Lauro Gripa Neto

Blockchain and the cost of trust

MAGRATHEA LABS

www.magrathealabs.com

MAGRATHEA LABS

Lauro Gripa Neto
Software Engineer

lauro@magrathealabs.com laurogripa

THE NEED FOR TRUST

What's trust?

Definition

- trustor ➜ trustee
- directed to the future
- abandonment of control over trustee
- uncertainty and risk of failure or harm

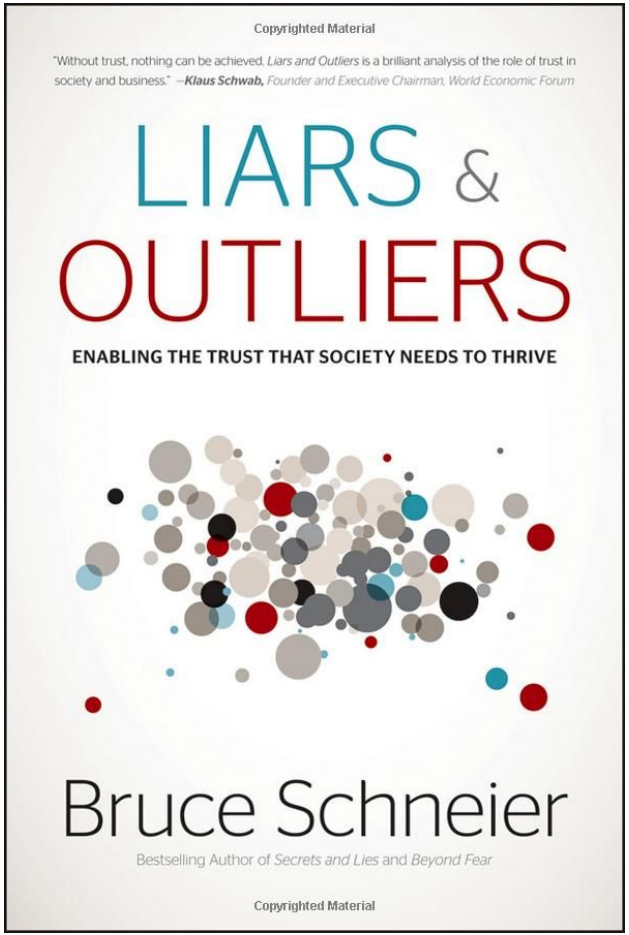
Aspects

- belief in:
  - honesty
  - fairness
  - benevolence

What's trust?

General trust systems

- Morals
- Reputation
- Institutions
- Security Systems



Morality

Reputation

Institutions and contracts

Security Systems

The Cost of Trust

The Cost of Trust: A Pilot Study

Sinclair Davidson[1]
Mikayla Novak[2]
Jason Potts[3]

This version 24 July 2018

Abstract: Trust is a fundamental precondition underpinning exchange and economic coordination between heterogeneous agents, but is costly to maintain. Given the potential for agents to enjoy zero-sum gains by opportunistically betraying the trust of exchanging counterparties, an edifice of occupational roles, organisational forms and institutional practices have emerged in an effort to uphold trustworthy behaviour and conduct. In simple terms, there exists a "cost of trust" and this cost is non-trivial for a highly specialised economy operating at an increasingly global scale. This paper provides numerical estimates of the cost of trust for the United States economy, based on an attribution of labour force occupational data with varying degrees of trust-maintenance. Occupations which are represented in high cost-of-trust activities include managers, lawyers and judges, tax professionals, accountants and auditors. Overall, it is estimated that the cost of trust accounts for 35 per cent of U.S. employment in 2010. The cost of trust has significant implications for the economic applicability of distributed ledger technologies, such as blockchain, compared with conventional forms of ledger technology largely maintained by centralised third-party organisations.

Keywords: blockchain; measurement; opportunism; transaction costs; trust.

