Game Theoretic Challenges in Distributed Trust

John Augustine

"ReLaX" Workshop on Games

ReLaX Research Lab in Computer Science

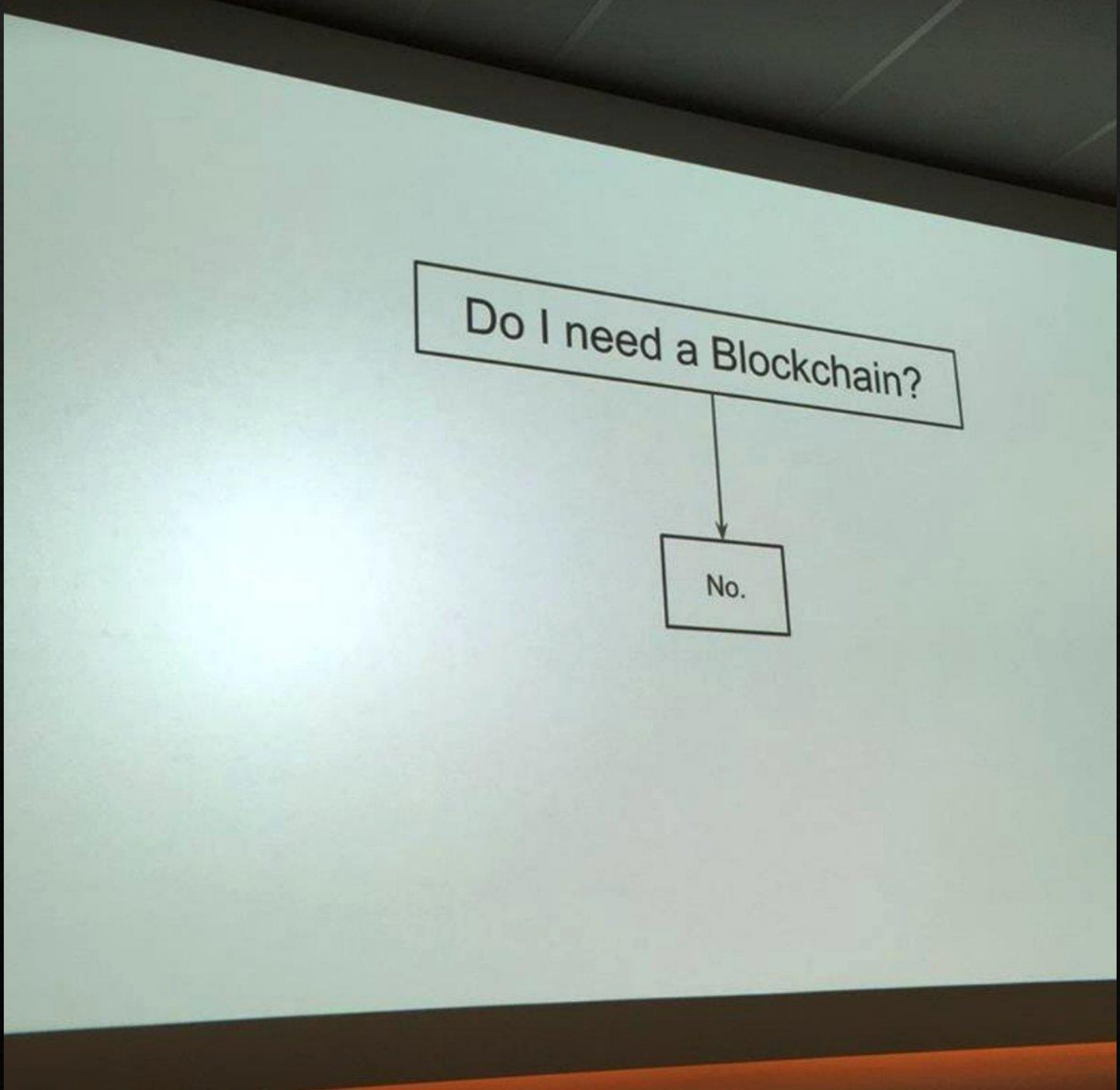
Chennai Mathematical Institute, February 1 - February 4, 2021

Cryptography, Cybersecurity and Distributed trust

CSE IITM

INDIAN INSTITUTE OF TECHNOLOGY MADRAS

सिद्धिर्भवति कर्मजा


Do I need a Blockchain?
No.

