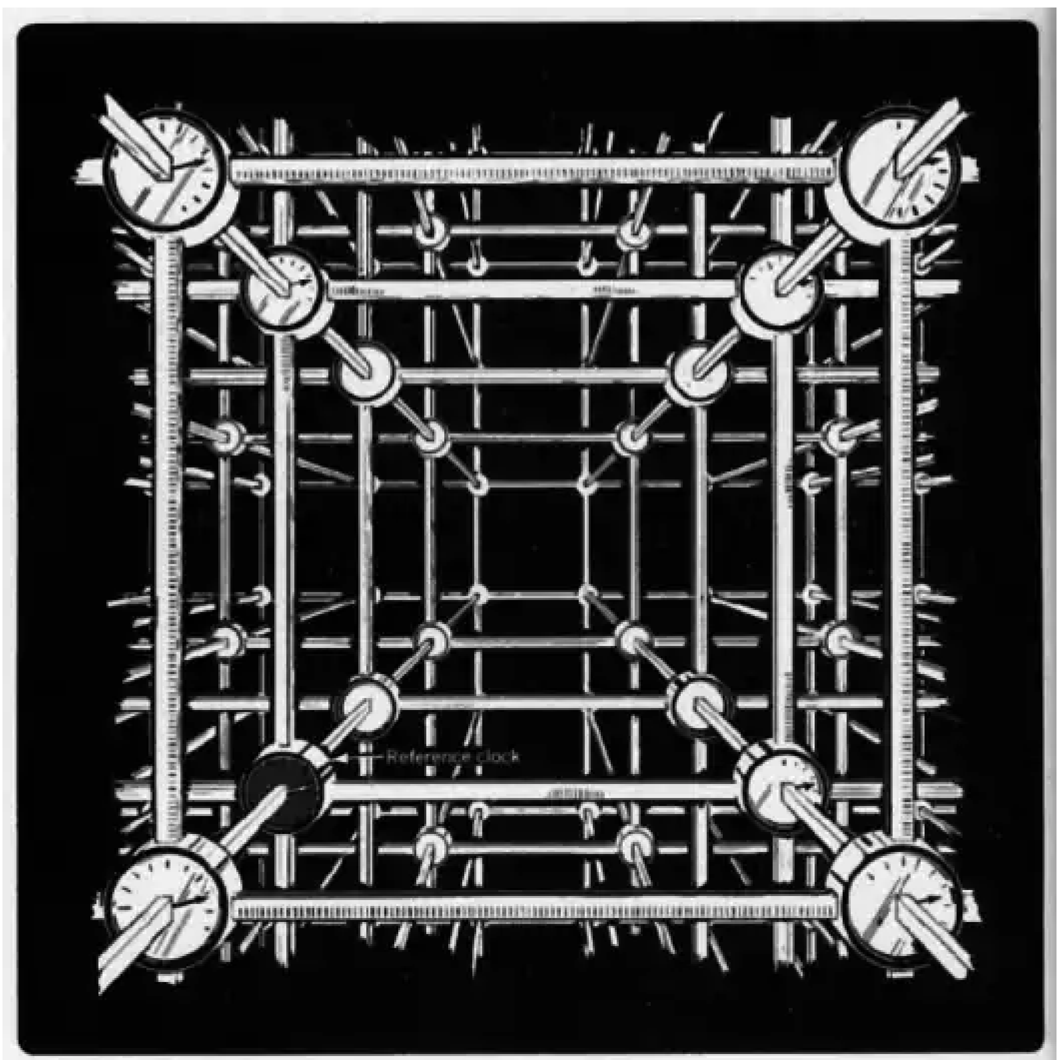
Published in FOAM

Ryan John King Follow

Apr 11, 2018 · 12 min read · Listen

Save

FOAM: The Importance of Time Synchronization



Lattice of Space and Time. Cartography requires machine like clock procedures to produce space coordinates

The fundamental tenet of the FOAM Proof of Location protocol is time synchronization. Fixed radio beacons called Zone Anchors can discover each other in a permissionless and decentralized fashion. Together the anchors synchronize their clocks and establish a Zone, and in doing so maintain a quorum over space and time.

