Location Proof Exchange

Proof-of-Location Protocol Summary and Comparison

Kiersten Jowett
kiersten@layoftheland.space
www.layoftheland.space
2018-12-6

Abstract. *The United States military's Global Positioning System (GPS) is jammable[1], hackable[2], spoofable, full of dark zones[3], takes enormous battery power to localize a device and cannot offer a two-way cryptographic "handshake" to confirm location. An enormous portion of the global economy relies exclusively on GPS[4] thus endangering its stability. A small cohort of blockchain protocols are pioneering location proof solutions for the internet of things, smart cities, autonomous driving vehicles, drones and other services requiring more certainty and exchangeable, digital proof about where things are in the real world. Summary and comparison resources of new proof-of-location (PoL) protocols are sparse. This paper chronicles existing and planned protocols. As the PoL environment evolves, further analysis of PoL protocols will be made available at www.layoftheland.space.*

1. Introduction

The purpose and structure of permissionless proof of location (PoL) blockchain protocols is outlined in this introduction and Table 1 reveals the participants in the field and defines some of their attributes. The table is dynamic and will be revised and re-published biannually to reflect ongoing research and the evolution of PoL protocols. Beyond the table, this paper outlines the attributes of each protocol, highlights its strengths and weaknesses, addresses privacy in PoL and, finally, summarizes the status of the PoL ecosystem.

Disclosure: At the time of writing the author owns at least one FOAM token, participates as a cartographer in the FOAM network, is an active member of the FOAM development community and has interviewed the Platin team on the Lay of the Land podcast. All protocol teams were given the opportunity to respond to the table. Platin and Helium teams responded and some of their suggestions have been incorporated.

The purpose of PoL permissionless blockchain protocols is to offer a more robust, secure, private and accurate source of positioning, navigation and timing (PNT) services than is currently possible with GPS and to provide location proof, which is not possible with GPS.

In very broad, general terms this example outlines the structure of a PoL flow on a permissionless blockchain:

1. Alice wishes to prove the location of a device she owns (the device could be her phone, or a chip in a parcel she is sending or a chip in her dog's collar). Alice makes a micropayment in cryptocurrency to Bob, a protocol participant in her area whom she engages digitally to witness and verify the location of her device. Anyone can be a protocol participant by downloading the protocol software from the Internet and running it on their phone or computer. Protocol participants like Bob are called miners and are incentivized to run the PoL protocol because they are paid in cryptocurrency to witness and verify presence claims like the one Alice is making.
    a. The tool Bob uses for witnessing the location of Alice's device will depend upon which protocol Bob and Alice decide to use. (Four different PoL protocols are listed in Table 1.) The tool might be a phone, a Bluetooth device, a hotspot that picks up signals from long range low power radio frequency devices, or an artificial intelligence algorithm that pools data from various sources such as cellular towers, GPS, reputation information or NFC (near field communication). All of these tools are used in one or another of the PoL protocols discussed in this paper.

2. The witnessing tool, sometimes called a gateway, a hotspot or a node (we really need naming standards in this field) writes the encrypted information about Alice's device location (latitude/longitude and time) to a permissionless blockchain on the Internet. This permissionless blockchain, rather than a permissioned database belonging to a single company, is the place where her location data is stored.
    a. Alice's location data is verified by protocol participants like Bob and word is spread to all participants about where Alice's device (using an encrypted identifier) is located.

3. Alice, or anyone she gives permission to, can access her location data by looking at the blockchain records. Alice chooses who sees her data, how much they see and how long they see it. (See the privacy section of this document for more detailed notes.)

4. Finally, in theory, proof of location is strengthened as a network increases in size (i.e. more people like Bob). The larger the network running the permissionless blockchain the stronger the presence claims will be. That is, assuming the network has been well designed, incentivized correctly, coded well and thoroughly audited. In other words, the more independent devices operating the location protocol and witnessing presence claims the stronger the proof of location.

Proof of Location Protocol Comparison

QUICK GLANCE GUIDE

by Kiersten Jowett (chart may be used with credit to author) December 10, 2018 (evolving chart), www.LayoftheLand.space

	FOAM	Helium	Platin	XYO
Whitepaper	https://www.foam.space/publicAssets/FOAM_Whitepaper.pdf	http://whitepaper.helium.com	https://platin.io	https://docs.xyo.network/XYO-White-Paper.pdf
Protocol live on Ethereum main net				
Geospatial Technologist on Team				
Token sale complete		No info	Began Oct. 28, 2018	Ongoing
Uses dedicated radio signalling device				
Uses secure, encrypted location data information				
Uses GPS (Global Positioning System)				
Uses Bluetooth and NFC (near field communication)				
Uses cellular towers				
Uses Smartphone				
Fork of Ethereum blockchain				
Uses gateway to provide internet coverage for local IoT devices				
Creating own new blockchain		`		
Element of proof based on reputation				

