GEO Protocol

Max Demyan Dima Chizhevsky

April 21, 2019

Abstract

GEO Protocol is an open-source economic technology that enables a global network for value transfer by connecting economic participants across both cryptocurrency and traditional finance. It forms a multi-layer protocol stack akin to TCP/IP, which disparate financial relationships within the banking, financial, and blockchain infrastructures combine into a cohesive network that can perform complex economic transactions across multiple value networks. At scale, GEO Protocol is designed to mostly eliminate volume-based transaction fees, replacing them with fiat subscription fees paid to the network service providers. The protocol uses local consensus, which allows high throughput and transaction speed. GEO enables complex atomic transactions in multiple assets, and can also be used to implement a variety of novel topologies for IoT payments, cross-border payments, and cryptocurrency on- and off-boarding. GEO implements post-quantum cryptography for long-term sustainability.

Contents

1 Introduction

A number of challenges are currently causing stagnation in the payment processing industry. Weak integration between different payment systems results in high fees and slow transactions; the payments market is highly monopolized; fragmented regulatory environments place a burden on international payment processing. The innovative space of blockchain technologies suffers from different but significant challenges. Due to insufficient interoperability and limited scalability, processing payments can be slow, require high transaction fees for on-chain actions, and lead to an ever-growing resource consumption.

The main technical challenge in payment processing is to ensure participants cannot misrepresent their holdings, and ultimately spend money they do not have. The three known ways to prevent participants from making false claims of payments (also known as the double-spend problem) are:

- Using a trusted intermediary to hold a database that, at all times, expresses the global truth (the trust-based model);
- Using a consensus protocol, such as the one used by Bitcoin (the trustless model);
- Using a distributed loan accounting mechanism, such as the one used in the historical Hawala payment network in the Middle East (the distributed-trust model).

Only the trustless and the distributed-trust models such as GEO can enable peer-to-peer payments, where individuals transact without putting their faith in an intermediary (which may abuse or misuse their power).

The era of peer-to-peer payments started with the Bitcoin protocol, which enabled fully trustless transfers of an abstract asset between network participants. Additionally, the Bitcoin network is completely open and highly censorship-resistant: it is impossible for anyone who does not possess a vast (and visible) amount of economic power to prevent users from holding funds or from sending payments.

The trustless approach to P2P payments has a number of drawbacks, extensively covered in the cryptocurrency literature. To summarize: it is computationally expensive and wasteful; it cannot operate on lightweight and mobile devices; it is often slow; and it requires secure key-management – a big hurdle to broad adoption.

Moreover, the interoperability between different cryptoasset networks is limited, and presents significant technical challenges. GEO Protocol solves this problem by creating a lightweight overlay network that enables a seamless exchange of value between disparate blockchain networks.

GEO Protocol provides an alternative to existing payment systems that is based on the distributed trust model of peer-to-peer payments. However, when applied to blockchain-based cryptoassets, it becomes a fully trustless layer for payments, based on the innovation of blockchain layer 2 networks. Thus, GEO can simultaneously serve as a viable link between distributed ledgers and enable transactions in non-digital assets (e.g. fiat money, commodities and securities). GEO Protocol can be used for three types of operations: to send and accept payments; to freely exchange assets for other assets, including both crypto- and fiat currencies; and to provide onboarding and offboarding capabilities for cryptoasset networks and exchanges.

1.1 Market overview

Technology has already reached a level sufficient for sending money easily and safely — as easily as sending a text message between smartphones. Yet, the existing infrastructure has been slow to adapt to this new landscape. At present, the financial industry is mostly built on trusted intermediaries that manage assets and process transactions. These intermediaries are poorly interconnected and possess many inefficiencies. Sometimes they even rely on manual operations. The current challenges include:

- *Weak integration.* Due to the high costs of integration, only a few payment service providers cooperate with each other. Fees are charged for transactions (with commissions for international transfers especially high), and the transaction speed is low (in some cases, it could take several days to get the money from sender to recipient). A payment can even get lost during the execution of a transaction between parties. The level of fraudulent activity is high.

- *Monopolization of the payment processing market.* Monopolies and their closed-source software limit the interaction between market players and consumers. The lack of open-source payment processing technologies is a deterrent for innovation in the sector: one should be able to integrate payments and finance into a broad spectrum of mobile and web applications, but the hurdle of integrating with a large number of payment systems is insurmountable. This dynamic prevents the expansion of e-commerce into areas such as reward points, gift cards, and other innovative commercial models.

- *Regulatory challenges and cross-jurisdictional differences*, which make cross-boarder payments difficult and expensive. GEO simplifies global payments by pushing regulatory obligations onto individual participants, and provides a simple, uniform method of decentralized connectivity between them. In contrast, traditional payment systems had to ensure regulatory compliance with every jurisdiction in which they operated, representing a significant startup cost.

The emergence of trustless technologies for asset accounting and payments made secure financial transactions without intermediaries possible. Because of the challenges within the legacy system on the one hand, and the high availability of newly developed trustless technologies on the other, the use of the latter has grown significantly. This has led to the creation of an entirely new economical and technological ecosystem - the crypto industry.

But despite the revolutionary properties of digital assets, blockchain technology is objectively insufficient to fully serve as retail payments, exchanges, or national currencies.

Moreover, each cryptoasset exists as a closed ecosystem due to regulatory requirements, incompatible technologies, and an absence of industrywide standardization. This makes the crypto industry even less flexible than legacy finance.

Technologies in the cryptocurrency sector have been evolving rapidly, but mostly in the direction of consensus mechanism improvement. Simultaneously, a demand for off-chain ("layer 2") solutions has emerged to answer the foundational constraints of today's blockchain systems, such as the low speed and high cost of transactions.

State channels are a specific form of layer 2 solutions that operates by routing transaction in a pair-wise connected network where intermediate nodes commit capital as a trust-mitigating guarantee of payments. Analysis of existing projects shows that state channels are not able to provide a solid answer to the overall challenges of payment networks. Some problems, such as the limited liquidity (low maximum flow) of state channel networks and the lack of interoperability between different state channel networks, still exist.

