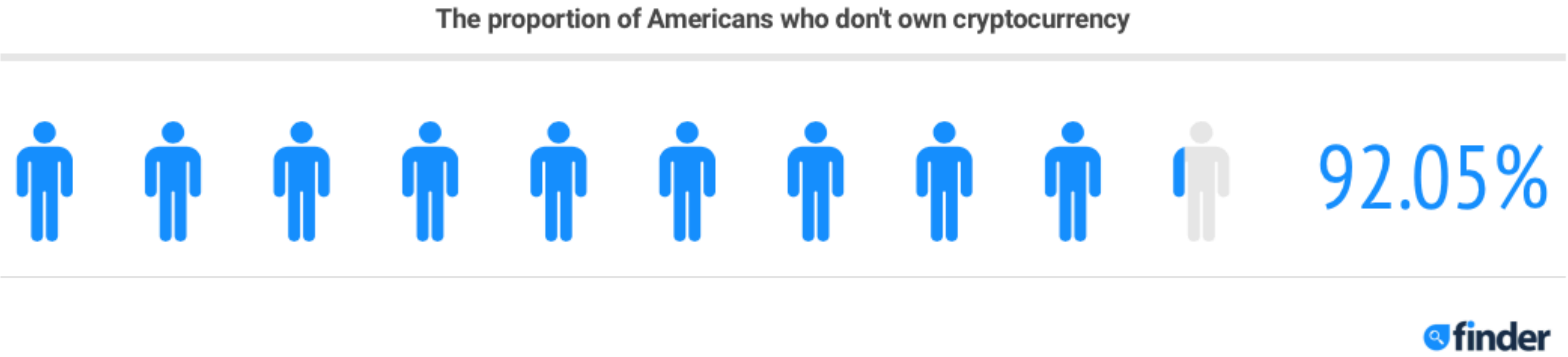
Today*

- 2,400+ different cryptocurrencies/tokens
- $309 billion “market cap”
- $62 billion daily trading volume
- ICO’s now also called STO’s,TGE’s, IEO’s, and ILP’s

