

STRĀTUMN

CRYPTO
NIGHTS
Nº2

DECENTRALIZATION DILEMMA

ANU JD AS GUPTA


—
12.07.2018

Definitions




Trust.

The willingness to allow someone else to “make decisions on your behalf”,
based on the belief that your interests will not be harmed.



Trustlessness.

The willingness to allow someone else to “make decisions on your behalf”,
as long as they have the interests of the entire network as a whole.



AND they are not mutually exclusive.

Trustlessness \neq Decentralized

“A lot of people automatically dismiss e-currency as a lost cause [...] it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we’re trying a **decentralized, non-trust-based** system.”

Satoshi Nakamoto

<http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493>

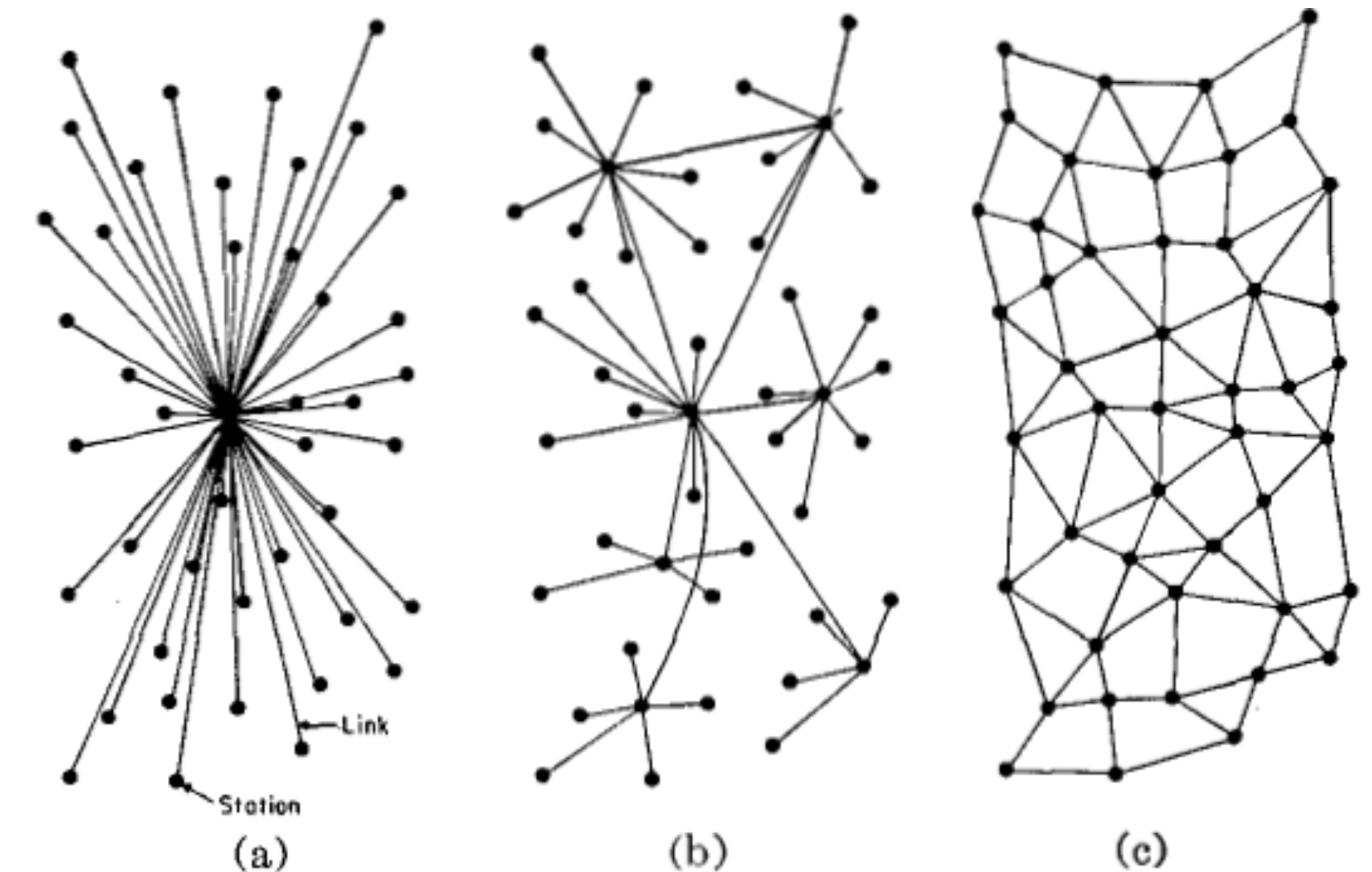


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

<i>Tends towards</i>	Centralization	Decentralization
Trustlessness	Green/Teal Orgs	Blockchains
Trustedness	Trad Corps	Direct Democracy

(de)Centralization is a topological category – w.r.t. networks.
Trust(lessness) is an economic category – w.r.t. delegation of decision making.

