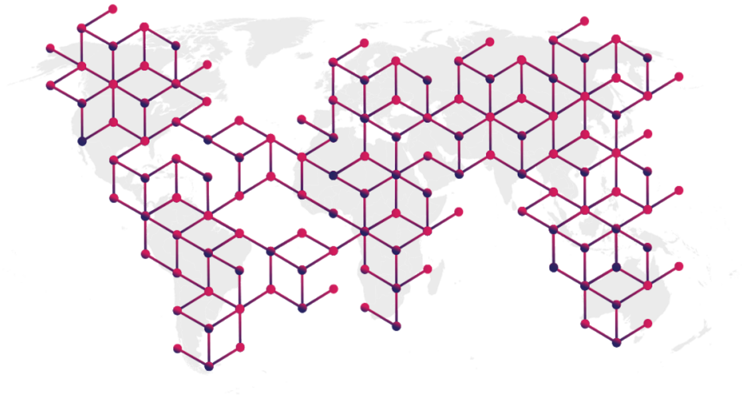
Mysterium Network Project

WHITEPAPER

Release 3



2017 May

Table of Contents

1. Motivation behind Mysterium 4

1.1. Mission Statement 4

1.2. Core Objectives 5

1.3. Mysterium Solution 5

1.4. Market driving forces 6

2. Token Mechanism 8

3. Platform layers 9

3.1. Decentralised Services Infrastructure and Databases Layers 10

3.2. Service Providers Layer 10

3.3. Service Clients Layer 10

4. Roadmap 10

4.1. Competitive Analysis 10

4.2. Funding Breakdown 11

4.2.1. Core Development – 40% 11

4.2.2. Operational – 25% 11

4.2.3. Marketing and Sales – 25% 11

4.2.4. Legal and Compliance – 10% 11

4.3. Development Roadmap 11

4.3.1. Phase I 11

4.3.2. Phase II 13

5. Token Creation Details 13

5.1. MYST Creation Ratios 14

5.2. Additional MYST 14

5.2.1. Future Funding 14

5.2.2. Founders, Foundation, Bounty program and Advisors 14

5.2.3. Seed Participants 14

5.2.4. Example of Token Structure after Creation is over 15

6. Mysterium Architecture 16

6.1. Technical Overview 16
6.1.1. Core components 17
6.2. Service Provisioning 17
6.3. Identity Service 17
6.3.1. Registered Identity Value 18
6.3.2. Cryptographic Mechanisms 19
6.4. Service Discovery 19
6.4.1. Outdated Service Announcement Handling 20
6.4.2. Service Proposal 20
6.4.3. Types of Services 21
6.4.4. Service Selection 21
6.5. Payments Handling 22
6.5.1. Accounts 22
6.5.2. Deposits 22
6.5.3. Issuing Promises 23
6.5.4. Clearing of Promises 23
6.5.5. Withdrawal 25
6.5.6. Risk Management 25
6.6. Messaging Between Nodes 26
6.6.1. Dialogues 26
6.6.2. Payment Scheme 27
6.6.3. Service sessions 29
7. Contact 31

Executive Summary

Privacy - most of us think as if it's a given fact of life, but behind the scenes there is a race going on with its participants secretly trying to get into as much of our private lives, as is possible.

Today, as Internet users, we are being restricted in ways we are allowed to use services and applications due to censorship employed by various agenda groups from all over the world. It comes to us in many forms.

Nation states consistently monitor the Internet traffic so they can construct political profiles of its citizens. In such a paradigm, dissent becomes dangerous, and honest political discord in some places - an impossibility.

In a similar manner, content and Internet Service Providers have become unhinged in their objective to monitor, track and profile every user across the Internet. The daily Internet activity, communications and habits of every user are consolidated and sold to advertisers and basically any willing buyers. Such transactions occur with little to no conscious consent of the users and with a complete disregard for any notion of personal privacy.

Access to content is being restricted by its content providers to certain areas due to Intellectual Property limitations or purely because of low valuation of users from these particular locations.

Today there is still a lack of investments into research, implementation and maintenance of tools capable of restoring privacy to the Internet users. These circumstances create the necessity for creation of protective measures designed to preserve the open and unobstructed nature of the Internet.

With the invention and maturity of powerful peer-to-peer computing technologies such as Ethereum and Bitcoin, the capability to employ blockchain technology in the development of trustless censorship evasion mechanisms becomes feasible.

Mysterium team believes in and strives to build a future that respects our privacy, which will result in disrupting existing and creating new industries in the near to long term. Looking forward, we expect Mysterium Network platform to form the basis for a world of open access to content and applications to all citizens of this planet without fear of censorship or of someone secretly looking over our shoulder.

1. Motivation behind Mysterium

1.1. Mission Statement

“Our mission is to create distributed, trustless and sustainable network - providing open access and privacy to all Internet users.”

The Internet in its current state is neither open nor private. At Mysterium we believe censorship and spying is both unethical and unnecessary, which are forms of intimidation and social control impeding technological and social progress.

It’s commonly believed that if you need encryption - you must be hiding something, assuming it’s something illegal. Here is a short list of 6 commonly used and very legitimate use cases where strong encryption is a proven solution:

1. travelers visiting places where their personal email & social media accounts are censored or blocked by the local authorities;

2. communications in your private life about your political, religious, gender / orientation, entertainment preferences that could result in discrimination or reprisals against you;

3. businesses needing privacy to avoid corporate espionage;

4. journalists communicating with whistleblowers, especially when the source is within the very government or corporation that controls the communication network being used;

5. dissidents and activists needing to organize meetings and protests without being spied on by the powers they plan to protest;

6. citizens, protesters and journalists needing to send reports on events about human rights violations to the outside world news agencies - as they occur. To request help or to inform the outside world, while being sure that the local powers that be will actively try to suppress all kinds of communication.

Thus we intend to develop the Mysterium Node Network, as an open and distributed peer to peer platform embedded with sustainable incentivization protocols, while using continuously evolving censorship evasion mechanisms, developed by the community. Once developed and released, Mysterium technology will enable anyone around the world to both: provide and receive access to content and privacy, removing censorship imposed by third parties.

We’ve spent a lot of time discussing the ethics of creating Mysterium tools which allow the avoidance of censorship. We believe the cost of censoring content is not worth the supposed benefits (assumed lower crime, higher profits of certain corporations, stronger political power, etc..) as these ends can be reached by other, more ethical means. Most of the solutions are well known to censors and effective filtering is used to limit access. For example machine learning is applied by censors to study Internet usage patterns and detecting unwarranted behaviours.

1.2. Core Objectives

Phase I: Building a Decentralized Network of VPN Nodes

Our first goal is to completely decentralize VPN node network, by using technologies such as existing VPN and proxy protocols, Ethereum blockchain, smart contracts, state-channels, decentralized database solutions, privacy ensuring coins like Monero or Zcash and other solutions.

This will be achieved throughout the development of Phase I, which is made up of 3 different stages (see 5. Roadmap). At the end of the 3rd Stage of Phase I, a completely decentralized and open source VPN network with all of its functions also decentralized will be released. No single point of failure will be possible from this time forward.

Phase II: Building Mysterium Protocol - as standard

In Phase II - our vision is to build Mysterium protocol capable of “dissolving” user data and sending it deep into the Network of Mysterium Nodes without the possibility of trace or censorship. The Network will take care of sending this shredded and encrypted data in an unrecognizable form to the receiving end, where Mysterium Protocol will ensure this user data to be “reassembled” again.

Mysterium protocol will eventually become a combination of different elements united into a coherent system.

Once complete, this Protocol will ensure that user data cannot be overtaken neither by nodes nor by third parties.

1.3. Mysterium Solution

Mysterium aims to be fully decentralized, peer to peer based and serverless node network, designed to provide privacy restoring techniques to its users with financial incentivization to its node operators (providers). Mysterium achieves this goal by utilizing already-existing technologies such as Ethereum blockchain, smart contracts and advancing their features with state-channels, evolving mechanisms of promises, combined with censorship-evasion protocols developed by the community acting as applications of the network.

Once Phase I Stage 1 is developed and released - this Network will protect user privacy and data, while enabling all users to share their spare bandwidth access with those who need this open access in exchange for financial compensation.

Mysterium network will act as a decentralized marketplace between providers and consumers participating in building and maintaining this infrastructure. The costs of providers will be paid by consumers using cryptographic currencies.

The development of the technology, its capabilities and functionality will come in several phases to minimise risk, learn from early experience and to benefit from development of complementary technologies(eg. state-channels). The decentralisation of all functions maintaining the network will be achieved by the end of the Phase I, Stage 3 (see 5. Roadmap).

Participants of the Mysterium Token Sale will gain access to tokens which will form the foundation to all transactions happening within the network. The network we are building will have opportunities for various levels of development by entrepreneurs and communities after it has been deployed. The Network will also be open to applications to make censorship less effective, ways to make payments easier and more efficient and new networking related services to be made available by reusing infrastructure and protocols developed by Mysterium Foundation.

VPN-like services on Mysterium network will be available early into Phase I, after completion of Ist Stage. VPN service provided by the Network in this stage will be comparable with the and may even improve upon existing Centralized Virtual Private Networking services. Mysterium market model will result in creating a VPN service which is both competitive and almost infinitely scalable, giving other entities (e.g. other VPN providers or app developers) an option to buy VPN service from the Network, integrating it into their solutions. This competitiveness comes from the open nature of the network and the ease with which anyone can earn money by joining it as a VPN service provider. Further improvements and new applications will follow in later stages, with complete decentralization achieved by the end of Stage 3.

