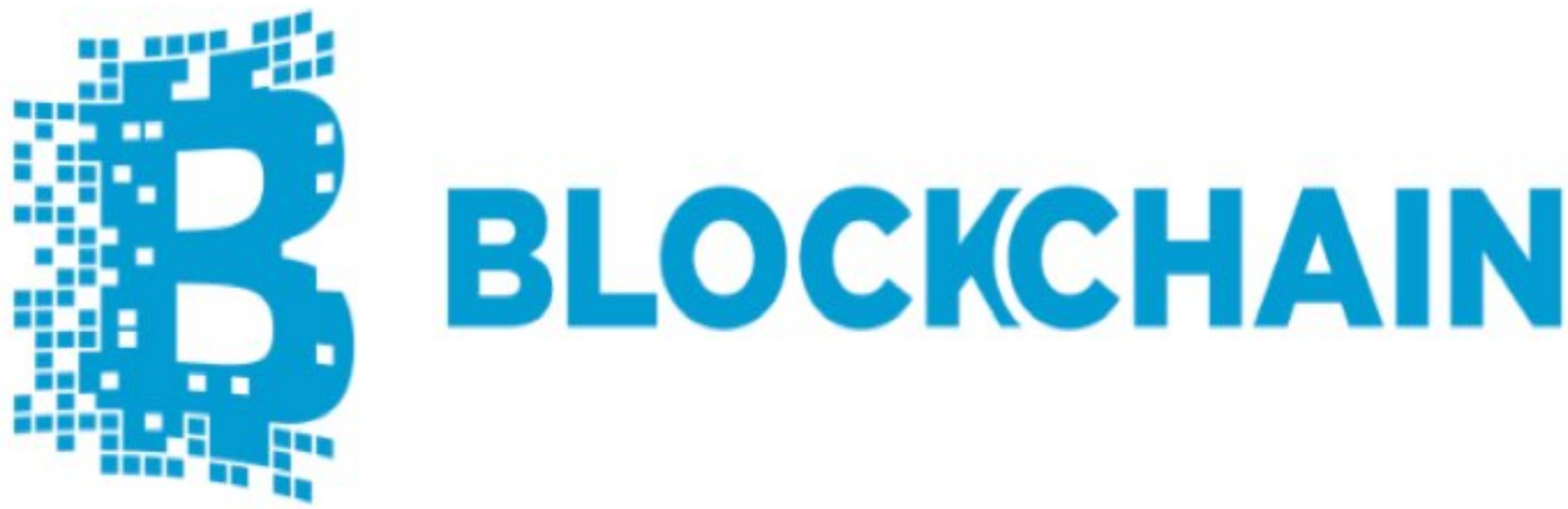



# Bitcoin's Central Nervous System

*"The Blockchain technology will fundamentally transform the institutions our societies are built upon. Because the Blockchain technology powers the digital currency Bitcoin, it will not only affect how business is being made, but also our legal systems. Ultimately, the effect of the Blockchain technology will be much more far reaching; it will also transform governance, healthcare, education, and various other pillars of our societies."*

BLOCKCHAIN

TechCrunch.com

"The "blockchain" — the engine on which Bitcoin is built — is a new kind of distributed consensus system that allows transactions, or other data, to be securely stored and verified without any centralized authority at all."

– Jon Evans

BBC.com

"With blockchain technology, you could create a truly tamper-proof record system… records can go into the Blockchain in a way that I know if anybody tries to change it."

– Peter Kirby

Bloomberg.com

"You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990's."

– Blythe Masters

BLOCKCHAIN

## Forbes.com

"Both the financial services and Bitcoin communities perked up last week when Citi, Nasdaq, Visa and other large financial institutions invested in Chain.com, a Bitcoin blockchain services provider."

– Laura Shin

## Telegraph.co.uk

"Bitcoin is giving banks a run for their money. Now the same technology threatens to eradicate social networks, stock markets, even national governments."

– Matthew Sparkes

BLOCKCHAIN

# Overview of Bitcoin (BTC)

Big Ideas Forum: 2016-10-10

BLOCKCHAIN

# Bitcoin: Overview

## What is Bitcoin?

Bitcoin is a consensus network that enables a new payment system and a completely digital money.

## Who created Bitcoin?

The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto

## Who controls the Bitcoin network?

Nobody owns the Bitcoin network much like no one owns the technology behind email. Bitcoin is controlled by all Bitcoin users around the world.

## How does Bitcoin work?

The Bitcoin network is sharing a public ledger called the "block chain"

## Is Bitcoin really used by people?

YES!  But it's adoption has —by some estimation— leveled out (and many Bitcoin alternatives are emerging). Blockchain is the more important invention here.

BLOCKCHAIN

# Send me Bitcoin!


1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu

A bitcoin address is public (like your email address), so anyone can send money to it.

BLOCKCHAIN

# Given the guy's bitcoin address, how much BTC did he collect?

## Psuedo Anonymous – Who is he?

Blockchain — Home Charts Stats Markets Developers Wallet Search

**Bitcoin Address** Addresses are identifiers which you use to send bitcoins to another person.

| Summary | |
|---|---|
| Address | 1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu |
| Hash 160 | b7546de774a35b56b7ce668a4a96c5ab8a4b8614 |
| Tools | Taint Analysis - Related Tags - Unspent Outputs |

| Transactions | | |
|---|---|---|
| No. Transactions | 120 | |
| Total Received | 23.00532488 BTC | |
| Final Balance | 11.88022488 BTC | |

Request Payment | Donation Button

**Transactions** (Newest First) — Filter

4cf3d96a661daa9e33bc57a3aaefaa1dcefd40915df4001f0ea31bde6e93f8fb (Fee: 0.0001 BTC - Size: 1980 bytes) 2013-12-04 04:47:27

1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (5.30267557 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (4.69722443 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (5.80470682 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (0.25 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (0.1337 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (4.19529318 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (0.25 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (0.5 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (1 BTC - Output)
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu (0.1 BTC - Output)

| | |
|---|---|
| 1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu | 11.1085 BTC |
| 15nqQGfkgoxrBnsshD6vCuMWuz71MK51Ug | 0.05 BTC |
| 14PCvBG5YtNPc2ZqShUoNBwmMKhdzSicNS | 0.025 BTC |
| 1GnAgbY2cPv5qNyyBQwfKWHNGKYJPmZD6L | 0.05 BTC |
| 1M72Sfpbz1BPpX... (Seans Outpost) | 11 BTC |

98 Confirmations | -11.1251 BTC

1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu

Answer: > 23 BTC

Valuation (at that time) > $23,000 ($14,000@$614 today)

BLOCKCHAIN

# How do you use Bitcoin?

Get a bitcoin wallet (and app), then add some bitcoin to it.




Bitcoin address is like your Gmail address. Public, anyone can send to.

Your wallet maintains your private key. Keep it secure!!

# Who do you trust?

Your keys secure your bitcoin wallet
Do you trust a 3rd party with your keys? (easier)
Or do you want to keep your keys yourself (harder)