The challenges on the near-term horizon for the crypto industry in general and the layer 2 network in particular include:

- Barriers to mass adoption, low flexibility and customizability
- Difficulty performing transactions between different ledgers and ecosystems
- Edge cases that break transaction atomicity guarantees in layer 2 networks, thus increasing implementation complexity and reducing customer's confidence
- Growing transaction costs
- Low or insufficient maximum flow capacity due to capital commitment requirements imposed on intermediate nodes
- Difficulty in accommodating lightweight and mobile clients

1.2 GEO Protocol summary

The main task of a payment processing system is to transfer the financial rights counterparty A (an individual or an organization) has against value store X (a bank or a blockchain network) to counterparty B, with the result that counterparty B can now be assured of having similar financial rights against some other value store Y. Importantly, X and Y may be different, and in the process of payment between A and B, X and Y may engage recursively in a similar process of transferring obligations to each other. Ultimately, every party in the payment network must trust its respective value store.

GEO Protocol provides generality, flexibility, and versatility of financial relationships by encoding the relationships between participants explicitly, permitting every member of the

network to express their trust in a specific value store or counterparty. Where the value store is a blockchain network, such a relationship will carry the same guarantees that a blockchain provides to its users. Namely, it will express trust not in the people, but in the technology. GEO Protocol reformulates the role structure of a financial network from multiple roles (customer, value store) to a single role, participant, whereby any participant can use any other participant as a source of financial guarantees.

Conceptually, this is similar to the transition between pre-Internet line-switched networks where the roles of an end-point and a switch were technologically distinct, to the Internet-era TCP/IP packet switched networks, in which the switch and the end-point were no longer technologically distinct, but rather became parties to a peer-to-peer connection that could be combined with other such connections to ensure incredibly flexible global connectivity. By eliminating distinct roles within the payments network, GEO similarly removes architectural complexity and enables global payments in a uniquely flexible and accessible network.

Economically, GEO Protocol replaces transaction-based fees with subscription fees wherever possible.These fees are paid to service providers in the network that provide its greater functionality. The majority of GEO network's operations, as defined by the protocol, are purely technological services (with the notable exception of hubs and market makers that require a commitment of capital). Recognizing that reliably running prepackaged software is inexpensive, GEO Protocol aims to transition critical services to a model in which subscription fees are sufficient to cover operational costs and to adequately reward operators. This creates an ecosystem that can disrupt the traditional financial infrastructure on both cost and availability.

GEO Protocol takes into account both the problems within the legacy financial system and the challenges of cryptoeconomy. Our solution is to build a sustainable and efficient network that can process financial transactions between different value hubs, some of which are cryptocurrency networks. The key features of the GEO Protocol are:

- Like TCP/IP, GEO is a multi-layer protocol. GEO Protocol is a high-level routing and settlement protocol that can function on top of a variety of financial "transport layer" protocols provided by either traditional financial networks or blockchain value hubs.
- GEO operates as a network of pair-wise connections established between network participants. Individual connections are combined by participants to establish routing of payments to six degrees of separation.
- GEO automatically detects and resolves obligation cycles of up to six nodes, improving the resulting network liquidity.
- The protocol guarantees the full atomicity of complex transactions that involve multiple payment networks and assets.
- Transaction data in GEO is only stored by the nodes engaged in the respective transactions and, consequently, is distributed across the entire network. This approach enables high throughput, as well as accessibility for mobile devices.
- A transaction is executed by the local consensus of only the nodes that engage in the transaction.
- Because GEO is a high-level protocol in a multi-layered system, it allows atomic transfers of cryptocurrencies and tokens using blockchain technology, while simultaneously integrating payments in fiat and traditional asset equivalents. Trustlines (section 2.3) and state channels (section 2.4) provide low-level integrations for these systems.
- The protocol utilizes post-quantum cryptography for digital signatures, ensuring its sustainability in the long term.

GEO is an open and accessible solution that will connect industry participants, an adoption process similar to base Internet protocols. The protocol allows large players and individuals to interact with each other, gaining access to all the services available in the network. This ability greatly contributes to a network effect that increases the value of the network for all participants.

At the same time, GEO Protocol enables building from scratch a variety of decentralized applications and use cases, such as: payment systems, cross-chain decentralized exchanges (DEX), rating systems and loyalty programs, delegated democracy organizations, decentralized credit networks, clearing systems, and IoT solutions.

1.3 Related work

Several projects are aiming to build layer 2 solutions to increase blockchain scalability. They are often limited in scope: either trying to improve the capacity of a given network, such as Ethereum or Bitcoin, or providing inter-blockchain solutions that do not integrate with traditional assets.

This section provides an overview of related ideas, along with an analysis of GEO's differentiating factors.

Feature	GEO Protocol	Interledger	Lightning	Celer
Blockchain compatibility	Any ledger and registry (including real world)	Any ledger	Bitcoin and blockchains with the same hash function	Blockchain agnostic (focuses on Ethereum)
Channel types	Trustlines, state channels	Payment channels, trustlines	Payment channels	Generalized state channels
Atomicity	Full atomicity due to Observer chain	HTLA	HTLC	HTLR
Topology and Routing	Distributed routing processing. Each node knows its first level only	Routing is done by Connectors using routing tables	Each node has to have a global view of the network	Nodes only know their first level
Development stage	Beta	Beta	Beta	MVP

1.3.1 Interledger Protocol

Interledger Protocol[17] (ILP) is closest to GEO among all off-chain solutions in that it also provides integration between different payment networks, which may include both crypto and fiat payment rails. As explained below, ILP imposes strict roles on payment nodes, once again making a protocol level distinction between an end-point and intermediary nodes. Additionally, ILP does not provide atomic multipath transactions.

ILP implements secure payments through an arbitrary chain of connectors. The relationships between connectors can refer to mutual guarantees against a variety of ledgers and financial systems.

Topology collection and Routing algorithm
In ILP, similarly to IP/BGP [25], each connector in the network constructs its own routing table that indicates the next node to which a specific payment is to be send. Routing is performed by connectors only and requires them to store routing tables, which becomes an obstacle to scalability as the network grows.

In contrast, GEO Protocol processes transactions in a distributed fashion: each node only knows its first-level connections. Routing is limited to 6 hops (7 participants).