1.4. Market driving forces

Everyday more and more of our lives are transferred onto the Net, which inevitably creates more opportunity for our data to be stolen, hacked, filtered or abused.

Research shows that increased data vulnerability is one of the main forces driving an expanding market for Internet privacy and security solutions:

1) Government legislation

There is a visible trend for governments to intrude into our private lives. As more of our lives are on the Internet this intrusion will only increase.

2) Western countries become accustomed to VPN services

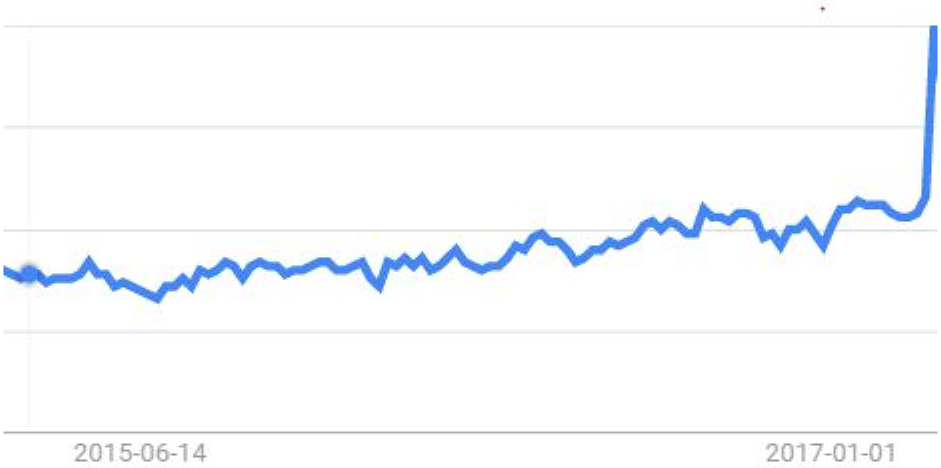
Currently, the main countries using VPN are located in Asia. However, following recent changes in western government policies, the number of people looking for Internet privacy solutions in the Western world is rapidly increasing.

3) Risk of cyber threats grows

Every year the number of cyberattacks increases followed by a greater awareness of the need for countermeasures. Companies and individuals tend to invest and change their online behaviour in response to cyberattacks, resulting in rapid expansion of VPN market.

4) Freelance workforce needs safe connection to corporate servers

Every year more work is done by freelancers. Having a safe connection to corporate servers becomes more urgent. Small businesses also require secure communications, but creating their own VPN can be a financial challenge.



Google trends graph for VPN days after USA Congress Overturned Internet Privacy Regulation.

Keeping the current world situation and visible trends in mind, increasingly people are growing concerned about their privacy. According to one study the use of ad blockers has risen by more than **40%** (198 million monthly active users in total). After recent Federal Communications Commission (FCC) change of regulations, the search for privacy solution in USA has skyrocketed.

According to Market Research Future project report:

“the global VPN market is expected to reach at USD **106 billion** by end of year **2022** with compound annual growth rate of **13%**.

VPN can be used to provide a security layer to both private and public networks such as WiFi Hotspots and the Internet. Organizations operating in healthcare, BFSI and telecommunication industry deal with sensitive information that needs to be protected constantly. Hackers are mostly targeting these industries due to very high price of data in black market. Same study shows that “currently, the world is experiencing more than half million attacks every minute, which will rise due to high technology proliferation”.

Keeping these trends in mind (increasing demand after privacy policy changes in multiple countries, increasing cybercrime, IoT and growing dependence on online services) the need to restore privacy on the Internet is becoming essential to counter the serious threat posed to both personal liberty and business security. Restoring privacy has become a salient global trend worldwide. Once developed, Mysterium Network will help it’s users restore privacy, providing freedom of speech and peace of mind while conducting personal and business life.

2. Token Mechanism

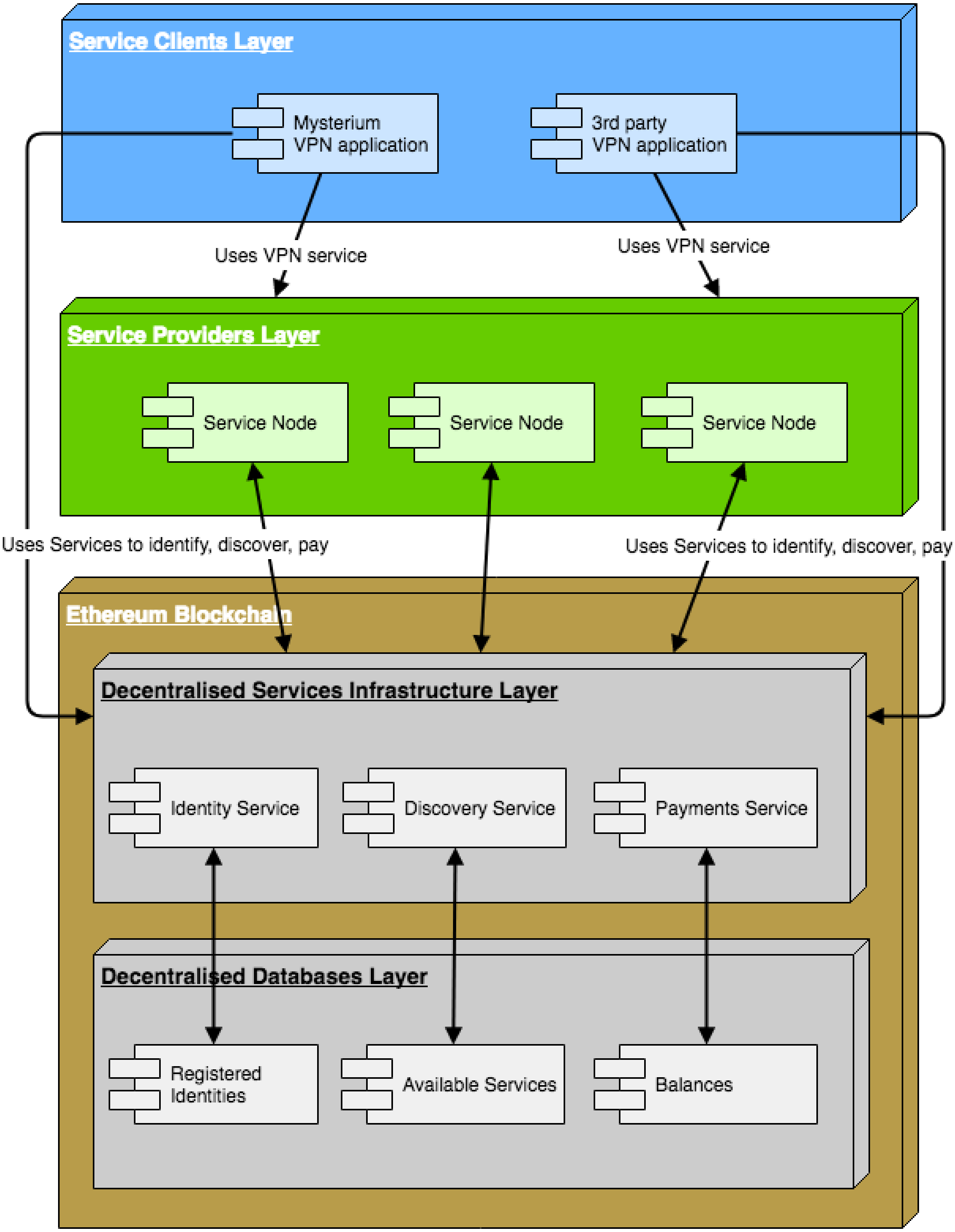
The token issued during the Token Creation is known as the Mysterium Token, or MYST. This is the only time that these tokens can be created, and therefore the total supply of MYST is fixed.

MYST will be an integral part of Mysterium Network where VPN consumers will be charged fees for services. The biggest slice of those fees will go to the VPN node owner (service provider) the leftover will be dedicated to protocol development and support. These fees will initially be denominated in MYST, which is a subject to change in the future.

As aforementioned node owners who run their nodes will be incentivized for their support of the network. In such a way node owner will essentially act as a miner, with reward coming in MYST token form. Differently from the typical blockchains the miner will be rewarded not for his computing power (proof of work), ownership of the currency (proof of stake), but for sharing their bandwidth.

The token will likely reflect growth of Mysterium Network. Mysterium Foundation will pursuit the possibility to enable MYST holders benefit by receiving a commission for each transaction in the Mysterium Network with payments being conducted in currencies other than MYST.

3. Platform layers



The Mysterium Network will be composed of four primary layers: Decentralised Databases, Decentralised Services Infrastructure, Service Providers and Service Clients.

3.1. Decentralised Services Infrastructure and Databases Layers

Mysterium Decentralised Services Infrastructure and Databases layers provide the foundational smart contracts enabling Mysterium nodes to identify themselves in the network, discover each other and send micropayments between the nodes.

3.2. Service Providers Layer

Mysterium Service Providers layer consists of Mysterium nodes, acting as VPN service providers.

3.3. Service Clients Layer

Mysterium Service Clients layer consists of Mysterium network client applications which will be developed by Mysterium, and by 3rd parties using Mysterium Network as a VPN service provider.

4. Roadmap

4.1. Competitive Analysis

The following table compares typical VPN provider, TOR and Mysterium networks.

