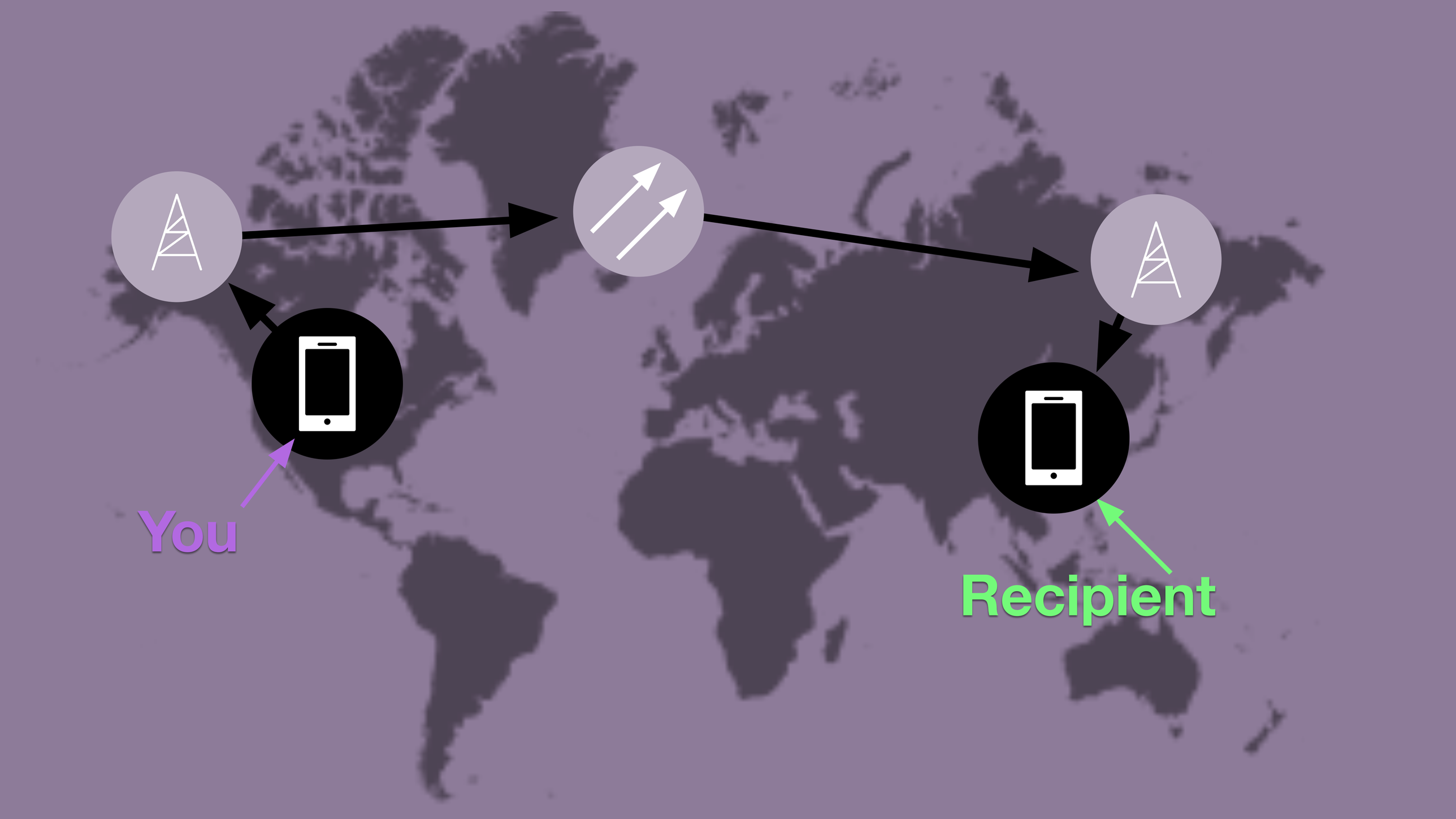
Incentivizing Mobile Mesh Networks with Bitcoin Lightning