Atomicity
ILP uses HTLA [28] - hash time-lock agreement, which is essentially an HTLC [29] modification. If a cross-chain payment passes through a blockchain not supporting HTLC, the connectors (special ILP nodes that are responsible for routing) can replicate it using alternative methods, so that all contract provisions (e.g. payment time, amount, payment unlock conditions) are met. HTLA enables an agreement based on trust between participants, but all payments are divided into small parts, so that if one of the intermediaries steals the money, it will damage its reputation and will no longer be used by the participants of the network. This approach doesn't provide 100% atomicity, but is compatible with many systems, including those not using HTLC.

In GEO Protocol, there is full atomicity due to Observer chain (section 2.7 that provides assurances of payment finality. Observers in GEO Protocol are responsible for resolving conflicts in situations where a transaction counterparty or intermediary disconnects from the network or withholds critical data.

Multi-path payments
When there is not enough capacity to perform a payment through one direct path, GEO Protocol splits the transaction into several paths, all of which are part of the same atomically finalized process. This ensures increased maximum flow in the network. Before the actual payment starts, it is possible to predict the maximum volume that can be transferred between the sender and the recipient by considering all available paths.

For large payments, ILP uses an approach based on STREAM Protocol that splits larger transfers into smaller packets and sends them as quickly as the network can support [27]. This does not ensure atomicity for the whole payment, which limits the applicability of ILP in the real-world environment.

1.3.2 Lightning Network

Lightning Network[6] handles the routing of multi-hop payments on behalf of Bitcoin network users across a distributed network of nodes, secured using Hashed Time-Locked Contracts (HTLC) [29]. It uses a modified Dijkstra's algorithm [22] for finding the shortest paths between nodes in the graph and onion routing Sphinx[23] to securely and privately route HTLCs within the network.

The key differences between GEO Protocol and Lightning are:

- Lightning is built on top of Bitcoin, is dependent on the Bitcoin codebase and does not provide an inter-network transfer of assets.
- Lightning uses the gossip protocol to discover the network topology, requiring frequent updates for the nodes to have up-to-date routing information.
- Lightning uses HTLC, which may cause the loss of intermediary funds in case of network partition.
- Lightning supports only single-path transactions. Atomic multi-path transactions, which GEO Protocol supports out of the box, only exist as a form of proposal for Lightning[24].
- Geo Protocol has no transaction fees, while the Lightning Network requires transaction fees.

1.3.3 Celer Network

Celer Network[14] employs a generalized state-channel technology that aims to scale individual blockchain networks. Its main differentiating feature is the ability to scale smart contracts. Celer's routing algorithm is based on the Backpressure algorithm[9; 10], which aims to achieve high throughput instead of finding the shortest path (as most path-based projects do).

In contrast, GEO aims to provide interoperability between different cryptoasset networks, and is focused on payments and asset transfer. GEO enables non-blockchain assets as part of the same payment infrastructure and does not rely on on-chain features (such as the HTLR approach that Celer uses to provide atomicity).

2 GEO Protocol: components and participants

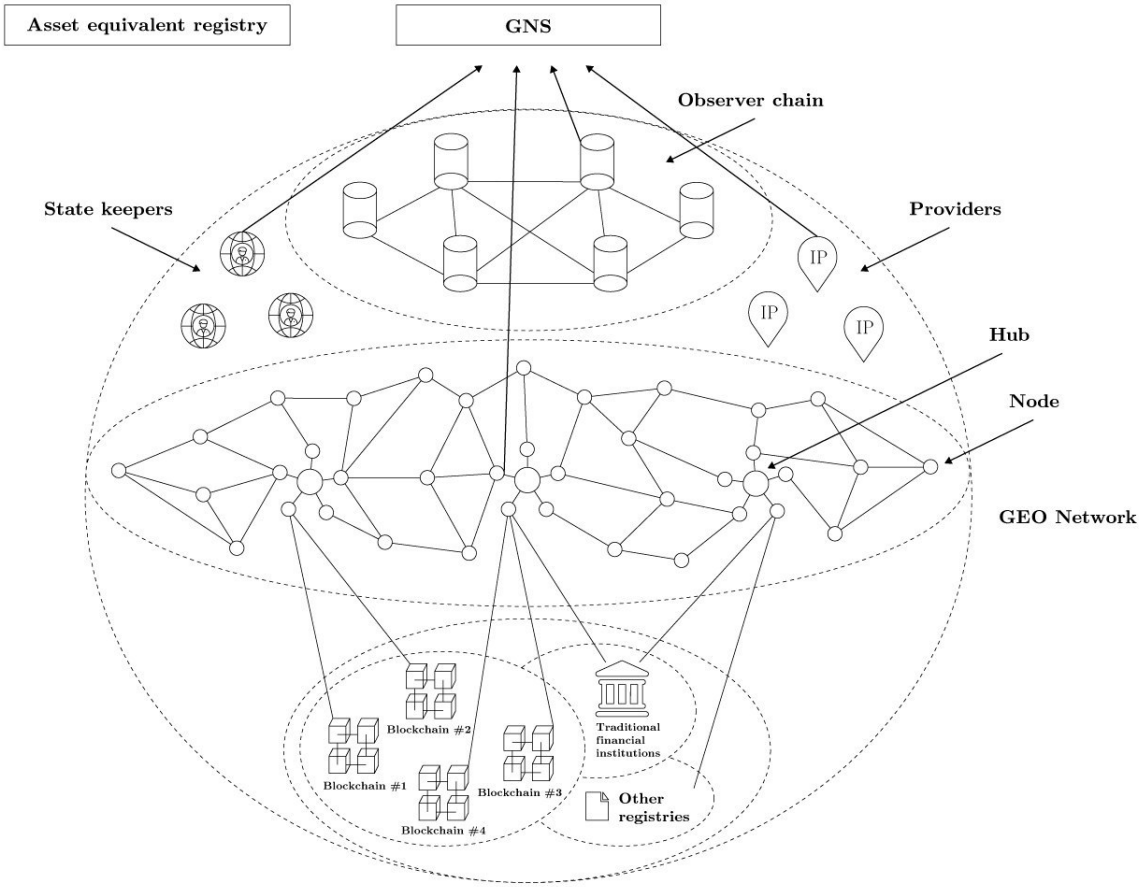

Figure 1: GEO Protocol

GEO Protocol forms a decentralized peer-to-peer network, GEO network (section 2.5) that allows members to transfer and exchange assets atomically. The protocol design addressed the limitations of existing distributed financial systems, including the scalability and throughput challenges of most existing systems.