Kiersten@LayoftheLand.space

**Darker shades suggests more durability*

Table 1 – *POL Protocol Comparison - Quick Glance Guide*

2. Summary of Protocols

Brief overview of each protocol:

FOAM is a set of PoL protocols, standards, and applications that, as FOAM put it, "bring geospatial data to blockchains and empower a consensus-driven map of the world."[5] FOAM is also a utility token on the Ethereum blockchain. The FOAM team is a first mover in the PoL space having launched their protocol on the Ethereum main net in September 2018. They have successfully deployed third-party audited smart contracts for signaling and points of interest (POI) contracts on the Ethereum blockchain. FOAM display exemplary governance in their community consultation and their work with Token Foundry for their token generation event (TGE). In conjunction with Token Foundry, FOAM built a mandatory investor questionnaire/exam requiring potential purchasers to pass the exam in order to purchase tokens. Furthermore, to prove the FOAM token is a utility token FOAM requires the tokens to be used on their proof-of-location network for 45 days before they can be moved to a secondary wallet or traded on a third party exchange. Monday, December 10, 2018, marks the end of FOAM's proof of use period and the first time FOAM tokens (that have successfully met their proof of use requirements on the network) can be traded.

Curating points of interest (POIs) on the FOAM map (live at map.foam.space) is possible when cryptocurrency (FOAM) is staked against POIs. Any or all community members can challenge any POI for any reason and the community can vote on whether the POI should remain or be removed. The vote winners receive the FOAM tokens staked by the vote losers in the vote. This gamification of POI curation and maintenance creates incentive to build accurate POIs and pays the community to maintain the map.

FOAM is well funded. The team did a seed round in 2017 and raised USD$15.5 million in their token generating event in 2018.

Strengths:

1. Hardware solution increases the dependability of location proof.
2. Currently uses Ethereum blockchain, a three-year-old "known quantity" blockchain, to run its smart contracts.
3. Creates a consensus-driven map of the world and potentially provides more privacy to its users than company-owned maps (Google, Apple).
4. Potential to provide location, navigation and time synchronization as a backup to GPS.

Weaknesses:

1. Relies on human beings to install, run and maintain hardware locally.
2. At present, the security and scalability of FOAM is dependent on the Ethereum blockchain. (FOAM can change blockchains in the future.)

Helium is a decentralized machine network (or DMN as they call it;) running a new, wireless Low Power Wide Area Network (LPWAN) protocol called WHIP (Wireless Helium Internet Protocol). Helium is also employing a bespoke consensus mechanism based on proof-of-coverage instead of proof-of-work called HCP (Helium Consensus Protocol). WHIP and HCP run over a mesh of physical hotspot devices. The deployment and maintenance of these devices are incentivized by a new cryptocurrency, the Helium token. That's a lot of acronyms and a lot of new products.

All these new products support Helium's primary purpose, which is to provide a network of wireless Internet coverage for the Internet of Things (IoT) devices. This coverage enables the IoT devices to communicate with Internet and blockchain protocols without having to be connected to the Internet themselves.

Building a new blockchain from the ground up with proof-of-coverage instead of proof-of-work ensures the mesh of RF (radio frequency), wireless hotspots provide useful and re-usable work to the network. Helium hopes people (a.k.a. miners) will be enticed to set up and maintain hotspot hardware running Helium software because the miners can get paid in Helium tokens by users (i.e. IoT devices) accessing the Internet through their hotspot. The information passing through the miner's device is encrypted so miners cannot read it. Miners set their own fees for user access. Proof-of-coverage works to secure the network but because Helium is not relying on a proof-of-work blockchain to secure their protocol it does not inflict the same cataclysmic energy drain on the environment.

Helium is co-founded by Shawn Fanning of Napster and other heavyweight technologists with substantial funding, USD$38.8 million[6], behind them. Google Ventures have contributed funds to Helium.

Strengths:

1. Does not rely on proof-of-work.
2. Substantial funding and a strong team of veteran technologists.
3. Hardware solution increases the dependability of location proof.

Weaknesses:

1. So many new things to go wrong.
    a. New consensus mechanism.
    b. New blockchain.
    c. New hardware.
2. Relies on human beings to install, run and maintain hardware locally.

Platin was founded in 2017 by two Cornell University graduates and is a software-based solution that promises to provide fast, lightweight proof of location solutions based on GPS, artificial intelligence (AI), reputation, in-phone sensors and other existing data to contribute to better location information and proof. Platin geo-locates any digital asset using, what they call, three pillars of security; sensor fusion, location over time and peer-to-peer witnessing.

The ability to geo-locate any digital asset means users can only gain access to that digital asset when they are in a particular location (for example, a store can place digital assets such as discount coupons around their physical store for customers to collect or a business can restrict access to sensitive, digital work documents granting access only when the user is within the confines of their office building).

Augmented reality (AR) plays a big role in Platin's protocol making their solution more accessible, engaging and understandable to non-technical users. Platin uses zero-knowledge proofs to protect location data.

