Introduction to Blockchain

Oleg Lodygensky - LAL - Mai 2017

https://www.lal.in2p3.fr

http://www.u-psud.fr

http://www.cnrs.fr

Table of contents

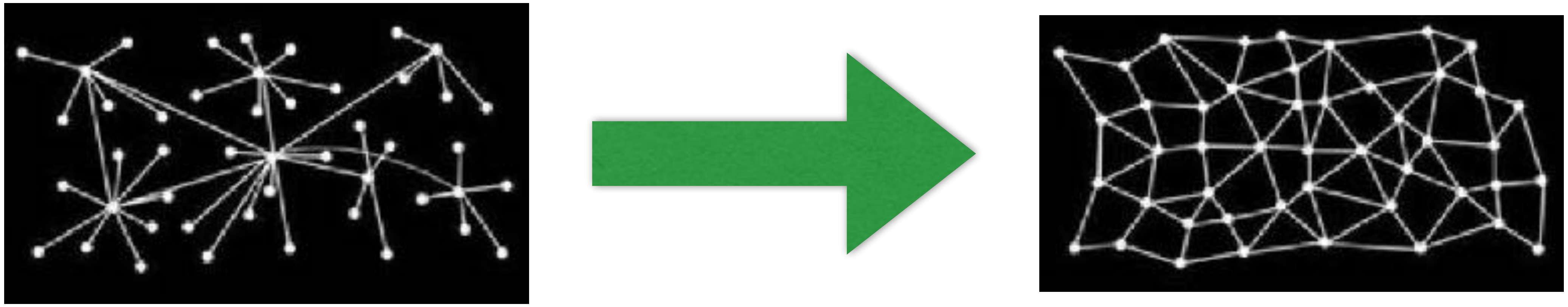
1. Introduction
2. Paradigmes
3. Concepts
4. Usage
5. Drawbacks
6. Decentralized applications

Blockchain

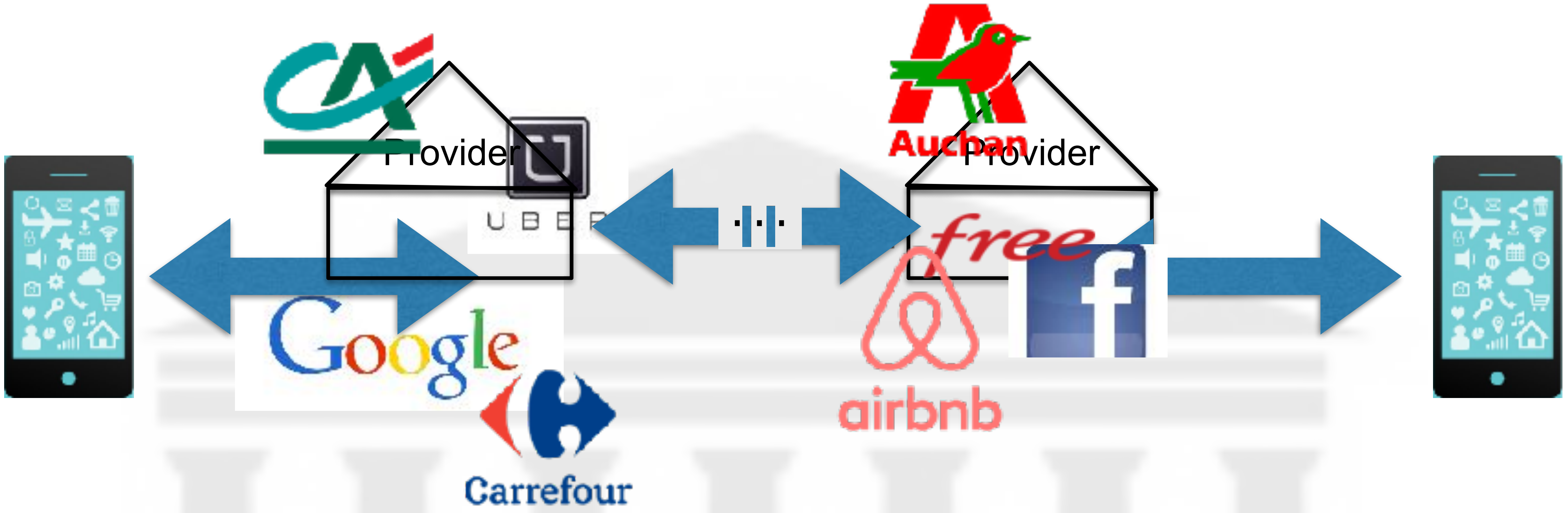
Since 2009

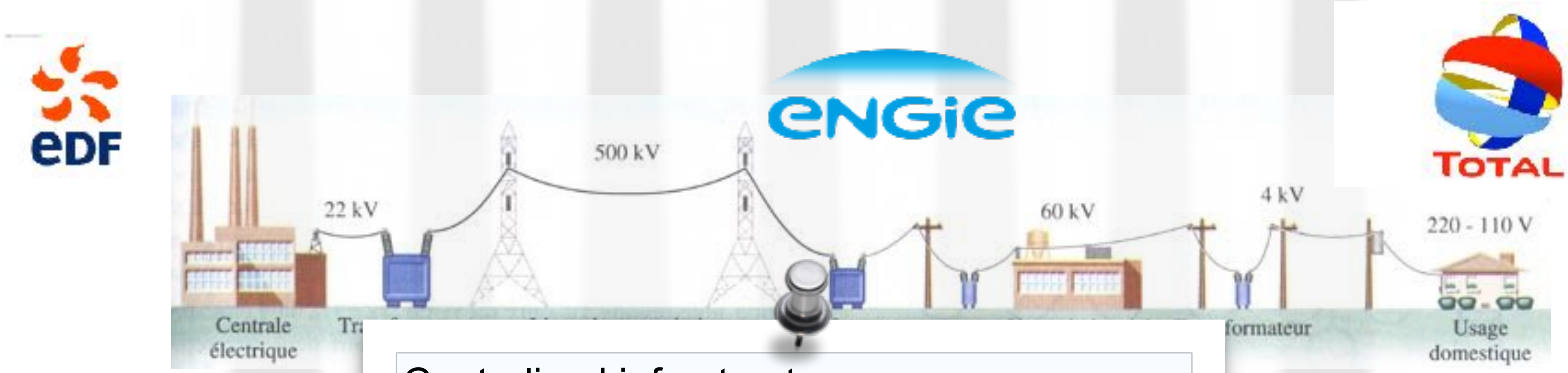
Open Source

- ★ Electronic transaction revolution
- ★ Digital assets management
- ★ Decentralized transactions



Centralized transaction





Centralized infrastructures manages:

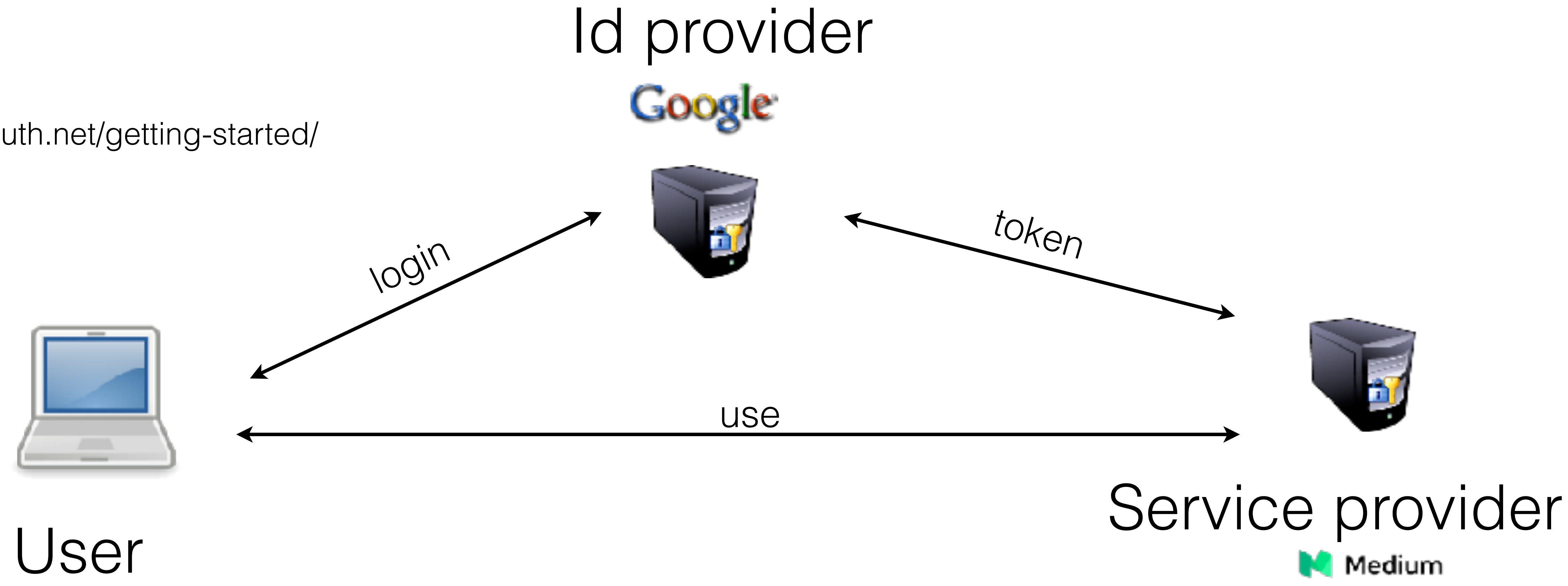
- identity
- assets
- transactions

Centralized Transactions Issues

1. Identity management
2. Censorship
3. Vulnerability
4. Costs

Centralization Issue #1 : Identity Management

https://oauth.net/getting-started/



Problem

Identity provider may:
- refuse your registration
- close your contract
- fail / shut down

