Ideas for using Cryptography and Blockchain to extend computing resources

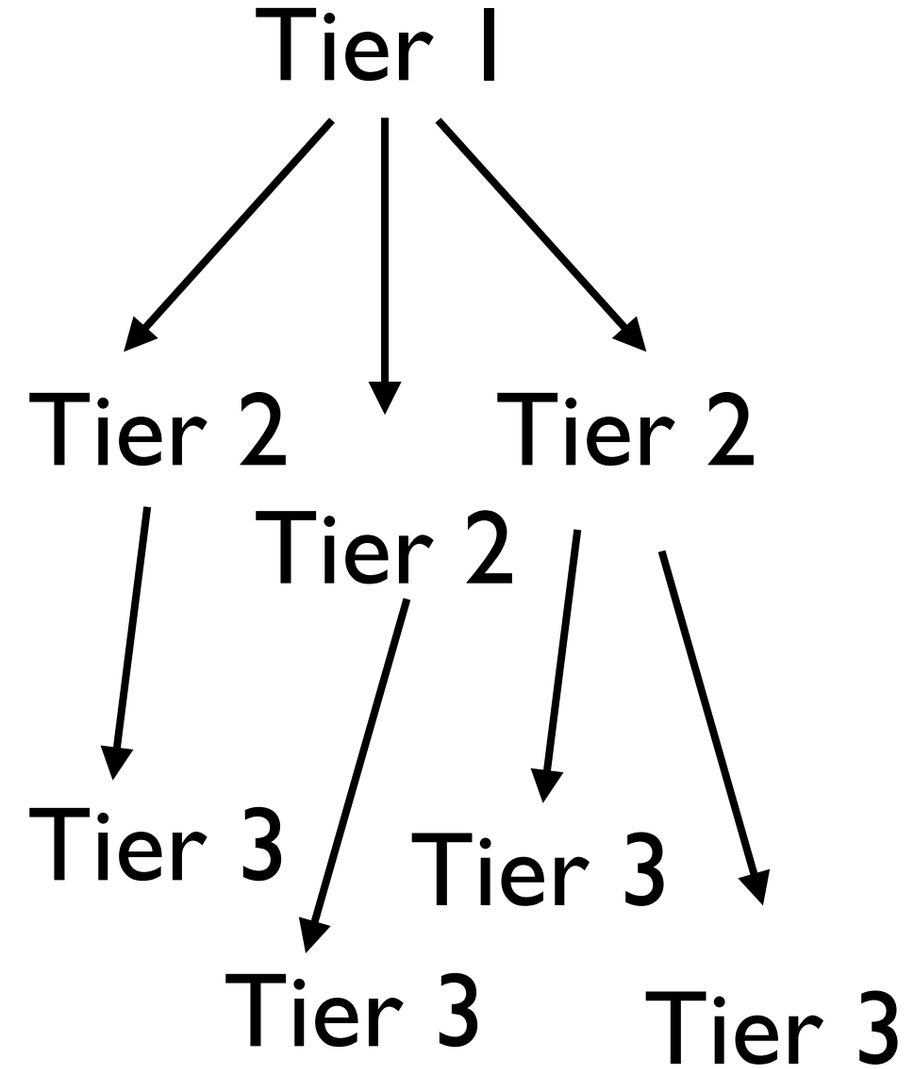
Lindsey Gray

20 April 2018

Ways of Amassing Compute Power

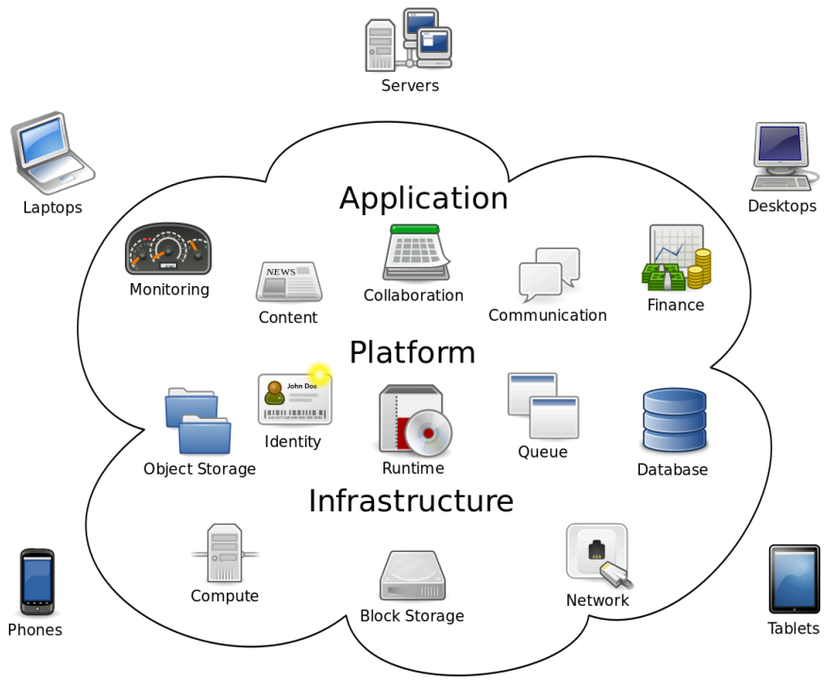
highly centralized
data-local

Grid Computing



highly centralized
have to ship data

