GEO protocol

Max Demyan Dima Chizhevsky

August 30, 2018

Abstract

This document describes GEO – a protocol for highly efficient decentralized processing of peer-to-peer payments in a distributed network of nodes not based on a common ledger or consensus process. GEO can both serve as a highly efficient trustless payment network layer for existing blockchain systems, and facilitate payments in fiat or other non-blockchain-based units of exchange through a network of distributed trust. By emphasizing routing features, cross-unit exchange, and transaction atomicity, GEO enables efficient inter-blockchain exchange of value. It also provides a unique mechanism for on-boarding users onto the cryptofinance ecosystem. Because the GEO network does not make use of specialized hubs for routing, even your smartphone can act as a miniature payment processing node, making large intermediaries entirely unnecessary. GEO is blockchain agnostic and integration with a large number of blockchain networks is trivial.

Contents

1 Introduction

The fundamental need in payment processing is ensuring against the possibility of an actor misrepresenting their holdings to others and ultimately spending money they don't have. The three known ways to prevent participants from making false claims of payments (also known as *the doublespend problem*) are: using a trusted intermediary to hold a database that at all times expresses the global truth (this is the *trust-based* model); using a byzantine fault tolerant consensus protocol, such as that used by the Bitcoin cryptocurrency (this is the *trustless* model); and, finally, using a distributed loan accounting mechanism, such as that used in the historical Hawala payment network in the Middle East (this is the *distributed-trust* model). Only the trustless and the distributed-trust models could be said to enable peer-to-peer payments.

The era of digital 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 possesses less than 51% of the network's hash rate to prevent users from sending or receiving payments.

On the flip-side, the trustless approach to P2P payments has a number of drawbacks, fully described elsewhere in the cryptocurrency literature. To summarize: it is computationally expensive and wasteful, it cannot operate on lightweight and mobile devices, it gives rise to highly volatile asset prices, it is often slow, and, finally, it requires secure key-management – a big hurdle to broad adoption.

The GEO protocol delivers an alternative based on the distributed-trust model of peer-to-peer payments, but when applied to blockchain-based cryptoassets it becomes a fully-trustless system for payments, based on the innovation of blockchain layer 2 networks.

1.1 Market overwiew

We live in the world where technologies have already reached the level which is sufficient for sending funds (money) easily and safely - as easily as sending a message, even between smartphones.

Nevertheless, the existing infrastructure adapts very slowly to the new digital landscape. At present, the financial world is mostly built on trusted intermediaries who account for assets and ensure the transactions processing. However, those intermediaries are very poorly synchronized between themselves (sometimes there are even manual operations still present), there are no universal standards of interaction, etc. The highlights characterizing the current state:

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

- Monopolization of the payment processing market. Monopolies and the closed-source software limit the interaction between the market players and consumers. The lack of open-source processing technologies is a deterrent for innovations in the sector. It is possible to create a great mobile application but many financial institutions will not be able to use it simultaneously;

- Extreme overregulation of the system plus multiple international restrictions;

- Uneven development of the infrastructure.

While, for instance, the share of online payments in the UK already nears 50%, 2 billion people in the world have not even got a smartphone yet; The emergence of trustless technologies of accounting for assets and payments allowed performing protected transactions without intermediaries. Due to the absence of the regulation, geographical restrictions and a high availability level, the use of this technology grows actively, and has, in fact, led to the creation of the whole new economical and technological ecosystem that we call the crypto industry.

At the same time, despite really new technical possibilities of digitizing and trustless transfers of assets, the parameters of the known technologies of distributed registries are objectively insufficient to serve such financial sectors as, for example, retail payments, the exchanges, national currencies etc. Moreover, each 'crypto asset' exists, for all that, as a closed-source system due to the lack of standards and the difference in technological approaches. In this sense, the crypto industry is even less flexible for the synchronization then the other world's financial elements.

So, at the moment, going beyond is connected with high costs, wait times or is impossible at all though one can send an asset relatively easily within a country or a blockchain registry. At the moment, our team is working on a concept that exactly fits the following description: *We are not followers of a certain crypto-asset or technology. On the contrary, our goal is to create a flexible infrastructure protocol that connects different ideas and ledgers, including centralized ones. We believe that only an open and equally accessible solution will connect all industry participants evolutionarily (as it happened with HTTP or SMTP).*

The key features of the protocol:

- It is off-chain protocol — there is no general ledger, and the interaction occurs through the chain of channels. Productivity and scaling are limited mostly by the speed of one's internet connection.
- Multi-asset — support for an unlimited number of values of any kind (including created centrally). The protocol allows operations to be performed quickly and safely and with different assets. Operations include but not limited to:
  - transfers
  - decentralized currency exchange
  - off-chain smart contracts (complex multi-asset transactions)
- Flexibility — the infrastructure and terms of interaction are built and determined by the network participants themselves, same as with the Internet.
- Liquidity in the network — the ability to simultaneously use state channels, IOU, hubs and so on.

Due to its architecture, the GEO protocol enables users to build an infrastructure for various applications and solutions, such as payment applications and their integration, decentralized currency exchange services, services for voting and loyalty programs, credit and clearing systems, interaction between different blockchains, IoT solutions (communications and data exchange between devices and appliances), etc.

Despite these barriers, the construction of the infrastructure of the Internet of Value, sufficient for mass adoption, is possible. However, it requires solving several important challenges. At the very least, we need:

- Competition in the sphere of DLT
- Flexible and interoperable off-chain atomic protocols (or several compatible ones) which include:
  - unlimited scalability;
  - productivity comparable to common processing technologies;
  - speed.
- IoT devices accessible to the masses by price and type (including smartphones)
- Decentralized cross-chain identification or compatibility

1.2 Background and motivation

The idea of establishing a platform that enables participants to create different assets and exchange them appeared in 2013 and was a result of researches in the sphere of economy, human evolution and monetary policy. That is a result of such fundamental reasons as decreasing the

effectiveness of centralized decision-making systems and the imperfection of the contemporary financial world.

In 2014 our team was inspired by blockchain technology and started seeing into the existing challenges. The Ripple project [8; 22] was the closest from the ideological point of view, but the project had limited censorship resistance and functionality. While looking into DLT more closely we faced a wide range of constraints: limitation of productivity and scalability, transactions cost and time etc. Furthermore every existing DLT project was focused on itself and is not interoperable with other ledgers.

Thus, in 2015 our team decided to build a protocol corresponding to the following criteria:

- availability (accessible by the majority of potential users);
- scalability;
- productivity (consistent with traditional processing technologies);
- multi-equivalence (possibility of creating an equivalent for every participant);
- transaction speed appropriate for retail payments (is about several seconds)

After 2 years of research and testing we created the basic GEO protocol stack enabling a decentralized distributed network that:

- has no common ledger;
- any device can be a node, including a smartphone (expenses for energy and traffic being minimal);
- transactions are executed by a local consensus of nodes participating in these particular transactions;
- has no fees;
- boasts near unlimited productivity and scalability;
- enables transaction rates of only a few seconds (depends on network topology);
- enables nodes to form channels simultaneously in any asset.
- transactions are executed over channel chains .

At the time these channels were called 'Trustlines' since they perform the function of accepting IoU from other nodes (not backed by any crypto asset).

Since the technology is new, we have created a mobile application with protocols implementation for demonstration purposes.

Meanwhile, by the year 2017-2018 the crypto industry gradually came to the conclusion that blockchain technology with a number of independent participants had a range of functional limitations. In order to solve blockchain problems of scalability and transaction costs, plenty of projects that use state channels [15; 28] technology appeared, starting with the Lightning Network [6]. By analyzing existing projects, we came to the conclusion that state channels solve only some limitations. The following problems still exist:

- liquidity inside a state channel network;
- compatibility of different blockchain projects.

1.3 Related works

Lightning network

The most famous implementation of the state channel is the Lightning Network [6], which was recently launched on mainnet. The network handles the routing of multi-hop payments across a distributed network of nodes, secured using the hashed time-locked contracts (HTLCs) approach. It uses modified Dijkstra's algorithm [31] (it is an algorithm for finding the shortest paths between nodes in a graph, which may represent, for example, road networks) and onion

routing Sphinx [32] to securely, and privately route HTLC's within the network. By itself, HTLC is an atomicity solution for Lightning. The key differences between Lightning and GEO Protocol are:

1. Lightning is built on top of Bitcoin and can be implemented only by blockchains with same hash function as Bitcoin has. GEO Protocol is able to connect different ledgers and to exchange different kind of assets.

2. In terms of topology collection method, GEO nodes need only to know their first level of relations, unlike in Lightning, gossip protocol is implemented, that requires to store more topology information and refresh it. This may lead to network overload and scalability issue.

3. Atomicity is also reached in different ways. Lightning uses HTLC that may cause a lost of intermediary funds in the case of disconnecting from the network. GEO Protocol relying on observers - network participants with a separate protocol that provide fully atomicity payments.

4. GEO Protocol supports atomic multi-path payments, and Lightning Network in its turn, doesn't support this type of operations. There is only a proposal [33] how to maintain them.

5. Also, there are no transaction fees when using GEO Protocol, but in Lightning Network transaction fees are required.

Interledger

Interledger Protocol (ILP) [21] has proposed a protocol for secure interledger payments across an arbitrary chain of ledgers and connectors. Each particular payment is routed through chain of connectors, that can use different types of relations for this purpose, to reach the final destination - receiver.