In GEO Protocol, consensus is reached only between parties directly involved in the transaction. Consequently, nodes can be lightweight because they do not have to store information about unrelated parts of the network.

The GEO Protocol consists of a stack of components and service roles that enable routing, topology discovery, atomicity of transactions, asset exchange, and network connectivity for all financial nodes in the network. These roles are:

- Observers (section 2.7) receive and process requests from network participants to finalize the transactions that are delayed beyond the predefined deadline, either due to malicious behavior or network connectivity issues. Observers use a specialized blockchain system to record the final state of disputed transactions - Observer chain.
- IP providers (section 2.8) ensure the connectivity of mobile nodes, whose connections are expected to flicker and frequently change IP addresses.
- Hubs (section 2.9) improve the connectedness of the GEO financial network. Hubs launch GEO nodes and create a large number of connections to individual users. Hubs are not required by the protocol, but are optionally added to the network to improve the network's maximum flow capacity and connectedness.
- Market makers (section 2.10) provide liquidity to the GEO network by offering to exchange one GEO-based asset equivalent for another.

- State keepers (section 2.11) store the state of other nodes. This feature of the protocol allows users to delegate their nodes to another party that has a more reliable hardware deployment and network connection. State keepers are unable to send payments on behalf of the delegating user, but are able to route and receive payments.

Additionally, GEO Protocol requires use of information registries to store critical information about the network in a form that is accessible to all participants. These registries will initially utilize the Ethereum network for data storage.

- GEO Services Registry (GSR) (section 2.12) is an Ethereum smart contract that publicly lists all recommended GEO service providers – observers, IP providers, state keepers, hubs and market makers. As described below, to register in the GSR and to start receiving subscription fees from users, network service providers must stake GEO tokens to signal their reliability.
- Asset Equivalent Registry (section 2.2) is a public registry of available asset equivalents inside the GEO network. The list is updated by participants as new assets are listed.

2.1 Nodes

Nodes are the basic building blocks of the GEO network. They represent parties, end-points, and intermediaries to any financial transaction. Nodes access services provided by observers, IP providers, and market makers in order to route payments to each other. Nodes retain a history of only those transactions in which they were involved, along with information on their relationships with their peers. Behind the node could be an end customer, a machine, or a professional industry player.

2.2 Asset equivalents

Interactions between nodes are denominated in *asset equivalents*. Asset equivalents can represent differing asset classes or forms of value, including BTC, USD, and kilowatt-hour. Asset equivalents may be backed by (1) an external ledger, e.g. freezing a cryptoasset in a state channel, (2) legal agreements, e.g. a contract with a financial institution, or (3) interpersonal distributed trust.

Two nodes can interact in different asset equivalents simultaneously. Operating seamlessly across multiple assets allows GEO to form a network with high liquidity and to improve the interaction process between different systems (blockchain, off-chain networks, fiat, physical assets). For example, to perform a cross-border payment, the GEO network may route the sender's fiat payment to a party that will exchange it into a cryptocurrency, then route the cryptocurrency to someone in the recipient's country who will convert it to the local fiat currency, and, finally, route the fiat payment to the recipient.
All asset equivalents are registered in Ethereum-based Asset Equivalent Registry, which lists basic information about all assets with the GEO network.

2.3 Trustlines

A *trustline* is an accounting structure that represents the willingness of a participant to accept a limited amount of financial obligations (IOUs) from another member of the network. Trustlines are unidirectional, and the trust you give to a peer is not the same as the trust that peer gives you. Each such peer relationship also contains a balance that changes after each transaction.

To establish a new trustline, two nodes must complete the following steps:

- Create an end-to-end secured communication channel for P2P data transfers between participants
- One node must create an outgoing trustline
- The counterparty node must accept or reject the incoming trustline
- Nodes must set the trustline capacity (the maximum amount of value with which they trust each other)

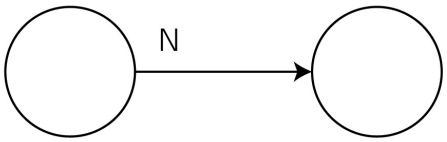

Figure 2: A unidirectional trustline

A unidirectional trustline establishes trust without reciprocation.

A bi-directional trustline represents trust in both directions. In cases when two nodes trust each other (not necessarily to the same amount), a bi-directional trustline (rather than two unidirectional trustlines) will be created by the protocol.

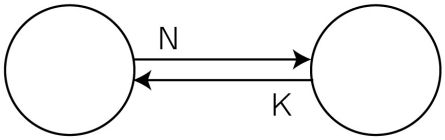

Figure 3: Bidirectional trustline

A single bi-directional trustline is more efficient then two unidirectional trustlines for the following reasons:

- Only one shared key pool is used
- Simpler accounting and audit logic
- Less space is used on the node's devices

Each operation on the trustline must be signed by both parties. Each operation has to utilize its own key pair; in order to process several operations, nodes must establish key pools. Depending on the node configuration, key pools might contain virtually any number of keys, from a few keys to several thousand.

If an error occurs, nodes enter an "audit state," during which they re-synchronize their balances, as well as their outgoing and incoming amounts. A node can open a trustline to its counterparty in any equivalent. The number of such trustlines is unlimited, provided each one is denominated in a different asset equivalent. It is not possible to open two trustlines to the same counterparty in the same asset equivalent, because that would significantly complicate the routing process.

2.4 State channels

State channels are a type of a financial connection between two parties in the GEO network. They use the trustline mechanism as a foundation, but operate on assets hosted by an external ledger, and mirror their balances to that ledger.

For example, let's say two members, Alice and Bob, want to pay each other in tokens hosted by some blockchain network. Alice and Bob do not trust each other; however, the tokens they use already exist and are serviced by the existing trustless network. The amount of tokens deposited by the participants into the state channel is the amount to which they can trust each other. By using state channel plug-in components to the GEO network, Alice and Bob are able

to transact directly in tokens. In this case, they utilize the trust they both have in the token's blockchain network.