The goal of this post is to explain the importance of time synchronization in a Proof of Location system by way of a historical examination. As we will see clock coordination and time synchronization has been a key factor in cartography and will continue to be for the FOAM protocol. See our previous post for more context:

Video: FOAM — How Proof of Location works

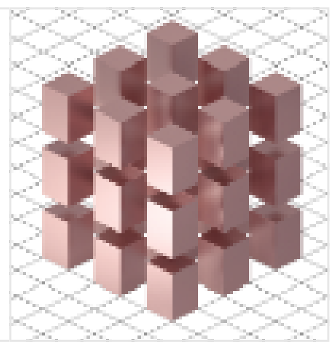
This demo video explains in detail and visualizes how the FOAM Proof of Location protocol works.

blog.foam.space

Introduction to Proof of Location

The case for alternative location systems

blog.foam.space



. . .

General Relativity

In the classical mechanics of Newtonian physics, time is defined as absolute and independent with its own unidirectional flow and pace. With the introduction of spacetime, absolute time was admonished. Albert Einstein's 1905 paper "On the Electrodynamics of Moving Bodies" introduced the theory of relativity while forever dismantling Newtonian physics. He wrote, "Time can not be absolutely defined and there is an inseparable relation between time and signal velocity". Under this new theory, the only means to define time is in reference to a definite system of linked, coordinated, and synchronized clocks.

> ”Time can not be absolutely defined and there is an inseparable relation between time and signal velocity”

Today, distributed clock coordination and in turn time synchronization power our economy and schedule our lives. The history of this development touches on the convergence of Capitalism, Globalization Modernity, Technology, and Philosophy. The Global Positioning System(GPS) of satellites relies on synchronized atomic clocks across ground-based stations in order to offer location services to receivers. However, because the clocks on the satellites are moving through space at varying velocities, relativistic effects on the clocks need to be resolved. **With GPS, the theory of relativity has become a proven technology and has augmented all conventional surveying and cartographic tools.**

Independent of GPS time, International Atomic Time(TAI) is an international time scale computed by taking the weighted average of more than 300 atomic clocks that are located at more than 60 timing laboratories around the world. Additionally, Coordinated Universal Time(UTC)– the primary time standard by which the world regulates clocks and time — is based on TAI but further accounts for “Leap Seconds” which corresponds to the speed that the Earth is rotating. UTC keeps the time synchronized and aligned with the astronomical time of the stars, with corrections defined by the International Earth Rotation Service(IERS).

There is no master clock and there is no single source for the time.

Needless to say, Einstein's breakthrough that coordinated systems require synchronized clock simultaneity holds true, and dictates how we program our technology today. If the the only way to have a coherent meaning of time is through a frame of reference, today we have many to pick from when considering the current differences in the global time keeping standards. Interestingly enough: *"no clock keeps the "official" version of UTC, because TAI and UTC are "paper" time scales that can only be calculated after all of the data from the international contributors are received."* **There is no master clock and there is no single source for the time.**

Canonical Time

Even before the invention of mechanical clocks in the Middle Ages, there was a single source of time known as Canonical Time. Maintained and administered by Catholic churches, Canonical Time was a physical broadcast from powerful bells, hung on high towers. This form of public time broadcast affected the architecture and design of cities. The Medieval Church was much more than a religious institution. It also maintained Canon Law which in addition to time contained standard weights of elements for fair markets and dispute resolution. The church bell tower became the tallest and most expensive structure in every European settlement.

Nick Szabo has documented the simultaneous rise of the mechanical clock and the sandglass in the 14th Century. Both worked separately to redefine the structure and ordering of human relations. The sandglass was used for decentralized portable time and as a means to independently check the public mechanical clocks in the bell tower for fraud. Szabo attributes both the mechanical clock and the sandglass to an economic revolution in time-rate wages over serfdom and standard equal hours that sophisticated institutions and coordination of departments and people could occur. **Common time synchronization allowed for the first "fair and fungible measure of sacrifice" and contracts to be fulfilled around time**. Szabo writes in the Sacrifice of Time:

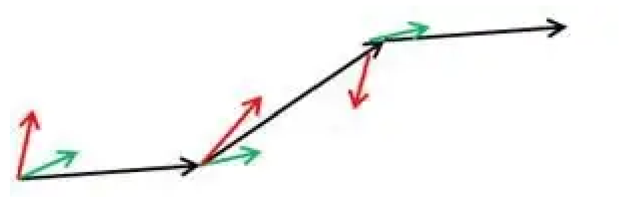
> *"The most valuable property of the bell tower time was not its accuracy, but its fairness. Even if it broadcast the wrong time, it broadcast the same wrong time to everybody."*
>
> *"The productive synchronization of human relationships funded the bell towers; the bell towers would provide a ready market for public clocks. Thus did in Europe emerge a"virtuous circle" that would advance both its timekeeping technologies and time-dependent institutions beyond those of the other continents."*

