Onchain

# Decentralized Network Architecture

Onchain

# Agenda

- What is Blockchain?
- What can Blockchain do?
- Decentralized Network Architecture

Onchain

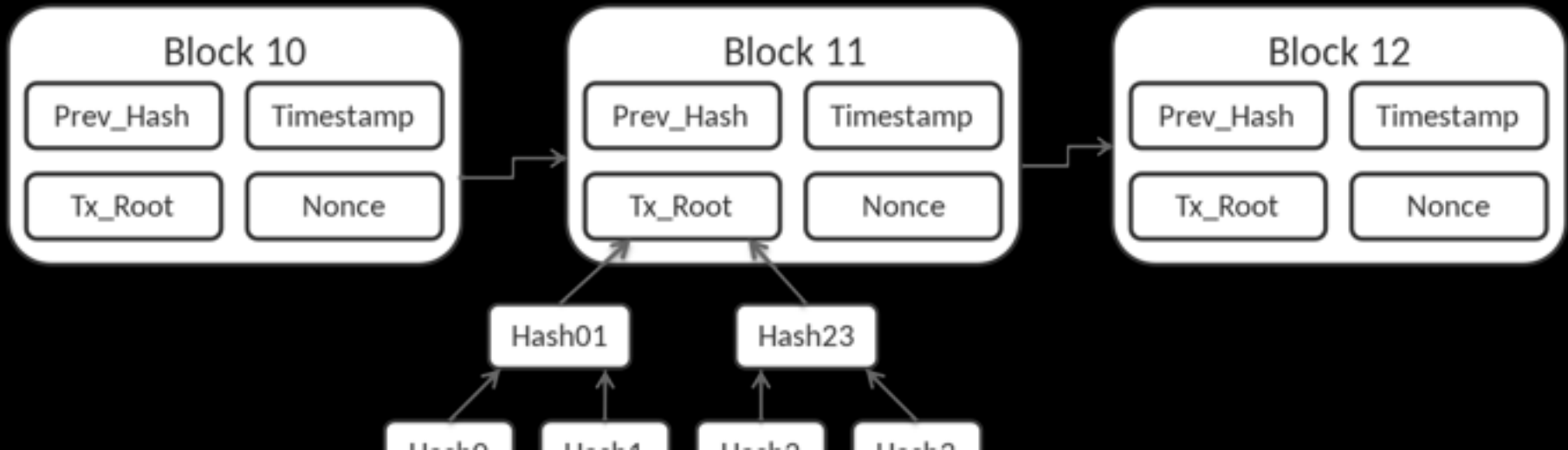
# The Origins of Blockchain

- Bitcoin
- Ethereum
- Distributed Ledger Technology
