dPoL: A Peer-to-Peer Digital Location System

Kiersten Jowett

PoLA – Proof of Location Alliance

kj@locationalliance.space

www.locationalliance.space

2019-10-10

**Abstract*.*** *Digital, peer-to-peer proof of location systems, simply known as dPoL, have the potential to uncouple personalized location information from centralized authorities and place the ownership of location information back into the hands of individual device owners[1]. These systems also aim to strengthen trust in the gathering, verification, storage and reporting of digital location information. With a two-way, encrypted communication channel the protocol can send and receive commands from real world devices. dPol is made possible by the combination of two relatively new technologies: LoRa; which stands for long range, low power radio frequency technology; and blockchain technology. This paper explores how the new discipline of dPoL may evolve on top of these new technologies. Specifically, we outline the characteristics that define dPoL and review some potential consequences, both compelling and concerning, that may result from the features of this foundational field during the process of its contribution to the development of the Internet of Things.*

**1. Introduction**

dPoL exists at the intersection of two relatively new technologies: LoRa, a long range, low power radio frequency chirping technology that can both transmit and receive data (first patented in France in 2008[2][3])and blockchain technology, a free and open-source software (FOSS) protocol for witnessing, verifying and storing peer-to-peer transaction records (first published on October 31, 2008[4]). Through digital coordination, via an encryption based blockchain protocol, dPoL builds, arrives at consensus and maintains a historical and ongoing append-only truth(truth defined here as scientifically verifiable and reproducible facts). This system publishes an amalgamation of location data, such as time, latitude, longitude, device identity, reputation and signal strength produced and broadcast by LoRa hardware chirping chip and gateway pairs. LoRa is the physical, hardware layer sending and receiving location, plus environmental and/or sensor information, through its radio signals. Blockchain is the Internet software protocol layer that sets the rules and organizes the information being shared through the radio devices. Both LoRa and blockchain are emerging technologies whose individual strengths and fragilities are actively being discovered.

As these participating dPoL technologies are relatively young, it is difficult to develop predictions for the future of dPoL, based on past observations. However, one might use the first blockchain, the Bitcoin blockchain, as an analogy for dPoL. In the same way that Bitcoin was the first peer-to-peer electronic cash system to solve the double-spend problem, dPoL is the first peer-to-peer digital location system to solve location uncertainty by introducing mechanisms to witness, verify, record and broadcast presence-claims between peers.

**2. Definition**

We define proof of location (PoL) as peer-to-peer location information that is gathered, verified and delivered through consensus, rather than through traditional, single-entity, central authority models. dPoL, a sub-class of PoL, is always implemented through digital means, so it may utilize the strengths of computer science, cryptography, blockchain mechanism design and radio frequency technology. dPoL is a digital, distributed, end-to-end encrypted, peer-to-peer location system, often decentralized to some degree, and always employing both hardware (in the form of a distributed, peer-to-peer meshed network) and software (in the form of a peer-to-peer blockchain or similar) to reach consensus on location information.

dPoL is currently being built on blockchain protocols, but the potential exists for dPoL to be implemented on other network protocols, or meshed designs such as dags (directed acyclic graphs), other gossip protocols, or other future network protocols.

dPoL is in its infancy. There may be more than one definition. The term dPoL is occasionally defined simply as ‘decentralized proof of location’. This is a common definition and is in keeping with other blockchain ecosystem nomenclature, such as dApps (decentralized applications) and DeFi (decentralized finance). However, the term ‘decentralized’ is an evolving, unresolved classification and is to be used with educated care[5][6]. There are other dPoL definitions as well, such as ‘dynamic’ proof of location[7]. None of these definitions is wrong and definitions may change over time.

**3. Characteristics**

The characteristics setting dPoL apart from traditional, single-entity, central authority location services are as follows:

1. **Certainty**

Unlike traditional location services, dPoL is not exclusively concerned with location accuracy. In fact, accuracy is not even dPoL’s first concern. dPoL is designed to produce the optimum amount of location certainty first, through consensus, before addressing accuracy. This structure is based on the design theory that accuracy is only meaningful when it is derived from certainty.