Clock Tower in Bern, Switzerland where Einstein worked as a Patent Officer

Time for Navigation

To make precise spatial measurements a coordinate and time system is needed. Today technological machines have brought maps and clocks closer together than ever. This also applies to historic navigation systems from the Middle Ages as well, which could not use GPS or any radio assistance for navigational assistance. Instead, local synchronized clocks in the form of sandglasses formed the basis of navigation for early explorers.

A technique known as Dead Reckoning, also discussed by Nick Szabo, relies on predicting movement based on direction, duration, and speed. Originally a manual computation, Dead Reckoning was used by aviators during the Cold War. Distance can be calculated from time and speed in order to generate a sequence of vectors. In addition to sandglass time intervals, a magnetic compass was utilized. This method is highly prone to error. It is also difficult to follow Dead Reckoning directions as it is only a means of navigating through space to a destination. In short, localizing oneself on a map was not possible. Dead Reckoning is made up of **"temporally constant but spatially variable vectors"** that can not be projected onto a Ptolemaic map with lines of latitude and longitude or a Euclidean plane, it only can manifest as a scaleless vector with measurements of time. A Ptolemaic is one that corresponds to the coordinates of the Earth at scale.



The Vectors of Dead Reckoning Directions can not be Mapped to Coordinates

The difficulty of being able to locate your position on a map was historically known as the Longitude problem. Latitude is easily determined through celestial measurements, however **there are no natural elements that can be used to measure longitude. Because of this, getting lost navigating at sea was a real danger to commerce and lives.** Following the disastrous loss of the British Fleet in 1707 near the Scilly Isles due to such navigational errors, the British Parliament passed the Longitude Act of 1714, which created a panel of experts to oversee rewards for solving the problem of finding longitude at sea.

This spurred a breakthrough by John Harrison, a clockmaker who invented a marine chronometer and solved the problem of longitude at sea. The marine chronometer could mechanically keep a reference time of a specific location and remain accurate over long periods, despite changes in temperature, pressure or humidity. **Knowing the difference in time between a fixed location, the Greenwich Meridian and the time of a moving ship can be used to calculate the longitude of the ship using spherical trigonometry.** The chronometer served as a portable time standard, for every hour of difference in local to reference time 15°of longitude could be accounted for.

The electro-coordinated simultaneity of clocks drove the growth in the early 20th century of industry, railroads, telecommunication, and commerce synchronization, synchronized time also became a symbol of interconnected modernity. Simultaneously, there was a rush to establish time coordination systems over radio waves. Radio time soon took over for the marine chronometer and long distance radio allowed more precise determinations of longitude, not only for ships but modern municipalities in colony countries that needed to synchronize their clocks with London, for example as well as orient their location on the map by obtaining an accurate longitude reading from the radio time.

The Eiffel Tower was once a great Radio Time Synchronizer

The Eiffel Tower was slated for demolition in 1909 until its usefulness as a radio tower was discovered. **By 1910, the Eiffel Tower had been transformed into a radio tower, becoming the greatest time synchronizer in the world.** The tower's signal could be used to configure longitude anywhere it could be received. The tower would broadcast a signal every 1.01 seconds and receivers would subtract the difference in seconds of local signals before collision to obtain longitude. In 1913 The Paris Observatory, using the Eiffel Tower to broadcast, exchanged signals with the United States Naval Observatory in Arlington, Virginia to securely verify longitude.

The Asynchronous Internet

Today, clock synchronization protocols– some relying on radio broadcast — are used to provide accurate location and time for many systems without fault. However, all of these systems are centralized and are not interactive. It is not possible to produce a verified digital certificate about your location, the radio broadcasted time signals of GPS can only be used to calculate location. Global clocks have been difficult to maintain between nodes on the Internet because the network is asynchronous, a trusted third party would be needed. Szabo writes, "on our computer networks such "Byzantine" attacks are possible, without advanced safeguards, when"broadcasting" time or other information".