## Wallet Providers

coinbase

- Coinbase stores your private keys

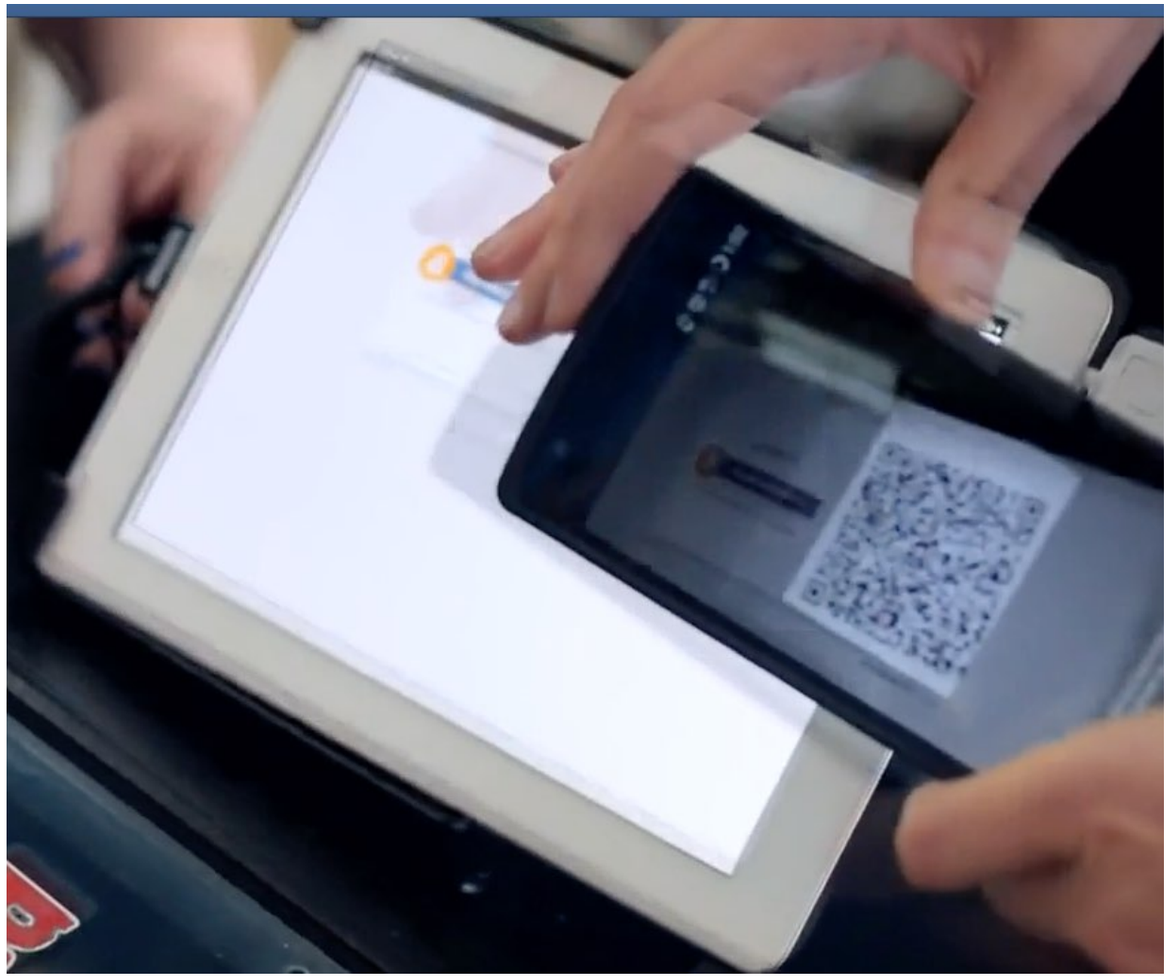
BLOCKCHAIN

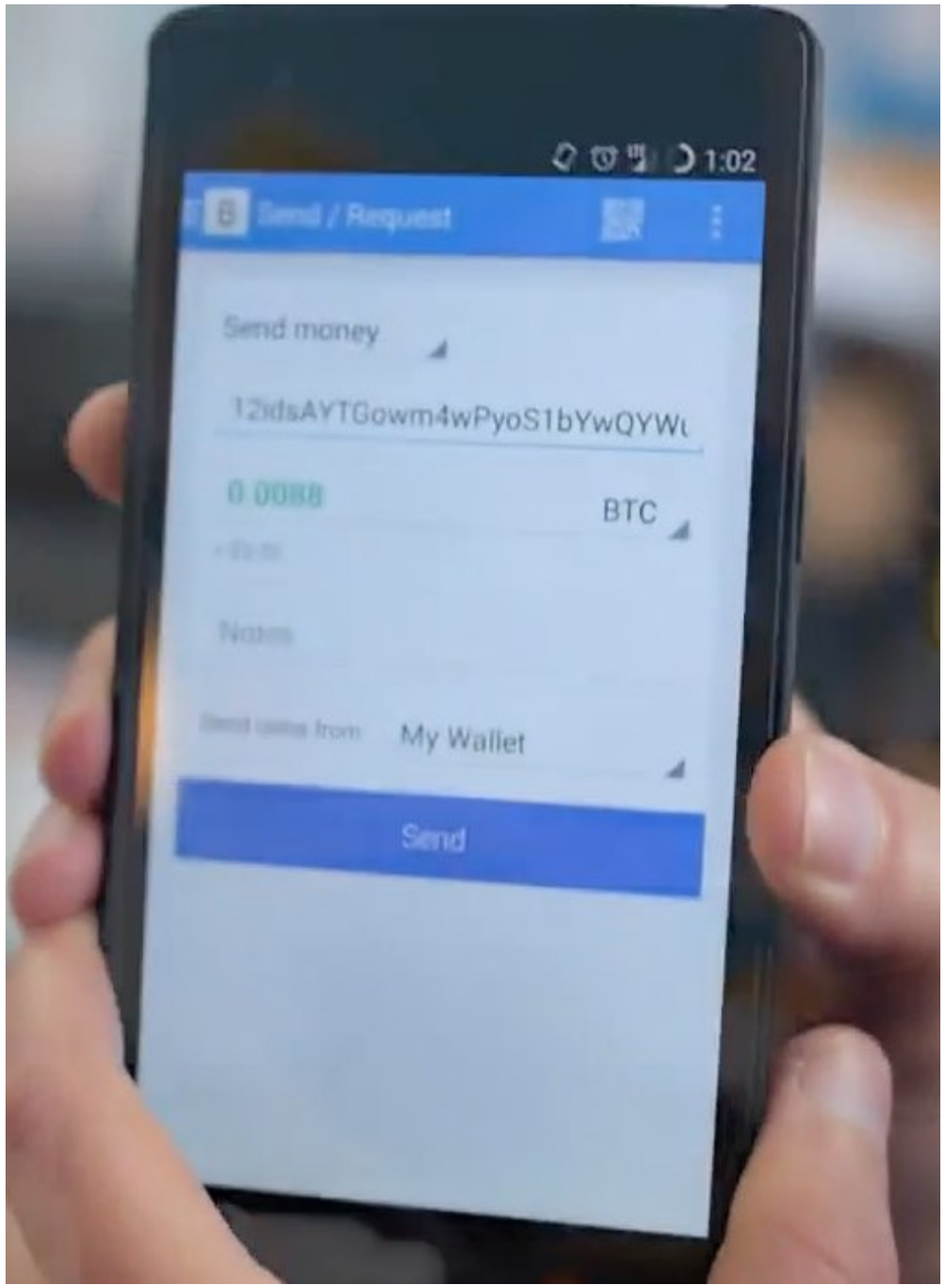
- Give tools for you to hold private keys

Wallet providers generate bitcoin addresses

BLOCKCHAIN

# Paying with Bitcoin






Wallet app on phone scans merchant's bitcoin address (and purchase amount) from POS terminal.

Click Send to pay!

BLOCKCHAIN

# Our Expectations Must Change

## As things are currently defined

## Accountability

Bitcoin lacks accountability against fraud since it's decentralized. Just because you pay someone doesn't mean that someone has to keep their end of the bargain.

## Bitcoin functions like cash

No option for charge-back (as done by the bank): the Receiver would need to reverse the transaction for you to get your $ back

...

BLOCKCHAIN

# Bitcoin Risks and Issues

## The Risks

- **Cash vs. Credit Cards**
  Change in consumer expectations: rights, responsibilities
- **Not insured**
  No FDIC. BTC could get lost, just like cash. No recourse.
- **Law Enforcement**
  Banks report movement of large $$$.  BTC is anonymous (somewhat)
- **Regulation**
  Bitcoin blockchain bypasses regulation completely

## Solutions?

- Add “hooks” to facilitate auditing, trade investigations
- **lots** of ongoing activity in the regulatory space to address these issues

BLOCKCHAIN

# What is the blockchain?

## Short Answer

*"The blockchain is often described as **distributed digital ledger.**"*

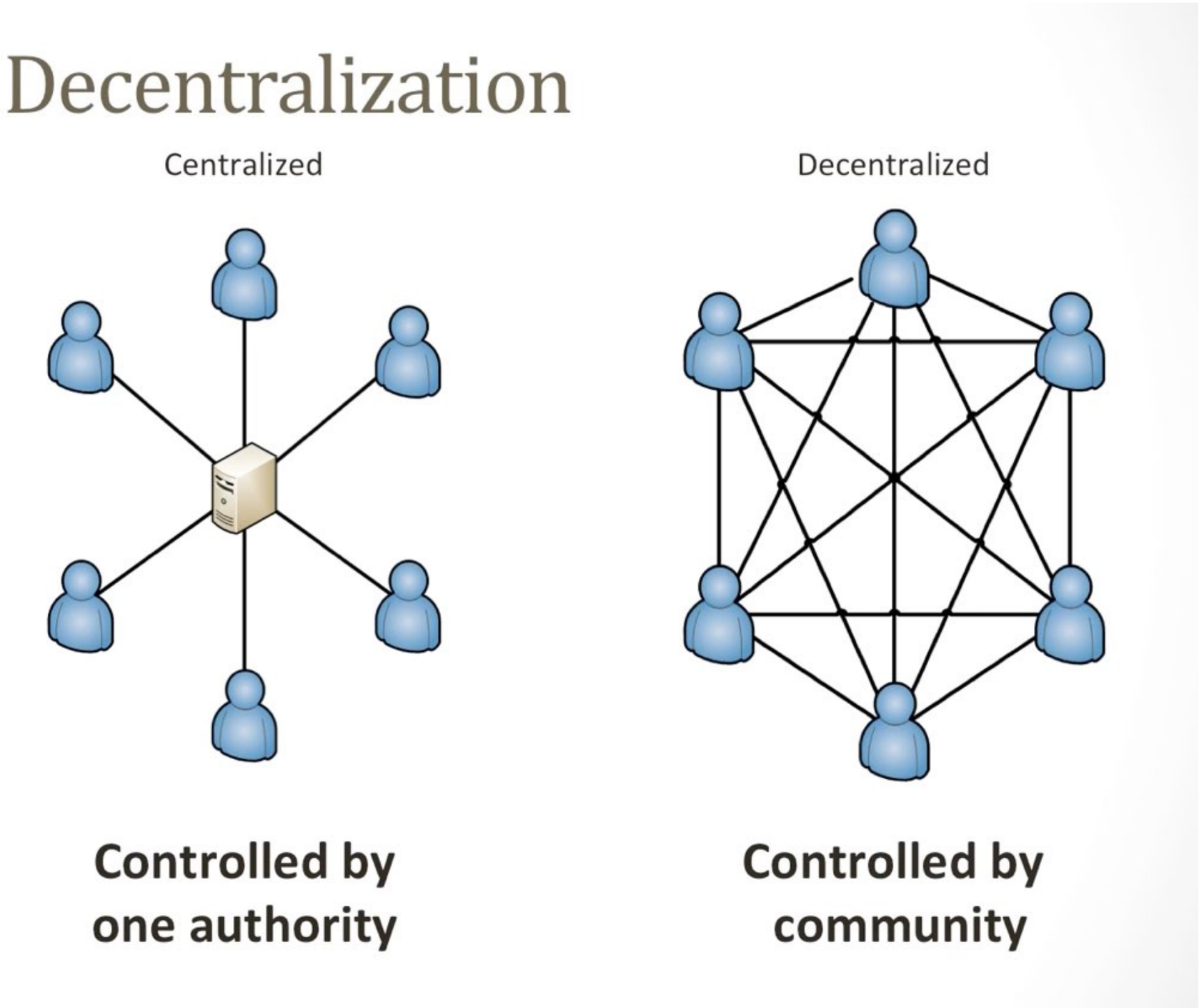
## Long Answer

*"The blockchain is a distributed database that provides an unalterable, **(semi-)public record** of digital transactions. Each block aggregates a **timestamped batch of transactions** to be included in the ledger – or rather, in the blockchain. Each block is identified by a **cryptographic signature**. These blocks are all back-linked; that is, they refer to the signature of the previous block in the chain, and that chain can be traced all the way back to the very first block created. As such, the blockchain contains an **un-editable record of all the transactions made**."*