	Centralized VPN	TOR Network	Mysterium Network
Anonymity	No	Yes	Yes
Decentralised traffic routing	No	Yes	Yes
Possibility for end-to-end encryption	No	Yes	Yes
Honeypot risk	High	Low	Low
Network participants incentivised	No	No	Yes
Open source	No	Yes	Yes
Speed	High	Low	High/Medium
Platform as a Service	No	No	Yes

4.2. Funding Breakdown

Funds donated during the Token Creation will be used solely for the development and benefit of the Mysterium network. The following distribution of funds is preliminary and can be a subject to change.

4.2.1. Core Development – 40%

Core development will involve the development of the technology as described in this document. This includes: Mysterium node network, integration of VPN protocols, smart contract systems, supporting protocols and services, end user applications, ..

4.2.2. Operational – 25%

This covers the necessary costs incurred for a functional system. This includes: hosting and infrastructure costs, staffing, outsourcing, management and other related expenses.

4.2.3. Marketing and Sales – 25%

Marketing costs will be used for partnerships development and direct consumer marketing. Sales costs will largely be incurred by direct B2B sales to businesses selling Mysterium as a platform solution.

4.2.4. Legal and Compliance – 10%

There are legal costs associated with privacy protection and fighting censorship. The legal costs might vary from region to region.

4.3. Development Roadmap

The whole development is spread out into distinct phases starting with Phase I and Phase II. Each phase is further divided into several internal stages.

4.3.1. Phase I

Goal of this Phase is to build a fully decentralized VPN.

Phase I components:

- Discovery mechanism - node and customer matchmaking smart contracts;
- Smart contract managing Mysterium Identity;
- Payment mechanism - a combination of state channels and smart contracts clearing

payments;

- VPN Node protocol and libraries - the “*workhorse*” of the network, providing the actual VPN service to customers;
- Node applications - native node applications built for major operating systems, capable of running Mysterium protocol and providing VPN service to customers;
- Client applications - allowing end users to connect to the network as VPN customers;
- Interface into the Network for third party applications.

Achieving this will take 3 stages to complete.

Stage 1

Goal of this stage is to launch Decentralized node network, leaving certain elements centralized for speed, security and learning purposes.

Development goals for Stage 1:

- Smart contract for clearing payments;
- Mysterium Node V1.0 - developed for Linux;
- Mysterium Client V1.0 - developed for 3 major operating systems;
- Mysterium client on 3 main operating systems;
- Mysterium central server overseeing node Discovery, Identity management and Micro payment accounting processes;
- Node network deployment and initial testing.

Stage 2

Goal of this stage is to integrate additional VPN protocols into the node and work further towards decentralization

- Mysterium Node V2.0 & Client V2.0 - adding new protocols, developed for major operating systems, integrating with new smart contracts;
- Smart contracts for Discovery and Identity Management;
- Simplified Central server - down to oversight of Micro Payment accounting processes;
- Marketing.

Stage 3

Goal of this stage is complete decentralization, with removal of central server role as oversight and management position, moving to decentralized infrastructure.

- Removal of Central server;
- Smart contract performing Micro Payment accounting;
- Mysterium Node and Client V3.0 - State channel integration, removal of all ties to central server connection;
- Interface into the network for third party applications.
- B2B Sales and Marketing;

Once initial technology is in place and a Decentralized node network is functional - Mysterium will open up for various third party services to be built on top of this network.

According to our evaluations 6MM is enough to develop everything promised for the Phase I to have a fully decentralized and open network, fully operational and without a single point of failure, where even we as a team will not pose that risk anymore.

4.3.2. Phase II

Goal of Phase II is to develop Mysterium protocol as standard, capable of “dissolving” user data and sending it deep into the Network of Mysterium Nodes - providing complete end to end encryption.

If we are able to attract anywhere up to 9MM CHF during this token creation - we will have enough funds to finish and polish Phase I. Once that is done - we will research, design, plan, start developing and implementing Phase II protocols.

5. Token Creation Details

Mysterium Token Creation will commence on May 30th 2017.

- Primary accepted currency is Ether when turning it into MYST
- Other currencies like Bitcoin or Fiat currencies can also be contributed via our partners Bitcoin Suisse and turned into MYST.
- MYST-price is defined in CHF. The final exact ETH price per MYST will be defined from the ETH/CHF rate on May 30th 2017, 12:00 (CEST) and remain fixed throughout the entire contribution period.
- The creation will be capped (“Soft Cap”) upon receipt of ETH equivalent to 6 million Swiss Franc (CHF). This amount is a subject to change before Token Creation commences.
- The Token Creation period will last fourteen days max if Soft Cap is not reached sooner.
- If the Soft Cap is reached before the end of fourteen days, additional donations will be accepted for 72 hours in case some contributors missed a very short window for MYST creation.
- Minimum goal of donations is 700.000 CHF. If this goal wouldn’t be reached, all early contributors would get refunded.
- Token Creation will also be hard capped: upon achieving this cap, token creation will stop and no further contributions will be accepted. The hard cap amount is set to 14.000.000 CHF.

5.1. MYST Creation Ratios

- Before Soft Cap is reached, 1 CHF = 1.2 MYST (ETH price per MYST will be determined 3 hours before Token Creation Event).
- After Soft Cap is reached (72 hours period), 1 CHF = 1 MYST.

5.2. Additional MYST

Additional MYST will be created, designating it for the Future Funding, Foundation operations, Bounty program, Advisors early Seed investors as follows.

5.2.1. Future Funding

Part of MYST supply will be reserved for future as an additional fundraising mechanism for the Mysterium network project to continue development of Phase II, but may never be issued, depending on circumstances in the future.

The amount reserved for future funding will be as following:

- If up to 2 million CHF is collected, 50% of all tokens will be reserved for future funding.
- The percentage will decrease gradually to 15% with further funding until 6 million CHF is reached.
- After 6 million CHF, the number of tokens reserved for future funding will be fixed at 15%.

Tokens reserved for future funding will be locked for 12 months, after which they will be sent to a multisig wallet belonging to Mysterium Foundation.

5.2.2. Founders, Foundation, Bounty program and Advisors

- Mysterium Foundation, Bounty program and Advisors will receive 9% of all tokens. Tokens will be received by the Foundation multisig wallet, and will be used to reward assistance from: early node operators (mining), bounty program participants, advisors and new employees via a Vesting program, etc.
- Founders will receive 10% of all tokens. Founder tokens will be locked for 12 months.

5.2.3. Seed Participants

Seed Participants will be rewarded with the following token multipliers for their early commitments with ETH/CHF ratio calculated at the commencement of the Token Creation:

- 1x if 2 million CHF (or less) is collected.
- 1x to 5x gradually increasing seed multiplier if more than 2 million CHF and less than 6 million CHF is collected.
- Multiplier will stay at 5x if 6 million CHF (or more) is collected.

Seed Participant tokens will be separated in two parts: the 1x multiplier part will be released to Seed Participants right after the Token Creation ends. The second part will be locked for 12 months.

5.2.4. Example of Token Structure after Creation is over

As contribution is pegged to ETH value in CHF, in this example we assume that 1 ETH value at the moment Token Creation will be at 50 CHF.

Donation, in CHF	**2m**	**3m**	**4m**	**5m**	**6m**	**9m**
Token Creation Contributors (instant)	27.60%	34.10%	40.80%	47.70%	54.60%	57.50%
Foundation, Bounty, Advisors (instant)	9.00%	9.00%	9.00%	9.00%	9.00%	9.00%
Seed Participants (locked)	3.40%	5.70%	7.70%	9.50%	11.40%	8.50%
II'nd Phase (locked)	50.00%	41.20%	32.50%	23.80%	15.00%	15.00%
Founders (locked)	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

6. Mysterium Architecture

Mysterium is still undergoing intense development and will be for a while. Parts of this section are subject to change.

6.1. Technical Overview

VPN service consumer find and pay service providers in Mysterium network by using Mysterium built-in smart contract based Identity, Service Discovery and Payment services. The network itself works over the Internet and relies on Ethereum blockchain for censorship resilient distributed storage and transactional processing needs. The Mysterium network uses Registered Identities to enable means of creating limited trust when engaging with services and payments.

