geospatial blockchain

jonas ellehauge

frontend developer

at

DHI GRAS

See what's possible:

We analyse satellite images for mapping, monitoring and forecasting of the earths natural resources.

DHI GRAS

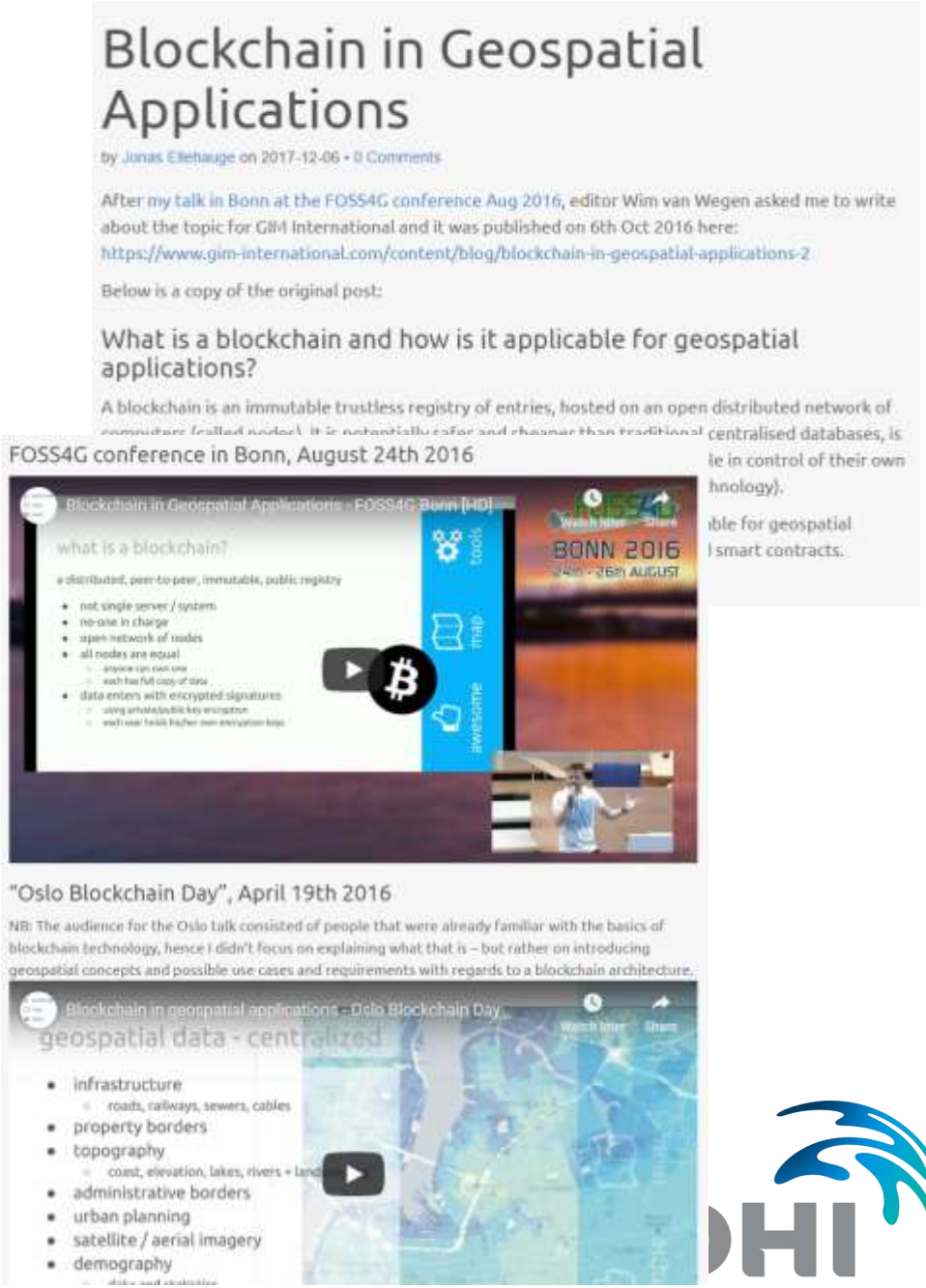
The plan

- Context
- Blockchain basics
- Geospatial use cases
- The FOAM project
  - The token
  - Proof of location
  - Community map
- Relevance

DHI GRAS

Context

- 2016
  - **Oslo Blockchain Day**, April – youtube video
  - **FOSS4G** Aug – youtube video
  - **GIM International**, Oct – blog / article
- 2017
  - **Iterate Inc** (LA) consulting, Dec
- 2018 work
  - **brainbot** – Infrastructure for Ethereum
  - **Bitcoin Suisse** – Broker and Crypto Assets
- Emails & calls
- Invited to speak here

