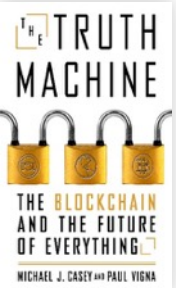
THE TRUTH MACHINE: The Blockchain and the Future of Everything

MIT EUROPE CONFERENCE
MICHAEL CASEY
February 20, 2019



digital currency initiative

"Empowering individuals by making it as fast and easy to move value across the world as it is to move information."

mit media lab

Why us, not them?

Ledgers:
An ancient
trust solution

The Centralized Trust Model

The Problem with Centralized Ledgers:

The Problem with Centralized Ledgers:

LEHMAN BROTHERS

The Problem with Centralized Ledgers:

LEHMAN BROTHERS

THE COST OF TRUST

THE COST OF TRUST

THE COST OF TRUST

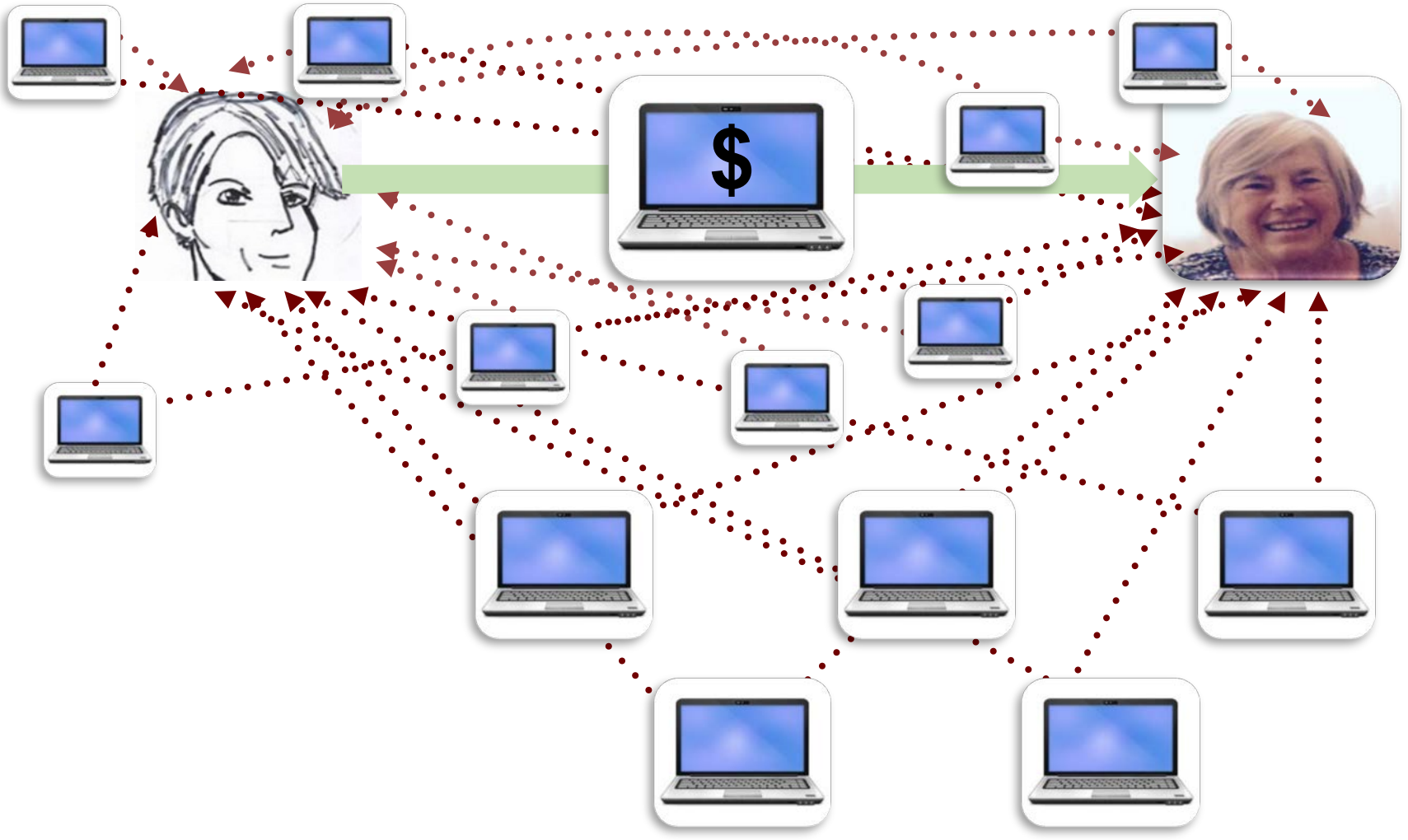
Cryptocurrency

A New Approach to a Difficult Problem

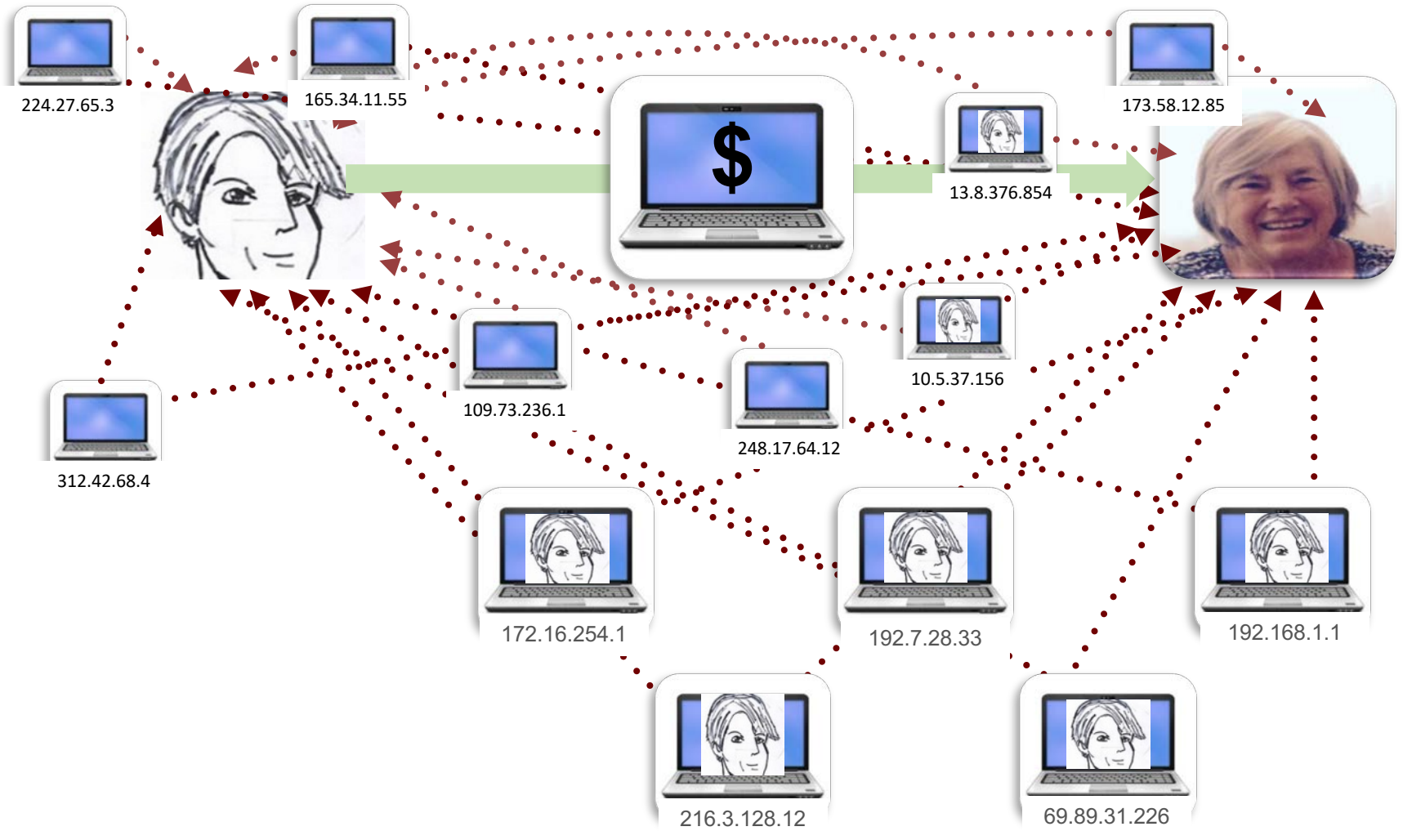
$

Problem 1: Double-Spending

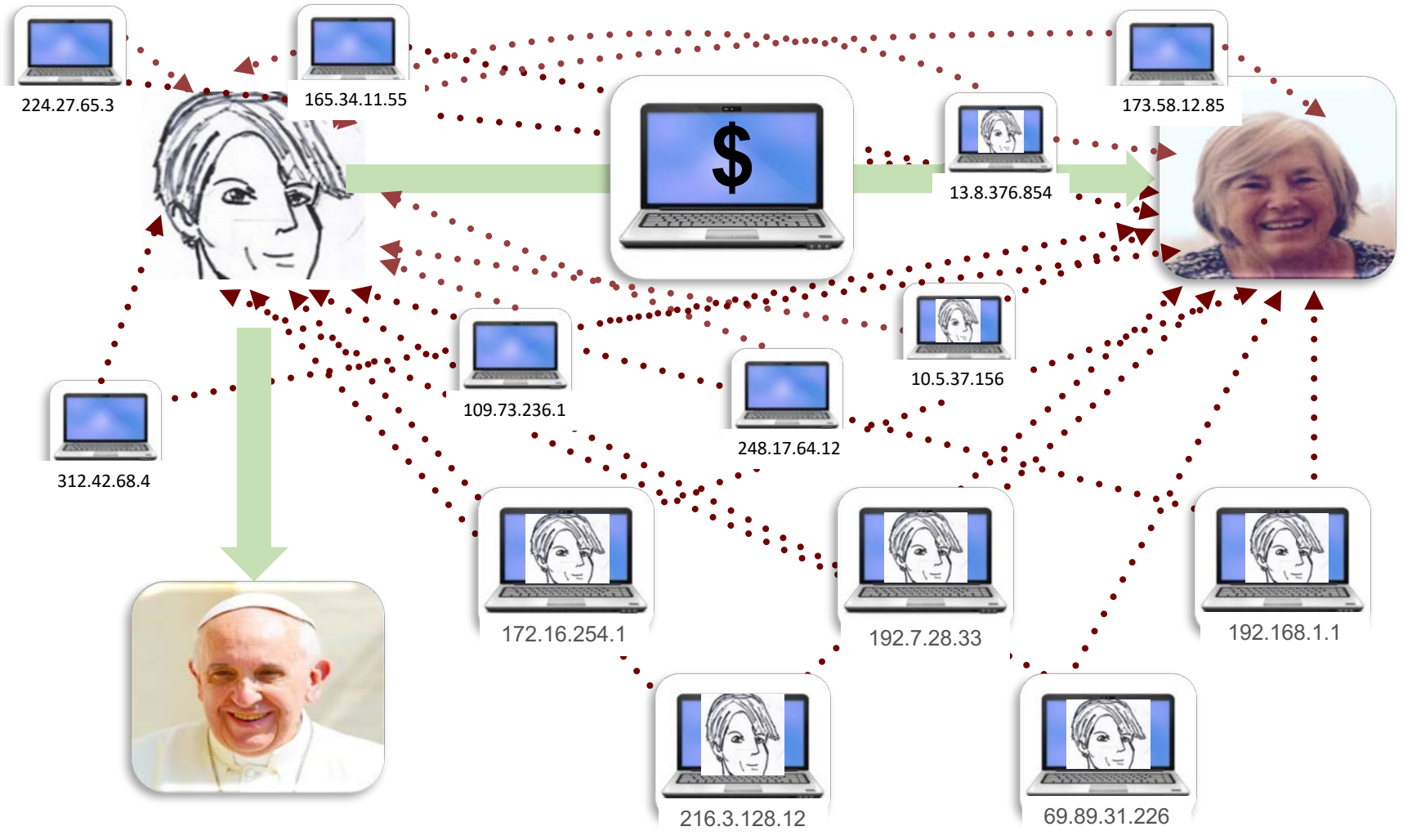
Solution: Consensus?