https://coinmarketcap.com

*August 2019

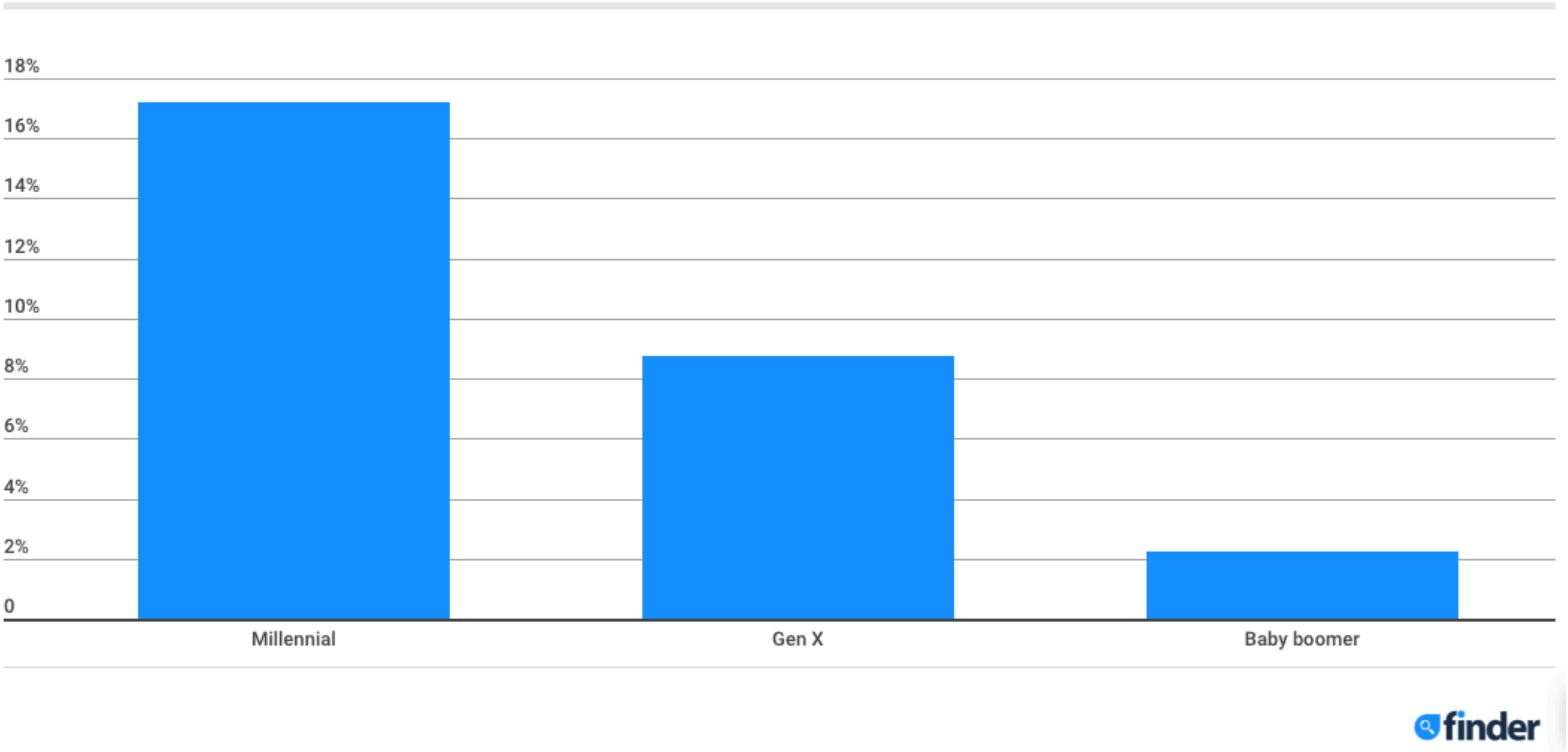
Who does not own crypto



The proportion of Americans who don't own cryptocurrency

https://www.finder.com/why-people-arent-buying-cryptocurrency

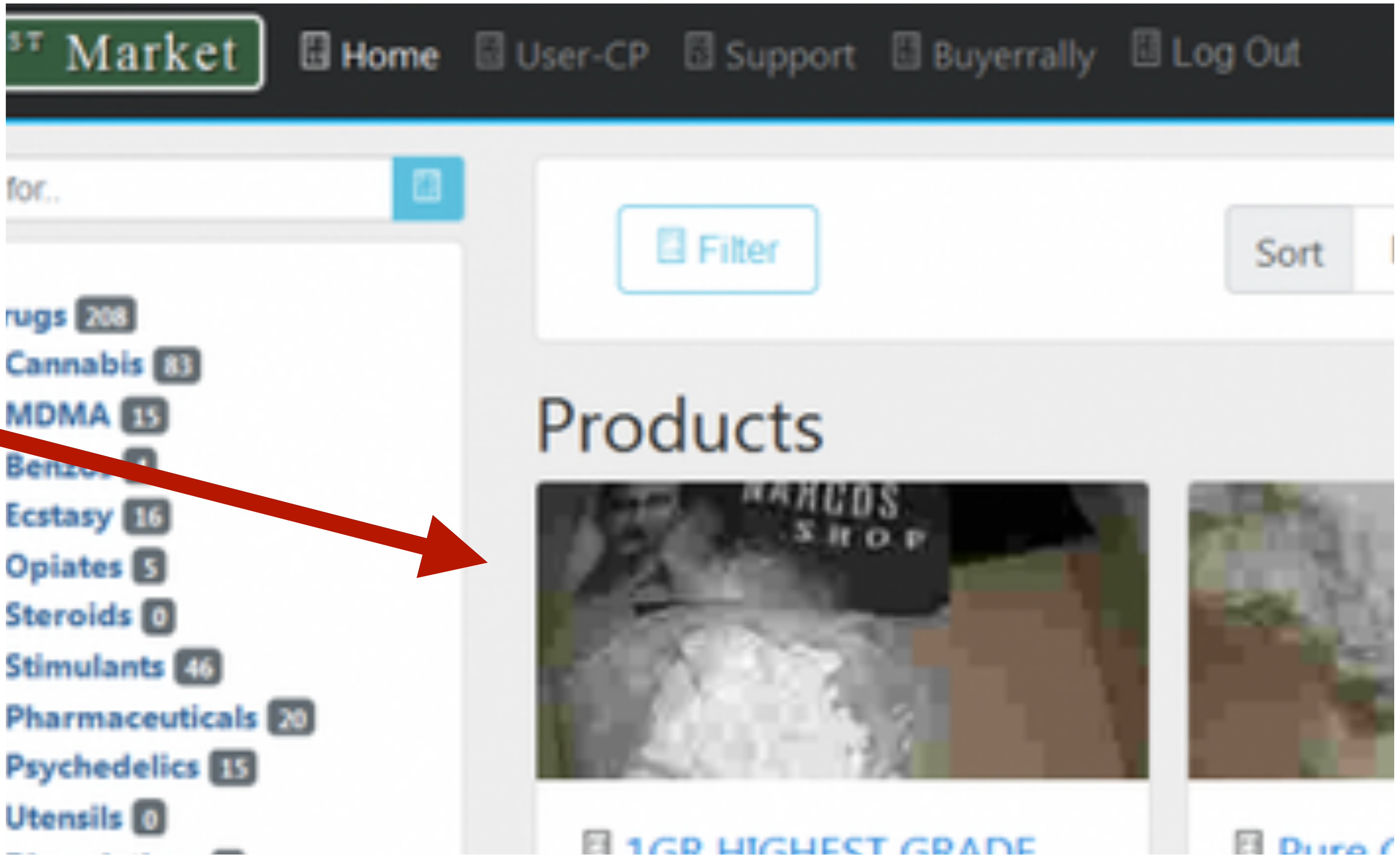
And those that do, by generation



https://cointelegraph.com/news/how-many-americans-really-own-crypto-skewed-results-of-polls-and-surveys

Cryptocurrency uses (today)

- **Speculation**
- **Illegal goods**
- **Ransomware**
- Commercial adoption has failed to date

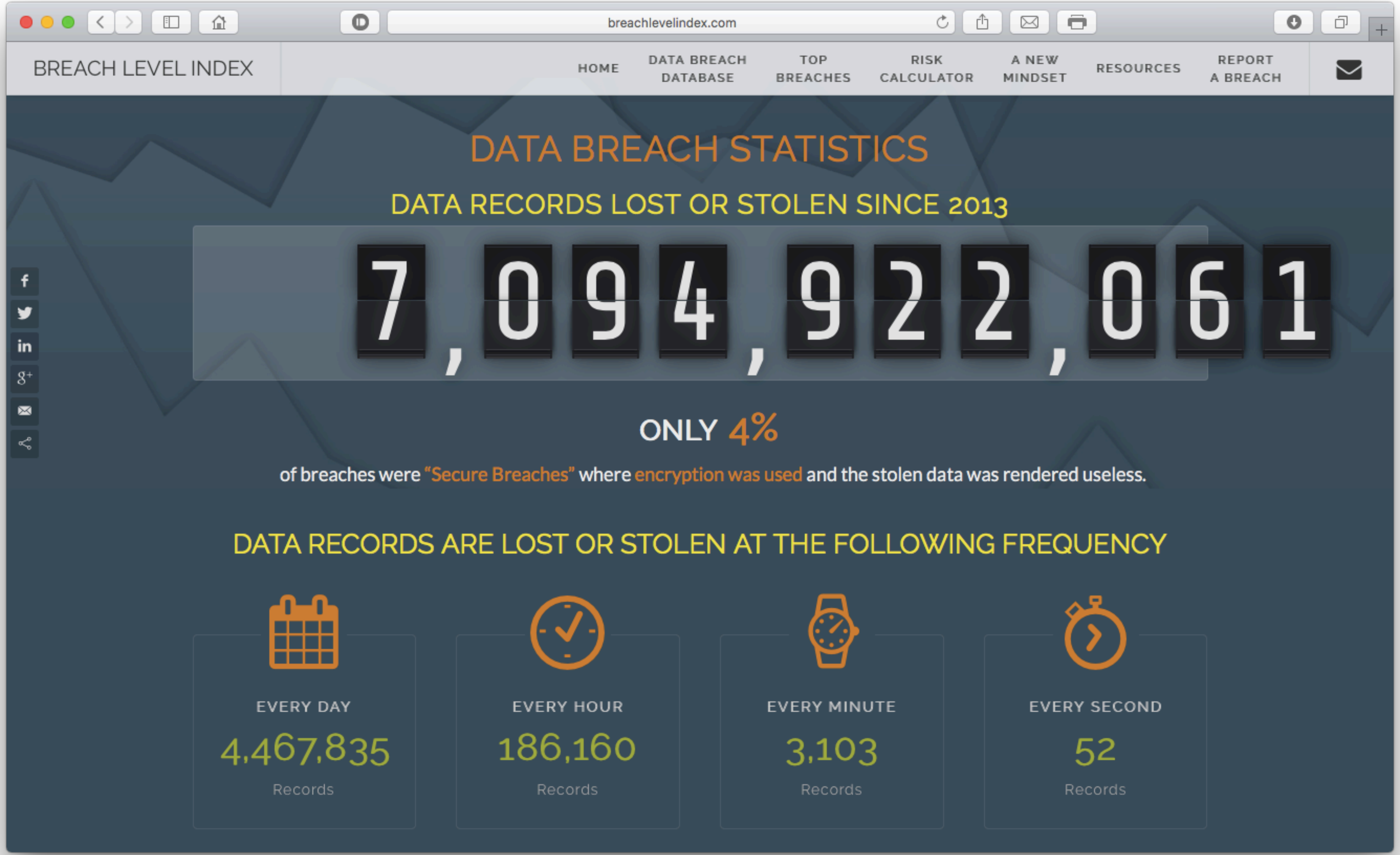


Part 3:
Cybersecurity

Protect computers, networks, programs and **data**

from

unintended or unauthorized access, change or destruction.



DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

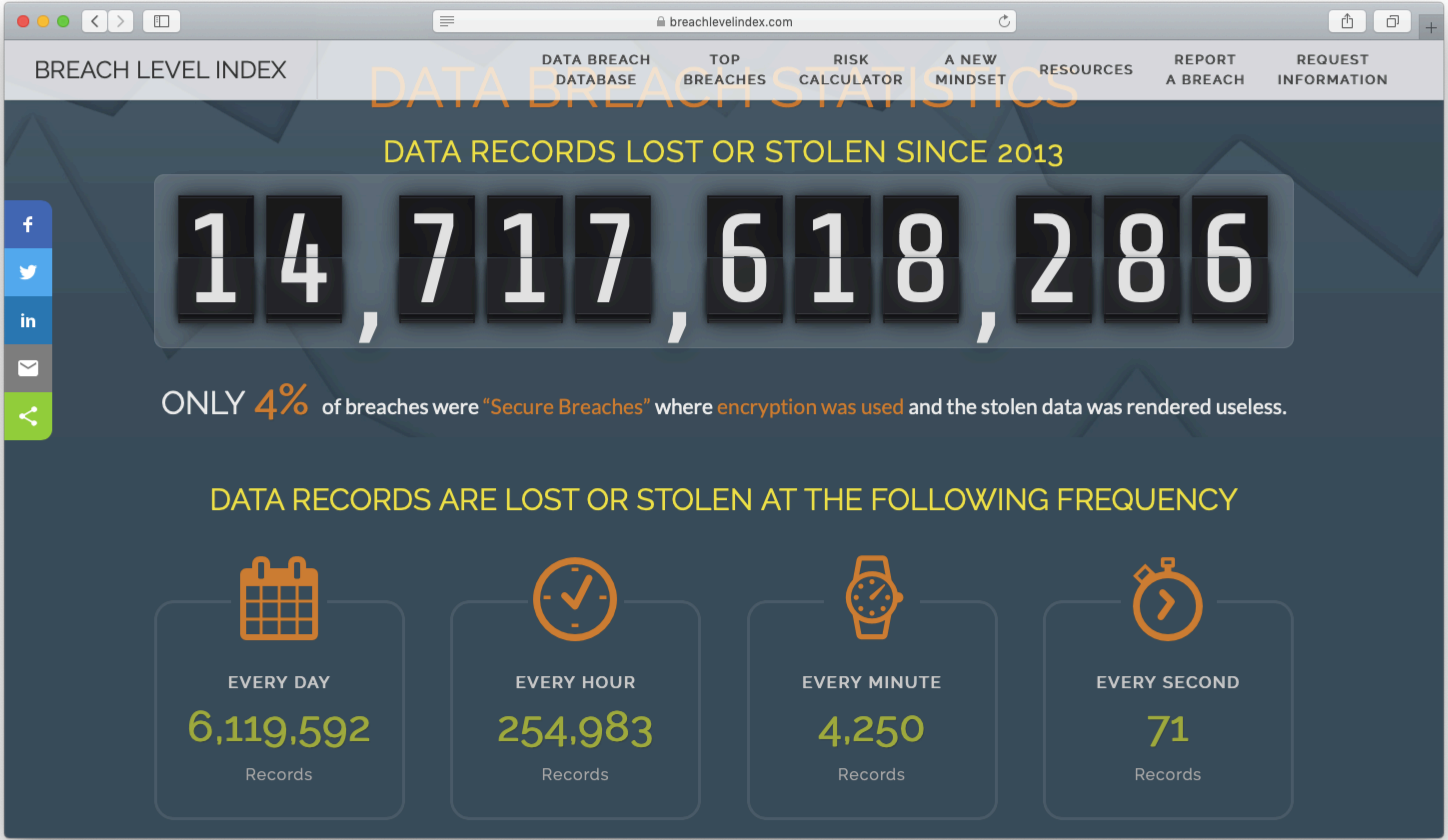
7,094,922,061

ONLY 4%

of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY	EVERY HOUR	EVERY MINUTE	EVERY SECOND
4,467,835 Records	186,160 Records	3,103 Records	52 Records



DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

14,717,618,286

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY	EVERY HOUR	EVERY MINUTE	EVERY SECOND
6,119,592 Records	254,983 Records	4,250 Records	71 Records