BLOCKCHAIN

# The Big Innovation

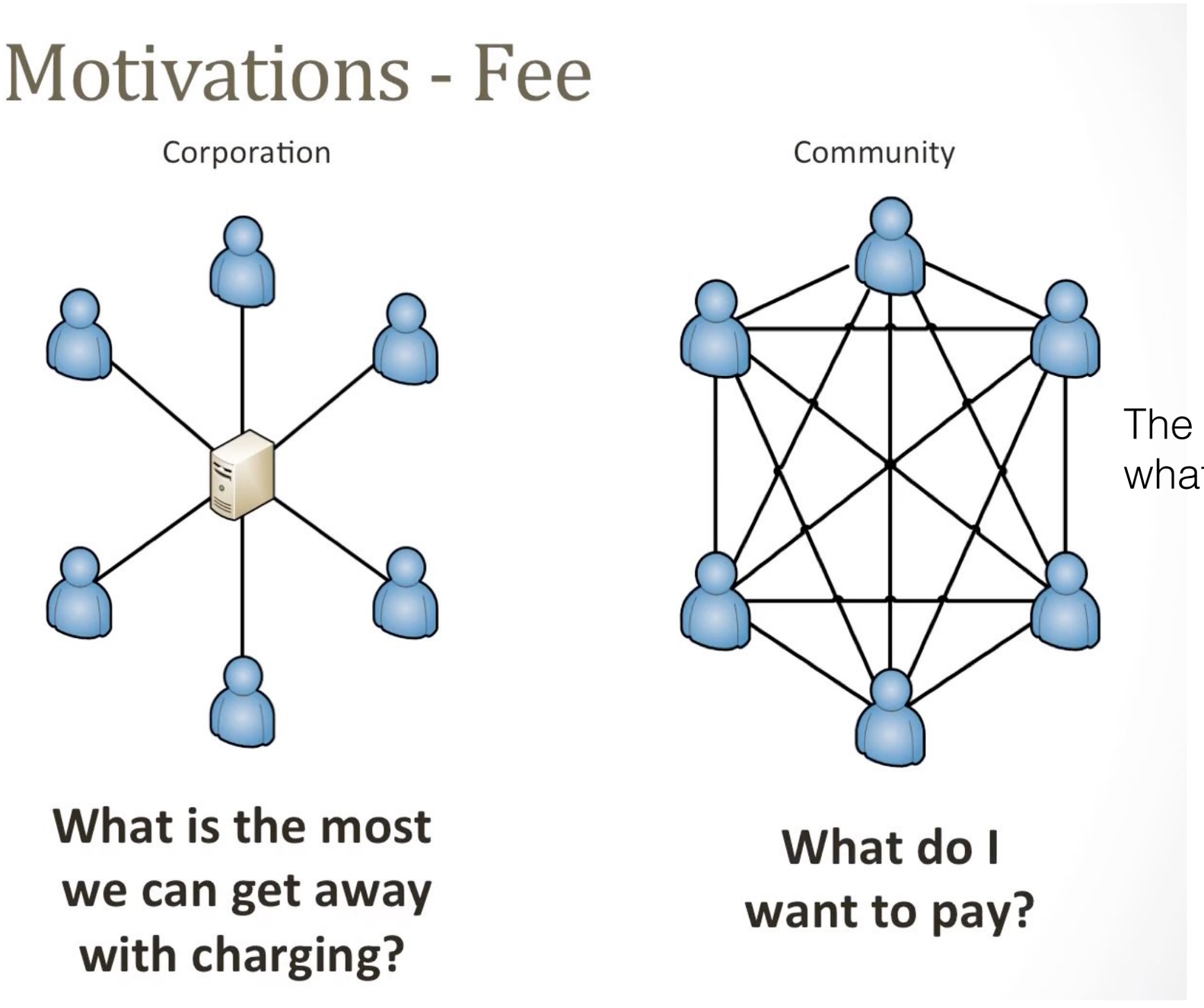
## A Shift from Centralized to Decentralized



BLOCKCHAIN

# Where (and how) Fees are Collected

## Changes in the decentralized model




The network can decide what something is worth

# Blockchain is one of these

## With copies distributed throughout the network

## A Ledger

- Transactions in/out
- Date Stamped
- Current balance

**ACCOUNT: Cash**

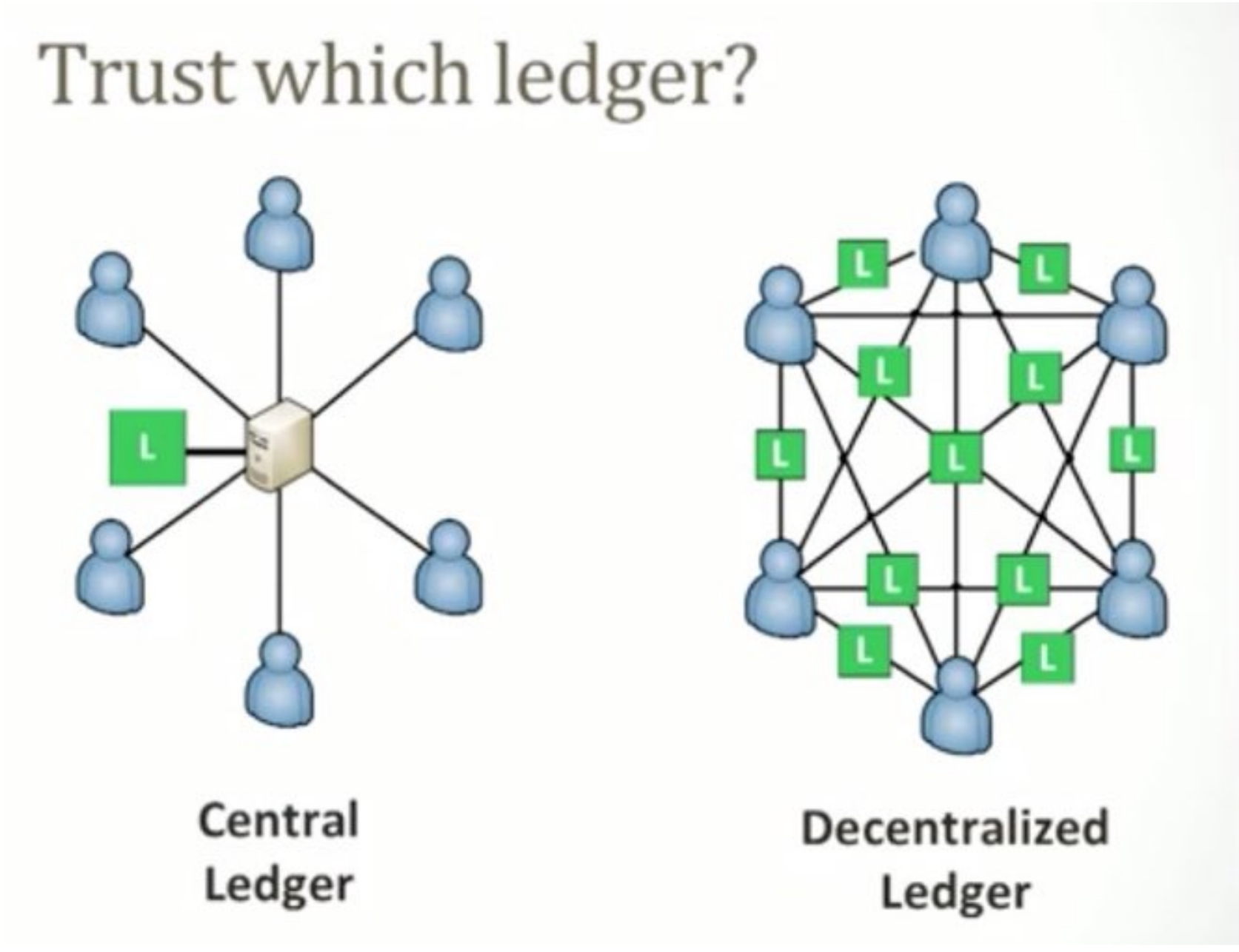
| Date | Description | Increase | Decrease | Balance |
|---|---|---|---|---|
| Jan. 1, 20X3 | Balance forward | | | $ 50,000 |
| Jan. 2, 20X3 | Collected receivable | $ 10,000 | | 60,000 |
| Jan. 3, 20X3 | Cash sale | 5,000 | | 65,000 |
| Jan. 5, 20X3 | Paid rent | | $ 7,000 | 58,000 |
| Jan. 7, 20X3 | Paid salary | | 3,000 | 55,000 |
| Jan. 8, 20X3 | Cash sale | 4,000 | | 59,000 |
| Jan. 8, 20X3 | Paid bills | | 2,000 | 57,000 |
| Jan. 10, 20X3 | Paid tax | | 1,000 | 56,000 |
| Jan. 12, 20X3 | Collected receivable | 7,000 | | 63,000 |

No single authority to “fudge the books”