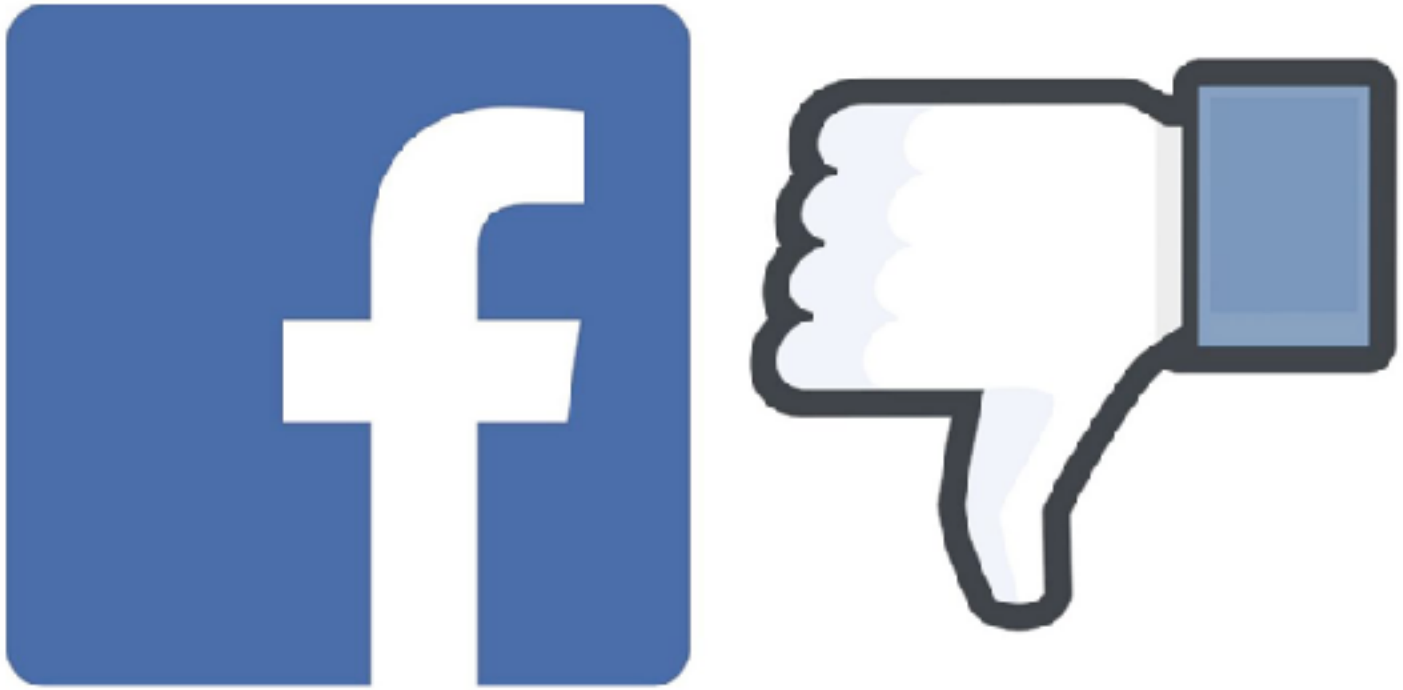
Action tracking

Private life intrusion

Centralization issue #2: Censorship

Quelqu'un a fait des mouillettes ?

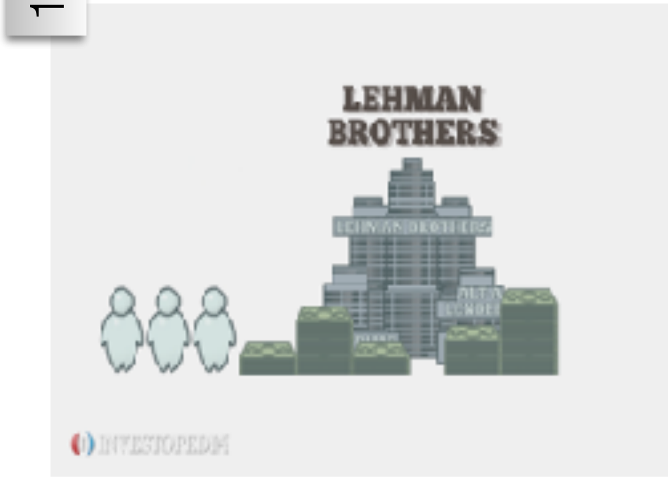
source photo : wafs

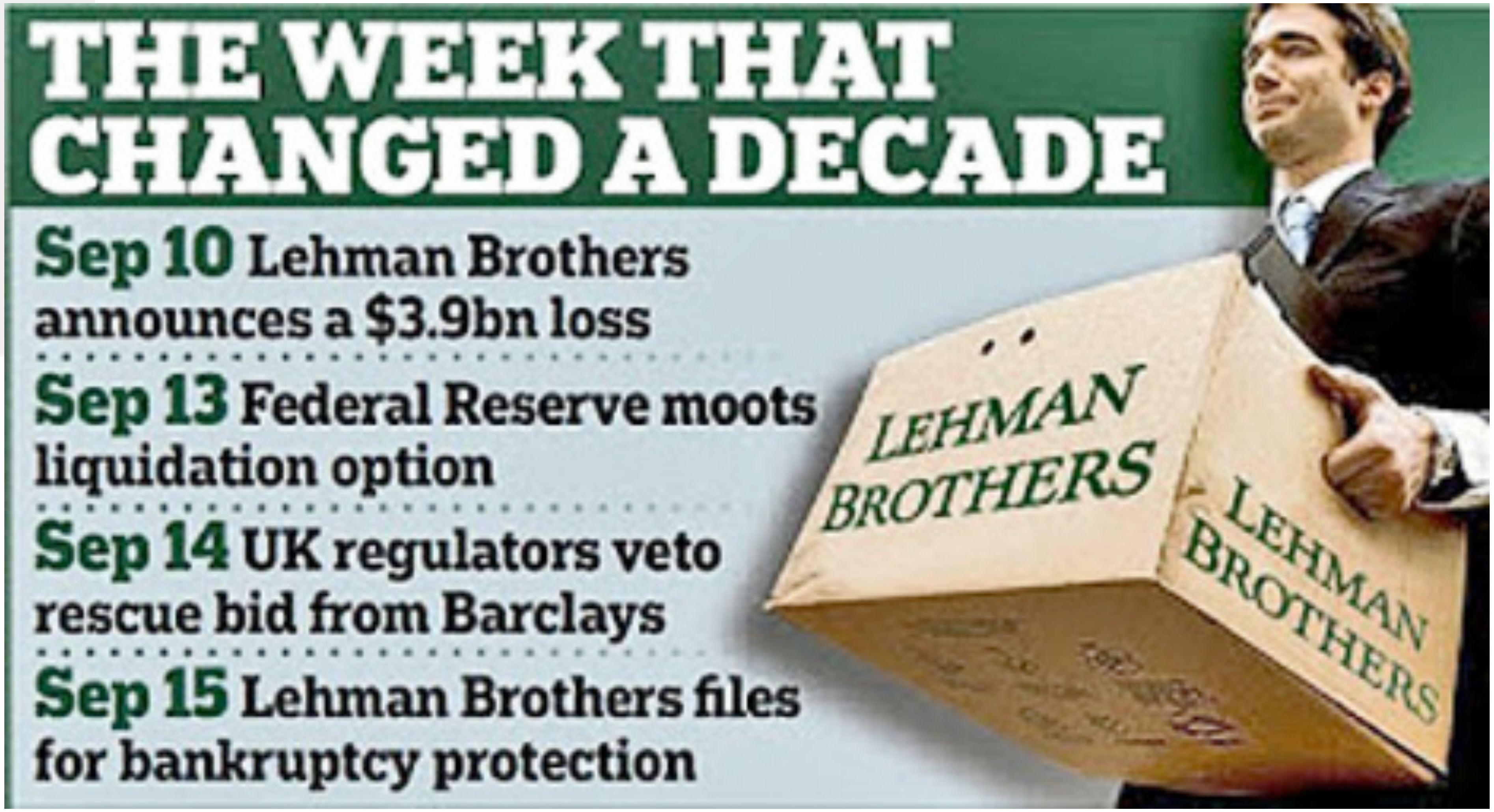


Problem

Who write the rules ?

Centralization issue #3 : Vulnerability





THE WEEK THAT CHANGED A DECADE

Sep 10 Lehman Brothers announces a $3.9bn loss

Sep 13 Federal Reserve moots liquidation option

Sep 14 UK regulators veto rescue bid from Barclays

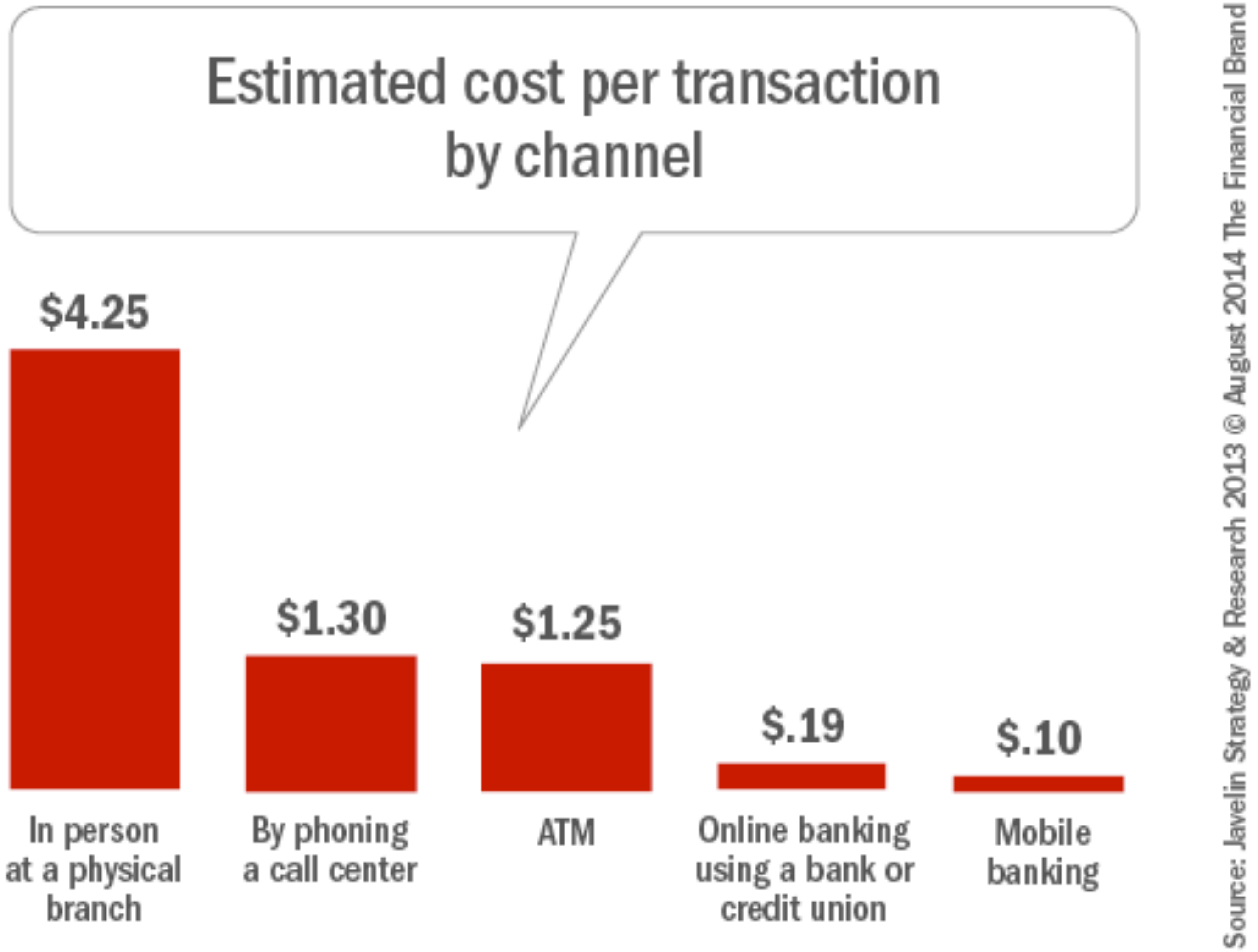
Sep 15 Lehman Brothers files for bankruptcy protection

LEHMAN BROTHERS
LEHMAN BROTHERS

Problem

What compensations ?