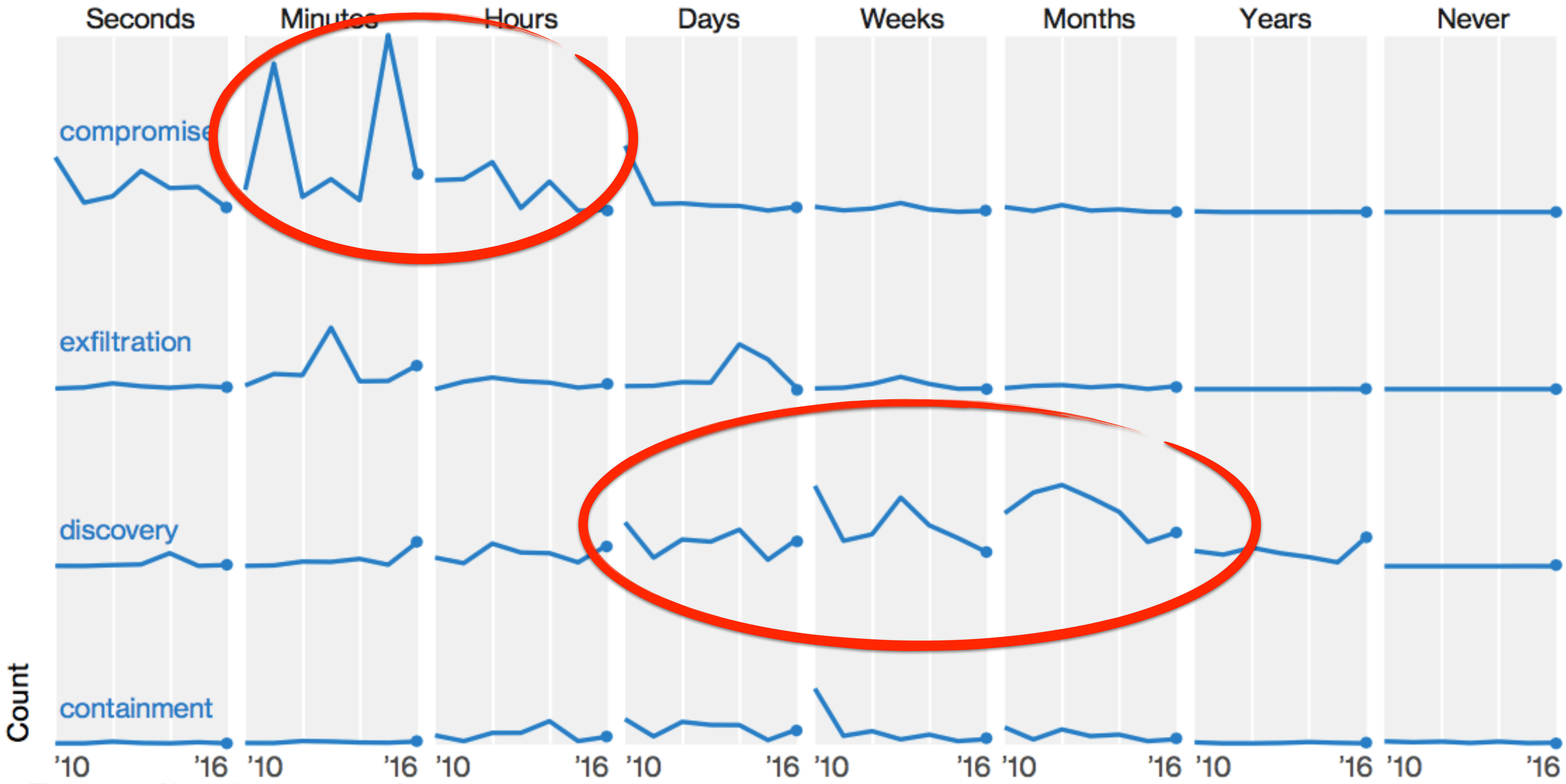


Figure 8: Timespan of breach events over time

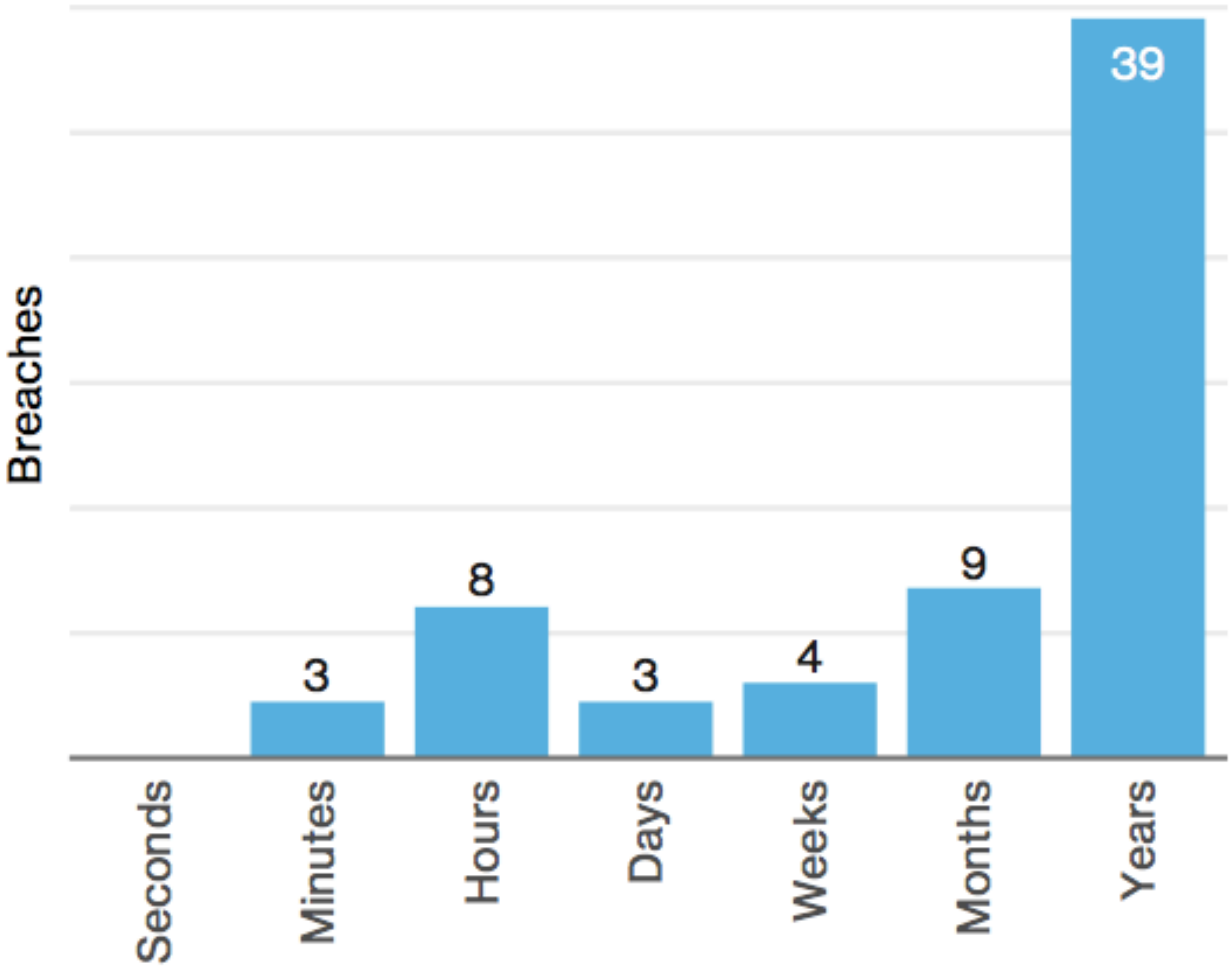
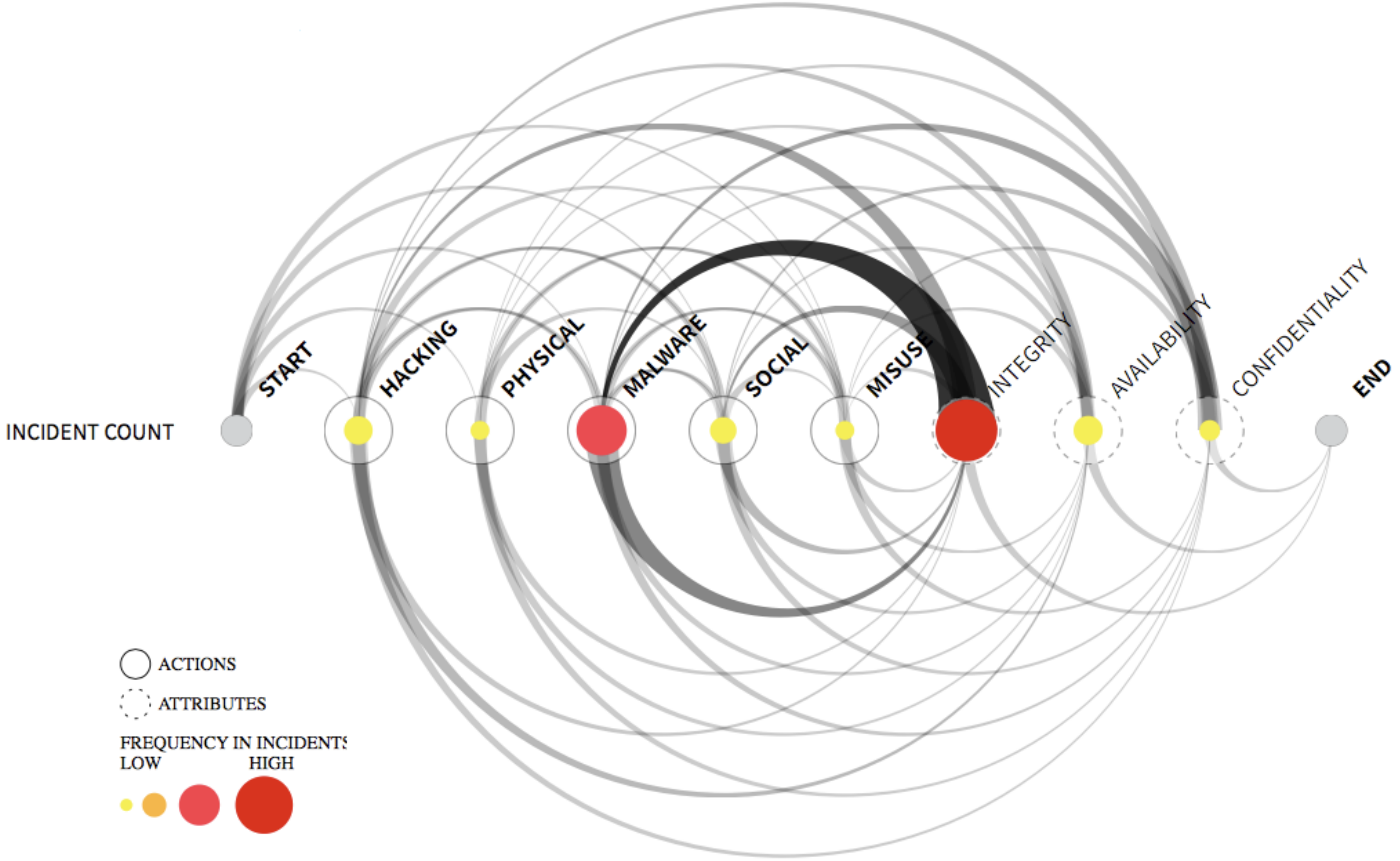