BLOCKCHAIN

# Who do you trust more?

## One entity?  Or the consensus of hundreds?

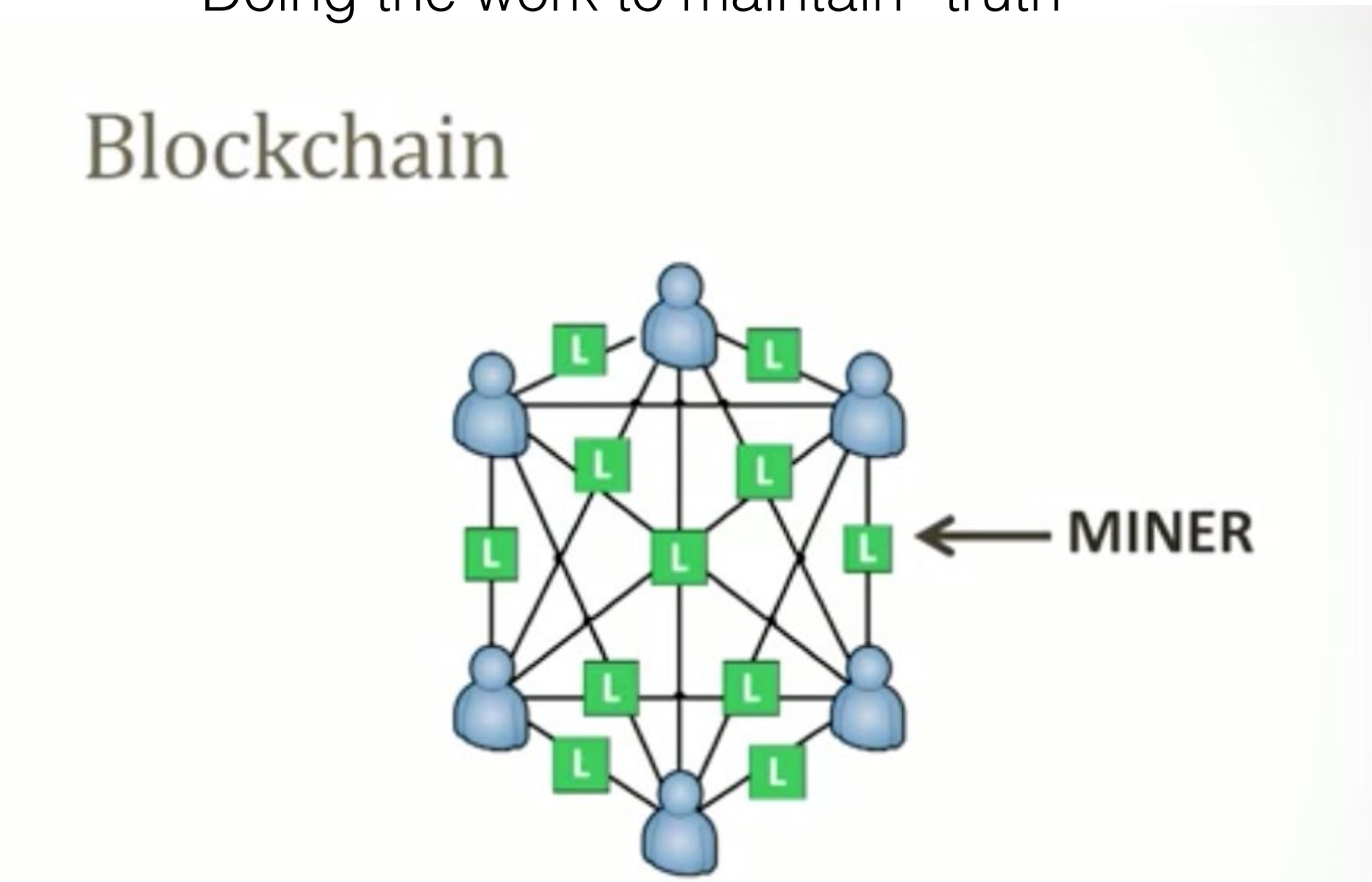



A distributed ledger is more difficult to attack.
By design, it's a self-healing network.

BLOCKCHAIN

# Blockchain Miners

## Doing the work to maintain “truth”

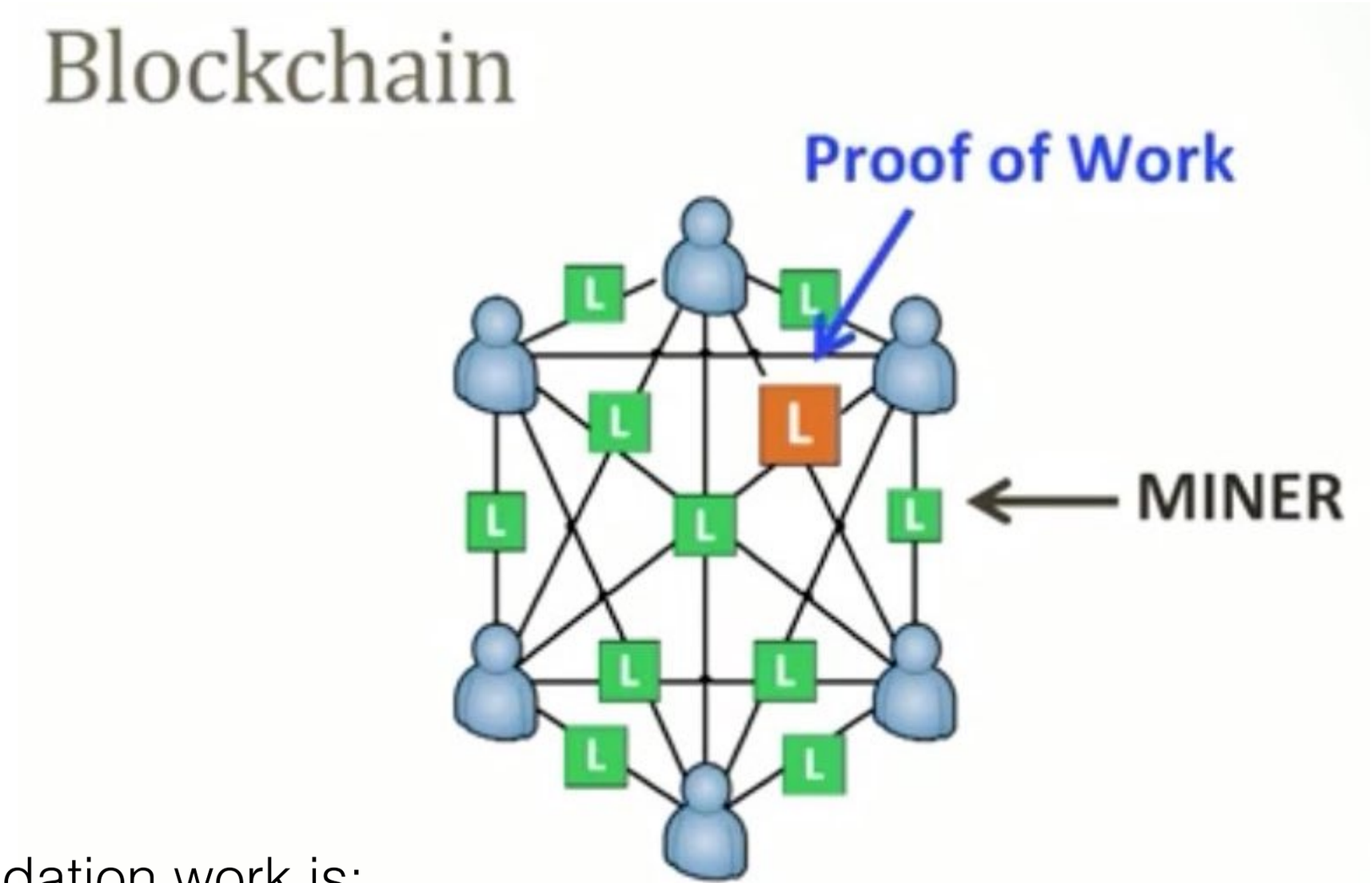



Thousands of “miners” in the network.
Each miner hold a copy of the current ledger.
Miners perform the ledger update/validation processing.

BLOCKCHAIN

# New transactions birth a new block

## Miners compete to “prove” the validity of new transactions.



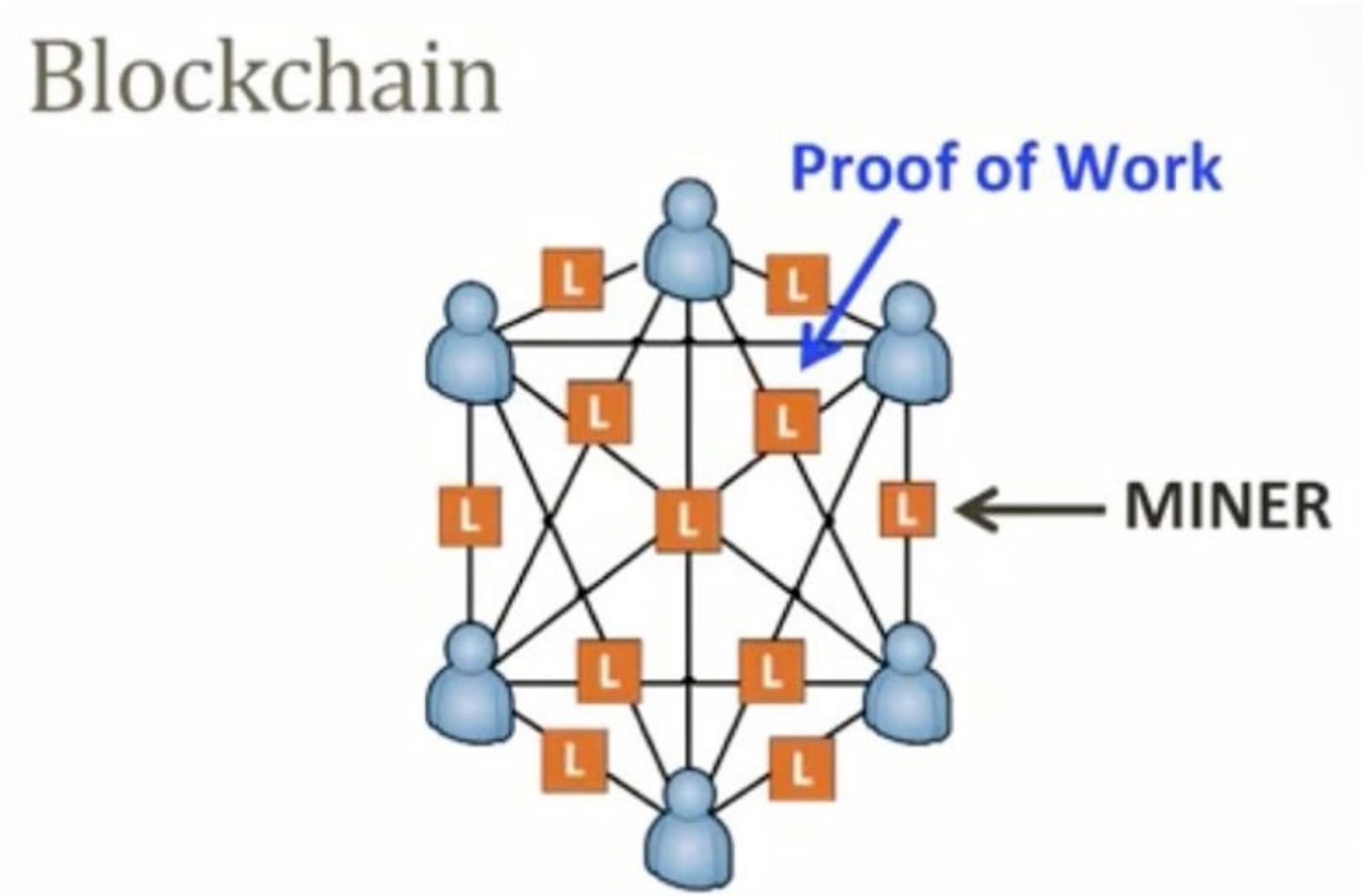

Validation work is:

- Energy intensive
- Easy to verify

First miner to solve the problem adds the new block to his ledger then broadcasts the new block L to the network.

# Consensus Achieved

## Everyone accepts the new “truth”




Other miners verify the work then update their ledgers to add the new block. The new block is thus propagated throughout the network.