ILP routing is similar to BGP routing. It's being performed by special nodes - connectors(they could be run either by a person or by a large enterprise and they may act as a DEX). Each connector has its own routing table where path and next hop are determined These tables are created when a new connector is added based on the tables that belong to other connectors or can be configured manually. When a packet is received, the connector sends the packet further based on its table and using the Longest prefix match rule.

Interledger uses HTLA - hash time-lock agreement - is an agreement that based on trust between participants, but all payments divide into small parts, so if one of intermediaries stole the money then he will lose a reputation. GEO Protocol supports full atomicity due to Observers Chain - a private blockchain with BFT consensus that provide payment finality.

Preliminarily, ILP had the atomic mode that provides atomicity for payment chains in which the participants can agree upon a group of notaries. However, due to the concept complexity of the implementation in a cross chain environment, as well as the fact that users would have to trust notaries, this concept was not implemented yet.

Celer Network

Celer Network [18] constructs generalized state channels technology that aims to scale different blockchains. The main difference is the ability to scale smart-contracts. Celer is based on Backpressure algorithm [10; 11] that is aimed to achieve high throughput instead of finding the shortest path like most path-based projects. In a nutshell, it works is as follows: each node in each point of time calculates congestion of its first level. During the calculation, transactions queue and channel imbalance are taken into account. When a calculation is completed, node sends a transaction to a node with the lowest congestion. This process repeats until a node reaches receiver node or its first level (in this case congestions of receiver believe to be 0).

The key difference between GEO Protocol and Celer Network lies in the mission of the projects. Celer Network aims to scale every blockchain, but the goal of GEO is to make different assets transfer as easy as possible and to connect different ledgers. Another difference lies in the way of atomicity achieving. Celer uses HTLR (hash time lock registry) that is the extension for PM [34] (Preimage manager) - something like an arbitrator for the HTLC that would allow delegating the function of taking decisions regarding the expiration of the lock contract period from each individual node to the central registry, and thus avoiding the problem where one of the payment participants loses money when being offline.

In the HTLR, there are 2 dependency endpoints - IsFinalized, QueryResult. The first one returns whether a preimage has been registered before the block number, the second one returns whether a preimage has been registered. Potentially, these 2 functions can be united into one. It should be noted that the HTLR is always on-chain.

Related research

Also, there are few papers that are developing routing algorithms for distributed networks.

Landmark routing [9] was proposed as one of the options for decentralized payment routing in several payment channels. The key idea of Landmark routing is the definition of the shortest path from the sender to the receiver through an intermediate node called Landmark - usually a well-known node with high connectivity.

SpeedyMurmurs [2] complements the previous shortest path routing algorithms by accounting for the available balances in each payment channel. For routing in the protocol is used embedding prefix tree - node coordinates tree, in which coordinates are assigned in the form of vectors, starting with an empty vector at the landmark/root. Each internal node of the spanning tree enumerates its children and appends the enumeration index of a child to its coordinate to obtain the child coordinate. The distance between two such coordinates corresponds to the length of the shortest path in the spanning tree between them. When changing the network topology (especially when removing nodes), there are often situations when one needs to update information on a large part of the nodes (update the prefix tree). Also, this approach is very sensitive to malicious modification of the prefix tree and the generation of duplicate coordinates (there must be a central register of already issued coordinates to solve this problem).

Flare [26] is a routing algorithm that was proposed for Lightning network by the team ACINQ. It also aims to find the shortest path, but uses totally new approach. Node constructs its own routing tables where it can find a path to first (second or even more) level nodes. When two nodes have to make transaction between each other, they exchange their tables and search for intersections. If there are no such intersections they can use another routing tables using special nodes - beacons (it can be any basic node that agreed to be a beacon for a particular user). Process repeats until path is found.

All the proposed solutions have made a significant contribution to the development of the entire industry and specific directions as well. Nevertheless, the mentioned constraints such as atomicity gaps, topology collection ineffectiveness and, interoperability issues are crucial and relevant for rapid market evolving.

2 GEO Protocol

The GEO Protocol provides ability to implement a decentralized peer-to-peer network that allows its members to do atomic assets transfers including exchange of different types of assets. While designing the basic principles of the protocol, we addressed the limitations of existing distributed systems, including most blockchain-based systems, and their scalability and transaction throughput challenges.

Single ledger systems are suitable for accounting assets, due to the nature of their consensus models and, as a consequence, – strong persistence against various byzantine attacks. But, from the other hand, most of them are trade-offs between security of the assets and transactions throughput and scalability, which makes them a doubtful choice for dynamic exchanges, microtransactions, and for building decentralized applications on top of them.

In the GEO Protocol, consensus is reached only between the parties who are directly involved in the transaction. At the same time, they do not have information about the state of the rest of the network. There is no common ledger for the assets that present in the network, as well as the general source of information about the network itself.

It is possible to use two types of channels in the GEO network at this moment:

- *Trust Lines* – channels between two parties in the network, that provide ability for simple and fast assets transfers, but which are not connected to any external ledger and, as a result, are not related to any external environment.
- *State Channels* – channels between two parties in the network, that use trust lines as its basis but are also related to external ledger, and are mirroring their balances to it.

Both types of channels might be used by any pair of participants of the network simultaneously and for processing various types of assets.

The GEO Protocol allows to build a decentralized peer-to-peer network that allows parties to exchange different types of assets. While developing the basic principles of the GEO Protocol, we addressed the limitations of existing distributed systems, including a single ledger-related systems. This kind of solutions are suitable for storing assets, but neither for dynamic exchange, microtransactions, nor for decentralized applications. In the GEO Protocol consensus is reached only between the parties that are directly involved in a transaction. At the same time they do not have information about the status of the whole network and about processes affecting other network members. Now in the GEO network it is possible to use two types of channels simultaneously - state channels and trust lines; in the future it is possible to develop new interconnection concepts.

Due to the state channels (which are part of the protocol), one can bypass the existing limitations like scalability and operability. The structure of most modern ledgers allows one to implement state channels on top of them and make most of the calculations off-chain. The main idea of GEO Protocol is not to attach to one blockchain, but to allow users to have multiple channels between two nodes in different assets. The advantage of using state channels is obvious - the security of assets storing is delegated to the blockchain, and routing, payments processing and the rest of operations are made in the channels. In this case, only nodes that are directly involved in operation are used.

However, taking advantage of distributed technologies, we do not want to ignore the existing financial solutions of the real world. Therefore, an important approach of GEO Protocol is the transfer of financial relationships to decentralized realities through the use of *trust lines*. Trust line is the implementation of widely used promissory notes in the world, also known as *"IOU"*. This solution, taking advantage of distributed systems, allows creating a multi-equivalent credit network without a central issuer. Users form such a network independently with the help of their existing real-life relations.

We have combined two technologies. Thus, GEO Protocol combines the flexibility of real financial relations (digitizing the selective trust of the real world) and the security of decentralized solutions in the environment of lack of trust. Thanks to this, we get a flexible and universal system in which the user is able to combine the solutions as he pleases. Therefore, GEO Protocol can be used in various areas described in Section 2.5.

We named this structure of the relationship between nodes "composite channels". This name fully reflects its multi-component nature, taking into account different types of channels,

equivalents and assets. Advantages of this system are following:

- almost instantaneous consensus limited only by the speed of data transfer between all participants, involved in the transaction, as well as the slowest participants' computation ability;
- secure assets transfer using post-quantum cryptography without imposing additional restrictions on users;
- transactions without fees: each participants' device spends only its computing power;
- high availability of the system: any modern device can be a node, from an average smartphone and up to a high-performance cluster;
- multicurrency: users can simultaneously use any assets and equivalents of these assets, as well as freely exchange them, which is a default functionality of the network.

2.1 GEO ecosystem

2.1.1 Roles and key components

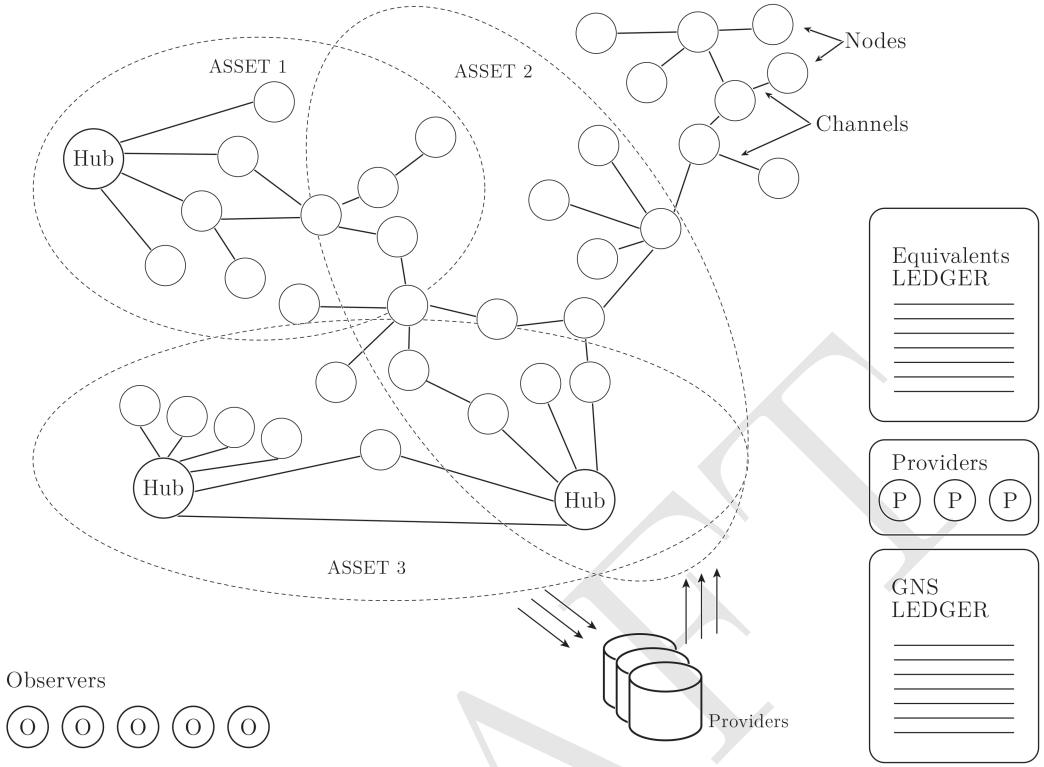

Figure 1: Key roles interaction in GEO Protocol

Basic components

1. **A node,** or a network node, is a participant in a peer-to-peer network. A node interacts with other participants in the Geo Protocol, installed on a specific hardware device (allowed to create copies on several other nodes). A device may even be a smartphone.