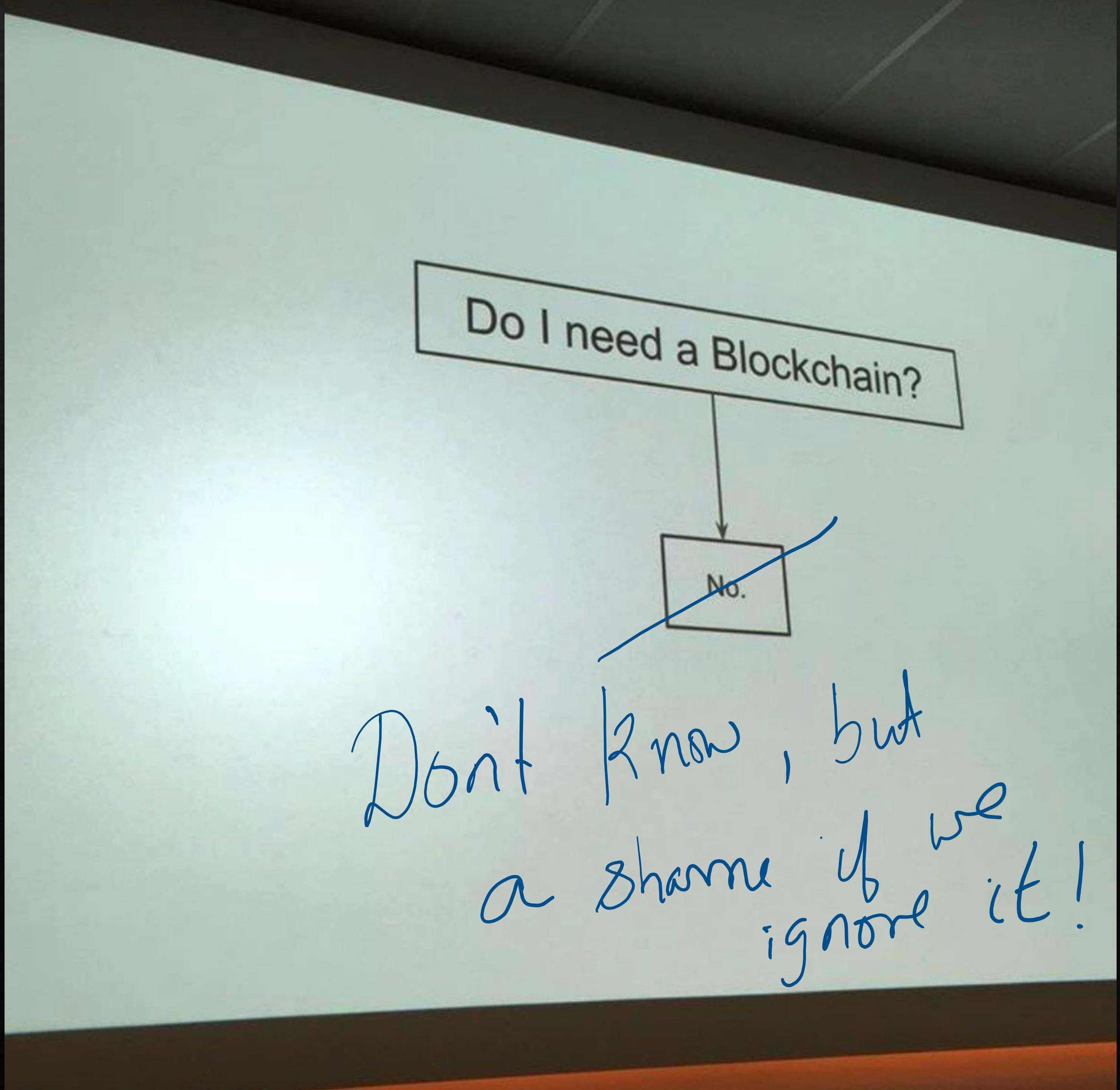
“

I think there's a world market for maybe five computers

”

(Allegedly by) Thomas Watson, Chairman & CEO of IBM

Circa 1943


Do I need a Blockchain?
No.
Don't know, but
a shame if we
ignore it!