outbound data
particularly expensive

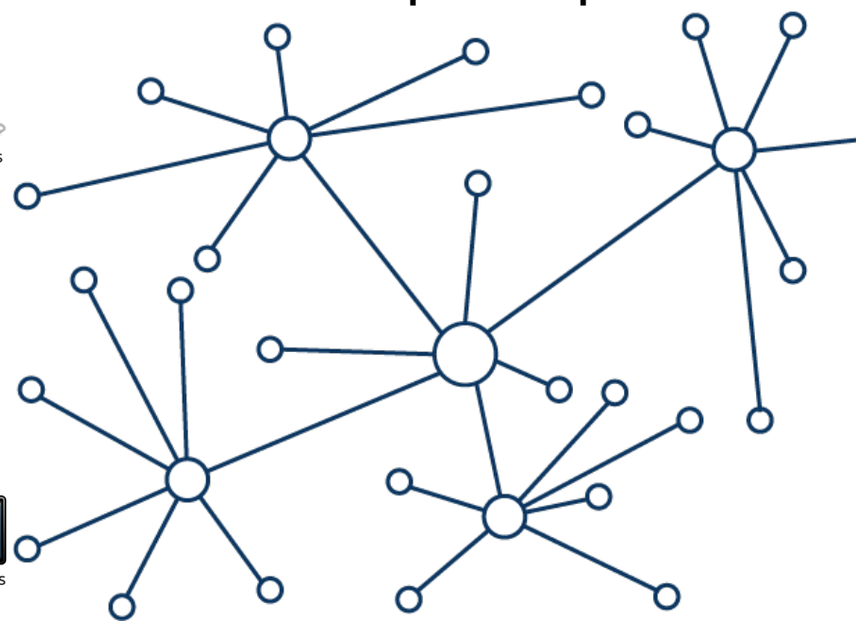


Cloud Computing

Decentralized Computing

actually other
people's computers?
How to trust?

possibility for data locality
or cheap transport



cloud without a company

governance/authorship
through blockchain?