The specifics of the interaction between Alice and Bob are as follows:

- Through GEO, Alice (side A) and Bob (side B) form a transaction to open a multi-signature address on the blockchain that hosts the tokens. The purpose of this operation is to atomically create an address that belongs to both A and B, and to which both parties can send funds. When the channel is closed, funds will be withdrawn from this address.
- After the channel is established, the parties create a bi-directional trustline in the GEO network that mirrors the state of the shared wallet. At the commit stage of a GEO transaction, the parties create and sign a transaction in a format that will be accepted by the host network. The transaction data contains the current balances and the transaction's sequence number.

Once Alice decides to close the channel and withdraw funds, her node exports the last transaction from the history of the trustline to the blockchain network. As a result, the blockchain starts the process of channel closure. The system then waits to withdraw funds from the shared wallet for a period of time that allows for a dispute to occur, with two possible outcomes:

- Cooperative closure — the parties mutually agree to close the channel. Alice sends her last transaction to the network. Bob waits for the closure request on the network, checks the balances of this transaction, and, if everything is correct, sends a transaction to the network confirming the cooperative closure. After that, funds from the shared wallet are sent to the parties' addresses indicated in the settlement transaction in the amount that reflects their final balances.
- In the event of non-cooperative closure, Bob finds that the balance specified in the closure request by Alice does not match the expected balance. This could happen if Alice had sent an outdated transaction to the network, possibly for fraudulent purposes. In this case, Bob sends his version of the last transaction to the blockchain. Having received two (or more) requests to close the channel, the blockchain contract chooses the request with the highest sequence number, and restarts the waiting procedure, this time allowing Alice to dispute Bob's view of the final state of the shared account.

2.5 GEO network

In GEO, nodes can transact even if they do not have direct connections to each other. This is achieved by routing payments through multiple peer-to-peer connections.

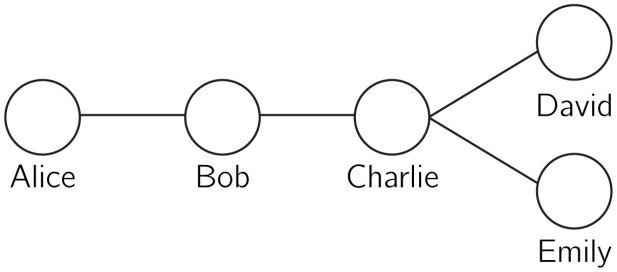

Figure 4: A multi-hop connection

For instance (fig. 4), Bob has connections to both Alice and Charlie. If Alice wants to send funds to Charlie, she will need Bob to assist with the transaction, since Alice does not have a direct connection to Charlie.

In order for nodes to transact in a multi-hop network, the protocol must solve the issue of availability and honesty of intermediary nodes, otherwise referred to as "the atomicity problem." Atomicity is ensured with the help of the observer nodes, and the specific protocol will be described in subsequent documents. A node with a large number of connections may become a hub (described in section 2.9).

This approach enables a variety of applications using assets and their equivalents. One example would be a decentralized exchange with fast cross-chain connectivity. If you need to use US dollars in a Chinese market that only accepts yuan, GEO Protocol will perform an exchange transparently and atomically. Similarly, if you receive electricity in watts, and pay for it in USD via a smart contract that represents a utility bill, the GEO network will route payments and perform exchanges as part of one transaction.

2.6 Transactions

Transactions in the GEO network can be carried out through chains of up to six peer-to-peer hops; i.e. there could be up to five intermediary nodes between the sender and recipient in any transaction. Simulation results have shown that, to conduct most transactions in a fully connected global networks, it is sufficient to use 3-6 hops between nodes. Where connectedness becomes an issue, hubs can fill in the gaps, enabling nodes to transact even in the absence of peer-to-peer trust between intermediaries.

Transactions can include multiple linear paths to increase the payment capacity without compromising atomicity.

A transaction is reflected as an eventually consistent change of balances on all peer-to-peer channels participating in the transaction.
Transactions can include multiple assets and their equivalents and take a few seconds to complete.

2.7 Observer chain

GEO Protocol must be resilient to the network connectivity fluctuations, which are especially common to mobile environments. Therefore, it must ensure that transactions can be completed, and that a transaction is recorded by all participants, despite any network problems. bservers guarantee atomicity of transactions, allowing participants to have a common view on whether a transaction has succeeded or not.

Observers are members of the GEO ecosystem that work on a separate protocol, participate in the consensus, record the information about disputed transactions, and resolve state conflicts.

The basic principles of the observer role and their operational requirements are:

- Observers act only when a transaction is delayed, or if there is a suspicion of a malicious actor attempting to prevent transactions from completing. Consequently, they do not possess any information about transactions that are successful.
- An appeal to an observer can be generated by any participant of a payment, at any time after the transaction has begun and before it has been completed. However, participants will seek help from an observer only when there are problems completing a given transaction.
- In order to prevent denial-of-service attacks on observers, users are required to purchase rights to use their services, which enable them to appeal in a certain number of disputes.

Any participant may become an observer. He or she must run a separate protocol, and register on the GSR in the observer list. If they receive a sufficient number of votes in the form of GEO tokens, they attain the authority to sign blocks in the Observer chain, audit disputes in the GEO network and mint Token Certificates (see section 3).

Observers are elected to the Observer chain based on a rating list in the GSR. Consensus of the Observer chain is achieved when a quorum of BFT - 2/3 + 1 nodes signs and validates a block. To use the observer service, a user must create an account there and buy a certificate (the native token of the Observer chain). It is expected that some decentralized applications that use GEO will perform this step on behalf of their users. Before utilizing it, the user must first activate the certificate.

2.8 IP providers

To transact, nodes need to find each other on the Internet. Specifically, the sender node needs to know the IP address of the recipient node, and of all the intermediary nodes. Currently, decentralized protocols and blockchain networks require nodes to have static IP addresses, which is a serious limitation because it prevents mobile users from joining blockchain ecosystems. In contrast, the GEO model supports dynamic IP addresses that may change several times a day.

In GEO, IP providers fulfill the need to maintain a current list of IP addresses for all active nodes in the network. (IP providers may be eliminated with broad adoption of IPv6, which natively ensures network dynamicity.) IP providers are listed in a separate table in the GSR.

