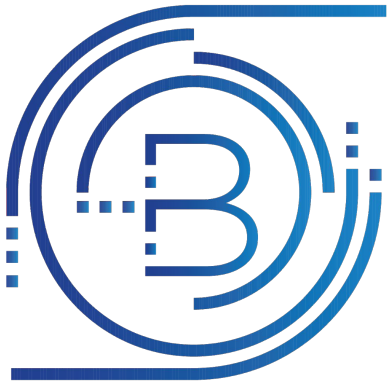
How Blockchains work and How to Scale Them



BLOXROUTE

LABS

Uri Klarman | June 2018

Agenda

- bloXroute who?
- Blockchains 101
- The Scalability Problem
- bloXroute Design
- Q&A

BLOXROUTE
LABS

bloXroute Who?

- Crypto & Networking Experts
- Cornell & Northwestern University
- Google's M-Lab, IC3 Falcon Network
- Scalability Infrastructure

BLOXROUTE
LABS

Blockchains 101

- Bitcoin - 1st blockchain, still golden standard
- **Goal: cut out financial middlemen**

<u>Money that is:</u>

- easy as Credit Cards, w/o 3% fees
- Safe as a bank, w/o bank fees

BLOXROUTE
LABS

Blockchains 101

Cut out financial middlemen

- How does it work?

Alice wants to buy an apple from Bob 

BLOXROUTE
LABS

Blockchains 101

Cut out financial middlemen

1. Every user has a *wallet*

Public key (address) - send money here!

8a792d3fb9823a4987624d7623be454

Private key - proves ownership of public key

92cb55a01d55c97a899c2197a9b452f3

BLOXROUTE LABS

Blockchains 101

Cut out financial middlemen

2. Alice buys Apple from Bob

   She creates a transaction:

   a. From: Alice (public key)
   b. To: Bob (public key)
   c. Signed by: Alice private key

BLOXROUTE LABS

Blockchains 101

Cut out financial middlemen

3. Transaction propagated to entire P2P network

BLOXROUTE
LABS

Blockchains 101

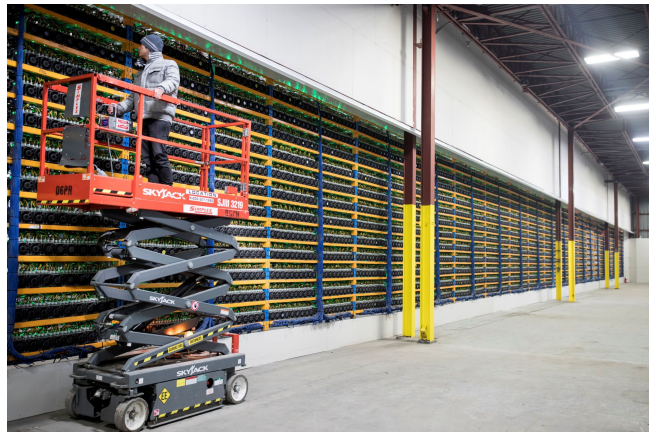
Cut out financial middlemen

4. *Miners*:
    a. Listen to transactions
    b. Aggregate Txs into *blocks*
    c. Each block reward it miner

BLOXROUTE
LABS

Blockchains 101

Cut out financial middlemen



5. Mining steps:
    a. Aggregate Txs in *block*
    b. Hash block and arbitrary value (*nonce*)
    c. Try different values until valid (result < target)
    d. Propagate to P2P

BLOXROUTE LABS

Blockchains 101

6. **Outcome:**

BLOXROUTE
LABS

Blockchains 101

6. **Outcome:**
    a. Entire history of Txs in a chain of blocks - the blockchain (longest blockchain is Truth)

Blockchains 101

Important!

Miners Hash:

a. Txs in block
b. Nonce
c. Hash of prev. block

BLOXROUTE
LABS

Blockchains 101

6. **Outcome:**
    a. Entire history of Txs in a chain of blocks - the blockchain (longest blockchain is Truth)
    b. For attacker to change history (add/remove) must revalidate consecutive blocks

BLOXROUTE
LABS

Blockchains 101

6. **Outcome:**
    a. Entire history of Txs in a chain of blocks - the blockchain (longest blockchain is Truth)
    b. For attacker to change history (add/remove) must revalidate consecutive blocks
    c. Faster than everyone else combined

BLOXROUTE LABS

Blockchains 101

6. **Outcome:**
    a. Entire history of Txs in a chain of blocks - the blockchain (longest blockchain is Truth)
    b. For attacker to change history (add/remove) must revalidate consecutive blocks
    c. Faster than everyone else combined
    d. Fork: when 2 blocks mined at ~same time