- Blockchain

Onchain

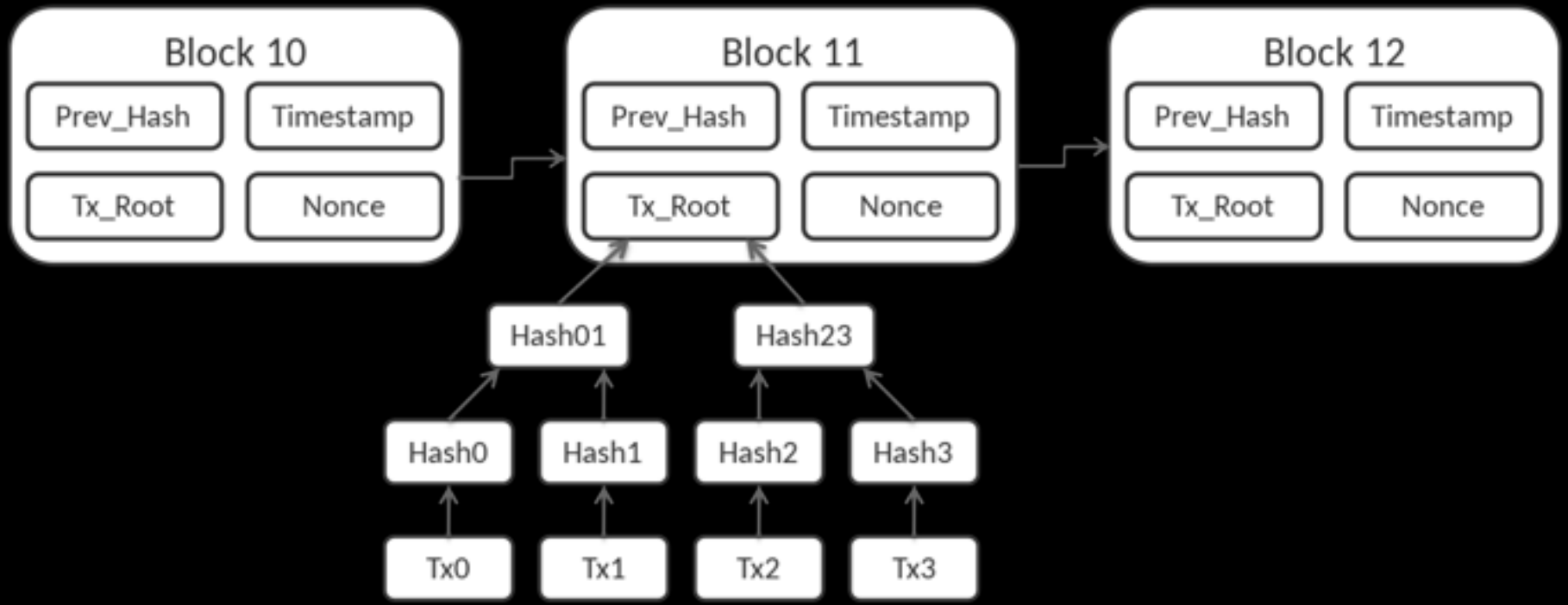
# What is Blockchain

- A growing list of blocks (transactions)
- Chained by cryptographic hash.
- By design:
  - resistant to modification of the data
  - record transactions in a verifiable and permanent way