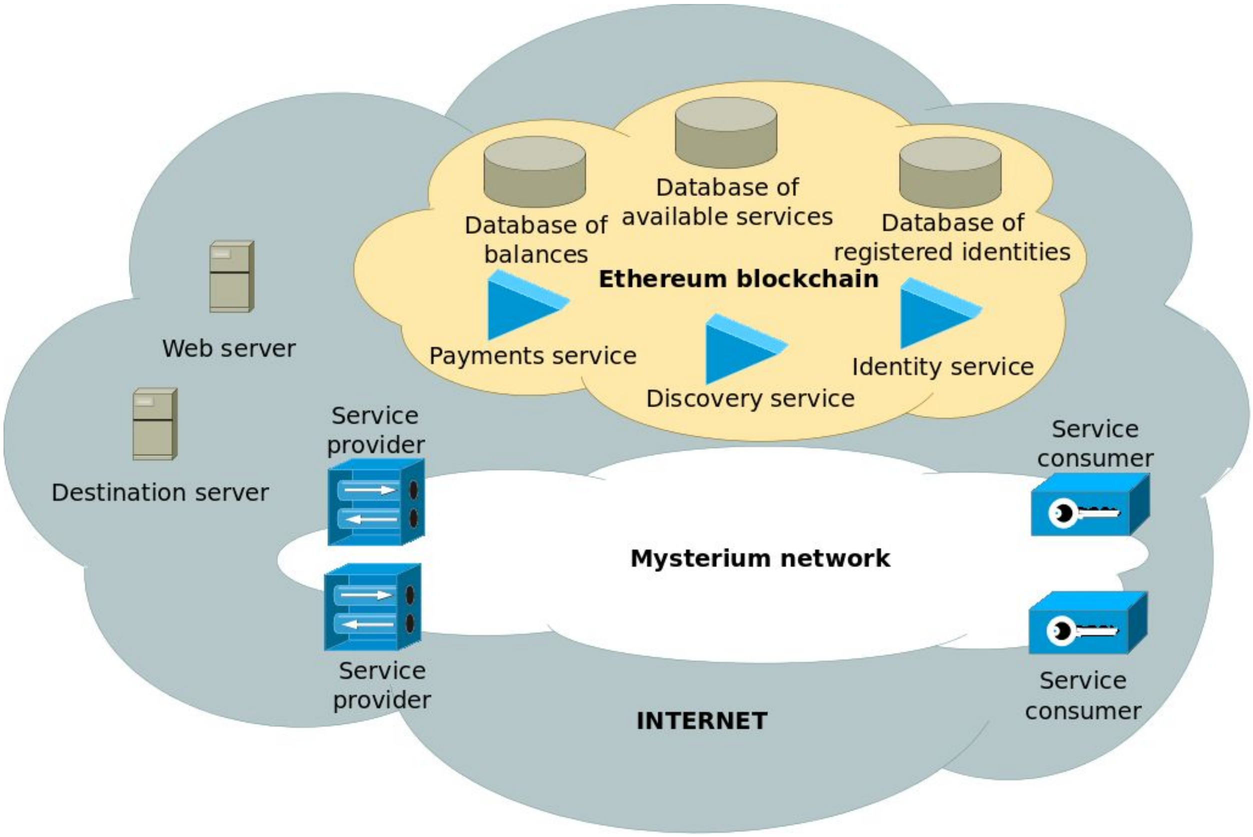


Illustration: Bird's eye view of the Mysterium network

Any person who has their identity registered on The Mysterium network can announce VPN services (compatible with the network's VPN service protocols) along with the payment terms these services will be available at. Other users of the network will be able to find services matching their specific needs (location, price, etc...) and use search results to establish a connection to selected VPN service providers and use the announced services. A consumer of VPN service and VPN service providers will exchange several messages to negotiate the payment terms (e.g. service metering granularity) and technical information necessary to establish the secured VPN session. During this negotiation, a consumer of the service will make a promise to pay for some amount for services to be received in advance and this promise will be updated by the consumer every time an extension of service is desired. The VPN service provider later will use this promise to clear payment via smart contracts on the Ethereum blockchain. If the consumer's balance held in the network's deposit account is sufficient then the promised amount of MYST tokens will be transferred from the consumer's deposit account to the service provider's account.

6.1.1. Core components

1. **Ethereum** allows to run decentralized code with smart contracts, enabling reliable services and payment handling.
2. **Identity service and database of registered identities** ensures the proper identity acknowledgement between client and service provider.
3. **Discovery service and database of available services** provide means to announce VPN services availability and pick the most suitable VPN service.
4. **Payment service and database of balances** allows secure promise-based micropayments for services.

6.2. Service Provisioning

When a client (a service consumer) is in need of VPN services provided by VPN service providers on the Mysterium network, they must first choose a service matching their needs. After a service is chosen, the client's identity starts a dialogue with an identity providing this advertised service. During the course of dialogue a value transfer may be promised and VPN service sessions may be provisioned. Dialogue can be started over existing messaging channels between the nodes or a new channel is established. Dialogue ends when one peer stops listening to the other party or any party loses connection to the Internet.

6.3. Identity Service

There are interconnected software agents (we call one instance of this an **identity agent**) representing digital identities. Each identity agent acts on behalf of a person controlling the identity. This software agent is a functional part of the application (a Mysterium network node) used to connect to the Mysterium network to provide or consume VPN services. Each agent has access to a digital identity represented by the agent's ability to electronically prove service by signing and decrypting all communications using a private key associated with the identity. A node may have access to more than one identity. The identity is created by generating public and private keys. The identity is identified by a unique identifier derived from a public key by using the last 20 bytes of a keccak256 hash of the public key. This identity can be made publicly known to other network users by announcing its existence through invoking an identity registration smart contract on the Ethereum blockchain. The contract must be supplied with an identifier and a public key of identity as an argument. After the identity contract is successfully executed the public key of identity is appended to the Ethereum blockchain by miners. At this point the appended identity becomes a Registered Identity. All Mysterium nodes in the network follow the blockchain and read transactions of the newly registered identities and maintain a local copy of the database of all Registered Identities using data gathered from transactions. Nodes can use a local copy of the Registered Identities database to lookup public keys associated with other identities. This database is used by nodes to check if the communications received from other nodes comes from valid registered identities and are properly signed.

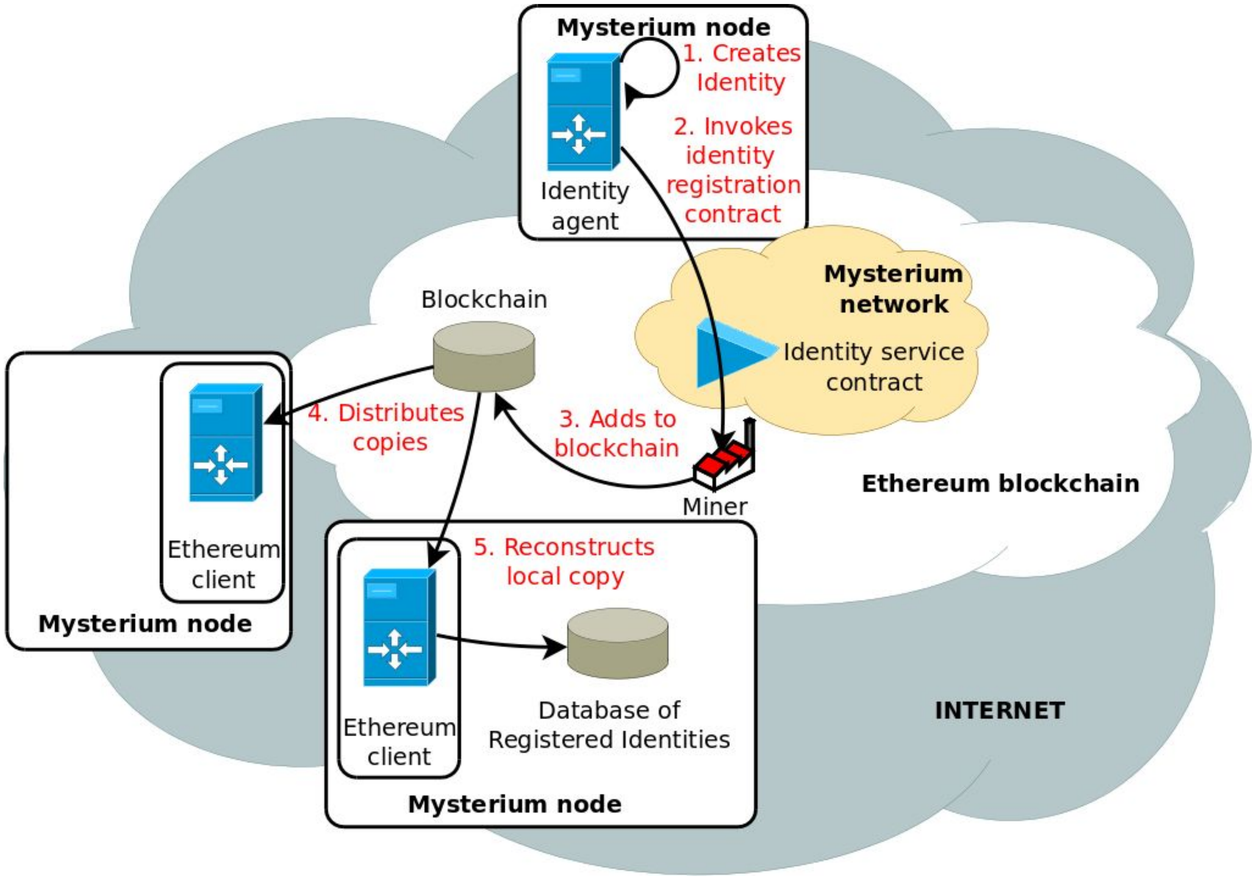


Illustration: Identity data registration and replication

6.3.1. Registered Identity Value

Mysterium nodes must attach a predefined amount of value (MYST) to successfully invoke the identity registration contract and have the identity registered. The amount of value will be adjusted periodically automatically to reflect the value of MYST in fiat currencies. This forfeiture of value (MYST) has a purpose of making identity something of value. By attaching cost to identity we make it unattractive to abandon. Also, because it is expensive to produce identities in large quantities the system limits exposure to several types of trust exploitation. We see Registered Identities as something to be reused to users' own benefit. By reusing an identity for payments users will have their payments history and balances made public, and their identities made more predictable and thus trustworthy for service providers. We will discuss risk and trust relationship further when describing payments.

6.3.2. Cryptographic Mechanisms

Because of computation costs and limitations of running long computations on Ethereum Virtual Machine, the cryptographic mechanisms backing the registered identities technically will use EVM's built-in implementations of keccak256 hashing, ECDSA signature verification and identifier recovery functions. A key pair and an identifier used behind the identity are technically identical to the cryptologic security artifacts behind Ethereum's external account. A Mysterium key pair should not be reused to hold value in Ethereum blockchain.