BLOCKCHAIN

# Blockchain Features

• A blockchain is **digitally distributed** across a number of computers in almost real-time: the blockchain is decentralized, and a copy of the **entire record is available to all users** and participants of a **peer-to-peer** network. This eliminates the need for **central authorities**, such as banks, as well as trusted intermediaries, such as brokerage firms.

• A blockchain uses **many participants** in the network to reach **consensus**: the participants use their computers to authenticate and verify each new block – for example, to ensure that the same transaction does not occur more than once. New blocks are only adopted by the network once a **majority** of its participants agree that they are valid.

• A blockchain uses **cryptography and digital signatures to prove identity**: transactions can be traced back to cryptographic identities, which are **theoretically anonymous**, but can be tied back to real- life identities with some reverse engineering.

• A blockchain has mechanisms to make it **hard (but not impossible) to change historical records**: even though all data can be read and new data can be written, data that exists earlier in a blockchain cannot in theory be altered except where the rules embedded within the protocol allow such changes – for instance, by requiring more than 50 per cent of the network to agree on a change.

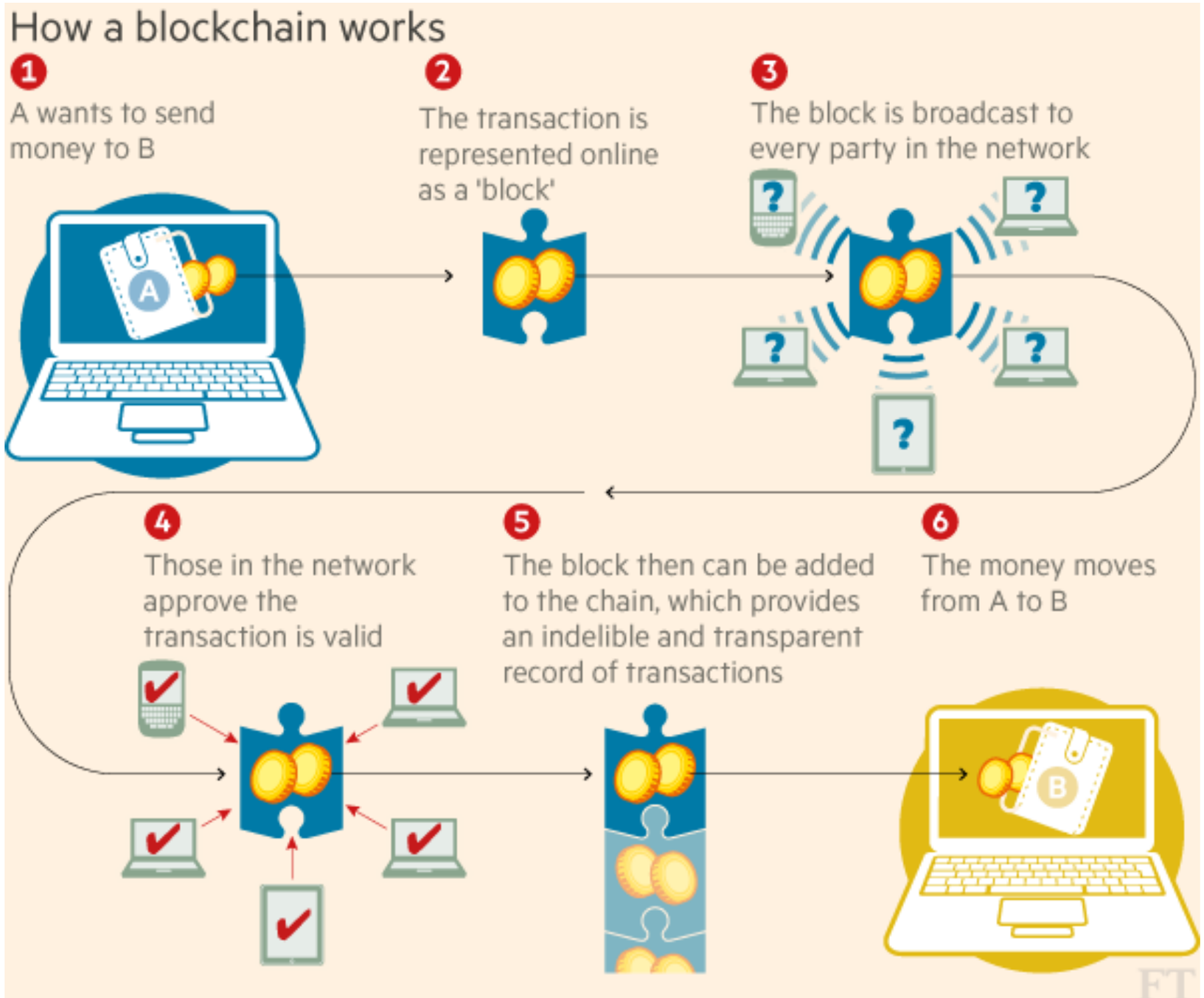
• A blockchain is **time-stamped**: transactions on the blockchain are time-stamped, making it useful for tracking and verifying information.

• A blockchain is **programmable**: instructions embedded within blocks, such as “if” this “then” do that “else” do this, allow transactions or other actions to be carried out only if certain conditions are met, and can be accompanied by additional digital data (e.g. smart contracts)

BLOCKCHAIN

# Making a Purchase

## How the blockchain updates



# How it works

## LOTS of complicated math!!

$M_{N,b,n}(X,Y)$

$N_0' := b-(N_0^{-1} \bmod b)$;
$c := 0$;
**for** $k \leftarrow 0$ **to** $n-1$ **do**
  $c := c+\sum_{0 \le i < k}(X_i \times Y_{k-i}+Q_i \times N_{k-i})$;
  $c := c + X_k \times Y_0$;
  $Q_k := c \times N_0' \bmod b$;
  $c := c + Q_k \times N_0$;
  $c := c/b$;
**for** $k \leftarrow 0$ **to** $n-1$ **do**
  $c := c+\sum_{k < i \le n}(X_i \times Y_{n+k-i}+Q_i \times N_{n+k-i})$;
  $R_k := c \bmod b$;
  $c := \lfloor c/b \rfloor$;
$R_n := c$;
**if** $R \ge N$ **then**
  $R := R-N$;
**return** $R$;

Blockchain miners are working to validate thousands of new transactions every ~10 minutes by solving a difficult math puzzle.

The miner who solves the puzzle first is awarded new Bitcoin as reward.

Blockchain.info estimates that Bitcoin miners are now trying 450 thousand trillion solutions per second to solve these puzzles.

BLOCKCHAIN

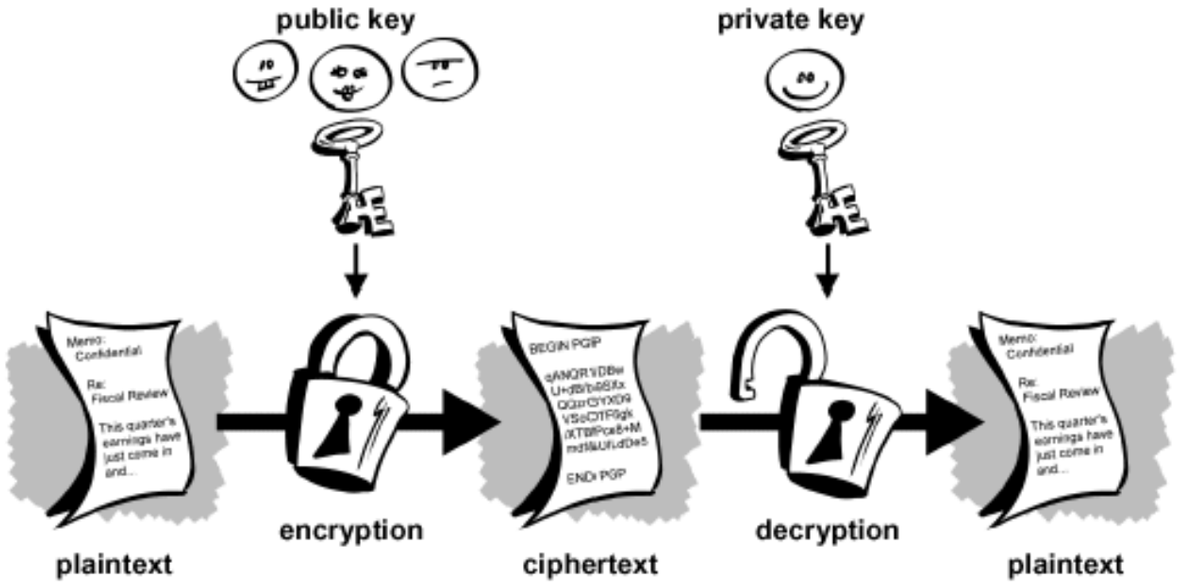
# What ensures the privacy of data?
## Public Key Cryptography

- **Transactions** on the blockchain are **signed digitally**, using public key cryptography.
- Public key cryptography uses **two keys**, which makes it harder to crack.
- There is a **public and private key** – related mathematically but because of the complexity of that math, nearly impossible (or at least computationally infeasible) to guess.
- The **public key** can be used to **sign and encrypt** a message that's being sent; the recipient – and only the designated recipient – can decrypt that transaction with their private key.
- In addition to encrypting messages, public key cryptography can be used to **authenticate** an identity as well as to verify that the message – or in the case of a transaction on the blockchain – **has not been altered**.)