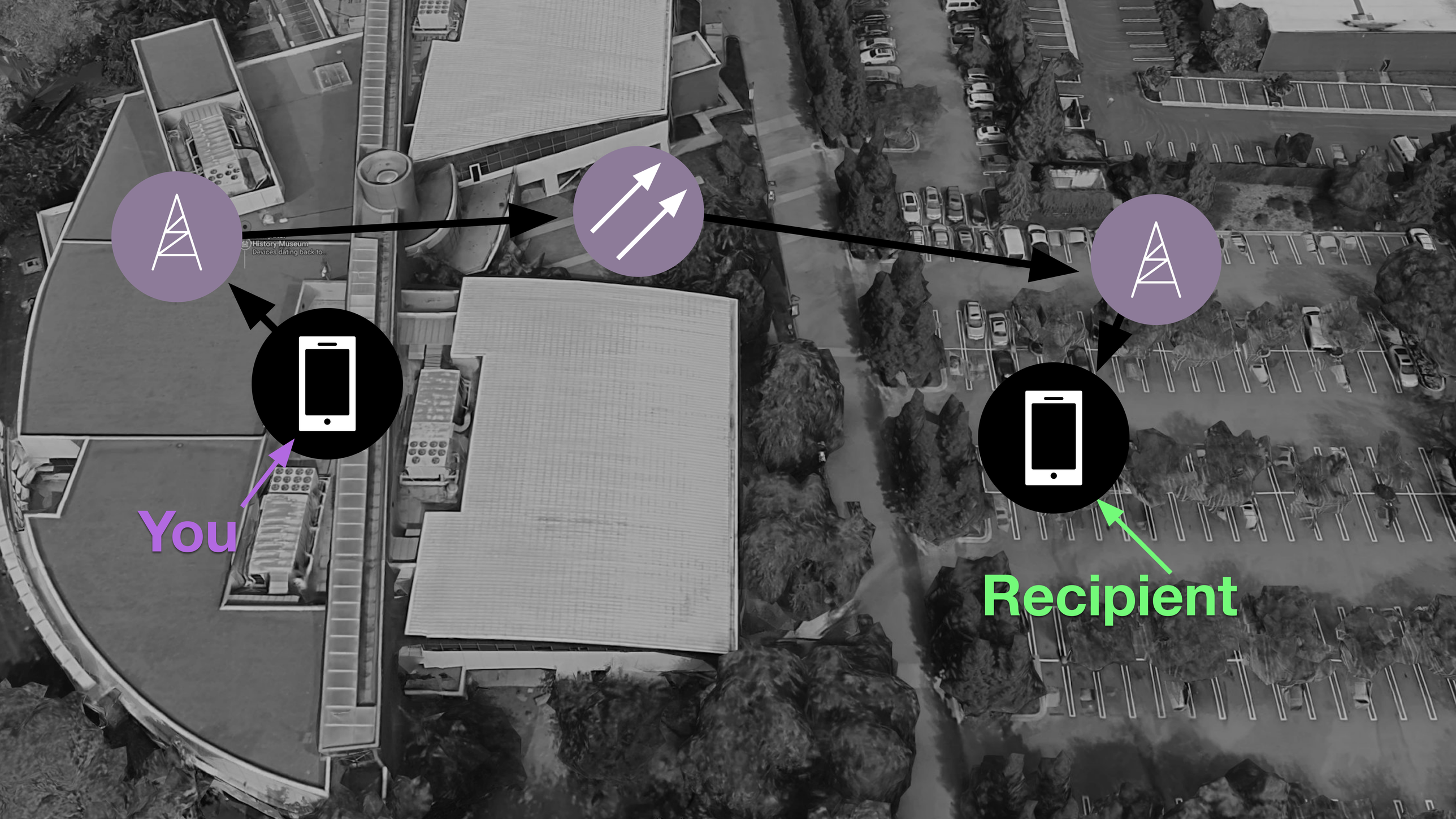
Daniela Perdomo, co-founder & CEO, goTenna
Richard Myers, Software Engineer at Global Mesh Labs

10 July, 2019

@GlobalMeshLabs

WILL THE DECENTRALIZED INTERNET RUN ON CENTRALIZED CONNECTIVITY?


You
Recipient


History Museum
Devices dating back to...
You
Recipient


フジテレビ
7/25(水)
8.24
ROAD TO NINJA
大盛堂書店

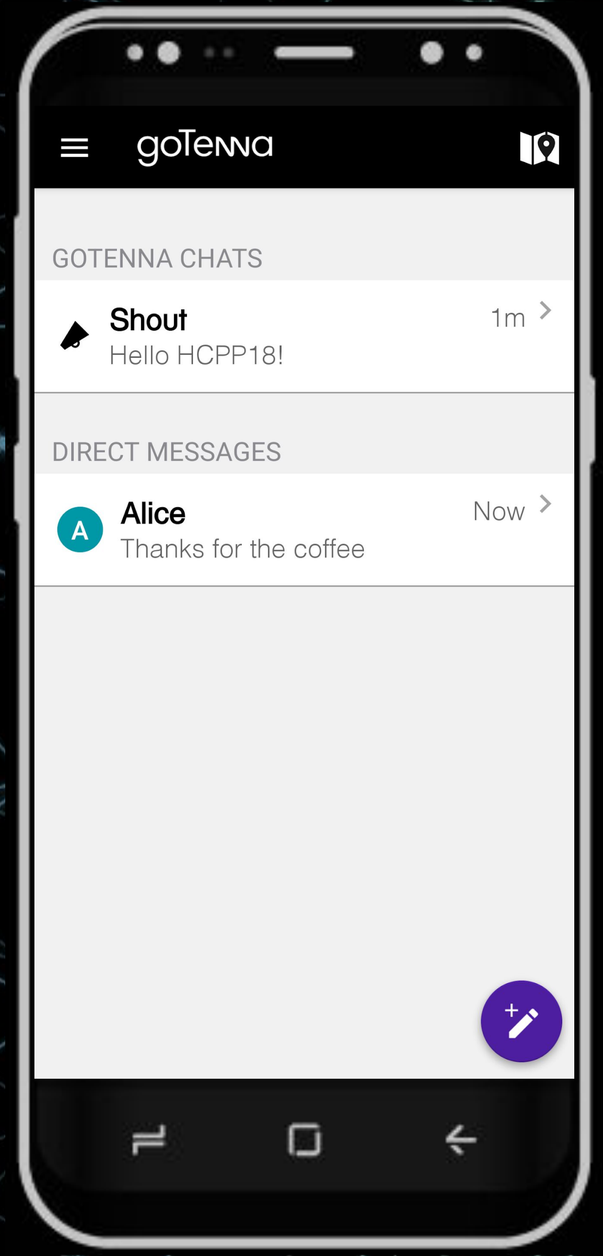
OUR PHONES ARE DESIGNED TO NOT ENABLE PHONE-TO-PHONE COMMUNICATION AT ANY USEFUL DISTANCE