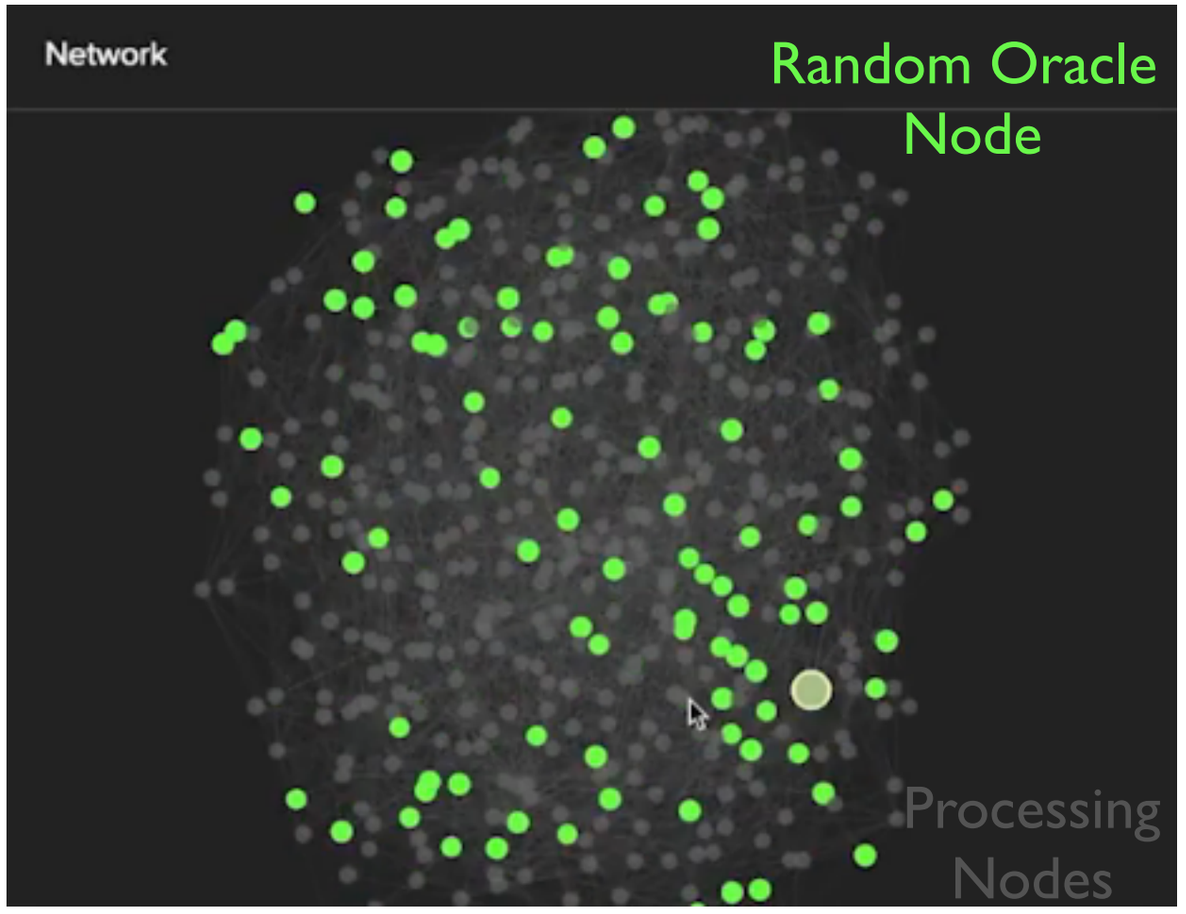
Possibly very interesting
for MC production.

Monte Carlo Use Cases

- Random Oracle
  - An object in a network that takes some input and gives a very random output
  - Essentially a good hash function

- Multiple random oracles may collective sign some dataset they've contributed to
  - Using variants of elliptic curve encryption it is possible to set a threshold at which bad actors may contribute to computation
  - Enables collective agreement