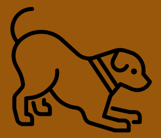

Overview

01

BLOCKCHAIN AND DISTRIBUTED TRUST

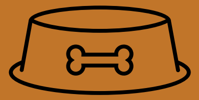
02

THE MINING GAME



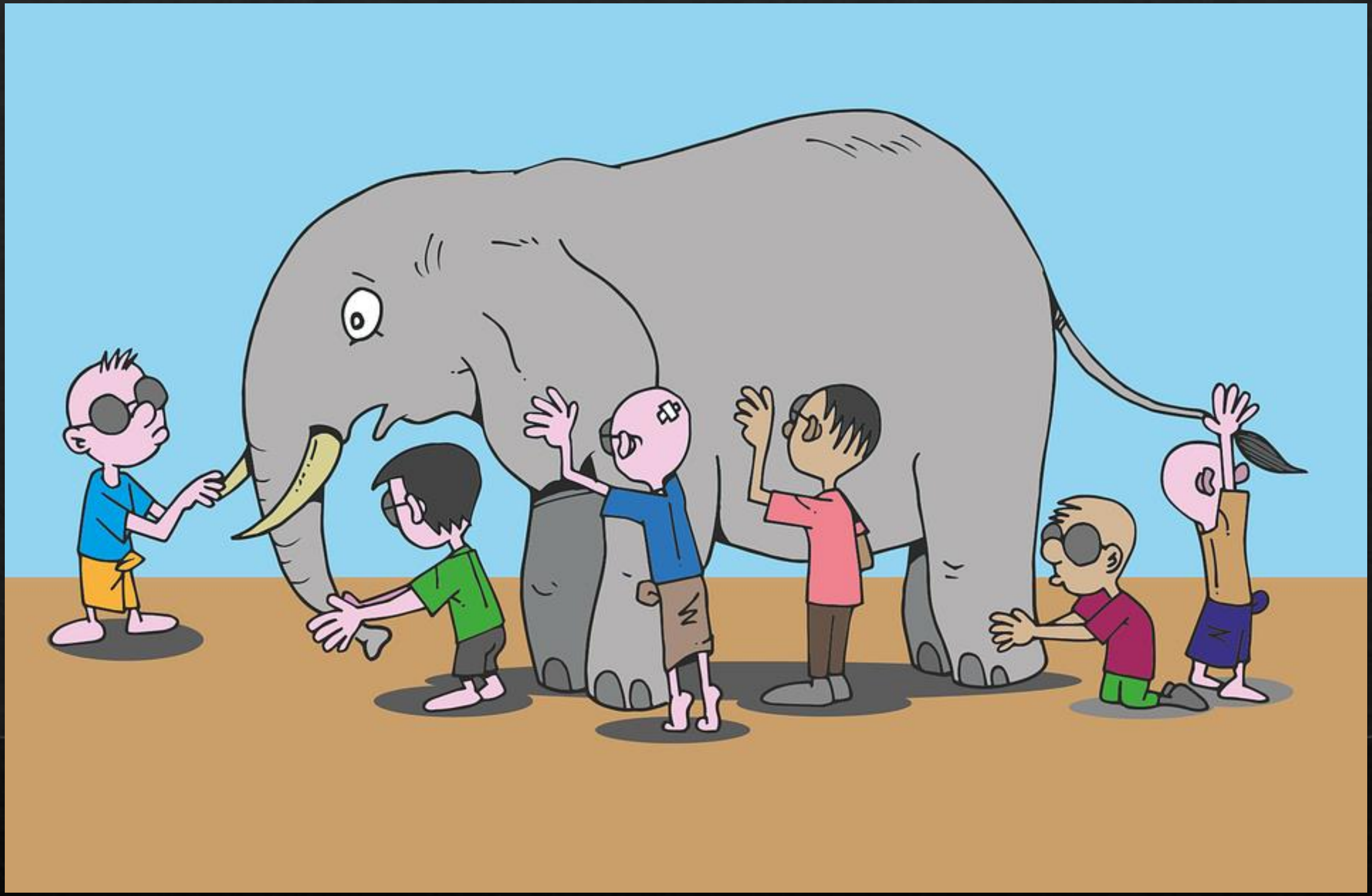
03

THE POOL GAME

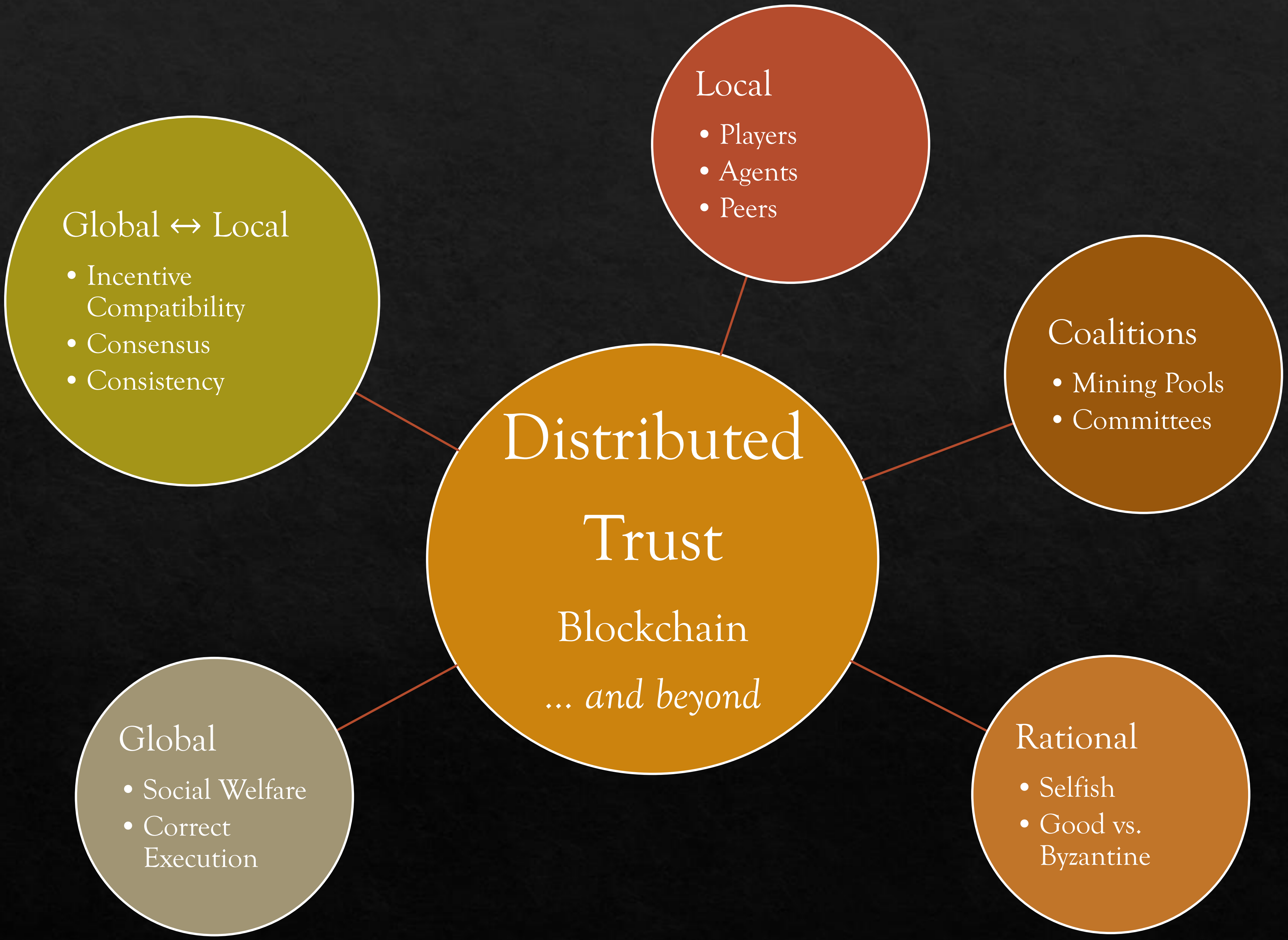


04

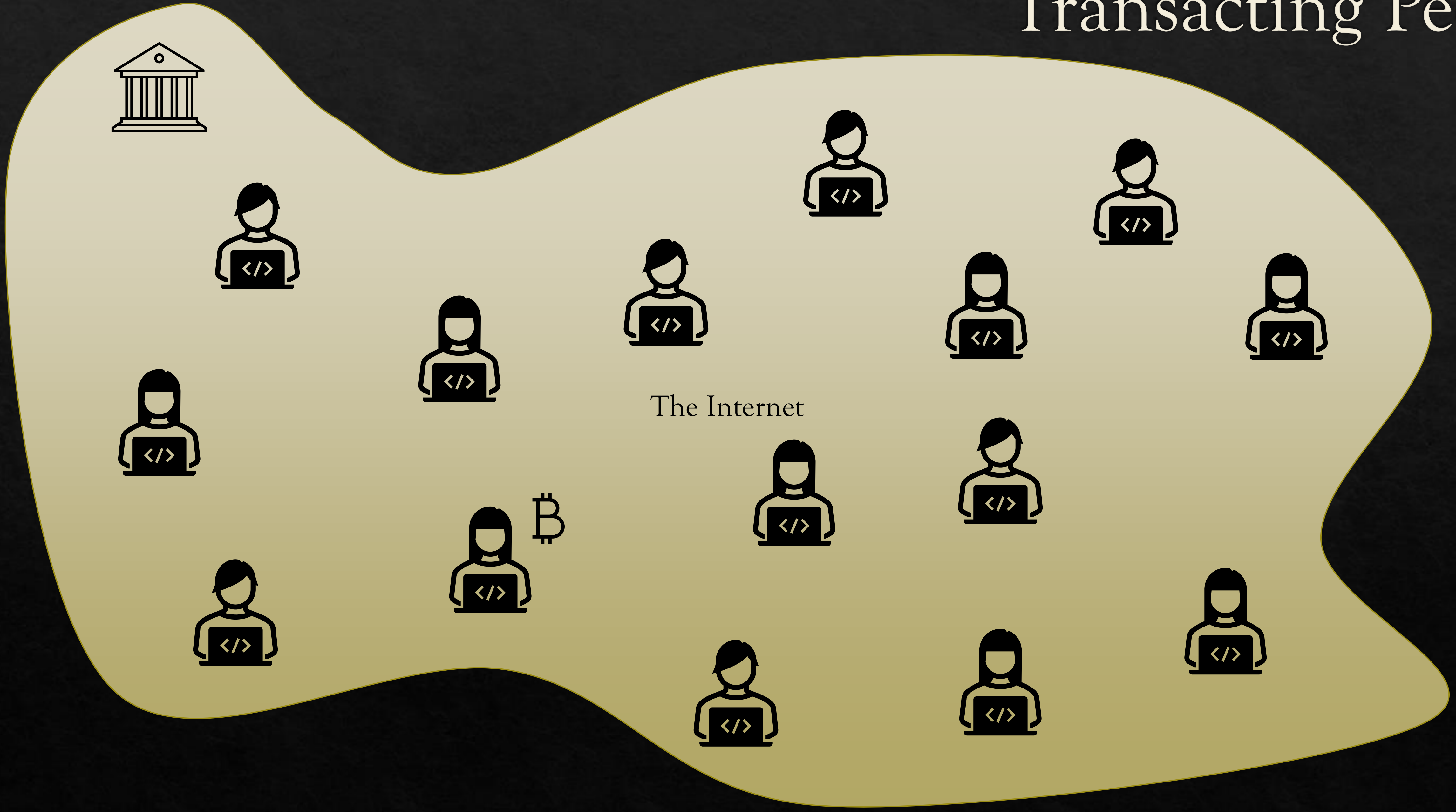
SOME GENERAL THOUGHTS



The Elephant and the Blindfolded Children


Distributed
Trust
Blockchain
... and beyond
Local
• Players
• Agents
• Peers
Coalitions
• Mining Pools
• Committees
Rational