Centralization issue #4 : Transaction costs

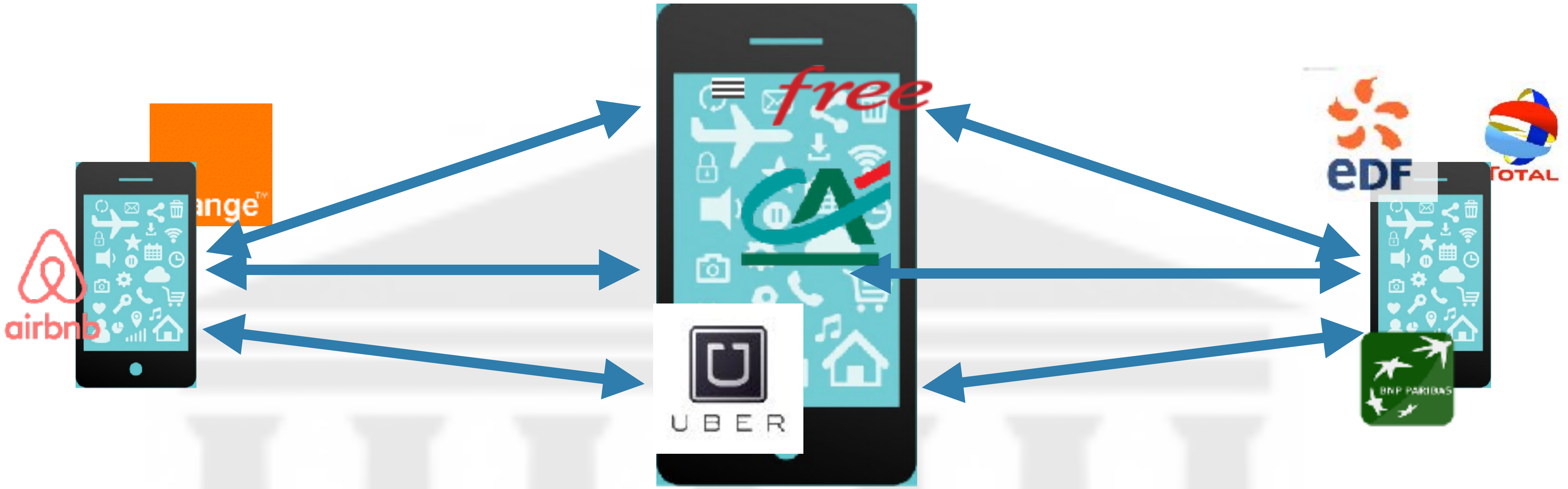


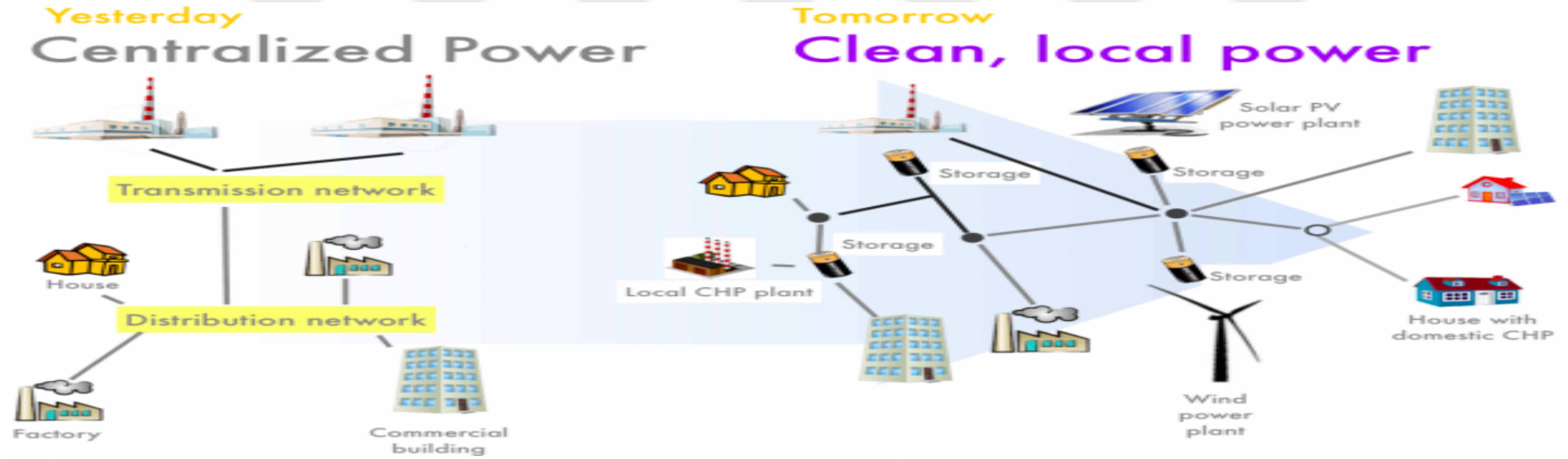
Source: Javelin Strategy & Research 2013 © August 2014 The Financial Brand

Problem

What about micro payment ?

Decentralization promises





https://cleantechnica.com/2011/11/28/americas-energy-future-a-battle-between-entrenched-utilities-and-clean-local-power/