Certainty is a spectrum. The value of data produced by a system is directly correlated to the level of certainty a system can prove it secures. The higher the degree of certainty within a system, the more valuable the data produced within that system. dPoL recognizes that location data delivered through a trustless network, such as a properly incentivized, encrypted, permissionless blockchain, increases certainty and value over location data delivered via unencrypted, more centralized, less-certain systems. Increasing certainty strength, dPoL couples blockchain technology with a real-world, peer-to-peer, meshed hardware network. These two aspects of dPoL, working in conjunction, create what we call the consensus certainty spectrum.

Any claims of certainty must withstand tests of proof built into both the software protocol and the peer-to-peer hardware meshed network. The system must be able to prove it can produce, broadcast, confirm, store and disseminate data with the claimed and expected amount of certainty.

As dPoL is usually deployed through FOSS, claims of certainty, protocol rules and incentive mechanisms are available for public scrutiny.

A large degree of certainty in dPoL comes from its two-way communication feature. No only can a device report its location which has been verified by its peers but it can also send code back and forth between device and system. This means that a device can report its location to the system, have that claim be verified by its peers but it can also receive commands from the system.

Free and open-source blockchain technology assumes some participants who provide work to the system in return for financial reward (technically called nodes or miners) may attempt to corrupt a network for its value: power or money. This dilemma is known as the Byzantine General’s Problem[8] and is one of two crucial problems (the other being the double-spend problem) solved by Satoshi Nakamoto in the Bitcoin whitepaper. Blockchain’s design mechanism reduces the incentive to cheat the system, by spreading the expense and burden of maintaining the system to participants (nodes/miners). Blockchain technology theorizes (and has, so far, successfully demonstrated this theory on the Bitcoin blockchain) that participants should find the system more financially rewarding to play than to cheat.

1. **Localization**

dPoL reverse-engineers the traditional localization process. Instead of pushing location information from a central authority down to the end user’s device, via the platform’s proprietary identity credentials, dPoL device owners use an encrypted private/public key pair. It will generate a presence-claim that requests system participants (sometimes called nodes or miners) to witness, verify and record certain aspects of their claims and publish that encrypted information to the network.

This novel design serves as the foundation for proof of location. Traditionally, location services publish information to a device owner notifying them of where the service thinks a device is located, but the service is not equipped to receive confirmation back. dPoL is purposefully built to provide two-way communication between a device and the network. Significantly, this feature also provides the structure for service level agreements that are unattainable in traditional location systems.

Furthermore, it is not only the devices that need to prove their location to the network, but also the local witnesses (aka nodes or miners) who are constantly required to prove their claimed location by bouncing data back and forth between their device and their peers in order to prove their location to the system. Without confirmation from their peers, they are not allowed to participate in the network, contribute work to the network, or receive network rewards.

Some aspects of dPoL work in similar ways to the traditional Global Navigation Satellite System’s (GNSS’s) triangulation model. This requires four overhead satellites in order to calculate a device’s X axis, Y axis, Z axis and time variant. dPoL localization also requires four nodes: again, one for X axis, one for Y axis, one for Z axis and one for time variant. dPoL nodes must share an atomic clock in order to provide accurate time stamp. Interestingly, this creates the relatively unexplored by-product of decentralized time services.

It is worth noting that the nodes in dPoL can be privately and independently owned by any party wishing to participate in the network. The only requirement for running a node is the will and means to purchase a node (sometimes downloading software is required) and provide electricity to keep the node connected to the Internet.

In effect, through its radio frequency communication, the node provides Internet access for the data produced by devices wishing to publish to and receive information from the Internet. In other words, dPoL is a major IoT (Internet of Things) play.

1. **Location History Storage**

dPoL introduces the potential for location history to be stored with the device owner. Because location information is generated exclusively at the request of the device owner, rather than pushed from a central authority to the device owner, in the dPoL model, location history is the property of each device owner, rather than that of the network. dPoL device owners decide whether or not to publish their location information to the network and can choose sharing parameters such as how much data, for how long and to whom it is visible.