• Selfish
• Good vs. Byzantine
Global
• Social Welfare
• Correct Execution
Global ↔ Local
• Incentive Compatibility
• Consensus
• Consistency

Transacting Peers



A Ledger of Transactions

No central Authority

Anonymity & Confidentiality

Consistent
Everybody sees the same

No Double Spending

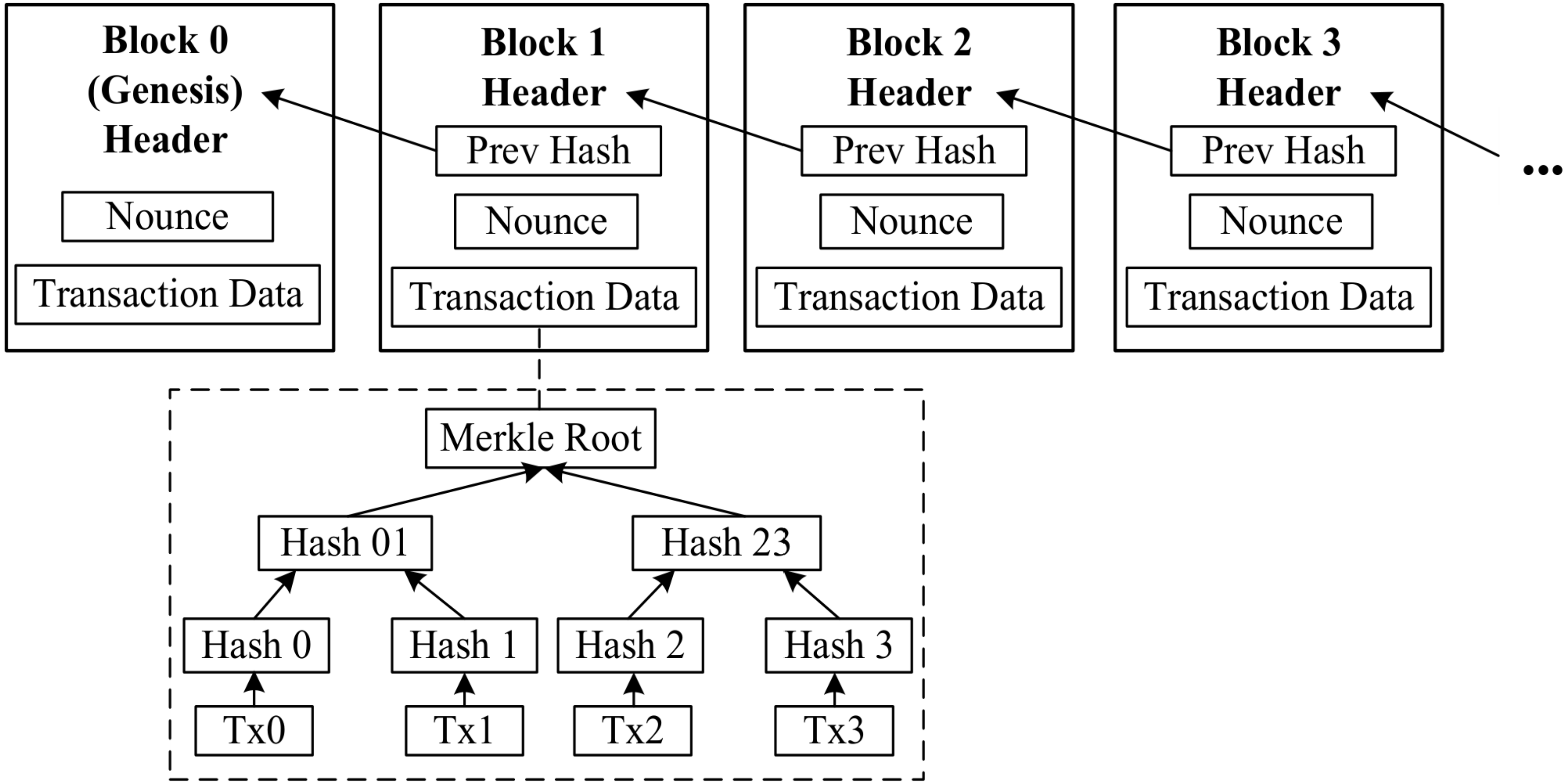
Integrity of Transactions

Ease and Availability

Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain.
ACM Comput. Surv. 52, 3, Article 51 (July 2019)