Academic Solutions addressed this problem, but not until the implementation of Bitcoin and the blockchain was the consensus problem implemented at scale for the asynchronous network of the Internet. All participants in Bitcoin are financially incentivized to maintain a ledger of transactions and order them by their corresponding time-stamp. In such a distributed system there is no global "now" and the clocks of local machines drift apart, eliminating the possibility of relying on machine local timestamps for the ordering of data. As a solution, **Satoshi Nakamoto proposed that in the absence of a global clock a Distributed Timestamp Server can be used**, and this is essentially what Bitcoin implements. As Nakamoto writes:

> *"Every general in the Byzantine's general's problem, just by verifying the difficulty of the proof of work chain can estimate how much parallel CPU power per hour was expended on it, and see that it must have required the majority of the computers to produce that much work in the allotted time… the proof of work chain is how all* ***synchronization****, distributed data base, and global view problems you've asked about are solved."*

Such an advancement in Distributed Network Security has encouraged a new resurgence in Byzantine Fault Tolerant(BFT) research with projects such as Tendermint, Casper and DFINITY. For the first time **"a wide variety of services on which civilization depends, whether synchronized clocks, public directories, censorship-proof file sharing and publication, or issuing money or securities"** will be possible over the asynchronous internet with decentralized consensus.

When it comes to repurposing BFT consensus protocols from traditional distributed computing:

dom.icp ∞ · Nov 19, 2017
@dominic_w · Follow
Replying to @dominic_w @VladZamfir and 6 others

2/ Such consensus protocols proceed through rounds of message passing and “decide” on an output value, providing instant consistency rather than converging on a value like a traditional blockchain

dom.icp ∞
@dominic_w · Follow

3/ The protocols come in three main flavors: Synchronous, Partially Synchronous and Asynchronous consensus. The first two flavors make assumptions about how fast participants in the protocol can exchange messages over the network

2:47 AM · Nov 19, 2017

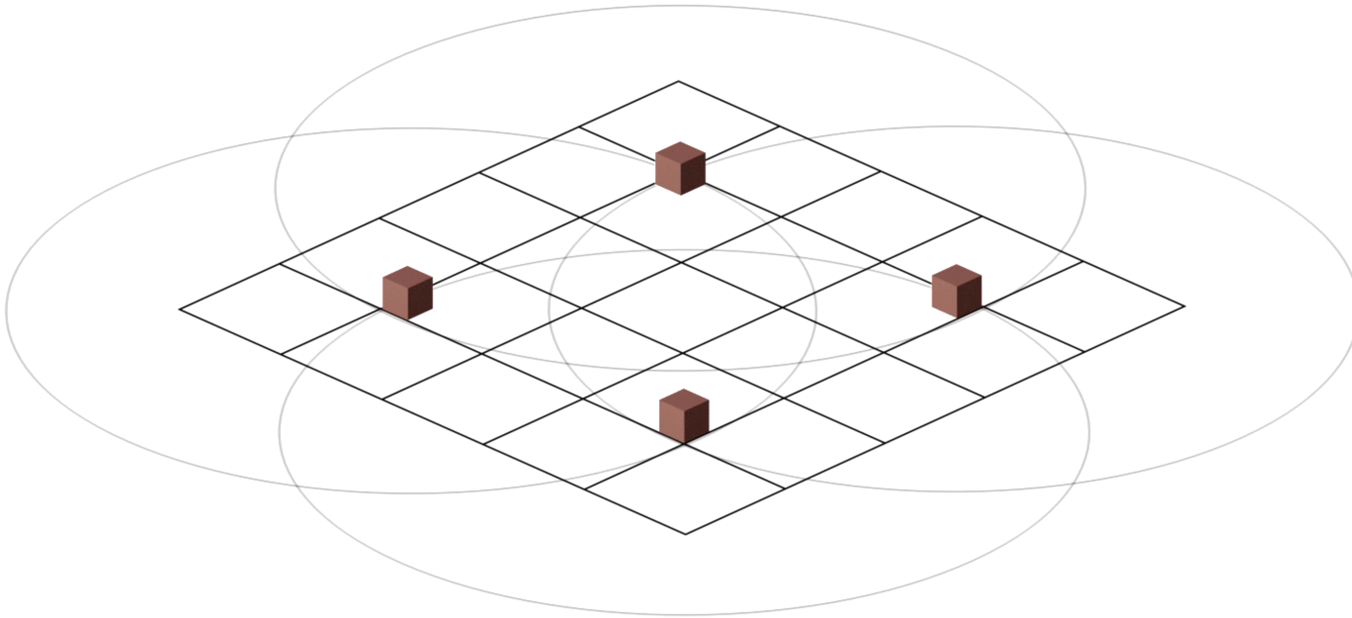
17 Reply Copy link

Read 1 reply

FOAM is focused on implementing synchronized clocks for Proof of Location as a decentralized, privacy preserving, and interactive alternative to GPS and means of measuring space and time for cartography and map making. **The entirety of the FOAM protocol relies on Synchronous, Partially Synchronous and Asynchronous consensus.**

