

Skynet: a decentralized platform of “Nano” Communication Satellites in LEO-orbit to extend Off-chain networks Physical topology

White paper(first draft)

Amro saeed*

Oct 20, 2018 (Version 1.0)

Abstract

Solving an efficient routing path in the Lighting Network or any of future's off-chain layers that tries to afford scalability on-chain within its blockchain and with concerning source-routing scheme would eventually produce a solution its abstraction becomes the first general solution for mesh networking, under the current computing architecture (von Neumann's), and as quantum computing is still in its theoretical and early experimental phases, unfortunately it would be near impossible to solve such problem, especially when blockchain's developers relaying solely on software vector, it is not feasible now or in the near future until 2050 when quantum computing would be reality, without even mentioning the concepts and requirements imposed by the Blockchain community, which adds a new level of complexity to develop a propriety solution to such problem, parallel to the fast pace of changes at the economic side where cryptocurrencies suffers the most and specially Bitcoin from being mainstreamed, a huge need emerged to the surface to find a solution fast enough for cryptocurrencies to avoid economical relapses and losing its current momentum at the time of writing this paper, The philosophy behind This paper is to set the foundations of building a platform of hardware components in space as a Blockchain network's backhaul and inheriting Blockchain's special characteristics of decentralization and distribution of its ownership to the community, extending Blockchain's networks physical topology out of the reach of any centralized institution on the planet while introducing scalability will be the final frontier under von Neumann's computing architecture, the paper tries to find the suitable placement of such network in Blockchain's ecosystem shadow, and it specially targets Cryptocurrencies which by its role drives Blockchain's community financially towards developing the technology.

© 2018 Dixipay Group Limited

Without permission, anyone may use, reproduce or distribute any material in this paper for noncommercial and educational use (i.e., other than for a fee or for commercial purposes) provided that the original source and the applicable copyright notice are cited.

*a.amin@dixipay.com, Dixipay group

Introduction

Physical topology an important playground

Physical topology of a network is defined simply as the placement of the various components of that network in geographic locations (e.g., device location and cable installation) to extend the reach of the network, in the light of recent advancements in cryptocurrency fields, specially in routing algorithms (e.g., Flare algorithm) that has been proposed to be applied in lighting network a problem faces

Skynet a Nano-satellite communication network:

In conclusion Skynet is a constellation of custom-designed Nano satellites “Cubesats” that works as an orbital vector for Lighting Network as both proactive & reactive LN nodes out in space, it works in the context of Flare algorithm a hybrid routing algorithm, forming a global network map for LN nodes with specific goal of decentralization Lighting Network routing and such network mechanisms paving the way for Blockchain’s applications to get rid of centralized internet backhaul on the planet and reaching broader access for all Blockchain applications users worldwide, On a border sense the paper goal is to Harness Network routing to simulates as the core solution for different Blockchain’s networks as the solely practical distributed and decentralized solution for circulation of currency whether its crypto or fiat as a medium of exchange, by providing the opportunity to open payment channels or form micro decentralized exchanges among different nodes which by its role can play in different modes depending on their placements in the network physically and/or logically, Emerging of new technology the (Cubesat) Concept helps to build a decentralized hardware network by public (Crypto community): modularity of Cubesats (1U, 2U, etc..., easy to design), (COTS) commercial of the shelf components (availability), (P-POD) launched and deployed using a common deployment system (avoiding launching bottleneck), classified in different categories (variety of designs and available capabilities).

Why a decentralized network of hardware to work as internet is essential for cryptocurrency ecosystem now?

- Recent developments in building internet networks in space as SpaceX plans to launch first internet-providing satellites in 2019 The Company will launch additional satellites in phases until 2024, at which point the network should have reached full capacity, with the craft operating on the Ka- and Ku-band frequencies.

Lightning network protocol

We know that lightning is at least technically feasible. We don't know if it's economically feasible or even a desirable alternative. Will it be a decentralized peer-to-peer payment layer or will it end up as a quasi-centralized payment network similar modern banking?

THE ANSWER CAME OUT LIGHTNING NETWORK PAPER

Payment Routing

It is theoretically possible to build a route map implicitly from observing 2-of-2 multisigs on the blockchain to build a routing table. Note, however, this is not feasible with pay-to-script-hash transaction outputs, which can be resolved out-of-band from the bitcoin protocol via a third party routing service. **Building a routing table will become necessary for large operators (e.g. BGP, Cjdns). Eventually, with optimizations, the network will look a lot like the correspondent banking network, or Tier-1 ISPs.** Similar to how packets still reach their destination on your home network connection, not all participants need to have a full routing table. The core Tier-1 routes can be online all the time —while nodes at the edges, such as average users, would be connected intermittently. Node discovery can occur along the edges by pre-selecting and offering partial routes to well-known nodes.

