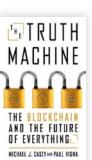
THE TRUTH MACHINE: The Blockchain and the Future of Everything

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."



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

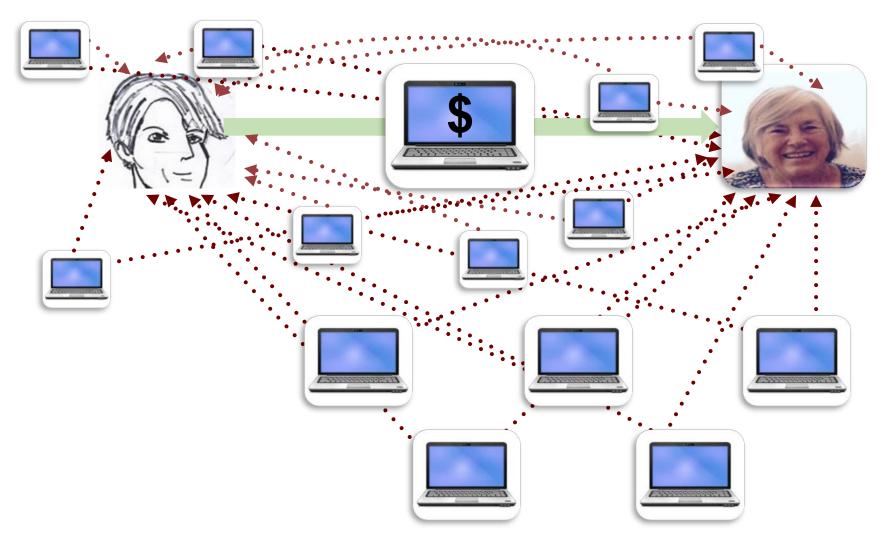




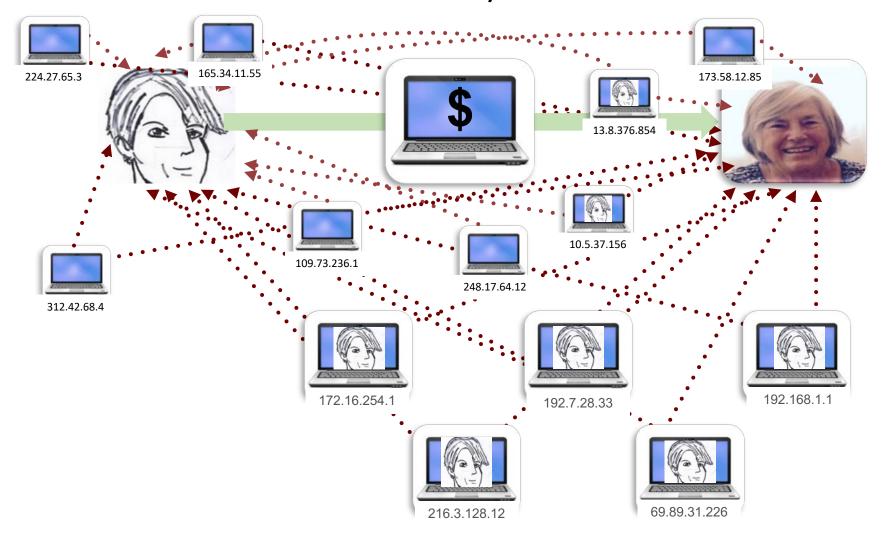
Problem 1: Double-Spending



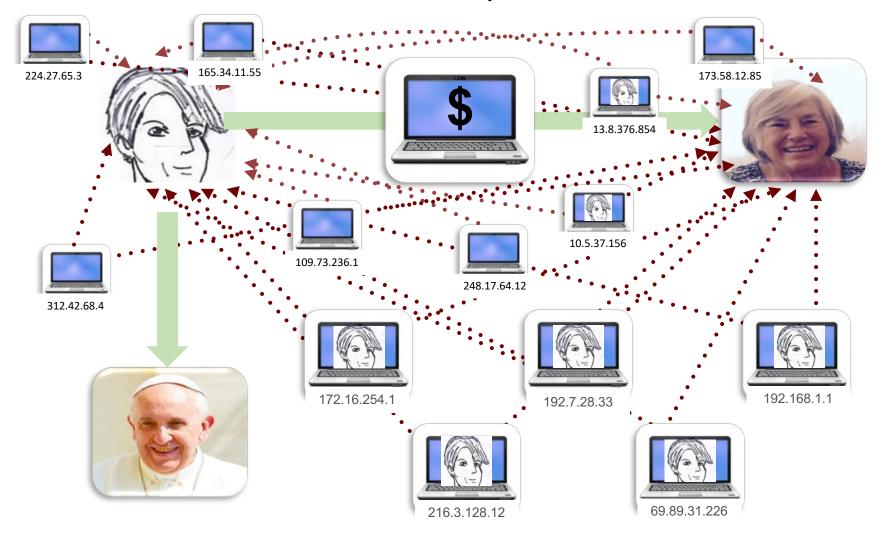
Solution: Consensus?