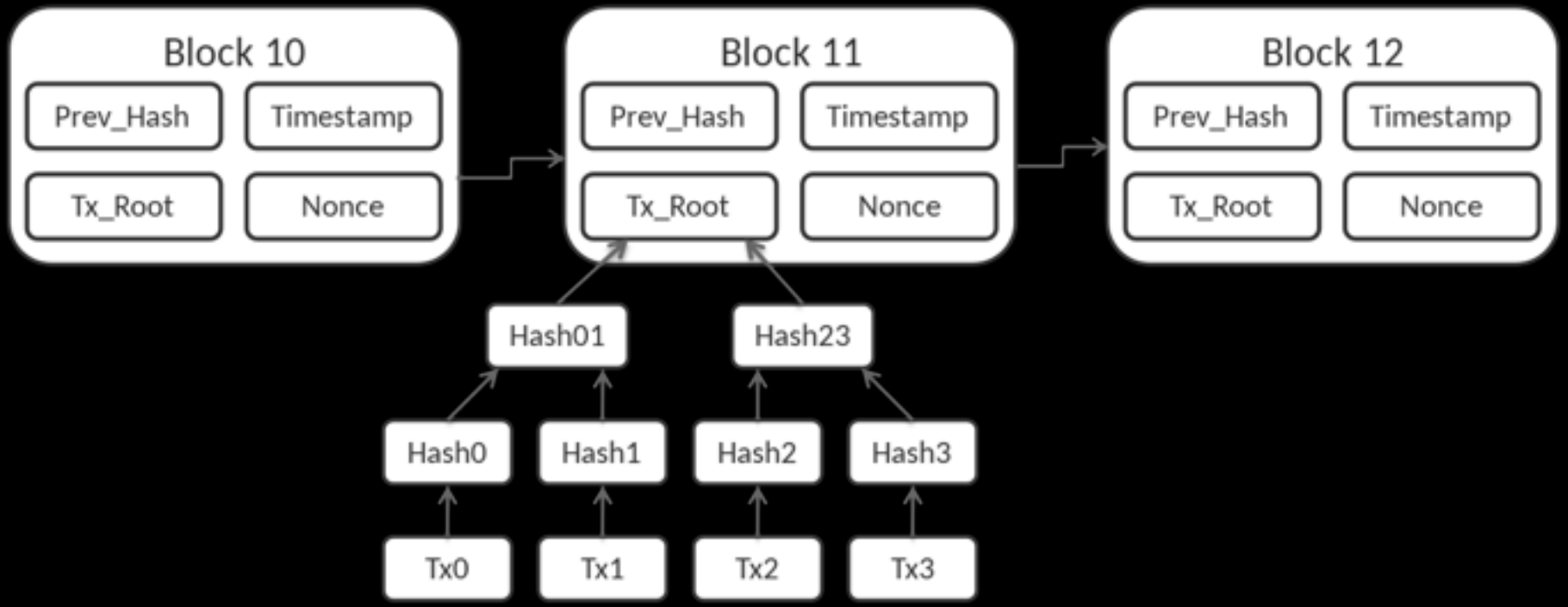
Onchain

# What is Blockchain



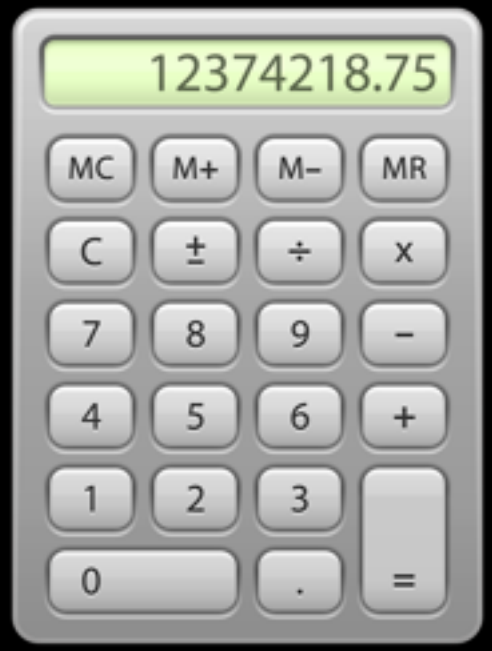

- A growing list of blocks (transactions)
- Chained by cryptographic hash.

Onchain




- Blockchain can be used to hold data and run computations in a way that is fault-tolerant: no single computer can cause the computation to stop or give a faulty answer.
- This is useful for building applications that are guaranteed to keep running for a long time and resist attacks.

Onchain




- 2009 – Single function blockchain (Bitcoin)
- 2012 – Multi-function blockchains
- 2014 – General-purpose blockchain

Onchain

# Bitcoin

- Bitcoin - A Peer-to-Peer Electronic Cash System

- Contributions
  - Proof-of-Work
  - Network
  - Incentive

Onchain

# Ethereum

- proposed in 2013, funded at 2014, went live in 2015
- Ethereum: a Secure Decentralized Generalized Transaction Ledger

- Contributions:
  - Proof-of-Stake
  - Smart Contract

Onchain

# Blockchain Network

**GLOBAL BITCOIN NODES DISTRIBUTION**

Reachable nodes as of Tue Mar 27 2018 18:20:21 GMT+0800 (CST).