Random Oracle Test Network from Dfinity



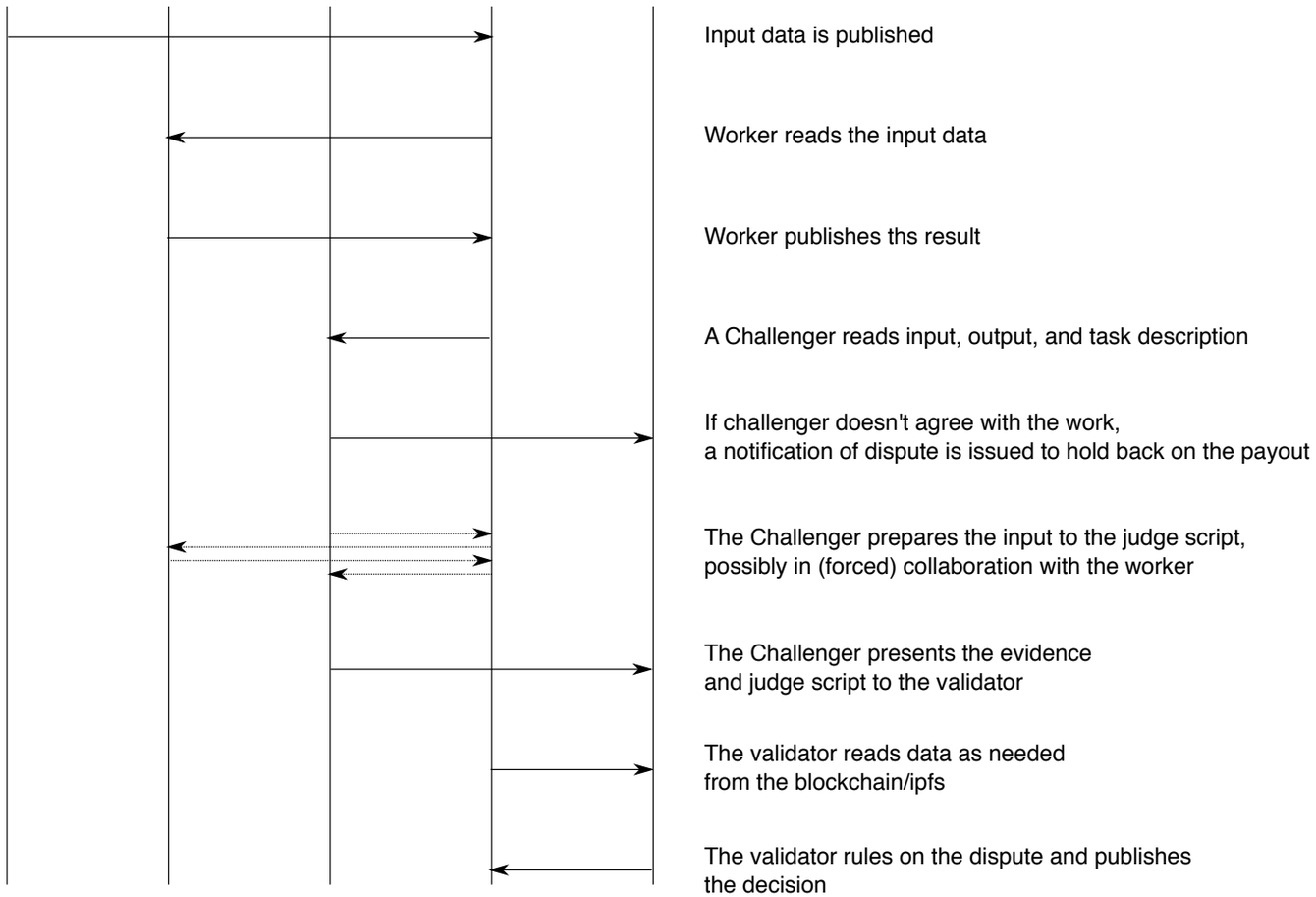
Monte Carlo Generators also fit the properties of a Random Oracle.

We could use a similar iteratively signed network to generate MC events where statistical independence and trustability is enforced by the computation model, hence we could trust random nodes!