2. **A channel** is two-way communication between two nodes. A channel is an agreement to automatically perform a transaction on demand in the future, in a specific equivalent and quantity. Peculiarities:

   - is set in a specific equivalent and a measure unit
   - there could be an unlimited number of channels between two nodes (in different equivalents)
   - channels are trusted, unidirectional by default
   - the channel may be a state channel, i.e. with an appropriate reserve of crypto assets in multi-sig
   - the channel is initiated by one node, and received by another

3. **GNS register** is the register of cross-accounts with identification, information about the provider and additional data for custom solutions. It is a kind of virtual passport for the Geo network nodes.

   - records are stored in a separate ledger (Testnet on Ethereum)
   - minimal information required is: ID / user identifier / provider
   - entries in the register may be created by Providers only
   - custom solutions are possible
   - the ability to provide selective access to individual values

- the ability to delegate records to specific values: ID / user identifier / provider/ custom information
- the ability to supplement the "virtual personality" with custom information (for example, private key on BTC, identity number, medical records, etc.)

Roles:

1. Participants - the basic role allowing equitable interaction with the network within the protocol. Each participant must activate the node to use the network. A participant may:
   - Create or delete a channel
   - generate transactions
   - participate in the implementation of other transactions (automatically)
   - assume any other role in the system
2. Hubs are nodes with a large number of first level links. Their main function is logistics: they provide greater connectivity and network capacity. The hub can receive a reward for its services.
3. Observers - a separate protocol that protects the network from a certain type of attack. It is not necessary to be a node in order to be an observer on the GEO network.
4. GNS Provider – a separate protocol. The provider stores the IP addresses table for the Geo network nodes. Due to this, information routing between the participants is ensured.
5. State keeper - a separate protocol. Allows the nodes of the GEO network to delegate the state of their open connections. A state keeper can sign transactions for the node, and also ensure that the channels are closed correctly while the node is offline. At the same time, it cannot intercept funds. This service protects the network from some attacks and ensures its greater reliability and availability.

Events:

1. Transaction
   - can only be done through channels
   - can be split into several paths
   - a 100% local consensus is established between all participants in the transaction
   - is reflected as a simultaneous change of balances on all channels participating in the transaction (there may be situations where some nodes commit the transaction later: dropouts, network failures, etc.)
   - transactions can be in one equivalent, or cross-equivalent
   - duration is only several seconds, double-spending is impossible
2. Clearing (closing cycles) - automatic netting (within the protocol) of accumulated balances in a closed chain. After the cycle is found, a process similar to the transaction is initiated
3. Creating (or deleting) a channel
   - can be created only by the node-initiator
   - an exchange of crypto-signatures for future changes in the balance through the channel is necessary
4. Creating an equivalent (for example creating GEO BTC or GEO LTC which are equal to BTC or LTC)
   - list of equivalents on a separate contract for Ethereum
   - everyone can create an equivalent
5. Recording into GNS Registry
   - entry into the register is made by the providers only according to the contract
   - can be initiated by either users or applications

2.1.2 GNS

Geo Name Service (GNS) is an independent decentralized participant identification system designed to serve the financial infrastructure of the Geo protocol. GNS has the following tasks:

- keeping a register of participants, their identification data, as well as their pseudo-addresses in financial services and services, the benefits of which are used by a (specific) participant;
- routing requests between GEO network members from "gray" areas of the Internet. This aspect of the system is important for the GEO network as a whole, since it allows one to create and maintain a direct connection between Internet participants without having a static ("white") address;
- providing the necessary identification data to the services on behalf of and by agreement with network participants (authentication in various services);
- excessive backup of the participants' data of the GEO network to prevent irreversible loss of credentials.

Identification of participants is provided by a separate independent protocol. This solution allows nodes of GEO network to be involved simultaneously in payment and other systems with different interaction logic.

Basic mechanics

GNS is a structured cumulative distributed decentralized register, providing high-level access to the GEO network infrastructure and consisting of three main subsystems:

- an identification system that generates and distributes unique identifiers for members of the Geo network. It can also be used to map the identity of the GEO network to the identity of other systems (Bitcoin, Ethereum, etc.). The main area of responsibility of this subsystem is the deduplication of the IDs of the GEO network members in the public registry;
- a high-speed distributed register of public IP addresses that processes real-time requests of network participants and allows direct (p2p) connection of GEO network participants from "gray" Internet areas (for this purpose we use NAT, a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device). The main area of responsibility of this subsystem is the exchange of IP addresses between the participants in real time;
- IP routers. The role of distributed routers on the network comes to hold a "key-value" table in the following format: "Participant Subzone: Current Public IP Address and NAT back port."

Each service provider maintains this table independently through its infrastructure in order to provide direct access to GEO Protocol participants who have chosen this provider as a representative in the public Internet segment.

Entities

- Node / GEO Node is a participant of the Geo network; It needs real IP addresses of other nodes in the network. It uses its Provider for fetching IP addresses of known members via their GNS names.
- Provider is high-level service, working in public Internet, provides names resolution for the Nodes in the network by request. Each Provider maintains its own high-throughput map (Name -¿ IP Address).
- GNS Blockchain is the public ledger that contains high-level GNS entries.

Architecture

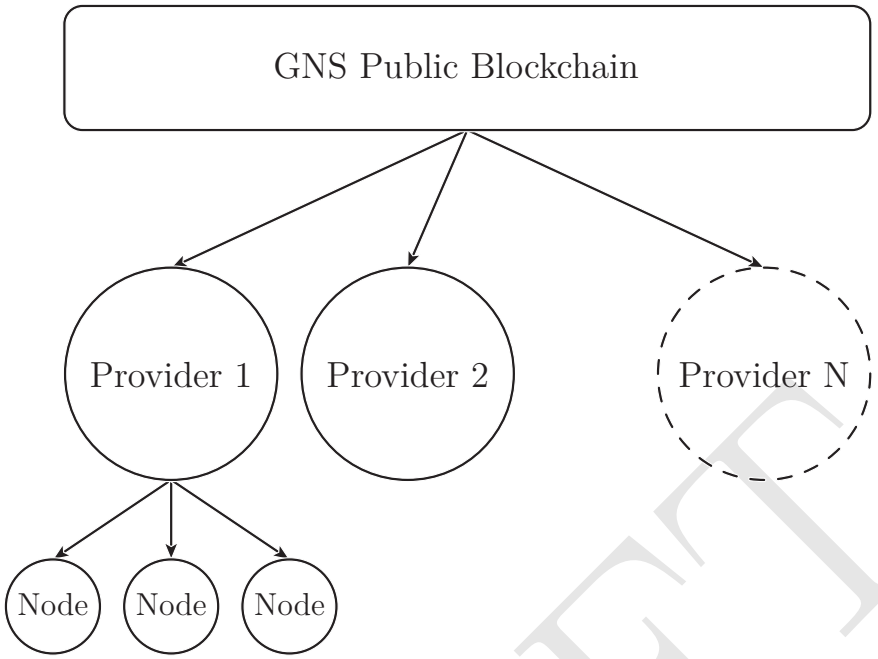

Figure 2: Architecture of GEO Protocol

2.1.3 Providers

Each GEO Node knows its internal Provider alias and pings it from time to time to update its global IP address in internal Provider's database and to bypass the possible NAT. Provider caches Node's global IP addresses for some time and shows it to the other Nodes by request. Once cached, each IP address would be probed from time to time by the Provider to keep the connection alive. If remote node doesn't responds to the ping then connection would be considered as obsolete and would be removed from the cache.

This addressing technique is needed to provide NAT-agnostic addressing for IPv4 networks. IP Address discovering flow:

- Node knows it's contractor's global alias or provider-specific alias and sends discovering request to its provider. Optionally, the request might contain a fields list, which should be returned. By default, the whole record would be returned back to the node in case of success.
- Provider looks in its internal aliases namespace and, in case alias is present there — returns whole record if no additional fields specifications are present in the request, or only a subset of fields.
- If no alias is present in provider-internal namespace — then Provider parses the requested alias and extracts global alias, goes into global addressing zone (blockchain) and looks for the specified record in it. In case of success Provider transfers the request to Providers behind it and waits for the response. In case of success retrieved record would be cached for some time and returned to the originating Node.