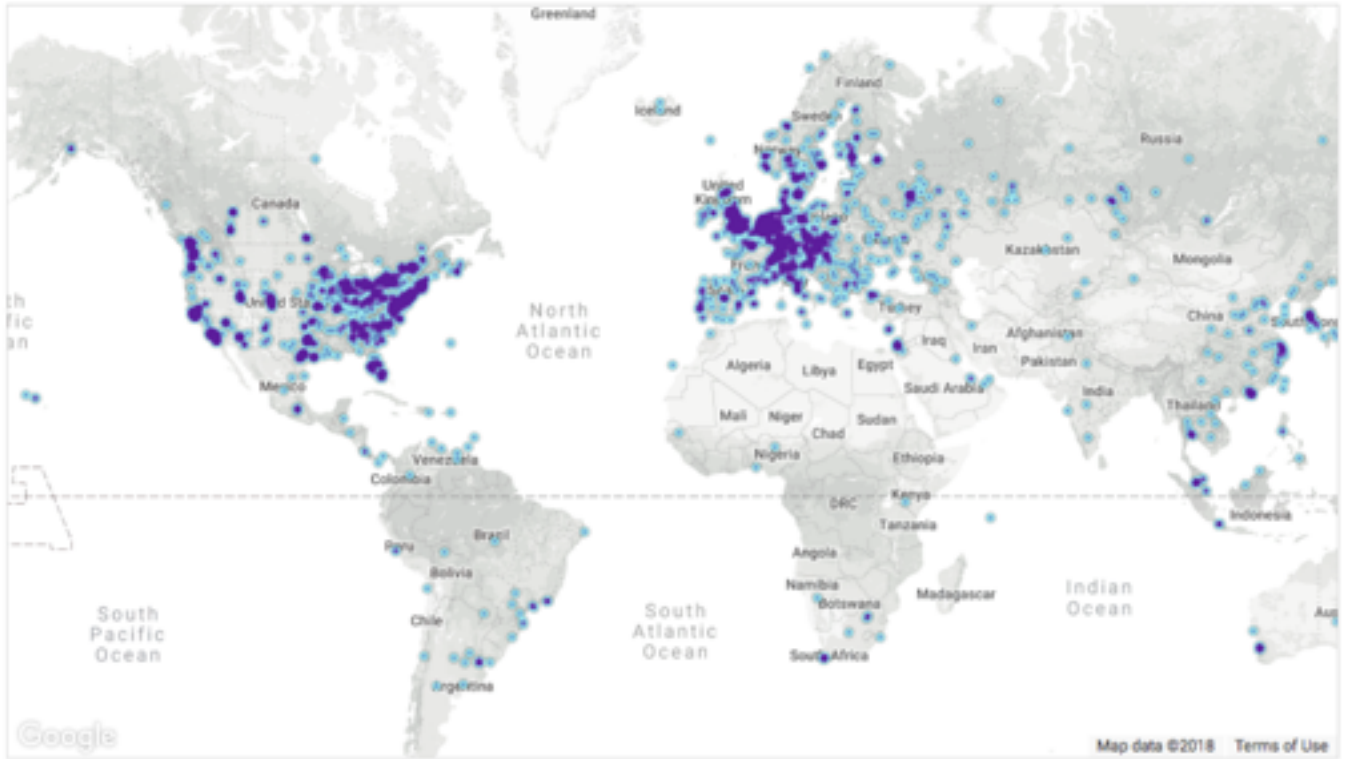
## 11869 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

| RANK | COUNTRY | NODES |
|---|---|---|
| 1 | United States | 2674 (22.53%) |
| 2 | Germany | 1945 (16.39%) |
| 3 | China | 1910 (16.09%) |
| 4 | France | 690 (5.81%) |
| 5 | Netherlands | 502 (4.23%) |
| 6 | United Kingdom | 410 (3.45%) |
| 7 | Canada | 394 (3.32%) |
| 8 | Russian Federation | 360 (3.03%) |
| 9 | n/a | 316 (2.66%) |
| 10 | Singapore | 234 (1.97%) |