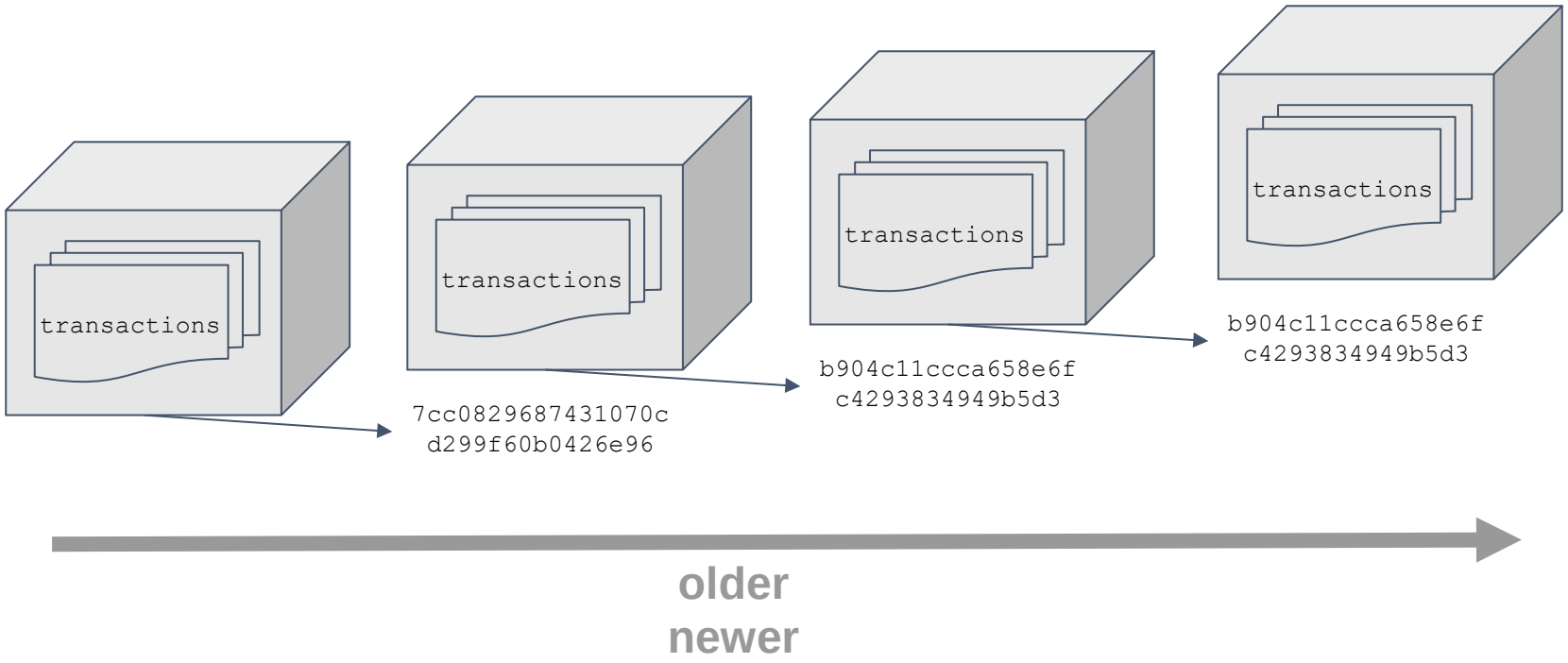


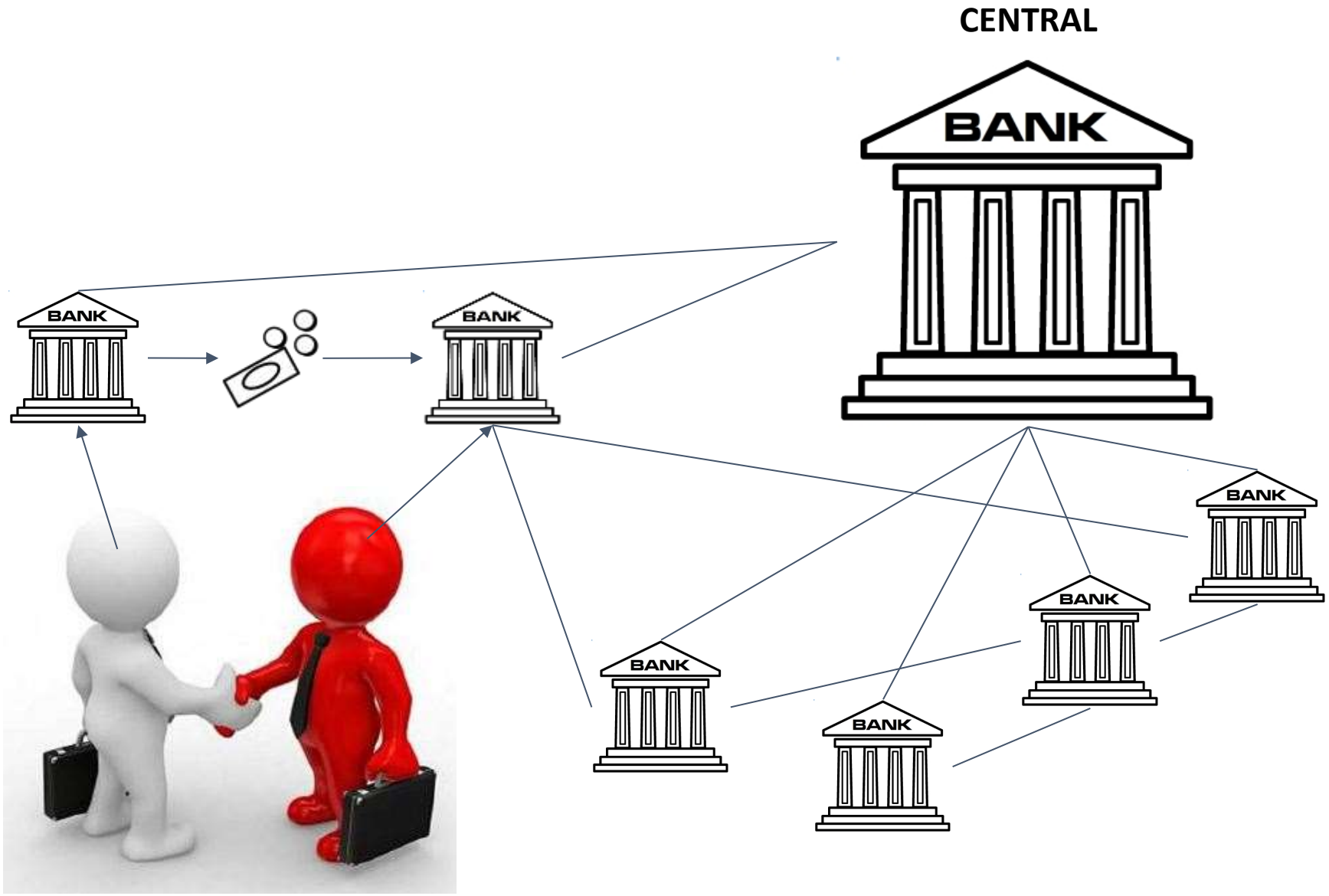
Blockchain Basics

a blockchain is a:

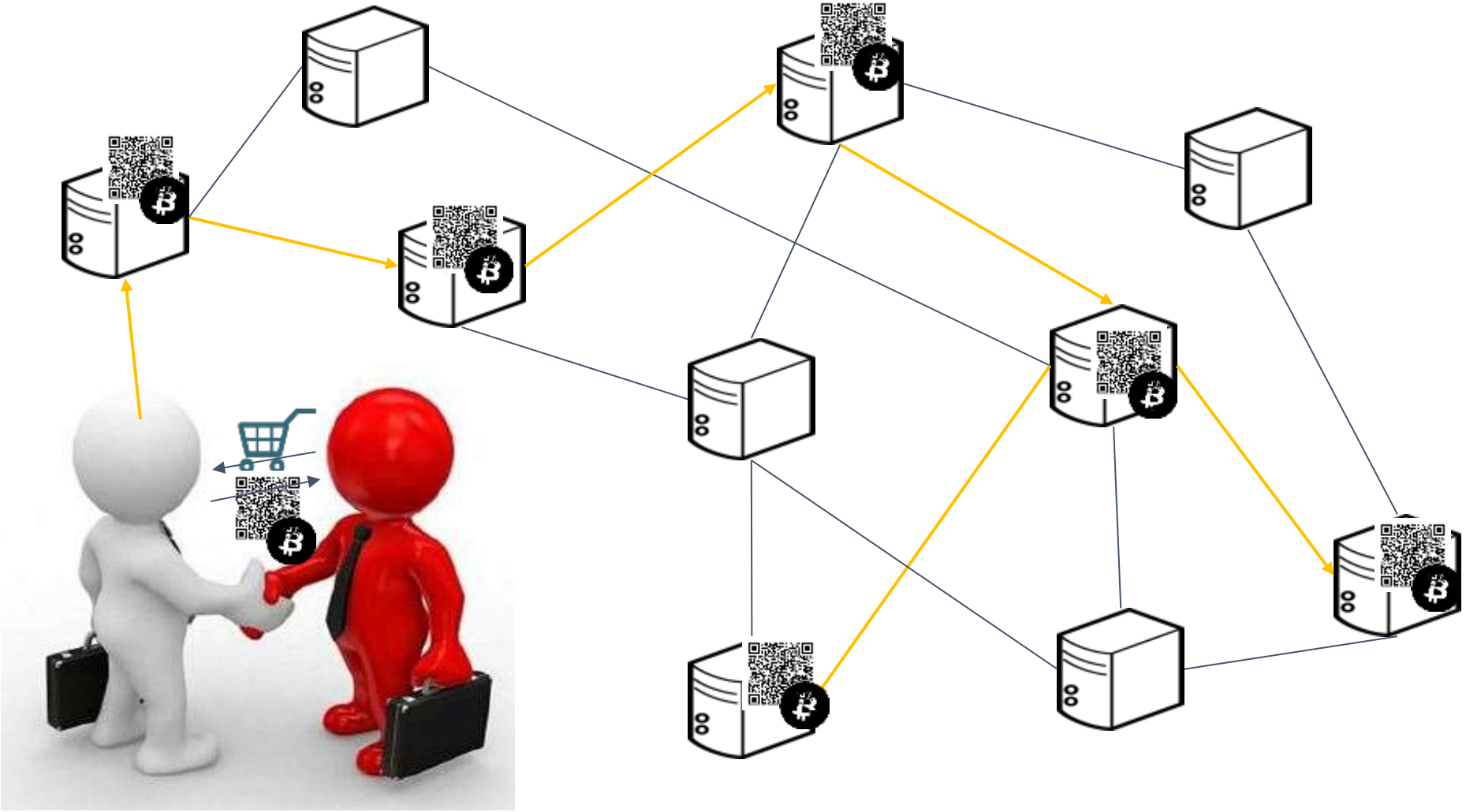
- decentralized
- immutable
- peer to peer
- trustless
- public registry
  - (ledger / database)