6.4. Service Discovery

Service providers willing to provide VPN services and be compensated for doing so can announce their services to the network. To announce the service, the provider's node prepares a service proposal. A proposal encodes the proposal format version, provider description, qualitative service definition, and a list of methods to reaching the provider's node. The provider's Identity agent then signs this proposal and the node invokes a service announcement smart contract on the Ethereum blockchain with the signed proposal as an argument. After a miner runs the contract and adds the proposal to the Ethereum blockchain the proposal becomes publicly available for anyone to read and to copy. Mysterium nodes follow the blockchain and copy transactions containing proposals from it, noting the Ethereum blockchain block number they appeared on. Nodes then extract proposals from transactions and use these extracted proposals to construct and locally store a consistent database of all services available on the network. Nodes can query a locally stored database or a database on other trusted nodes to search for services matching user specific needs.

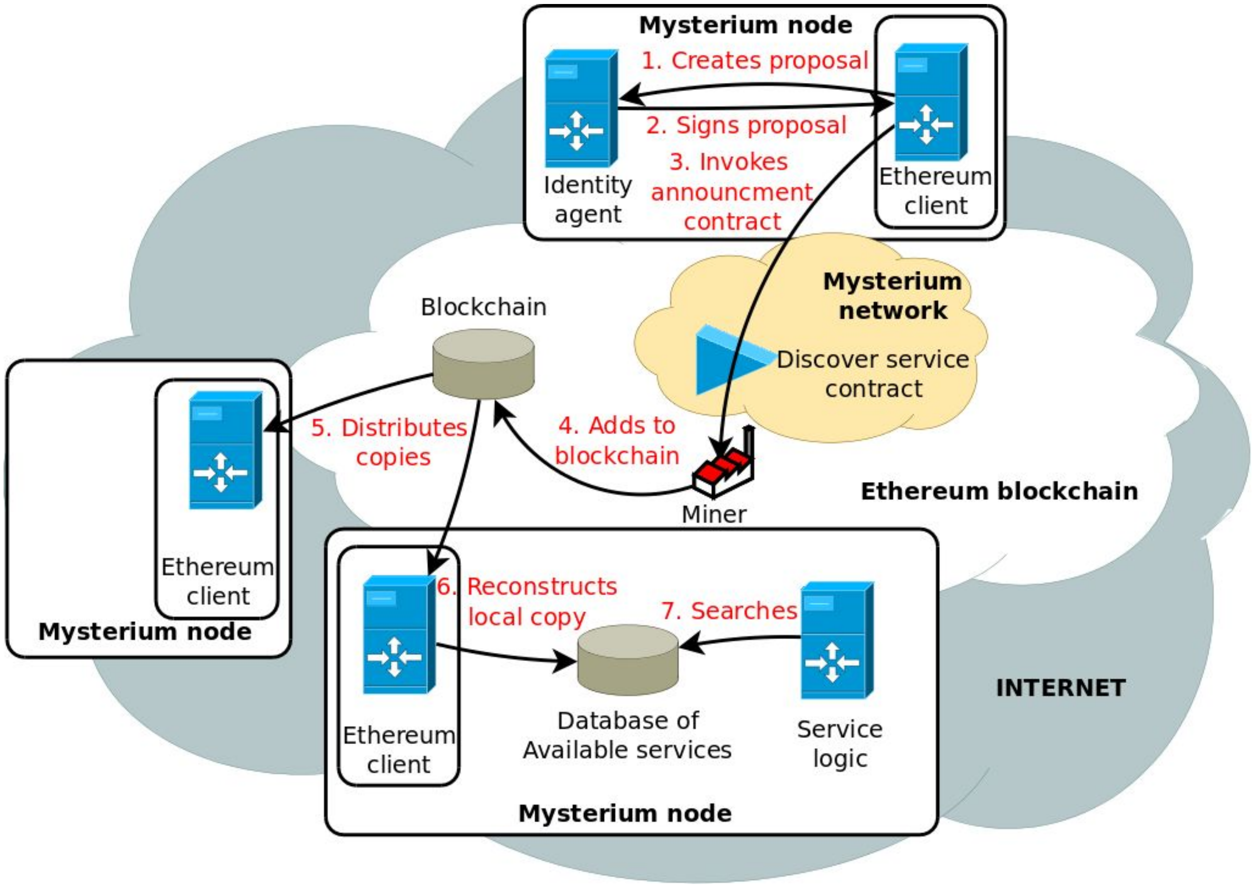


Illustration: Service announcement and discovery

6.4.1. Outdated Service Announcement Handling

Proposals added to the blockchain stay there forever, but the announced services may not be available for that long. In order to get rid of outdated proposals we define simple network user behaviour: users discard all proposals received before a predefined number of blocks (~60000 which is somewhat near to ten days) and service providers re-announce their services before the old proposal gets discarded. When service providers re-announce service reusing the same serial number, all network users replace old proposals stored in their local copy of the database to a the new proposal taken from the blockchain. This simple method ensures all outdated service announcements will expire.

6.4.2. Service Proposal

As mentioned above, an instance of service proposal encodes: proposal format version, provider description, qualitative service definition and information needed to contact the provider's node. A version number is included in the proposal to allow extensions to the proposal format. Provider description includes the identifier of a provider and per provider unique serial number of service provided. The serial number may be reused to update node contact information, but should be changed to a new unique value if any of qualitative parameters (including price per unit) has to be updated.

A qualitative service definition includes: 1. Definitions of VPN service type offered 2. Approximate information on location where the service is provided from 3. Approximate information on location where the tunnelled traffic will originate from 4. Available per session bandwidth 5. Service usage metering method and the service price per unit of metering as in MB/MYST or seconds/MYST.

6.4.3. Types of Services

There will be several distinct types of VPN services available on the Mysterium network. IP tunnelling and Socks proxy style services are first in the queue to be implemented. Other kinds of networking-related services may follow. Approximate location will have Internet attachment point (ip address) mapped to Internet Autonomous System number and ISO 3166 Alpha-2 country codes. Approximate location will be used to quickly search for services available on a specific Internet service provider or country level precision. Information needed to contact provider's node includes a list protocols supported by provider's node accompanied with protocol specific data. This list will contain mandatory information to implement default node to node protocol type with associated IP (v4 and v6 if available) address and port information attached.

Nodes may support multiple types of VPN services. Every service type has to be advertised as a separate service. Nodes durably store all proposals they announce and still regard as valid. The valid proposal is a proposal of service the provider is willing to deliver on terms defined in the qualitative description.

6.4.4. Service Selection

Every client is free to choose different services from the same or multiple providers on the Mysterium network. A consumer of VPN services uses local or trusted remote database of announced services (service proposals) to search for a service adhering to their requirements: service type, locations of where service is provided, where your traffic will appear from, metering units, maximum price per metered unit and committed bandwidth.

All candidates matching requirements then can be sorted by ascending price, and service session establishment may be tried in an order of increasing price until a functioning dialogue is started. Users may prefer using services from providers they have successfully used before and these providers can be flagged as preferred even if the price per unit is higher than lowest available options from other providers. After the client (or automatic process) selects a preferred service to use, the following events occur: a dialogue between the client's and provider's nodes is established, some value is debited by means of issuing promises, a carrying connection is established and terminated after use. In the case where establishment of dialogue fails, an establishment of dialogue with the next best service candidate can be tried manually or automatically.

The Mysterium network clients may provide a varying degree of automation to assist the client in the service selection process. Logic and presentation can vary between client software implementations. The protocol for remote database query functions and trust model are not defined yet and subject to further research and design.

6.5. Payments Handling

Mysterium network will implement a state channel payment method. The mechanism remotely resembles the way checks work. A bank account holder can write a check to another person (the benefiter) as a form of payment. A check has the issuer's name, payee's name and a sum of money promised. All written down and signed by the issuer. While at the bank, the payee can exchange a check for the sum of money promised in the check. The bank may refuse to pay and return the check if the issuer's account does not have enough funds left to cover the promised value.

In the Mysterium network, all network users have an account managed by the smart contract on Ethereum blockchain. Users store some value (MYST) in their accounts. When one user wants to use VPN services provided by another user, they issue promises to give some of this stored value to the service provider in exchange for services. A service provider collects these promises by requesting a Mysterium smart contract to transfer value from the account of the issuer to their account in exchange for the collected promises. All value transfers will be netted, and the balance of each account will be stored in the contract state. Users may request a smart contract to withdraw some value from their account to any Ethereum account of their choice.

6.5.1. Accounts

We will develop and deploy a smart contract on Ethereum blockchain used to manage user accounts and execute value transfer transactions. A single contract instance will hold value for all Mysterium accounts. All transactions executed by the contract will be added to the Ethereum blockchain. The transactions include deposits, payment clearing and withdrawal. Anyone with proper software can follow transactions added to the public blockchain and reconstruct the state of any account. Service providers may want to reconstruct current balances of their clients to make sure sufficient funds are left to pay for services provided.

6.5.2. Deposits

Any Mysterium user can transfer some MYST to an account managed by a Mysterium payments contract. To deposit some value (MYST) a user must invoke the contract and supply it with value (MYST) and provide an identifier of the provider account as an argument. A successful execution of the contract will result in credit in the amount of value supplied.