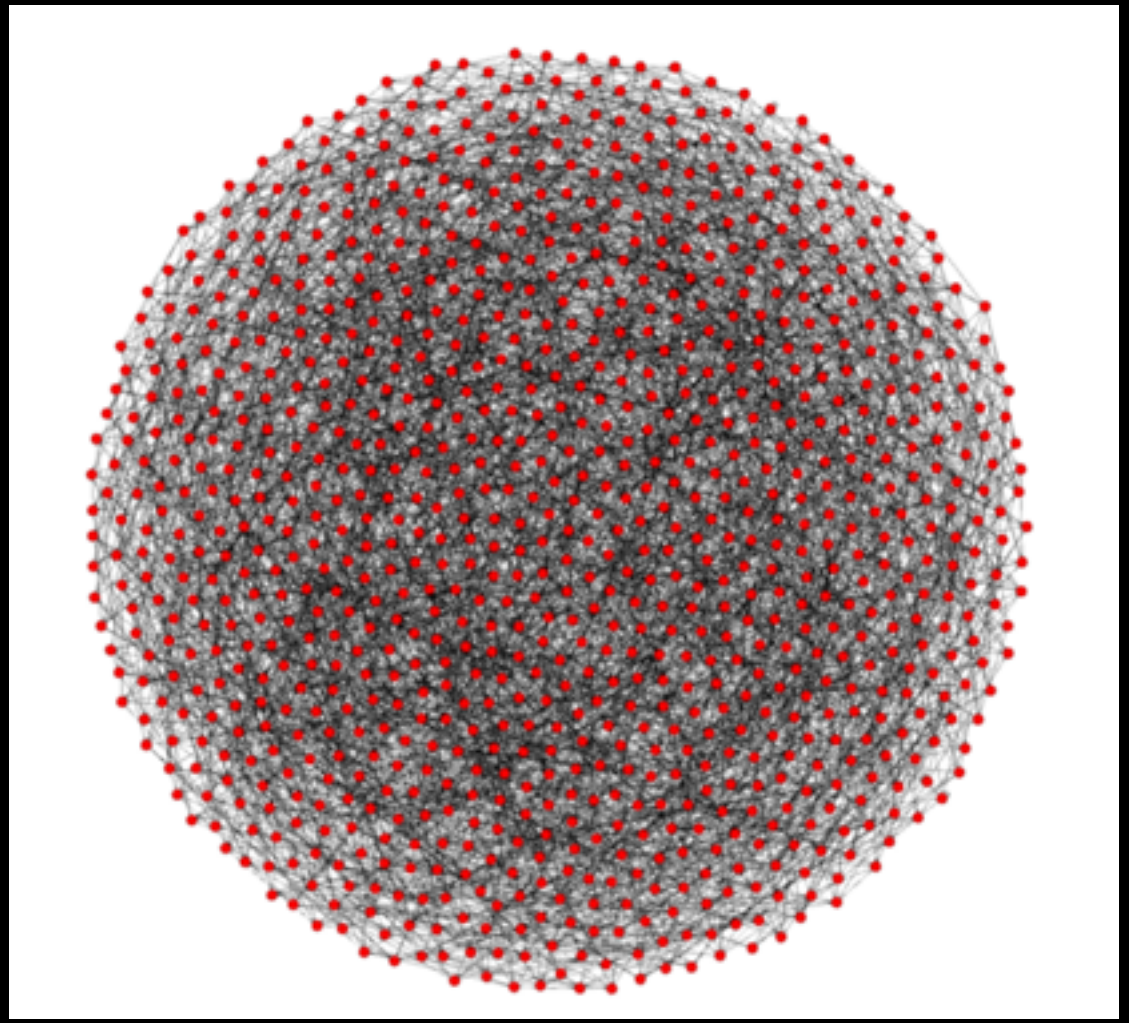
More (103) »




Map shows concentration of reachable Bitcoin nodes found in countries around the world