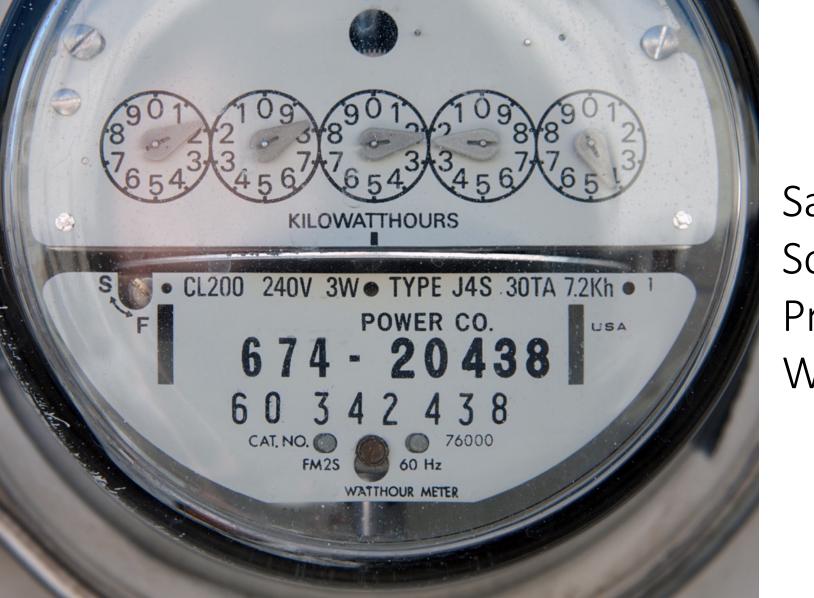


Problem 2: Sybil Attacks



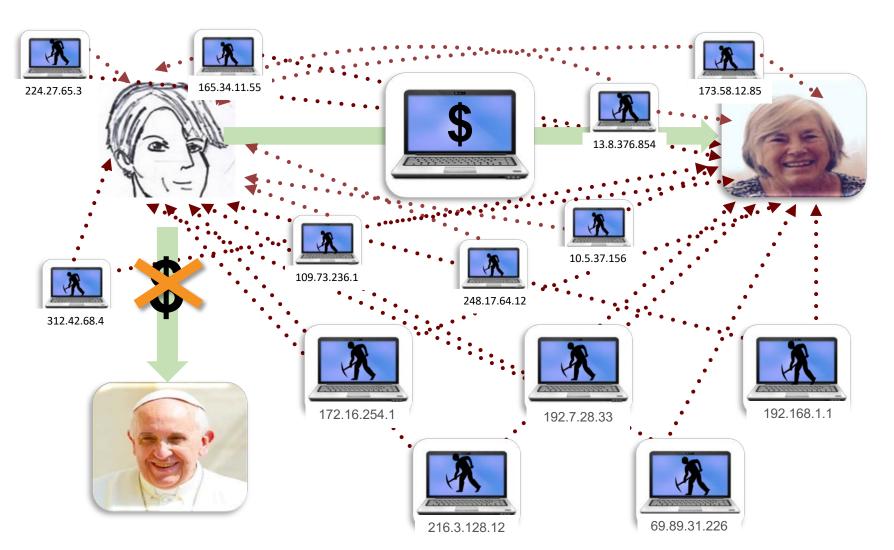
Problem 2: Sybil Attacks



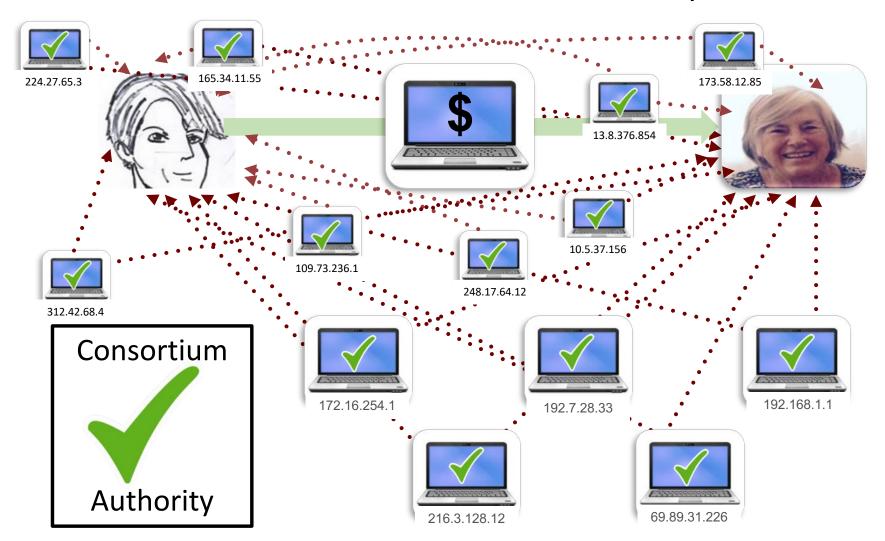


Satoshi's Solution: Proof of Work

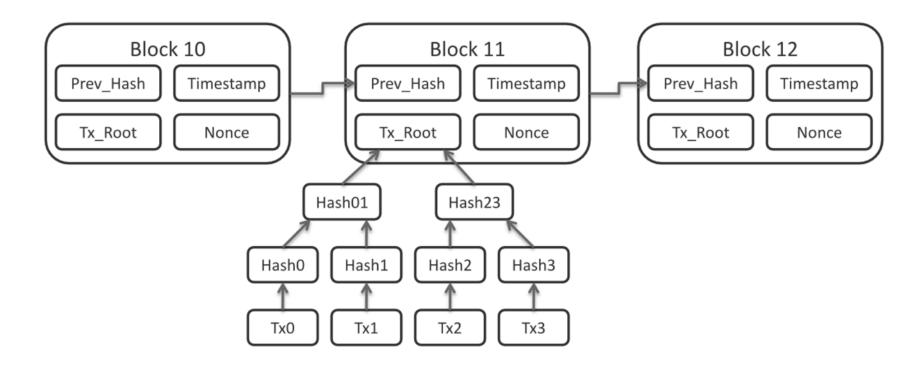
Solution: Permissionless Consensus



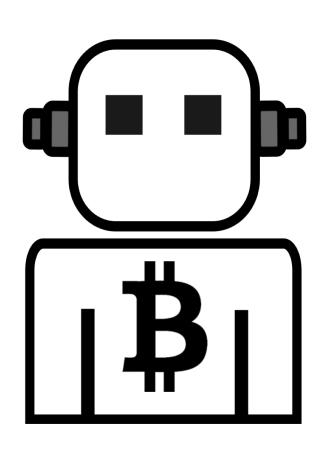
Alternative: Permissioned System



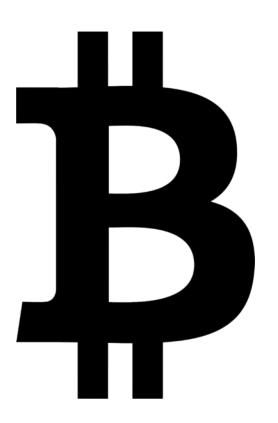
Result: "Immutable," Distributed Ledger



"Programmable" Currency



The First Digital Asset



"Smart Contracts"



```
ata("target");if(d||(d=b.attr("href"),d=d&&d.replace(/.*(?=#[^\
                             %e.bs.tab",{relatedTarget:b[0]}),g=a.Event("show.bs.tab",{relat
                             h-a(d); this.activate(b.closest("li"),c), this.activate(h,h.pare
                             >s.tab*,relatedTarget:e[0]})})}}},c.prototype.activate=function
                             lass("active").end().find('[data-toggle="tab"]').attr("aria-e>