A record of transactions





DHI GRAS



DHI GRAS

Egalitarian or reciprocal – not Hierarchical

- All nodes are equal
  - and have a full copy of the blockchain
- Anyone can install the software
  - and become a node in the network
- Nodes are paid with transaction fees
  - or new crypto coins

DHI GRAS

Consensus

- It's a consensus algorithm
- for anyone who cares to take part
- to agree on the state of the shared record

DHI GRAS

Ethereum blockchain

- Currency is Ether - ETH
- Programming language – Solidity
- Smart contracts
  - has API / ABI
  - holds funds (Ether/tokens)
  - has methods / functions
  - properties
- Custom tokens
  - a smart contract
  - regulates a token

ethereum

BLOCKCHAIN APP PLATFORM

Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts** : applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

These apps run on a custom built **blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.**

This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middleman or counterparty risk.

The project was bootstrapped via an ether presale in August 2014 by fans all around the world. It is developed by the Ethereum Foundation, a Swiss non-profit, with contributions from great minds across the globe.

DHI GRAS

Ethereum

- Runs computations
  - not only transactions

- Change state of smart contract
  - requires mining of new blocks
  - gas – the cost of computations

Geospatial use cases

- Public good data
- IoT – autonomous devices
- Land ownership

- GPS alternative
- Proof of location
- Supply chain

Use Cases

Here are some geospatial use cases:

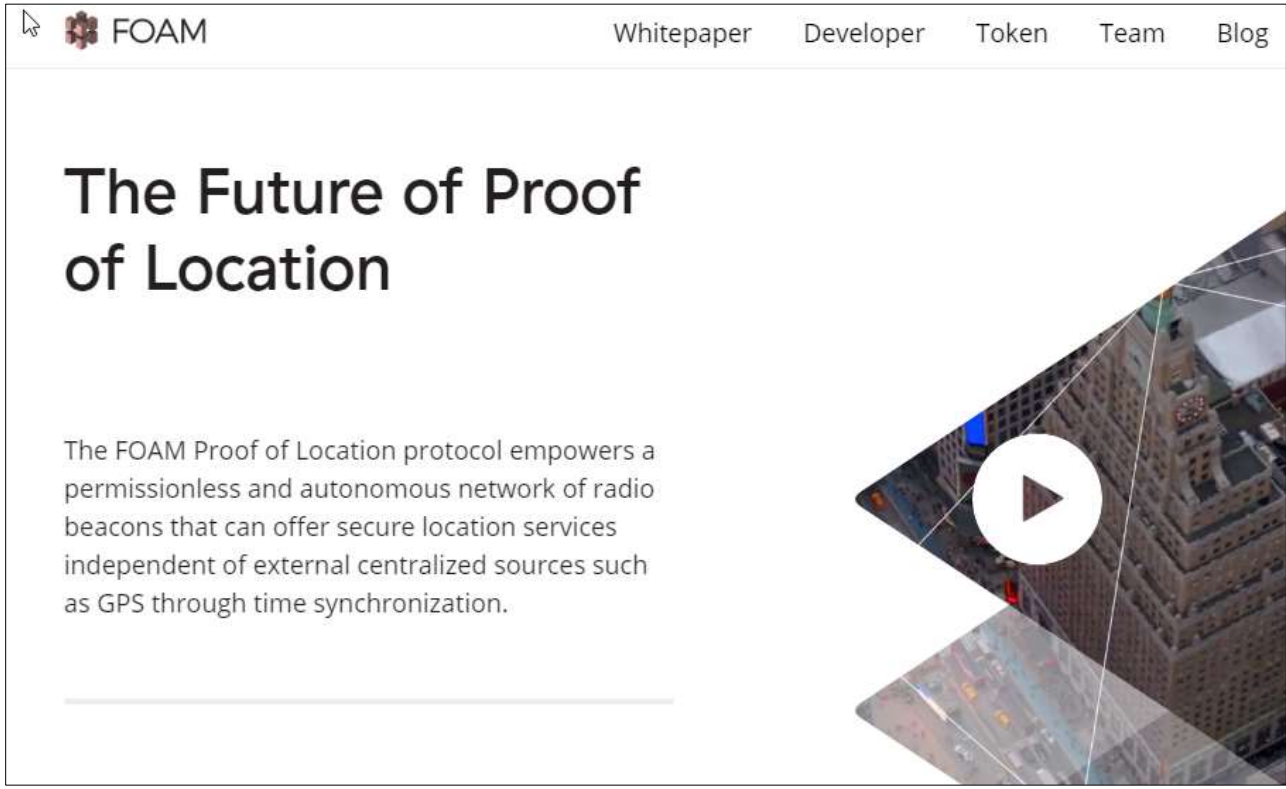
1. **Public good data** such as street maps, parcels, terrain models, aerial footage, sea maps – publicly available without a central hub that can restrict access to the data; reward contributors to the map with tokens; keep a public history of changes and contributions.
2. **IoT – Autonomous devices & apps:** Devices that negotiate and pay each other, such as drones that negotiate use of air space, self-driving cars that negotiate lane space or pay for road usage, mobile/wearable devices pay for public transportation. Apps similar to Uber and AirBnb that connect clients and providers without a middleman.
3. **Land ownership** – register land / real estate ownership on a blockchain; render corruption nearly impossible; enable people in developing countries to register land ownership themselves with inexpensive mobile devices without the need for slow or expensive overhead.

The use cases are discussed further below. Recently, I gave a few short talks about this topic at various conferences – the most recent one at the international FOSS4G conference in Bonn 2016.