Onchain

# Blockchain Network



Onchain

# PoW and PoS

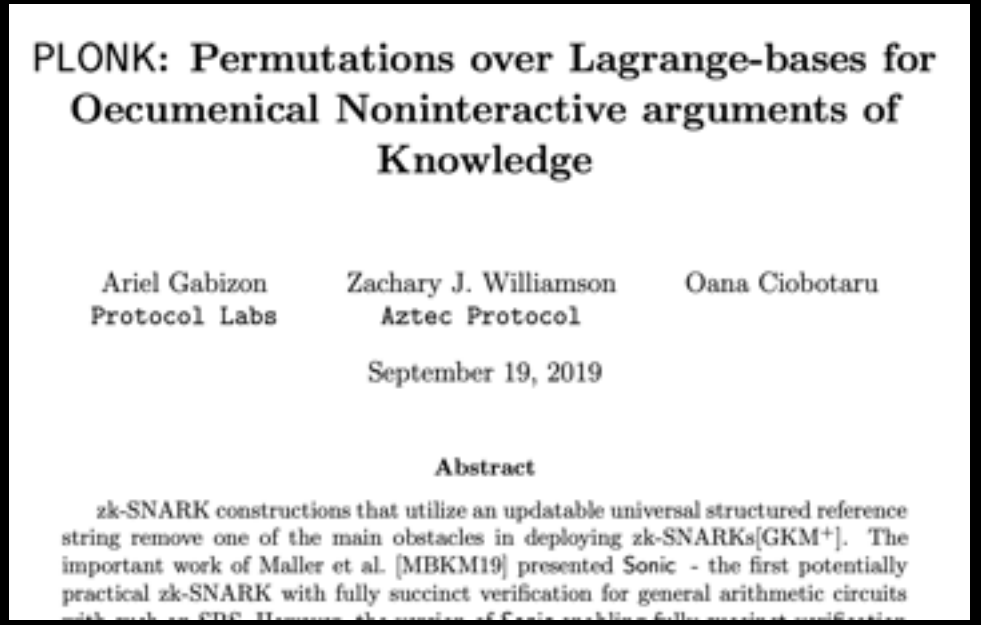
- If there are many nodes, who can create a block?

- PoW: choose randomly based on computing power
- PoS: choose randomly based on coins
- BFT

Onchain

# General Purpose ZKP

- Prove results of computation without revealing data
- Useful for enhancing privacy of blockchain applications
- Proofs can be verified much more quickly than the original computation, also useful for scalability.



PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge

Ariel Gabizon
Protocol Labs

Zachary J. Williamson
Aztec Protocol

Oana Ciobotaru

September 19, 2019

**Abstract**

zk-SNARK constructions that utilize an updatable universal structured reference string remove one of the main obstacles in deploying zk-SNARKs[GKM+]. The important work of Maller et al. [MBKM19] presented Sonic - the first potentially practical zk-SNARK with fully succinct verification for general arithmetic circuits