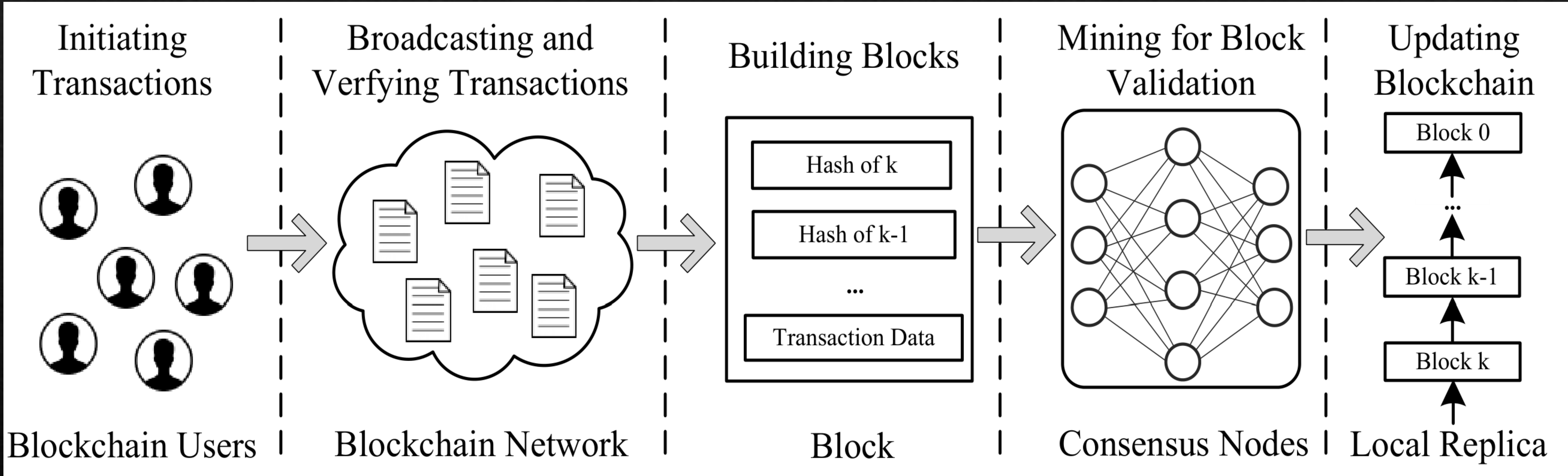
The Blockchain System

A brief primer



An illustrative example of blockchain data structure where the transactions are included in the block and the block is represented by a merkle root.

Figure taken from:
Z. Liu *et al*., "A Survey on Blockchain: A Game Theoretical Perspective," in *IEEE Access*, vol. 7, pp. 47615-47643, 2019



An overview of the blockchain workflow.

Figure taken from:
Z. Liu *et al*., "A Survey on Blockchain: A Game Theoretical Perspective,"
in *IEEE Access*, vol. 7, pp. 47615-47643, 2019

The Mining Game

Where to Mine in a Forked World?

- Kiayias, Koutsoupias, Kyropoulou, and Tselekounis
- EC 2016

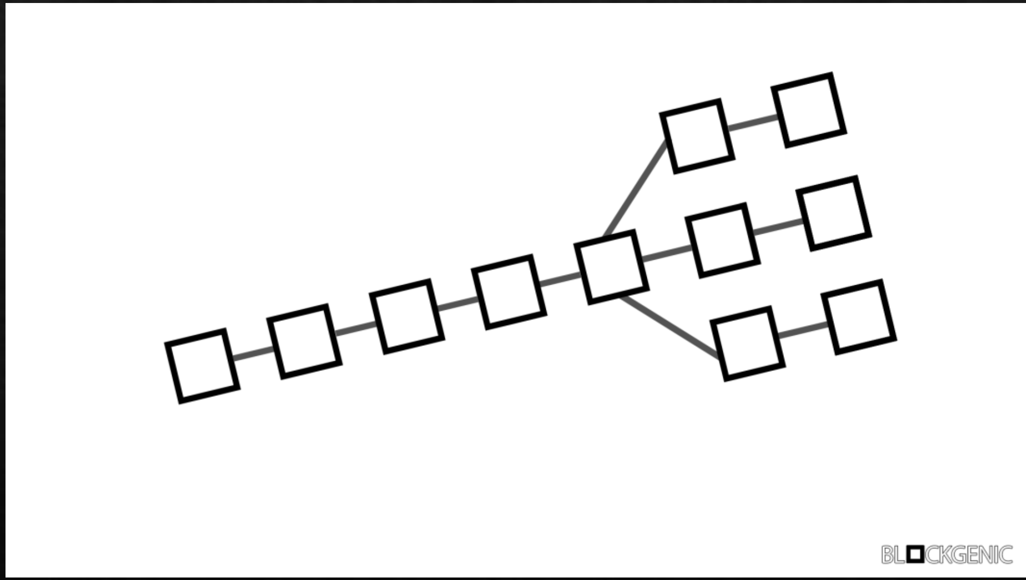


Figure from: https://medium.com/@blockgenic/blockchain-forks-explained-17f22efbf5d3

Why do forks appear?

- Inadvertently when multiple miners mine blocks in parallel
- Frontier Strategy (proposed by Nakamoto): Mine on the longest chain

- Strategically to increase the number of blocks mined → our focus.
- Maliciously to double spend → Not our focus.

When is Frontier no longer optimal?

The Mining Game

- Stochastic Game
- States are rooted trees (represents the blockchain; root is the genesis block)
- Players are the n miners.
- Strategy set: nodes in the state
- Probability of solving puzzle: $p_1, p_2, \dots, p_n$.
  - Assume one winner per round.
  - $\sum_i p_i = 1$
- Variants: Immediate Release or Strategic Release

Immediate Release Variant

- When a miner succeeds,
  - the block is released and is part of the state.
  - State is always common knowledge

- Theorem: Frontier is a Nash Equilibrium when every miner has relative computational power $p_i \leq 0.361$.

- Theorem: When all other players play Frontier

  and $p_i \geq 0.455$

  Frontier is NOT player i's best response.

Strategic Release Variant

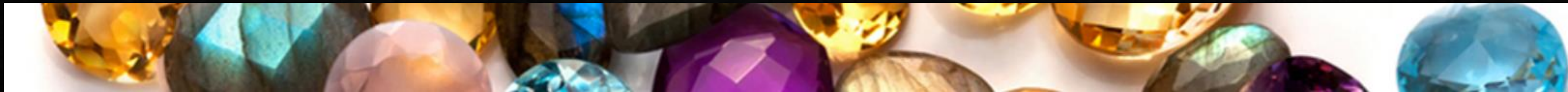
- When a miner i succeeds,
  - everyone knows she succeeded
  - Miner i can choose to postpone releasing the block
  - Consequence: others cannot mine from that block
- Unrealistic, but useful. [Miners can also hide success]

- Theorem: Frontier is a Nash equilibrium when $p_i \leq 0.308\ \forall i$. [Kiayias et al.]
- Theorem: ….. When $p_i \leq 0.329\ \forall i$. [Sapirstein et al.]