6.5.3. Issuing Promises

A promise is a binary representation of an issuer's promise to pay. The promise consists of an identifier of the party issuing a promise (an issuer), a serial number of the promise, an identifier of the party to receive payment (a benefiter), the sum (in MYST) promised. When users need to pay other users they issue a new payment promise (or update an existing promise) and send it to the benefiter. A unique serial number is assigned to each promise and it must be incremented each time a new promise is issued. Serial number uniqueness must be maintained on an issuer and benefiter pair basis. A promise can be updated by increasing the value promised while keeping other components of the existing promise unchanged. A benefiter of a promise may request the issuer to stop updating a promise and to issue a new promise on the next payment. Every time a promise is sent to a benefiter it is digitally signed by an issuer. After receiving a promise a user should check if it is valid. A valid promise is properly signed by the issuer, if it has a serial number higher than the last cleared promise and if it was not updated after issuer was asked to not update it.

6.5.4. Clearing of Promises

To receive the value promised in a payment promise it must be cleared. Users must request the Mysterium payments contract to clear the payment promises received from other users. Promises with the lowest serial number must be cleared before other promises with the same issuer and benefiter pair. The clearing request to a contract must include: a promise received from the issuer, issuer's digital signature of the promise and the benefiters digital signature of the promise. Both signatures represent a mutual agreement between the issuer and benefiter to transfer a promised sum.

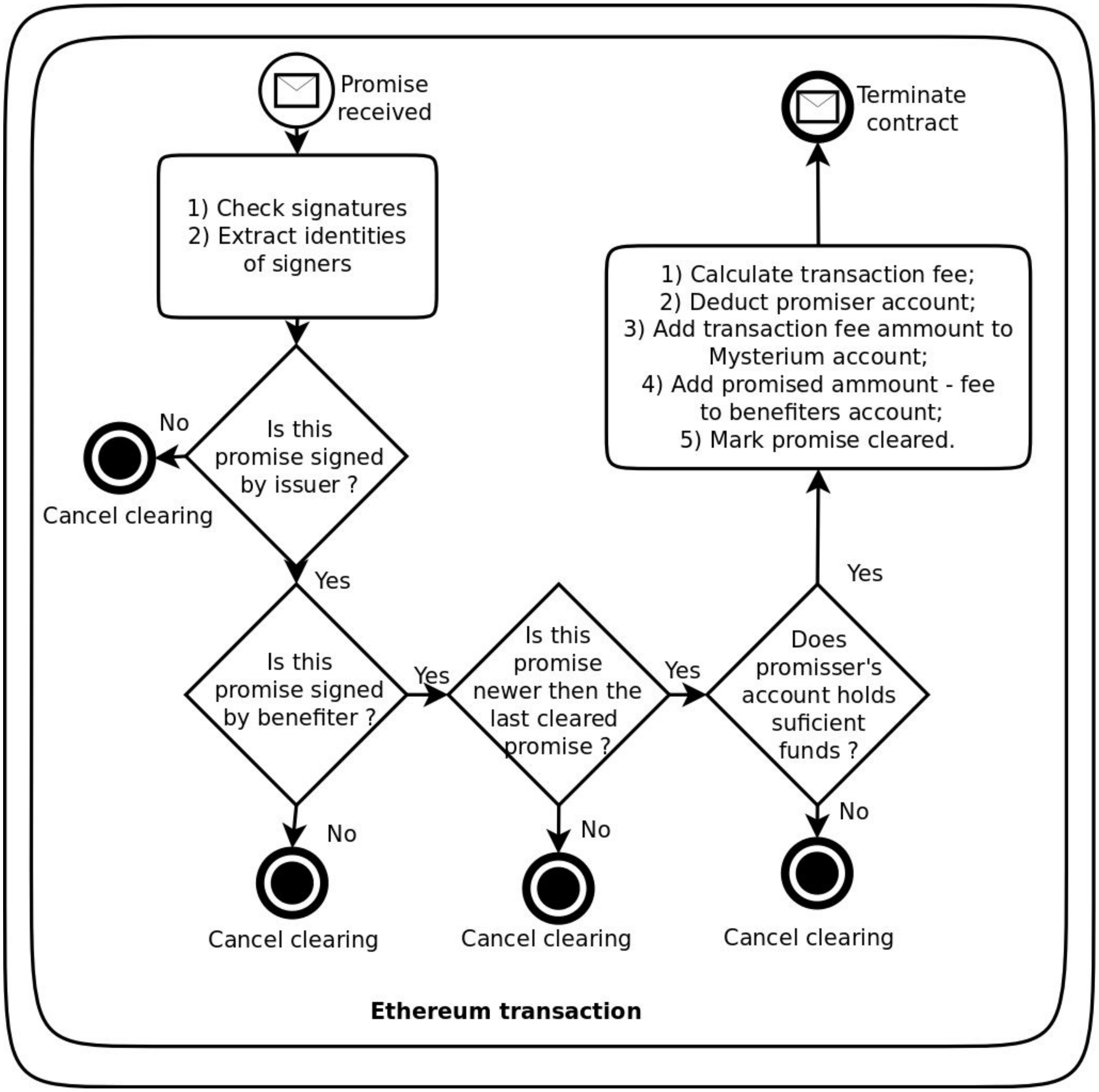

Promise received
1) Check signatures
2) Extract identities of signers
Is this promise signed by issuer ?
No
Cancel clearing
Yes
Is this promise signed by benefiter ?
Yes
No
Cancel clearing
Is this promise newer then the last cleared promise ?
Yes
No
Cancel clearing
Does promisser's account holds suficient funds ?
Yes
No
Cancel clearing
1) Calculate transaction fee;
2) Deduct promiser account;
3) Add transaction fee ammount to Mysterium account;
4) Add promised ammount - fee to benefiters account;
5) Mark promise cleared.
Terminate contract
Ethereum transaction

Illustration: Payment promise clearing

When a smart contract is executed it checks if an encapsulated promise is properly signed by an issuer and benefiter. First digital signatures are verified and identifiers of signers extracted from signatures and then extracted identities are compared with identifiers defined in the body of promise. If the promise was not signed by an issuer and a benefiter then clearing is cancelled. Otherwise the clearing process is continued and contract code checks if the promise was not cleared before. The payment contract uses state storage to store the last serial number of payment promise which was cleared. This saved information is unique for any issuer and benefiter pair. The simple comparison of two serial number is enough to determine if a promise was not cleared before.

In the case where the promise was cleared before, the clearing is cancelled. In the case a promise was not cleared before the balance of the issuer is checked to make sure it has at least the amount promised. If the issuer's balance has insufficient funds, clearing is cancelled, but it does not mean the promised value is lost. The benefiter may choose to try to clear payment later when the issuer deposits more MYST to their account. And finally, in case the issuer's account holds a sufficient amount of funds the clearing can be completed. The value defined in the promise is credited from the issuer, a small transaction fee is calculated and debited to the account of the Mysterium network and the rest of the promised value is debited to the benefiter's account. Then a serial number of the payment promise is stored in contract state storage and clearing process ends. When invoking a payment contract a benefiter may demand payment contract to clear promise even when there are no sufficient funds left to completely honour the promise at a loss of difference in sums available and promised.

6.5.5. Withdrawal

In the case where the promise was cleared before, the clearing is cancelled. In the case a promise was not cleared before the balance of the issuer is checked to make sure it has at least the amount promised. If the issuer's balance has insufficient funds, clearing is cancelled, but it does not mean the promised value is lost. The benefiter may choose to try to clear payment later when the issuer deposits more MYST to their account. And finally, in case the issuer's account holds a sufficient amount of funds the clearing can be completed. The value defined in the promise is credited from the issuer, a small transaction fee is calculated and debited to the account of the Mysterium network and the rest of the promised value is debited to the benefiter's account. Then a serial number of the payment promise is stored in contract state storage and clearing process ends. When invoking a payment contract a benefiter may demand payment contract to clear promise even when there are no sufficient funds left to completely honour the promise at a loss of difference in sums available and promised.

6.5.6. Risk Management

Promises do not guarantee payment. The sum written in the promise is not limited to the value held in a user's account. All promises are signed by a user and are valid until cleared. This means users will not be able to safely use their identities after making false promises to other Mysterium network users. As soon as an issuer of a false promise deposits value to his/her account, anyone holding a valid promise issued by that account holder can take this value. It costs to create a Registered Identity, but it becomes worthless the moment it is abused. Loss of value of identity should deter users from issuing false promises. The proposed payment method will be limited to payment transactions worth half the value needed to create Registered Identity.

All the transactions of a payment contract are stored in a public ledger based on the Ethereum blockchain and as a result they are accessible for everyone to read. Anyone can reconstruct all transactions and eventually view balances for each Registered Identity on the Network and track all promises kept and promise serial numbers used to clear payments. This means anyone can check your balance before accepting your promise and check your payments history to make an educated guess of how trustworthy you are.

There is also a balancing act of risk and benefit related to costs of clearing transactions. Invocation of payments from a smart contract has costs in gas and transaction fees. Some service providers may choose to forbid users from updating promises with higher value, and clear promises as soon as possible at the higher relative cost compared to value received. Other providers may choose to take higher risk and allow promises to accumulate value to make cost of clearing negligible compared to value received.

Promises received from clients (not signed by benefiter) can be shared with other users without fear of giving away a value associated with the promise. Sharing and matching promises received from other providers may be instrumental in mitigating risks of clients having a low balance and also using a huge number of false promises to many service providers.

