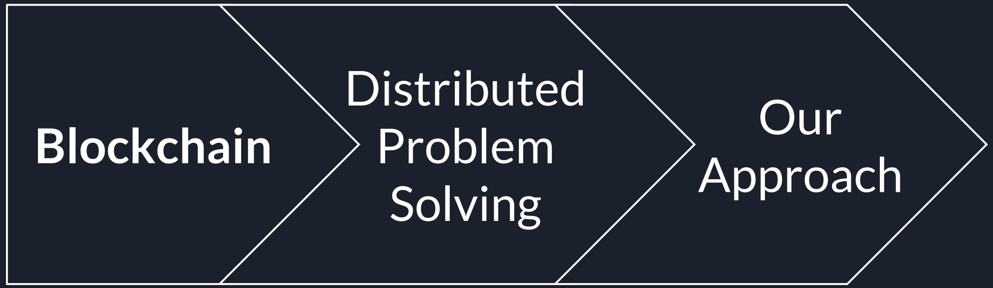
Hybrid Mining:

Exploiting Blockchain's Computational Power for Distributed Problem Solving

Arash Pourdamghani (Sharif University)
Krishnendu Chatterjee (IST Austria)
Amir Kafshdar Goharshady (IST Austria)

Spring 2019
The 34th ACM/SIGAPP Symposium On Applied Computing

Outline

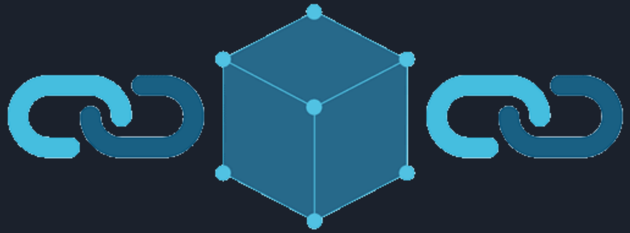


Blockchain

Distributed Problem Solving

Our Approach

Blockchain



Mining Protocols

- Proof of Work (Bitcoin, Ethereum)
- Proof of Space (SpaceMint)
- Proof of Stake

Challenges

- Energy Consumption

- Dedicated Hardware

- Centralization

Distributed Problem Solving (DPS)

Real-world Problems

- Protein Folding (folding@home)
- Search for Extraterrestrial Intelligence (SETI@home)
- Mersenne Prime Search (GIMPS)

Challenge

Total Computational Power is Limited!

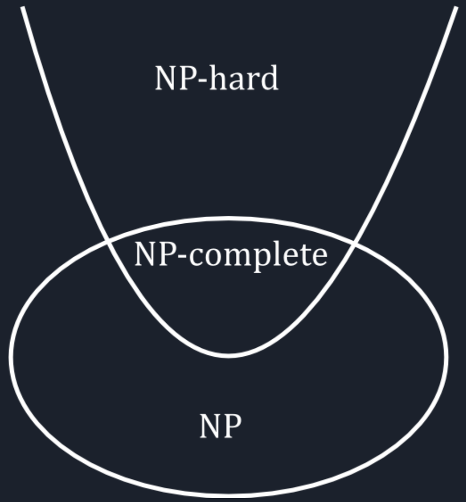
CureCoin

Limitations

- Focusing on a specific problem
- Artificially/Self generated instances
- Incompatible with current dedicated hardware