BLOCKCHAIN

# Public Key Cryptography

## Why information on the blockchain is secure




Keys are huge strings of random characters.
Public keys available via online registries.

audreywatters's public key

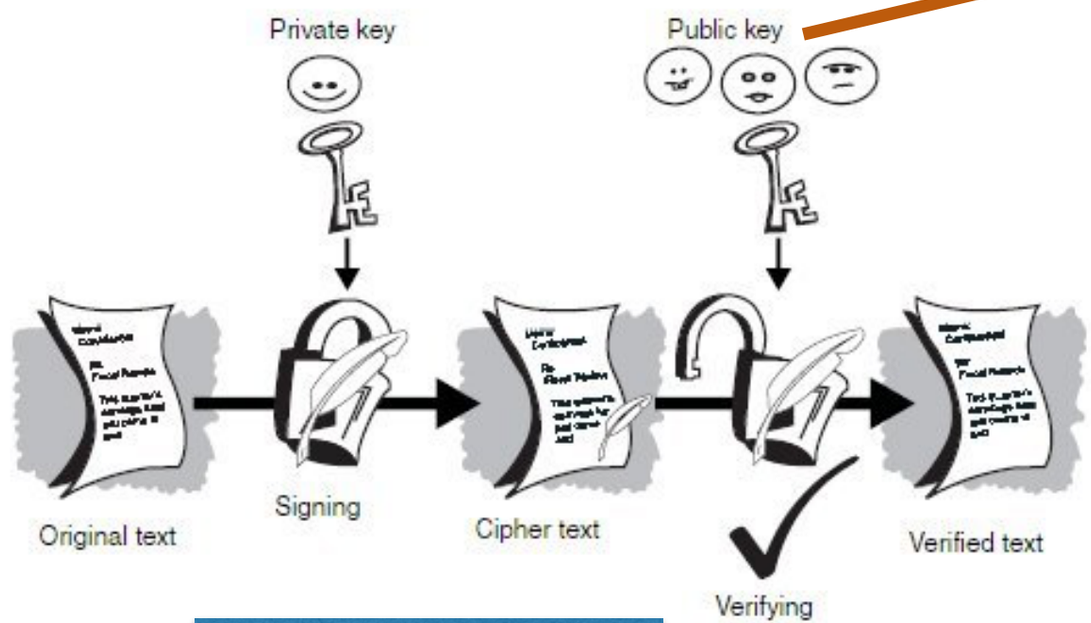
fingerprint: 6B8B 1DAF 0C36 9EA2 73D6 39C2 C757 9389 4FFA 4436
64-bit: C757 9389 4FFA 4436
curl/raw: keybase.io/audreywatters/key.asc

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Keybase OpenPGP v2.0.8
Comment: https://keybase.io/crypto