BLOXROUTE LABS

Blockchains 101

- Blockchains **ARE NOT** useful if you:
  - Trust (banks move money between accounts)
  - Trust (Servers to hold data)
- Blockchains **ARE** useful for:
  - Interaction w/o middleman
  - Immutable Data w/o trust
  - Visibility (anti-corruption)

BLOXROUTE
LABS

The Scalability Problem

- Bitcoin is GREAT! But...
- 1MB-block/10min + 540B Tx = ~1900 Tx / 10 min
- **~3 Tx/sec (TPS)** (Similar for all blockchains)

BLOXROUTE
LABS

The Scalability Problem

- Use cases:
  - Credit Cards — 5,000 TPS
  - Vending Machines (4/day) — 1,000 TPS
  - Autonomous Robot-chains — 50,000 TPS
  - Global micro-payments — 70,000 TPS
  - Social Media (4 likes/day) — 200,000 TPS

BLOXROUTE LABS

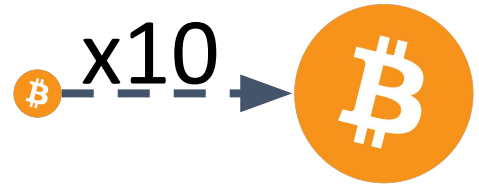
The Scalability Problem

- Bitcoin capacity is just too small
  - Increase block size?
  - Reduce time between blocks?

BLOXROUTE LABS

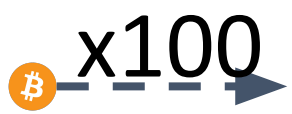
The Scalability Problem

- block size x10
- Sending block A→B takes x10 longer
- x10 longer to entire network (Empirically shown)
- **x10 more forks!**
- Even in Optimal Scenario
- It still works



BLOXROUTE
LABS

The Scalability Problem



- block size x100
- x100 longer to propagate
- **Longer than 10 minutes interval!**
- Fork ~every block
- Forks of forks of forks… blockchain breaks
- This **IS** the scalability problem

BLOXROUTE
LABS

The Scalability Problem

- Fork Probability depends on ratio:

$$\frac{Propagation\ Time}{Block\ Time\ Interval}$$

- Block Size and Block Interval has same effect
- Permissioned blockchains similarly restricted
  - IBM/Hyperledger requires same data center
  - Conflicts with regulations

BLOXROUTE LABS

Scalability Solution

- A Networking Problem
- Wait… We know how to send a lot of data…

- Sending Terabytes to Billions of users
- Akamai solved it (’96)