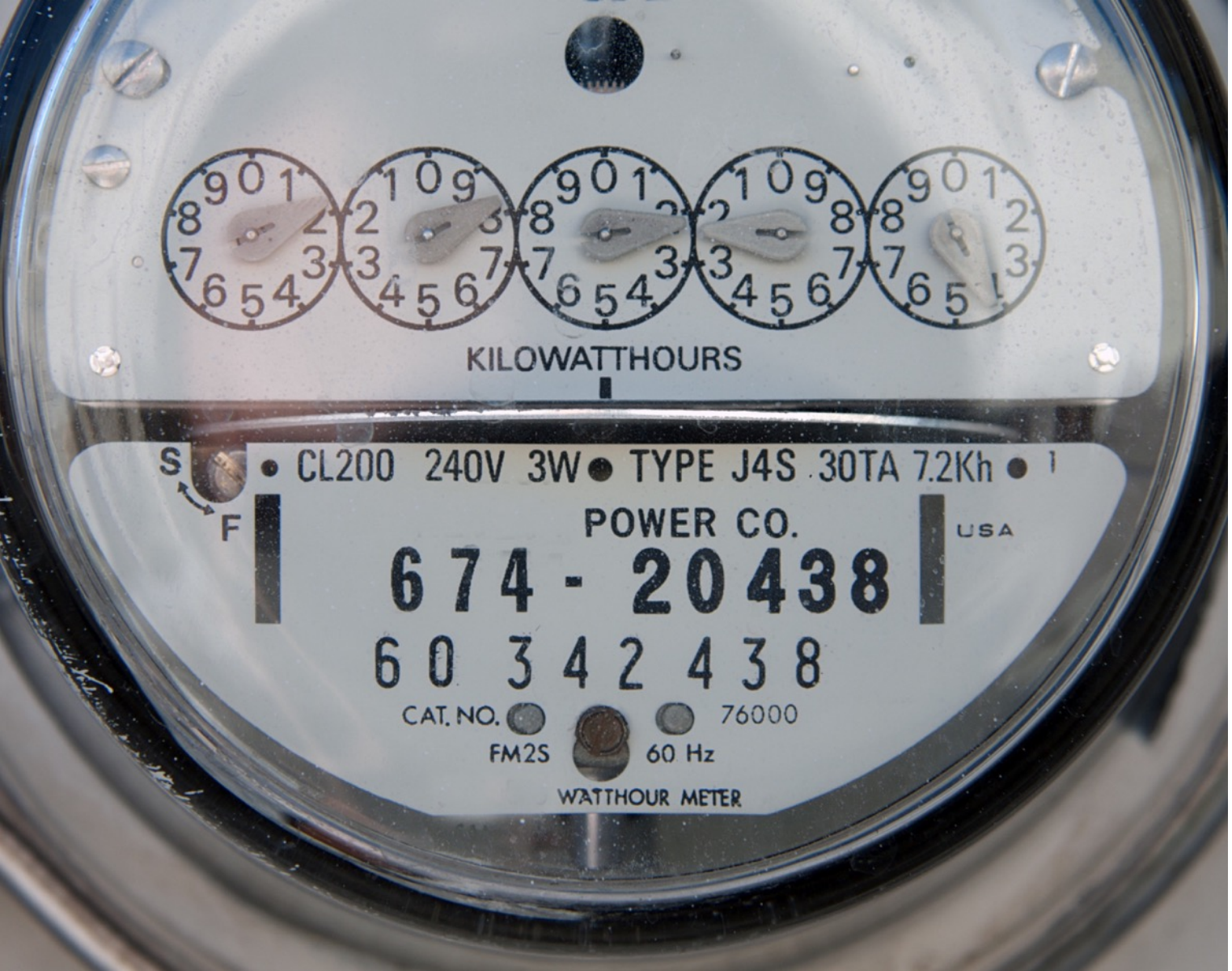


Problem 2: Sybil Attacks



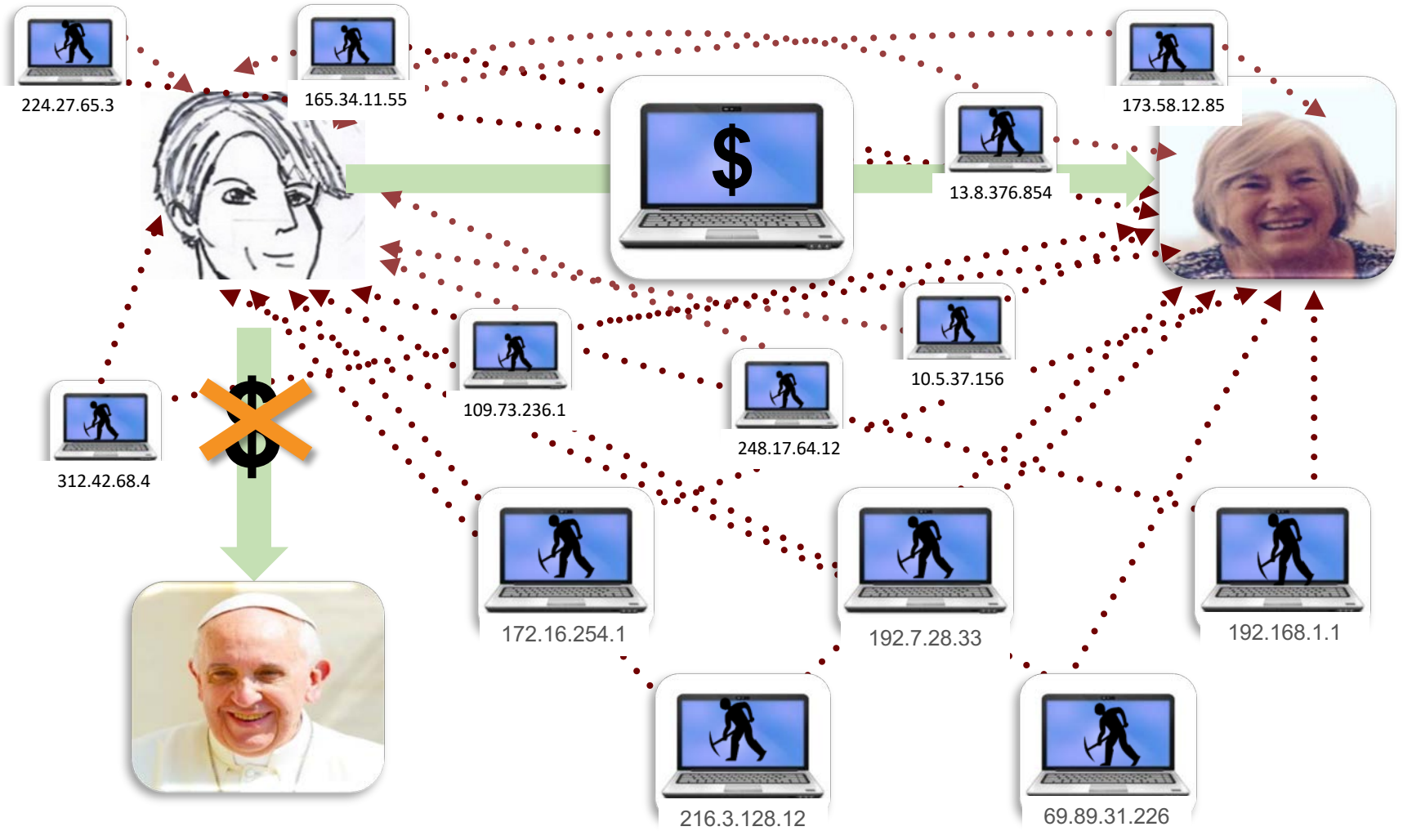
Problem 2: Sybil Attacks



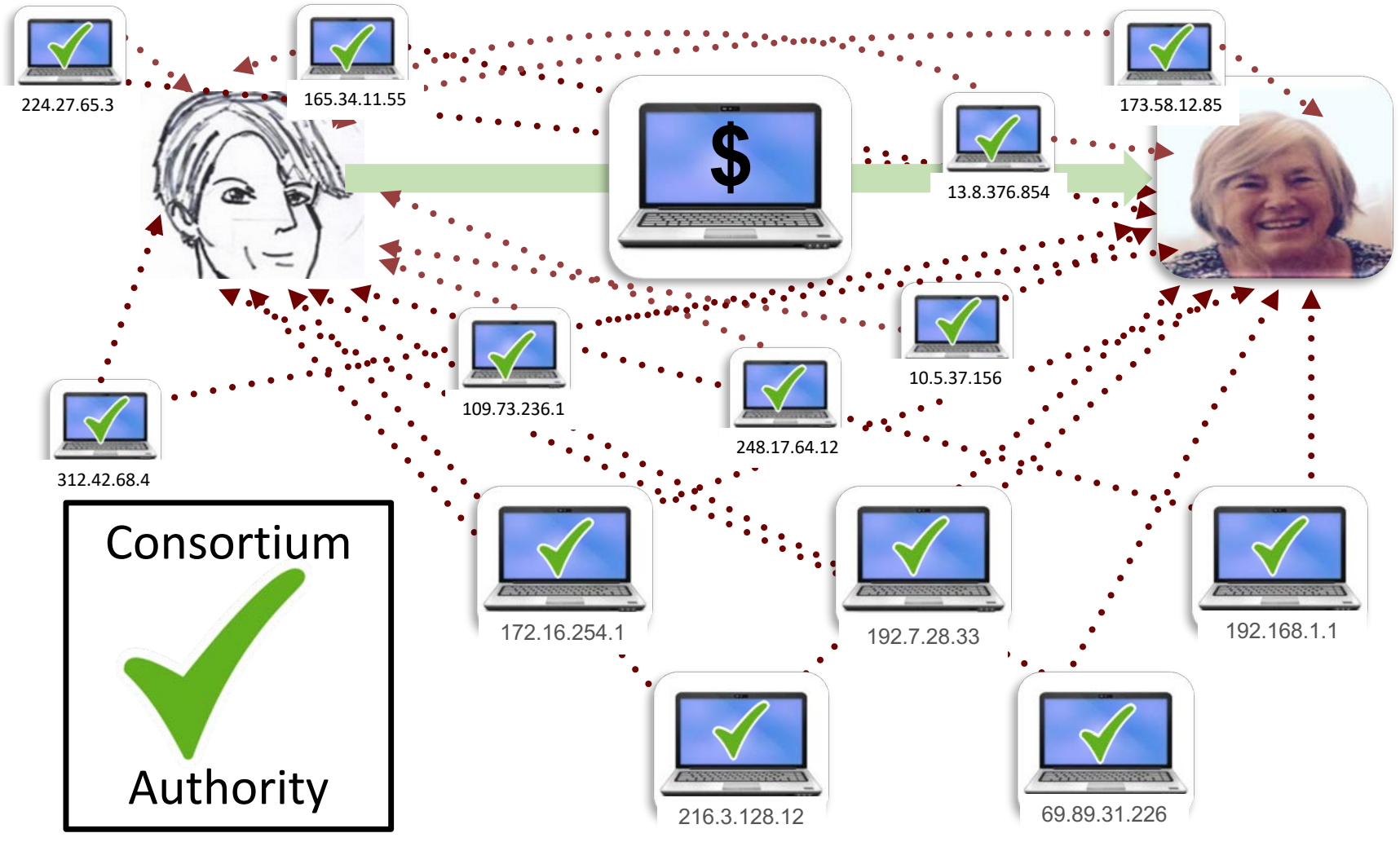


Satoshi's Solution: Proof of Work

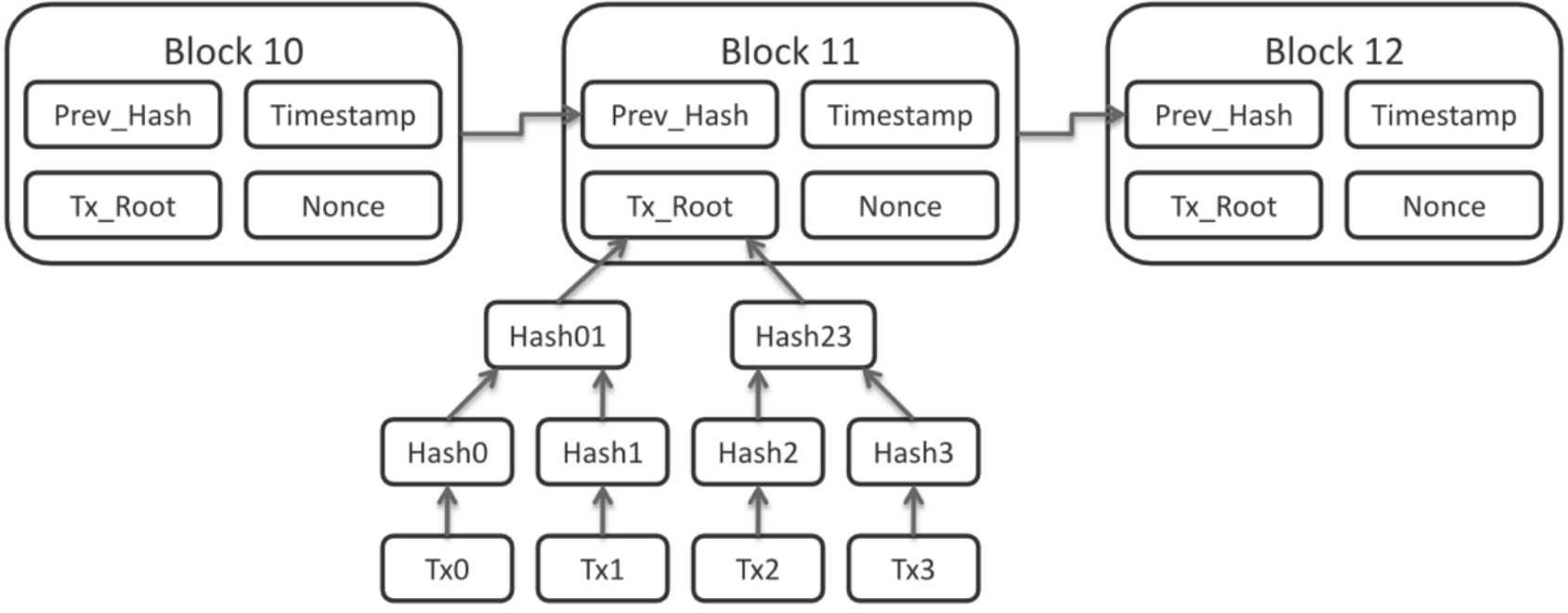
