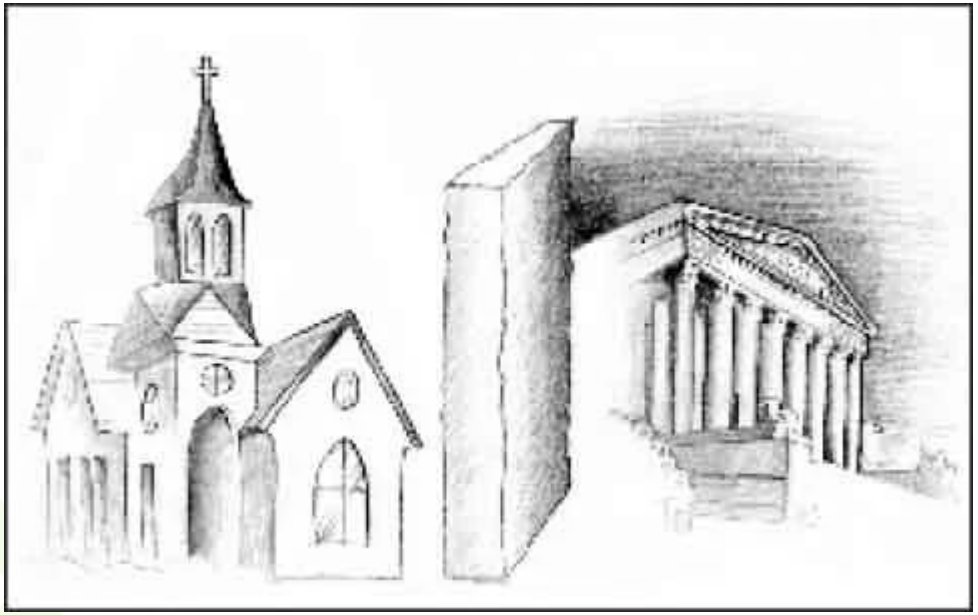
Crypto Protocols

Ergodicity & Consensus

WOLFRAM
BLOCKCHAIN LABS
Steph Macurdy, Head of Research & Education

Separate Money from State

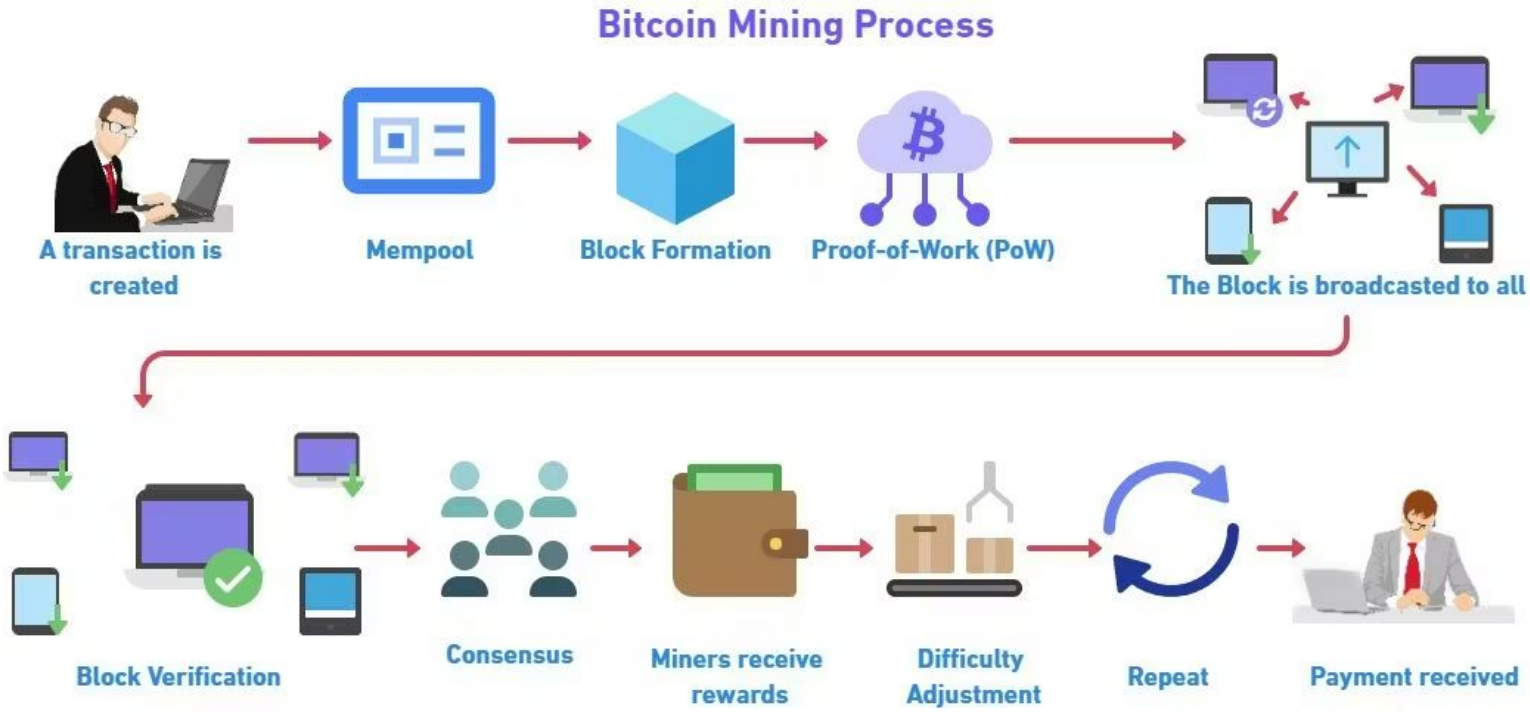


- Must tap fundamental ideas:
  - Physics
  - Information Theory
  - Distributed Systems
  - Economics
- Metacrisis
  - Generative functions
  - Arms races
  - Tragedy of Commons
  - Chaos or Tyranny?

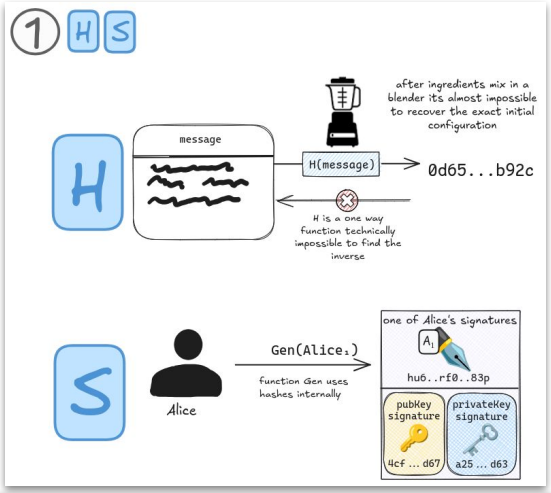
“Must erect a wall separating church and the state for the benefit of free society.”