Anatomy of a Zone

A Zone Anchor is a device with a radio transmitter, a local clock, and a public key. A node is capable of engaging in a clock-synchronization protocol and requires a connection to a gateway. Four or more Zone Anchors form a Zone, establishing a quorum and maintaining clock-synchronization for a given region. Once synchronized, the Zone can determine the location of a requesting node by using time of arrival measurements for a verifiably triangulated position.

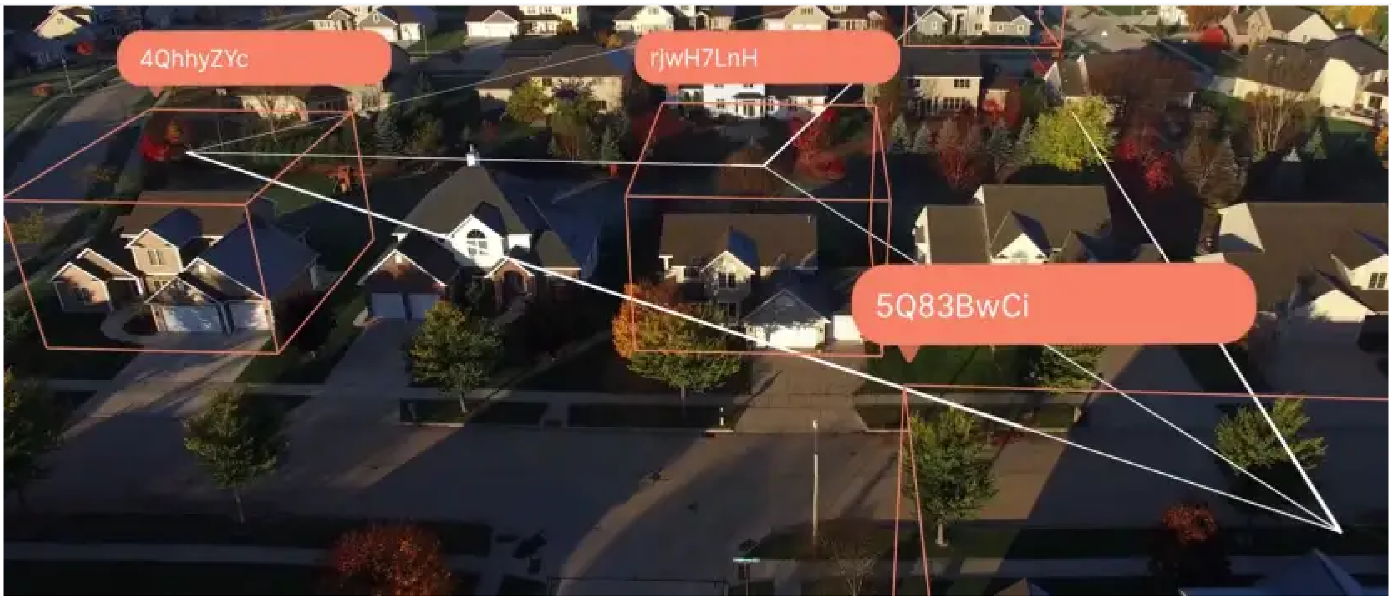


To Triangulate Position over Radio with Time of Flight a minimum of Four Zone Anchors are required for X,Y,Z and variance in time. Trilateration relies on the intersection of 3d spheres.

In FOAM, the anchors in a Zone are running a time synchronization protocol over radio which is self-stabilizing and Byzantine Fault Tolerant. The nodes can synchronize up to one clock tick, depending on the accuracy of their clocks, and determine the geometry of the network without an external input like GPS. **As distance is computed as a function of signal timing from spatially discrete sources, to most accurately compute such positions precise clock synchronization is a required.** Radio Frequency(RF) Time of Flight(ToF) Distance-Bounding algorithms are the family of algorithms most robust against malicious actors. All Radio ToF algorithms rely on having precise clocks, some also rely on clock synchronization. The FOAM Proof of Location protocol utilizes a Byzantine Fault Tolerant clock synchronization algorithm to provide the best possible support for RF ToF algorithms.