Solution: Permissionless Consensus



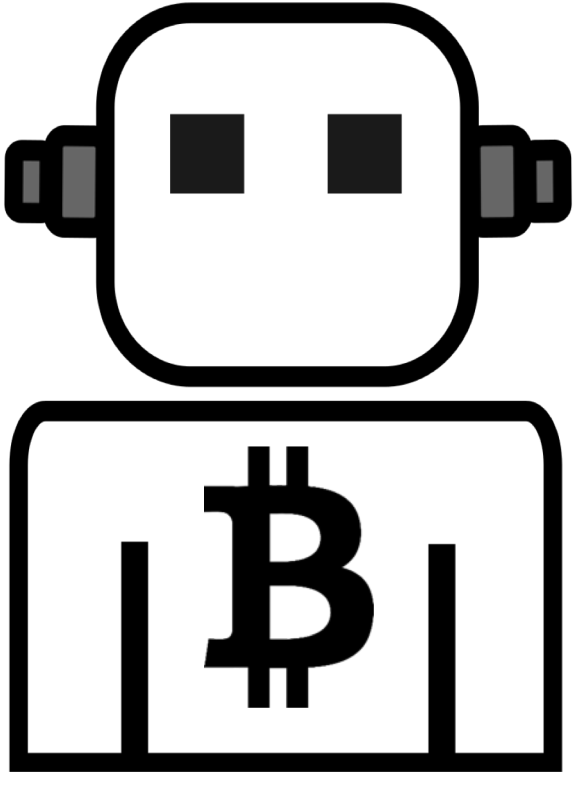
Alternative: Permissioned System



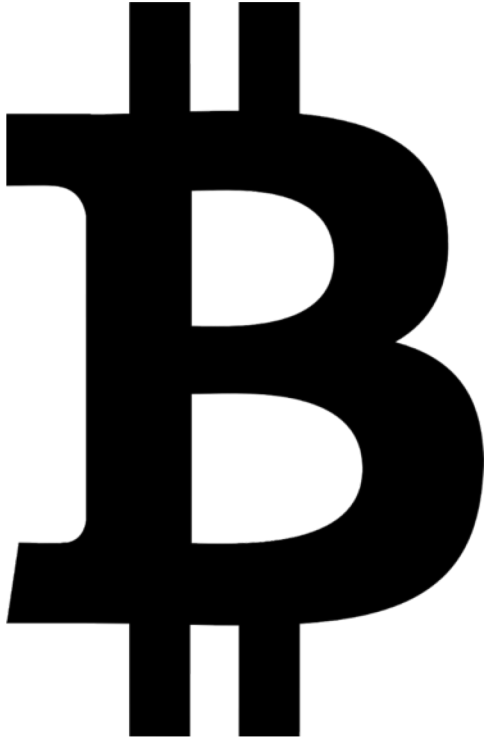
Result: “Immutable,” Distributed Ledger



“Programmable” Currency



The First Digital Asset



“Smart Contracts”