Once location information is published on a permissionless network the information is no longer private. However, the ability to generate, publish and/or sell location information remains exclusively in the hands of the device owner. The level of anonymity of the device location depends on which dPoL protocol is employed and what rules are written into the protocol. The protocol rules will either be established on an ongoing basis through consensus governance, or through the decisions of centralized core developers, if the protocol contains centralized elements.

1. **Digital Identity**

The digital identity of a device can be a cryptographic public/private key pair. Or, in more centralized dPoL protocols, it can be tied to a known or pseudonymous user identity.

As the name suggests, the public key is used for identification within a public network and the private key is used to control the flow of information communicated to the network. Device ownership can be proven by altering the quantity, characteristics and timing of information that is broadcast to a public network. Digital identities and device location histories are associated with real world hardware devices in dPoL and not usually designed to hop between different devices. This is particularly true in more decentralized protocols. dPoL accounts are, therefore, most often associated with a single hardware device.

This design provides a different kind of privacy for device owners than has typically been associated with traditional location information services. According to Giacomo Brambilla, Michele Amoretti and Francesco Zanichelli, at Distributed Systems Group, in the Dept. of Engineering and Architecture, University of Parma, Italy:’The decentralized nature of peer-to-peer systems guarantees higher privacy levels, as it removes the central authority knowing both the geographic location of users and the information they exchange.’ *[5]*

1. **Power**

dPoL requires power for both its hardware network and its software protocol.

* + Hardware

Power consumption requirements are relatively low for hardware devices initiating radio frequency communication across a localized meshed network. Both the frequency and quantity of data being transmitted between dPoL hardware devices are customizable and can be optimized for low power consumption. For example, sometimes just a few lines of code sent at very infrequent intervals are all that is required. These customizable message times and low data volume packets are notably different from traditional location services which require enormous battery power to continually localize a device, through a combination of cellular signal and satellite information.

* + Software

The power consumption requirements for dPoL software protocols vary widely. Some dPoL protocols have the potential to be extremely low in power consumption, while others pull a heavy load of electricity from the grid. Four types of protocols and their energy consumptions are explored here: proof-of-coverage, proof-of-work, proof-of-stake and propriety networks.

The free and open-source Helium Inc. blockchain is an example of a protocol with low power requirements[9]. Helium advertises their ‘hot spot’, a device that witnesses, confirms and writes data to the Helium blockchain, as needing about the same amount of energy as an LED light.

FOAM, also a free and open-source blockchain protocol, is presently running on the Ethereum blockchain[10], which may or may not require large energy consumption, depending on its consensus algorithm. Ethereum is proposing to move from the current, power-hungry proof of work consensus algorithm, to proof of stake, a lower power option, when it upgrades to the Ethereum 2.0 protocol (presently reported as scheduled for release in 2020). If the upgrade to proof of stake is successful then energy requirements for dApps running on the Ethereum protocol will decrease. In addition to speed, proof of work versus proof of stake protocols affect the security of a network. Security of free and open-source blockchains is a deep, wide and fascinating field and, though it is not explored in this paper, it holds major implications for dPoL and remains in the scope of further work. Extensive research that compares proof of work and proof of stake has already been completed and what remains is to overlay these findings onto the dPoL field.

Finally, permissioned, propriety networks, such as Amazon’s newly announced Sidewalk, which is a proof of location radio frequency technology, does not typically share protocol power consumption data publicly.