xsFNBFUTN4wBEACog/pyr+uHv9HgCO6VKzn0KuAkWps5068+iI3ZtIXDTbAkL9Al
acWIW+IFZq0r9KhoElTSTWeAaiVQk/L6Fnt6DTmKeKx4I5kA2DHQvXsxdDLCavOg
ZcCU0seEj3iIA0+p40UWxsul6qf1n+RPa+PSFoQzAdF1+L+UPmsqHgeEOrChTABE
8KWXx0cOUpx5bfGKQY+MBo7QioSUlb3d+WCJKs3EHFyYdrMd97u13G5pqEOMi5ri
UMRvrqN7mc4wXjX1D0HMJ8j3e3jHSqw1G7K8IOmaGchVLywfDO1vsv2m2JpGrxj0
dIszhanIRAv+3DQzE2Myt/QTfWdoZftYUfkzlsqCPPSPMtlessgeb5rmoGGVyD0Z
vukEQAdImbM1zenO4jyg/Sxv94Zeeol2AfUV6LtnUkC4t5LCUdhIabNkkp2Da4wW
RMy6VavE1jIWGG+pA54Ra38stxl3rbSjPtIWX/4sY3bAC0fSdHLdNmJLMD6Q4WbT
6N4WbgdI1S9j/T+doxtcYYQrvY9PFGwNSr51YTvxjI27Mp3uWhjTysi9EecLtl94
rmjU2WpMyBTUK/K6jIE4wr4oTKEuDaE8xW/V5Pj1bpvaNs9i5xzbayaa1kbrdHu9
VH6Srn0zElZCqJi/DqF+UUj6cTfs2FjCtA3X5CGHporIYpcR6QF+ocUQLQARAQAB
zTNrZXliYXNlLmlvL2F1ZHJleXdhdHRlcnMgPGF1ZHJleXdhdHRlcnNAa2V5YmFz
ZS5pbz7CwXAEEwEKABoFAlUTN4wCGy8DCwkHAxUKCAIeAQIXgAIZAQAKCRDHV5OJ
T/pENm2/D/9E5cIwRSFpbMfbydkg/6RqLLKi8HE92sUlFc2DETFC9klDNn1RqVIB
DvcAnbSekyO+pfdK9Xw413WYZlPjOmhqs+2mPwK5QOt/eTjCwA863okqGqcrj2By
tloNGR66SPcWFfXJu2HQpCpq8o0yXG7GsRaMZJO/Gb+ej/i2YYDcerEw8rKG7s3w
PLAfzYiwk3me3mRUgkMVZYYO8NG22VF6Nj7BKXULmpvW26yf8nOx8Y7AWvra4Y9G
CoOVTQAFHMMSdmniwmglDqC01LqDfQ2RUyO+WK5wTwWCgsNGVh/JPpjGucEvnKzl
S1CDCFMRZL0ytAme6DU2wZIHiFlIIpCVvjcixlOipkIFhyOgf1rtmvdpit5e/eS/
ttzz4lieSHFnLpQpE12hOFXocc+W/8eGtUuihBcaUeJeYssl5JhSo/NWENxIZps1
fnTSZIyyL9cypZmF9+oFF8TzFiNYm+vVnXBqRzYkMcyDKyBkyszVOhQYNhEsyyYT
V6RnlXSxvRckHsLGC7stza0GugvkTP3iyEStb8kxqGdheFRu+9C2ll//JFuFQR3O
y5ULbcP/k1l54Dzyb1m7qqOKSCktJKQON0ELU7XmuVG4VQAGcbsUKitwFpRk/55T
9qfFQzEpL7KuxrEqXj23nN8UcECIgFuj8bpWU6jY+5kMVwpzoCYx9c7ATQRVEzeM
AQgA0IdPy9mcPeUv4W/vXKzyx0eJZyPe46NladCN76PwAFeRdpvOcHVePbCF+E0l
CQyXRwVhgdCIt+frgBh7kwvPXu6iK198LxY2LWwmT/jysPUbm0eCmHjgnSzoiin9
Hr8Twk67Sk1Mr0siIdhtFWJDJWT397DKLDSzJKoUa7C1osC5SsvJJHqO+lsz+ygG
0kusJKj1xdi88zll0CLsBR2d4o+z76D9DhGDjJjkDQFpniXucc1aKV6saS9ovaja
qxbKKkkamjsRZu0jJOxoGLKiZPsLZG7RV7LFbcLiOWb1UwB3DXZXyou0AqH/dcjJ
+NM3a5Wl32b9TNIGB2DQwULsBwARAQABwsKEBBgBCgAPBQJVEzeMBQkPCZwAAhsC
ASkJEMdXk4lP+kQ2wF0gBBkBCgAGBQJVEzeMAAoJEDkLDOui4WJdQxgH/0yGo9nK
s9V1EBvK+u2gyYOP6fTncU/bSM2L/E0yuIgBgdt6q8kXhuc78o1DtVk/8t5ghHR1
bgJKTIJ9kqJ8ifEv4lo4xf82SJKSUS/vot+ACAeQV2jmxwFGXEamEed0oGxY86p+
HiWMe6lF7r2OeGLPTtY/rtcTgaNZlWxflGJFBScSPp4XZRr0G8ZQ+SBofN7tYKo5
TQ9RdRlhuN0/Sn/G3Dp+TeJMbpE5Ogxv1Sxz8S3sLh3CbizlFp7hw6s9F/eKRclb
PstA/671n2s83OeV4IZw4/pTdPvqtbD4y065qDXZDRPerypZ1jCzP58s6+vzfH2c
bl/CmmhLv0uVolvdwRAApHKVvHy4hOA9VTbPMPgo0IwRFRq1kRsynSNADCSUVCYf
NHexLLWPFofz5GjaZktiSHfHiKOJ/4ApJU9F9sa3bmV9YCxTzp5Gfi1kXb1tChKP
Mga4ng/6Md8cE517TDKEjb+1LiiuQXq0ZvLiGWho8nZ2eQe4OiPlWoN6wjvVw7T
lGuXsHw28GqCxo54hTQMnyhblOrJtAY2gWhvBk3pSpg87XUfLMFJIT2FyrtuQ9+k
trjFtKALfmTuS8G09ONd49dEqxOu5YQF2ySTk2tJ7mEFJyzruLlEG188QN6xPV3g
AWVp9fnojLZJR2rsHOwCKz+BoHeFoNOoodGRqJGuyhv4Z8PUqtk4aioeBHLFX880
WeSIonK4l61wv731A5yVHvCJ/xy6687M3X+lWQJqDWUN4+FwUJvaFyf38uaJW8fF
vJXGJoemoyeKCiZllIoQOTTQOcNdbxFkcEW3UEDARGI95AGK/PivPqWBbbQeftcao
45j6loTjWpBSmCBsRuwVN86VLWvwFVk3wix5uFpAP6IGgH4wh5frSSeAMO+1/+0D
AUbaZVyjWLOwzquZrpZujwR5K/cL1Lh1ZnTiyoz96jjYEjdwECV+qT1CYWzS/RB7
```

Big Ideas Forum: 2016-10-10

Privacy



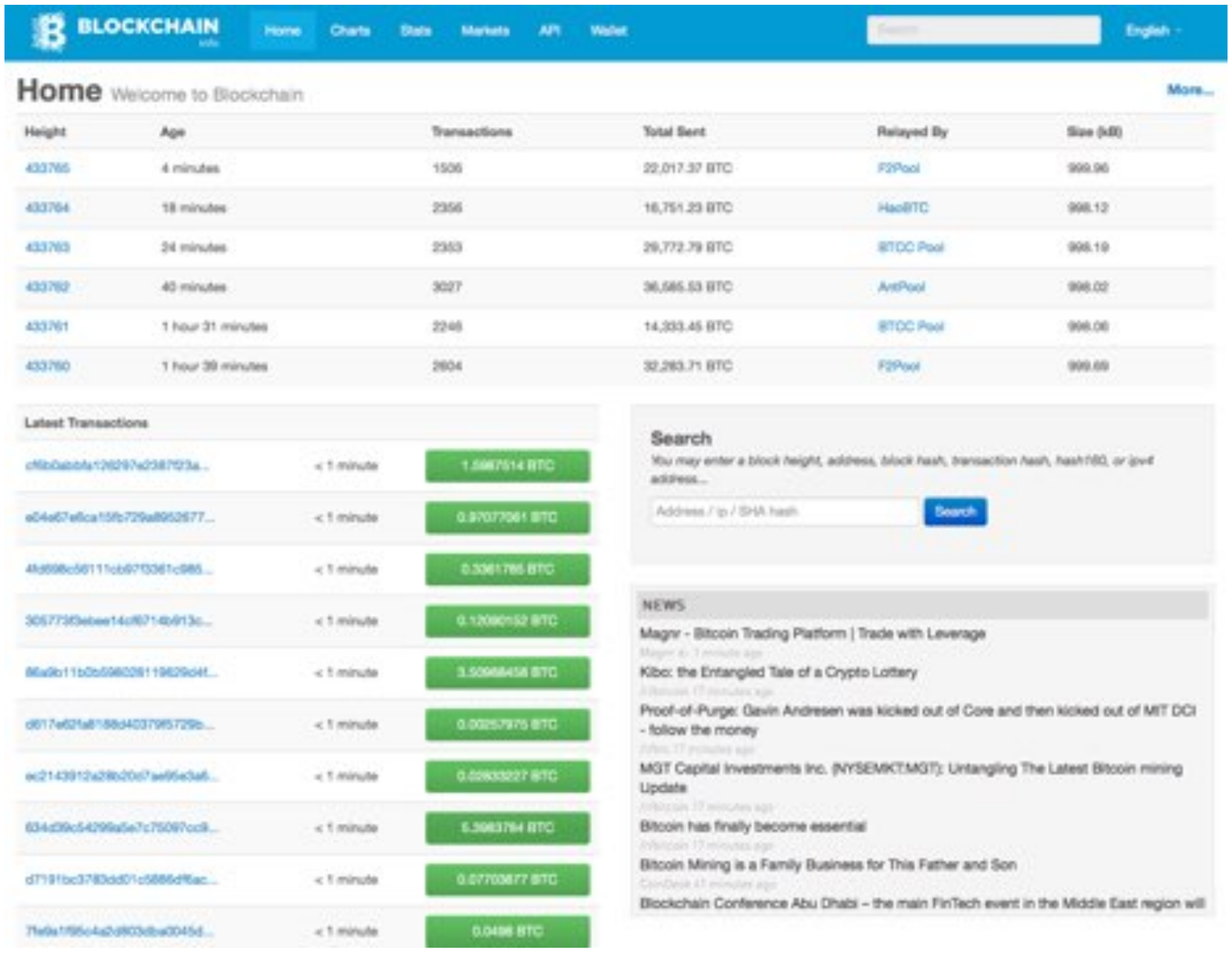

Digital Signature

BLOCKCHAIN

# Live Demo

## The blockchain in action

https://blockchain.info



BLOCKCHAIN

# Bitcoin 2.0

Working to extend blockchain into
all corners of the economy

Bitcoin brought us blockchain.

But Bitcoin is only one use of blockchain.

Where is it all going?

BLOCKCHAIN

# Blockchain Application Areas

- **Currency -** Bitcoin began as a P2P electronic cash system. Anyone can hold bitcoin and pay anyone without a middle man. Examples: Bitcoin, Litecoin.

- **Payment Infrastructure** - You can use Bitcoin to send money around the world. Merchants can accept bitcoin payments. This is slightly different than using bitcoin as a currency. Uses cases include merchant processing and remittances. Examples: BitPay, Abra.

- **File Storage -** Peer to Peer file sharing networks removes the need for centralized databases and heavy storage areas. e.g. IPFS (InterPlanetary File System)

- **Digital Assets -** The blockchain can be used to create digital assets such as stocks, bonds, land titles, and frequent flyer miles. These assets are created using protocols on top of the Bitcoin blockchain. Example protocols include Coloredcoins and Counterparty. Companies using this technology: Chain, NASDAQ, Openchain.

- **Identity Management** - Companies offer blockchain IDs that can be used to sign in to apps and web sites, digitally sign documents, etc. These 'profiles' are called Passcards, and are meant to soon replace usernames and passwords online. Companies: Onename, Keybase

- **Verifiable Data -** Create a verifiable record of any data, file, or business process on the blockchain. Examples: Tierion, Proof of Existence, Factom

- **Smart Contracts -** Software programs that live on the blockchain and execute without the possibility of third-party interference. Examples: Ethereum, RootStock.Onename allows users to create tamper-proof digital identities for themselves by being the "first comprehensive blockchain-based identity service."

BLOCKCHAIN

# Blockchain Examples

- Create a verifiable audit trail of insurance claims.
- Create an audit trail for healthcare processes and patient data.
- Ensuring drug safety - modum.io
- Track the purchasing approvals of goods and services in Salesforce.com
- Archive every Slack (a messaging service) communication, creating a verifiable record of your company's online conversations. Handy for regulated industries such as finance and healthcare.
- Enable people to buy and sell renewable energy to their neighbors