Data Veracity

Beating the Tragedy of the Commons

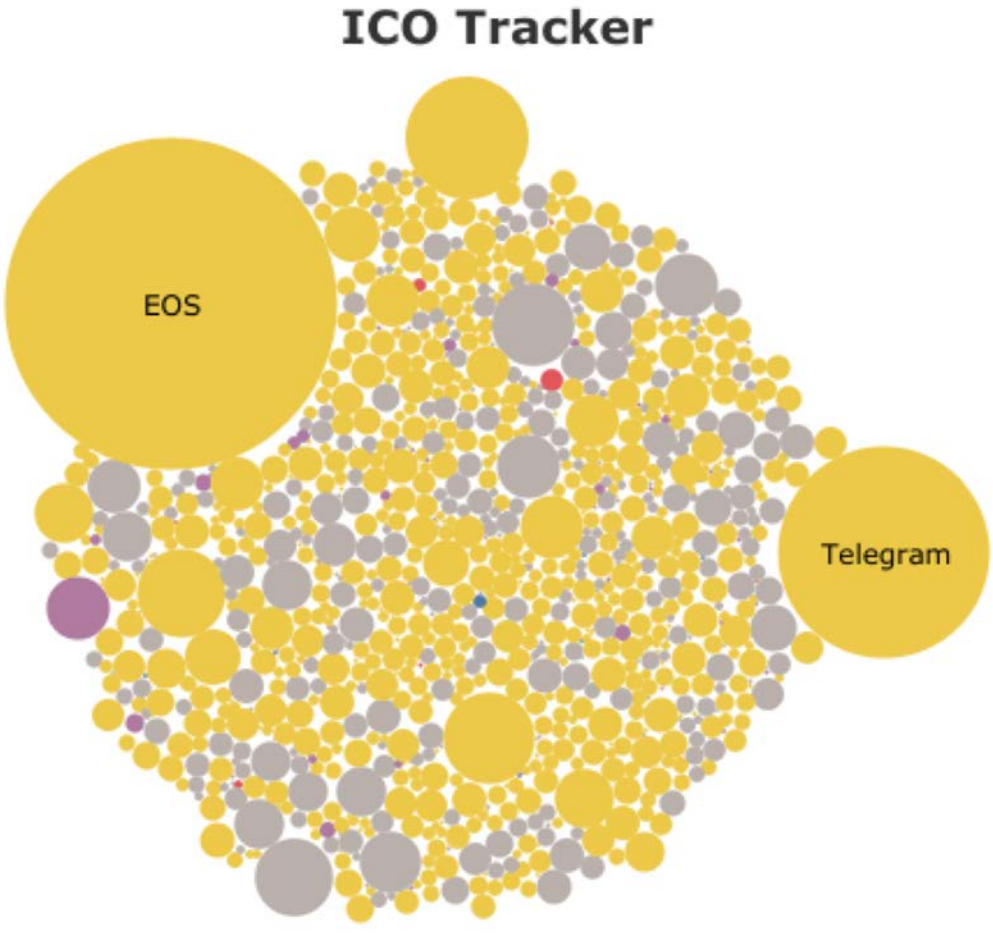
The First Use Case

Other Use Cases

- ICOs and STOs
- Real-time securities trade settlement
- Supply chain management
- Trade finance
- Middleman-free marketing
- A transactional Internet of Things
- Property rights: trusted title, fractional usage
- Green investments: self-made carbon credits
- Identity
- Non-fungible tokens and digital scarcity

ICOS: Bypassing Regulated Capital Markets?