Figure 27: Time-to-discovery within Public breaches (n=66)


INCIDENT COUNT
START
HACKING
PHYSICAL
MALWARE
SOCIAL
MISUSE
INTEGRITY
AVAILABILITY
CONFIDENTIALITY
END
ACTIONS
ATTRIBUTES
FREQUENCY IN INCIDENTS
LOW
HIGH

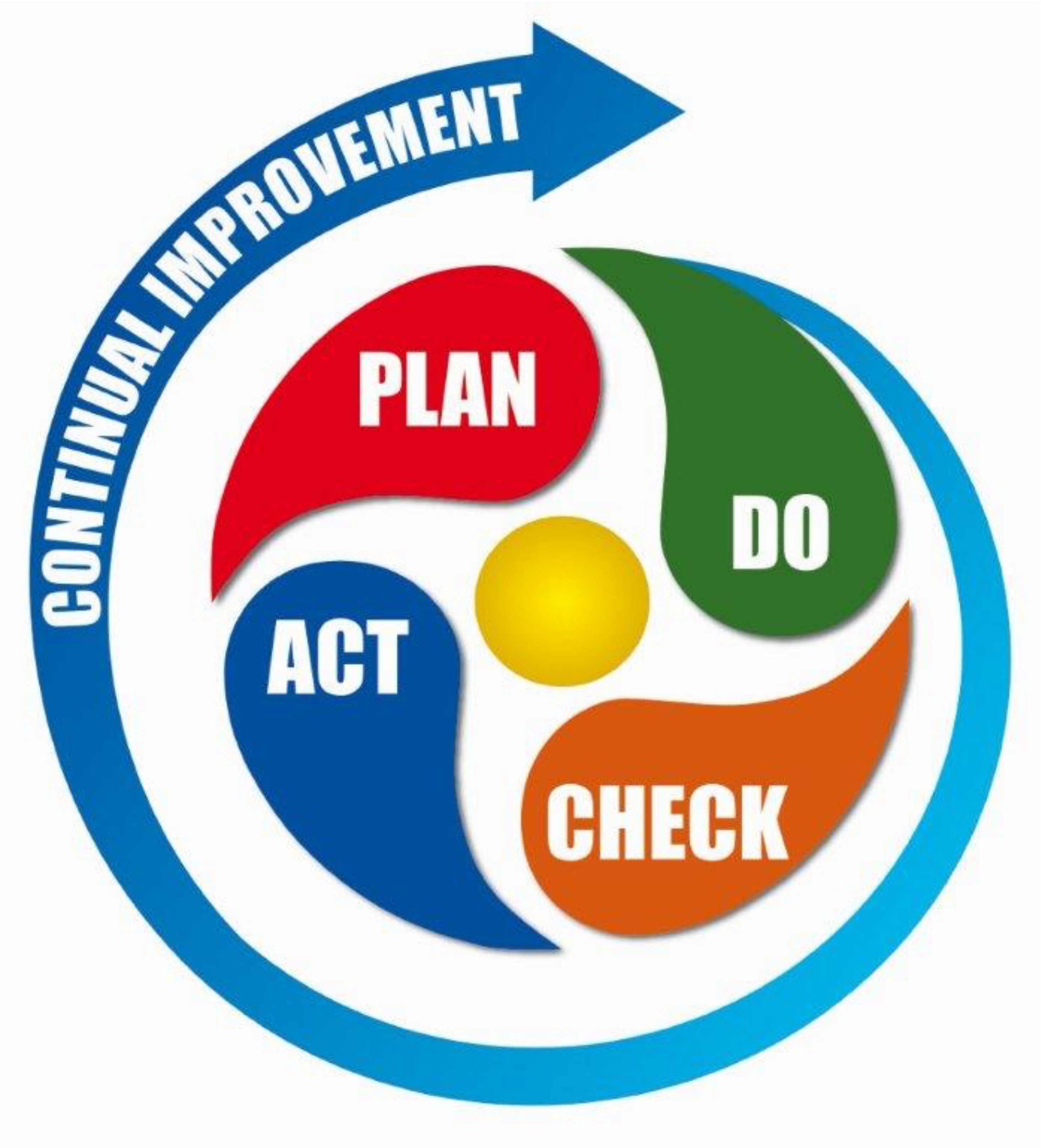
V.

Observations

- It is impossible to be 100% safe.
- Change is the constant.
- It’s not going to get any better, at least in the short term.
- Any part of a computing system whether it be hardware, software, storage media, data, and **people** can be an entry point for an attack and any system is most vulnerable at its weakest point.