JEL codes: D02, J21, K42, O33, Z13

---

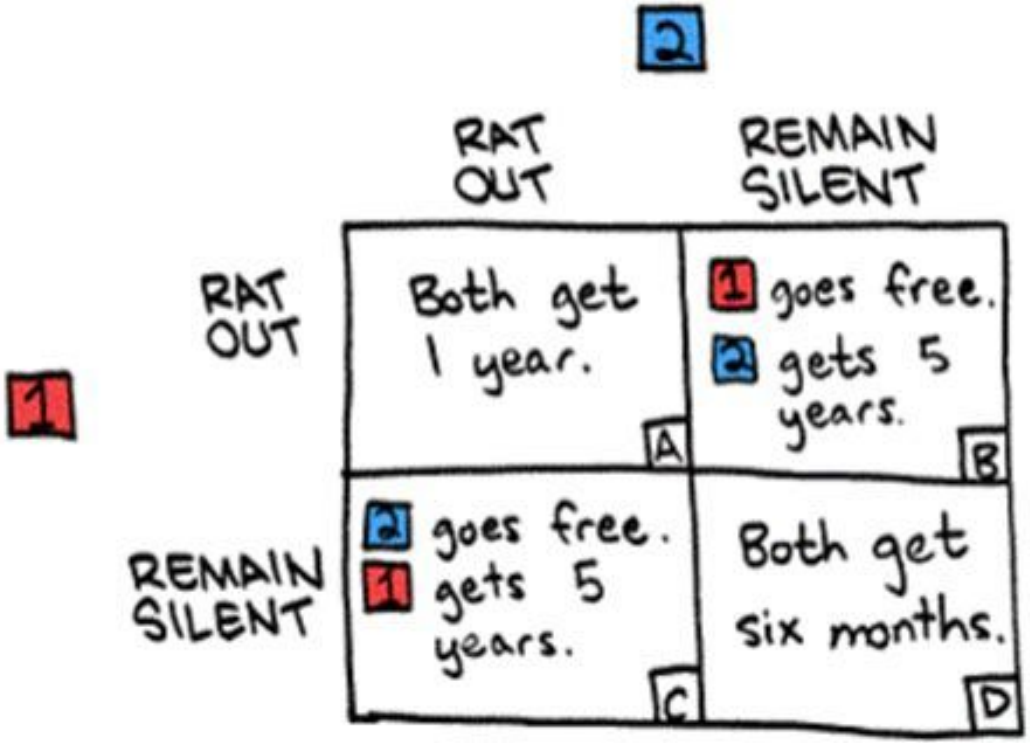
[1] Professor of Institutional Economics and Fellow, Blockchain Innovation Hub, RMIT University, Melbourne, Australia. Email: sinclair.davidson@rmit.edu.au
[2] Postdoctoral Research Fellow, Blockchain Innovation Hub, RMIT University, Melbourne, Australia. Email: mikayla.novak@rmit.edu.au

The Cost of Trust: $29 TRILLIONS

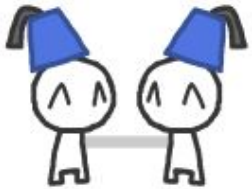

THE
EVOLUTION
OF TRUST
playing time: 30 min • by nicky case, july 2017
PLAY →

Game Theory

Prisoner's Dilemma

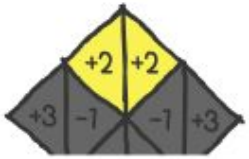


Game theory has shown us the three things we need for the evolution of trust:



1. REPEAT INTERACTIONS

Trust keeps a relationship going, but you need the knowledge of possible future repeat interactions *before* trust can evolve.



2. POSSIBLE WIN-WINS

You must be playing a non-zero-sum game, a game where it's at least possible that *both* players can be better off -- a win-win.

3. LOW MISCOMMUNICATION

If the level of miscommunication is *too* high, trust breaks down. But when there's a little bit of miscommunication, it pays to be *more* forgiving.