Different settings for the lightning network routing:

- **Hub-and-Spoke network topology:** As a hub-and-spoke payment layer, there would be very few hubs and the network would be quasi-centralized and a regulatory sitting duck
- **Organic, wallet-to-wallet routing:** Bitcoin Core developers have bet the house on it

But there is a catch.....

Routing paths are much harder to find when values are considered.

1. We could end up making more on-chain transactions.....
2. The vast majority of users will be offline.....
3. Channels cannot be created on-the-fly.....
4. Recipients have to be online.

Flare algorithm:

Hybrid routing protocol

Table-driven (proactive) protocol: maintain up-to-date routing information about all the nodes in the network in the form of routing table whether if they are neighborhood, beacon and orbital nodes

On-demand (reactive) protocol: on-demand protocols execute the path-finding only when a path is required and it accomplish that by gathering quickly changing information of the network graph, information that is essentially to nodes in order to open a payment channel with other nodes like: status of nodes, distribution of funds within payment channels and fees for using a channel.

Table-driven (proactive) protocol:

Proactive node (neighborhood node)

In certain radius node can very quickly gather information on channels/opening closing, thus having up to date picture, but it is not scalable to have radius too big.

- a. Each node propagates information on its channels closing and opening in certain radius.
- b. This allows each node to have up to date picture of all open channels (with their total capacity) in certain radius.

Proactive node (Beacon node)

To enhance long range visibility node finds paths to distant nodes (beacons) which can help to find route to receiver if he is not in the neighborhood

- a. Each node finds paths to nodes whose addresses are closest to the one's (claiming those beacons).
- b. On reactive stage this allows to search for longer paths iterating over known nodes in DHT like manner.

On-demand (reactive) protocol:

When node E wants to send money to D:

1. E and D find path candidates on the graph of their routing tables

Finding candidates once joint routing table is created one may find k paths using approaches like breadth-first search

2. If no candidates are found E requests tables from nodes whose addresses are closest to D and so on...

3. When several candidates are found E collects dynamic information on them
4. If the one is found E creates HTLC and sends money to D

Disjoint paths

By adding vertex weights to network graph one may find shortest paths that are most different from previous found.

Dynamic data

- Found candidates are paths that potentially can route the payment
- To tell if there is the path that we can use to route the payment we need to gather dynamic data for candidates (funds, fees)
- The simple solution - probing onion messages that traverse through candidate paths and quickly collect dynamic information graph one may find shortest paths that are most different from previous found

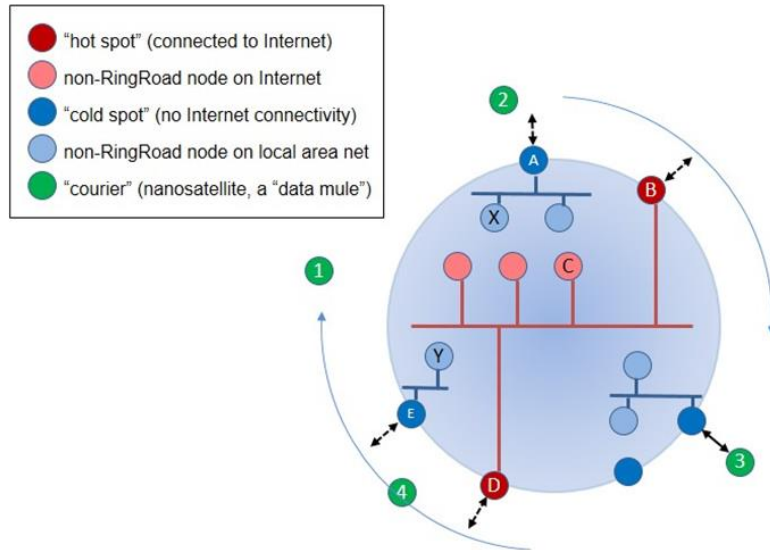
Dynamic data

But how do we know which candidates to check first? Need ranking.

- Distribution of funds in the channel - uniform if know nothing.
- Probability that channel with capacity C would be able to route the payment x is equal to $\max(0, 1-x/c)$.
- Probability payment X would make it through is $P(x|\text{path}) = \max(0, 1-x/C)$
- after we get the probabilities we can start sending probes through the candidates with highest chance of success.

The Ring Road concept

An infrastructure proposal: a constellation of Nano-satellites using delay-tolerant networking to provide low-cost access to lighting network.



Why?....