Cybersecurity frameworks

- **Identify assets** and classify them
- Perform a **risk assessment** and identify necessary controls
- Formulate standards, procedures and behaviours to enable the **controls**
- **Apply**, review/test and **improve**



Framework	Focus	Sponsoring organization
COSO	Financial operations and risk management.	Committee of Sponsoring Organizations (COSO)
ITIL	Best practices for managing and delivering IT services.	Information technology Infrastructure Library (ITIL)
ISO	International member organization focusing on IT service management, information security management, corporate governance of IT security, IT risk management, and quality management.	International Organization for Standardization (ISO)
COBIT	International governance, assessment, and management of IT security and risk management process.	Information Systems Audit and Control Association (ISACA)
NIST	IT security standards for federal agencies mandated by the Federal Information Security Management Act (FISMA).	National Institute of Standards and Technology (NIST)
CSF	Voluntary risk-based framework that focuses on IT security and risk management processes.	Presidential Executive Order 13636, Improving Critical Infrastructure Cybersecurity, dated 12 Feb 2013
ISF	International member organization focusing on IT security, governance, and managing information risk.	Information Security Forum (ISF)
PCI DSS	IT security standard for the protection of credit card account data security. Card companies include Visa, MasterCard, American Express, Discover, and Japan Credit Bureau.	Payment Card Industry (PCI) Security Standards Council
SANS Institute	Although not a framework, the widely adopted top 20 critical security controls are based on the NIST SP 800-53 control standards.	SANS Institute

Risk Areas

1. Policy
2. Governance control
3. Personnel security
4. Physical security
5. Asset management
6. Access control
7. Security of operations
8. Network security
9. Computer security
10. Software development and maintenance security
11. Acquisition
12. Incident management
13. Compliance
14. Continuity
15. Elements of human factors such as training and education

Seven things
you can and should do now

1. Get good at spotting phishing.

(91% of cyberattacks begin with a spear phishing email)

https://www.techradar.com/best/best-free-cybersecurity-courses-online

https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email

2. Use 2 factor authentication

Something you know.

Something you have.

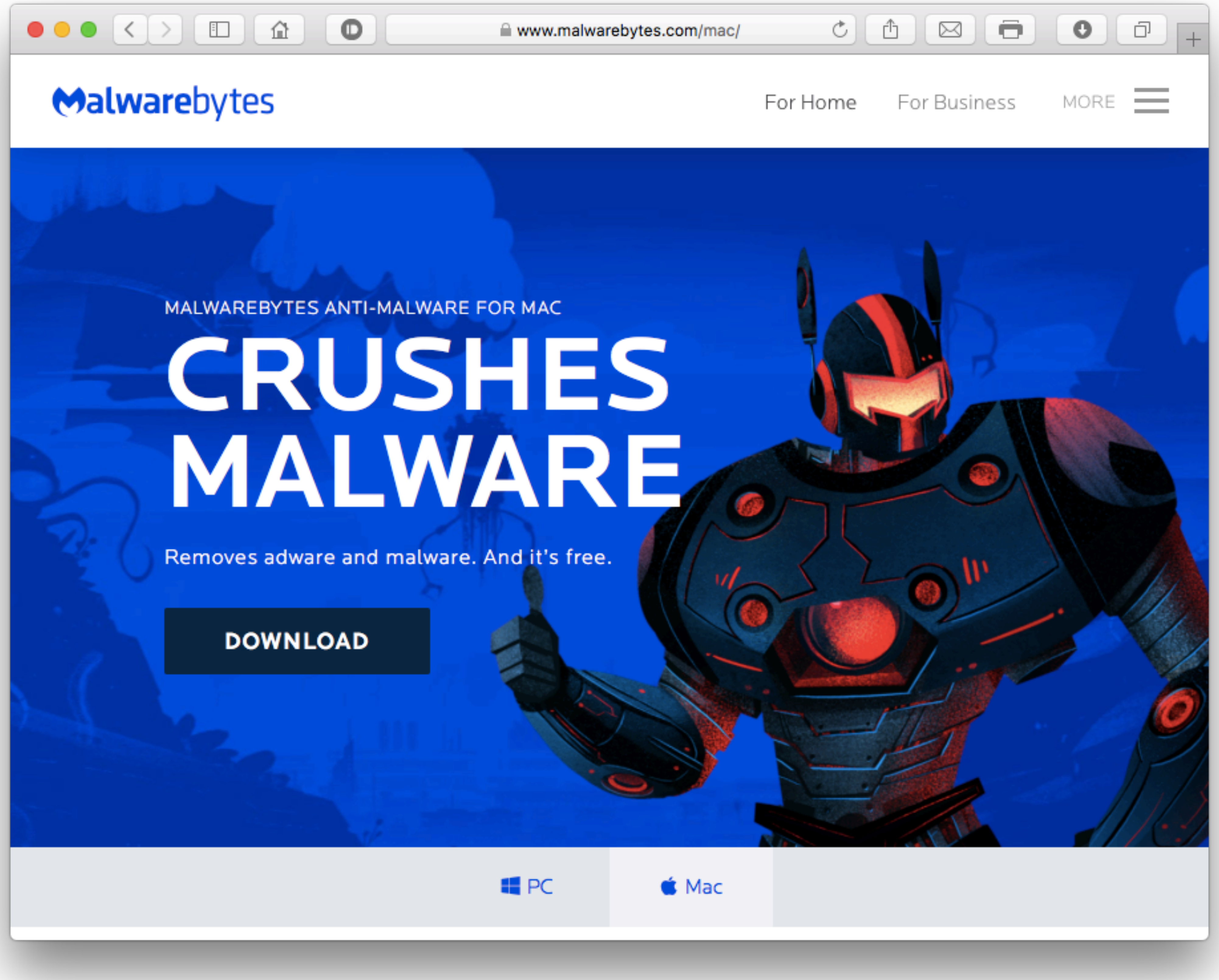
http://www.pcmag.com/article2/0,2817,2456400,00.asp

3. Do passwords right

- Use different email addresses for account creation
- Long passwords (word-word-word-number-character)
- Don’t re-use passwords
- Use a password manager (e.g. Apple Keychain)