DHI GRAS

FOAM.SPACE

- FOAM token on Ethereum
- CSC - Crypto-Spatial Coordinates
  - Coordinate and smart contract reference standard
- Public good data
  - community map – SIV
- Locator & Proof of location
  - work in progress



DHI GRAS

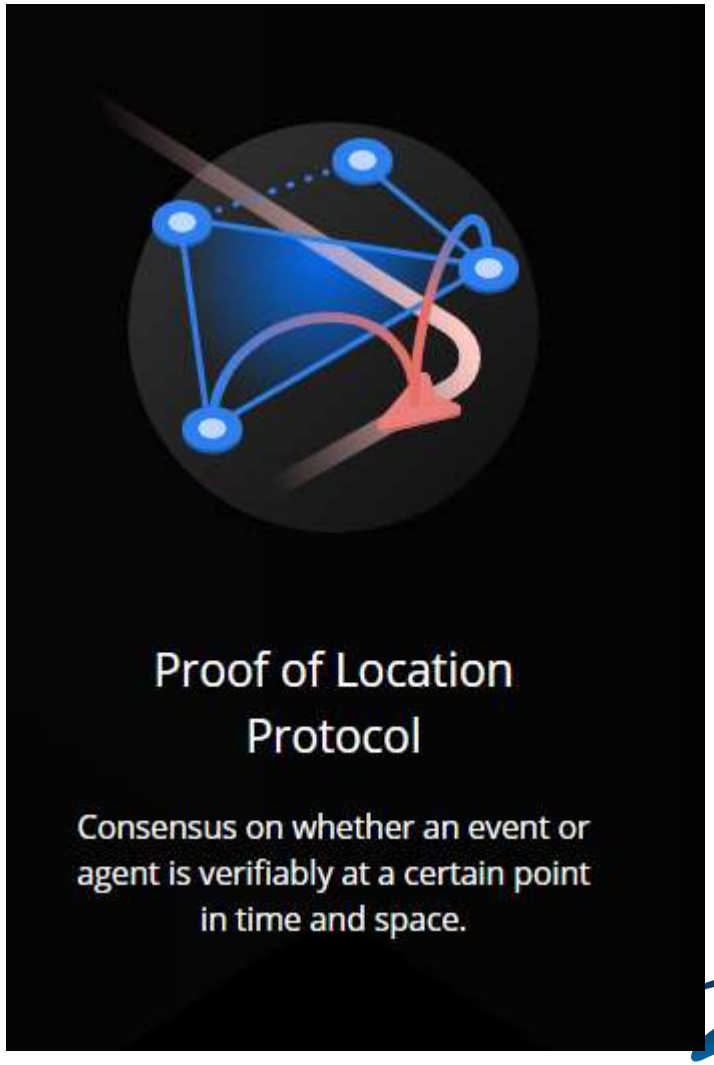
Locator & Proof of Location

GPS drawbacks

- Central point of failure
  - owned/run by one org
- Can be jammed
- Can be spoofed
- No indoor location
  - buildings / mountains
- Security / privacy
- No proof
- Accuracy limited
- Battery greedy & slow

How to prove location?

- how can you provide proof
- that you were at a specific location
- at a specific time?



DHI GRAS

How to prove that regular money is yours?

- You ask a bank to verify it
- who in turn can ask the central bank to verify it
- that's it – you gotta take their word for it
- i.e. requires trusted middleman

DHI GRAS

How to prove a Bitcoin is yours

- You sign a digital message
  - with your private encryption key
- Anyone who wants can prove
  - that it fits the public key
- No trust / middleman required
  - it's mathematical proof

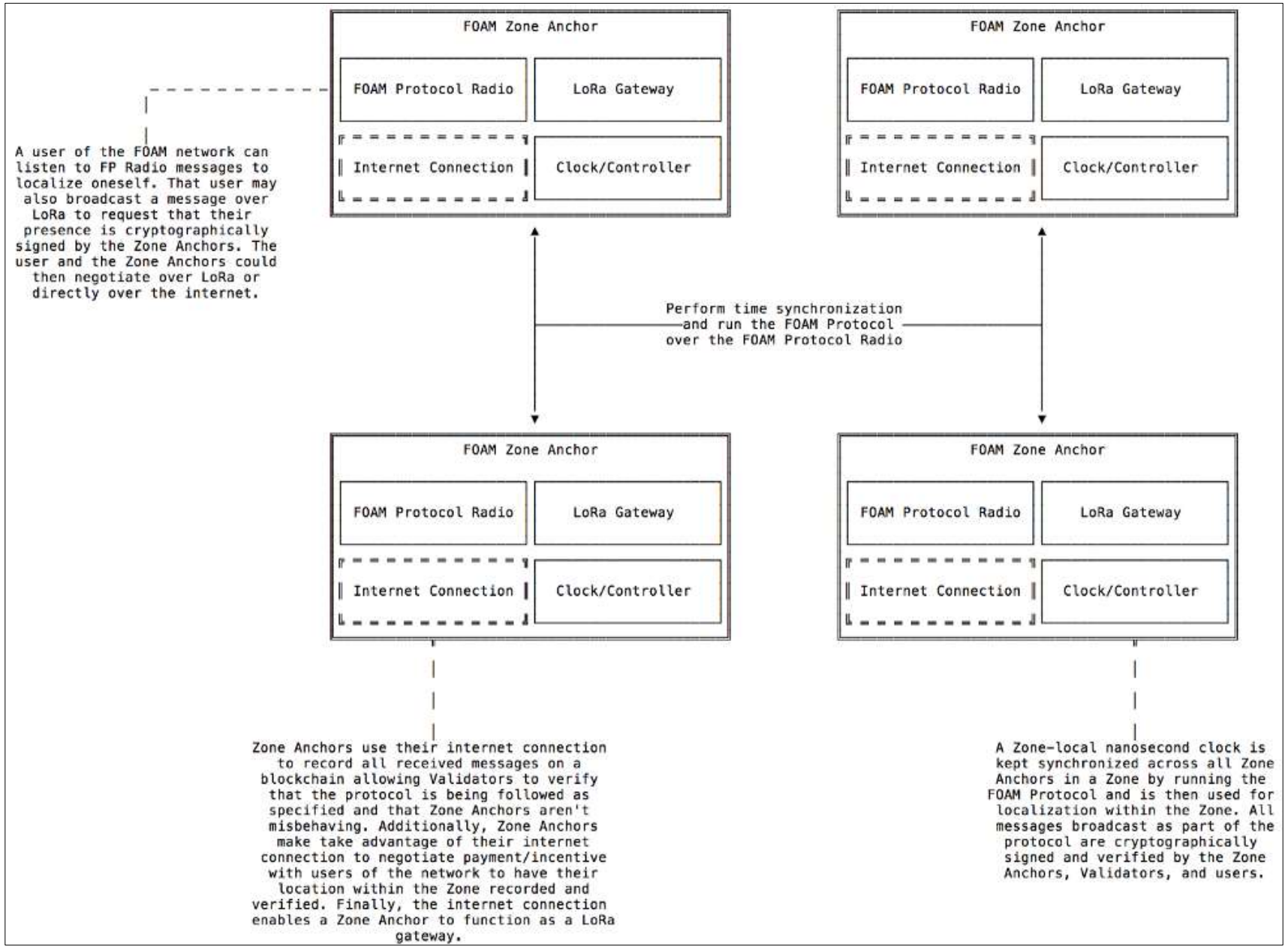
DHI GRAS

Dynamic Proof of Location

- FOAM aims at providing an infrastructure
  - to prove location in time for an object
- Beacons
  - use geometry and time synchronization
- Anyone can set up a beacon
  - and get paid in crypto tokens

- Result:
  - determine your location
  - a fraud proof location certificate
  - a "Presence Claim"

DHI GRAS


FOAM Zone Anchor
FOAM Protocol Radio
LoRa Gateway
Internet Connection
Clock/Controller
FOAM Zone Anchor
FOAM Protocol Radio
LoRa Gateway
Internet Connection
Clock/Controller
A user of the FOAM network can listen to FP Radio messages to localize oneself. That user may also broadcast a message over LoRa to request that their presence is cryptographically signed by the Zone Anchors. The user and the Zone Anchors could then negotiate over LoRa or directly over the internet.
Perform time synchronization and run the FOAM Protocol over the FOAM Protocol Radio
FOAM Zone Anchor
FOAM Protocol Radio
LoRa Gateway
Internet Connection
Clock/Controller
FOAM Zone Anchor
FOAM Protocol Radio
LoRa Gateway
Internet Connection
Clock/Controller
Zone Anchors use their internet connection to record all received messages on a blockchain allowing Validators to verify that the protocol is being followed as specified and that Zone Anchors aren't misbehaving. Additionally, Zone Anchors make take advantage of their internet connection to negotiate payment/incentive with users of the network to have their location within the Zone recorded and verified. Finally, the internet connection enables a Zone Anchor to function as a LoRa gateway.
A Zone-local nanosecond clock is kept synchronized across all Zone Anchors in a Zone by running the FOAM Protocol and is then used for localization within the Zone. All messages broadcast as part of the protocol are cryptographically signed and verified by the Zone Anchors, Validators, and users.