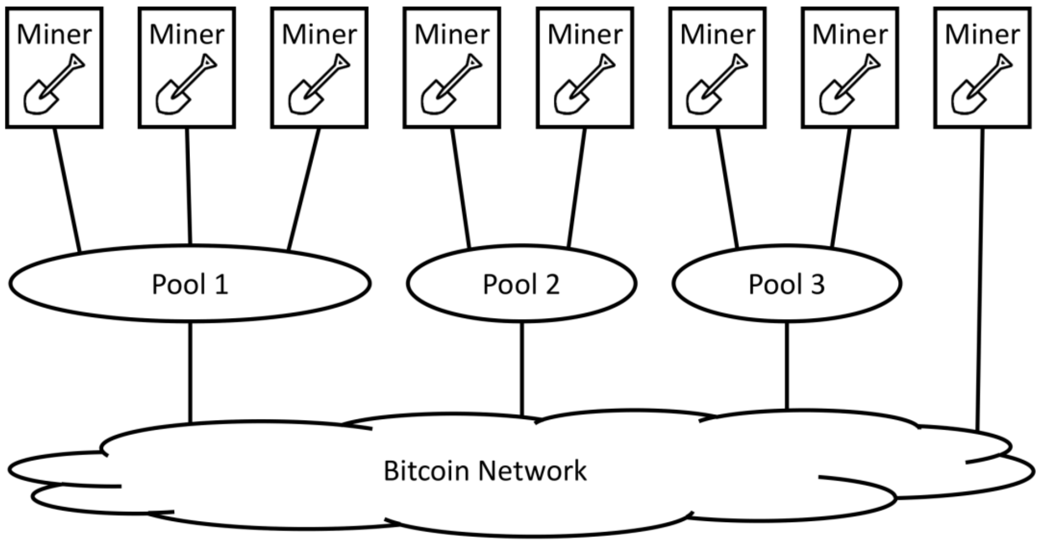
The Pool Game

Ittay Eyal

SSP (Oakland), 2015



Mining in Pools



A system with 8 miners and 3 honest pools. Pool 1 has 3 registered miners, pools 2 and 3 have 2 registered miners each, and one miner mines solo.

I. Eyal, "The Miner's Dilemma," *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, 2015, pp. 89-103

- Group of miners
- Share revenue
- Mitigate individual risk
- Open system – any peer welcome

- How to ensure fair payment for individual miners?
- Ans: allow partial proofs

Pool Block Withholding (PBWH) Attack

- Miners infiltrate pool
- Mine but only release partial solutions and withhold full proofs
- Revenue based on partial solutions
- Hard to detect because full proofs are rare.

- Pools can sabotage each other through PBWH

- An infiltrated pool
  - Can (statistically) sense the rate of infiltration, but
  - Cannot detect infiltrators

Two Pools Infiltrating Each Other

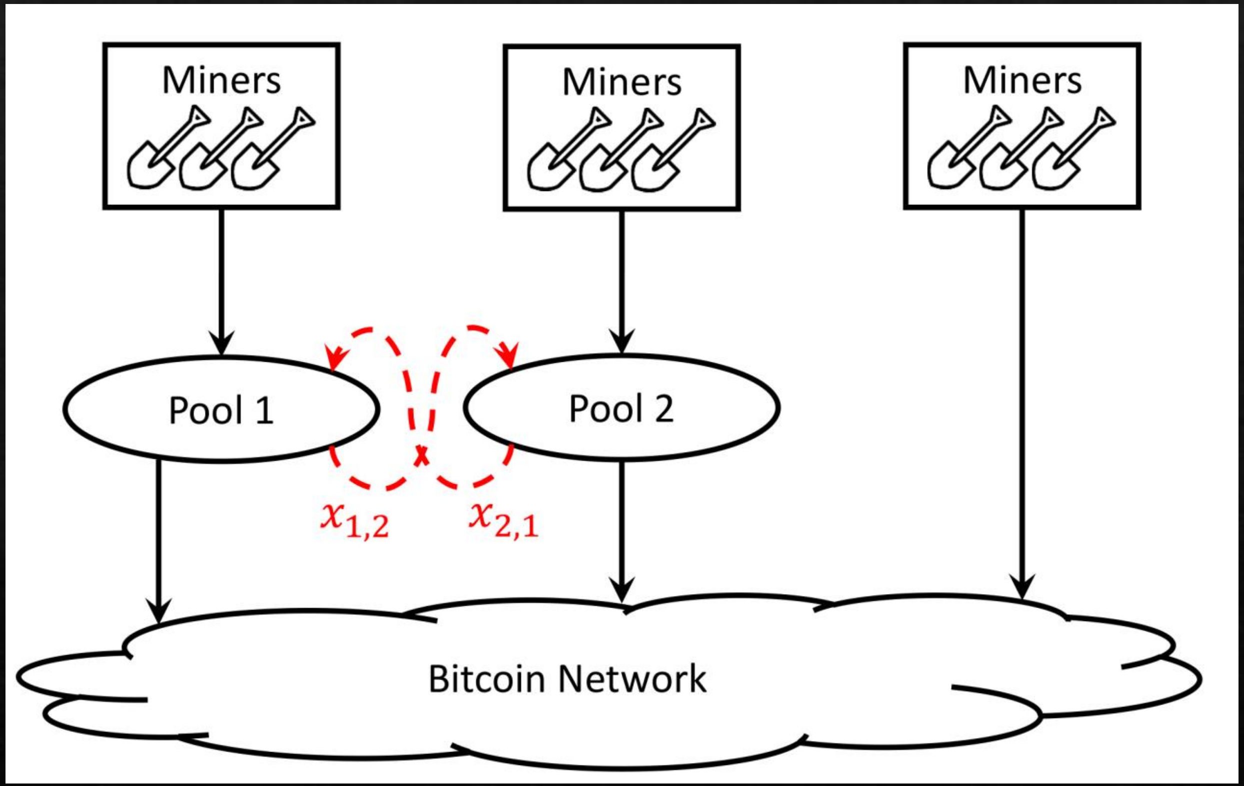


Figure from:
I. Eyal, "The Miner's Dilemma," *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, 2015, pp. 89-103

The Pool Game

- The goal is to model pools infiltrating each other
- Pools p_1 and p_2 (for simplicity).
  - Other miners exist, but do not interact with p_1 and p_2
- Strategy set: fraction of loyal peers infiltrating other pool
- Time in round (time taken for a unit of revenue earned)
- Each round, a pool (chosen via round robin) updates its infiltration rate.