BLOXROUTE
LABS

Relay Networks

- Highly-connected networks of servers

Send to Relay - Relay **Broadcasts**

- Deployed in 2015
- ~10 sec. propagation today

BLOXROUTE
LABS

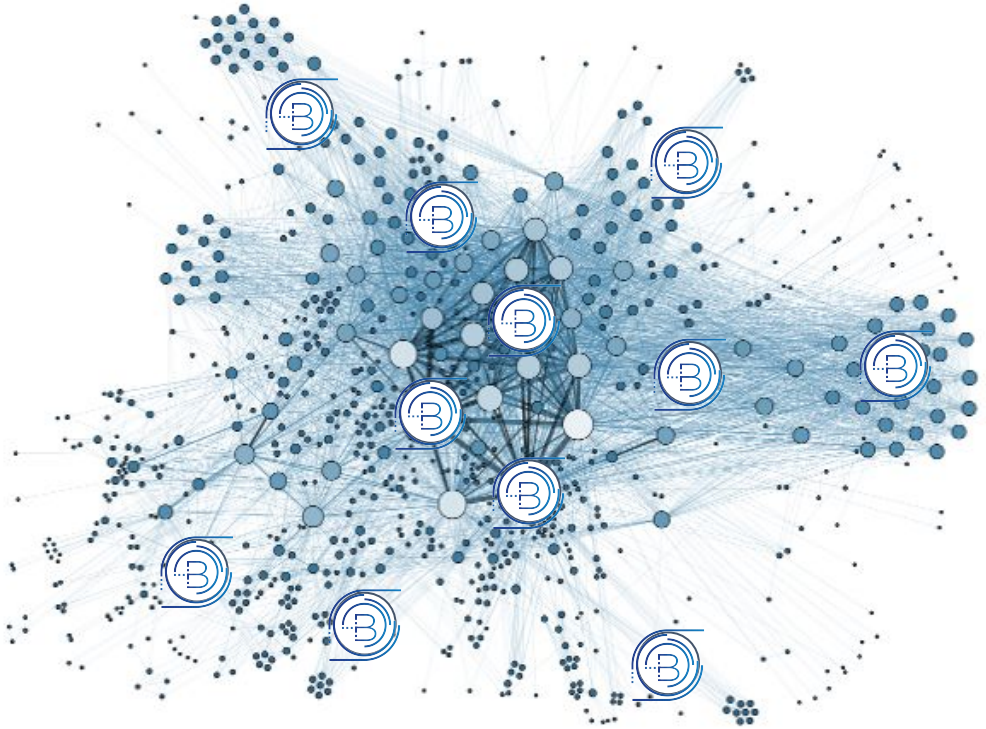
Relay Networks

- If **Protocol** depend on Relay...
- …Relay decides what goes on blockchain
- Censorship
- Discrimination
- Ban Wallets
- Requires everyone's trust - *what's the point?*

BLOXROUTE
LABS

bloXroute!

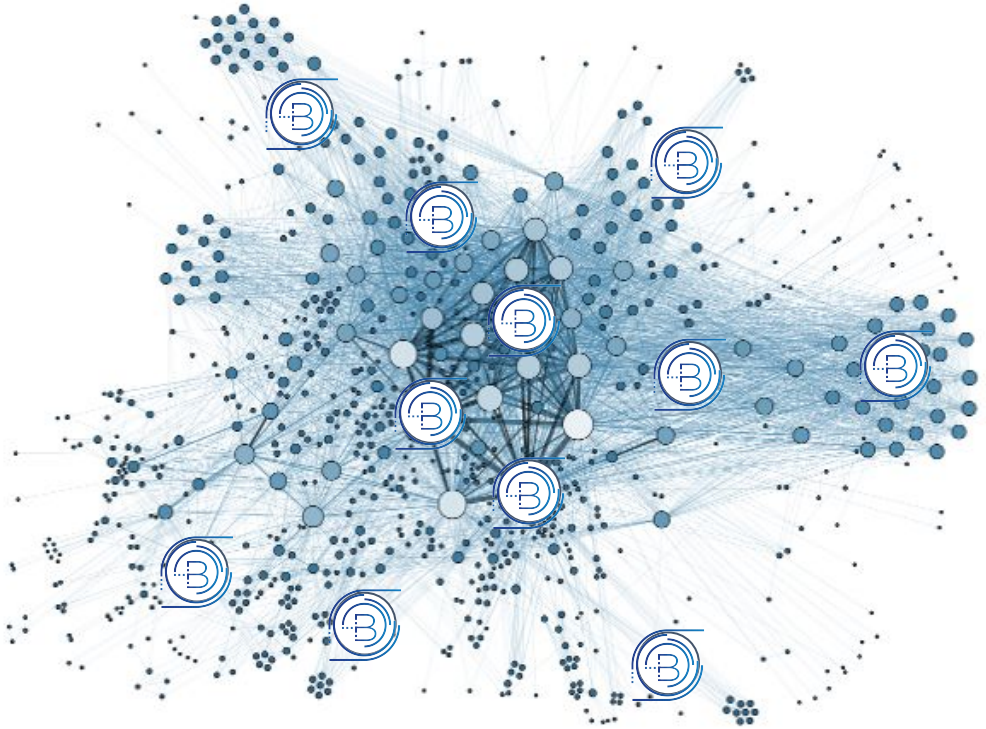
- Blockchain Distribution Network (BDN)
- New network primitive
- Similar to Relay
- **Provably Neutral**



BLOXROUTE
LABS

how bloXroute works?