The Evolution of Trust

In the **short run** we are influenced by our environment

In the **long run** our environment is affected by us

source: https://ncase.me/trust/

ENTERS THE BLOCKCHAIN


What’s a market?

The need for a currency

- Medium of exchange
- Unit of account
- Store of value

The "Double-spending" problem

"**Double-spending** is the result of successfully spending some money more than once."

Combating Double-Spending Using Cooperative P2P Systems

4
Author(s)

Ivan Osipkov ; Eugene Y. Vasserman ; Nicholas Hopper ; Yongdae Kim

View All Authors

Abstract:
An electronic cash system allows users to withdraw coins, represented as bit strings, from a bank or broker, and spend those coins anonymously at participating merchants, so that the broker cannot link spent coins to the user who withdraws them. A variety of schemes with various security properties have been proposed for this purpose, but because strings of bits are inherently copyable, they must all deal with the problem of double-spending. In this paper, we present an electronic cash scheme that introduces a new peer-to-peer system architecture to prevent double-spending without requiring an on-line trusted party or tamper-resistant software or hardware. The scheme is easy to implement, computationally efficient, and provably secure. To demonstrate this, we report on a proof-of-concept implementation for Internet vendors along with a detailed complexity analysis and selected security proofs.

Published in: Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference on

Date of Conference: 25-27 June 2007

Date Added to IEEE *Xplore*: 09 July 2007

CD-ROM ISBN: 0-7695-2837-3

Print ISSN: 1063-6927

INSPEC Accession Number: 10290180

DOI: 10.1109/ICDCS.2007.91

Publisher: IEEE

Conference Location: Toronto, ON, Canada

source: http://ieeexplore.ieee.org/document/4268195/

Distributed Double Spending Prevention*

Jaap-Henk Hoepman

TNO Information and Communication Technology
P.O. Box 1416, 9701 BK Groningen, The Netherlands
jaap-henk.hoepman@tno.nl
and
Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, the Netherlands
jhh@cs.ru.nl

Abstract. We study the problem of *preventing* double spending in electronic payment schemes in a *distributed* fashion. This problem occurs, for instance, when the spending of electronic coins needs to be controlled by a large collection of nodes (e.g., in a peer-to-peer (P2P) system) instead of one central bank. Contrary to the commonly held belief that this is fundamentally impossible, we propose several solutions that do achieve a reasonable level of double spending prevention, and analyse their efficiency under varying assumptions.

1 Introduction

Many electronic payment schemes exist. For an overview, we refer to Asokan *et al.* [AJSW97] or O'Mahony *et al.* [OPT97]. Some of those are coin based, where some bitstring locally stored by a user represents a certain fixed value.

Coin based systems run the risk that many copies of the same bitstring are spent at different merchants. Therefore, these systems need to incorporate *double spending* prevention or detection techniques. To *prevent* double spending, a central bank is usually assumed which is involved in each and every transaction. In off-line scenarios (where such a connection to a central bank is not available), double spending *detection* techniques are used that will discover double spending at some later time, and that allow one to find the perpetrator of this illegal activity. A major drawback of double spending detection techniques is the risk that a dishonest user spends a single coin a million times in a short period of time before being detected. This is especially a problem if such a user cannot be punished for such behaviour afterwards, e.g., fined, penalised judicially, or being kicked from the system permanently.

* This research is/was partially supported by the research program Sentinels (www.sentinels.nl), project JASON (NIT.6677). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.
Id: double-spending.tex 18 2008-02-06 14:01:34Z jhh