Table of contents

1. Introduction
2. Paradigmes
3. Concepts
4. Usage
5. Drawbacks
6. Decentralized applications

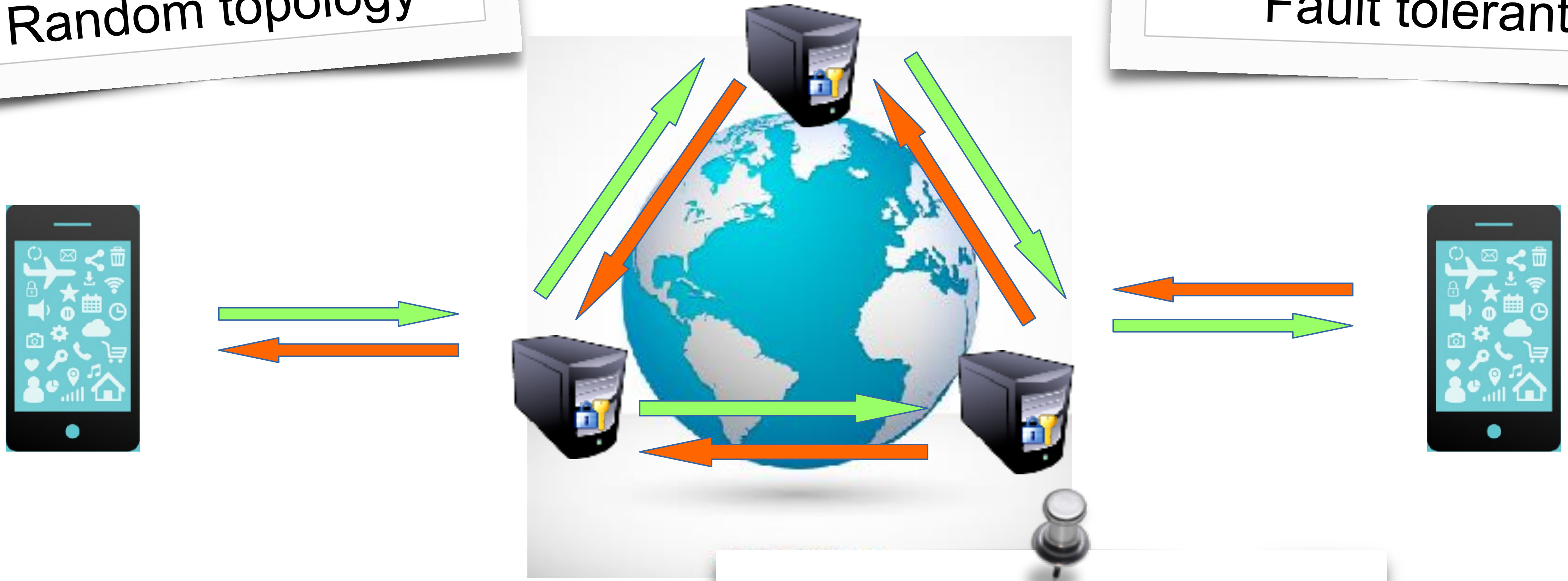
Main Paradigmes

- P2P Network
- Shared Ledger
- Distributed Consensus
- Security

P2P network

Random topology

Fault tolerant



Untrustable

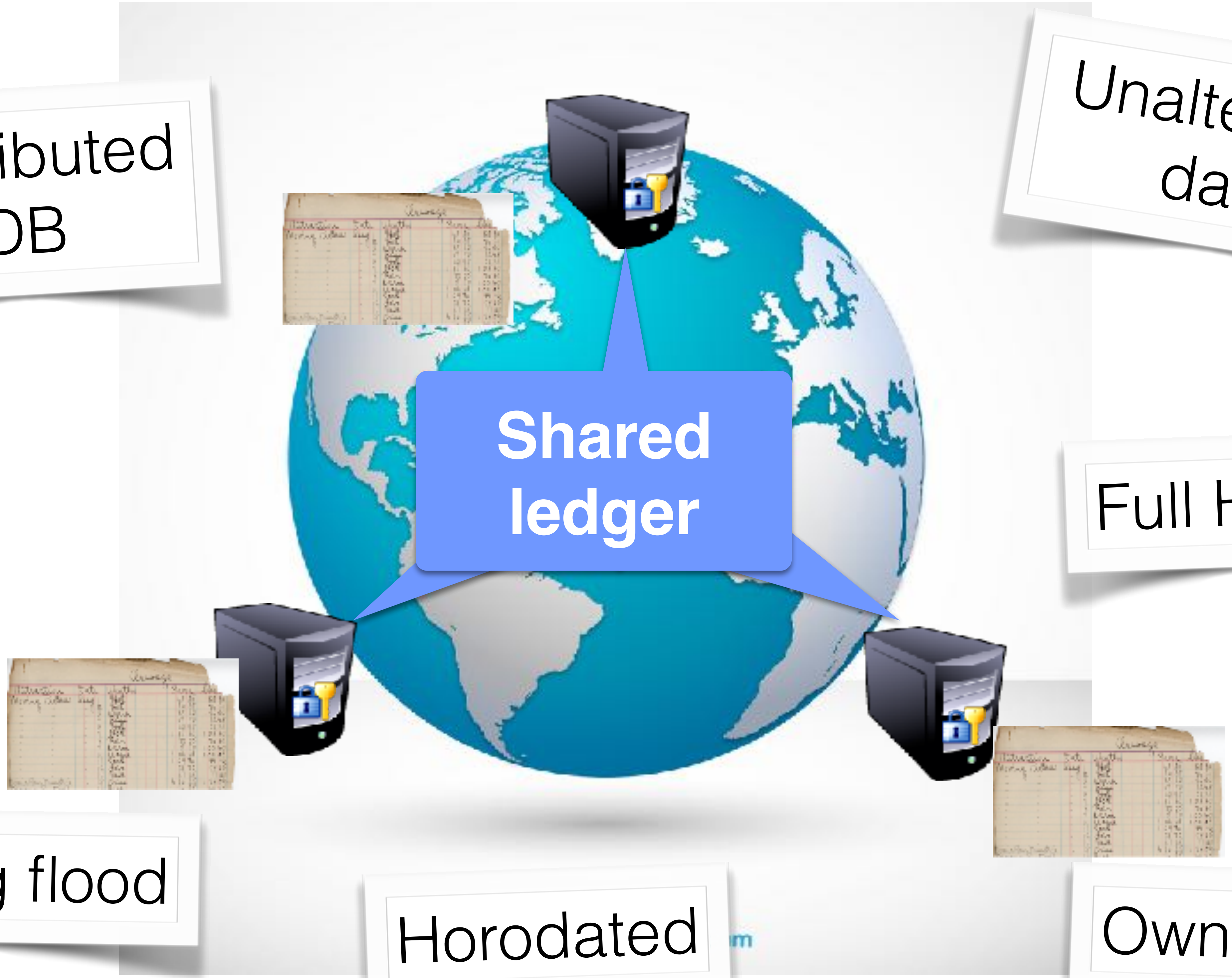
Unbounded communications

Latency

Shared ledger

Distributed DB

Unalterable data



Full History

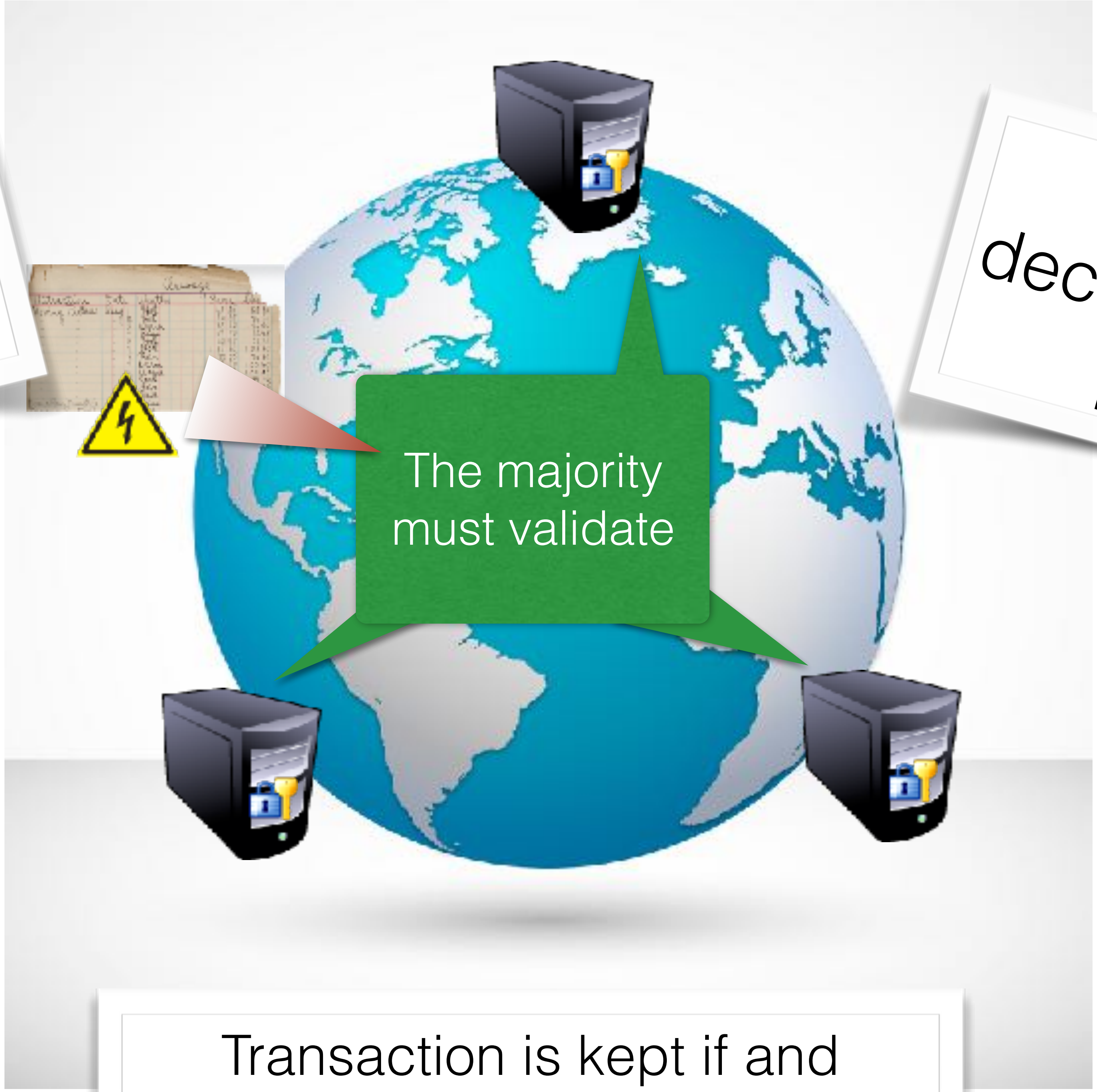
Gossiping flood

Horodated

Ownership

Distributed consensus

Frauding & Stealing Resistance



Collective decision-making process

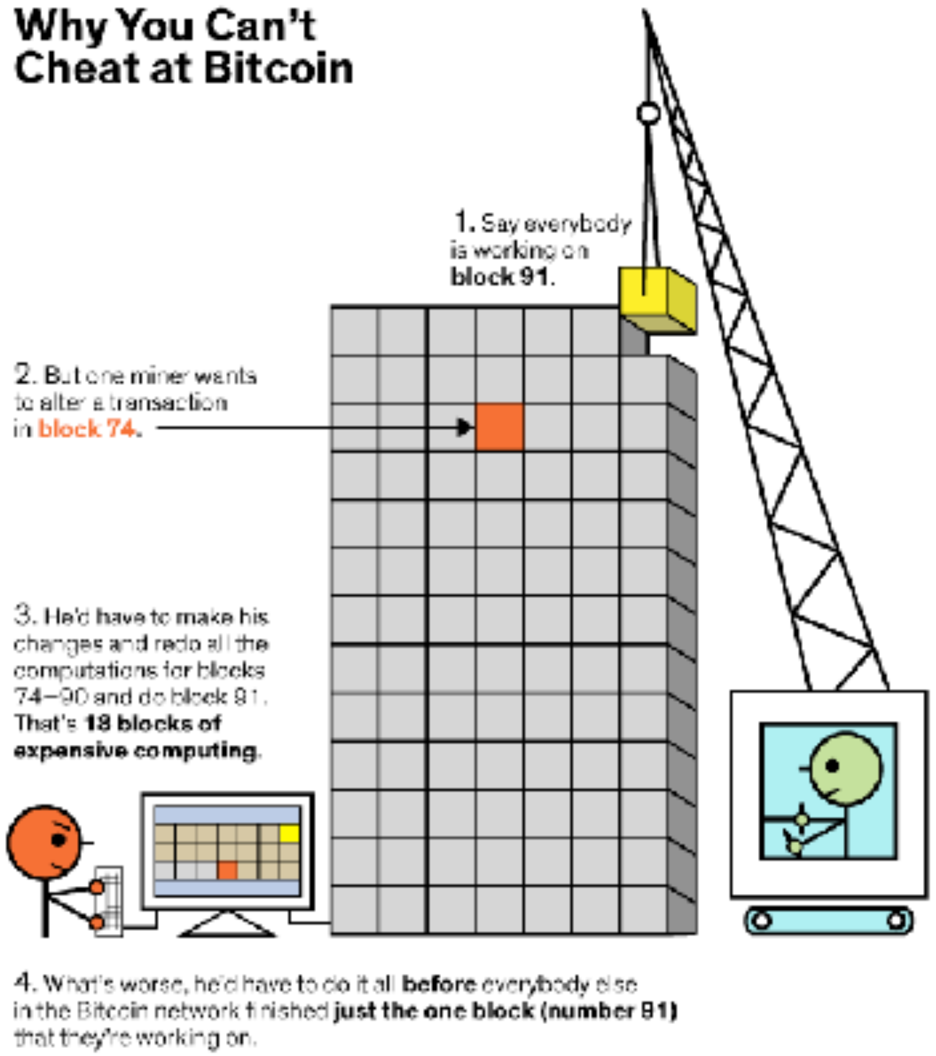
Transaction is kept if and only if the consensus is reached

Security

Security is ensured at different levels:

- electronic keys
- encryption
- distributed validation
- data replication
- linked blocks (history)

Until now blockchain protocol has never been hacked



Why You Can't Cheat at Bitcoin

1. Say everybody is working on **block 91**.

2. But one miner wants to alter a transaction in **block 74.**

3. He'd have to make his changes and redo all the computations for blocks 74–90 and do block 91. That's **18 blocks of expensive computing.**

4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

Illustration: Mark Montgomery/IEEE Spectrum

Table of contents

1. Introduction
2. Paradigmes
3. Concepts
4. Usage
5. Drawbacks
6. Decentralized applications

Coin

Coins are immutable:

- they can be created
- they must be digitally signed

They can’t be modified in any manner:

- no transfert
- no division
- no combination

Transactions

Transactions aim to:

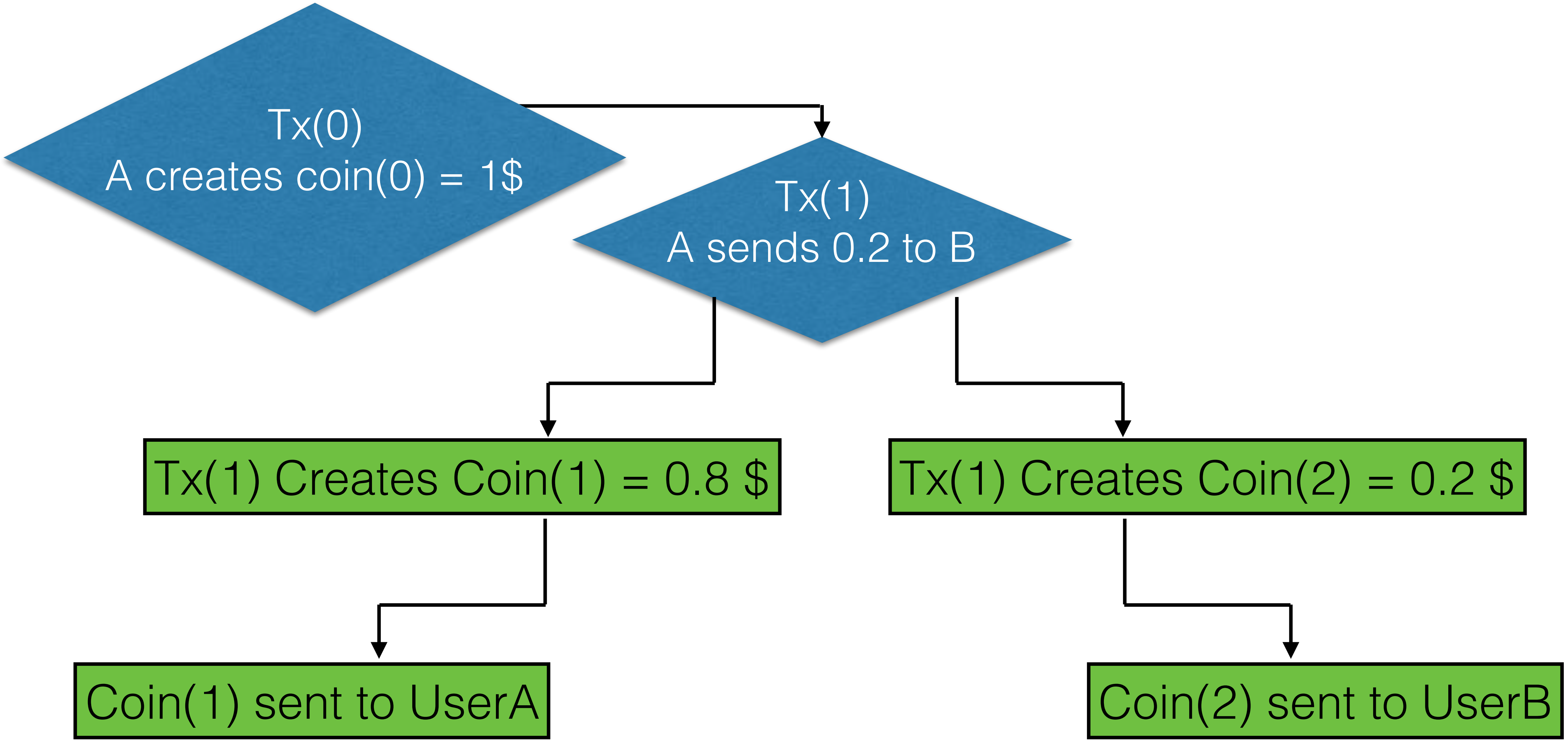
- consume coins
- create new coins

Requirements:

- sig(consumed coins) must be valid
- sum(consumed coins) == sum(created coins)
- must sign (created coins)

Validation is cryptographic only !

Transactions



Tx(0)
A creates coin(0) = 1$

Tx(1)
A sends 0.2 to B

Tx(1) Creates Coin(1) = 0.8 $

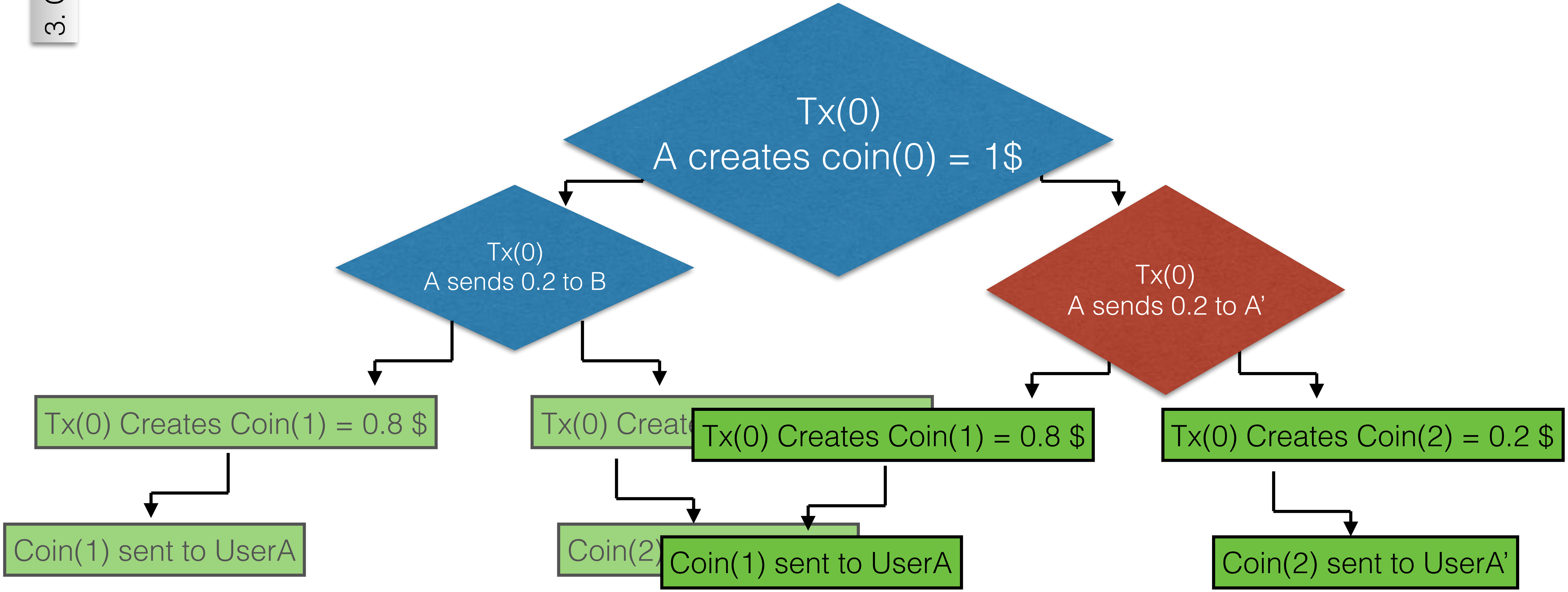
Tx(1) Creates Coin(2) = 0.2 $

Coin(1) sent to UserA

Coin(2) sent to UserB

Registered in the ledger by **consensus**
(*by blocks of transactions for efficiency*)

Double Spent Attack



Tx(0)
A creates coin(0) = 1$

Tx(0)
A sends 0.2 to B

Tx(0)
A sends 0.2 to A'

Tx(0) Creates Coin(1) = 0.8 $

Tx(0) Creat

Tx(0) Creates Coin(1) = 0.8 $

Tx(0) Creates Coin(2) = 0.2 $

Coin(1) sent to UserA

Coin(2)

Coin(1) sent to UserA

Coin(2) sent to UserA'

The theory says there is no way to determine the « honest » path.

If validating nodes are randomly chosen,
distributed consensus is **probabilistic** only !

Incentives

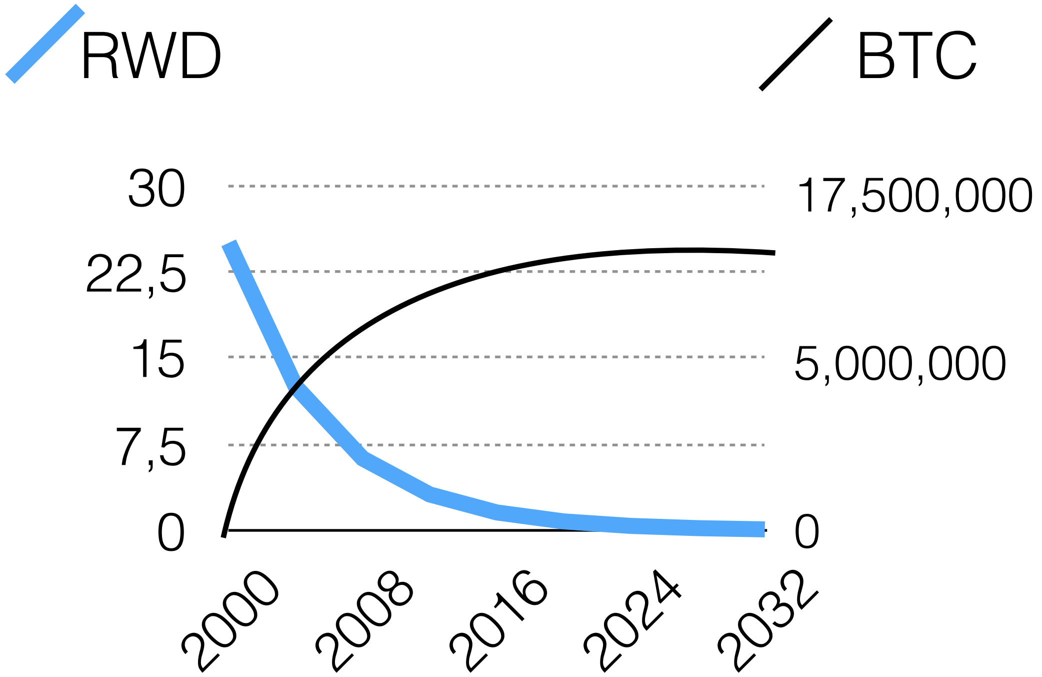
Incentives aim to encourage nodes to be honest