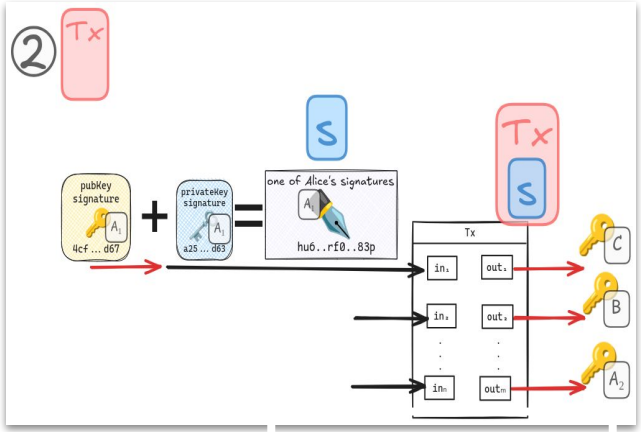
4+ Hours of Philosophical Foundations

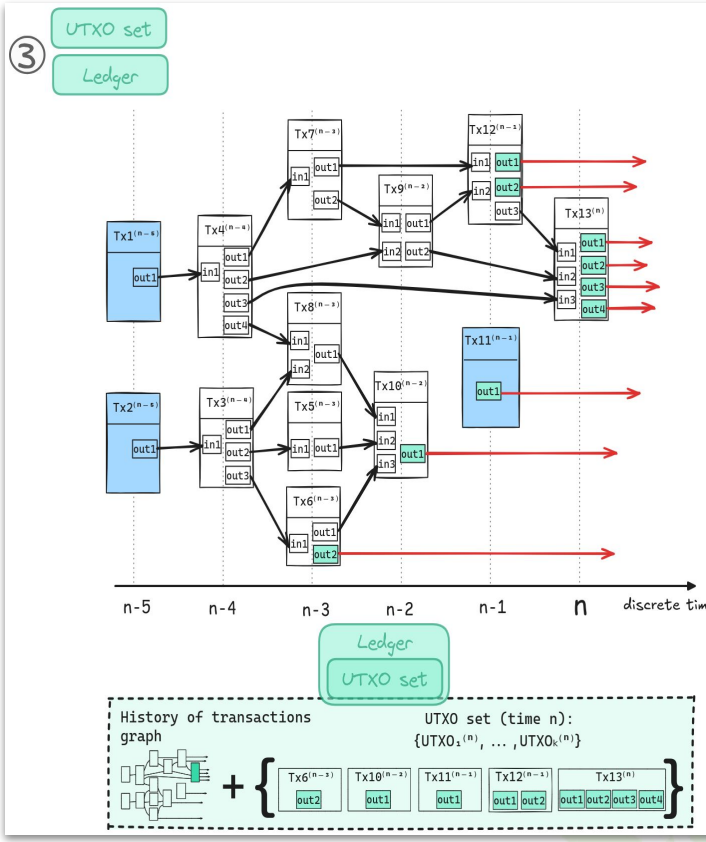
Bitcoin’s Proof of Work

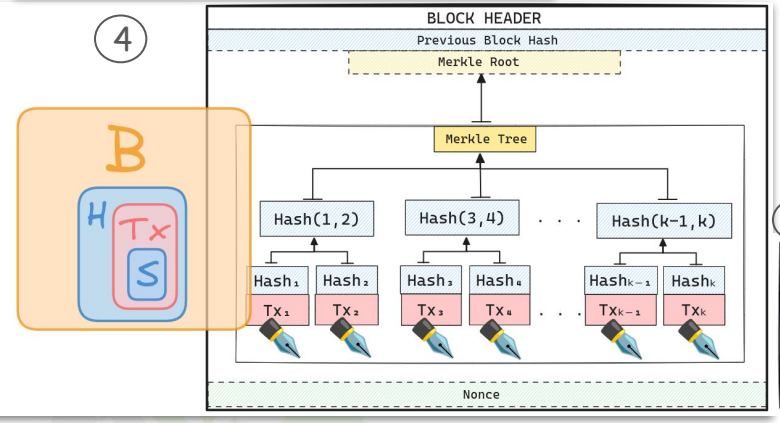