1. **Data Ownership**

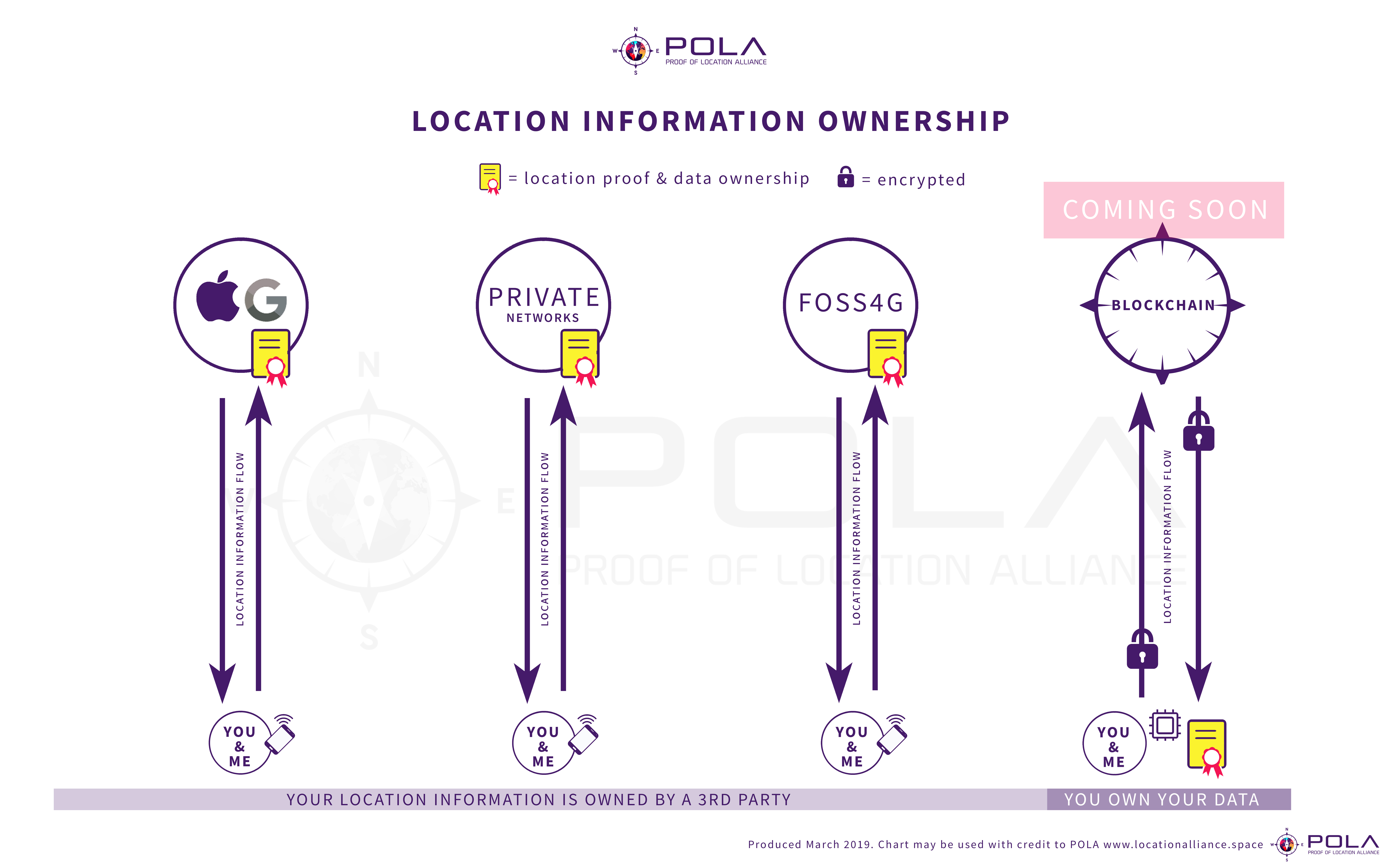
dPoL is classified as a disruptive technology because it enables a new distribution of authority. It inverts the ownership structure of current location information service providers, such as Google, Apple (figure 1.). They presently own the location and history information for all devices accessing their centralized network. dPoL introduces a more sovereign model, removing authority from the service provider and, through its use of cryptographic key pairs, places location information ownership in the hands of individual device owners. For now, LoRa exists as specialized, technological hardware out of the reach of the general population. However, it is not a difficult leap to imagine LoRa may one day be incorporated in a wide variety of personal devices mass produced for commercial consumers.

dPoL’s introduction, as a new location information model, into a narrow field previously dominated by GNSS, mainly GPS (The United States deployed and owned Global Positioning System) and Galileo (Europe’s global positioning satellite system), exposes the field to disruption. Specifically, through the use of cryptographic public/private key pairs within the blockchain layer, dPoL is poised to invert the traditional structure of location information ownership. This is done by taking ownership away from traditional protocol owners and passing it to owners of long range, low power radio frequency device, who will be able to choose what, with whom and for how long they share their location information.

Still, location data ownership may not be a compelling reason for much of society to adopt this new technology.