Reconstruction/Analysis Use Cases

Problem Example	Cost		Task	Overhead	
	Verification	Runtime	proportion	task	network
Matrix Multiplication[a)]	$O(n^2)$	$O(n^{2.6})$	2.0%	$2.51 \cdot 10^{-4}$	$5.02 \cdot 10^{-6}$
ML Training[b)]	$O(WS)$	$O(IWS)$	50.0%	$5.00 \cdot 10^{-5}$	$2.50 \cdot 10^{-5}$
VF-SPARK[c)]	$O(\log(n))$	$O(n)$	40.0%	$9.88 \cdot 10^{-4}$	$3.95 \cdot 10^{-4}$
NP-complete problem	$O(1)$	$O(2^n)$	5.0%	-	-
CFD[d)]	$O(n)$	$O(C \cdot n)$	0.0%	$5.00 \cdot 10^{-2}$	-
Image Rendering[e)]	$O(m)$	$O(n^2 \cdot m)$	0.0%	$1.53 \cdot 10^{-5}$	-
TrueBit[f)]	$O(n)$[g)]	$O(n)$	3.0%	$2.75 \cdot 10^{1}$	$8.25 \cdot 10^{-1}$
				Sum of Verification overhead	$8.25 \cdot 10^{-1}$
				Sum of Verification overhead excluding TrueBit	$4.38 \cdot 10^{-4}$