                             b[0].offsetWidth,b.addClass("in")):b.removeClass("fade"),b.par
                             e="tab"]').attr("aria-expanded",!0),e&&e()}var g=d.find("> .ac
                             de").length);g.length&&h?g.one("bsTransitionEnd",f).emulateTr.
                             .tab=b,a.fn.tab.Constructor=c,a.fn.tab.noConflict=function(){
                             on("click.bs.tab.data-api", '[data-toggle="tab"]',e).on("click
Data
                             b(b){return this.each(function(){var d=a(this),e=d.data("bs.a
                             var c=function(b,d){this.options=a.extend({},c.DEFAULTS,d),th
Veracity
                             Position, this)).on("click.bs.affix.data-api",a.proxy(this.ch
                             et=null,this.checkPosition()};c.VERSION="3.3.7",c.RESET="aff:
                             :,d){var e=this.$target.scrollTop(),f=this.$element.offset(),
                             ed)return null!=c?!(e+this.unpin<=f.top)&&"bottom":!(e+g<=a-
                            !!=d&&i+j>=a-d&&"bottom"},c.prototype.getPinnedOffset=functi
                             ffix");var a=this.$target.scrollTop(),b=this.$element.offset
                            on(){setTimeout(a.proxy(this.checkPosition this) 411
```

strict"; function b(b){return this.each(runction(){voi

ion(b){this.element=a(b)};c.VERSION="3.3.7",c.TRANSITION_DURATI







Other Use Cases

ICOs and STOs

Real-time securities trade settlement

Supply chain management

Trade finance

Middleman-free marketing

A transactional Internet of Things

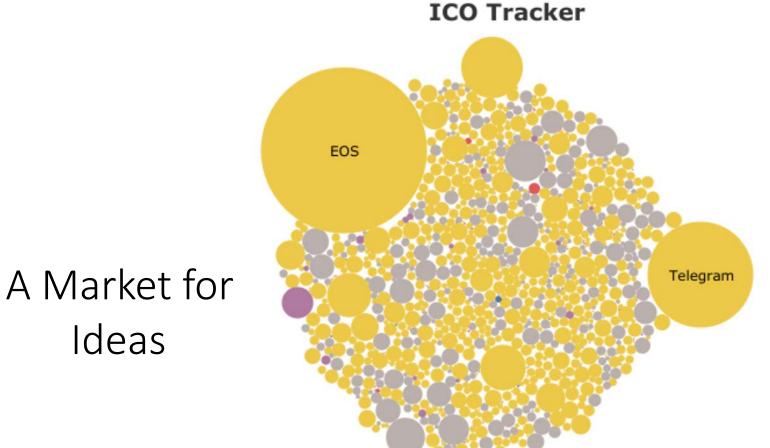
Property rights: trusted title, fractional usage

Green investments: self-made carbon credits

Identity

Non-fungible tokens and digital scarcity

ICOS: Bypassing Regulated Capital Markets?