In a blockchain based system



There are Rules that everybody agrees to



Everybody ensures all rules are being followed



No one can decide on another's behalf unless it is in everyone's interest

Not all rules are created equal



A priori rules to be part of consensus rules.

E.g. Check nonce.

E.g. Check number of incoming vs outgoing coins per tx



The more interpretive a rule, the more it gets pushed to governance.

E.g. Blocksize debate, Tx rollback, Account recovery/lockup




Application specific rules gets pushed to ad-hoc scripts/programs.

E.g. BTC Scripts, ETH Smart Contracts

But all rules must be followed




Approvals over Agreements: Hierarchy of Agreements.
E.g. Deciding "To Fork or Not" depends on "Hack or Feature"
depends on "Intent-of-Code to be over Execution or not"



Verifying every operation to ensure all rules are being followed

- The cost of verification < the value gained by the verifier.
- The burden of proofs is on the verifiers, not provers.

Deciding for others: Fairness



No one should have stakes less than the value they provide

E.g. Monopoly rent.

–

Decision making powers should reflect the value distribution.

E.g. PoW winners provide more value than regular nodes, thus, they have the power to “get some new coins”

–

Not all nodes have the capacity to decide on all matters.

E.g. In Bitcoin mining, “comparatively” higher hash power has more “capacity”

In PoS, how have the block producers “earned” their stake is not clear, in contrast to PoW

The Paradox of Power Law: Fair but Unequal



Stateless (non-cumulative) coordination is more trustless.
But cumulative integrity (hashChain) helps converge on the canonical data.

You don't "gain" trust by solving PoW, every round you start your PoW from zero.

Think: One time ASICs > PoW > POS > DPoS

"trust no one", not "trust everyone collectively".



Making everyone equal, reduces the overall security.

Think: If everyone had the same number of ASICs.



Diversity of providers plus freedom of choice from consumers results in inequalities.

Think: Fashion, Free Market Brand Leaders.

Deciding for others: under competition



Can the customer get a better price elsewhere?

Monopsony < Oligopsony < Perfect Competition



Can the provider sell at a higher price?

Monopoly < Oligopoly < Perfect Competition

Deciding for others: under risk



The party who incurs the greater risk must be compensated
E.g. New brands price cheap.



Decision making power should always reflect the relative value-at-risk



The level of privilege of a node must be proportional
to the amount of risk it is insuring against.
E.g. ICO's must provide “acceptable” insurance measures or be banned

Trust (Decision-Making) Grid



Between providers and their customers,
does the decision-making power distribution
match its relative value-at-risk distribution?

- Yes = Fair
- No = Unfair

	Partnering btwn Providers	Fighting btwn Providers
Unfair w/ customers (Antitrust)	Collude	Coerce
Fair w/ customers	Collaborate	Compete

AND these are not mutually exclusive.

“decentralized, non-trust-based system”



Rules Engine

There are Rules that everybody agrees to
w.r.t.: consensus, governance, ad-hoc

Proof System

Everybody ensures all rules are being followed
by approving: verified operations only

Trustless Economics

No one can decide on another's behalf unless it is in everyone's interest
to ensure economic fairness under risk and competition



<i>Tends towards</i>	Centralization	Decentralization
Trustlessness	Ideal Free Market	PoW
Trustedness	Monopolies	DPoS, Browsers, BitTorrent, IPFS

Decentralization doesn't mean anything

(unless qualified with topological & economic specifics)


Decentralization Dilemma



**In order to form or fork or join a decentralized network,
centralization is required to achieve critical mass.**

Example

6 DNS Seeds for BTC act as coordination hubs.
Centralized "trackers" for BitTorrent, centralized "directories" for Tor.



**In an effort to maintain economic equilibrium,
networks oscillate between the topologies as they evolve.**

Think.

Escrows. Gov Bureaucracies. Mining Pools. ETH Classic. BTG Hack.
Weak Subjectivity. Identifying the "correct" BTC genesis block. Timestamping.

Thank you