It has become apparent in the blockchain ecosystem, that different individuals place varying degrees of importance on self-sovereign financial custodianship. It can be expected that a similar spectrum of choice may also play out in the location information space.

However, regardless of whether or not dPoL is utilized for its self-sovereign properties, the structure of dPoL’s data creation, verification, dissemination, storage and two-way communication identifies it as a new kind of location information architecture.



*figure 1.*

*Blockchain technology relies on consensus algorithms to determine location*

*allowing encrypted data ownership to remain with the user.*

**3. Critical Analysis**

In this section we aim to provide a quick guide, accompanied by expanded, exploratory text detailing the most compelling, as well as the most concerning, aspects of dPoL.

|  |  |
| --- | --- |
| Compelling | Concerning |
| dPoL provides a new, alternative digital location information model, where only one existed before. | dPoL’s introduction of a new location information systems model brings new challenges, both defined and undefined. |
| If dPoL is deployed on a permissionless blockchain, then all the usual permissionless blockchain advantages exist, including but not limited to:   * + Self-sovereign identity, history, and data permissions. This enables one to own one’s own location data. Some protocol participants have the option to control with whom, how much and for how long they share their data   + Non-centralized data storage   + Fewer geo-political influences   + Censorship resistant network participation   + Free and open-source software for anyone to participate in   + Space to innovate outside stifling regulatory requirements in some jurisdictions   + Any knowledgeable software developer can suggest proposals to the protocol   + The option to implement voting on a decentralized permissionless blockchain   + Monetary incentivization and disincentivization of a network protects it from several different kinds of attacks: a 51% attack, or a ddos (distributed denial-of-service) attack. It also decreases the likelihood of purposeful, fraudulent data contributions   + Developers are not restricted to operating within specific bug reporting and fixing procedures   + Some blockchain protocols are energy efficient. (It depends on the blockchain protocol deployed). | If dPoL is deployed on a permissionless blockchain, all the usual permissionless blockchain challenges apply, including but not limited to:   * Responsibility for custodianship of identity and data * Lack of any ‘help desk’ on permissionless networks * Inability to disempower groups with conflicting motives, including restricted ability to police criminal activity * Few consumer data protection rights exist in blockchain technology; specifically, The Right to be Forgotten. The Right to be Forgotten is the antithesis of most current blockchain technology structures * Lack of regulatory clarity around cryptocurrencies in some jurisdictions prohibits development by mainstream contributors * System latency and compounding scalability issues * Lack of education and educational resources for blockchain user and potential users * More decentralized voting research is required. Various decentralized voting mechanisms are being explored on different blockchains but no definitive voting solution has been adopted as an industry standard * The present-day blockchain eco system suffers a reputation of supporting an unhealthy proportion of nefarious participants * A paradigm shift in the way blockchain technology is incorporated in business is necessary * Profound lack of software developers with knowledge about how to improve the protocol * Lack of standards. a) The gaping chasm of guidance standards for cryptocurrency issuance increases risk to participants and eliminates large, accredited, risk-averse players. b) In the absence of protocol standards for developers, trial & error and personal research are the only ways to proceed. A substantial developer standard framework is absent. * Blockchain is a rapidly evolving, shape-shifting technology which is extremely difficult, if not impossible, to fully comprehend. * There is no clarity around the procedure of reporting and fixing bugs when found in the FOSS. * Some blockchain protocols are not energy efficient. (It depends on the blockchain protocol deployed). |
| There are limitless dPoL protocol options. Developers can use FOSS and open-source hardware to build a protocol using radio frequency technology and blockchain technology. | Adoption of dPoL location systems remains slow and fractured, as each system attempts to build its network independently. |