source: https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

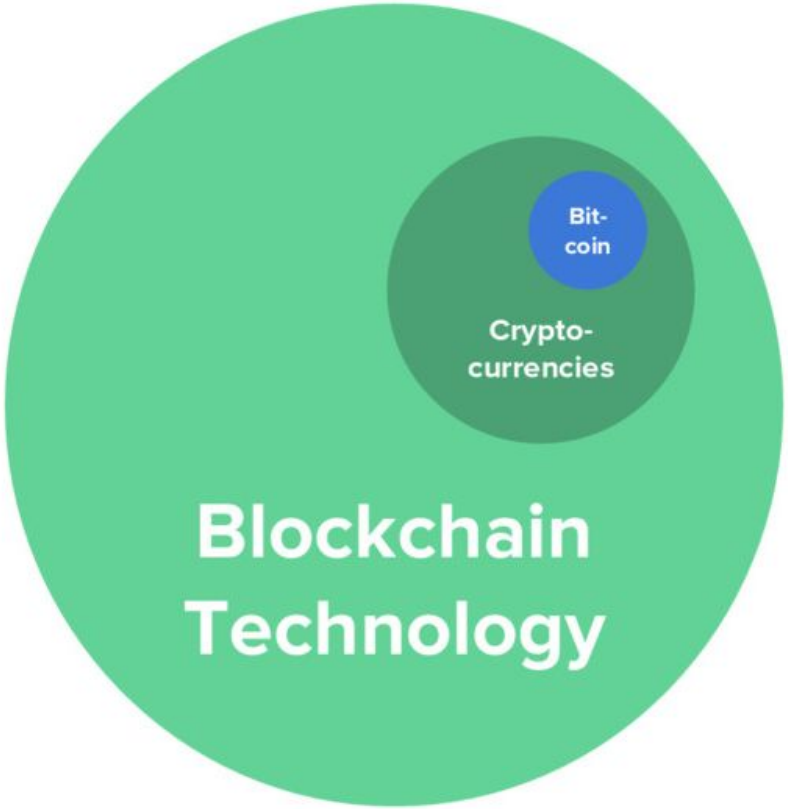
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

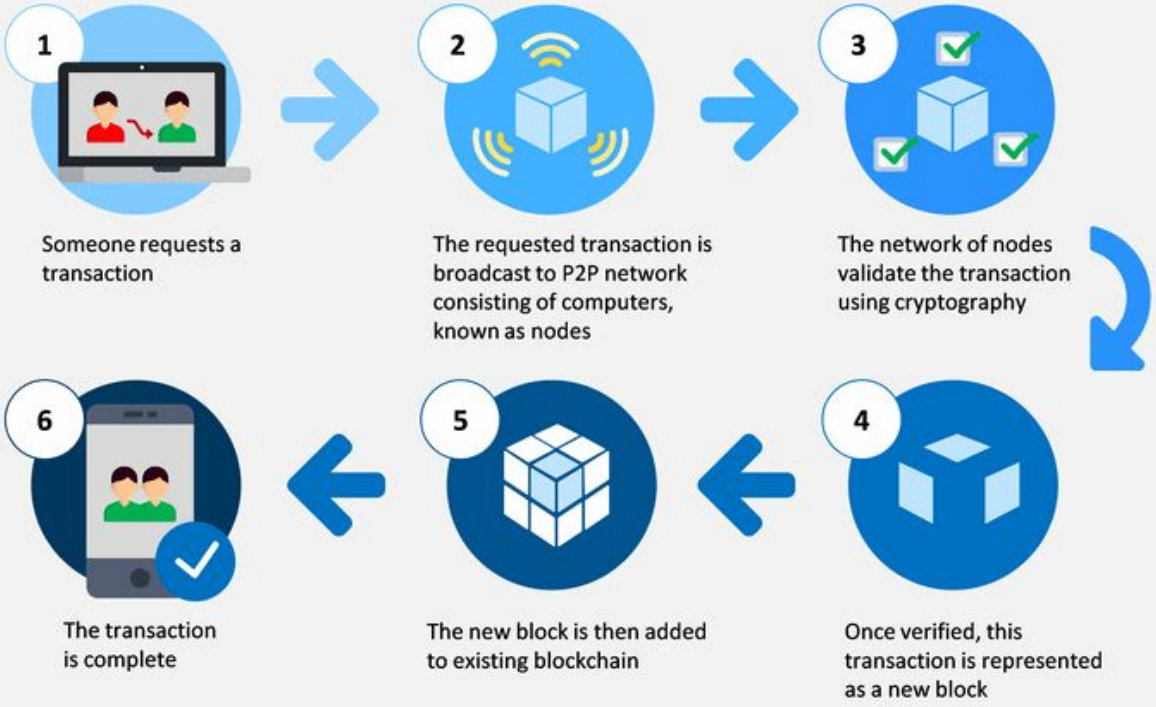
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