-1- **Rewards**

Block creator get reward

if created block ends on long-term consensus branch

- started at 25Btc
- halves every 4 years



-2- **Fees**

Transaction author may create a transaction
where outputValue < inputValue
The remaining is a « tips » for the block validator

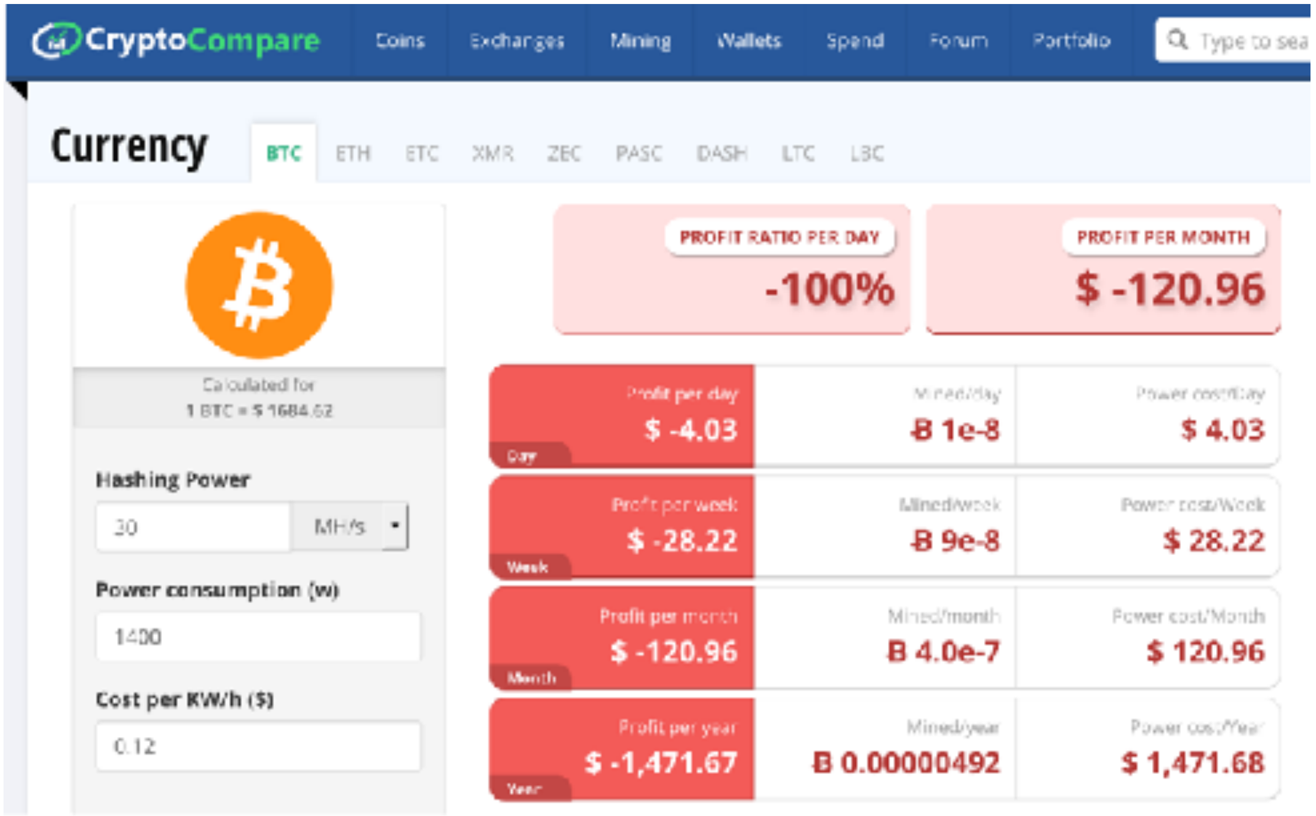
Table of contents

1. Introduction
2. Paradigmes
3. Concepts
4. Usage
5. Drawbacks
6. Decentralized applications

Usage

1. Mining
2. Funding and trading
3. Decentralized id
4. Decentralized IT

Usage #1: mining



CryptoCompare | Coins | Exchanges | Mining | Wallets | Spend | Forum | Portfolio | Type to sea

Currency: **BTC** | ETH | ETC | XMR | ZEC | PASC | DASH | LTC | LBC

Calculated for 1 BTC = $ 1684.62

Hashing Power: 30 MH/s

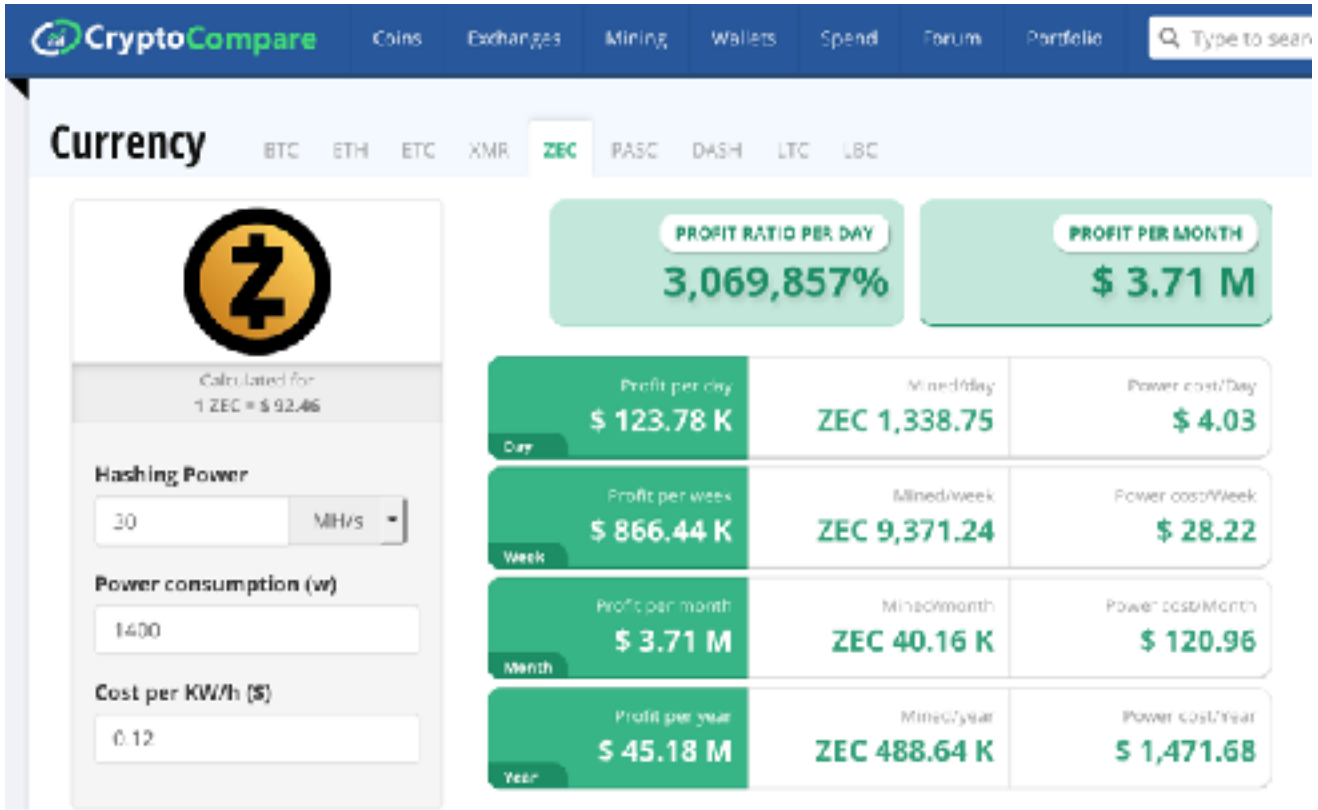
Power consumption (w): 1400

Cost per KW/h ($): 0.12

PROFIT RATIO PER DAY: -100%

PROFIT PER MONTH: $ -120.96

Day	Profit per day $ -4.03	Mined/day Ƀ 1e-8	Power cost/Day $ 4.03
Week	Profit per week $ -28.22	Mined/week Ƀ 9e-8	Power cost/Week $ 28.22
Month	Profit per month $ -120.96	Mined/month Ƀ 4.0e-7	Power cost/Month $ 120.96
Year	Profit per year $ -1,471.67	Mined/year Ƀ 0.00000492	Power cost/Year $ 1,471.68



CryptoCompare | Coins | Exchanges | Mining | Wallets | Spend | Forum | Portfolio | Type to sear

Currency: BTC | ETH | ETC | XMR | **ZEC** | PASC | DASH | LTC | LBC

Calculated for 1 ZEC = $ 92.46

Hashing Power: 30 MH/s

Power consumption (w): 1400

Cost per KW/h ($): 0.12

PROFIT RATIO PER DAY: 3,069,857%

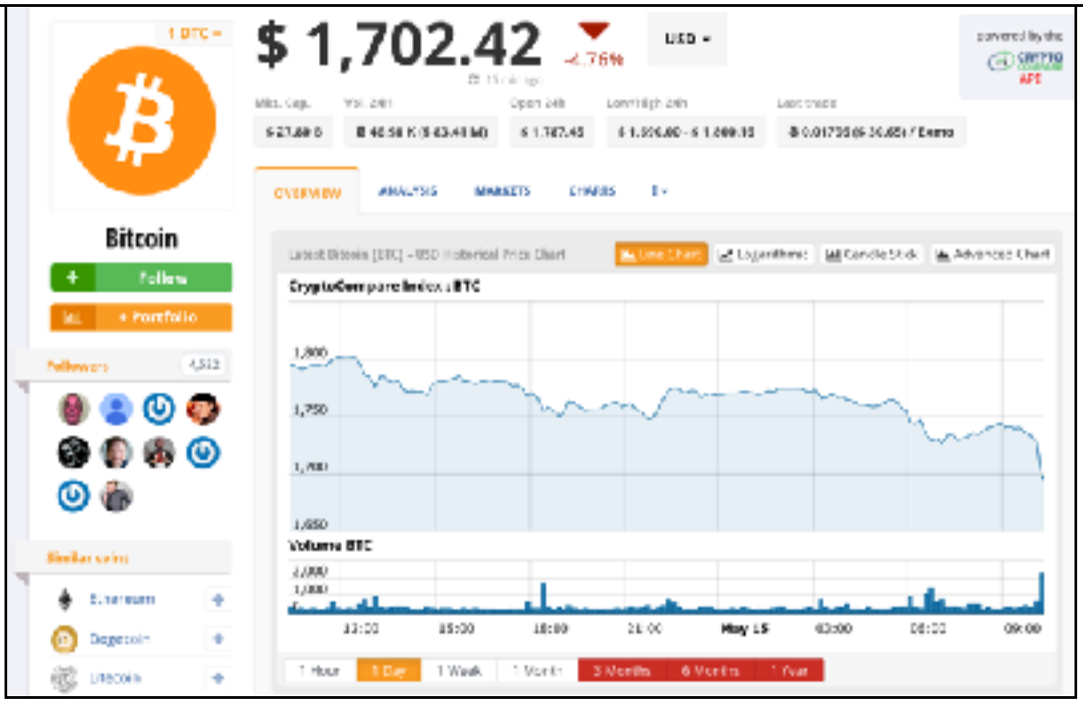
PROFIT PER MONTH: $ 3.71 M

Day	Profit per day $ 123.78 K	Mined/day ZEC 1,338.75	Power cost/Day $ 4.03
Week	Profit per week $ 866.44 K	Mined/week ZEC 9,371.24	Power cost/Week $ 28.22
Month	Profit per month $ 3.71 M	Mined/month ZEC 40.16 K	Power cost/Month $ 120.96
Year	Profit per year $ 45.18 M	Mined/year ZEC 488.64 K	Power cost/Year $ 1,471.68