Any receiver of the signals emitted by a Zone can localize themselves relative to the Zone. The Zone employs Synchronous consensus, nodes utilize the Time of Flight between the signals from other participants to order the signal arrival time and determine relative distance and location of all nodes in the network. **Simply by correctly operating a Zone, with the necessary token deposit, a Zone Anchor can provide secure localization to receivers of their signals.** Zones will offer Service Level Agreement smart contracts that define the acceptable amount of downtime before having their deposit slashed. Location customers can then purchase digital Presence Claims from Zones as a Proof of Their location.

The anchor nodes that make up a Zone need to keep a log of all the time stamped synchronized messages they receive in a very simple state machine, as well as update this log over time. Additionally, the anchors will need to share this state machine with the other nodes and come to consensus on updating the state machine. For this, the Zone will operate the Byzantine Fault Tolerant consensus algorithm called Tendermint developed in 2014 based on a Proof of Stake design. The main purpose and benefits to Tendermint are speed, consistency, safety, and instant finality.



Simply by operating a Zone correctly with the necessary token deposit, a Zone Anchor can provide secure localization to receivers of their signals

While the clock synchronization over radio and localization for nodes is determined with Synchronous consensus, the consensus algorithm for the replication of shared state machine for a single zone is partially synchronous. The synchronous radio time consensus interacts with Tendermint consensus through the Application Blockchain Interface(ABCI). In Tendermint:

> *Validators wait a small amount of time to receive a complete proposal block from the proposer before voting to move to the next round. This reliance on a timeout is what* ***makes Tendermint a weakly synchronous protocol, rather than an asynchronous one****. However,*

> *the rest of the protocol is asynchronous, and validators only make progress after hearing from more than ⅔ of the validator set.*

Ultimately, to become a validator in replicating the shared state machine of a Zone, and by extension to become a node running the time synchronization protocol over radio, collateral in the form of tokens is needed as a safety deposit on a root or parent blockchain. This deposit is needed to attest they will follow the rules of the protocol without being malicious or faulty. This deposit is subject to being slashed– as in destroyed–if the participant is found to be acting Byzantine. The time log data produced by a Zone is not considered final until it has been verified for fraud by a computation engine running trilateration and other triangulation location algorithms on the Zone's time data.

In this system, the security and consensus of the root chain is an asynchronous network. This can be the Nakamoto consensus of a Proof of Work chain like Ethereum or an established Proof of Stake blockchain like Casper or DFINITY. As such, FOAM employs Synchronous, Partially Synchronous, and Asynchronous consensus for Proof of Location. Further, Time Synchronization as a public good empowers a new class of emerging protocols such as Althea Mesh, a system of software that will let communities set up decentralized ISPs. Althea can benefit from proof of time because it can revolutionize network routing protocols by allowing true latency measurements (right now everything uses round trip time, since you can't rely on someone else's clock). Clock synchronization and a reliable authority on time can have a massive impact on the efficiency of organizing the topology of a mesh network like Althea.

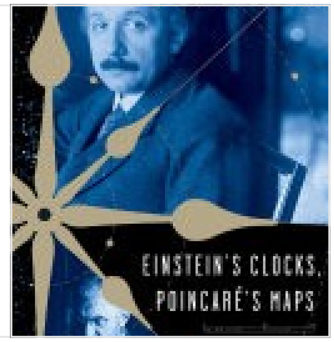
A single FOAM Zone that oversees the local time ultimately is fulfilling the **Lattice of Space and Time**. Cartography requires machine like clock procedures to produce space coordinates. FOAM hopes that the Cartographers on the protocol will contribute the necessary individual work, resources, and effort themselves at the time of launch and onwards to contribute to the ongoing community-driven growth and upgrade of this important cartography project. **With the addition and use of necessary radio hardware time synchronization can continue its historic role of supporting more accurate location and map data.**

Recommended Reading: Einstein's Clocks and Poincare's Maps: Empires of Time

Einstein's Clocks and Poincare's Maps

"More than a history of science; it is a tour de force in the genre."-New York Times Book Review A dramatic new account...

books.google.com



Thank you Rick Dudley and the FOAM team for feedback and comments on this post. Any errors are my own.

We welcome feedback from the community and are open to collaborations, so please get in touch.

...

Blockchain Geospatial Time Cartography Featured