Finland
Iceland
Sweden
Norway
Russia
Kazakhstan
Mongolia
Japan
Afghanistan
Pakistan
Iraq
Iran
Turkey
Algeria
Libya
Egypt
Saudi Arabia
Mali
Niger
Sudan
Chad
Nigeria
Ethiopia
Kenya
DRC
Tanzania
Angola
Namibia
Botswana
Madagascar
South Africa
Thailand
Indonesia
Venezuela
Colombia
Peru
Bolivia
Chile
Argentina
North Atlantic Ocean
South Atlantic Ocean
Indian Ocean
MTN


CENTRALIZED ≠
RESILIENT

THE WORLD'S FIRST OFF-GRID, LONG-RANGE, MOBILE, CONSUMER-READY MESH NETWORK

FREE MESSAGING, E2E ENCRYPTED UHF - ISM BAND EASY TO USE P2P TRANSPORT



DENSITY = CAPACITY

Destination

Relay Node

Connection

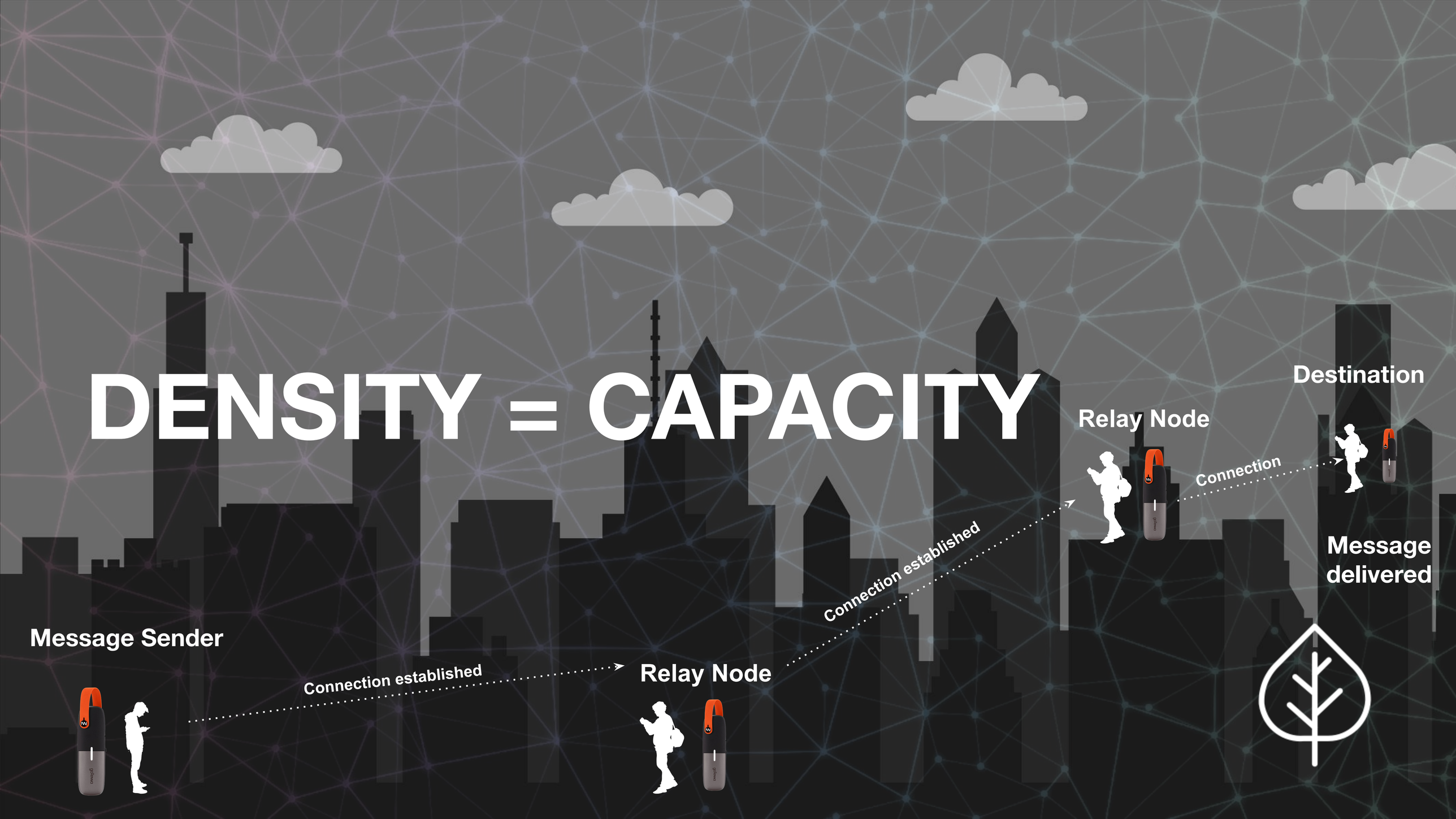
Connection established

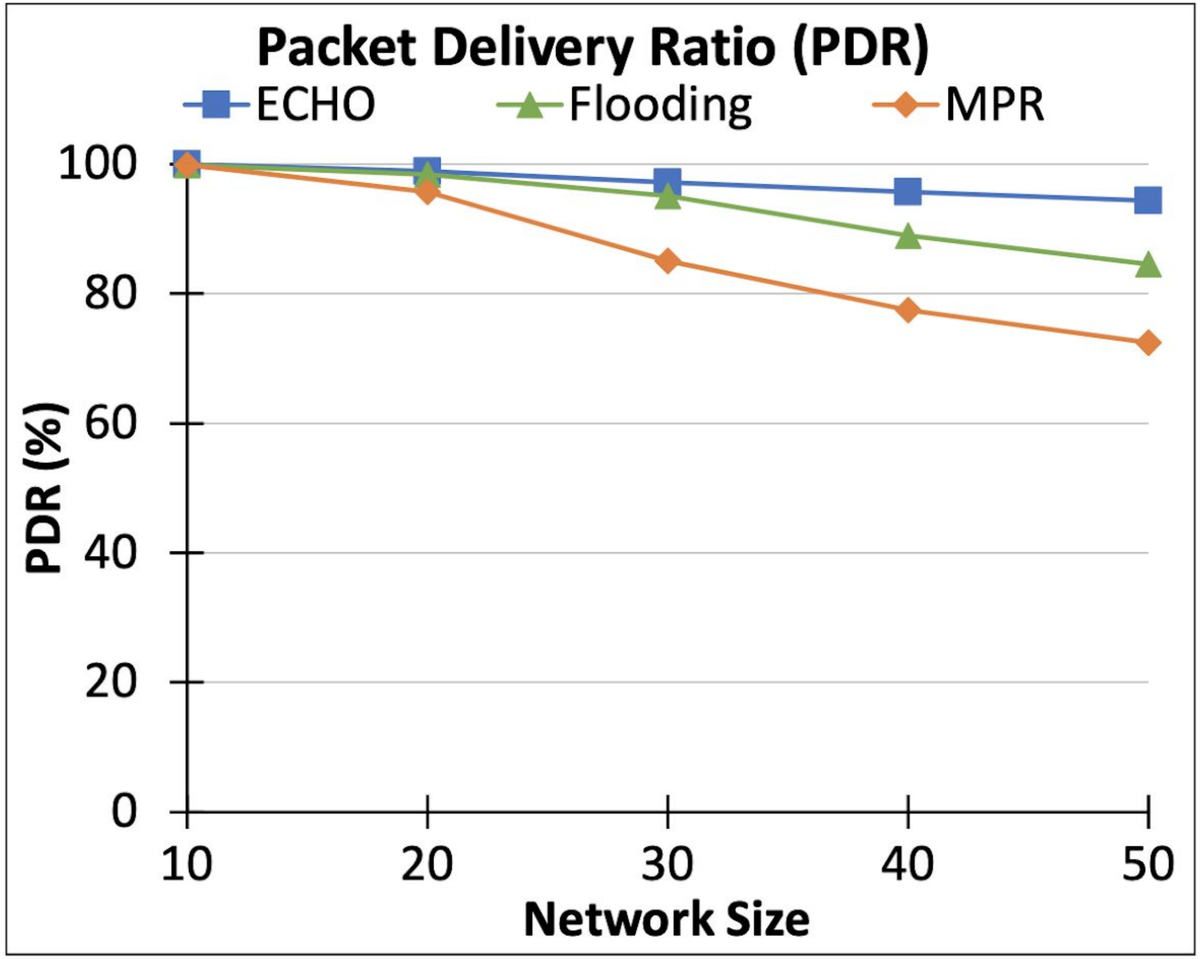
Message delivered

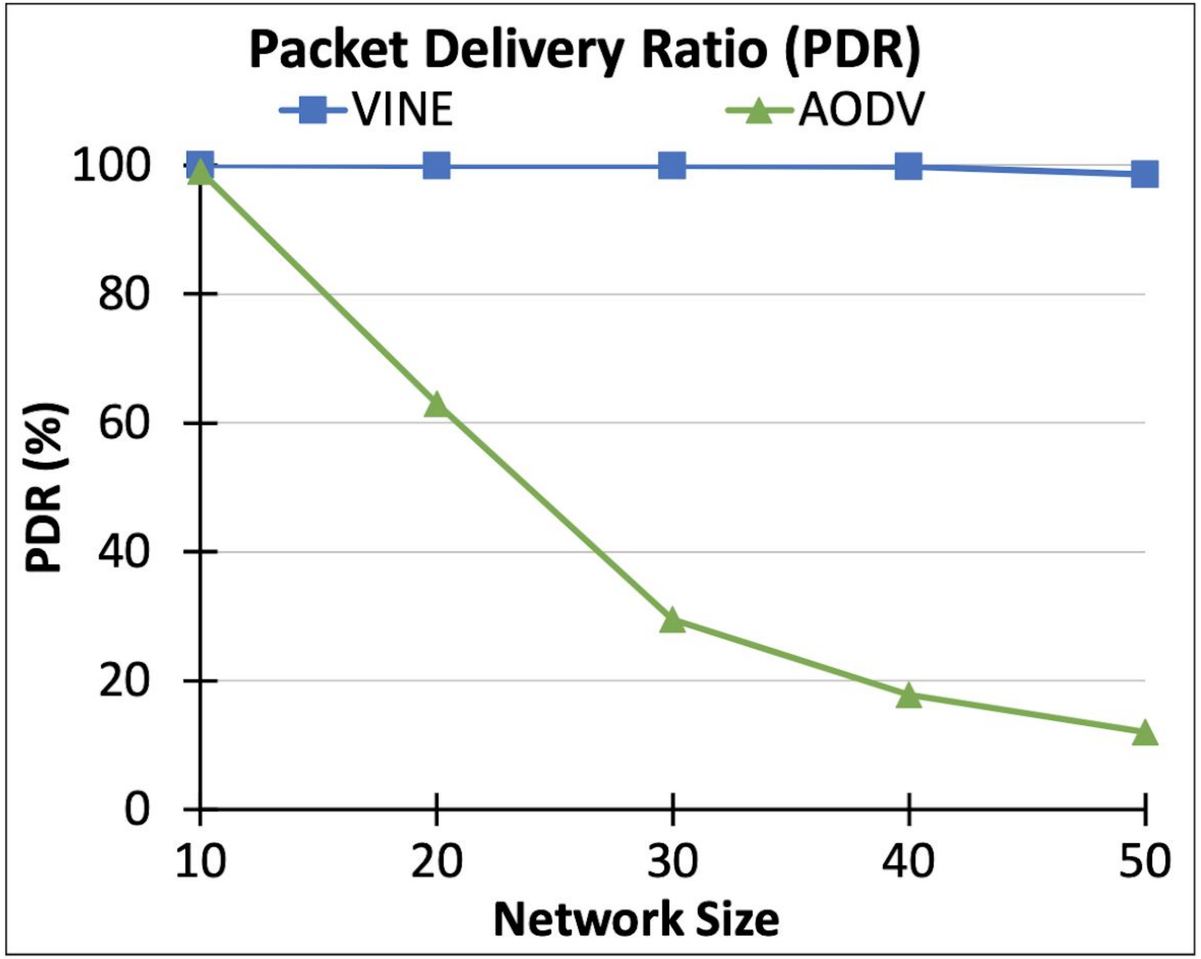
Message Sender

Connection established

Relay Node







(a) Broadcasting (b) Unicasting

Fig. 2. Simulation results using ns3 models.

HOW DO WE INCENT PARTICIPATION SO IT BECOMES THE MESH NETWORK IT CAN BE?