DHI GRAS

FOAM Whitepaper

05.01.2018

Foamspace Corp
info@foam.space

FOAM — The Consensus Driven Map of the World

FOAM is an open protocol for decentralized, geospatial data markets. The protocol is designed to empower users to build a consensus-driven map of the world that can be trusted for every application. As technology evolves and changes, maps need to change too. FOAM secures physical space on the blockchain, harnessing the power of Ethereum with a cryptographic software utility token used to provide computational work and verification to the network.

The component elements of the FOAM protocol are designed to provide spatial protocols, standards and applications that bring geospatial data to blockchains and empower a consensus-driven map of the world. Token mechanisms and crypto-economics underpin the elements of FOAM and empower the distributed users to coordinate and interact in a decentralized and permissionless fashion.

Table of contents

Abstract
Overview
Problem
Location Spoofing
User Experience
Location Verification
Solutions
Crypto-Spatial Coordinates
Properties of the CSC
The CSC functionality
The Spatial Index and Visualizer
Properties of the SIV
The SIV functionality
Proof of Location
Properties of the PoL
Token Curated Registries for Geographic Points of Interest
Signaling
The PoL Functionality
Block rewards

Elements of FOAM

The thinking behind FOAM is controlling when and with w solving this need by providin level of security and resilien services.

Proof of Location Functionality

1. Trustless:
Byzantine fault tolerant clock synchronization.

2. Independent:
Does not rely on a centralized service such as GPS.

3. Open:
Anyone can utilize the network or offer utility services.

4. Accountable:
The economics are structured to ensure honest behavior and verified with fraud proofs.

5. Incentivized:
Service providers may be remunerated for extending localization and verification zones.

Dynamic Proof of Location anticipated to verify location claims in 7 steps:

1. Zone Anchors and Zone Authorities

Radio beacons (Zone Anchors) and Radio gateways (Zone Authorities) are established and form a network to synchronize their internal clocks without the need for a trusted third party. With an encrypted and self-stabilizing time signal established, the network can determine spatial arrangements.

2. Clock Synchronization

Zone Anchors and Zone Authorities send messages until a consensus can be formed on the precise time. The timed difference of messages sent and received allows for location to be calculated and the geometry of the network to be determined.

3. Zone Formation

Once synchronized, Zone Authorities establish Zones and pledge to offer location services that are enforced by smart contract safety deposits.

4. Triangulation

Zones can provide presence claims for customers in a competitive market for a transaction fee. This is done while Zones are resynchronizing clocks and publishing their time logs to a data store.

5. Verification

Agents that contribute computational power, called Verifiers, check the time logs of Zones for fraud.

6. Proof of Location

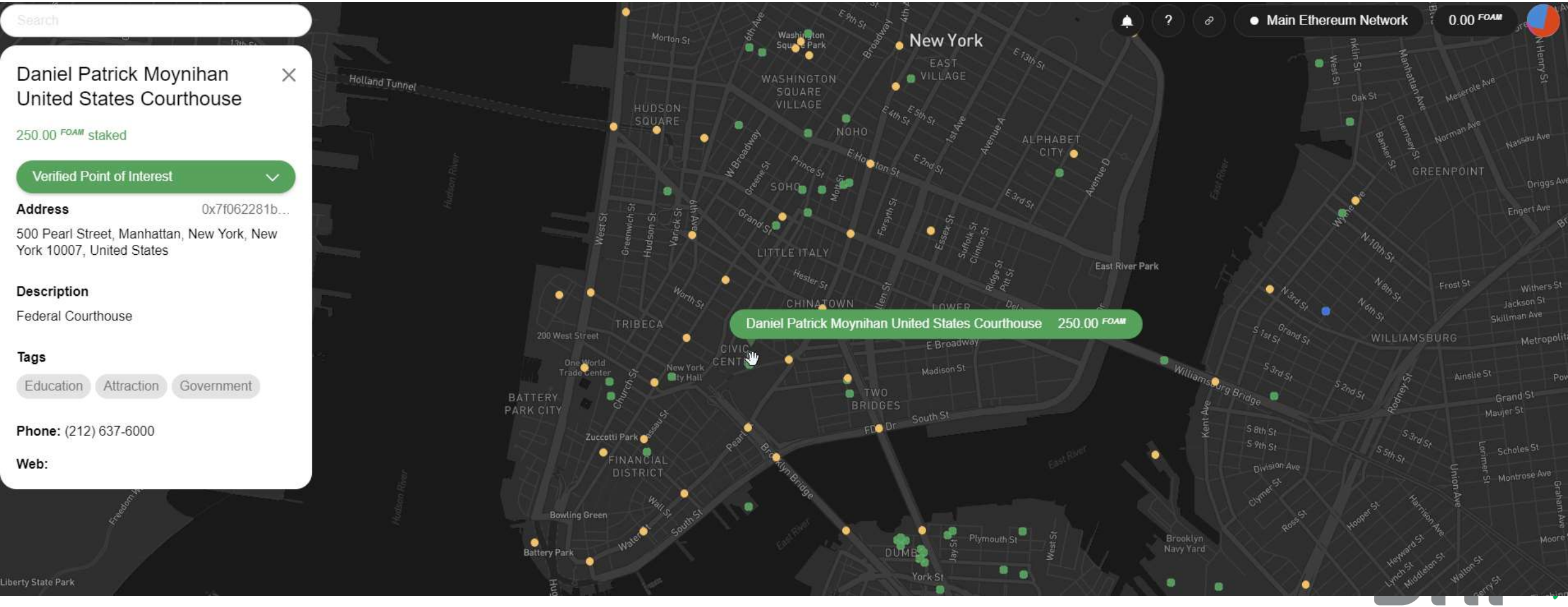
Verifiers send Fraud Proofs to the root chain (Ethereum Blockchain) and the Proof of Location certificates are getting created.