Our payment solution gives providers access to the information necessary to assess risks. It also gives them freedom to choose their position in the trade-off between lowering clearing risks versus having higher clearing costs.

6.6. Messaging Between Nodes

Messaging channels enable nodes to exchange messages. There will be multiple types of messaging channels. Each channel type may employ a different carrier protocol and communication scheme (direct node to node, relay over centralised service, relay over p2p overlay). A dialogue between nodes can be started over any type of messaging channel available to both nodes participating in a dialogue. One default channel type and associated communication protocol will be defined and supported on all Mysterium network clients. Other optional to implement messaging channel types will be added as needed to exploit weaknesses in information censorship deployed in real-time networks. Messaging channel implementations will provide an unreliable datagram messaging interface. Some channels types may implement transitive message routing and thus measures to secure content of communications is required. Each message sent over a channel is signed by the sender and then encrypted using the Elliptic Curve Integrated Encryption Scheme. This way of protecting message exchange will prevent eavesdropping on content of communications, but is still vulnerable to determination of the identities of communicating parties.

6.6.1. Dialogues

Dialogues provide a structured way for two identities (peers) to exchange information needed to arrange payments for services provided and provision service sessions. Only a single instance of dialogue can exist between two identities at any one time. If a new dialogue is attempted a previous dialogue is closed and a new dialogue is established. The dialogue will provide reliable message transmission over unreliable messaging channels by implementing a simple positive acknowledgement scheme for retransmission of lost messages.

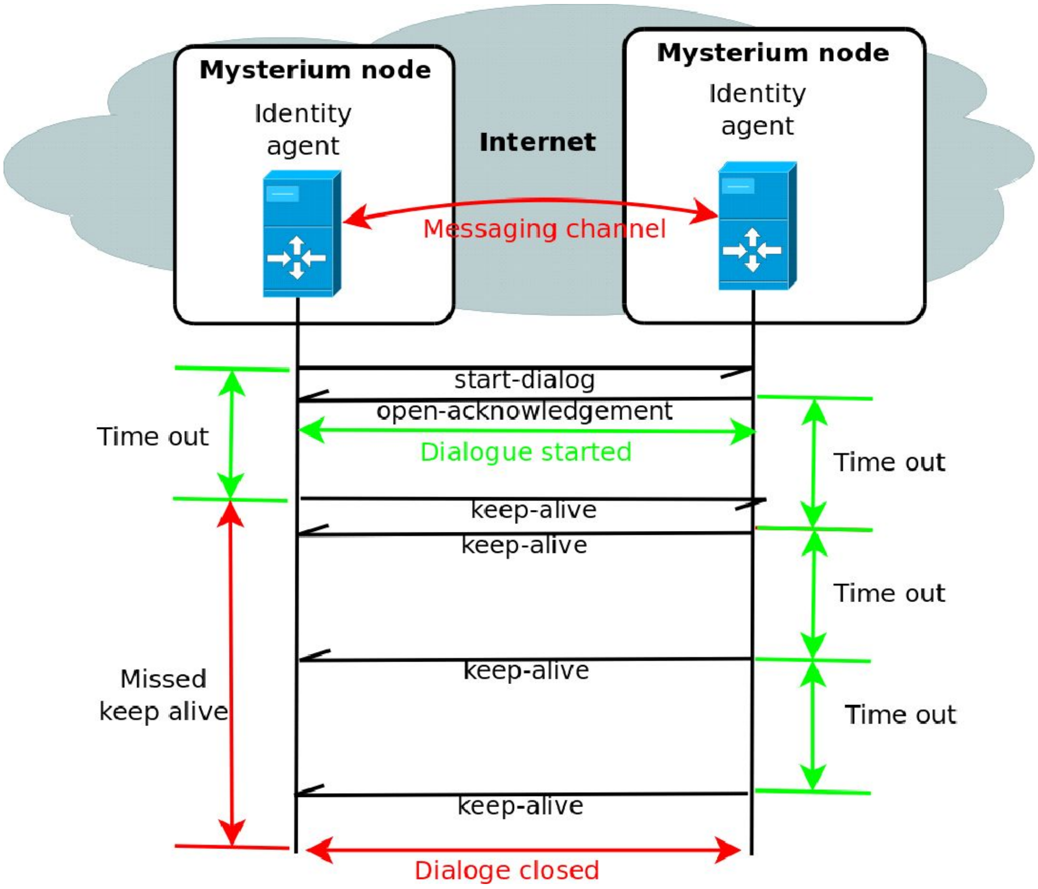


Illustration: Life-cycle of dialogue

Dialogue is established when one identity asks another identity to start the dialogue and the other identity acknowledges the dialogue establishment attempt. To keep dialogue open some messages have to be exchanged regularly. If a node has nothing meaningful to send, it should send keep-alive messages instead. Identity agents monitor when the last time any message was received from a peer and may decide to close the dialogue if no message was received for a long time. An identity can stop an existing dialogue by simply ignoring any messages arriving from the remote identity.

6.6.2. Payment Scheme

Identity agents may store state information on the node. This state may have records on each other identity that it has established a successful dialogue with previously. Record data includes: amount of MYST received from the peer but not yet used to pay for services provided, a last promise received from the peer and a list of all not yet cleared promises it has received from the peer. Choosing to store state information will allow providers to reduce costs of clearing payment promises received from clients. After a dialogue is established, both identities participating in dialogue try to lookup state information it has on the remote identity and each identity agent sends payment advice to the dialogue peer. Advices are sent both ways because the identity relationship is symmetrical and it is possible that both identities will use services provided by the peer simultaneously.

The payment advice includes the leftover amount of MYST received but not used to pay for services, a payment policy describing requirements to a newly issued promise and an optional request to update a previously sent promise instead of issuing a new promise. Some providers may choose to give away some services free of charge for service testing purposes. That is accomplished by telling the peer it has higher than zero leftover the first time it uses the service. The payment policy indicates a minimum amount of MYST has to be promised by the client to be deemed acceptable by a remote peer.

A request to update a promise contains a copy of the last not yet cleared promise received from a peer. Payment advice is sent by a node when: a) a leftover changes by more than 10 percent from previously reported amount; b) when leftover amount reaches zero; c) when service provider decides it want to clear the last promise received; d) when service provider accepts new or updated promise. Before clearing the last promise received from the peer the provider should notify his peer by sending payment advice not including the optional part of advice and making sure it was successfully received before proceeding with clearing. Notification is needed to avoid a race where a peer may send an updated promise while the previous version of the promise has already been sent for clearing.