4. Back it up

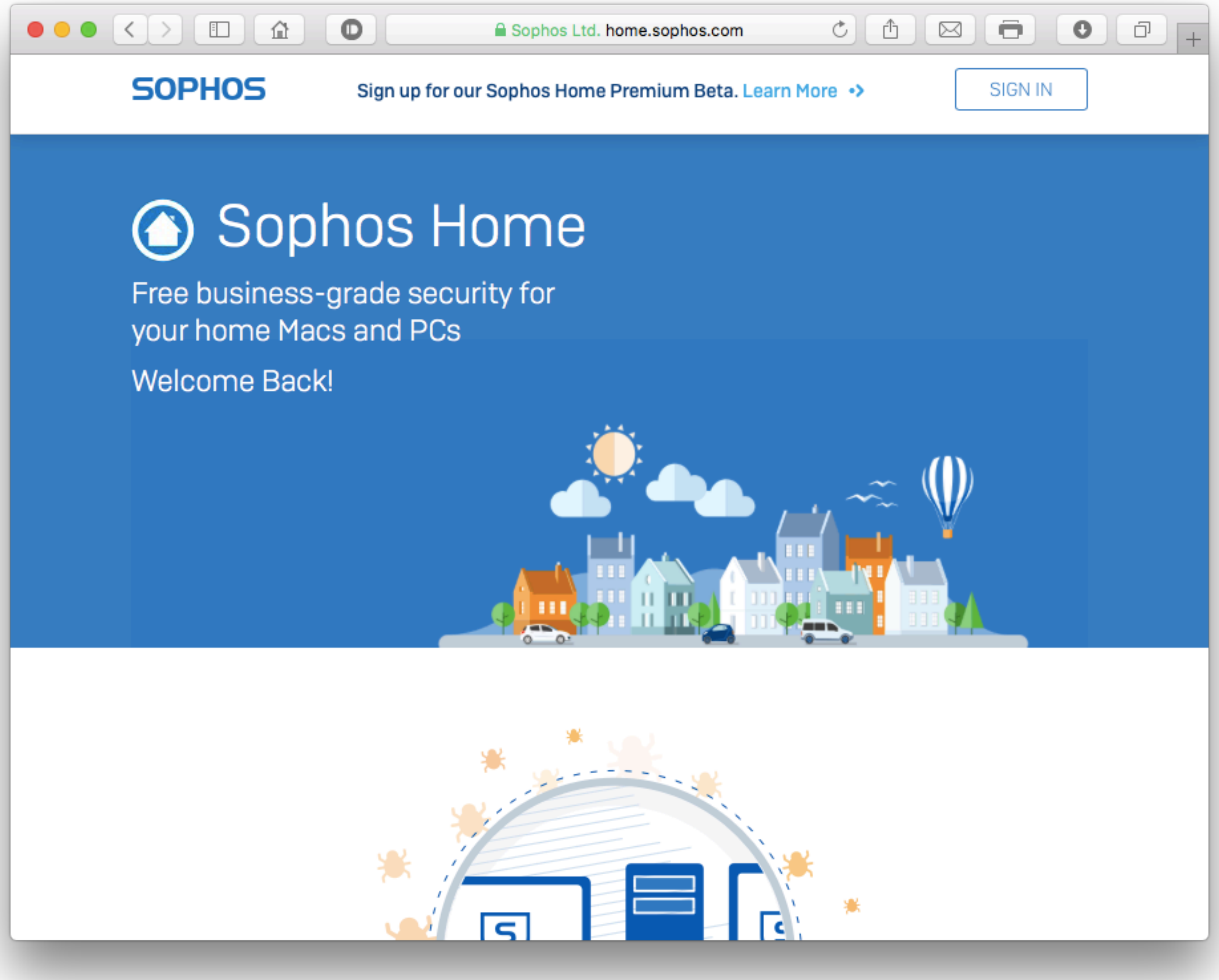
5. Install tools



MALWAREBYTES ANTI-MALWARE FOR MAC

CRUSHES MALWARE

Removes adware and malware. And it's free.



Sign up for our Sophos Home Premium Beta. Learn More

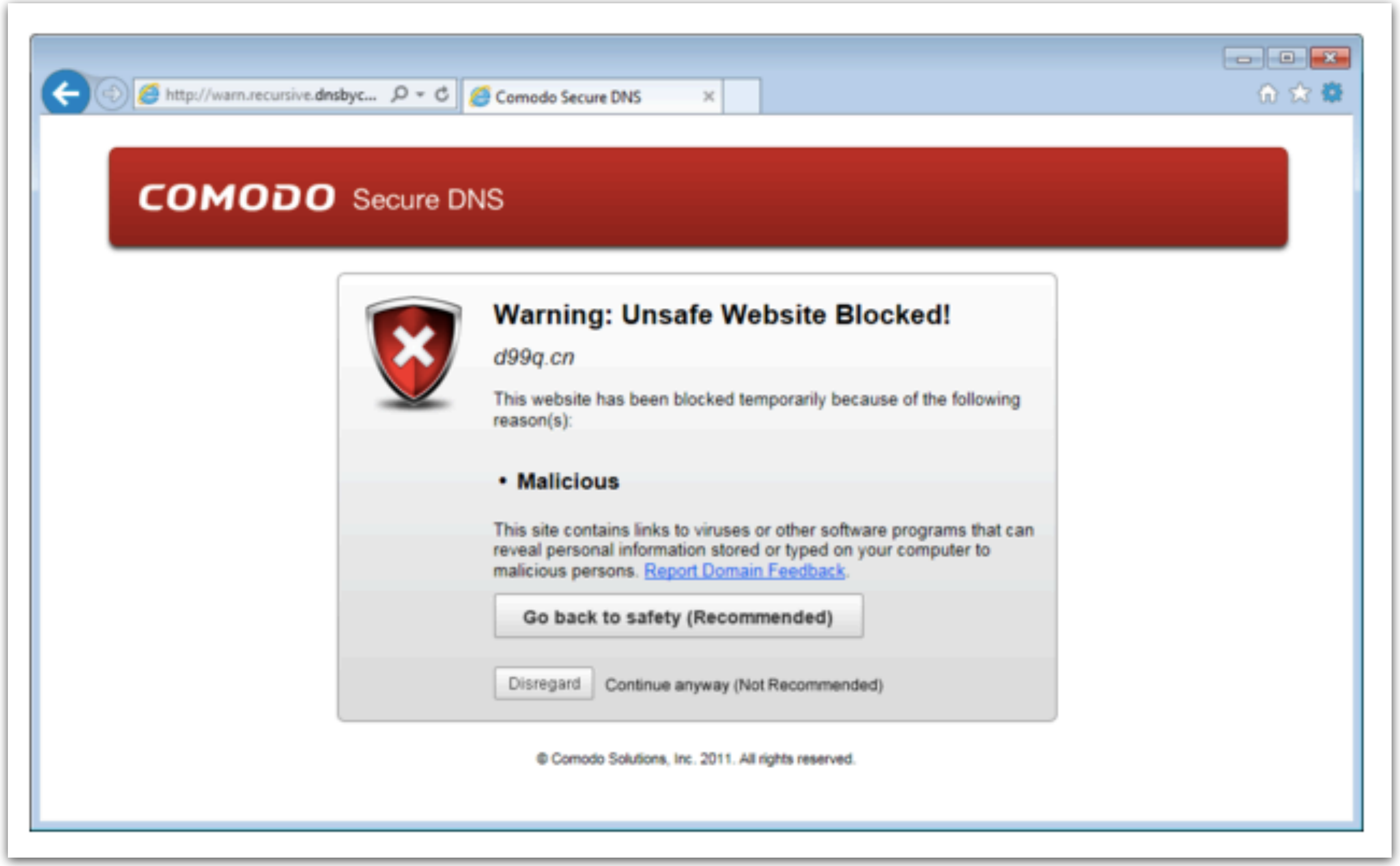
Sophos Home

Free business-grade security for your home Macs and PCs

Welcome Back!

https://www.malwarebytes.com/
https://www.malwarebytes.com/mobile (for Android)
https://www.sophos.com/en-us/products/free-tools.aspx

6. Filter your traffic



COMODO Secure DNS

Warning: Unsafe Website Blocked!

d99q.cn

This website has been blocked temporarily because of the following reason(s):