Core Ingredients of Blockchains

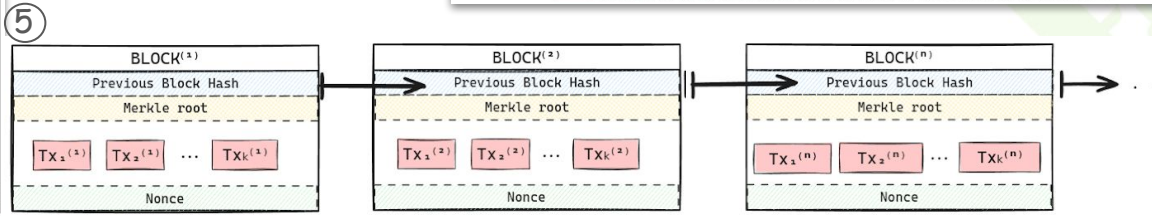






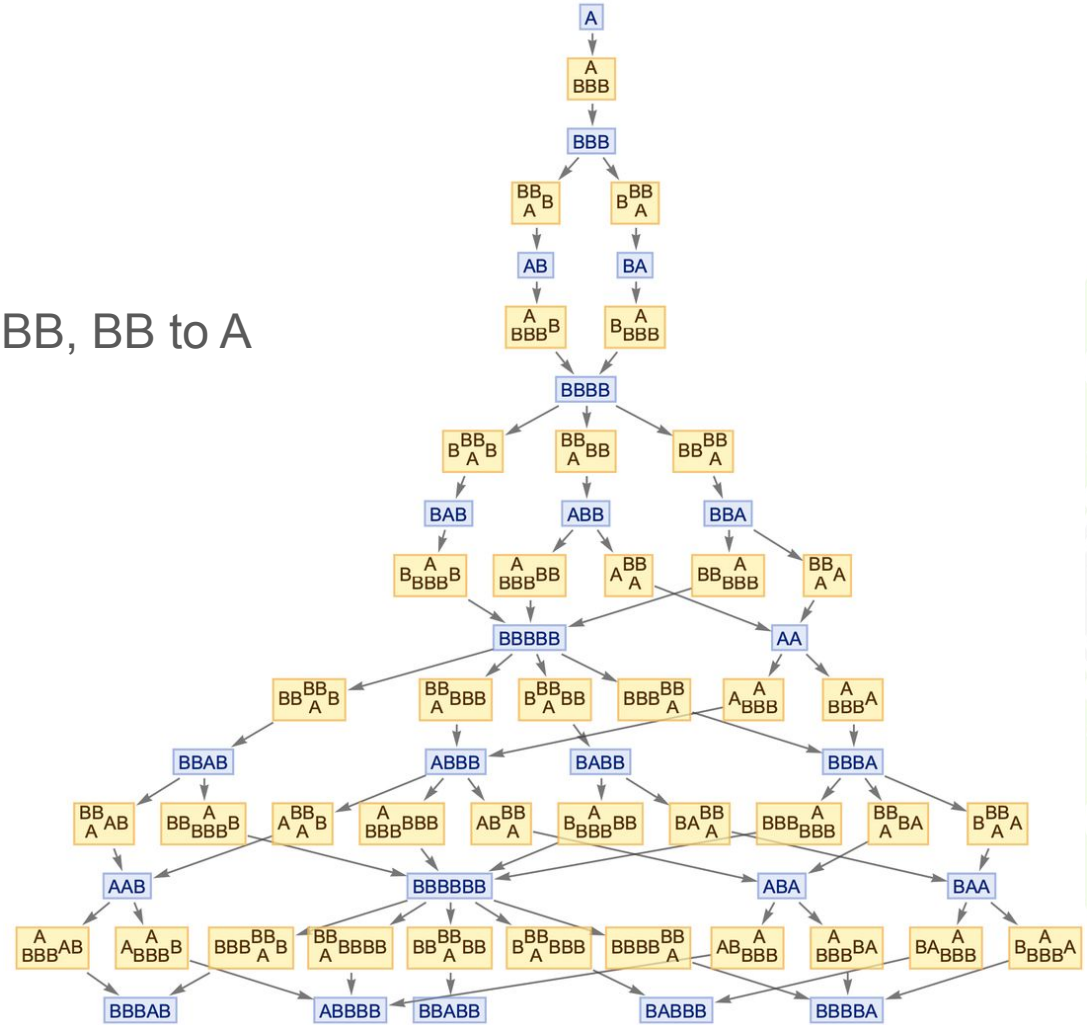


1. Hashes
2. Signatures
3. TX Ledger
4. Blocks