| dPoL’s innovative structure affords the opportunity to improve upon previous standards, as well as introduce competition. |  |
| The slow, time-consuming nature of building a decentralized network means mechanism design can be tested when the network is small: faults may be found before they create cataclysmic consequences; and improvements can be quickly deployed in new iterations of the protocol. | Mechanism design is an extremely complex practice. Often behaviour of participants on a network cannot be predicted during the initial design. It may change rapidly and regularly based on variables within the protocol, such as quantity of participants |
| Does not rely on one single source of unverifiable truth.  More nodes create stronger, more verified, more attack resistant consensus of ‘truth’.  If a single source of truth is corrupt, inept or insufficient, a second, third, fourth and maybe millionth (etc.) node can counteract that single sources fault and contribute to a more reliable truth. We have seen this play out in the Bitcoin blockchain with the greater number of participants both securing the network and consequently providing a more reliable network. | Does not rely on one single source of truth.  If the network is not secure, participating nodes can be compromised and nefarious actors can influence consensus |
| dPoL accounts are generally tied to encrypted public/private key pairs, making location information and transaction data partly anonymous. | Privacy on permissionless blockchains is not yet solved. Data privacy protection is determined by the protocol rules; security; certainty of location and time; and the ability to amend the ledger and protocol itself (note: not all blockchains are append-only). We don’t know what less-than-anonymous participation will mean for the location data of a ‘thing’, device, owner or identity. |
| Radio frequency technology provides:   * Relatively low cost options * Long range signal * Low power usage * Long battery life * Efficient data transmission for devices without Internet access * The ability to control devices in the field without Internet connectivity * Historic and ongoing data for better reporting and decision making. | Some radio frequency technology concerns include:   * Unproven attack vectors * Decentralized meshed networks sometimes provide little support for participants * Large buy-in by participants to build a network * Varying global restrictions. |
| dPoL brings decentralization advantages. Every dPoL protocol has unique features that make it more or less decentralized. dPoL improves on the level of decentralization that has existed previously, but it is a spectrum and different protocols will provide different levels of decentralization.  Location history control: a location history is available to all network participants. When a central authority provides location information the historic data is provided, or not, at the discretion of the entity. | Decentralization brings with it enormous challenges, including but not limited to:   * Governance * Voting * Improvement procedures * Security * Latency * Scalability * Privacy * User Interface (UI) * User Experience (UX). |
| Radio frequency technology has a global, diverse and connected development community with an abundance of tools and innovative solutions for solving real world problems. | Radio frequency technology is currently a highly technical field. User Interface and User Experience are hurdles to adoption for both new developers and users, and contributes to loss of participation. |
| New cryptocurrencies can be issued by entities to secure their network. | Monetary incentivization and disincentivization of a network comes with many complexities.  Protocol cryptocurrencies can be hijacked by speculators. Both innocent and malicious incentivization errors within a protocol can hijack protocol cryptocurrencies, crippling a network. |
|  | It is time-consuming to build a network. The costs are generally borne by the network participants who own their own device. The software is usually free and open-source, so cost is not so much a factor, but incentive and ongoing participation remain issues. |
|  | The concept of decentralization is, in fact, a spectrum, ranging from centralized to decentralized. It remains a utopian idea in most permissionless blockchains, with the exception of the Bitcoin blockchain.[11] |
| Decoupling time services from centralized entities broadens the resilience of global time services and opens new markets. | All problems associated with a decentralized network, as listed in the cell above (with the exception of UI and UX because users rarely interface with time services), apply to time services on a dPoL network. |