Platin's software solution could be utilized more easily in locations where a hardware proof of location is difficult or time-consuming to install. Platin runs on a fork of the Ethereum blockchain called Plexus.

Strengths:

1. Can be deployed quickly anywhere in the world with Internet access.
2. A cryptographic expert on the team.
3. Uses zero-knowledge proofs to protect user privacy.
4. Can pull information from other PoL protocols to assist in the geo-location of any digital asset.

Weaknesses:

1. Software solutions may provide less certainty than hardware solutions for location proof.

XYO aims to be the location oracle for smart contracts. XYO is a findable technology device company (i.e. "find my keychain" device) that has shifted into blockchain technology and are using their Bluetooth hardware devices along with smartphones and GPS to create reputation based proof of location.

Strengths:

1. Uses existing, well established Bluetooth hardware in their solution.

Weaknesses:

1. Bluetooth data is not encrypted and not secure.
2. Software solutions may provide less certainty than hardware solutions for location proof.

Other PoL projects worth noting are as follows:

Fysical aggregates sets of mobility data from mobile apps, machines, sensors, governments and consumers to create a data market for buying and selling location data on a blockchain. Fysical recently announced a partnership with XYO.

Street Cred, has recently run a test in New York paying independent cartographers in bitcoin to map the city. They hope to use blockchain as part of the solution but have not yet disclosed the details of their solution.

3. Privacy

Privacy is one of many hurdles to adoption for blockchain technology. Digital identity, scaling, education, regulation and user experience are also critical issues that need to be solved in order for blockchain technology to effectively reach its potential. But privacy seems most critical at this early stage due to its impact on the safety and security of users.

Blockchain technology offers the promise of better privacy than existing centralized database models. However, at this stage, it can only provide pseudonymity, rather than anonymity, to its users. Many sensitive use cases cannot be deployed until this issue is addressed. Some cryptographic solutions, such as zero-knowledge proofs, and some blockchains such as Zcash and Monero, hold promise for improved user privacy but privacy remains a blockchain ecosystem problem. For example, with a little forensic investigation a great deal of information can be garnered from the public trail users leave on most permissionless blockchains. This has serious ramifications for the privacy and safety of individuals, devices and entities using those blockchains to transact.

Privacy in proof of location is a field in its own right and more work needs to happen in this area of research and experimentation. Cryptography's purpose is to provide privacy. It is hoped that each one of these new PoL protocols will harness the privacy possibilities of cryptography. It is clear, however, the blockchain environment has a very long way to go toward ensuring user privacy.

4. Summary

PoL protocols prove location through peer-to-peer exchange of location data.

In the same way that bitcoin solved the double-spend problem PoL protocols are working to solve the location-spoofing problem to be able to prove, in a digital world, where things are in the physical world.

The PoL protocols outlined in this document represent new location data markets and herald in the beginning of self-sovereign location data where individuals own their own location data, control who sees their data, how much of their data is shared and when it is shared. This new dawn also brings financial rewards for individuals who witness and verify location claims and curate and maintain decentralized digital maps.

It is the author's belief that all PoL protocols outlined in this document add value to the present proof of location ecosystem. Each solution has different attributes, teaches us new ways to interact with location data, offers different

levels of location proof and brings different strengths and weaknesses to the fascinating field of proof of location.

5. Future engagement

This is not the end, but rather, the beginning of the PoL conversation. Feedback on this document as well as input and collaboration on future publications is welcome and encouraged. Write to the author at *kiersten@layoftheland.space*

6. Acknowledgments

The author is grateful to all the PoL teams for their ongoing community conversations which help to educate the public about their solutions. Special acknowledgment is extended to FOAM, Helium and Platin who offered valuable comments and contributions during the preparation of the comparison table.

A big thank you to all guests on the Lay of the Land podcast. They have contributed immensely to the author's knowledge and understanding of the proof of location space.

Last, but not least, a warm and heartfelt thanks to the incredibly supportive Melbourne blockchain community and RMIT University.

Works Cited

1. Federal Aviation Administration, International CGSIC Meeting, Geneva Switzerland, May 28, 2007, https://www.gps.gov/cgsic/international/2007/geneva/narins.pdf

2. A.P.D.G. Everett and Alex Berezow, 'If GPS Failed, We'd Be More Than Lost', November 26, 2017, Wall Street Journal, https://www.wsj.com/articles/if-gps-failed-wed-be-more-than-lost-1511730287

3. United States Air Force, Official U.S. government information about Global Positioning System (GPS) and related topics, December 5, 2017, https://www.gps.gov/systems/gps/performance/accuracy/

4. Paul Tullis, 'The World Economy Runs on GPS. It needs a backup plan.', July 25, 2018, Bloomberg, https://www.bloomberg.com/news/features/2018-07-25/the-world-economy-runs-on-gps-it-needs-a-backup-plan

5. FOAM blog, Medium, 2018, https://blog.foam.space/tagged/core

6. www.crunchbase.com, 2018, https://www.crunchbase.com/organization/helium-systems-inc