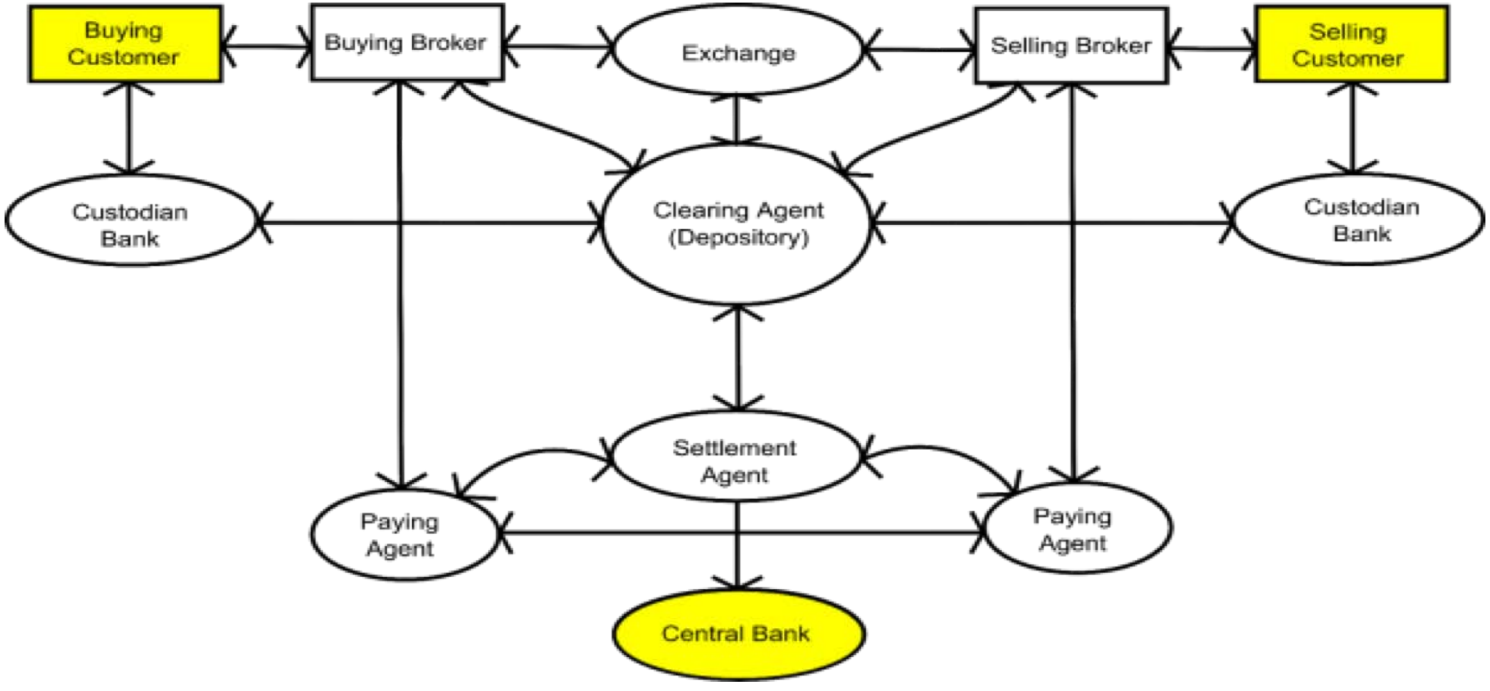
A Market for Ideas



Source: CoinDesk

STOs: Tokenizing regulated markets

Real-Time Trade Settlement



Source: Brave New Coin

From this…

To this…

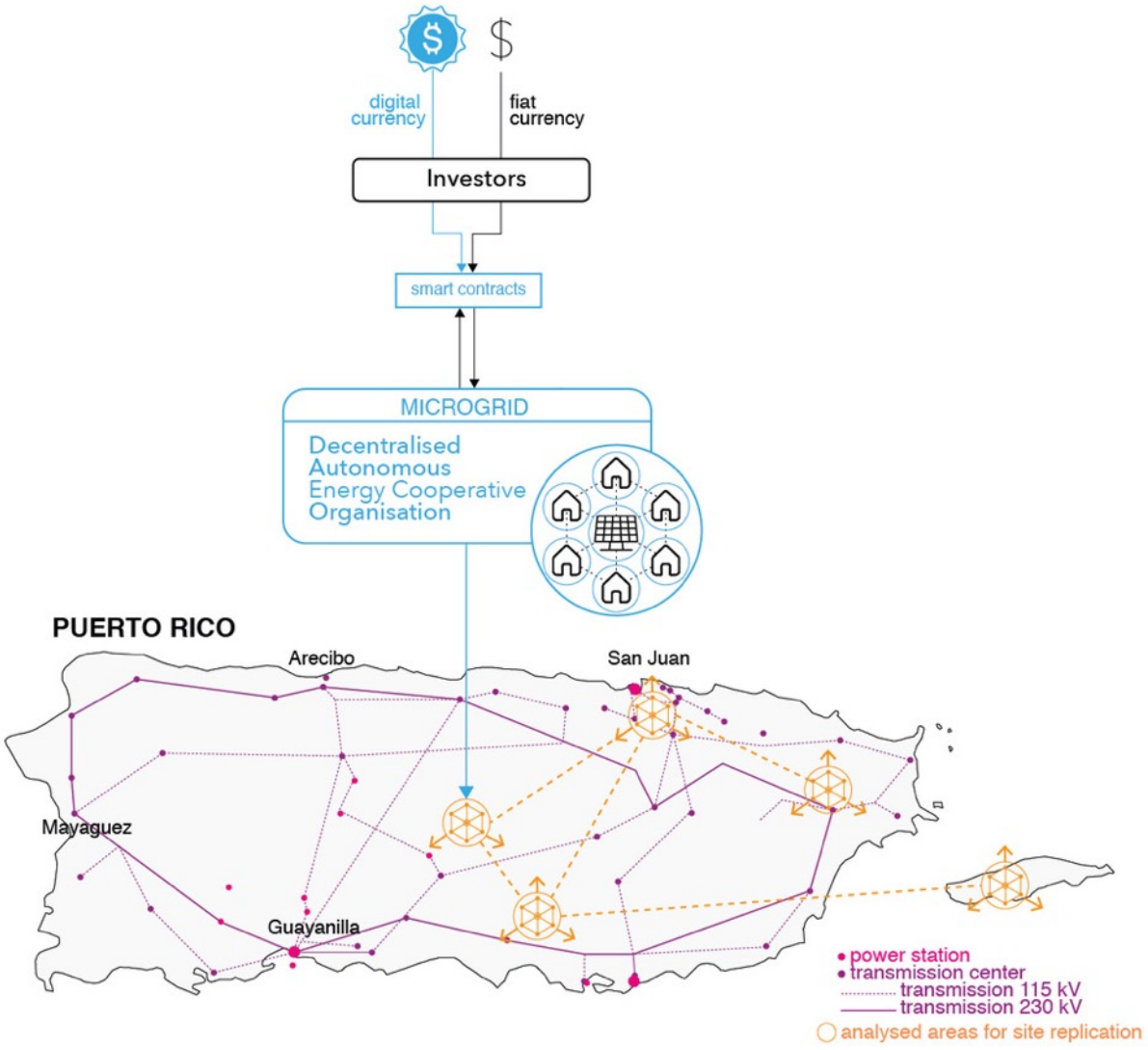
Supply Chain Management