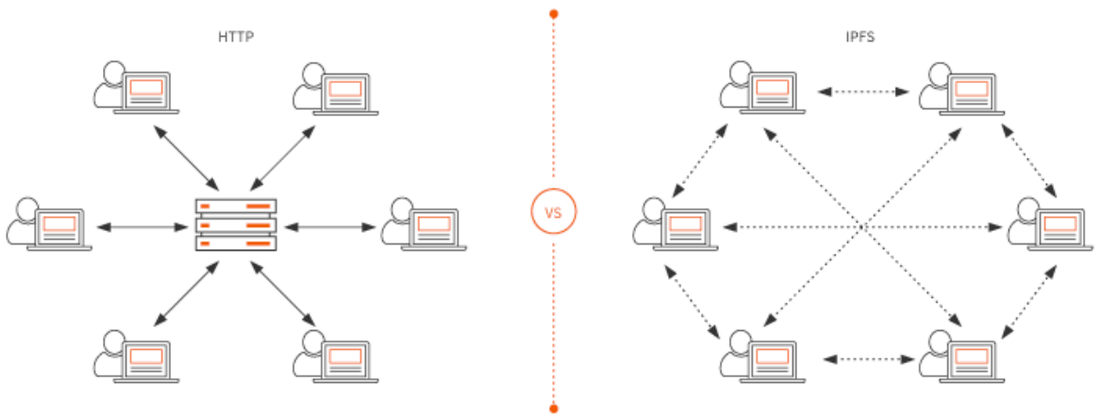
General Verification Data Flow

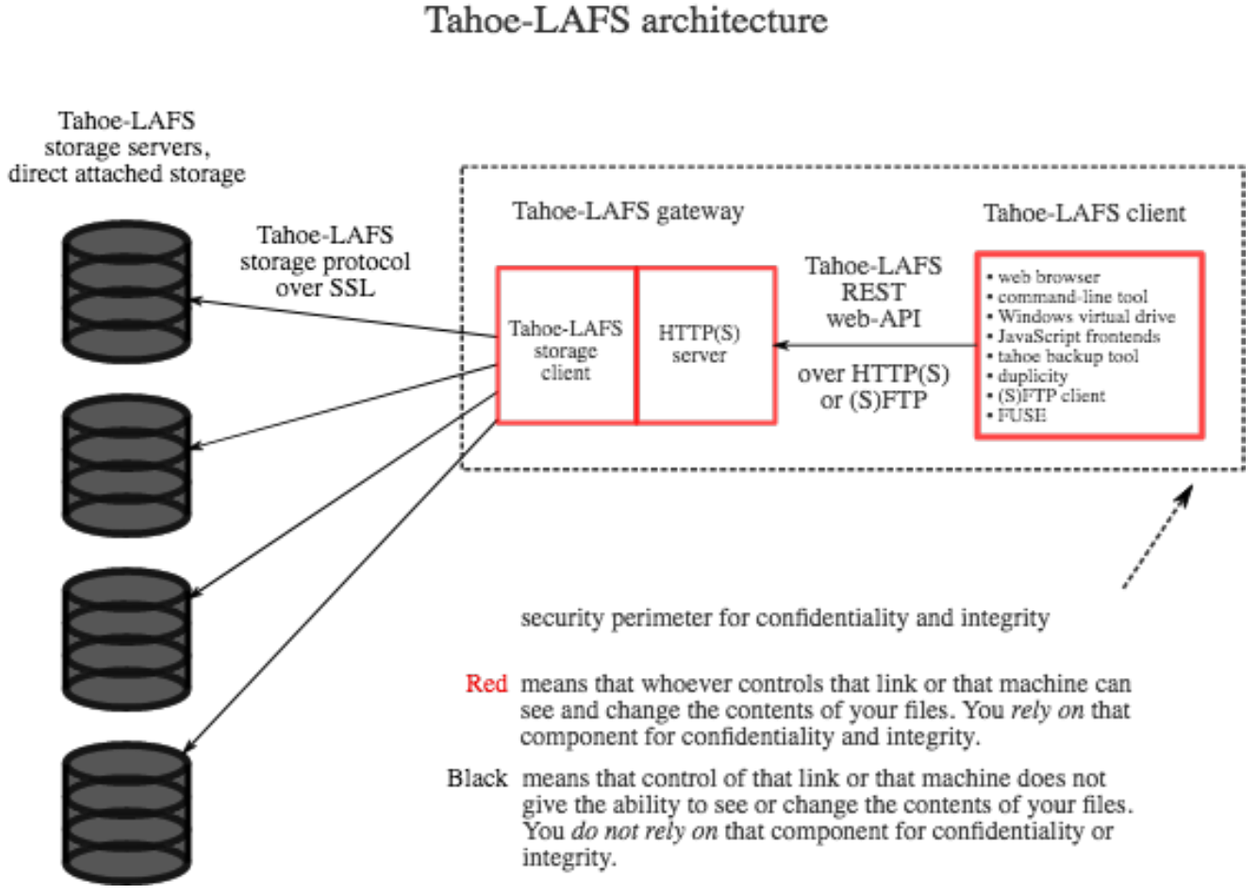


- Verifiable computation
  - Cryptographically verifiable algorithms
- Coron.ai
  - blockchain startup
    - lead by folding@home developers
  - API for implementing verifiable computing
    - BLAS with cryptographic verification
  - tunable levels of verification
    - remove overhead on known trusted nodes
  - cloud-like structure, benefits from containerization efforts
- Aim to try implementing Kalman filter within verifiable computing API
  - First try in two weeks, sitting with developers

Decentralized Data Stores

IPFS Architecture





- How to store distributed data in a safe and effective way?
  - Prevent tampering, maintain fidelity of data
- IPFS
  - Essentially git turned into a file system
  - Aim is embedded history, self-consistency
  - Directory structure as merkel trees
    - kind of similar to cvmfs
- Tahoe-LAFS "least authority filesystem"
  - FUSE mounted, similar to CVMFS, testing currently ongoing to ~0.5 PB
  - Tunable block-by-block erasure encoding
  - File are split up into chucks and reassembled as requested, all stored data encrypted
    - Similar to bittorrent but everything is encrypted
- Both have objectivity and could be used as layers beneath existing tools to tap decentralized resources

Outlook

- This is all very new and exploratory
  - The number of available computers on the planet is huge, could we access them?
  - Need to build up understanding of cryptographic models
  - Must maintain low overhead otherwise acquired resources don't scale well
- The main problem is ensuring to ourselves that code has been executed in the way that we want it on the data we expected
  - Random oracle networks and collective signing -> MC
  - Verifiable computing -> trustable algoritms (e.g. Kalman Filter)
  - Decentralized / encrypted datastores
- Notice I didn't actually mention blockchain that much
  - It's not intrinsic to this process, the cryptographic encapsulation of our algorithms and data is what matters first
  - More and more it seems that blockchain could be a way to govern such an amorphous computing infrastructure or to provide incentives