For the convenience of users, the Providers' services (storing the Node's IP address) can be paid directly through GNS. In this case, the user must specify the Provider and send him a payment. Users may not be registered in this system if their circle of relationships is limited, and find a local Provider that will also not be registered with GNS. But in this case an access to the rest of the network for them will be significantly limited, since other participants will not be able to find them on the Internet and convey the necessary information.

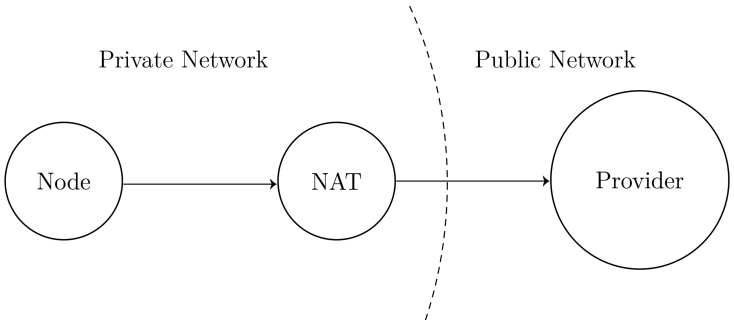

Figure 3: Providers arrangements

2.1.4 Observers

Since GEO Protocol considers usage of mobile phones working in mobile networks which much more often are subject of destructive network fluctuations than devices with a permanent Internet connection, the system should include solutions for leveling the situations of partial losses of network packets, their damage, etc. In this case, this kind of situation usually is not permanent and can be resolved at the level of the exchange protocol.

All payments can be conditionally divided into 2 categories:

- reversible by request nodes
- not reversible without a general agreement

The purpose of the issuing debt checks stage; their subsequent signing is the formation of a set of signatures of all participants in the transaction under an agreement to change their own balances in favor of the receiving party.

Difficulties arise in the event when part of the nodes issued their own debt checks, signed a general agreement on the transaction and transferred it to the payment coordinator, and then, due to destructive influence, did not receive a full set of signatures of the remaining participants in the transaction (the coordinator left the network or deliberately delayed the beginning of the operation). In this case nodes are in a state of uncertainty, because they cannot track the further fate of the operation and, therefore, cannot make a final decision about its completion. Also in order to avoid collision of funds, they are forced to keep reserves on their own lines of trust / channels until the clarity of the operation is ascertained. Theoretically, waiting may take a long time, and certainty may never come. This is a classic problem of protocols operating on the principle of a two-phase / three-phase commitment.

In this case, the attackers have the opportunity to compromise the network with the subsequent "freezing" of liquidity by initializing payments (i.e., assuming the role of coordinator) and delaying the beginning of the operation.

The idea of solving this problem is to provide the network with high availability points with the right to cancel operations initiated by other network members - Observers.

Observers are members of the GEO ecosystem, working on a separate protocol, participating in the search for or consensus building for operations, whose parties, because of destructive influence, could not reach consensus on their own. Observers have their own private blockchain, which is used to receive and process calls. Each Observer is chosen and paid by providers.

Principle of operation and role

- Appeal to the Observer occurs only in the event when there is a suspicion of unworthy behavior of other participants. Thus, Observers are deprived of any information about transactions which were completed successfully without their participation.
- Appeal to an Observer can be generated by any participant in the payment at any time after the start of a transaction and until it is completed, but it is assumed that participants will seek help from the observer only in the case of a problem situation. There are several events foreseen in the algorithm upon the occurrence of which an appeal to an Observer is inevitable. But at the same time this is a significant optimization: any potentially

problematic situation in achieving consensus can be reduced to a single solution that is predictable in terms of time and efficiency.

- Each appeal to an Observer must contain an operation identifier (unique ID) and a list of participants. Information about the amount of payment, purpose, payment topology (the ways in which the transaction is being performed), as well as who is the sender and who is the recipient is missing. Thus, Observers can collect very limited amout of information about ambiguous transactions.
- The Observer's role is to ask for a list of signatures from of all a transaction participants. Having received a request from the Observer, the participant can send him a package with signatures (i.e., signatures he collected from other participants during the transaction processing). In the case if the participant does not respond, his vote can be delegated to another participant of the operation. Thus, the Observer's goal is to collect a complete list of signatures of the transaction participants. If 100% of signatures are collected by an Observer, he should inform those participants who applied to him. In the case of a failure an Observer must repeat request attempts to the participants in a time span of up to 10 minutes from the moment of the first application for this operation. If 100% of signatures are not collected during this time span, the observer should generate a special reject packet informing all payment participants about the cancellation. The decision of the Observer is considered prevailing. After receiving a reject package signed by an Observer, participants can discard reserves, cancel an transaction and free up channel's liquidity for other transactions.

Thus, an Observer can cancel a transaction without the consent of all payment participants, but has no right to confirm the transaction without the will of all participants and, accordingly, does not affect the network node balances.

So the decision for each doubtful or problematic transaction can be made in a strictly defined time span.

2.1.5 Register of equivalents

Due to the register of equivalents, in the GEO Protocol system it is possible to create the equivalent of any asset for free exchange between protocol participants. The goal of creating multi-equivalence is to provide transactions liquidity and improve the processes of interaction between different systems. Equivalents are the context in which the relationship between two Nodes is expressed. Equivalent can be anything: USD, BTC, kWh of energy, time, etc.

Bitcoin	0001	First cryptocurrency
Ethereum	0002	Decentralized computer
USD	0003	Fiat dollar
Watt	0004	Energy
...	...	...
nameN	idN	short description

Addition mechanism

A list of equivalents is created in the blockchain (Ethereum). The name of the equivalent is added to the smart contract for this, the protocol refers to the registry, after which it becomes possible to freely exchange this equivalent. Anyone can add a new equivalent. Nodes freely decide in which equivalent and to whom to open the channel.

2.2 Types of interrelation channels

Geo Protocol allows one to create a distributed peer-to-peer network, supported by community members. Operations in the network are conducted by nodes - devices connected to the network on behalf of participating holders. A node in the network may act as a smartphone of one participant, and a whole datacenter of an organization that conducts tens of thousands of operations per second.

Assets in the network are transferred between the participants with the help of a sort of channel for the transfer of assets - trust lines. Trust line — is a digitally expressed willingness

of a participant to accept the obligations of another network member (IOU) without exceeding the confidence limit.

2.2.1 Trust lines

Geo Protocol allows one to create a distributed peer-to-peer network, supported by community members. Operations in the network are conducted by nodes - devices connected to the network on behalf of participating holders. A node in the network may act as a smartphone of one participant, and a whole datacenter of an organization that conducts tens of thousands of operations per second.

Assets in the network are transferred between the participants with the help of a special channel for the transfer of assets - trust lines. Trust line — is a digitally expressed willingness of a participant to accept the obligations of another network member (IOU) without exceeding the confidence limit.

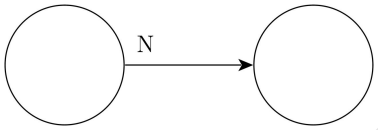

Figure 4: Single-sided scheme: trust lines (credit) for N units

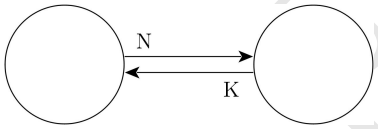

Figure 5: Two-sided scheme of trust line on N and K units respectively

Trust lines may be created both on the basis of personal social ties and on the basis of business relations. At its core, the trust line is a smart contract signed by both parties. At the moment there are only two conditions of interaction in the protocol - the equivalent and the limit, but in the future the number of conditions will be expanded, which will allow creating complex systems of interaction.

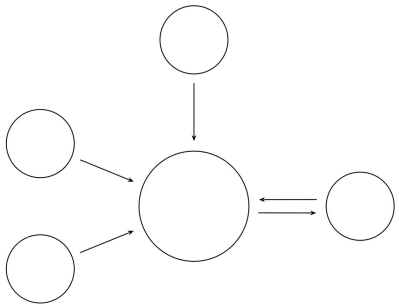

Figure 6: An example of a network topology that meets the needs of social relations

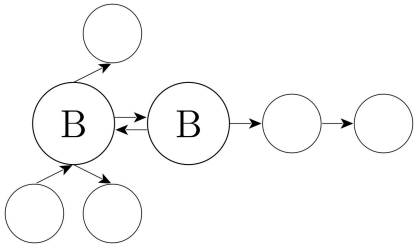

Figure 7: An example of a network topology, covering the business relationship

Transactions in the GEO network are the creation, modification and use of trust lines, as well as repayment of obligations arising from the use of trust lines.

Trust lines may be opened and changed (including closure) unilaterally without the consent of the counterparty. A Node may open a trust line to its counterparty in any equivalent. The number of such trust lines is unlimited, provided that each of the lines will be nominated in its equivalent: it will not be possible to open two trust lines by one counterparty in one equivalent because of the significant complication of the procedure for finding payment ways.

One of the main advantages of the system is that transactions may be performed by transferring (or paying off) obligations through a chain of links. Thus, each Node, while displaying business or social connections in the system, in fact is a part of a single logistics network for payments processing.