*chart 1.*

*Compelling and Concerning Qualities of dPoL*

dPoL provides a new, alternative, digital location information model where previously only one existed. dPoL does not eliminate existing models, but rather adds another location system option and provides new location features, such as being able to prove location and control devices without an Internet connection. However, this new model also introduces new problems, many yet undefined. As dPoL uses several technologies in unison, the advantages and disadvantages of each technology becomes a feature of dPoL. When combined these compound.

An extensive, but incomplete, list of advantages and disadvantages of blockchain technology is represented in chart 1. Blockchain technology is a complex and rapidly evolving field, making dPoL’s reliance on the technology equally complex and evolving. dPoL inherits blockchain technologies’ strengths and weaknesses.

Underlying blockchain technology is the emergence of a decentralized movement. While there is uncertainty in the classification of the term ‘decentralized’ it is clear that decentralization both fuels dPoL’s advancement and simultaneously cripples it with unsolved problems and unanswered questions.

In addition to blockchain technology and the progress of the decentralization movement, dPoL is also developed from the relatively young, long-range, low-power radio frequency technology, LoRa. Currently, only accessible to highly skilled technologists, Lora promises to provide opportunities for individuals, devices and environments to participate in broader coordination. While some LoRa networks, such as The Things Network, have successfully been globally deployed, it remains an emerging technology. The strengths and vulnerabilities of LoRa will also become part of dPoL.

Finally, time services enabled by dPoL create an opportunity to enhance the world’s resilience in the face of the fragilities of present, centralized time services. They will also unlock new flexibility for time services and time services markets. Time services will be both strengthened and hindered by the relatively early phase of decentralized philosophies and protocols.

How these elements combine to contribute to the growth and evolution of dPoL forms the scope of our further exploration.

Furthermore, we acknowledge ‘there are a number of radio technologies and techniques for localization/positioning systems without the use of GPS. These alternative position systems use a range of localization processes and techniques, which include Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA) and Received Signal Strength (RSS).’[12] Further research on these specific systems will inform future work.

**4. Conclusion**

We have outlined the characteristics that define dPoL and reviewed some potential consequences, both compelling and concerning, that may result from the features of this field which is proving foundational in the development of the Internet of Things. We started with a clear and precise definition of the field itself, as well as the technologies currently within the field. We acknowledge dPoL is a rapidly growing business and research field, with a swiftly changing landscape. These qualities mean definitions will change and numerous definitions may apply. In an effort to provide clarity for early participants, as well as mitigate confusion during representation to the general population, we provided the compelling case for dPoL and concerns participants may want to consider. dPoL builds on the solution of the double-spend problem solved by the Bitcoin whitepaper. It represents a second stage in evolution for peer-to-peer digital transactions, with the notable addition of two-way communication between participants for real-world device functionality.

dPoL makes a non-trivial contribution to the evolution of the Internet of Things.

**Works Cited**

[1] John Hermann, ‘Google Knows Where You’ve Been, But Does It Know Who You Are?’, The New York Times Magazine, September 12, 2018 <https://www.nytimes.com/2018/09/12/magazine/google-maps-location-data-privacy.html>

[2] Devopedia, 2018, ‘LoRa.’ Version 7, June 19, Accessed 2019-08-21, <https://devopedia.org/lora>

[3] Craig Hornbuckle, ‘Fractional-N Synthesized Chirp Generator’, United States Patent, Patent #7791415B2, Semtech Corp, May 16, 2008, https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2008144579

[4] Satoshi Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, October 31, 2008, <https://bitcoin.org/bitcoin.pdf>

[5] Vitalik Buterin, ‘The Meaning of Decentralization’, Medium, February 7, 2017, <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>

[6] Kiersten Jowett, ‘The Nomenclature and Procedures that Define Decentralization’, Medium, February 10, 2019, <https://medium.com/@kierstenJ/the-nomenclature-and-procedures-that-define-decentralization-aad599dcf46b>

[7] Ryan John King, ‘Introduction to Proof of Location’, Medium, January 24, 2018, <https://blog.foam.space/introduction-to-proof-of-location-6b4c77928022>

[8] Lamport, L.; Shostak, R.; Pease, M., ‘The Byzantine Generals Problem’, ACM Transactions on Programming Languages and Systems. 4 (3): 382-201, 1982

[9] Amir Haleem, Andrew Allen, Andrew Thomson, Marc Nijdam, Rahul Garg, ‘Helium, a Decentralized Wireless Network’, November 14, 2017, http://whitepaper.helium.com

[10] Kristoffer Josefsson, ‘The Rise of the FOAM GeoPickle TestNet’, Medium, February 28, 2019, <https://blog.foam.space/rise-of-the-foam-geopickle-testnet-22b20739d541>

[11] Louise Matsakis, ‘Rest Easy, Cryptocurrency Fans: Ether and Bitcoin Aren’t Securities’, Wired, June 14, 2018, https://www.wired.com/story/sec-ether-bitcoin-not-securities/

[12] Giacomo Brambilla, Michele Amoretti, Francesco Zanichelli, ‘Using Blockchain for Peer to Peer Proof-of-Location’, Medium, January 24, 2018, <https://arxiv.org/pdf/1607.00174.pdf>