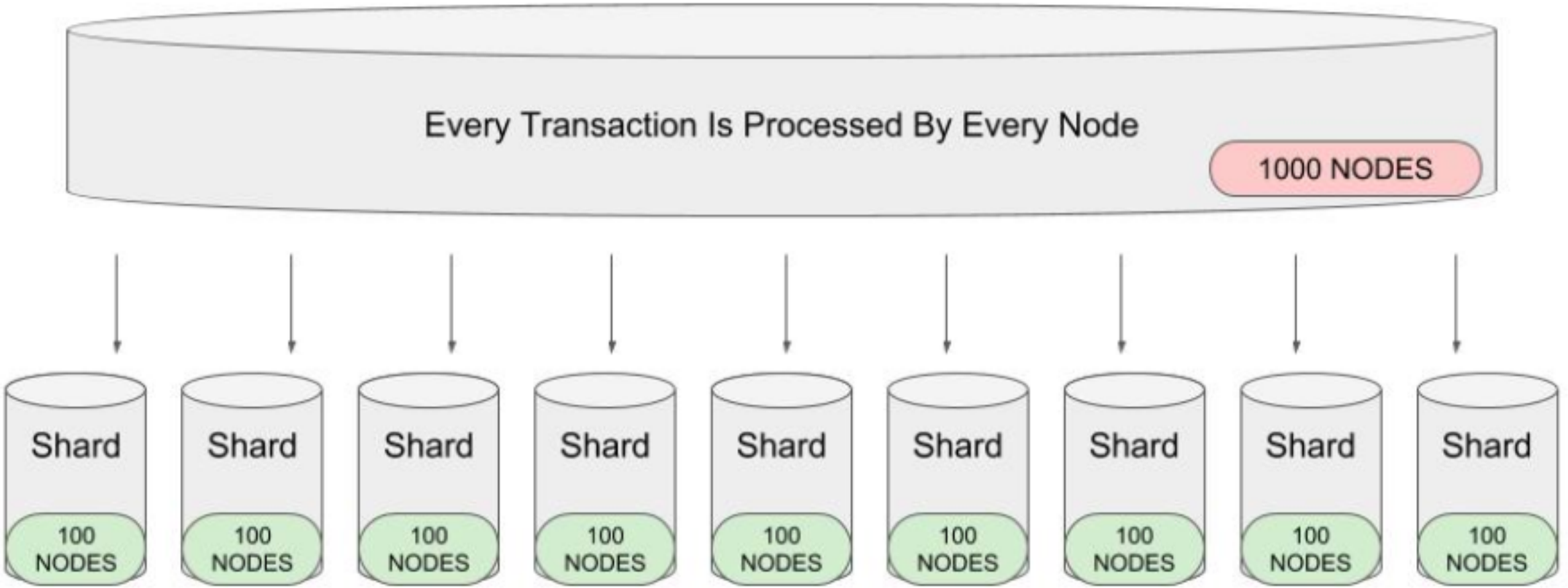
Onchain

# Blockchain Scalability

- Sharding
- Plasma
- Channels
- Offchain scalability

Onchain

# Sharding



Onchain

# What can blockchain do?

- Cryptocurrency for payments
- DNS
- Digitally representing assets
  - Badges
  - Conference tickets
- Smart-contract applications
- DAO
- Crypto-Economics

Onchain

# Smart Contract Applications

- Outsourced computation and storage
- Provable fair random number generation
- Providing true info about the real world
- DAO
- Bounties for solutions to math or CS problems

Onchain

# DAO

- (Decentralized Autonomous Organization)
- Smart contract that controls digital assets, and controls how a group of people can their collective resources.

- MakerDAO
- MolochDAO
- Aragon
- Used for
  - Charities
  - Open-source development

Onchain

# Crypto-Economics

- Using **cryptography** and **economic incentives** to achieve information security goals
  - Cryptography can prove properties about messages that happened *in the past*
  - Economic incentives defined inside a system can encourage desired properties to hold *into the future*

Onchain

“You know, there's sort of these two polarizing perspectives, right? Everything is great, the Internet has created all this freedom and liberty, and everything's going to be fantastic. Or everything is terrible, the Internet has created all these tools for cracking down and spying, and controlling what we say.  And the things is, both are true, right? The Internet has done both, and both are kind of amazing and astonishing and which one will win out in the long run is up to us.”