BITCOIN ≠ BLOCKCHAIN


Bit-
coin
Crypto-
currencies
Blockchain
Technology


1
Someone requests a transaction
2
The requested transaction is broadcast to P2P network consisting of computers, known as nodes
3
The network of nodes validate the transaction using cryptography
4
Once verified, this transaction is represented as a new block
5
The new block is then added to existing blockchain
6
The transaction is complete

GAME CHANGERS?

Ethereum

“Ethereum is a decentralized platform that runs smart contracts: **applications** that run exactly as programmed **without any possibility of downtime, censorship, fraud or third party interference**.”

source: https://ethereum.org/

Non-cooperative games ➜ Cooperative games

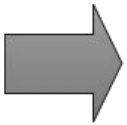
A \ B	Coop	Defect
Coop	1 / 1	2 / −3
Defect	−3 / 2	−1 / −1

Original Prisoners' Dilemma Game

+

A \ B	Coop	Defect
Coop	0 / 0	−1000 / 0
Defect	0 / −1000	−1000 / −1000

Ethereum contract of burning any player who chooses to defect



A \ B	Coop	Defect
Coop	1 / 1	−998 / −3
Defect	−3 / −998	−1000 / −1001

Composite Game

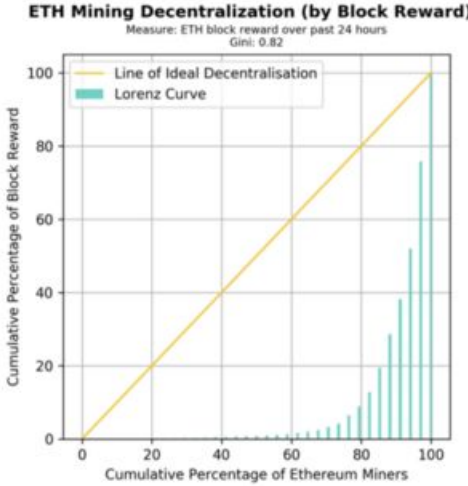
source: https://medium.com/@virgilgr/ethereum-is-game-changing-technology-literally-d67e01a01cf8