Optimal Infiltration Rate for Pool 1 As a Function of Pool Size

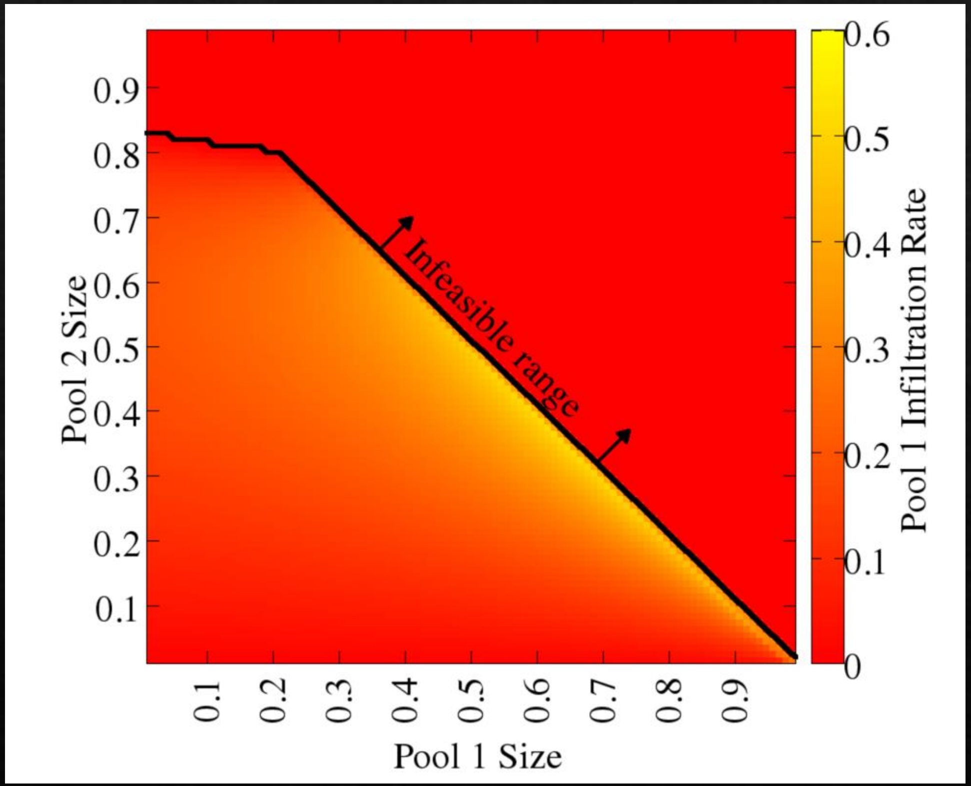


Figure from:
I. Eyal, "The Miner's Dilemma," *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, 2015, pp. 89-103