Community map

SIV – Spatial Index and Visualizer

DHI GRAS

SIV – Spatial Index and Visualizer



GRAS

Incentive model

Mapping incentives

Maintaining a global map is difficult! This goal requires an ecosystem of different types of users. Those users and their incentives look like this:

1. *Cartographers* should add points that will not be voted off the map
2. *Challengers* should challenge points that will be voted off the map
3. *Voters* should vote on the winning outcome

The rules behind these incentives are:

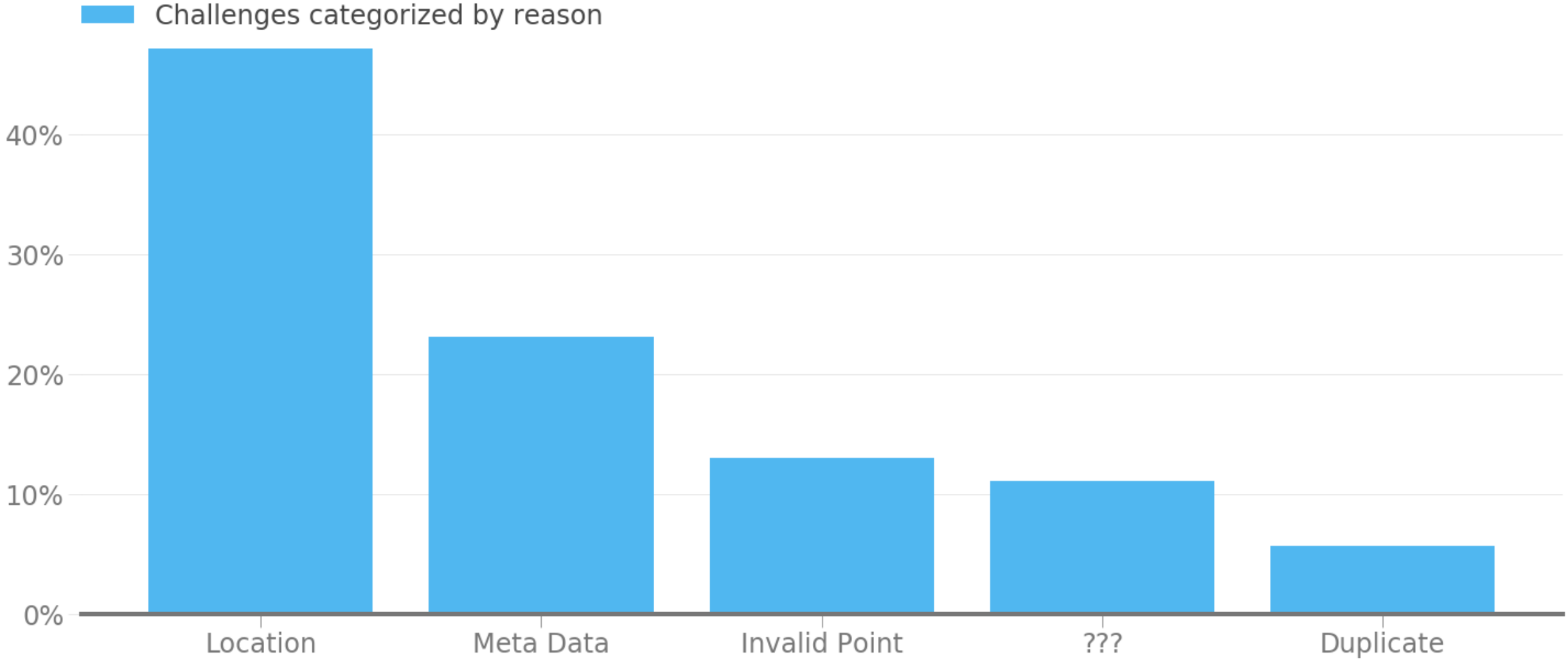
1. New points require a stake (deposit).
2. Any point can be challenged with a stake, which initiates a voting round.
3. If the vote results in a point being invalidated, the Cartographer loses their stake and, in most cases, the point is removed. 60% of the stake goes to the Challenger and 40% is split between the Voters on the winning side.
4. If the vote results in the point being validated, the Challenger loses their stake and the point stays on the map. 60% of the stake goes to the Cartographer and 40% is split between the Voters on the winning side.

- Cartographers added 7,756 points to the map
- Challengers challenged 4% of those points
- Voters voted to invalidate 93% of those points