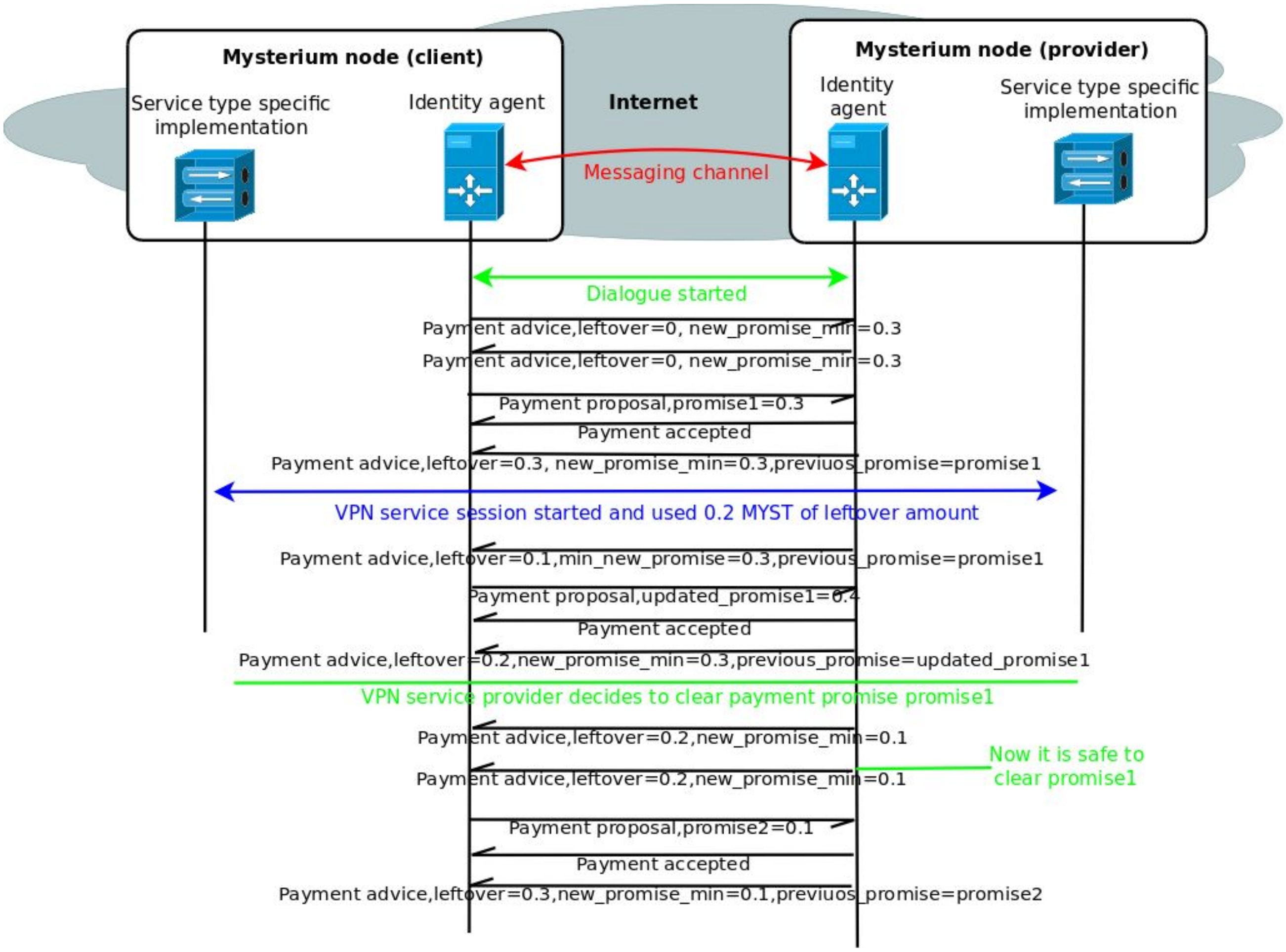

Mysterium node (client)
Service type specific implementation
Identity agent
Internet
Mysterium node (provider)
Identity agent
Service type specific implementation
Messaging channel
Dialogue started
Payment advice,leftover=0, new_promise_min=0.3
Payment advice,leftover=0, new_promise_min=0.3
Payment proposal,promise1=0.3
Payment accepted
Payment advice,leftover=0.3, new_promise_min=0.3,previuos_promise=promise1
VPN service session started and used 0.2 MYST of leftover amount
Payment advice,leftover=0.1,min_new_promise=0.3,previous_promise=promise1
Payment proposal,updated_promise1=0.4
Payment accepted
Payment advice,leftover=0.2,new_promise_min=0.3,previous_promise=updated_promise1
VPN service provider decides to clear payment promise promise1
Payment advice,leftover=0.2,new_promise_min=0.1
Payment advice,leftover=0.2,new_promise_min=0.1
Now it is safe to clear promise1
Payment proposal,promise2=0.1
Payment accepted
Payment advice,leftover=0.3,new_promise_min=0.1,previuos_promise=promise2

Illustration: Use of promises to pay in advance

To simplify explanations a bit, let's assume only one identity is using services provided by a peer identity (provider). In order to increase leftover (balance) tracked by the provider a client must send a payment proposal. The payment proposal is a message sent to a peer and it contains a payment promise. After receiving a valid payment proposal the provider will acknowledge the proposal as valid and accepted. If payment proposal is unacceptable the negative acknowledgement will be sent. Negative acknowledgement will also signal a reason for refusal. Clients should use advice received from a provider and try to update an existing promise if the optional part was present in advice. In case an optional part of advice is not received, a new promise must be issued by the client the next time a payment proposal will be sent. A client may choose to ignore advice received and always send payment proposals containing new promises with a sufficient amount of MYST acceptable by the remote peer.

6.6.3. Service sessions

To be useful a VPN service must provide an interface to user applications and have a data carrying channel(s) established to provider node(s). This interface is service type specific. It may manifest as Internet Protocol interface if IP tunnelling service is used or it may be a socket listening on the local IP address when a secured socks service is used. The data carrying channel(s) used to carry traffic generated by user application is also application specific. The Mysterium network will support many VPN service types and thus messages sent to establish service sessions need to be flexible enough to carry application specific negotiation payloads. To use an advertised service a node must have support for the advertised VPN service type. This support may come in the form of built-in node functionality or as a plug-in to the node software. One or more simultaneous sessions can be opened in a scope of one dialogue. All sessions will be closed by the provider in case a dialogue stops.

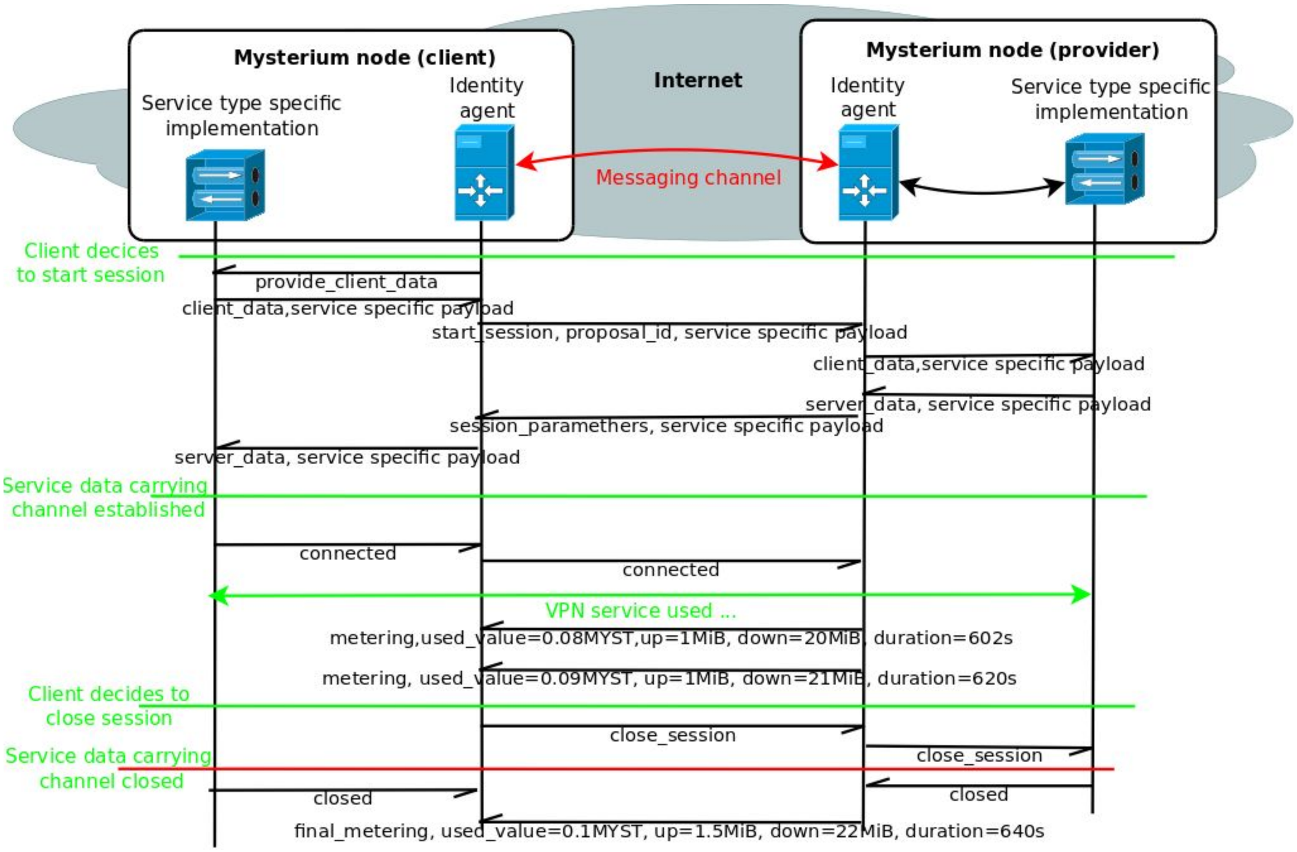

Mysterium node (client)
Service type specific implementation
Identity agent
Internet
Messaging channel
Mysterium node (provider)
Identity agent
Service type specific implementation
Client decices to start session
provide_client_data
client_data,service specific payload
start_session, proposal_id, service specific payload
client_data,service specific payload
server_data, service specific payload
session_paramethers, service specific payload
server_data, service specific payload
Service data carrying channel established
connected
connected
VPN service used ...
metering,used_value=0.08MYST,up=1MiB, down=20MiB, duration=602s
metering, used_value=0.09MYST, up=1MiB, down=21MiB, duration=620s
Client decides to close session
close_session
close_session
Service data carrying channel closed
closed
closed
final_metering, used_value=0.1MYST, up=1.5MiB, down=22MiB, duration=640s

Illustration: Life-cycle of service session

To start a service session a client must request creation of a session. The request must include a service proposal used to discover a service, a correlation ID used to correlate response, and an application specific data. This application specific data should be provided by the VPN service client software. After receiving this request, the provider may respond with an acceptance or refusal. In the case that a session opening was refused, a reason of refusal is also supplied. In the case that the opening of a channel is accepted, a session id is supplied and accompanied by application specific data supplied by provider.

A client should then use application specific information received from a provider to try to establish a data carrying channel(s) and report back to the node. The client node then sends a message indicating confirmation of successful opening of a session or failure to open a session to the provider. If an opening session succeeds, the provider's node starts to send periodic metering messages. Metering messages include information on total cost of the session in MYST, how much data is sent in both directions, duration of the session. If an unused amount value decreases to zero, a provider may notify a node and terminate any open session(s). A client may also request a session to be closed. Upon termination of the session a final metering message is sent.

To be compatible with dialogue semantics a specific service implementation (software) must provide functionality used by the node during setup and tear-down of sessions. When asked by a node the implementation must supply application specific information which may be needed by the provider node before it can supply the application specific data. Then implementation must accept application specific data received from the provider and try to establish its session. After successful establishment of session or failure to establish a session the implementation must notify the node with the results of session establishment. VPN service type implementation must terminate a session on request from the node and should be able to notify a node if the session was terminated by the provider.

Client-server type connection pattern was used, in our example the service implementations may choose any communication pattern to carry user application data

The session parameters negotiation mechanism is limited to client-server exchange of service implementation specific data. Any additional negotiation mechanisms should be implemented in service specific code.

7. Contact

To reach us visit our website at https://mysterium.network/