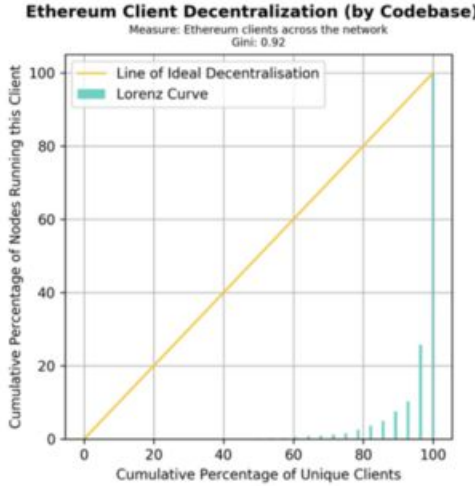
MAYBE NOT

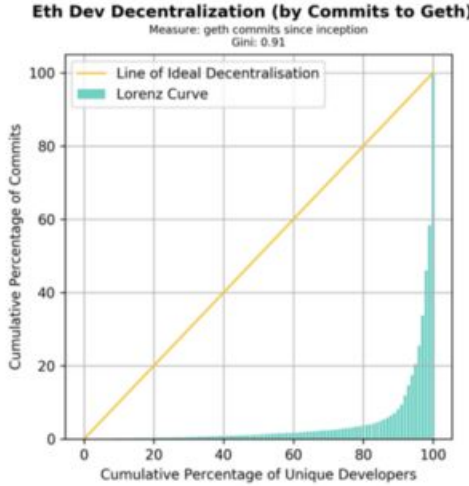
BRUCE SCHNEIER

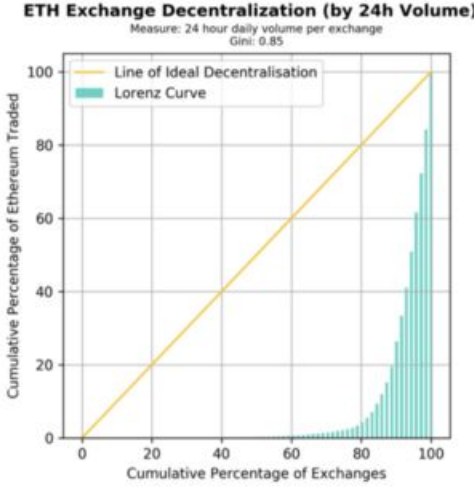
OPINION 02.06.2019 09:00 AM

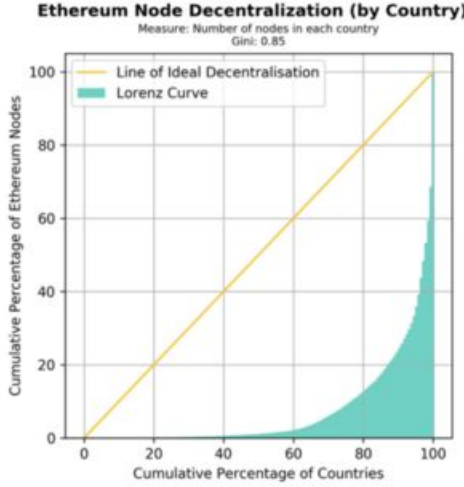
There's No Good Reason to Trust Blockchain Technology

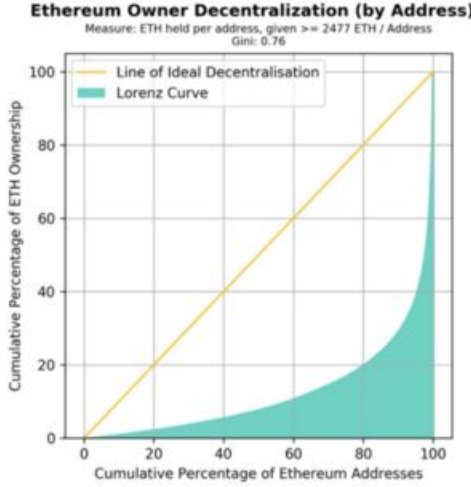

ETH Mining Decentralization (by Block Reward)
Measure: ETH block reward over past 24 hours
Gini: 0.82
Line of Ideal Decentralisation
Lorenz Curve
Cumulative Percentage of Block Reward
Cumulative Percentage of Ethereum Miners


Ethereum Client Decentralization (by Codebase)
Measure: Ethereum clients across the network
Gini: 0.92
Line of Ideal Decentralisation
Lorenz Curve
Cumulative Percentage of Nodes Running this Client
Cumulative Percentage of Unique Clients


Eth Dev Decentralization (by Commits to Geth)
Measure: geth commits since inception
Gini: 0.91
Line of Ideal Decentralisation
Lorenz Curve
Cumulative Percentage of Commits
Cumulative Percentage of Unique Developers