Each user can choose an IP provider (or several) that will keep data about their IP address up to date, producing a global address system for the entire GEO network. For example, the GEO network user (Bob) is listed by the IP provider (Alice) under his own name – Bob. If another network user (Charlie) wants to send a payment to Bob, he only needs to know Bob's global name – alice.bob. If a user node wants to search for a recipient by their global address, it goes to the GSR first, where it finds the provider's IP address, and sends a request with the recipient's global name to the IP provider in order to receive the counterpart's IP address. Through this method, Charlie can easily find out Bob's current IP address and make a payment.

When a user chooses an IP provider, they needs to agree on the terms of their relationship. It is up to the provider to determine the amount of subscription fees users have to pay for this service.

2.9 Hubs

An important issue to resolve in a peer-to-peer multi-hop payment network is the potential lack of liquidity. For example, Alice may want to send $100 to Bob, but the capacity of the channels that connect them is limited to $90.

To solve this problem, GEO introduces a special kind of nodes called *hubs*. Hubs are network participants with many connections and a large amount of committed capital. At the protocol level, hubs are no different from other nodes, and any node may become a hub, given sufficient capital and visibility. However, in order to incentivize the creation of hubs, GEO provides them with the ability to charge users for routing payments. Hubs may register on the GSR, where token holders can signal their reliability by voting on their behalf.

2.10 Market makers

Market makers exchange assets and equivalents on behalf of others and route payments between different asset networks. Market makers are similar to hubs. The only difference is that a market maker has channels denominated in different asset equivalents. Like hubs, market makers may register in the GSR and charge fees for their services.

2.11 State keepers

While a GEO node can run on a mobile device, network traffic and computation dedicated to routing payments for someone else may deplete the device's battery and incur additional expenses with the mobile operator. Additionally, nodes must be online to receive payments, a guarantee that is impossible to provide with a mobile device. Consequently, mobile users may benefit from an active mirror of their node, both in order to be available to receive payments, and to reduce the ongoing expense of a mobile device.

State keepers are operators that take on the burden of running nodes on behalf of others, reducing their routing expenses, and making them able to receive payments even when offline. State keepers also serve as node backup services. Functionally, they are able to route and receive payments on behalf of the node owner, but do not possess the cryptographic key necessary to send payments.

State keepers register with the GSR and may charge a subscription fee for their service.

2.12 GEO Services Registry

The GSR is an Ethereum smart contract that lists all services available to GEO nodes: observers, state keepers, market makers, IP providers, and hubs. GSR ranks services based on

the number of GEO tokens staked and delegated to them. It provides users with the ability to choose the most reliable services and enables service providers to establish viable businesses on the GEO network. The mechanics of the GSR and staking are described in more detail in section 3.

3 Participant Incentivization

The token economics of the GEO Protocol is designed to be largely invisible to ordinary users (except token certificates, see below). GEO tokens are designed to be used by service providers as a way to signal their reliability and commitment to the ecosystem. They create economic incentives that drive quality and availability of services in the GEO network.

3.1 GEO Token

The GEO Token is implemented on the Ethereum blockchain as an ERC-20 smart contract in the total amount of 100,000,000 GEO tokens.

GEO Token holders can use their tokens to vote for service providers (observers, state keepers, and hubs) to increase their ratings. Service providers, in turn, may remunerate the voters (delegators) with a share of their compensation.

The most important function of the GSR is to establish the pool of observers. GEO Protocol aims at creating a group of 1024 observers to validate the Observer chain and to guarantee transaction atomicity for the rest of the network. Observers are different from other service providers in that they operate the Observer chain jointly, working as a group. Consequently, it is important that the entire group of observers be sufficiently compensated for their efforts, rather than allow users to establish individual financial relationships with one of them.
To create the right incentive structure in this case, GEO protocol uses token certificates described below.

3.2 Token Certificates (TC)

TC is the Observer chain native token with which GEO users can buy services from the observers. The total supply of the certificates is unlimited, and a certain quantity is issued once per week to all observers, who may then sell them to users. Initially, the issuance quantity is restricted to 10,000 TCs per week, but it can be modified by the vote of the observers.

Observers sell the issued TCs through marketplaces or individual agreements to users and application developers. Users and applications then use TC to buy services from observers when needed.