Economic obstacles: Access to fixed broadband in some countries costs almost 40 times the national average income. Even in wealthy countries, affordability limits broadband access in impoverished communities. **Geographic obstacles:** Some communities are too far from population centers to make the extension of infrastructure — fiber, cell towers — cost-effective. **Political obstacles:** Some nations restrict citizens' network access and/or restrict the content that can be carried by the network.

Communication satellites: Earth-orbiting satellites can relay radio communications among sites on Earth can be visible from all points on Earth's surface, removing the geographic and political obstacles.

Not a new idea...(examples)

Geostationary (GEO): Exede (ViaSat), HughesNet (EchoStar), WildBlue, StarBand, Intelsat, Inmarsat, Thuraya

Low-Earth Orbiting (LEO): Globalstar, Iridium, Orbcomm, Teledesic.

So the problem solved:

Maintaining Internet connections with satellites isn't easy.

- GEO satellites do this by ensuring continuous radio contact with ground stations and customer equipment. But:
 - They are costly, on the order of \$300 million (manufacture & launch).

- Each one provides communication to a limited part of Earth's surface.
- Each one is a single point of failure.
- While data rates are high, round-trip latencies are also high.
- LEO constellations do this by constantly switching connections among moving satellites.
 - Broad coverage areas, low latencies.
 - But data rates are lower than for GEO, more satellites are needed, and
 - They're still expensive: \$150-\$200 million (manufacture and launch).

An emerging answer

- A capable Nano-satellite, such a Cube-Sat, can be fabricated and launched into low-earth orbit for .1% of the cost of a LEO communication satellite.
- An inexpensive Nano-satellite constellation in LEO would have a broad coverage area, no single point of failure.

There's a catch, though....

"Nano" Communication Satellites

- Nano-satellites are inexpensive in part because they are simple.
 - Maneuverability is limited.
 - Normally only single radio (UHF or S-band).
- This means the constant connection switching among cross-linked satellites that normally enables LEO constellations is not feasible.
- So we can't expect a constellation of low-cost Nano satellites to be able to sustain thousands or millions of continuous end-to-end internet connections.

Solving the catch.....

Rise of Nanosatellites: Nanosatellite optical downlink experiment (NODE)

The nanosatellite optical downlink experiment (NODE) implements a free-space optical communications (lasercom) capability on a CubeSat platform that can support low earth orbit (LEO) to ground downlink rates >10 Mbps. A primary goal of NODE is to leverage commercially available technologies to provide a scalable and cost-effective alternative to radio-frequency-based communications. The NODE transmitter uses a 200-mW 1550-nm master-oscillator power-amplifier design using power-efficient M-ary pulse position modulation. To facilitate pointing the 0.12-deg downlink beam, NODE augments spacecraft body pointing with a microelectromechanical fast steering mirror (FSM) and uses an 850-nm uplink beacon to an onboard CCD camera. The 30-cm aperture ground telescope uses an infrared camera and FSM for tracking to an avalanche photodiode detector-based receiver. Our approach is to transition prototype transmitter and receiver designs to a full end-to-end CubeSat-scale system. This includes link budget refinement, drive electronics miniaturization, packaging reduction, improvements

to pointing and attitude estimation, implementation of modulation, coding, and interleaving, and ground station receiver design. We capture trades and technology development needs and outline plans for integrated system ground testing all that could be the scope of another paper.

Key Enabling Technologies

The key enabling technologies for CubeSat lasercom are improved **pointing control** for the CubeSat and **ground terminal, power efficiency, and compact electronics and packaging**.

In order for lasercom on CubeSats to be competitive with RF solutions, the spacecraft terminal needs to be able to point a less than 5 mrad beam with a high slew rate (1deg/s1 deg/s) despite uncertain spacecraft moments of inertia. (An initial lasercom demonstration with this modest beamwidth would help to define a path toward much more efficient, higher-bandwidth systems that could support higher rates with 100 μ rad100 μ rad beams.) Most CubeSats use attitude determination systems that cannot achieve this level of control, although significant efforts are underway to incorporate low-cost star trackers onto CubeSats. CubeSat laser communication systems must therefore be able to accommodate coarse bus attitude control. In contrast, the beamwidths necessary for high data rate downlinks with low power. The demonstrated state-of-the-art in CubeSat control, as shown in, includes degree-level pointing control on several missions and 45 arc sec (0.2 mrad) pointing in the constellation, but the arcsecond pointing application was for staring at fixed distant objects (stars). While propulsive maneuvers requiring precise pointing have been demonstrated, this level of attitude control performance has not been reported during slew maneuvers similar to what would be required for LEO lasercom downlinks. Another challenge for CubeSat lasercom is power efficiency, given the limited power available to the host spacecraft. Per the design trades, space-rated erbium-doped fiber amplifiers (EDFAs) are available, commercially available EDFAs used in the telecommunications (telecom) industry, however, are available that meet the SWaP constraints. The use of COTS parts, if they can meet the power requirements of the space terminal and survive in the space environment for the CubeSat mission lifetime (typically less than 5 years) helps to keep the cost low.