The Provenance Problem

Innovative Trade Finance


IOT: M2M Transactions


Trusted
Property Title



Decentralized project finance

Green investments:

Self-made carbon credits

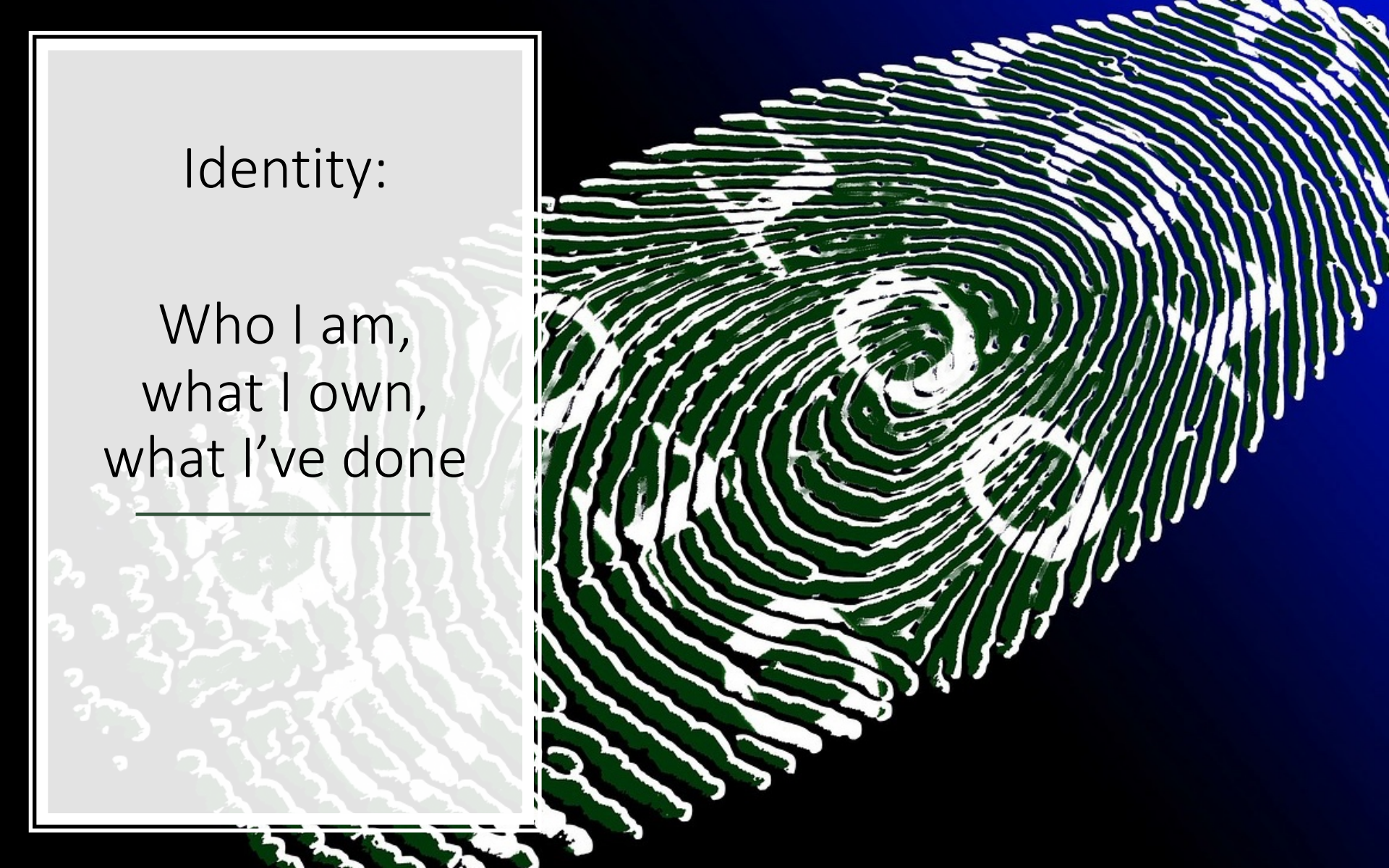
Creative work provenance:

Royalty management,

copyright registration

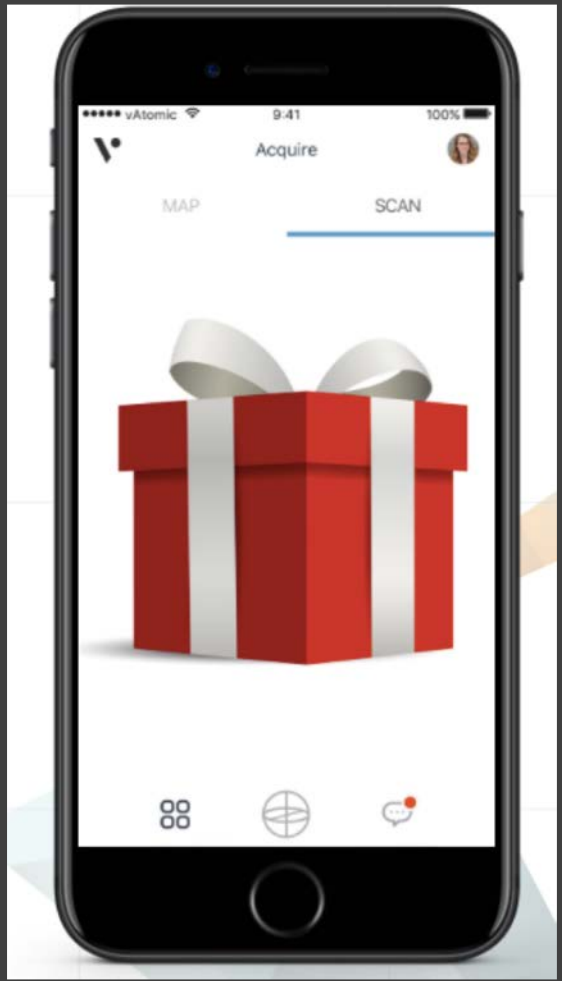
Identity:

Who I am,
what I own,
what I've done



The Token Economy:

Non-fungible tokens, digital scarcity, and a new system of value



Bubble or Boom?

Lessons from 1999

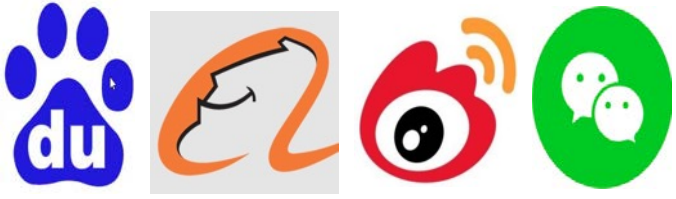
Bubble or Boom?

amazon

Lessons from 1999

The OTHER Lesson from 1999

G. A. F. A



B. A. W. T

Can We Do It Right This Time?

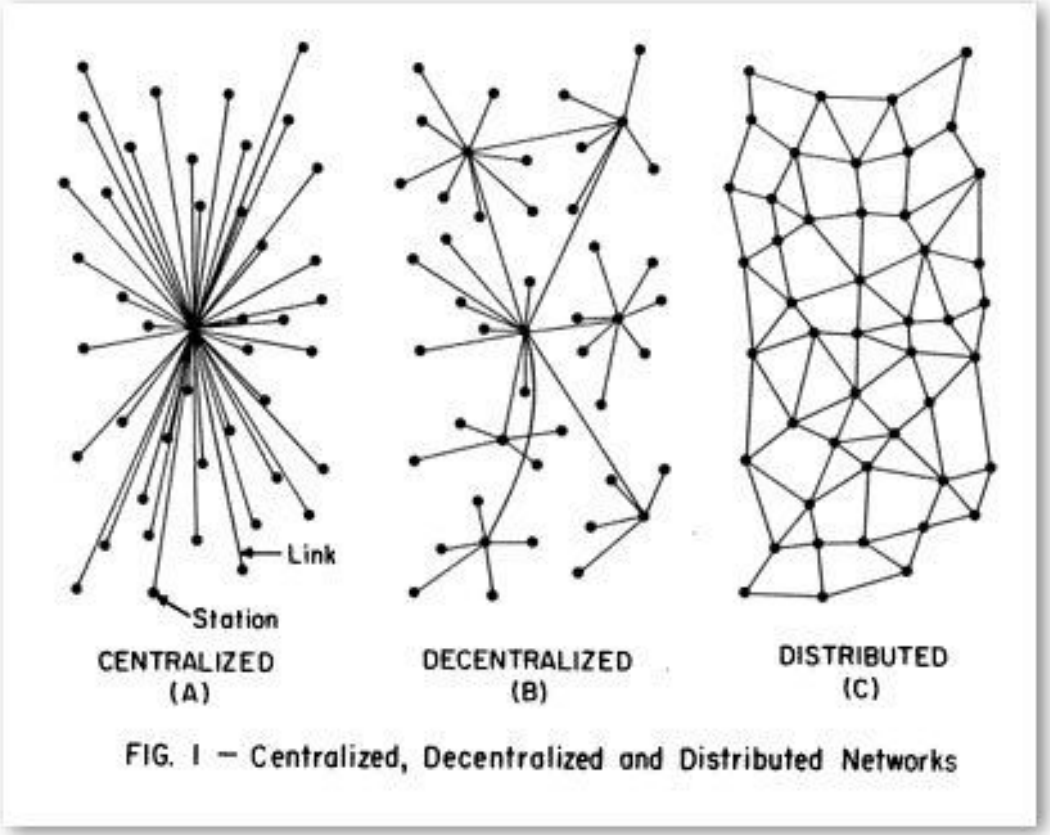


FIG. 1 — Centralized, Decentralized and Distributed Networks

Challenges

- Scaling. (A trust/governance problem, not just technical.)
- UX. (Ease of use. How do I store my keys?)
- Coordination. (Herding cats.)
- Regulation. (Square peg meets round hole.)
- Self-regulation. (Lots of growing up still needed)
- Redefining trust boundaries. (Trust enabling, not trustless)

So, do I need a blockchain?

So, do I need a blockchain?

You mean, do WE need a blockchain?

OK, do we need a blockchain?

OK, do we need a blockchain?

Answer: What is the cost of trust?

www.michaeljcasey.com

caseymj@media.mit.edu

@mikejcasey