https://www.cryptocompare.com/mining/calculator/

Usage #2: Trading & Funding

https://www.cryptocompare.com/coins/btc/overview



1 BTC

$ 1,702.42 -4.76%

USD

Bitcoin

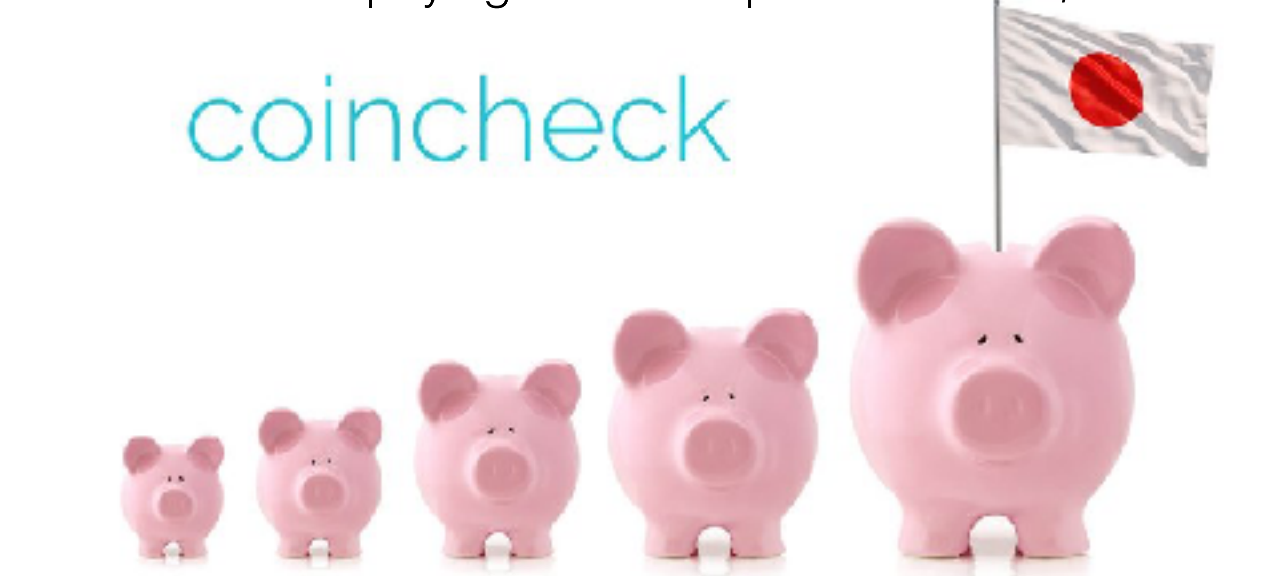
http://www.coindesk.com/icos-changing-way-vcs-deal-startups/

ICOs Are Changing the Way VCs Deal With Startups

Michael del Castillo (@DelRayMan) | Published on May 11, 2017 at 13:30 BST

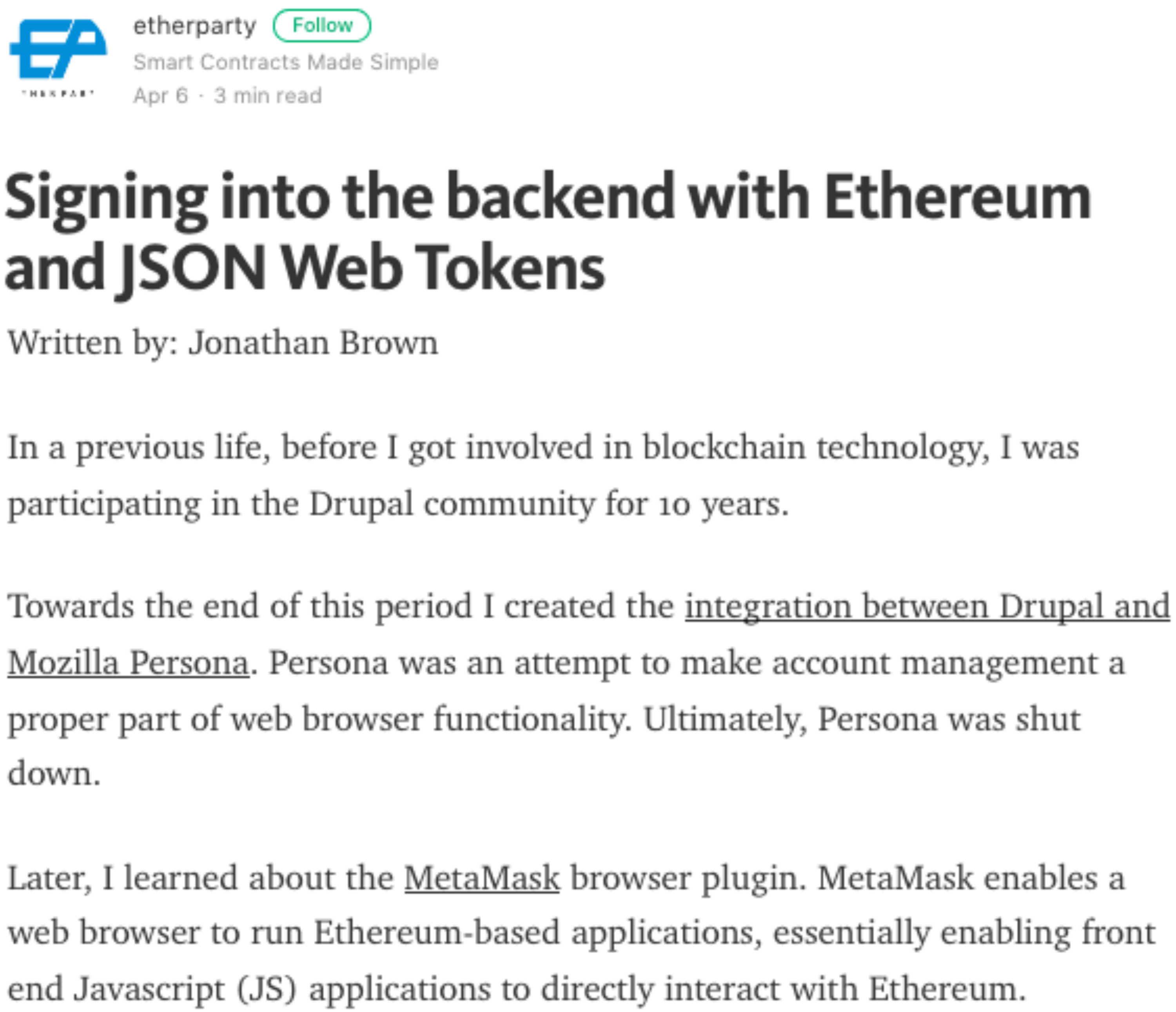
FEATURE

https://bitcoinmagazine.com/articles/japan-receive-its-first-interest-paying-bitcoin-deposit-accounts/



Usage #3: decentralized Id

https://medium.com/@etherparty/signing-into-the-backend-with-ethereum-and-json-web-tokens-9d1e765deed3



etherparty

Smart Contracts Made Simple

Apr 6 · 3 min read

Signing into the backend with Ethereum and JSON Web Tokens

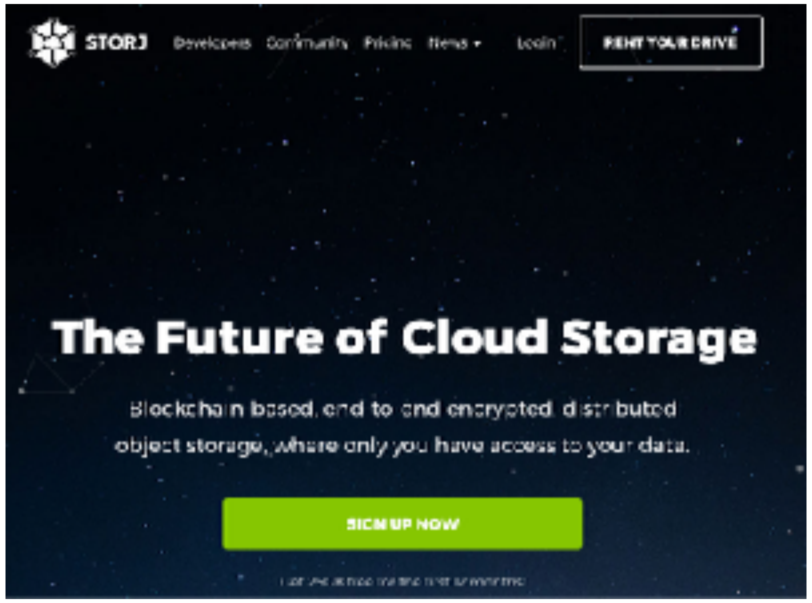
Written by: Jonathan Brown

In a previous life, before I got involved in blockchain technology, I was participating in the Drupal community for 10 years.

Towards the end of this period I created the integration between Drupal and Mozilla Persona. Persona was an attempt to make account management a proper part of web browser functionality. Ultimately, Persona was shut down.