5. Chain



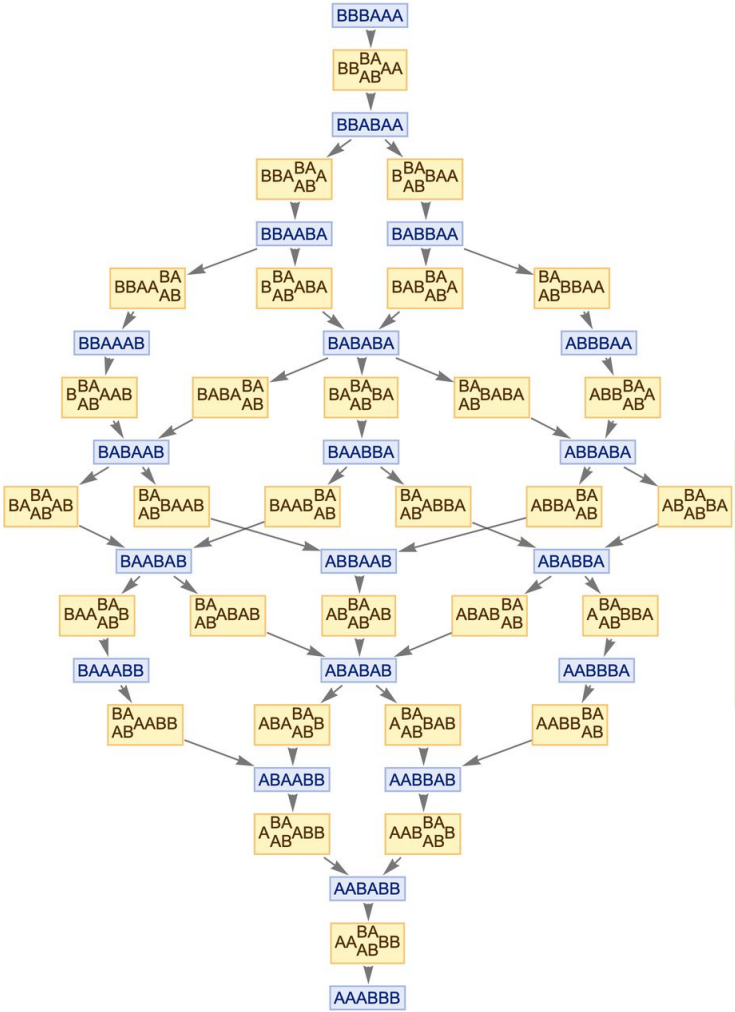
Physics

- Space of all possible rules
- Take one simple rule: A to BBB, BB to A
- Many transformations
- Multiway Hypergraph