Direct interaction. In the simplest model of the network, the interaction occurs between those nodes that are directly connected to each other, i.e. are willing to accept an obligation for a certain amount.

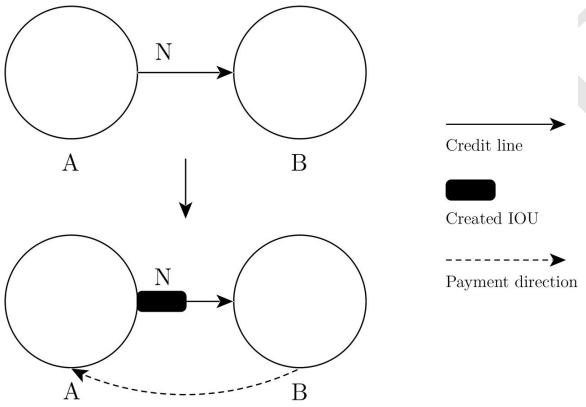

Figure 8: Example of payment transaction (before/after) from participant B to participant A

Indirect interaction. If there is no direct link between nodes, they may implement the transaction on the trust transitivity principle. In the GEO Protocol, a Node can send a payment to an unknown Node if it can be "paved" between them, i.e. build a chain of links through intermediate Nodes. The amount of available payment in this case (one payment path) will be equal to the smallest of the limits of the capacity of the path (chains of Nodes).

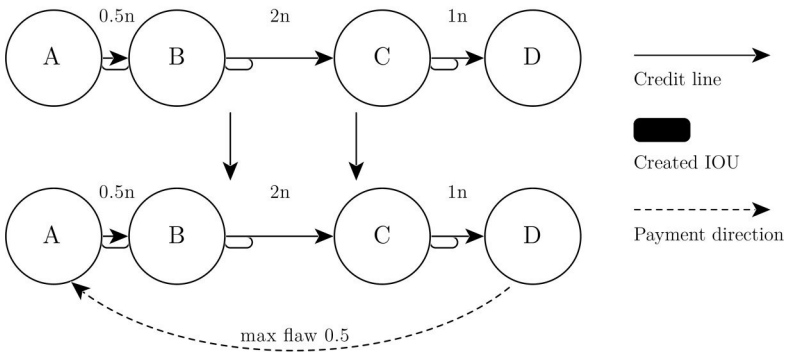

Figure 9: Example of payment transaction (before and after) from participant D to participant A, through B and C

Within one payment chain, both new obligations may be created and existing ones may be repaid. For example, if the next payment in the system passes through the chain A→D, A will be able to pay D 0.5n due to the existing obligations.

In the payment transaction, one to several hundred payment ways may be involved simultaneously with the automatic distribution of the payment amount for the selected routes.

At the same time, the growth of network connectivity leads to an increase in liquidity. The transaction paths are dynamically generated, during the initialization of payment.

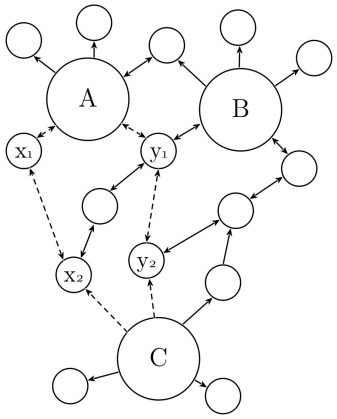

Figure 10: Formation of new payment paths through nodes X1, X2, Y1, Y2

Fees. The absence of a common ledger reduces the costs for the operation of the network. In the basic protocol there are no fees for transactions. Nevertheless, the third-party solutions that will be implemented by the GEO Protocol may establish their own rules based on such possible criteria as reputation, capital, risks, etc., depending on the goals of the derived projects.

2.2.2 State channels

This section describes how to build a universal network for off-chain-transaction processing, which allows implementation of a second level layer for the majority of existing blockchain systems, provided there some minimal integration improvements on the blockchain side.

Let's assume there are two members, Alice and Bob, who want to install a payment channel for exchanging tokens in some blockchain (token - TKN, blockchain). Alice and Bob do not trust each other. At the same time, the tokens that they want to exchange already exist and are serviced by a third-party decentralized solution (blockchain), so Alice and Bob want to exchange them, not their equivalents. To do this, Alice and Bob install the GEO node and the necessary extension for communication with the external blockchain that serves their token.

1. Through GEO Alice (side A) and Bob (side B) form a multisig transaction to open the multisig address in the blockchain. The purpose of this operation is to atomically create an address simultaneously belonging to both A and B, to send funds of the parties to it (not necessarily in a proportional amount), and to specify the addresses to which the funds will be withdrawn in the event of the closure of the channel.

2. Since the operation is created and signed by both parties, the situation when one party's funds are frozen in the channel while the other has not yet arrived is impossible, so additional temporary blocking of funds is not nessesary. Since the multisig address is derived from existing blockchain addresses, it is always possible to verify the validity of the signature of both parties in the transaction. The correctness of this operation is blockchain's responsibility. Creating a transaction through GEO allows parties to agree on an operation outside of the blockchain network, so they can send only one channel opening transaction to the network instead of two operations for opening and refilling the channel by each of the two parties.

3. After the channel establishment, the parties start exchanging assets in the GEO network. At the commit stage in GEO, the parties create and sign a transaction in a format suitable for export to the blockchain. Herewith the current state of the balances of the parties and the transaction sequential number (0 for the first transaction in the channel, N is subsequent, N tends to infinity) between them are fixed in the transaction. When exported to the network, any transaction of this kind triggers the mechanism for the channel closure.

- **Important:** Since the parties are fixing a state of a channel (the balances of the parties), they must conduct only one operation at one point in time. Otherwise, the integrity of history and balances can be violated, and the parties will have an opportunity of unfair behaviour in the network. This condition is checked by the module for the GEO protocol, which implements communication with the blockchain.
- **Important:** Since the GEO protocol implies the possibility of force canceling the operation (force rejection by an Observer), the signature of the state for the blockchain must be followed strictly after irreversibility of the operation is guaranteed.

Once one of the parties decides to close the channel, it exports the last transaction from the history to the blockchain network. As a result the blockchain starts the procedure of channel closure. In this case the funds are not transferred to the settlement addresses indicated in the settlement transaction instantly, but a waiting procedure of 500 blocks (or any other block interval equivalent to time sufficient for notifying the counterpart, since different blockchains have different conditions for finding blocks) is started, and so there are two possible outcomes:

1. *Cooperative Close* — the parties mutually agree to close the channel. The party that initiates the closure (assume it was side A) sends the last transaction to the network, the party that confirms the closure (side B) 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 closure of the channel (a separate type of operation for which only the signature of the response party is required). After that the funds from the multisig address will be sent to the addresses indicated in the settlement transaction, and the channel will be considered closed.

   Important: After the channel is closed, the parties can no longer carry out operations on the GEO network. The GEO protocol module, that communicates to the blockchain, is responsible for verifying this condition.

2. *Non-cooperative Close* — the party that must confirm the closure (side B) by receiving a channel closure request published in the blockchain network conducts a condition check and finds that the balance specified in this request does not match the expected balance (party A has sent to the network an outdated transaction, possibly for the purpose of fraud). In this case, the side B sends its version of the last transaction to the blockchain. Having received 2 (or more) requests to close the channel, the blockchain prefers the request an internal transaction number of which is larger (a sign of a newer operation), and restarts the waiting procedure from the receiving side (this time for side A). Thus, in case of suspicion of fraud, the parties may exchange transactions in the network with the hope that the blockchain will accept the transaction that is favorable for one them as the final one. But this is the finite process. First of all, it is expensive; also sooner or later, one of the parties will run out of signed operations with a higher number.

In the worst case scenario, the funds will be unlocked in the blockchain after 500 blocks. Important: In the proposed version there is no punishment for the participants of the network for sending outdated transactions. After all, the blockchain will always set the current balance of the parties based on the last published transaction confirmed by both parties.

Advantages of the state channels:

1. Universality. Extensions for different blockchains may use cryptography and solutions adopted in their ecosystem. The proposed solution does not impose a need for a common format for everyone.

2. Ease of implementation. The proposed solution requires the support of relatively simple primitives on the blockchain side. According to our observations, most modern blockchains can implement them through either a smart contract, or by customizing the internal logic.

2.2.3 Composite channels

Due to the tools available in the GEO Protocol, including trust lines and state channels that connect to any blockchain, each Node receives its own unique opportunities. Any pair

of Nodes on the network may create trust lines and state channels, and combine them. The variation of equivalents and the number of connected blockchains also allow users to conduct transactions in any of the available assets. Users can exchange a real assets frozen in a smart contract using state channels. By using trust lines or credit lines participants also have the opportunity to exchange non-secured equivalents.

Also users are not limited in the number of equivalents they can exchange. We call this multipurpose type of interaction "composite channels". Initially, the list of equivalents in the GEO Protocol will consist of several basic positions (USD, Bitcoin, Ethereum, etc.). However, any user of the system will be able to create new ones for a small fee (introduced in order to avoid the accumulation of spam positions in the register of equivalents).