ZERO-START

COVERAGE

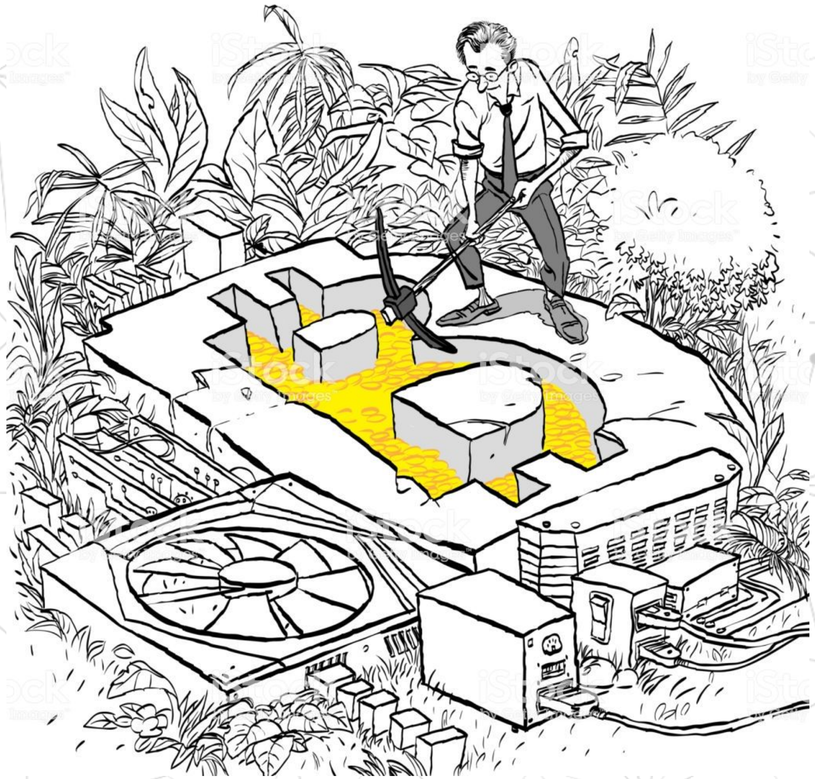
CAPACITY

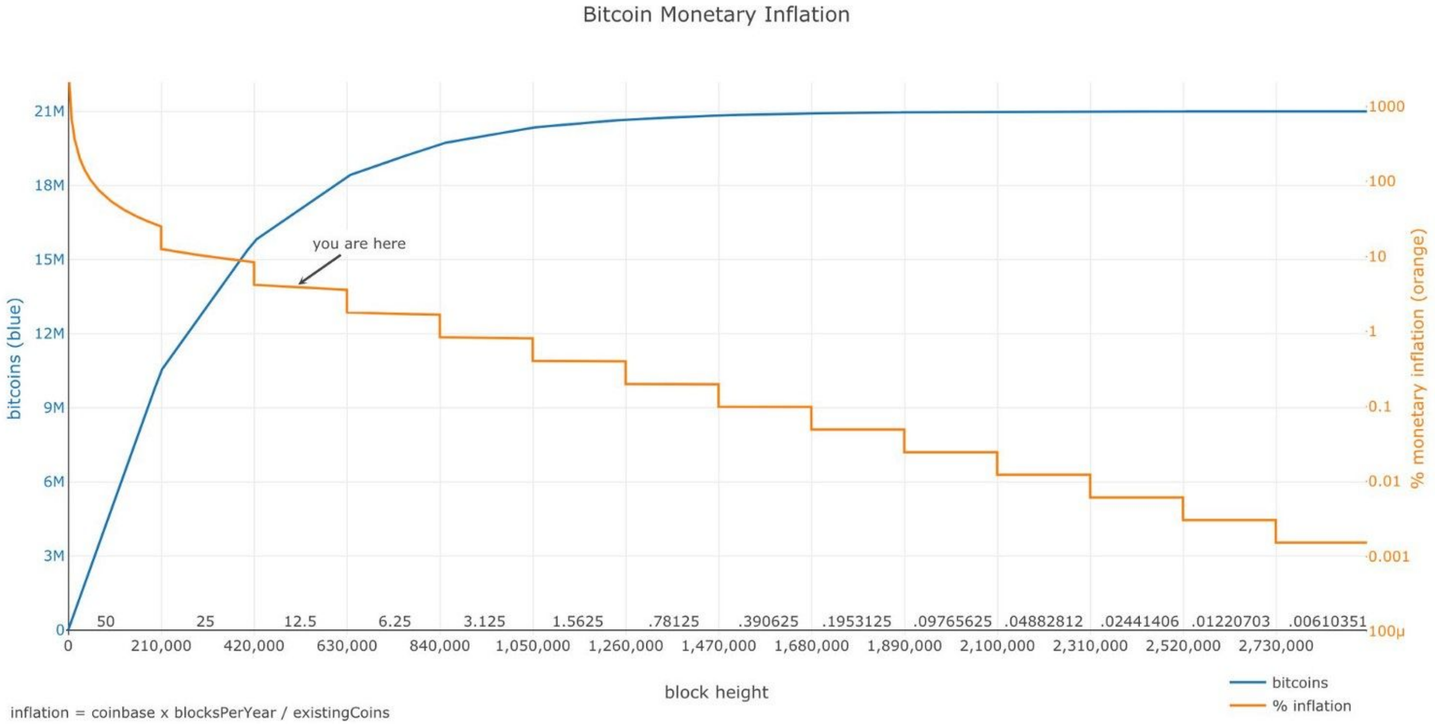
POWER

SPECTRUM

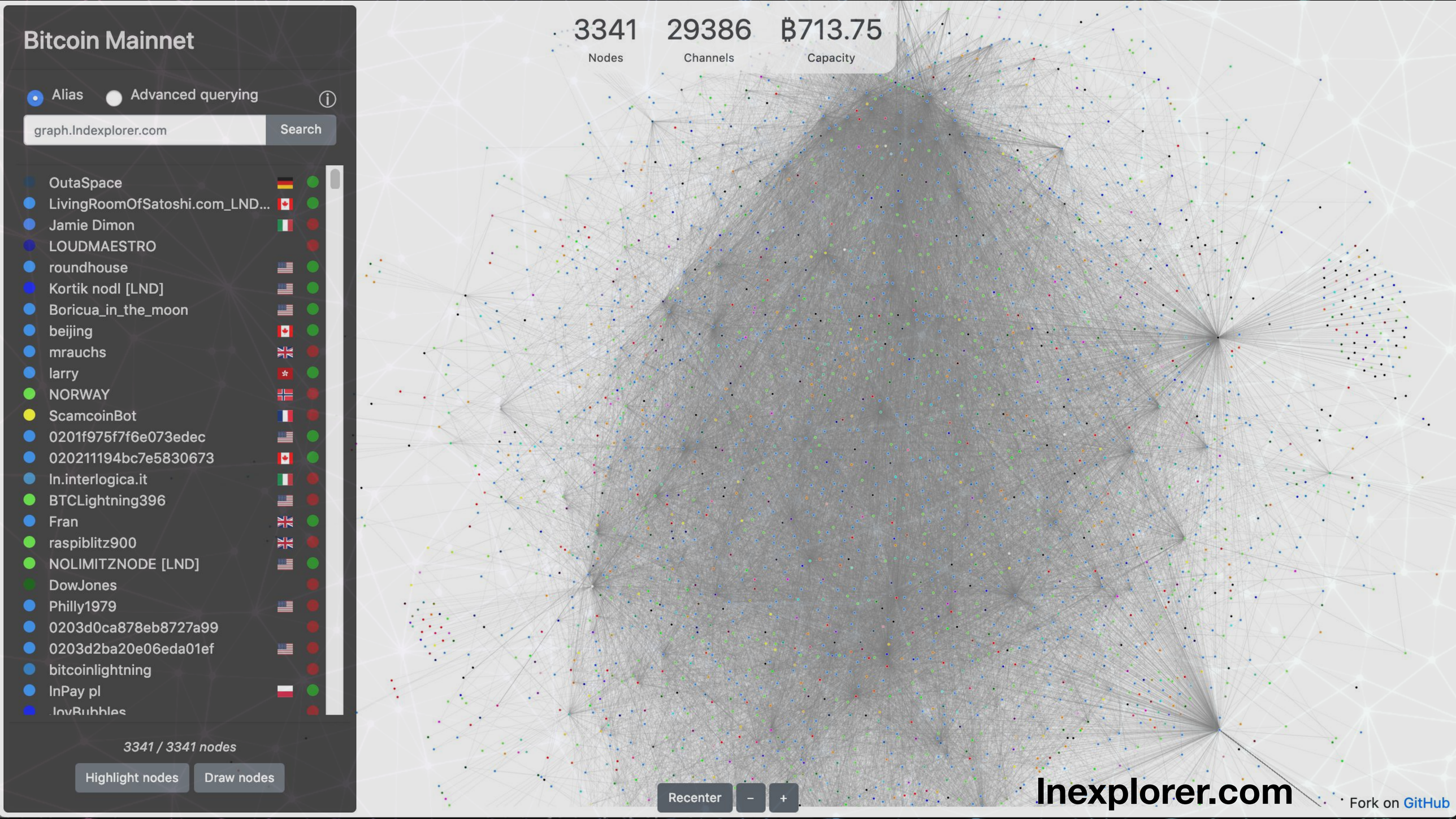
LOCAL V. GLOBAL

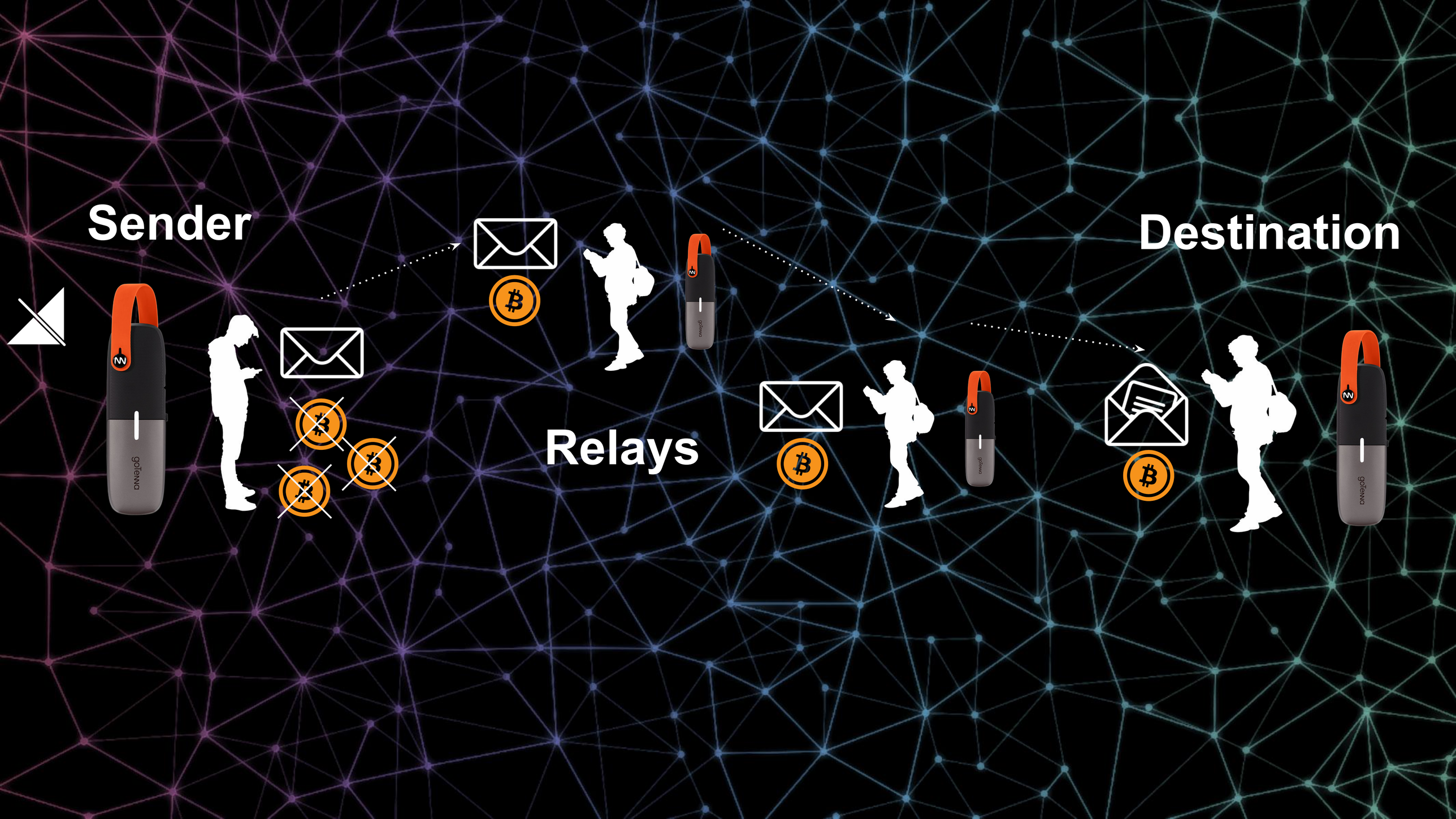
NETWORK INTEGRITY



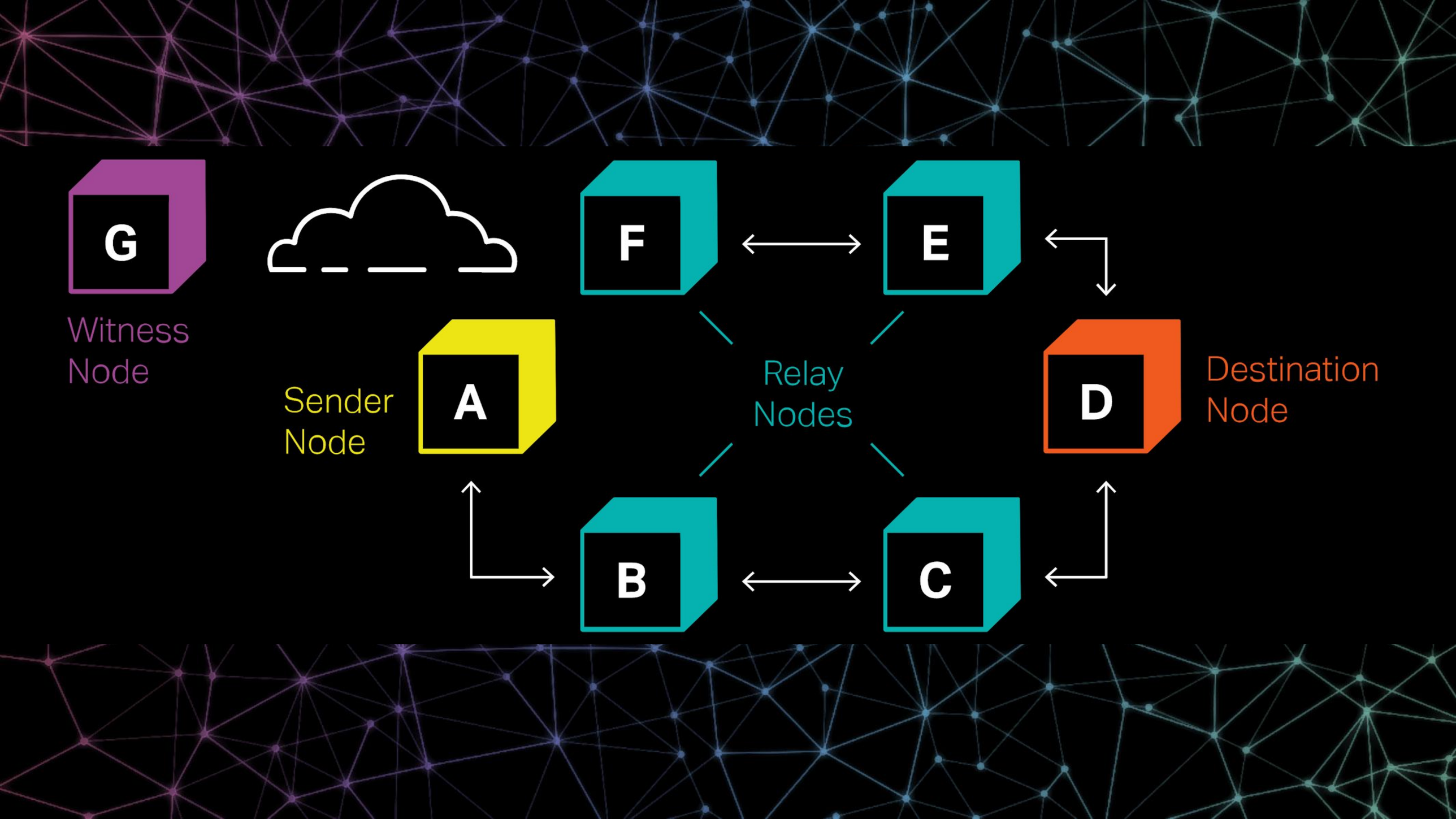


inflation = coinbase x blocksPerYear / existingCoins


Bitcoin Mainnet
Alias
Advanced querying
graph.lndexplorer.com
Search
OutaSpace
LivingRoomOfSatoshi.com_LND...
Jamie Dimon
LOUDMAESTRO
roundhouse
Kortik nodl [LND]
Boricua_in_the_moon
beijing
mrauchs
larry
NORWAY
ScamcoinBot
0201f975f7f6e073edec
020211194bc7e5830673