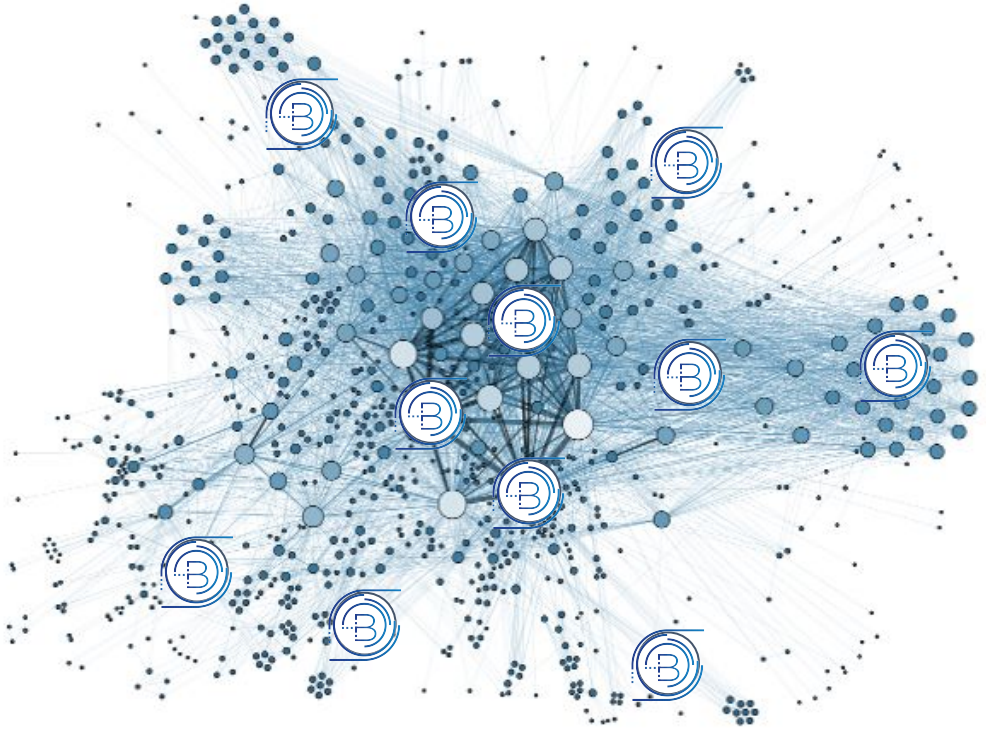
- Open-source “Magic Gateway”
- Runs on same machine
- Acts as Peer



BLOXROUTE
LABS

Performance

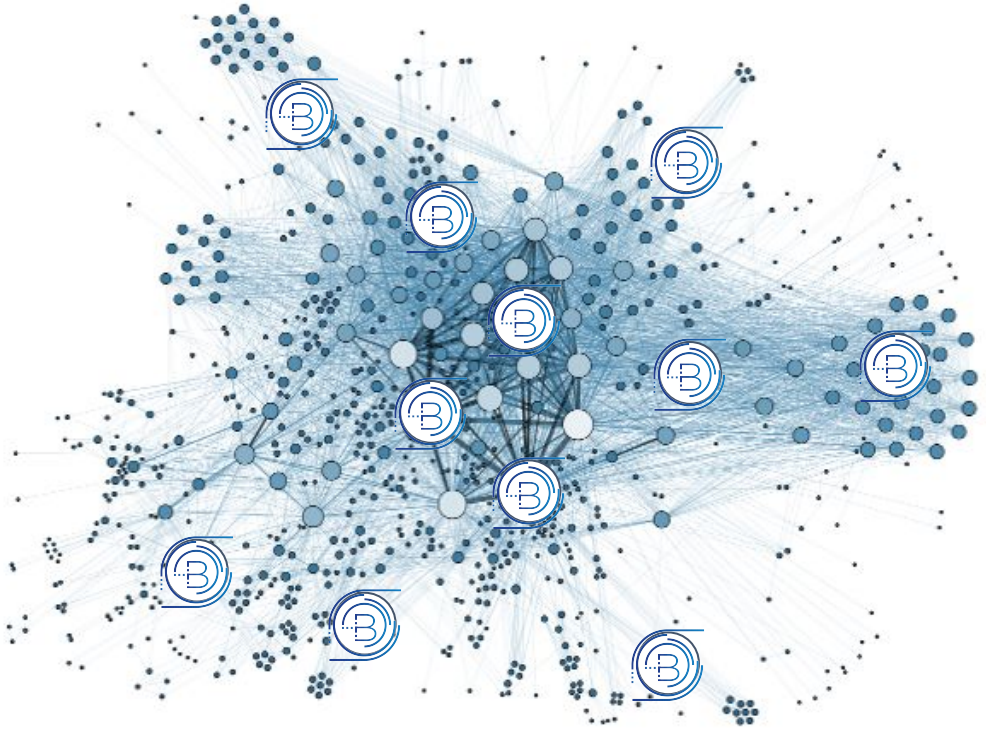
- x1000 faster than peer
- 540B Tx -> 3B ID (internal)
- Stream blocks
- Very Simple Techniques



BLOXROUTE
LABS

Neutrality

- Hide content, source, destination
- Encrypted Blocks
- Send Key Afterwards
- Relay via Peer (TOR-like)
- Receive via Peer



BLOXROUTE
LABS

Other Scaling Alternatives

- Sharding (layer-1)
- Lightning / Plasma (layer-2)
- Blockchain VS. DAG (e.g. Hashgraph)

BLOXROUTE
LABS

Questions?

Also… We're Hiring
Python, Linux and Networking Devs!
bloxroute.com/careers/

BLOXROUTE
LABS