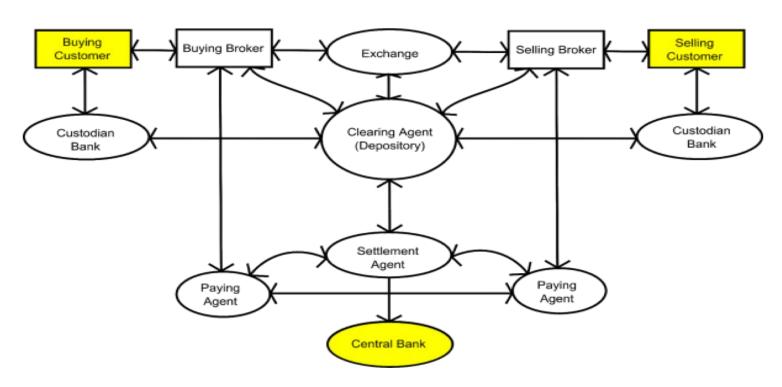
Source: CoinDesk

Ideas

STOs: Tokenizing regulated markets



Real-Time Trade Settlement



Source: Brave New Coin

From this...

To this...





Supply Chain Management

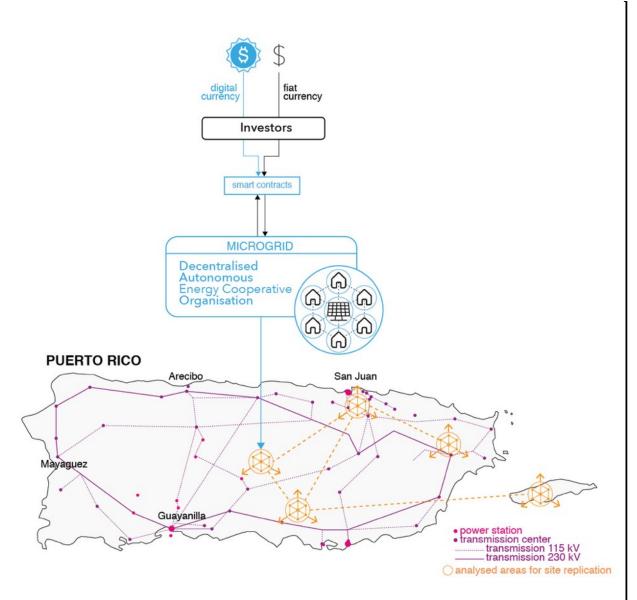
The Provenance Problem

Innovative Trade Finance









Decentralized project finance

Green investments:

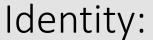
Self-made carbon credits





Creative work provenance:

Royalty management, copyright registration

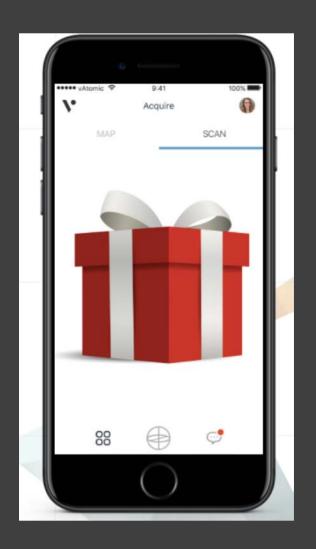


Who I am, what I own, what I've done



The Token Economy:

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



Bubble or Boom?





Lessons from 1999

Bubble or Boom?





Lessons from 1999

The OTHER Lesson from 1999

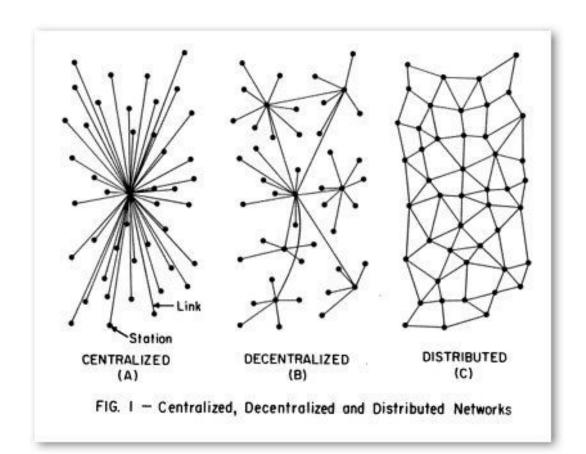


G. A. F. A



B. A. W. T

Can We Do It Right This Time?



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