- Reward people for crowd-sourced project participation (e.g. FoldingCoin.com, micro-payments for protein-folding help)
- There are many many more...

BLOCKCHAIN

# Digital Assets / Smart Matter

## Representing real things as digital things

**Digital assets** are assets whose ownership is recorded digitally.

**Smart contracts** are programs that encode certain conditions and outcomes. When a transaction between 2 parties occurs, the program can verify if the product/service has been sent by the supplier. Only after verification is the sum transmitted to the suppliers account. By developing ready to use programs that function on predetermined conditions between the supplier and the client, smart programs ensure a secure escrow service in real time at near zero marginal cost. See https://www.ethereum.org

A **Smart Property** is a property that has access to the Block Chain, and can take actions based on the information published there.

E.g. A car whose ownership is represented by a digital asset in the Block Chain. The physical car is connected to the internet and can read the Block Chain. Therefore it can keep track of the status of the digital asset representing it.

BLOCKCHAIN

# Smart Contracts

Smart contracts are applications with a state stored in the blockchain. They can facilitate, verify, or enforce the negotiation or performance of a contract.

Examples:

- **Energy** market: TransActive Grid enable people to buy and sell renewable energy to their neighbors
- **Internet of Things**: Securing the allocation and management of device addresses on the blockchain; micro-payments for sensor data collection usage (tilepay.org)
- Releasing **music as a digital contract**: See Imogen Heap

BLOCKCHAIN

# Smart Contracts

MYCELIA

Imogen Heap http://myceliaformusic.org

"Whether we stream it through our smartphones or buy tracks from our laptops, technology has made music more accessible than ever before.

For consumers, this is good news. But for the music industry, it's a different story."

Our mission is:

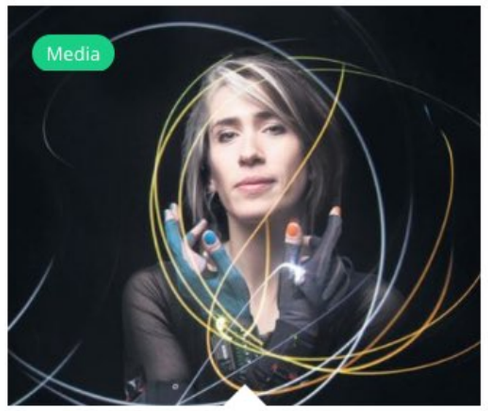
+ To empower a **fair, sustainable and vibrant** music industry ecosystem involving all online music interaction services,

+ To unlock the huge potential for creators and their music related metadata so an entirely new commercial **marketplace may flourish**,

+ To ensure all involved are **paid** and acknowledged fully.

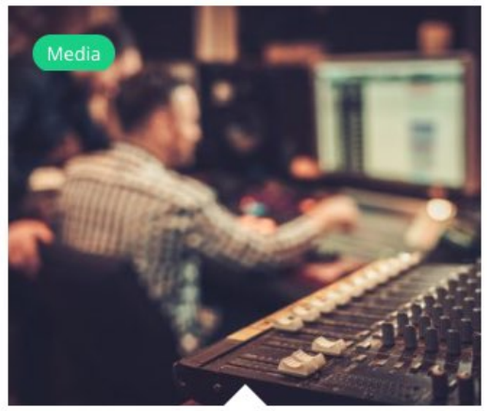
+ To see commercial, ethical and technical standards are set to exponentially **increase innovation** for the music services of the future,

+ To connect the dots with all those involved in this shift from our current **outdated music industry models**, exploring new technological solutions to enliven and positively impact the music ecosystem




HOW TO REVIVE THE MUSIC INDUSTRY, BLOCKCHAIN COULD BRING ABOUT A REVOLUTION

*10th July 2016*



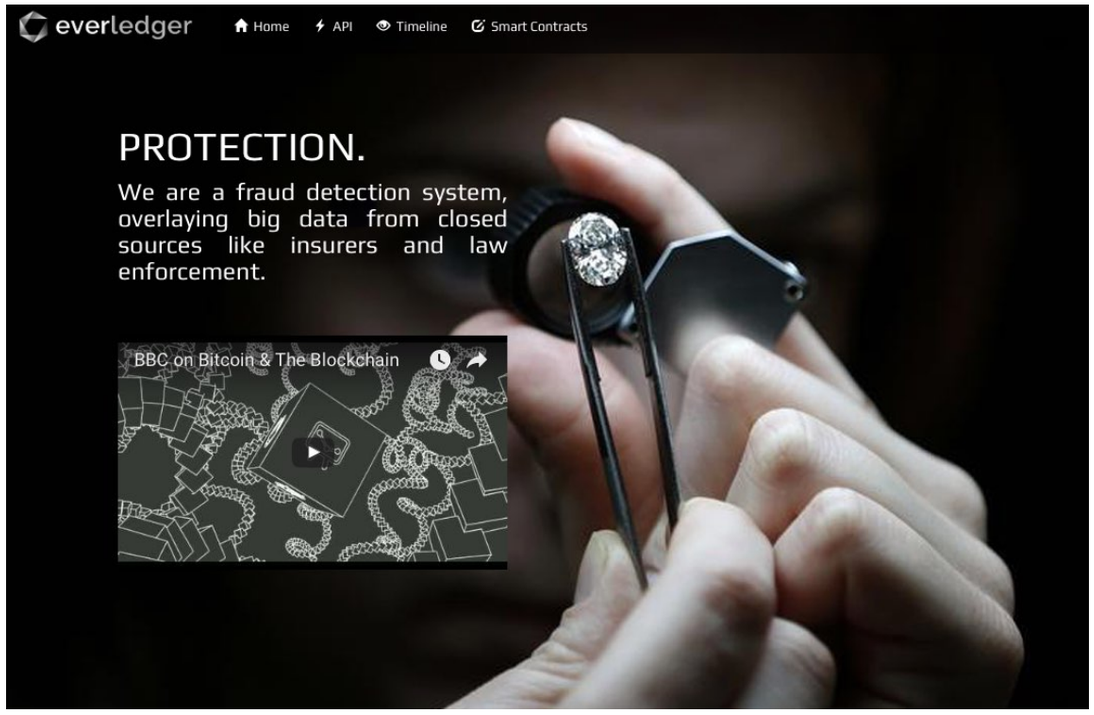

THE CONVERSATION : HOW BLOCKCHAIN COULD HELP MUSICIANS MAKE A LIVING FROM MUSIC

*7th July 2016*

http://myceliaformusic.org/2016/07/10/revive-music-industry-blockchain-bring-revolution/

BLOCKCHAIN

# Use Case: Diamonds




## The Problem

- Fraud:  Is it synthetic?
- Blood Diamond?
- Supply chain paperwork? (certificates, tracking)
- Recertification Attempts

## The Solution: Digital Provenance

- “DNA”of the stone tracked on Blockchain
  - 40+ points of data:
    - Source of the gem
    - Processing history
    - Certificates
    - HD photos, laser serial #s, 4Cs
- Uses a Hybrid Blockchain (public and private)

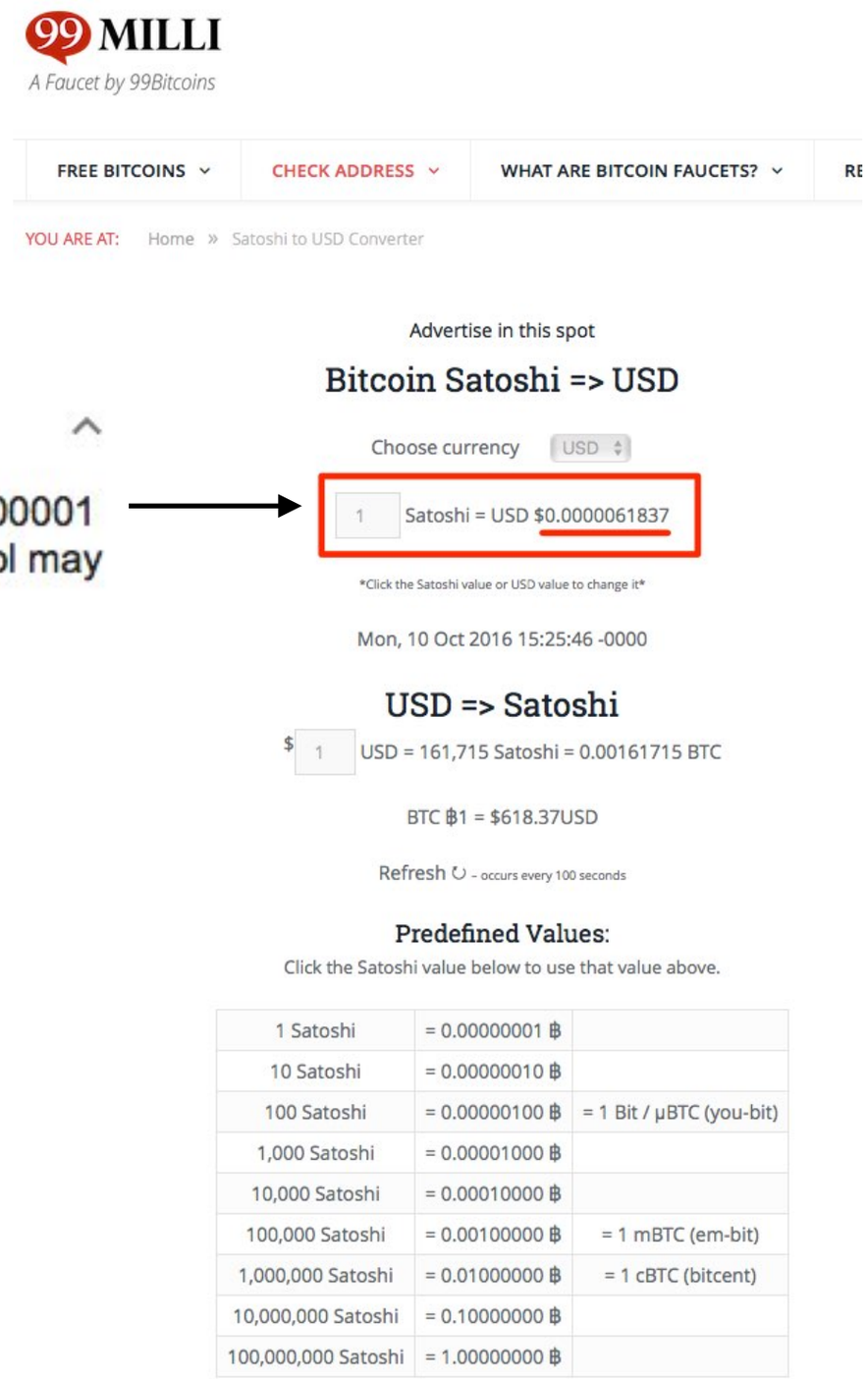
http://www.everledger.io

# Use Case: Micro Payments

## “Pay to Use”

Bitcoin divides down into such a tiny fraction that a payment of 1 millionth of a Cent is possible.


(Satoshi Nakamoto, anonymous inventor of Bitcoin)

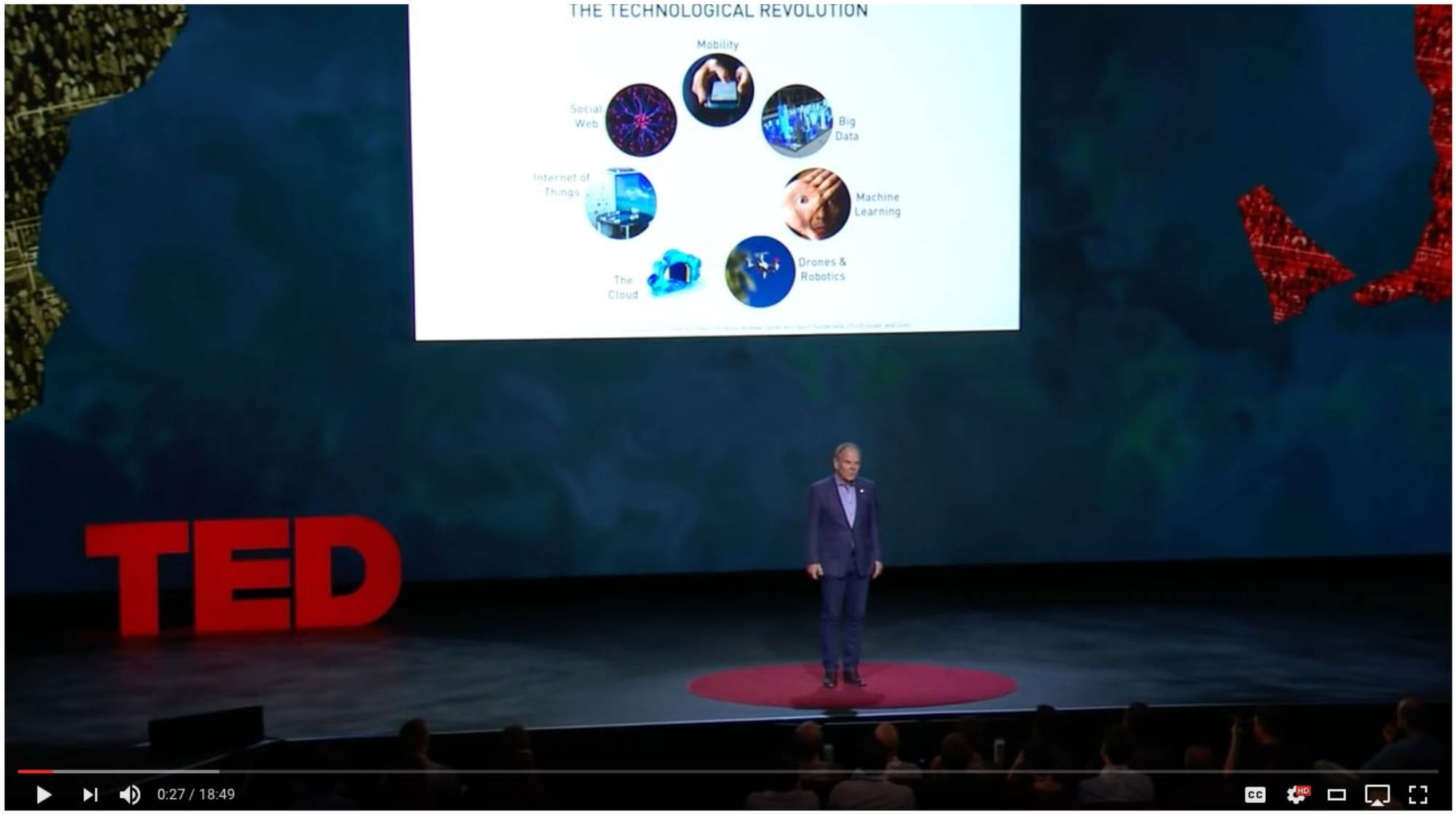



## Examples

- ala carte consumption:
  - pay to read an article/play a song
  - pay for wifi consumed
  - pay website advertisers
- Move from “pay wall” to “pay to use”

BLOCKCHAIN

# “How the Blockchain is changing money and business”




https://www.youtube.com/watch?v=Pl8OlkkwRpc (18:49)

BLOCKCHAIN

# Blockchain is not a silver bullet

"Because it's on a blockchain, it's true"


- In bitcoin "true" means that the network has agreed that a transaction has taken place, and nodes are in **agreement or consensus** that this has happened.
- The concept of "truth" as applied to blockchains doesn't extend to other meanings of "true". If a heart-monitoring piece of hardware becomes faulty and records incorrect heart-rate readings onto a blockchain, do the readings become truth? Clearly not.
- On a registry of car ownership, a blockchain may immutably record that a car has changed owner. If this transaction was made in error or fraudulently due to a hacking of the owner's phone, what is the state of the truth? If the transaction was found to be fraudulent by the police and needs to be 'unwound', then how will that be done, given the cryptographic security of digital signatures?
- In the case of blockchains, truth just means "what was originally **recorded and agreed** as valid by the majority of the nodes". **Valid doesn't necessarily mean true**. Don't confuse blockchain truth with *The Truth*.

BLOCKCHAIN

# Challenges


- This is emerging technology
- New blockchains popping up everywhere
- “What does it all mean?” projects being launched by major players (financial, computing, …)
- $$$ being invested
- Lots of opportunities for unique applications
- Lots of technical and business challenges
- Be wary of hype

BLOCKCHAIN