Capacity:

- 20x greater data rate over COTS RF radios

Security:

- very difficult to intercept

Size:

- ½ the size/mass/power
- ½ antenna diameter

Regulatory:

- No license required
- Downlink more data

Solving the catch “continued”

- But maintaining continuous end-to-end internet connections are not the only possible network service.
- **Delay-Tolerant networking (DTN) technology**, emerging over the past decade, enables a different model:
 - At each moment, each satellite points only at the ground station directly below it (when there is one).
 - While the satellites and ground station are in contact, they exchange network traffic. The satellites function as a router.
 - When contact is broken, the router satellite retains out-band messages in local storage while it continues on its orbital.
 - When contact with the next ground station begins, network traffic exchange resumes.

Proposed Constellation size

- Couriers are in near-circular low-Earth orbits at inclination of about 50 degrees (so the coverage area is from 50 degrees South Latitude to 50 degrees North); altitude about 500 km.
- Radius of satellite visibility is somewhat greater than 1000 km,
- Maximum separation of satellites is at the equator, which is about 40000 km, so 10 orbital planes are needed: each satellite crosses the equator twice per orbit, covering a circle of 2000 km circumference at each point,
- Coverage per satellite at the equator is 18 degrees of longitude; 12 satellites per orbital plane would allocate 18 degree of latitude coverage (out of 200) to each satellite, but say 15 to ensure some overlap. So 150 spacecraft in all.

Network capacity

- Satellites at 500 km altitude travel at about 7.8 km per second, an orbital period of 90 minutes; 16 orbits per day. Any single satellite will be in view of any single ground station for about 128 seconds per orbit, the maximum contact length.
- S-band transceivers can transmit at 230 kbps, could upload up to 3.6 MB during a single satellite contact of maximum length.
- Up to 42 contacts of max. Length per orbit, 150 MB could be inserted into the network per satellite per orbit, 2.4 GB per satellite per day.
- For 150 satellites, 360 GB per day. This is about 4 MB per second, 32 Mbps. But maximum upload is impossible because each satellite is often over open sea; figure 16 Mbps.

Deployment cost

- Estimated assembly cost per satellite: \$100,000.
 - Total satellite assembly cost per network: \$15 million.
- Estimated launch cost per group of three Cube-Sats: \$200,000.

- Total launch cost for network: \$10 million.
- 20 contacts per orbit (40,000 km Earth circumference, 2000 km diameter per contact) for 150-satellites would require 3000 base stations; 1500 if one-half of the covered surface is unoccupied. Estimated cost per base station, including S-band radio modem: \$2000.
- Total base station cost for network: \$3 million.

Incremental deployment

- The network would function with only a single satellite, but with very low capacity and terrible round-trip latency (days).
- As satellites are added, network capacity increases and round-trip latency drops in proportion.
- Correspondingly, loss of any satellite causes an incremental drop in capacity and increase in latency. Graceful degradation, no single point of failure.
- Replacing satellite with one that has greater capacity-more memory, higher radio data rate – likewise provides an incremental increase in network capacity and drop in round-trip latency.