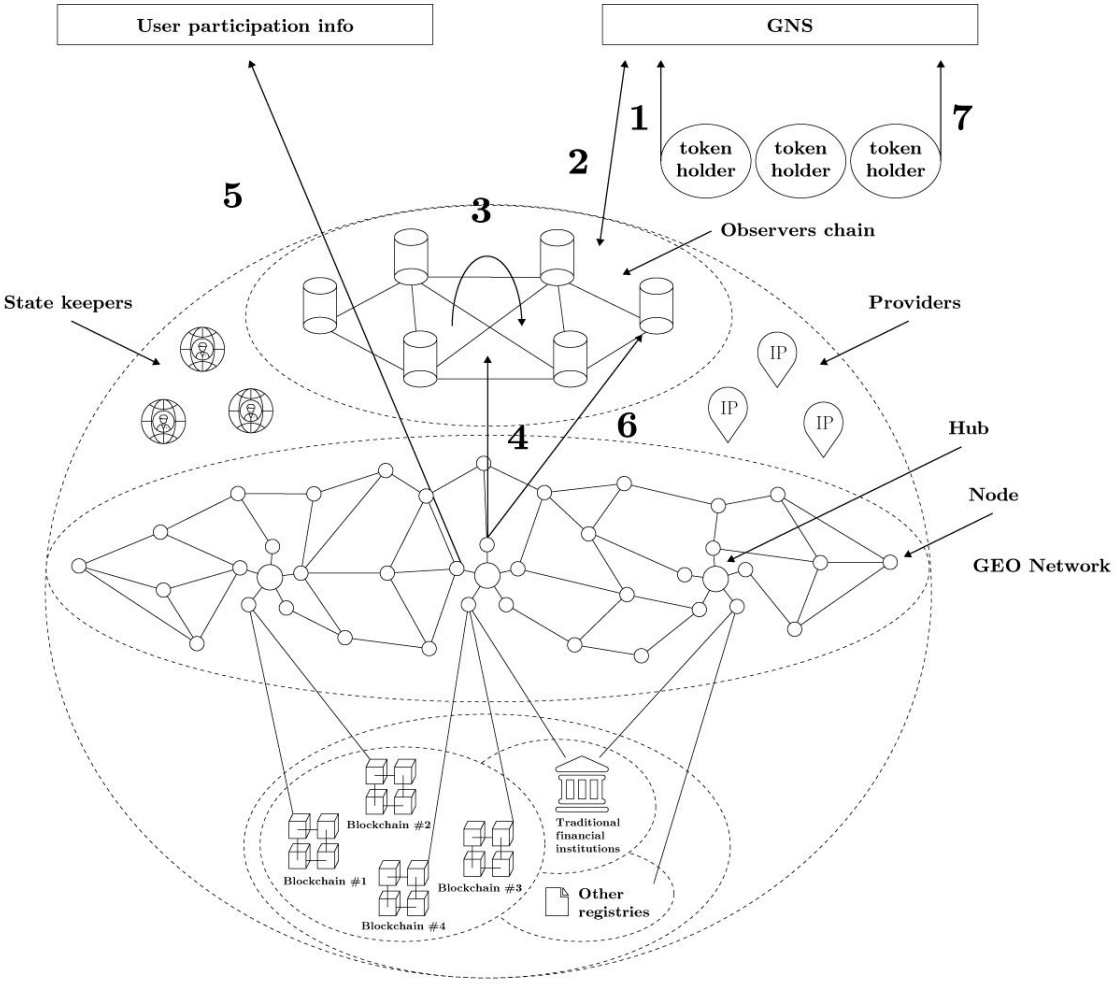

Figure 5: Token flow

Particpant roles within the ecosystem are shown in fig. 5:

1. Voting process: Token holders delegate GEO tokens to service providers
2. Based on the voting/delegation results, the pool of observers is formed
3. Audit of transactions and emission of token certificates by observers
4. GEO network nodes buy certificates
5. Users register their token certificates in order to use observer services
6. Appeal to the observers in case of suspicious transactions
7. Remuneration of the token holders/delegators by the service providers

4 Use Cases

4.1 Network effect

GEO's uniformity and ease of integration allow both large players and individual users to connect financially. This creates a network effect that with time will increase the value of the system for all participants. Importantly, this network effect is not based on one specific currency (experience shows that users are largely currency-agnostic and will pay with any means available), but rather on the connectivity and the accessibility of the network.

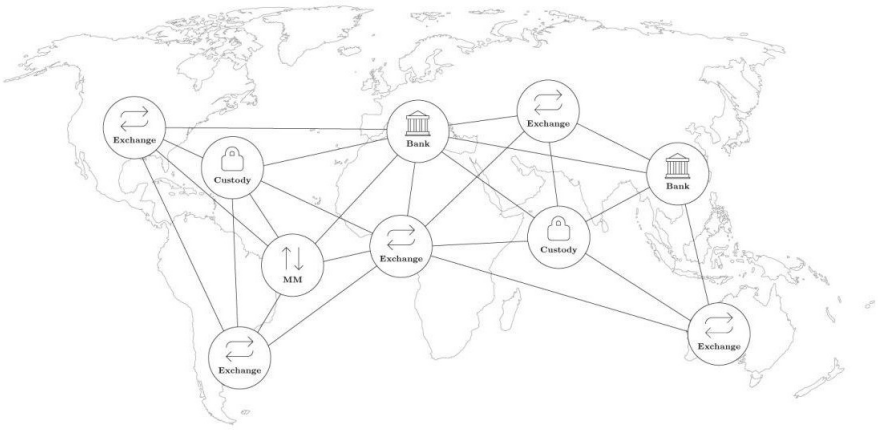

Figure 6: Network effect

As an example, below are the categories of services that benefit from the GEO network's connectedness and accessibility the most.

1. Exchanges, liquidity providers, stock and commodity markets
2. Custodians, banks
3. Blockchain networks
4. Wallets, mobile banking solutions, digital marketplaces
5. E-commerce businesses
6. Payment systems
7. Energy retail
8. Physical merchants

4.2 Exchanges

Current challenges for the cryptocurrency exchanges are:

- Low market liquidity
- Engineering complexity of integrating new blockchain assets
- Limitations on use of fiat currencies
- Difficulty attracting new users

GEO delivers solutions to these challenges:

1. As a network with shared global liquidity, GEO enables financial interaction between exchanges and other network participants, including transfer of fiat currency equivalent.
2. Multi-asset support: exchanges that integrate GEO protocol receive access to any blockchain asset available in the network.

3. Fiat infrastructure: financial institutions and custodian services that join the GEO network provide the ability to interact with multiple fiat currencies
4. Arbitrage opportunity: fast and secure multi-asset transactions make arbitrage possible across all exchanges available in the network

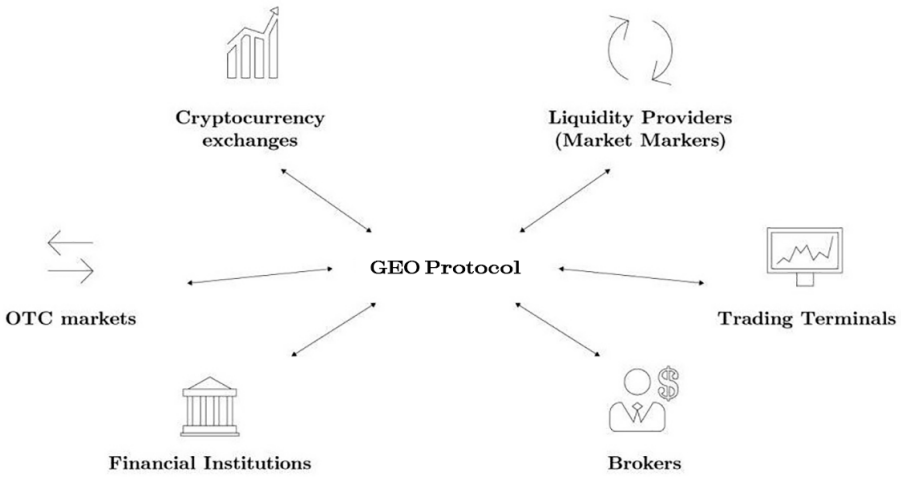

Figure 7: Global Liquidity Pool

4.3 Payment systems

GEO protocol enables low-fee payments globally, using any currency. The advantages of using GEO Protocol for payments include:

- Implementation of low-fee and open-source payment processing system
- Local data storage leads to a steep reduction in operational costs
- High transaction throughput, without an increase in resource consumption
- Operations are executed and accounted directly on user devices
- Complex international payments
- Micro-transactions and high-frequency transactions.