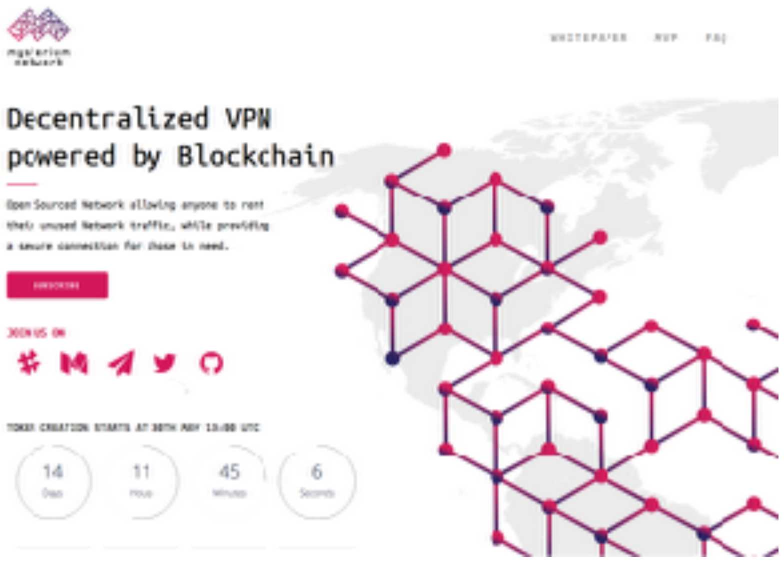
Later, I learned about the MetaMask browser plugin. MetaMask enables a web browser to run Ethereum-based applications, essentially enabling front end Javascript (JS) applications to directly interact with Ethereum.

Usage #4: decentralised IT



The Future of Cloud Storage

Blockchain based, end to end encrypted, distributed object storage, where only you have access to your data.



Decentralized VPN powered by Blockchain

Open Sourced Network allowing anyone to rent their unused Network traffic, while providing a secure connection for those in need.

TOKEN CREATION STARTS AT 30TH MAY 13:00 UTC

Chasm: Fault-Tolerant, Information-Theoretic Secure Cloud Backup

Alex Grinman, Akshay Ravikumar, Julian Fuchs, Kevin Li

Supercomputer Organized by Network Mining

SONM. Supercomputer organized by network mining

WORLDWIDE SUPERCOMPUTER

Table of contents

1. Introduction
2. Paradigmes
3. Concepts
4. Usage
5. Drawbacks
6. Decentralized applications

Drawbacks

1. ## Scalability

   Seven transactions per second can take place and each block of transactions requires a minimum delay of 10 minutes to confirm.

2. ## Resistance to centralization

   Proof-of-work activity has been mostly consolidated into four primary mining organizations, all based in China. This alters the conception of blockchain as a decentralized system. Any two of these four could theoretically collude and would together constitute a majority of the computational resources (hash power) needed for mining, and could then control the updating of the distributed ledger.

3. ## Transparency

   All transactions are public, which has its pros and cons in terms of access to transactional information but not necessarily identification of participants to the network

4. ## Governance

   The original author of the Bitcoin open-source software is unknown and is open to question. Thus there is no clear structure for decision-making and the Bitcoin blockchain is heavily dependent on individual personalities and agendas

http://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/

Table of contents

1. Introduction
2. Principles
3. Concepts
4. Usage
5. Drawbacks
6. <u>Decentralized applications</u>

Blockchain 2.0

Post Crypto Currency Era

Crypto currencies have demonstrated technologies revolutionizing transactions.

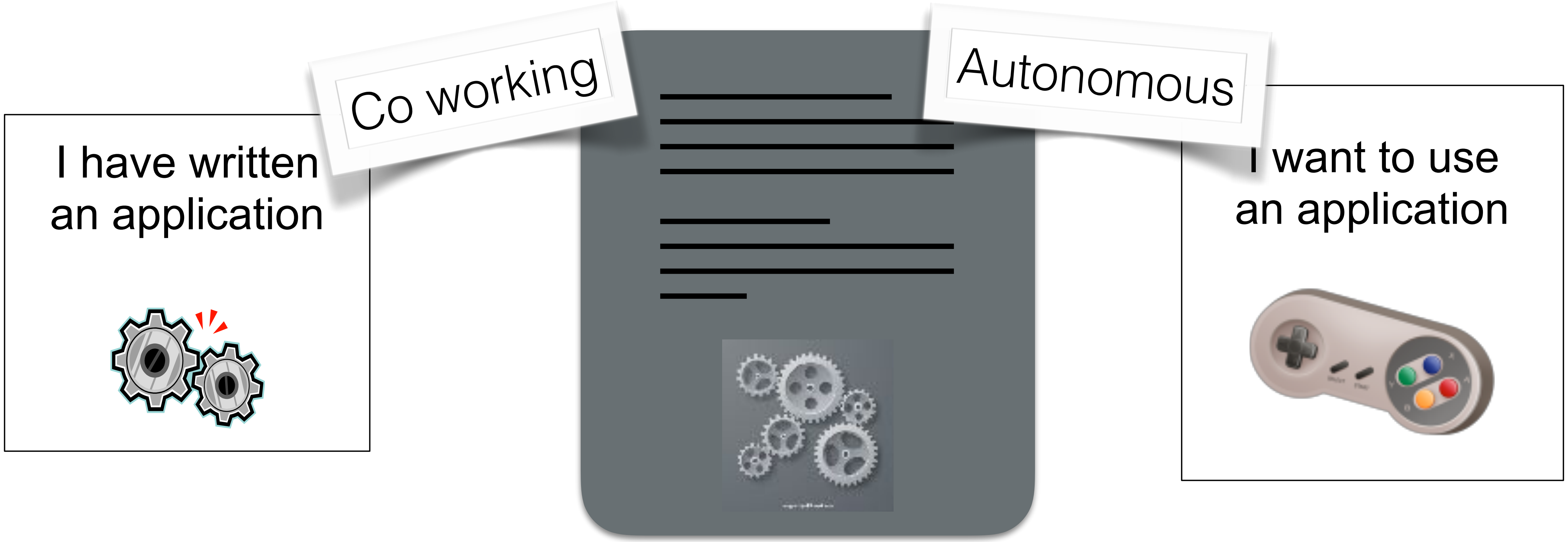
We are at the end of mining process; post crypto currency poses several challenges:

- What to do with all this computing power (several Tera flops available) ?
- Where to spend crypto currency?

- The Blockchain VM is very (deliberately) limited
- What to do with blockchain in the IT world?

Smart Contracts

Smart contracts
aim to write
distributed applications (*dApps*).



Co working

Autonomous

I have written an application

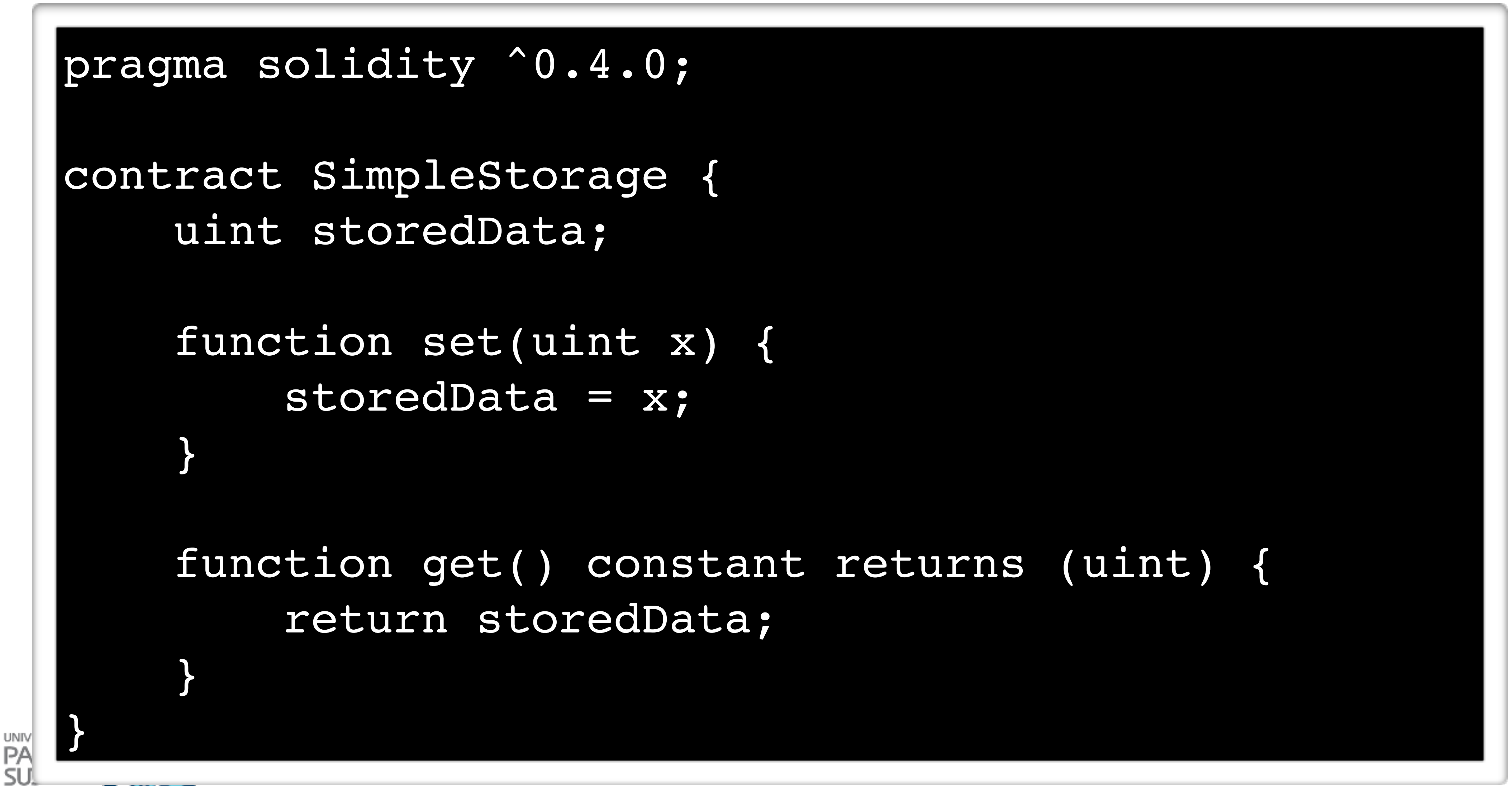
I want to use an application

Immutable

Solidity

http://solidity.readthedocs.io/

Solidity is a contract-oriented, high-level language whose syntax is similar to that of JavaScript and it is designed to target the Ethereum Virtual Machine (EVM).



```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) {
        storedData = x;
    }

    function get() constant returns (uint) {
        return storedData;
    }
}
```

Conclusion

- Bitcoin
  - ➡ Crypto currency introduced the first blockchain with success
- Blockchain
  - ➡ introducing SmartContracts to break limitations
  - ➡ we can now write decentralized application