ln.interlogica.it
BTCLightning396
Fran
raspiblitz900
NOLIMITZNODE [LND]
DowJones
Philly1979
0203d0ca878eb8727a99
0203d2ba20e06eda01ef
bitcoinlightning
InPay pl
3341 / 3341 nodes
Highlight nodes
Draw nodes
3341
Nodes
29386
Channels
฿713.75
Capacity
Recenter
–
+
lnexplorer.com
Fork on GitHub


Sender
Relays
Destination

“LOT 49”


G
Witness Node
F
E
Sender Node
A
Relay Nodes
D
Destination Node
B
C

LOT49*

- Multi-signatures (MuSig).
- The eltoo channel update scheme.
- Inferred or deterministic transaction data.
- No onions

* LN variant optimized for mobile mesh data networks

BANDWIDTH

- Aggregate signatures for channel setup and close transactions to reduce overhead.
- Smaller updates with simplex payments.
- Opportunistically checkpoint intermediate states; no punishment.

OFF-GRID

- Some transactions must still be verified and settled on-chain.
- Requires channels with nearby nodes.
- Inferred public keys and signature aggregation could reduce security.

REQUIREMENTS

- Soft fork changes to Bitcoin:
  - Eltoo: Sighash noinput or anyprevout*
  - Multi-signatures: Schnorr / MuSig

GENERAL ISSUES

- Amortizing payment overhead over multiple messages risks delivery failure when topologies change.
- The ‘Fair Exchange’ problem at the last hop can not be easily avoided.
- Trust minimized offline transaction verification.

FINAL THOUGHTS

- High incentive protocol overhead impacts the overall capacity of a network.
- Signature and public key data are the long tentpoles.

FUTURE

- Channel Factories / State Chains
- Off-grid blockchain sync
-

SCALABLE MOBILE AD HOC INCENTIVIZED MESSAGING DECENTRALIZED OPEN SOURCE PROTOCOL

HELP US!

Useful cryptographic trick?
Low bandwidth channel setup system?
Better aggregation method?

Learn more about goTenna Mesh and Global Mesh Labs at:
goTenna.com & GlobalMeshLabs.org
@GlobalMeshLabs