4.3.1 Internet of Things

GEO Protocol can be implemented as a payment protocol for the energy markets. It can also enable an IoT-based payment infrastructure globally. It brings:

- Security and privacy. Because all data is stored locally by participating nodes, it is impossible to observe data for the entire network, even in case of a hack.
- Streaming payments are time-based payments that are useful when consuming a resource in real time. For example, streaming payments are used to make frequent small payments for energy or network bandwidth.

4.4 Local currencies

In recent years, local currencies have become popular in regions that want to stimulate their economic activity. There are many successful examples of local currencies in the real world (WIR [30], Sardex [31]). GEO can provide for the needs of such economies at a minimal cost.

Any region, enterprise or community can create its own value equivalent, and freely exchange and transfer it using GEO Protocol, which also provides a simple accounting and clearing service.

5 Disclaimer and risk factors

Please see the Disclaimer [32] and Risk Factors [33] description.

References

1 Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer. On scaling decentralized blockchains. In FC, 2016.

2 Stefanie Roos, Pedro Moreno-Sanchez, Aniket Kate, Ian Goldberg. Settling Payments Fast and Private: Efficient Decentralized Routing for Path-Based Transactions. https://arxiv.org/pdf/1709.05748.pdf

3 Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf

4 Andrew Miller, Iddo Bentov, Ranjit Kumaresan, and Patrick McCorry. "Sprites: Payment Channels that Go Faster than Lightning". http://arxiv.org/abs/ 1702.05812.

5 Jeff Coleman. State channels. https://www.jeffcoleman.ca/state-channels/

6 Joseph Poon and Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, 2016. https://lightning.network/lightning-network-paper. pdf.

7 Patrick McCorry, Surya Bakshi, Iddo Bentov, Andrew Miller, and Sarah Meiklejohn. "Pisa: Arbitration Outsourcing for State Channels". In: IACR Cryptology ePrint Archive 2018. https: //eprint.iacr.org/2018/582.

8 P. F. Tsuchiya. The Landmark Hierarchy: A New Hierarchy for Routing in Very Large Networks. In SIGCOMM, 1988. http://www.cs.cornell.edu/people/francis/p35-tsuchiya.pdf

9 M. J. Neely and R. Urgaonkar, "Optimal Backpressure Routing in Wireless Networks with Multi-Receiver Diversity," Ad Hoc Networks (Elsevier), vol. 7, no. 5, pp. 862-881, July 2009.

10 Tassiulas and A. Ephremides, "Stability Properties of Constrained Queueing Systems and Scheduling Policies for Maximum Throughput in Multihop Radio Networks, IEEE Transactions on Automatic Control, vol. 37, no. 12, pp. 1936-1948, Dec. 1992.

11 Stefan Dziembowski, Sebastian Faust, Kristina Hostakova. Foundations of state channel networks. https://eprint.iacr.org/2018/320

12 Vitalik Buterin. A next generation smart contract and decentralized application platform. https: //github.com/ethereum/wiki/wiki/White-Paper, 2013.

13 K. Croman et al., "On scaling decentralized blockchains", in International conference on financial cryptography and data security, 2016. https://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

14 Celer Network: Bring Internet Scale to Every Blockchain. https://www.celer.network/doc/CelerNetwork-Whitepaper.pdf

15 Castro, M., Liskov, B., et al. Practical byzantine fault tolerance. In OSDI (1999), vol. 99, pp. 173–186.

16 Christopher Copeland and Hongxia Zhong. Tangaroa: a byzantine fault tolerant raft. http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf, 2016.

17 Stefan Thomas and Evan Schwartz. A Protocol for Interledger Payments. https://interledger.org/interledger.pdf, 2015.

18 Ryan Fugger. Money as IOUs in Social Trust Networks & A Proposal for a Decentralized Currency Network Protocol, 2004. http://archive.ripple-project.org/decentralizedcurrency.pdf

19 Pavel Prihodko, Slava Zhigulin, Mykola Sahno, Aleksei Ostrovskiy, and Olaoluwa Osuntokun. Flare: An Approach to Routing in Lightning Network. https://bitfury.com/content/downloads/whitepaper_flare_an_approach_to_routing_in_lightning_network_7_7_2016.pdf

20 L. Lamport, Constructing digital signatures from a one-way function, Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.

21 Edmonds, Jack; Karp, Richard M. (1972). "Theoretical improvements in algorithmic efficiency for network flow problems". Journal of the ACM. Association for Computing Machinery. 19 (2): 248–264

22 E. W. Dijkstra. A note on two problems in connexion with graphs. Numerische Mathematik, 1:269–271, 1959

23 George Danezis, Ian Goldberg. Sphinx: A Compact and Provably Secure Mix Format.

24 Olaoluwa Osuntokun. AMP: Atomic Multi-Path Payments over Lightning. https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-February/000993.html

25 A Border Gateway Protocol 4 (BGP-4). Y. Rekhter, T.J. Watson Research Center, IBM Corp., T. Li, cisco Systems, March 1995. https://tools.ietf.org/html/rfc1771

26 Lamport, L., Shostak, R., Pease, M. (1982). "The Byzantine Generals Problem". ACM Transactions on Programming Languages and Systems. 4 (3): 382–401.

27 STREAM: A Multiplexed Money and Data Transport for ILP. https://interledger.org/rfcs/0029-stream/

28 Hashed-Timelock Agreements (HTLAs). https://interledger.org/rfcs/0022-hashed-timelock-agreements/

29 Hash Time Locked Contracts. https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts

30 Official website of the WIR Bank. https://www.wir.ch/

31 Official website of Sardex. Bank https://www.sardex.net/

32 GEO Protocol Disclaimer.
https://geoprotocol.io/docs/GEOProtocolDisclaimer.pdf

33 GEO Protocol Risk Factors. https://geoprotocol.io/docs/GEOProtocolRiskFactors.pdf