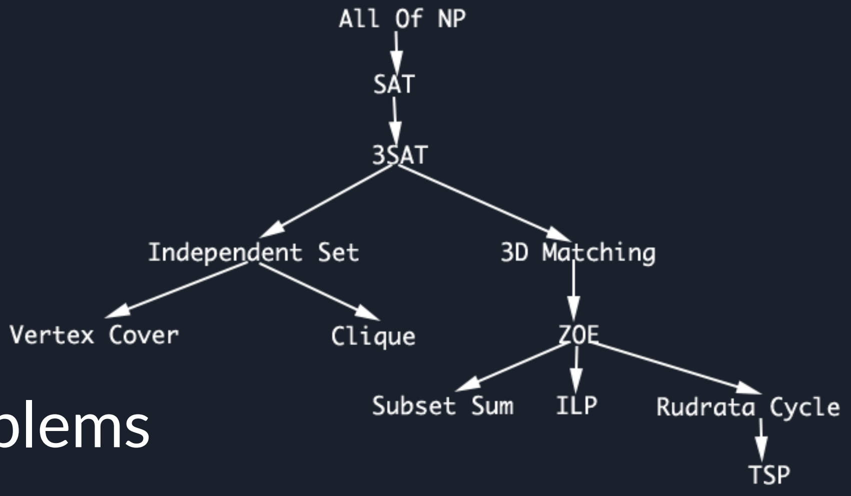
Our Approach

NP-complete Problems



- Verifiable proofs in polynomial time
- Reducible to/from other NPC-Problems

SAT



- Basis of other NPC-Problems
- Solutions are encoded in a short binary sequence

Our Goals

- Creating a general DPS platform
- Reducing blockchain’s energy consumption
- Compatible with current PoW hardware

Proof of Work (PoW)

- Hashcash puzzle:
    - Find a nonce such that:
        - Hash(nonce, previous block, new block) < C

Extension of PoW

- Hybrid solution
- Start with HashCash
- |HashCash blocks| > |Problem solving blocks|
- Longest chain = Longest HashCash chain

Problem Proposing

- Achieved by a specific type of transaction
- Provide a CNF formula
- Pay the required fees

Problem Proposing (cont’d)

- The fees are:
  - Proposal fee
  - Storage fee
  - Reward fee
  - Transaction fee

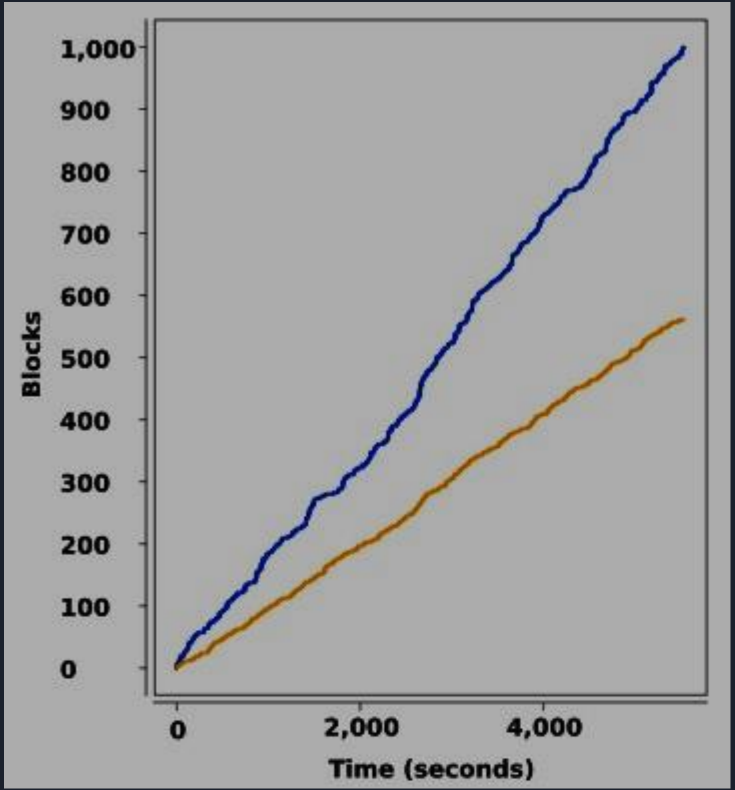
Mining by Problem Solving

- A two-step approach:
  - Claim you have the result and deposit money
  - Reveal the result after your claim has been stabilized in the system

Guarantees

- As resistant to double spending as PoW
- Resistant to problem/solution spamming
- Resistant to solution theft

Implementation



Thank you