Thanks to this feature, **users have a unique opportunity to build a composite channel infrastructure that combines the scalability of trust lines, trustlessness of the state channels and the possibility of using an unlimited number of various tokenized assets, as well as to create equivalents of non-tokenized assets.**

This complex system of the GEO Protocol will allow building of various applications for exchange of different assets and equivalents (like DEX with fast cross chain connectivity). For example, let's say you need to pay in dollars for chicken in the Chinese market, yet the seller only accepts yuan: Geo Protocol will solve this issue. Or on one channel you can receive electricity in watts, and on another you can pay for this electricity (the bill is a smart contract). All this is made possible by composite channels.

Advantages of the composite channels:

- flexibility that allows the use of different types of connections and also combines them
- cross chain interoperability - simultaneous operations with several assets
- scalability - one does not need to wait until a block is mined by each ledger, since all actions occur in channels.

3 Technical stack

3.1 Payment algorithm

In this section, we discuss the payment algorithm in detail. For simplicity, let's call the sending node the Coordinator, and the receiver node the Receiver. Let's imagine a network consisting of a Coordinator, a Receiver and several nodes. Using the algorithm for calculating payment opportunities, the Coordinator constructs three possible options for sending equivalents with limits of 200, 100, 300, respectively, for each single path. The total capacity of these paths is 600, however, in our hypothetical situation, the request was received for the transfer of 400 units.

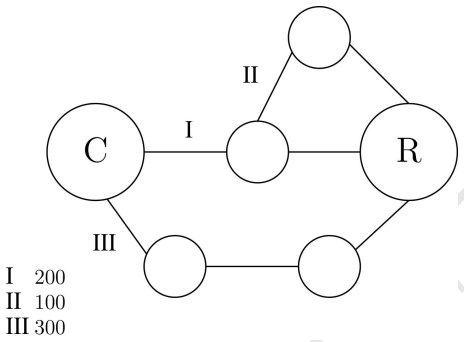

Figure 11: Three possible routes with different capacity

The algorithm is constructed so that, despite the amount of the payment request, the Coordinator still processes all possible paths. Thus, even if one or more nodes go offline, or the limits on the trust lines change on the way, the Coordinator could calculate new routes quickly.

After that the path processing begins. Routes are processed in order from a short to a long one. This order is chosen due to the fact that the fewer nodes are involved in the payment, the greater the probability of its success, because in a long routes chances of problems in one of the nodes are higher. The process is following:

In our case, the capacity of the shortest path is 200 units. The Coordinator reserves these 200 units on his side and, since the trust line mirrors the same data on two nodes that must be synchronous, he sends a request to the node at the other end of the line to make the same reservation. The reserve allows freezing the necessary part of the capacity of the trust line in order to secures it from possible impact of another transaction that may occur in the same time at the same trust line. After receiving the request, this node makes a reserve and answers the Coordinator. The first trust line of the path is considered to be processed. Then the Coordinator sends the same request to the next node down the route. That, in turn, also fulfills the reserve and reports to the Coordinator.

The process is repeated to the end of the route. After that, the route is considered to be processed, and the Coordinator notes that reserves on the first route are set.

The processing of the second path begins on the same principle. In our hypothetical case one of the nodes on this path has problems, so it cannot accept the request and make a reserve. In this case, the coordinator cancels this path, looks at all the paths that pass through this node, and deletes them.

The third route is treated similarly. Its capacity is 300. Since in this situation we need less, the coordinator will reserve only 200. So, the processing of the third path is completed. The coordinator sees that all the necessary reserves have been set, so now transfer of a certain amount of equivalent is possible.

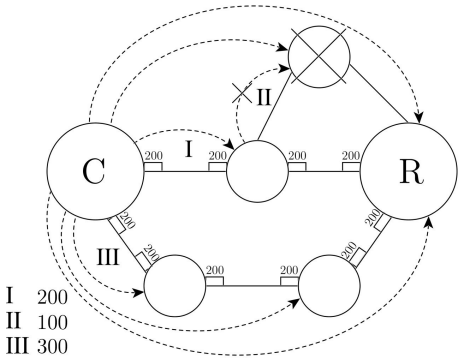

Figure 12: Route processing

At the final stage of the paying algorithm, each node, except problematic ones, receives a request with the final configurations (how much and with whom it should have reserves). The node, in turn, checks to see if its reserves meet this configuration, and if there are problems, signals that it is out. Also there is a list of all bidders in the request. This information is needed by the participants to exchange hashes of signatures for the transaction signing. Exchange occurs through hashes in order to save traffic, because the signature takes 80 kilobytes, whereas the hash takes only 256 bits.

Also, nodes are exchanging keys (all transactions on the trust line must have 2 keys: for the trust line and for the entire transaction). When a node receives all keys and all hashes, it passes its key, which will sign the entire transaction, to the Coordinator. When Coordinator collects all the keys, it sends out a complete list of nodes with signatures to all payment parties. After receiving this packet each node checks the presence of all participants from the previous stage, calculates the hashes of the signatures of participants and, if they coincide with those that it received at the previous stage, processes its reserve. Payment is completed.

3.2 Maximum payment possibilities calculation algorithm

Each node in GEO stores information only about those nodes it has trust line connections with. This allows solving the scalability problem and achieving high TPS of the network. In order to transfer funds between two nodes that are not connected with a trust line directly, and to calculate the maximum payment possibilities for such a transaction, the sender node needs to obtain network topology that allows it to perform such a calculations.

Let's consider the process of obtaining topology in more detail. Let's suppose that two nodes that are not directly connected to each other want to make a transaction. Both the Coordinator and the Receiver know only their first level connections only, that is, only those nodes they have direct trust line connections with. The Coordinator sends a request for a topology to the Receiver. The receiver sends a reply to the Coordinator about its first level and how much funds (amount) from each node it can receive. Amounts are calculated based on the information about incoming and outgoing trust, as well as current balance. The Receiver, in turn, sends requests to its first level connections, so they could also submit topology to their Coordinator. Those first level connections in turn send these requests to their first level, that is, to the second level in relation to the Receiver. This level is final. It receives request and sends information about its topology to the Coordinator. In total, the topology information is sent by the Receiver and its first and second level connections. A same thing happens with the first and second level connections of the Coordinator. So we have the topology of all 6 hops (the Coordinator, the first level of the Coordinator, the second level of the Coordinator, the Receiver, the first level of the Receiver, the second level of the Receiver). In other words, the Coordinator node collects information about its neighbors and neighboring neighbors, the Receiver node acts the same way, and sends its information to the Coordinator, thus forming a topological map.

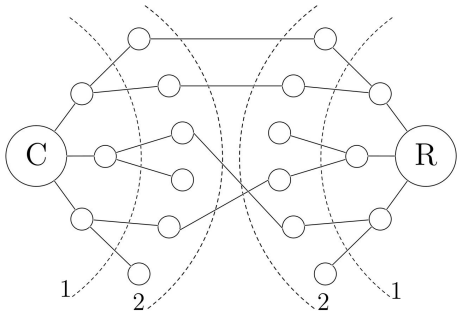

Figure 13: Coordinator, Receiver, their first and second levels

After that using the modified Edmonds-Karp algorithm [29; 30], the maximum flow is calculated. In terms of statistics, the average time to collect topology for a node with 10-20 trust lines is approximately 200 milliseconds, in some cases when the node has 200 trust lines, the time can take up to 1 second.

If the distance between the Coordinator and the Receiver is less than 6 nodes, one node may be the first level for the Coordinator and the second for the Receiver (or vice versa). This node will have to send information twice.

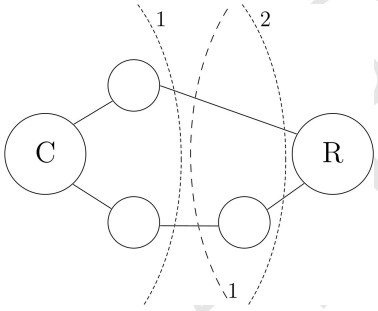

Figure 14: Overlapping Coordinator and Receiver levels

To avoid this, the nodes save the cache in the GEO network. The cache records information about which node and which data has already been sent. When a new query is received, a comparison is made and, if some data has already been sent, the node sends only the information in which the changes occurred (if there are any). After a certain period of time, the cache is deleted.

3.3 Routing algorithm

In the GEO network (just like in other projects related to state channels), communications have a logical nature: nodes which are linked via a trust line are not necessarily connected by a common physical data channel. Rather, the majority of network participants are expected to use the existing Internet topology (especially the 3G/4G network) for efficient routing of their own assets.

Problem associated with logical topology is, in particular, that it is much more prone to changes and reconfiguration than static networks. If we assume that the first level connections could be created/changed/deleted/recreated with a very little probability, then, with the increase of the remoteness level, the probability of such a change tends to 1.

Simply put, from the point of view of any network member, the connection at its 5-6th level of remoteness will be change relatively often, and its routing tables will become obsolete over time, which means that there is a need of an update mechanism. The social and economic nature of the network topology will contribute to the frequent changes in the topological tree, therefore, in addition to just updating the routing tables, the question of the time effectiveness of such a solution arises. Even if we hypothetically assume that routing tables may be placed in the memory of the end user devices, and that their updating takes up to one day (which is pretty time effective for the projected number of entries 150^6), then because of the changes frequency this process turns into a kind of "streaming of topology changes". There are 3 obvious shortcomings of this kind of solution:

- amount of traffic consumed
- the need to constantly keep large amount of irrelevant information (routing tables)
- permanent inconsistency of information from routing tables for nodes at remote levels

When faced wih similar tasks some systems opt to delegate computing power to third-party services, which entails the direct need for their financial motivation, so it definitely affects the network fee.