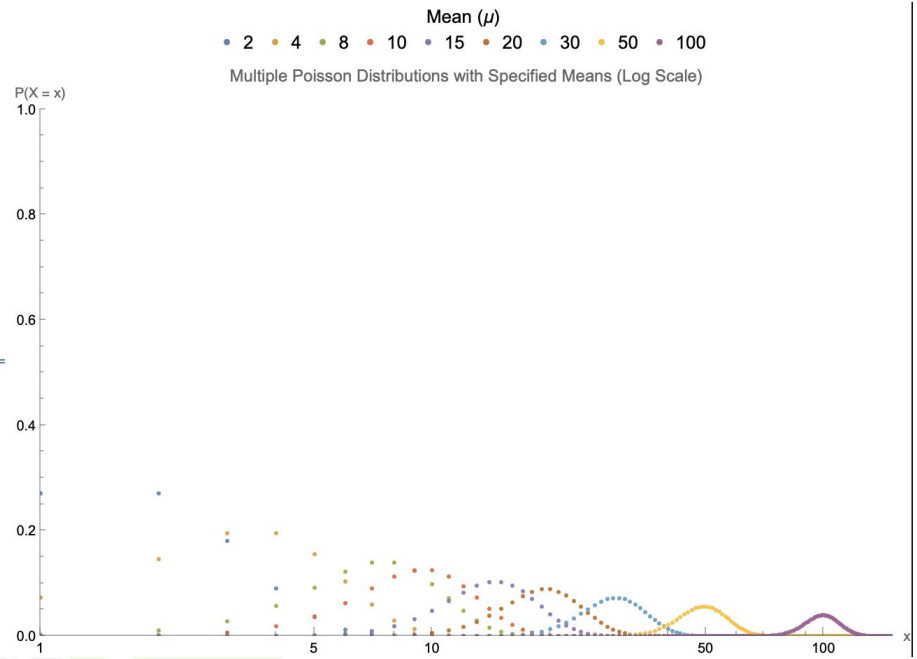


Distributed Systems

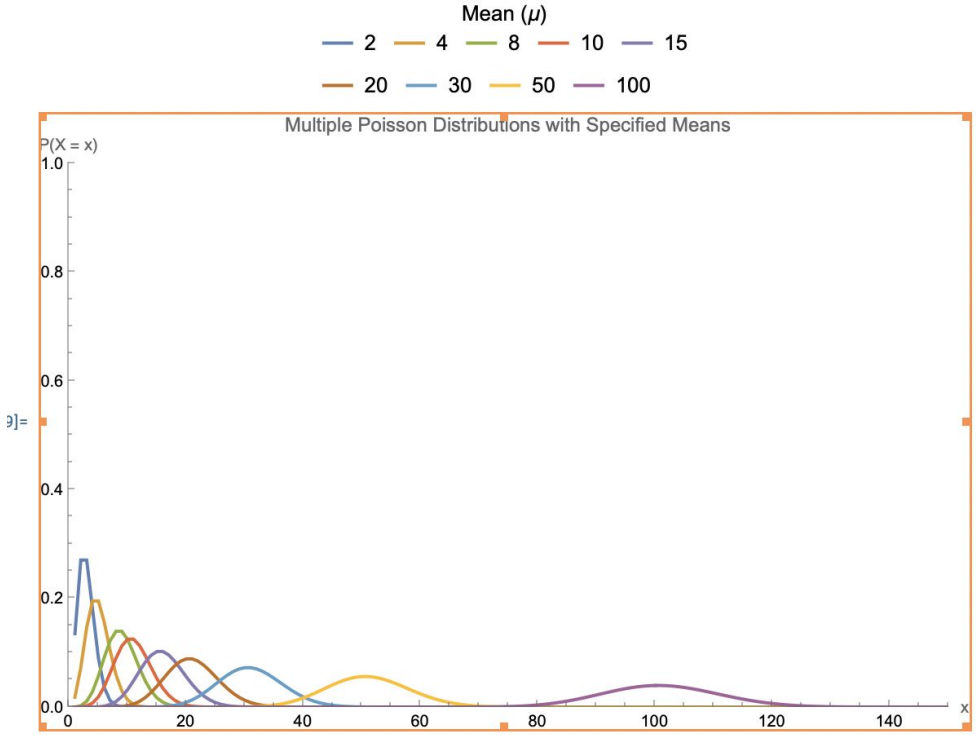
- Branching & Merging
- Directed Acyclic Graph
- Resolution Events
- Consensus