Optimal Revenue Increase Factor for Pool 1 As a Function of Pool Size

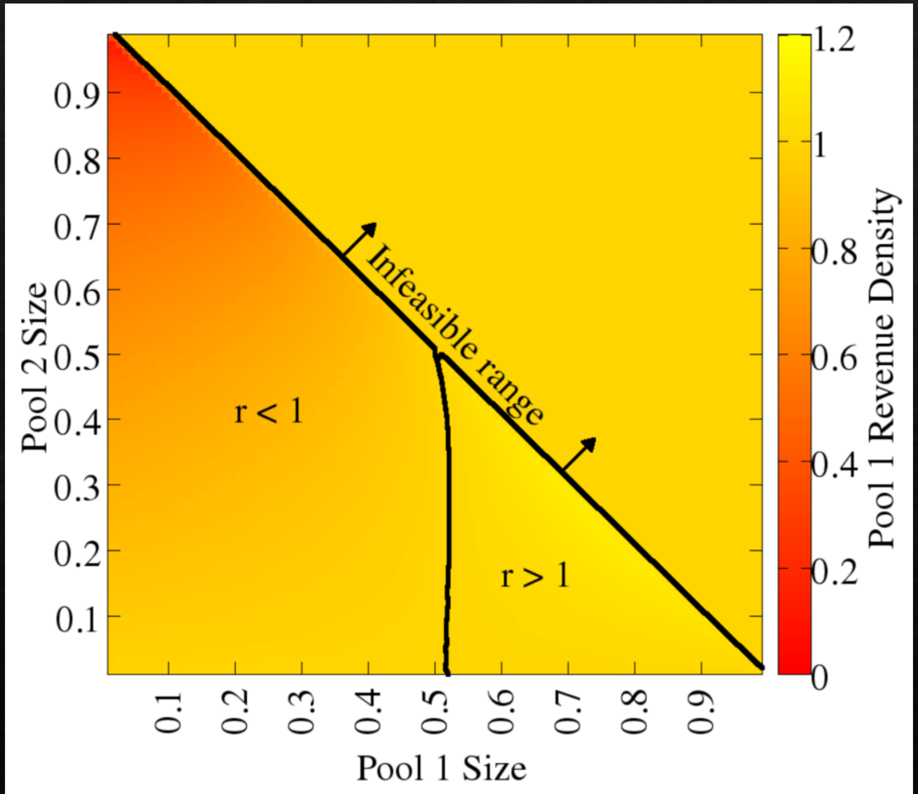


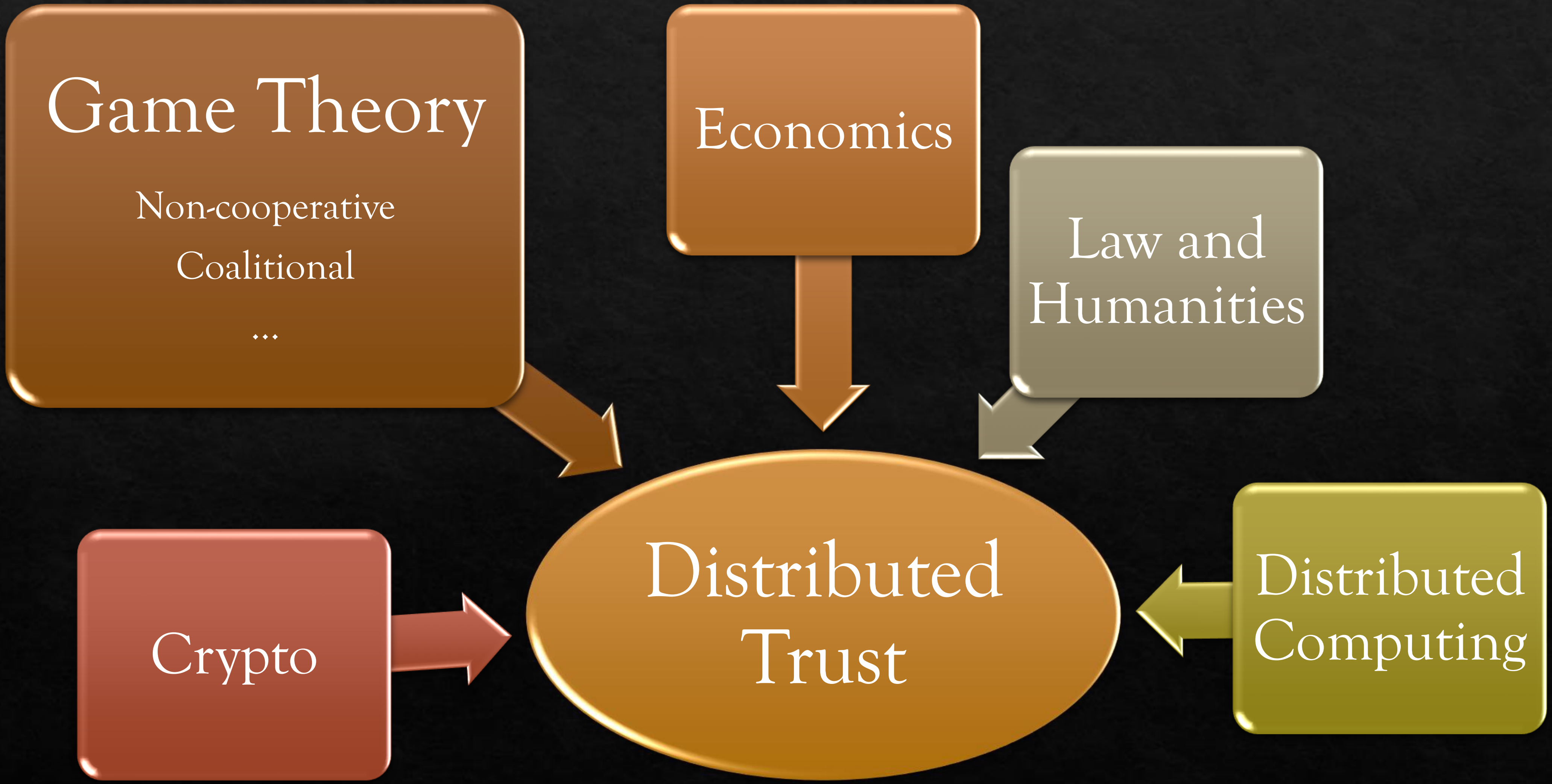
Figure from:
I. Eyal, "The Miner's Dilemma," *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, 2015, pp. 89-103

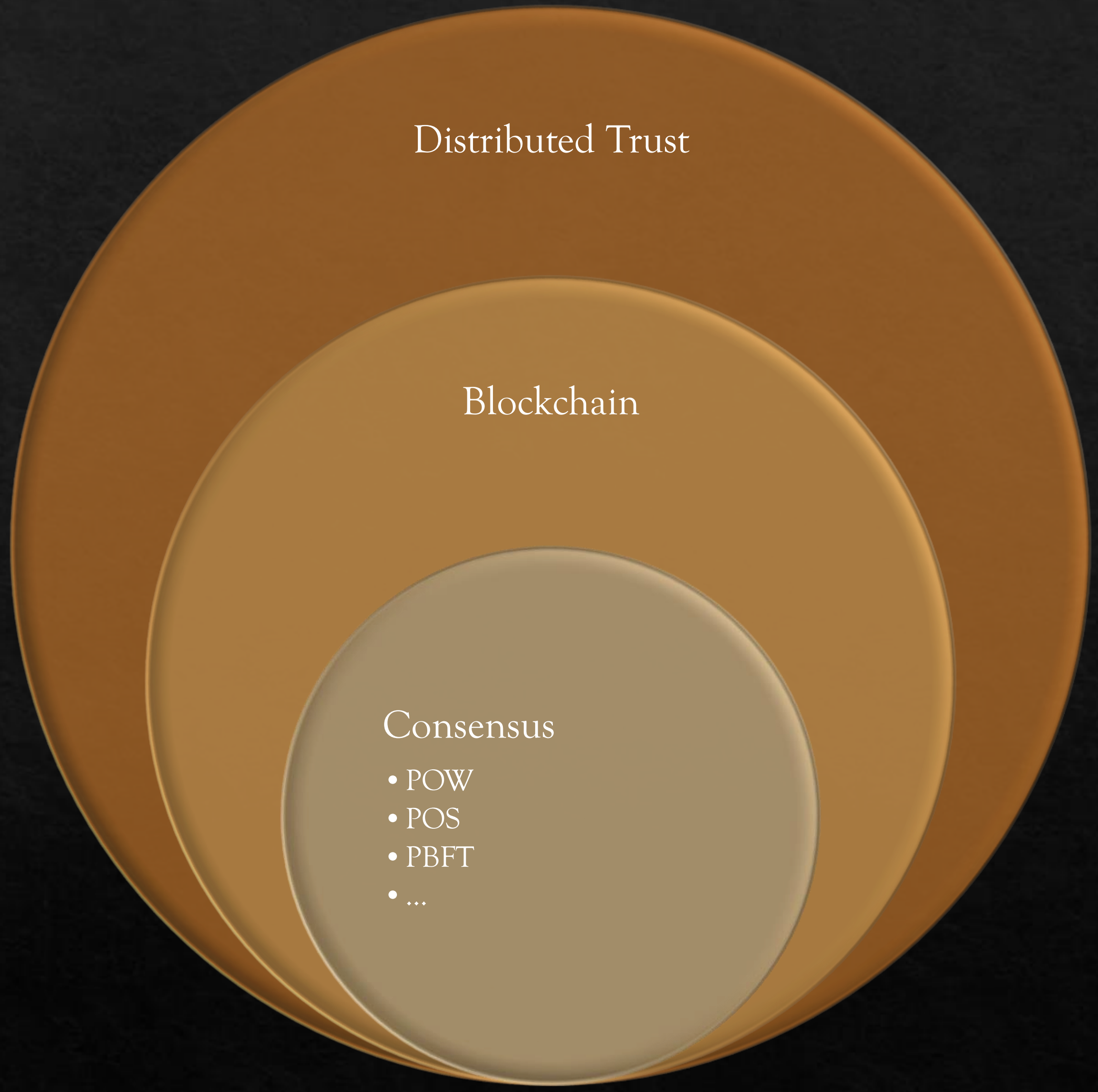
Summary of Insights

- Nash equilibrium exists
- No infiltration is not a Nash equilibrium
- Consequence: Suboptimal social welfare
- No incentive to infiltrate only when other pool is too large
- Improved revenue only when pool controls a strict majority of the total mining power.

Some General Thoughts

Amalgamation of Ideas




Distributed Trust
Blockchain
Consensus
• POW
• POS
• PBFT
• ...