Geo Protocol aims to create a decentralized solution that maximizes usage of the network nature to create a map of possible payments, while ensuring the formation of the first data portions during the first few seconds after a transaction is initialized, raher then delegating computing power to third-party services.

Ability to predict the maximum flow

One of the decisive factors in decentralized credit networks is the ability to quickly predict the maximum payment flow between any pair of network nodes. The difficulty is that with the increase in the number of participants and operations on the network, the frequency of change in channel states increases proportionally. The operational complexity of predicting flows also increases exponentially, and in some cases quadratic, just like in the above described difficulties in routing.

At the same time, while it is possible to cache network topology for a relatively long period of time (for example, using the mentioned routing tables), the state of the channels is very difficult to cache because each cached value on one node leads to potential distortions of information about the payment flow on other nodes. In general, the nature of these distortions depends on a number of factors, such as the length of the cache, the way information is collected from the network, etc.

Proposed solution

The solution offered by the GEO Project aims to rethink the way of the maximum flow prediction and combine it with the suitable payment paths between participants finding process.

A high-level solution requires several important refinements:

1. The Coordinator and the Receiver can be mutually addressed at the level of the data network (the Internet in most cases): the Coordinator can send a data packet directly to the Receiver, and vice versa.

Algorithm

Next is a high-level description of the algorithm for predicting the flow and collecting payment paths. The above description is for informational purposes only (for more detailed description, see the technical description of the flow forecasting algorithm).

1. Coordinator analyzes its first level of channels for maximum possibility of sending funds to the network. If it equals 0, the operation is interrupted, because, in relation to any node, its maximum capacity is zero.

2. Coordinator sends a message to the Receiver inorming it about the beginning of the flow prediction operation. The Receiver performs a similar check for the maximum incoming flow on his side. If it is 0, the receiver tells the coordinator that the operation should be canceled, since none of the channels/trust lines can be used.

At this stage, the maximum flow limits can already be outlined: it cannot be greater than the sum of all outgoing flows on the Coordinator side, and at the same time it cannot be larger than the sum of all incoming streams on the side of the Receiver.

If both the Coordinator and the Receiver have a non-zero potential flow, they both begin to collect network data simultaneously. The sequence of operations performed is as follows:

1. Coordinator sends a message initiating flow prediction to the nodes that have channel/trust line with non-zero outgoing flow. This message is as short as possible (just a few bytes) and contains only the operation type, short identifier and address (or GNS record) for sending the return message.

2. Having received a request to predict the flow, each node produces a similar operation with its own first line of connections, except for the following cases:
   - The sender of the request does not get the answer.
   - The message includes information about the maximum flow at the current level, i.e. at the second level from the coordinator, appears the information on the maximum flow at the level of the coordinator $->$ the first circle. At the following levels, this indicator can be reduced according to the status of the trust/channel line.
   - The message includes information about the current message level (distance hop). Due to this parameter, it is possible to limit the maximum distance of the packet. According to the protocol, this package must pass only 3 hops.
3. The Receiver performs a similar set of actions with its first level of connections.
4. The purpose of the algorithm is to collect information about the capacity of the intermediate channels on the path from the Receiver and the Coordinator to their 3rd level of nodes. Nodes, which will be common to both Coordinator and Receiver, send the collected packet back to the Coordinator.
5. Gathering the network topology and capacity of the channels, Coordinator builds a topology and with the help of the modified Ford-Fulkerson algorithm predicts the maximum flow.

Thus, the Coordinator, as the initiator of payment, takes the greatest computing load, as well as higher load on the network and traffic. All intermediate nodes and the Receiver perform trivial actions and spend minimum of computing resources.

3.4 Cyclic clearing algorithm

For ease of understanding of the cyclic clearing algorithm, let's consider its operation principle in the following example. Let's suppose that we have three sides: Alice (side A), Bob (side B), Charlie (side C). In our anticipated situation, Alice owes 10 TKN to Bob, Bob owes 10 TKN to Charlie and Charlie owes 10 TKN to Alice.

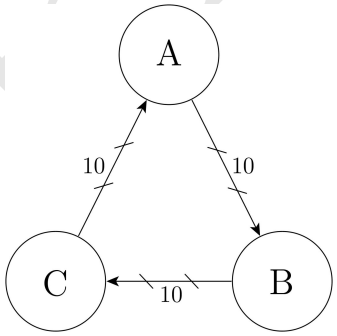

Figure 15: Debt securities Alice, Bob and Charlie

When each party pays their debt, the overall balance of the participants will not change. Accordingly, by accepting what no one owes to anyone or, in other words, completing the cycle, we can avoid the need for additional transfer of funds, thereby reducing the load on the network.

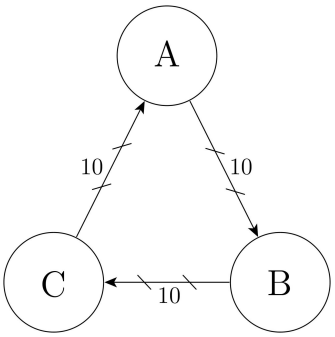

Figure 16: Closing all liabilities without changes in balances

The GEO system looks for these mutually settled cycles and debt obligations, and repays them automatically. The cycle itself is a simplified payment along one path, where the Coordinator and the Receiver is the same node. That is, payment occurs in a circle, writing off balances accumulated as a result of past actions of other nodes. Since GEO supports payments length of up to 6 hops, its cycles may be as long as 6, 5, 4 or 3 nodes.

Let's consider the process of the algorithm in more detail on the example of a cycle of 5-6 nodes. Since the node only knows its first level, first of all it is necessary to collect the topology. Suppose that the node opted to build the loops and then close them. In the first round of the node there are participants with positive balances (those who paid this node), and participants with negative balances (those who were paid by the node).

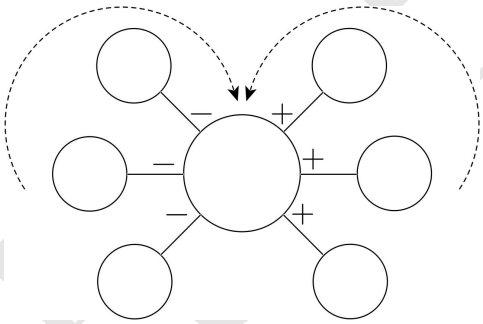

Figure 17: Node and its first level with negative and positive balances

The further course of action is as follows: the node sends requests to the participants of its first level with positive balances, asks them to collect all participants in their first level with positive balances, and sends similar requests to the participants of the first level with negative balances, and in turn, we would need to collect our first level participants with negative balances. As a result, each time the request goes further, a node, through which it passes, and the amount of payment are added to the packet (how many can go here). When these nodes return to the initiator node, it can build loops of 5 and 6 nodes, using these data. As a result of collecting such a topology, a large number of cycles are built, then they are transferred to the loop manager, which, in turn, tries to close each cycle separately. It closes them in turn, making corrections after the closure of one cycle regarding the following. This algorithm is run once a day, because there are not many cycles for 5 and 6 nodes.

The algorithm for 3 and 4 nodes is slightly different. It starts after each payment. If the node has transferred funds, potentially it has a promissory note. Now the node tries to build such cycles, when the payment goes the other way, to return the balance to the initial value. Node, knowing the participants of its first circle and participants of its participants, sends requests to these nodes for this so that they can answer whether it is possible to construct such a cycle through them. If the node gives a positive response, then the loop is considered possible, and it initiates a payment for one path with this.

3.5 Cryptography

The cryptography method is the Lamport signature [27] which is resistant against quantum computing, the digest of which is sufficiently optimal in size, which matches the network requirements regarding the amount of traffic used.

Current cryptanalysis of the Lamport signature reports some redundancy in relation to the brute force attack performed by quantum compuers. In turn, this leads to redundancy of the traffic used in each operation, protected by this signature. At the same time, in order to prevent a significant decrease in the crypto resistancy due to incomplete adherence to the classical algorithm, we decided to implement classical Lamport signature algorithm without weakening and decreasing the digests received. In order to save traffic, the Lamport signature protects only those operations that lead to a change in balances on trust lines. Operations on the exchange of service information are protected by more crypto-weak functions (SHA256), which is overall sufficient at the current technological level. A certain class of operations is not protected by cryptographic methods at all because of needlessness.

The pilot version of the protocol does not provide network participants with the ability to change cryptographic primitives, but it seems reasonable to give them the opportunity to independently choose cryptographic primitives that will be used for different kinds of counterparties. This will allow network members to make their own decisions on security issues and the traffic usage. At the same time, the standard version of the protocol will be released with certain cryptographic primitives set by default, which, according to the authors of GEO Protocol, are sufficient for the safe interaction of network participants for today's technological level.

The Lamport signature is one-off and should not be reused to confirm more than one operation, since with each additional operation the risk of compromising it increases. Therefore, the GEO Protocol introduced the mechanism for proactive signatures pre-generation at the time of the opening of the LD. By default, the number of pre-generated signatures is 1024, which allows us to confirm (or reject) 1024 direct or intermediary transactions on the network. Upon exhaustion of this limit or its approach to completion, the participants repeat signatures pre-generation (reinstall the context of trust). It is wise to conduct this procedure at the slightest suspicion of compromised data of one of the counterparties. Thus, the amount of data required to store information on one LD is about 1024 * (16kB + 8kB) = 24MB.