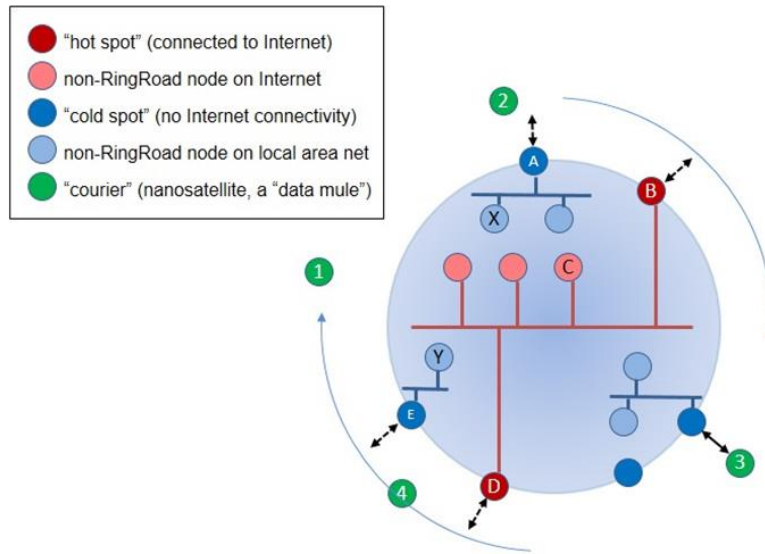
Service Cost Estimate

- Suppose network lifetime is 5 years and operating cost is \$1 million per year. Total lifetime of the network is $\$15 + \$10 + \$3 + \$5 = \$33$ million.
- At 16 Mbps, total lifetime traffic is about 300 TB. Mean cost of transmission is less than \$0.11 per MB.
- Commercial satellite services (as of September 2013):
 - Iridium pilot: \$7.41 per MB.
 - Inmarsat BGAN shared services: \$6.49 per MB.
 - Thuraya GmPRS NOVA: \$5.00 per MB.

Latency

- Total network capacity and data rate to subscribers could be increased 100-fold or more by using C-band or K-band radios, not currently available for Cube-Sats.
- But higher data rate can't solve the end-to-end round-trip time problem; latency in communication between satellites and ground stations is negligible, but round-trip latency in the network is extremely variable and can be very high.

A Perspective on Using a Network



Caveats

- **Operations: the core DTN protocol implementations are mature, but supporting software is needed.**
 - Route computation can be based on Contact Graph Routing.
 - Scalable network management protocols and tools will be needed.
- **Security:**
 - Basic network security measures (authentication, integrity, confidentiality) are supported by Bundle Security Protocol.
 - A scalable key distribution system will be needed.
- **The elephant in the room: where will the funding come from?**

Outlook

- DTN satellites in low-earth orbit are already a well-proven concept: Change Request 013799, authorizing deployment of two permanent DTN on the international space station, well approved on 10 September 2013.
- The Ring Road network concept has some clear advantages:
 - Surmounts geographic obstacles.
 - Not disabled by earthquake, storm, flood, fire.
 - Difficult to disabled intentionally.
 - Graceful degradation in the event of satellite loss.
 - Low barrier to entry.
 - Low operating cost.
- An opportunity to extend network service worldwide.

It would be a high-latency network, unsuitable for some applications. But for many applications it could work as well as the internet. Perhaps even better.

Implications on Bitcoin protocol & currency

What does Bitcoin protocol offers to global currency concept?

Problems face globalization “mainstreaming “of Bitcoin & the Differences between globalization and mainstreaming of Bitcoin currency?

Is there a break point at which fiat currencies “backed by central banks” defeated facing Bitcoin?

Existing Bitcoin critiques and commentary

- Bitcoin suffering deflationary spiral tracked by Grinberg
- Grinberg also touches legal problems; such as exchanges, potential failure of anonymity, denial of service attacks and violation of the stamp act
- Hoarding is tracked by Ron and Shamir Mielejohn, as well as Sergio
- Mielejohn, et al make an attempt to track circulation of bitcoins, claiming that roughly half circulate rapidly, However, since this occurs at gambling and trading sites, that activity does not represent buying and selling of goods and services.
- Tyler and Moore show that patrons of bitcoin exchanges run significant risk of loss due to failure of the exchange.
- The irony of bitcoin’s decentralized design being subsumed into dependency on a small number of exchanges.
- Selgin is intrigued about a bitcoin type of crypto-currency within a fiat currency system as a way to provide a perfectly elastic currency supply that could be targeted by algorithm to various monetary schemes, Selgin and Grinberg are both aware of issues inherent in an inelastic money supply. But the intractable nature of bitcoin’s inelastic design is not connected by them with this issue.
- Plassaras is concerned about the IMF being able to stabilize bitcoin, and states that bitcoin:
...poses a serious threat to the economic stability of the foreign currency exchange if it continues to grow in both value and usage. Any other digital currency that entered widespread use would pose similar problems.
- Eyal and Sirer point out a serious technical vulnerability of Bitcoin as Bitcoin depends on the longest block-chain being the honest one this requires that the majority of nodes are honest However, Eyal and Sirer describe a vulnerability that begins at 33% of computing resources. An implication is that a government (or wealthy private party) can take control of a cryptocurrency with this design (which is all cryptocurrencies now in existence) by applying superior computing resources, Even if the bitcoin algorithm is

modified, it is evident that bitcoin will always be vulnerable to brute force application of sufficient computing resources to overwhelm the system.

- Bitcoin's purported capacity for expansion is not credible.
- A Bitcoin financial system is a losing zero-sum game for investors, A system where the amount of money is fixed is a zero-sum game – for every winner, there must be a loser, because new money is not created that allows interest or investment return payouts.