DHI GRAS

FOAM Map Challenge Reasons

Location, Location, Location

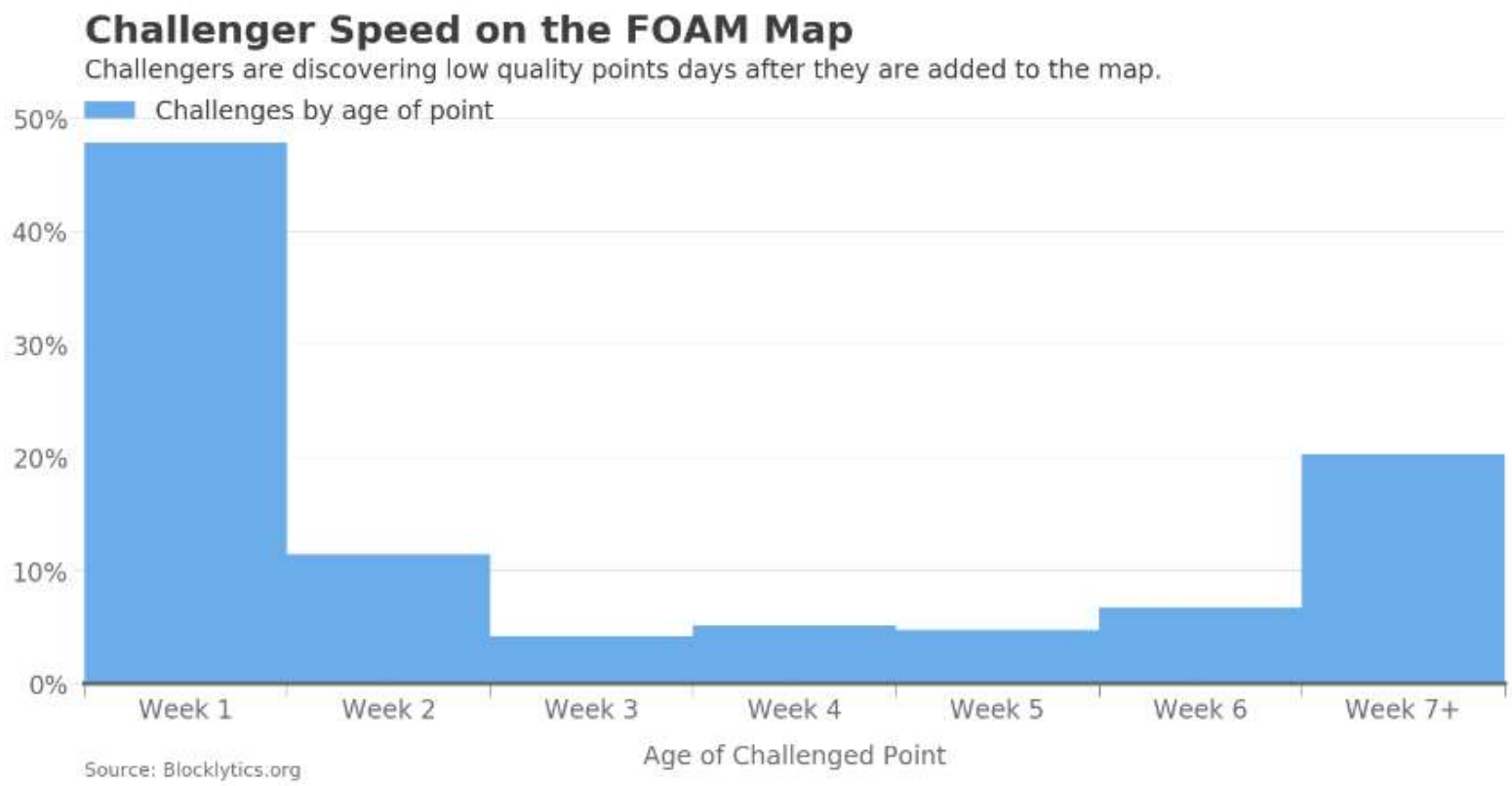


Sources: FOAM API, Blocklytics.org

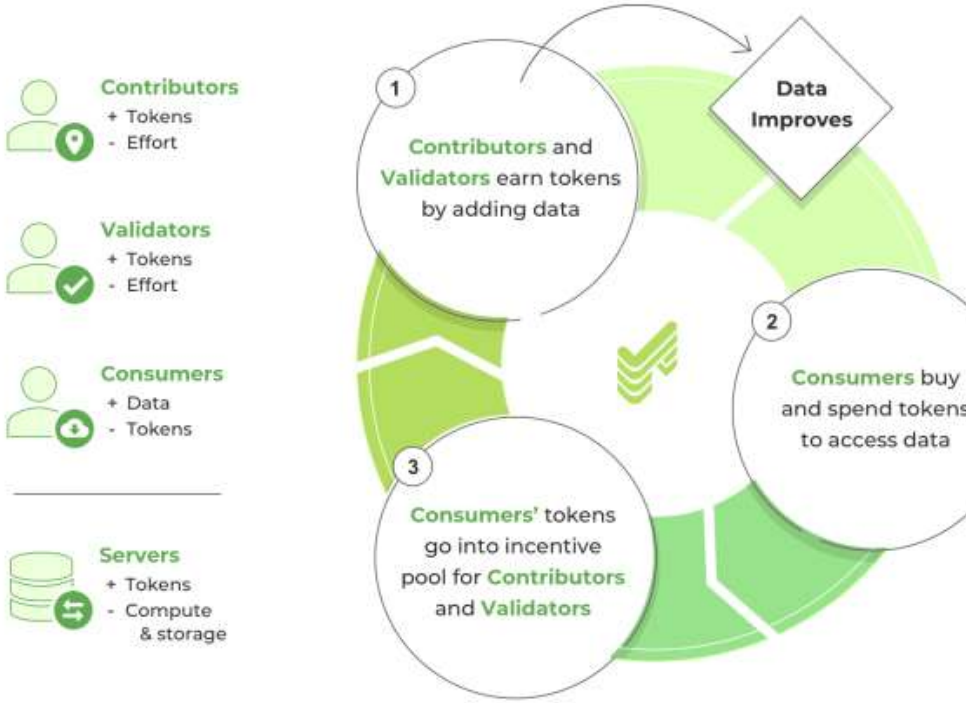
GRAS

Speed of Challenges

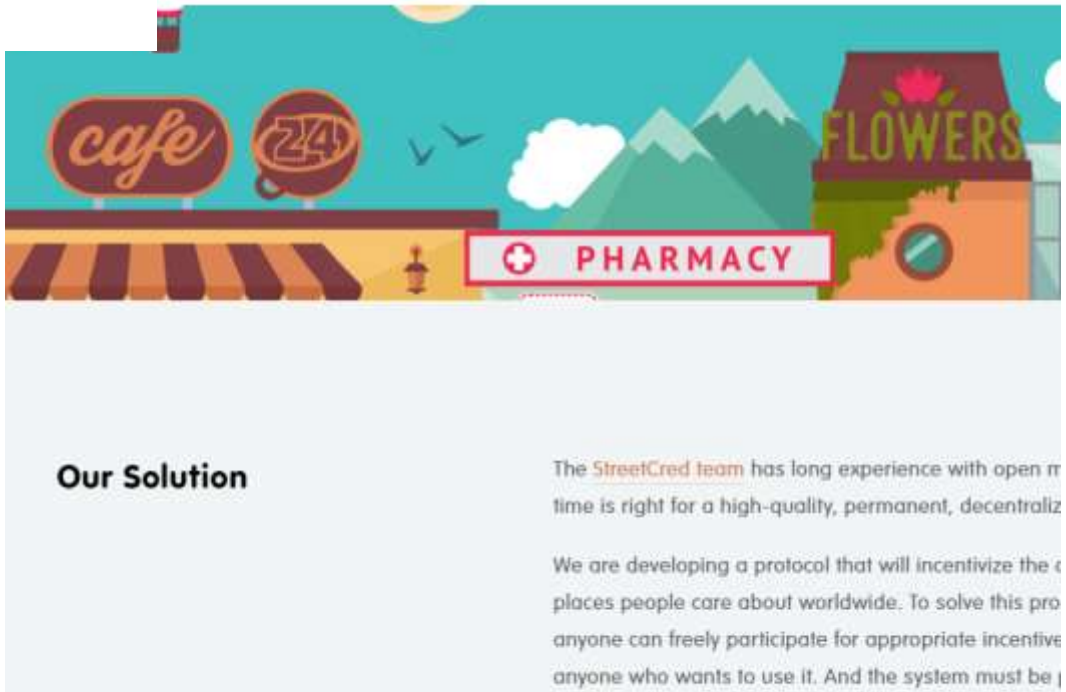
Another way to measure performance of a TCR is speed. A healthy ecosystem is one where low quality points are quickly being challenged and removed from the map. The incentive structure gives the biggest opportunity to the Challenger that is first to find and challenge a point.



Challenger Speed on the FOAM Map (Source: Blocklytics.org



But really the biggest safety mechanism to prevent data abuse is built right into the protocol via the Validator role. Validators are local participants who are tasked with verifying all the incoming data contributions for the region under their supervision. They need to simply travel to the nearby location and verify that the data being submitted objectively matches the ground truth. There must be at least three active validators in an area to complete any data contribution. Surveyed validators must reach consensus about the incoming data before it can be added to the database at which time all participants will be compensated. Validators will be anonymous and chosen at random so no collusion can take place. Should validators vote against consensus they risk losing tokens they've staked and their credibility on the network.



DHI GRAS

How is this relevant?