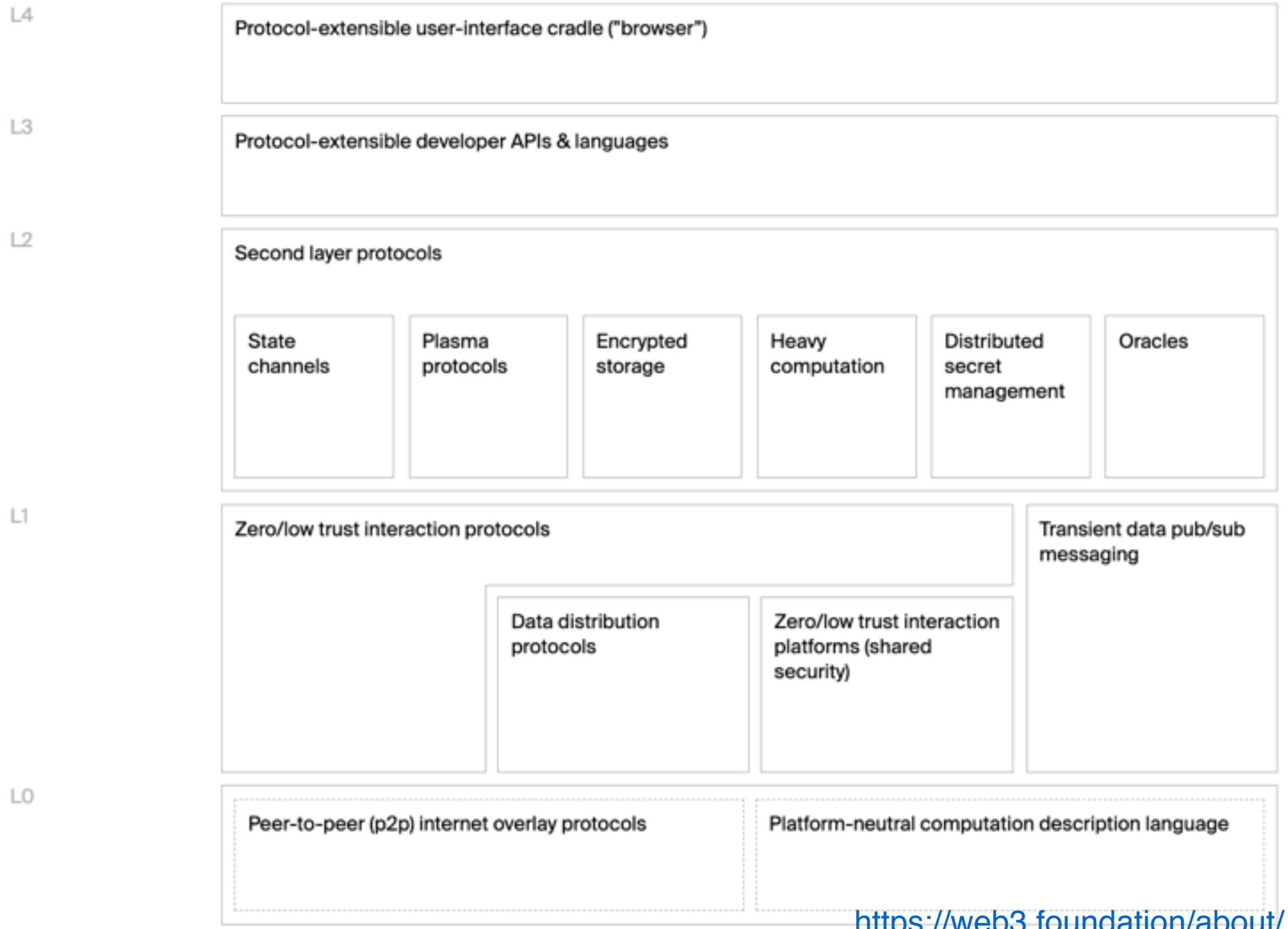
-- Aaron Swartz, Jul. 10th, 2012

Onchain

# Next Generation Internet

building a trustless infrastructure that empowers users to resist arbitrary authority and take back control of their sovereignty

- Facilitate Collaboration
- Ensure Transparency
- Progress Society




https://web3.foundation/about/

Onchain

# Decentralized Network Architecture

- Decentralized Network
- Consensus
- Compiler & Virtual-Machine
- Cryptographic
- Decentralized Storage
- Open Blockchain Platform

# THANKS!

Onchain

上海分布信息科技有限公司
Shanghai Distributed Technologies Co., Ltd.

contact@onchain.com

**onchain.com**