Ensemble Averages

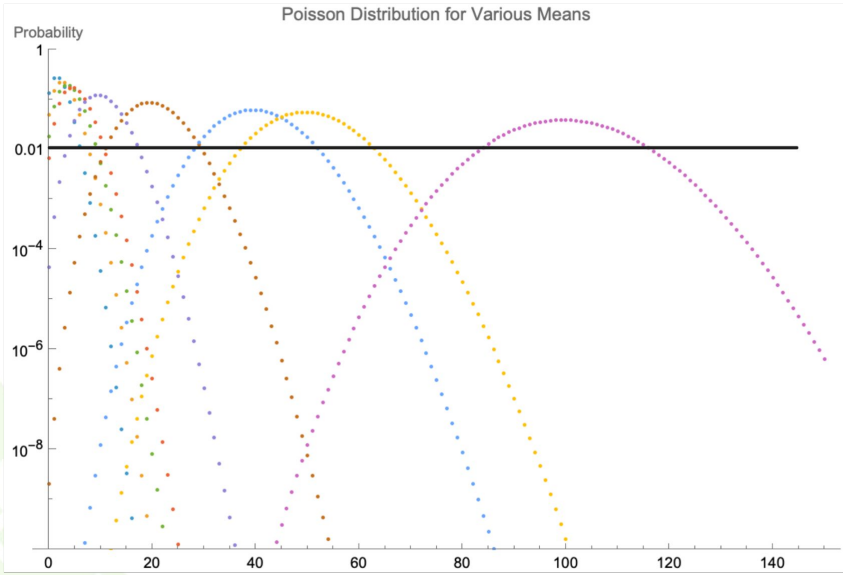


Linear/Log

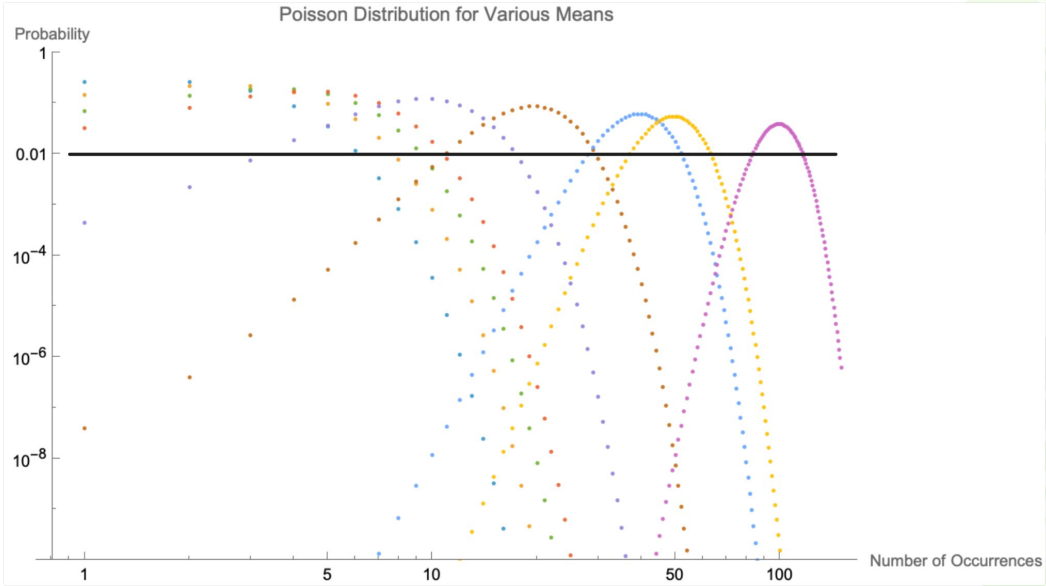


Linear/Linear

Ensemble Averages: Log/Linear, Log/Log

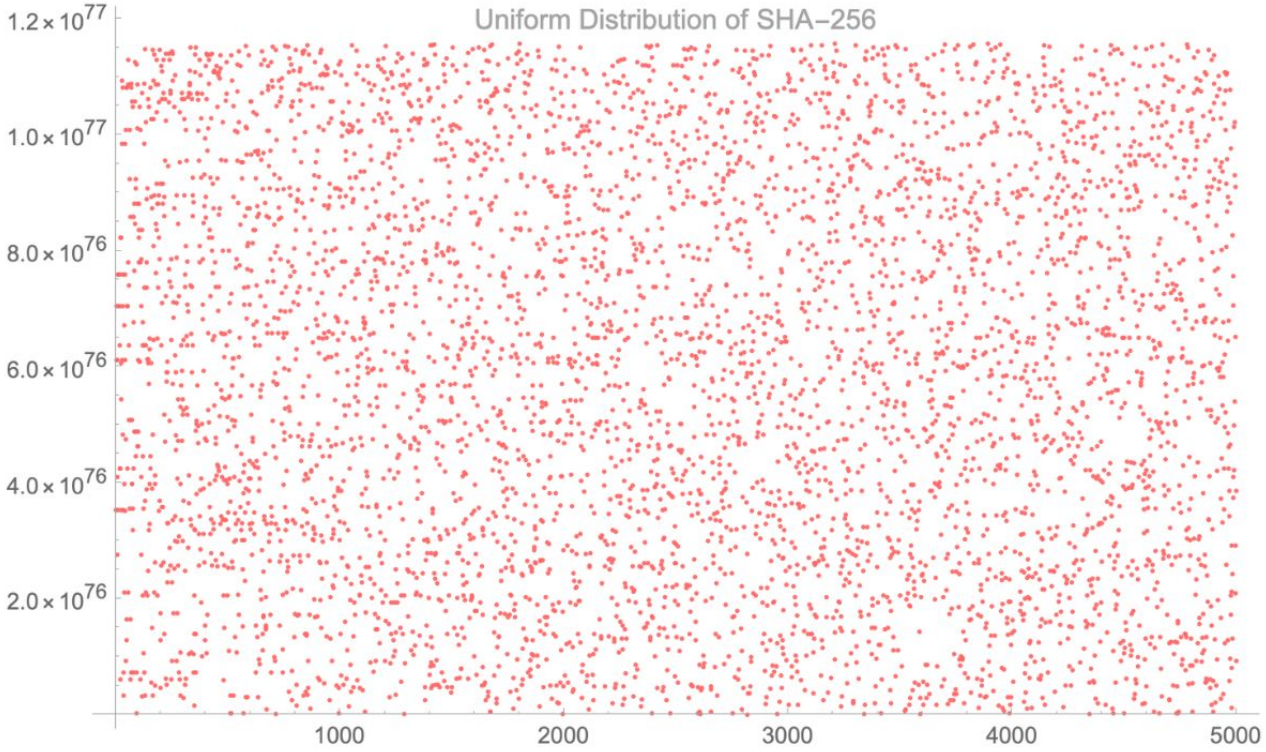


Log/Linear



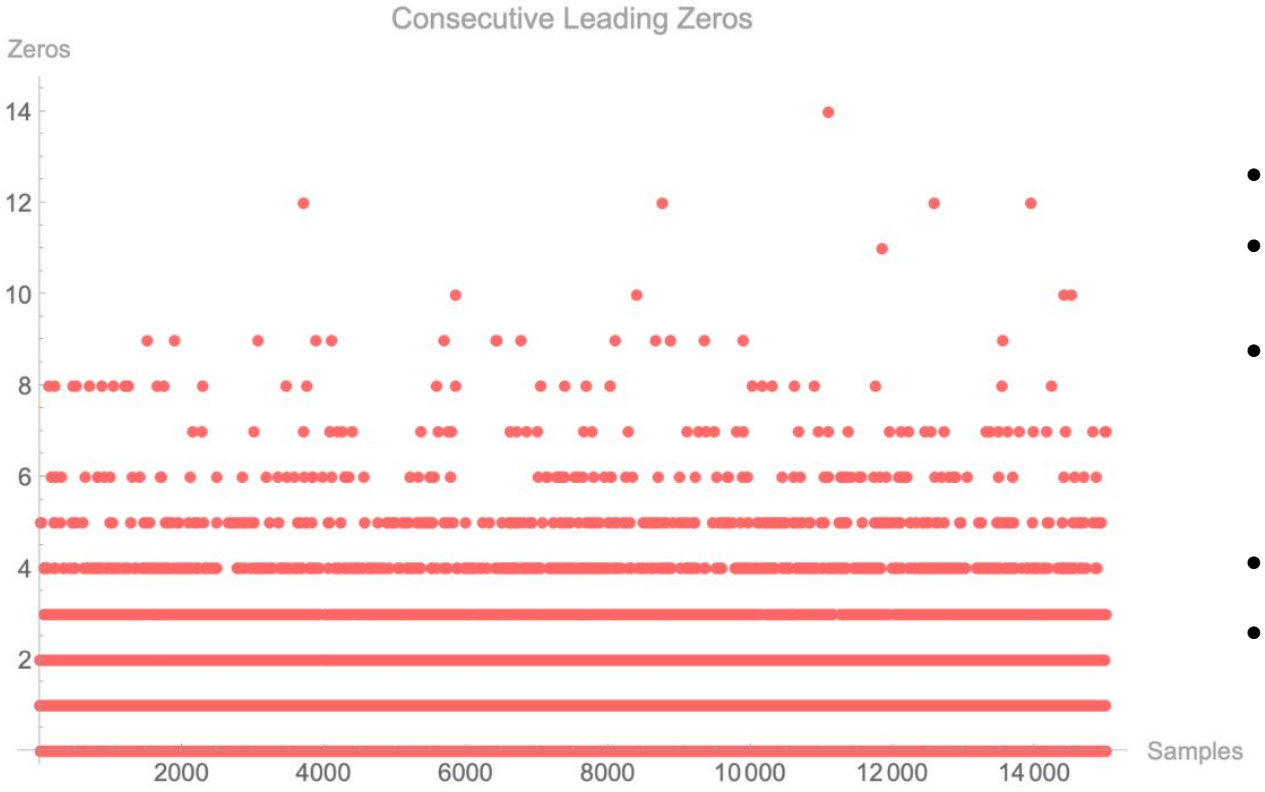
Log/Log

Information Theory



- Uniform, equiprobable, total state space
- The total possible state space of a SHA-256 output = 2^{256}
- Rule: # of consecutive leading 0s in SHA-256 output
- Beyond “arbitrary” threshold

Information Theory



- The total possible state space of a SHA-256 output = 2^{256}
- Rule: # of consecutive leading 0s in SHA-256 output (beyond arbitrary threshold)
- Example:
  - 0000000000101101001110101011100110110110101100001000000100101111111111100001010001100000010000011
- Interpretation: # of bits of uncertainty removed (accumulated/minimized)
- Occurs $1/2^{10}$

Hierarchical Sequences

Decentralized Global Monetary System

- Separation of Money from State
- Scalable
- Mitigate Gresham's Paradox
- Programmable
- Privacy
- Unit of Account

Hierarchical Sequencing