The GEO Protocol assumes that both counterparts mutually trust each other's public keys.

4 Participants incentivization

Token will be created using Ethereum smart-contract. The main purpose is to design an incentivizing system for effective coordination of protocol agents, i.e. (1) to tokenize Providers' services who are responsible for the network sustainability and protection and (2) to decentralize Observers who provide an atomicity of the network Records in ledger that contain information about network participants. It is used to identify members of the GEO network as well as to determine their roles. In addition, different operations with the GEO token happen here, such as user registration; paying for service functions; staking in order to obtain rights for providing these services; the vendor's valuation for their services. All entries to the ledger occur exclusively through Providers. Users registered in the ledger are serviced by Providers (in accordance with the reserved TIME). A ledger entry can be used as an identifier or a domain name. The user is the GEO node that buys the Providers' service time (TIME) for GEO tokens through GNS contract. Payments also can be made by application developers instead of their users. Each user can use one or more providers. They can make changes and provide additional information (within the limits of paid TIME). The user can refund TIME (except for the guarantee fee). Providers perform the basic service role. They are the nodes on the Ethereum blockchain through which participants of the ecosystem can make entries in the GNS ledger. Also, by default, providers supply the services of an observing and routing-provider in the GEO network (according to a separate protocol).

To become a Provider user needs:

- to create a stake of GEO tokens;
- to have a whitelisted static IP;
- protocol of the Provider.

Under the conditions above, the contract accepts a request to make a record to the GNS ledger of the new Provider. When creating / modifying new Provider, a candidate must transfer some amount of tokens to the GEO Foundation. When registering the Provider, its stake is frozen. Time could be reserved only through Providers. Guarantee fund is the amount of tokens that is frozen as security guarantees for users. It is calculated as the cost of the users' reserved TIME in tokens. In the case of provider's activity termination, reserve is given back to users. TIME means a period during which user can use GNS.

The service includes:

- creating / modifying a record;
- observing (security);
- IP routing support in a peer-to-peer network.

Custom offers for Providers:

- state guard;
- state keeping;
- backup.

TIME is sold by Providers for GEO tokens via the contract interface. The cost of recording is set by the market. Price in tokens is floating and is determined by each Provider independently (zero amount is rejected). The Provider may set own price for each additional services. Providers at the UI will be able to count the services themselves, passing only one number to GNS. The amount of the user's guarantee fee (a non-refundable amount) is also determined by Providers.

One can buy TIME for other users (for example, dAPP for its users). User can monitor the balance of the remaining service time for each provider. Users can refund their tokens (which they have paid for TIME), except for a guarantee fee. A provider can initiate a termination procedure. After that, all unused tokens are returned to users, and then the remaining amount of the provider's stake is returned too. Observers are nodes that provide security inside the network, looking out for suspicious transactions requests from nodes. Their motivation is to get profit from the provision of network support services. Observers work on a separate protocol and maintain a separate ledger of requests for transactions.

To become an Observer a user needs:

- to add a role to their entry in the GNS, as well as a proposal for the cost of providing the service. Observers assign the value of their services independently of each other;
- to have a whitelisted static IP;
- to maintain a separate request ledger (GEO service chain);
- to be chosen by the Providers.

The selection mechanics: Providers supply a list of Observers. After candidates are compared and selected judged by the number of votes received. Theoretically, voting can take place within each block, but in practice it occurs when one of the providers submits an updated list. The role of the Observer does not imply any contributions or fees. Observers receive reward from the Providers' stakes on each block.

Equivalents (Cross-Units) are used by network nodes when opening new channels as a list of contexts in which communication can occur on the network. Cross-Units are created on a separate Ether contract. Anyone can add a new Cross-Unit. To create one, you need to send tokens to the GEO Foundation.

5 Use Cases

The GEO protocol provides an infrastructure for applications of various types and purposes. Due to the design of the system, channels and trust lines may be used not only for payments, but also for useful computing, information exchange, voting, etc.

A. Payment solutions

Non-blockchain, fast, real-time, double-spending resistant, distributed multi-attendee payment crypto-protocol with time predictable 100% participants consensus. GEO protocol helps users safely send and receive payments in P2P marketplaces. It greatly enhances the buying/selling process with decentralized escrow for secure payments, third party dispute resolution, and very low transaction costs.

B. Interoperability protocol

The GEO protocol may act as a cross-chain protocol enabling interaction and interoperability among different blockchains. This makes instant payments across a network of participants easy and inexpensive.

C. Cross-chain DEX

The structure of the network allows the exchange of assets between two participants quickly and safely. The very process of exchange is similar to the technology of atomic swap. Therefore, it is expected that one of the first applications on the GEO Protocol will be a decentralized exchange.

D.Identity management

GNS, which is part of the GEO ecosystem, allows us to upload user information and delegate access to personal data in the GEO ecosystem. Thus it will be possible to create a digital passport.

E. Rating systems

The transitivity of trust reflects the amount of value that can be trusted to a node. It has a numeric measurement so the platform gives a tool to evaluate the rate or amount of trust, loyalty or support.

F. Clearing systems

Possibility to implement the automatic clearing with elimination of double expenditure.

G. IoT solutions

P2P protocol enabling the scalable, secure, private and highly trusted method to perform IoT transactions with participation of an unlimited number of nodes.

H. Mobile money operators transactions (protocol level)

P2P transaction protocol using SMS or any mobile app to perform transfer of funds. Nodes can be represented by phone numbers. The access to all online services is provided by duplication of node accounts to the cloud.

I. Mesh networks

Due to unique network architecture of the GEO Protocol it will be possible to create an infrastructure for mesh networks in the future.

J. dApp scaling solutions

The technology of state channels is actively developing, allowing more complicated operations to be carried out in the blockchain. In the future, many decentralized applications will carry out the main part of their calculations, which do not require the protection by entire blockchain, in such channels.

K. Loyalty programs

We are providing a platform for building loyalty programs and a developer interface, enabling customization of loyalty application for any need. Using GEO protocol, commercial brands will benefit from simple development and customization, low management costs and the elimination of liabilities associated with unredeemed items.

L. Delegated democracy

With the GEO Protocol we may create a voting system and a governance mechanism for decision making in the ecosystem. In addition, there is the possibility of anonymous delegation of votes in such a way that no one can know what power his voice really has.

M. Decentralized credit networks

The GEO Protocol allows us to implement a system of P2P lending, credit unions, and credit systems with guarantor . It is also possible to create a social and credit network - an alternative economic system built on social relations, which includes all the above elements of credit and payment networks.

6 Conclusion

In this work, we presented the GEO Protocol, a decentralized P2P network for fast and secure exchange of various data (financial and non-financial). It brings together existing financial systems and data registries .

The GEO Protocol implements the mechanics of multihop-transaction processing between several participants. By default, the GEO Protocol implies the consent of all participants to cooperate on the principle of debt obligations using the technology of trust lines.

In turn, it is also supplemented with components for implementing the logic of asset exchange in the absence of trust and/or the delegation of arbitrage to an external service through state channels - an offline scaling solution that allows implementing a second layer for most existing blockchain systems.

In order to make use of and eliminate the limitations of existing technologies, the GEO Protocol provides an opportunity to use composite channel infrastructure that combines the scalability of trust lines and trustless state channels, use an unlimited number of various tokenized assets and create equivalents of non-tokenized assets.

Due to its structure, the GEO protocol allows us to build an infrastructure for various public applications and solutions, such as: payment applications, voting services and loyalty programs, credit and clearing systems, interaction between different blockchains and IoT solutions. This takes you to the same place as [1] does.

7 References

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 Frederik Armknecht, Ghassan O Karame, Avikarsha Mandal, Franck Youssef, and Erik Zenner. Ripple: Overview and Outlook. In International Conference on Trust and Trustworthy Computing, 2015.

9 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

10 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.

11 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.

12 Raiden Network specification. https://raiden-network.readthedocs.io/en/stable/spec.html

13 Jeff Coleman, Liam Horne, and Li Xuanji. Counterfactual: Generalized State Channels. https://l4.ventures/papers/statechannels.pdf

14 Stefan Dziembowski, Lisa Eckey, Sebastian Faust, Daniel Malinowski. Perun: Virtual payment hubs over cryptographic currencies. https://eprint.iacr.org/2017/635

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

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

17 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

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

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

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

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

22 Schwartz, D., Youngs, N. and Britto, A. The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 2014.

23 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

24 Heiko Hees, Gustav Friis, Kristoffer Naerland Trustlines Network. https://trustlines.network /whitepaper_v03.pdf

25 K. Davis, R. O'Donnell. Kava Blockchain Overview. A scalable hybrid model of cross-chain decentralized liquidity provisioning, 2018. https://docsend.com/view/8mcbqrb

26 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

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

28 Bitcoin Wiki: Payment Channels, 2018. https://en.bitcoin.it/wiki/Payment channels

29 Edmonds–Karp algorithm. https://en.wikipedia.org/wiki/Edmonds–Karp_algorithm

30 Herbert S. Wilf. Algorithms and Complexity. http://www.cis.upenn.edu/ wilf/AlgComp3.html

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

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

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

34 A. Miller, I. Bentov, R. Kumaresan, and P. McCorry, Sprites: Payment channels that go faster than lightning, 2017. https://arxiv.org/pdf/1702.05812.pdf