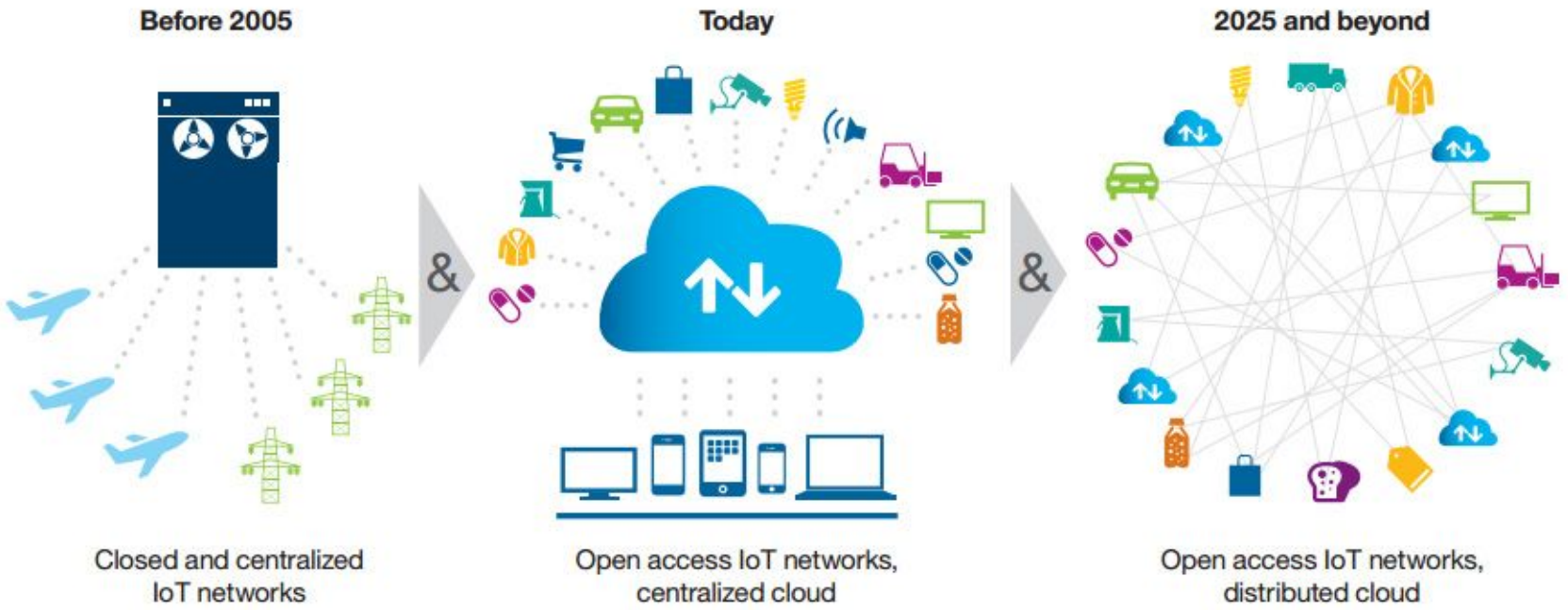

ETH Exchange Decentralization (by 24h Volume)
Measure: 24 hour daily volume per exchange
Gini: 0.85
Line of Ideal Decentralisation
Lorenz Curve
Cumulative Percentage of Ethereum Traded
Cumulative Percentage of Exchanges


Ethereum Node Decentralization (by Country)
Measure: Number of nodes in each country
Gini: 0.85
Line of Ideal Decentralisation
Lorenz Curve
Cumulative Percentage of Ethereum Nodes
Cumulative Percentage of Countries


Ethereum Owner Decentralization (by Address)
Measure: ETH held per address, given >= 2477 ETH / Address
Gini: 0.76
Line of Ideal Decentralisation
Lorenz Curve
Cumulative Percentage of ETH Ownership
Cumulative Percentage of Ethereum Addresses

BUT THERE'S HOPE

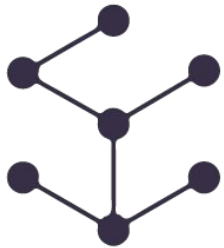
Self-sovereign identities



Questions?

MAGRATHEA LABS

www.magrathealabs.com



Blockchain Joinville

meetup.com/blockchain-joinville

MAGRATHEA LABS

www.magrathealabs.com
contact@magrathealabs.com

Thank you!

MAGRATHEA LABS

www.magrathealabs.com