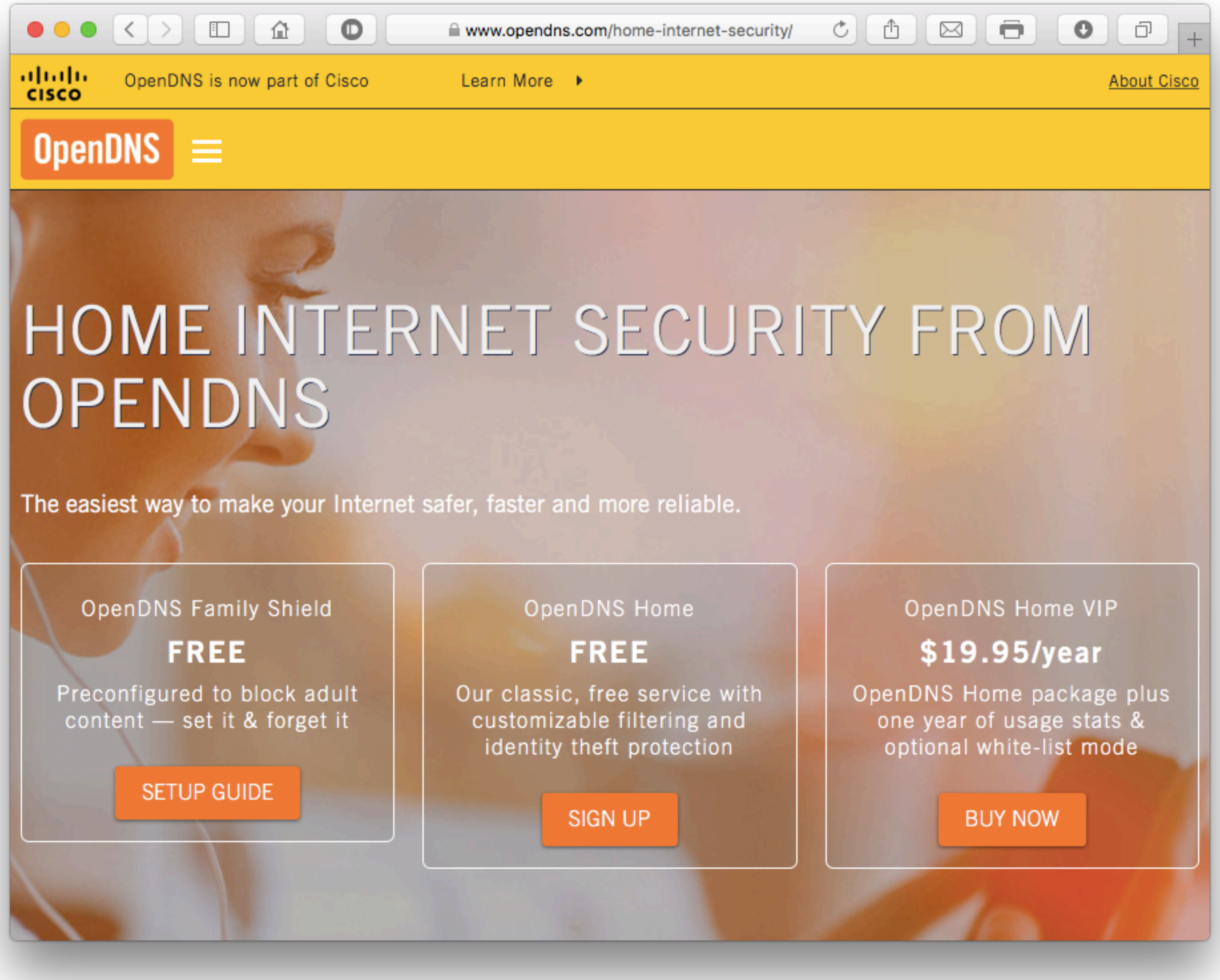
- **Malicious**

This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons. Report Domain Feedback.

Go back to safety (Recommended)

Disregard Continue anyway (Not Recommended)

© Comodo Solutions, Inc. 2011. All rights reserved.



www.opendns.com/home-internet-security/
CISCO
OpenDNS is now part of Cisco
Learn More
About Cisco
OpenDNS

HOME INTERNET SECURITY FROM OPENDNS

The easiest way to make your Internet safer, faster and more reliable.

OpenDNS Family Shield
FREE
Preconfigured to block adult content — set it & forget it
SETUP GUIDE

OpenDNS Home
FREE
Our classic, free service with customizable filtering and identity theft protection
SIGN UP

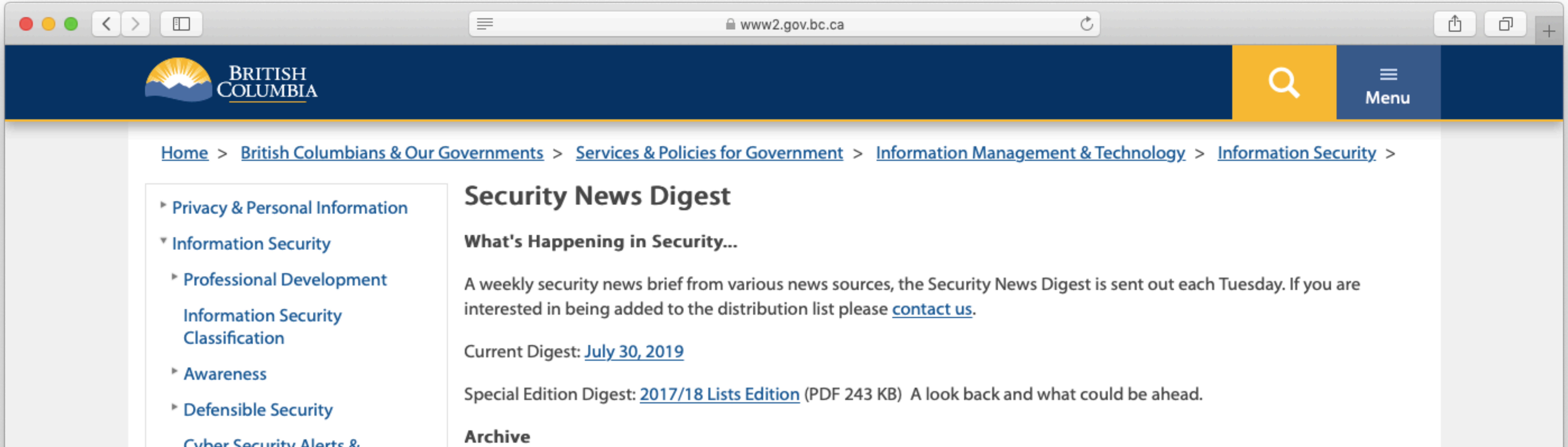
OpenDNS Home VIP
$19.95/year
OpenDNS Home package plus one year of usage stats & optional white-list mode
BUY NOW

https://goo.gl/NhfVYI

7. Stay up to date

https://www.globalsign.com/en/blog/top-10-cybersecurity-blogs/

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest



Home > British Columbians & Our Governments > Services & Policies for Government > Information Management & Technology > Information Security >

- Privacy & Personal Information
- Information Security
  - Professional Development
  - Information Security Classification
  - Awareness
  - Defensible Security
  - Cyber Security Alerts &

Security News Digest

What's Happening in Security...

A weekly security news brief from various news sources, the Security News Digest is sent out each Tuesday. If you are interested in being added to the distribution list please contact us.

Current Digest: July 30, 2019

Special Edition Digest: 2017/18 Lists Edition (PDF 243 KB) A look back and what could be ahead.

Archive

thank you

Questions?