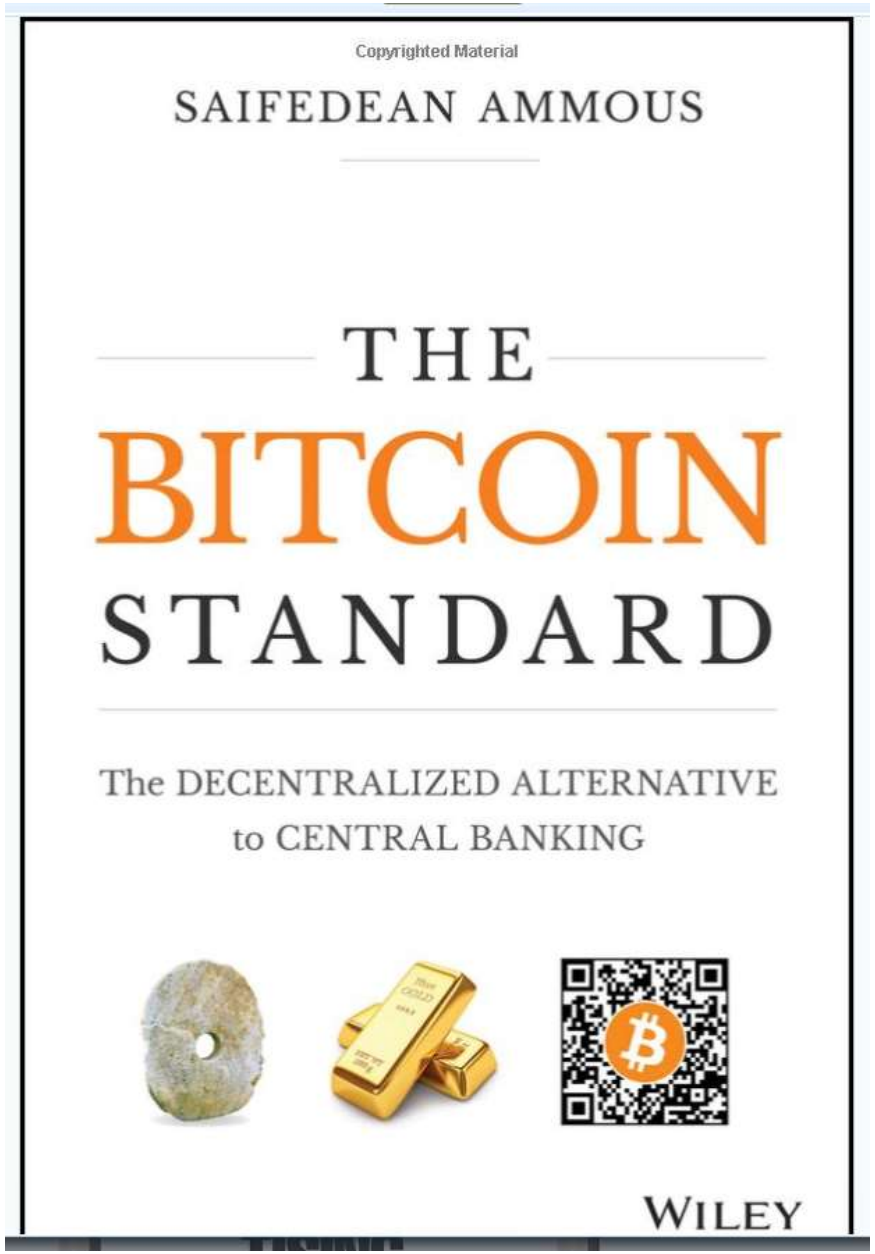
- Long term implications
  - infrastructure for geospatial data
  - no killer app around the corner
- Community map
  - of aerial footage (drone etc)
  - bounties => public tenders
- Proof of location

DHI GRAS

Incentives

- What makes or breaks a blockchain application
- are the correct economic incentives

DHI GRAS


Copyrighted Material
SAIFEDEAN AMMOUS
THE
BITCOIN
STANDARD
The DECENTRALIZED ALTERNATIVE
to CENTRAL BANKING
WILEY

DHI GRAS

THE END

DHI GRAS

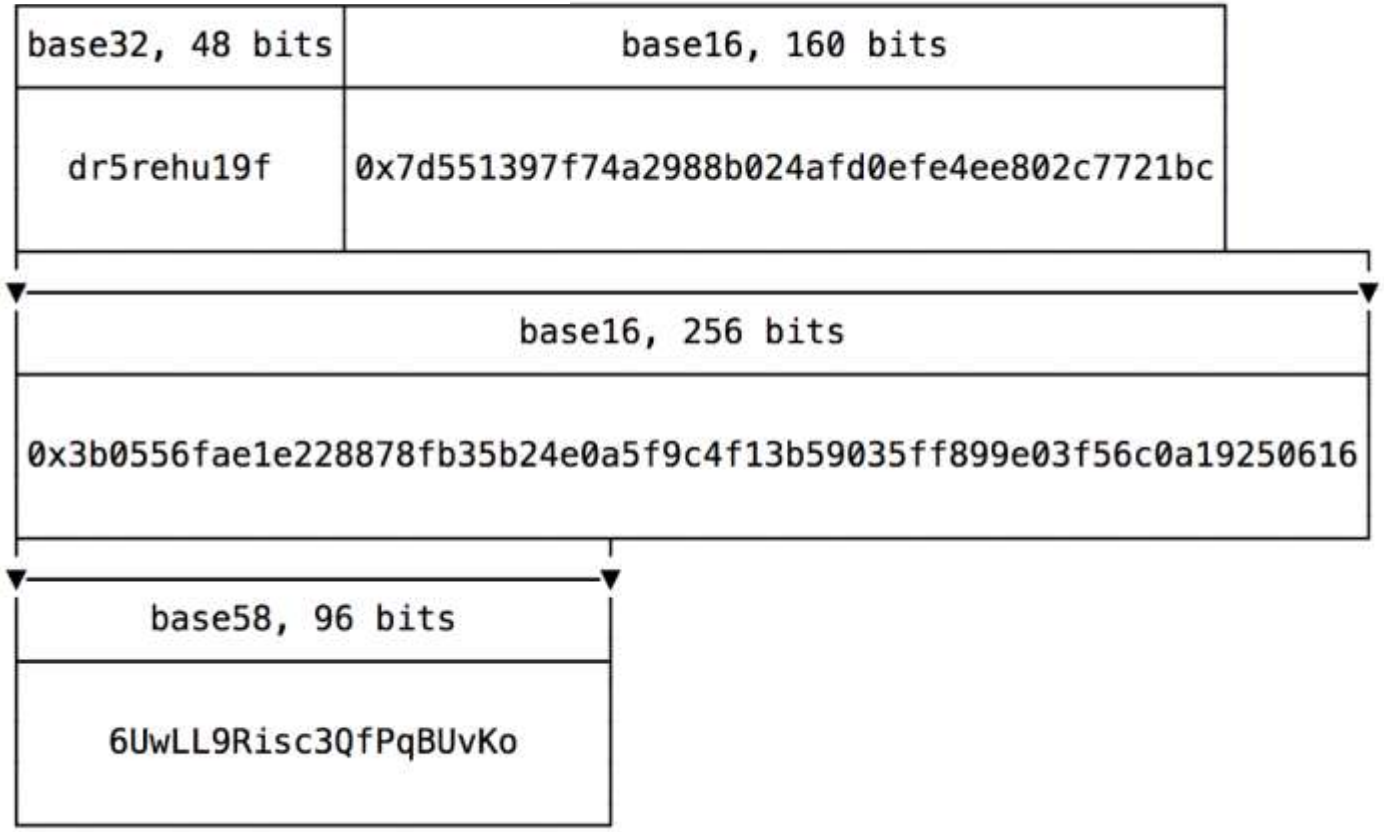
DHI GRAS

The CSC proposal

1. For geographical input, we use a geohash of up to length 10 characters in base32. The alphabet used is the standard geohash alphabet as defined here. This amounts to approximately 50 bits.
2. For the ethereum address, we simply use the 20 bytes, or 160 bits, associated with the address of a contract.

The CSC is a 96 bit identifier, defined as the first 12 bytes of the Keccak-256 hash of the concatenation of the geohash with the ethereum address. In Solidity, this looks like this:

```
function computeCSC(bytes12 geohash, address addr) returns(bytes12){
    return bytes12(sha3(geohash, addr));
}
```

DHI GRAS

In conclusion, the CSC is effectively a human readable representation of a pair of a geohash and an Ethereum address, together with an immutable pairing of the two on the blockchain. It is possible to verify the CSC of a contract and its associated geohash. We lose the ability to derive the location and Ethereum address from this format, but it still allows the CSC to be mapped back to the original geohash and address on-chain using the registry.