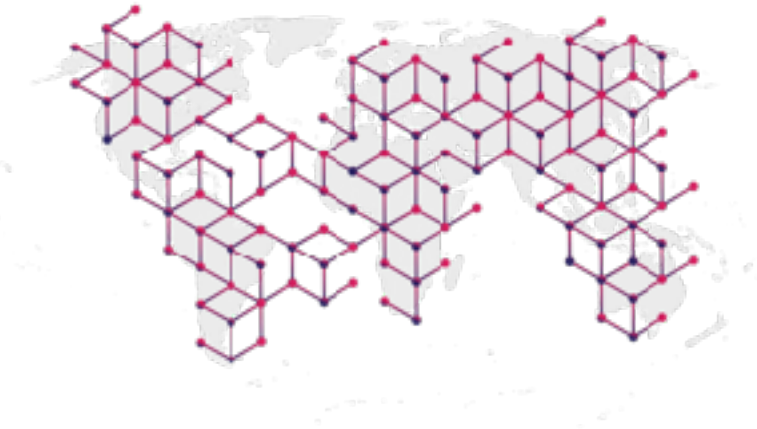
mysterium network

密链网络

白皮书

Draft v0.7



2017年5月

目录

执行摘要 **4**

使命宣言 4

核心目标 5

密链解决方案 5

市场驱动力 6

平台分层 **8**

去中心化服务基建和数据库层 10

服务提供商层 10

服务客户层 10

路线图 **10**

竞争者分析 10

资金细分 10

核心开发 – 40% 11

运营 – 25% 11

市场营销 – 25% 11

法律法规 – 10% 11

开发路线图 11

第1期 11

第2期 12

Token Creation Details **12**

MYST Creation Ratios 13

Additional MYST 13

Future Funding 13

Founders, Foundation, Bounty program and Advisors 13

Seed Participants 14

Example of Token Structure after Creation is over 14

密链体系架构 **15**

技术蓝图 15

主要模块 15

服务配置 16
身份验证服务 16
已注册身份信息 17
加密机制 17
服务查找 18
旧服务公告处理 19
服务标书 19
服务类型 20
服务选择 20
支付 20
账户 21
充值 21
承诺发布 22
承诺结算 22
提现 23
风险控制 24
通信通道 25
对话 25
支付机制 26
服务会话 28
联系方式 **30**

执行摘要

隐私是我们的基本权利，不知不觉 - 我们正在迅速失去。 由于国家，公司和互联网服务提供商的审查制度不断升级，因此必须采取额外措施来保持互联网的畅通无阻的性质变得更为重要。 作为互联网用户，因为受到全世界政府，媒体公司，内容和互联网服务商的审查，我们在使用服务和应用上受到限制。 同时存在能够减轻审查效果的技术措施，但是今天仍然缺乏对互联网用户工具的研究，实施和维护的投入。

随着以太坊和比特币之类的强大点对点技术的发明，加密审查逃避机制的探索可以不受限制地进行，并且以先前难以想象的速度进行。

密链团队相信，建立一个尊重我们隐私的未来，将导致在短期内破坏现有的行业和创造新的行业。 展望未来，我们期望密链网络平台能够为世界上所有公民的获取内容和应用奠定基础，而不用担心审查制度或者某些人的密窥。

使命宣言

“我们的使命是通过分布式，可信赖和可持续的网络来捍卫
所有互联网用户的隐私权和言论自由。”

今天的互联网既不开放也不是私有的。 每当我们不采取应对措施 - 我们的所有行动都将根据我们的物理位置进行监控，跟踪和过滤。 举个例子，如果你不在美国，就无法访问Netflix上的某些节目。 在密链的世界，我们认为这种类型的审查或刺探是不道德和不必要的。 因此我们打算通过开发，提供技术基础和激励协议来生成密链节点网络来解决，由社区持续开发创造出不断发展的审查制度逃避机制。

密链网络的主要目标是创建一个点对点技术，使世界各地的任何人都能够：提供和接收访

问内容，而不被第三方审查。

一些第三方机构是具有合法权力审查某些类型的内容（儿童色情，虐待，非法吸毒，赌博等）这些内容被统治阶级认为对社会有害。 其他类型的第三方机构为了获得更多的权力，运用自身权力进行内容审查。 这种类型的审查通常应用于国家或互联网服务提供商（ISP）的边境。 通过这些技术，可以跨越这些审查的边界传输数据，使用户能够避免这两种类型机构的审查。 因此这有助于犯罪活动保持未被发现和人们之间的沟通：同时传播新闻和知识不受限制。 技术本身是无偏见的。
另一个第三方机构 - 可能内容提供商根据你的物理位置限制访问内容，因为受限于使用内容的知识产权协议，营销的阶段策略，或只是因为对“眼球”的价值的低估，这是广告网络公司经常遇到的情况，还有许多其他原因。 尽管以你的住址为进行审查，但推行这种逃避审查技术是一种积极的不服从形式，表明我们愿意抗衡这种类型的审查制度和不公平待遇。

我们花了很多时间讨论创建密链工具的道德问题，引起避免审查，并相信手段的代价（审查内容）最终不值得（假定较低的犯罪率，较高的公司利润，更强政治权力等），因为这些目标可以通过其他更多的道德手段达到。 大多数解决方案都是审查员熟知的，有效的过滤用于限制访问，例如机器学习就是审查员用于研究互联网使用模式和检测非必要行为。

核心目标

第1期: 构建一个由VPN节点组成的去中心化网络
第一个目标是通过使用现有的VPN和代理协议，以太坊区块链，智能合约，状态路由，去中心化数据库解决方案来构建去中心化的VPN节点网络，加密数字货币像Monero或Zcash等

这将在第1期的开发中实现，该期由3个不同阶段组成（见路线图）。 在第1期的第3阶段结束时，一个完全去中心化的开源的功能也去中心化的VPN网络将被发布。 从此没有单点故障。

第2期：构建密链协议 - 作为标准

在第2期 - 我们的愿景是构建密链协议，能够“拆解”用户数据并将其发送到密链节点网络里，无可能追踪或审查。该网络将以无法识别的形式向接收端发送切片和加密数据，密链协议将确保该用户数据会再次“重新整合”。
密链协议最终将成为把不同元素组合成一个相关联系统的组合。
一旦完成该协议，将确保用户数据不能被节点或第三方得到。

密链解决方案

密链旨在完全去中心化，点对点和无服务器节点网络，为其用户提供隐私恢复技术，并为其节点运营商（提供商）提供财务激励。 密链通过利用已经存在的技术实现了这一目标，如以太坊块链链，智能合约推进它的状态路由和承诺机制的功能，加上社区开发的审查逃避协议作为网络上的应用。

一旦第1期第1阶段开发完成和发布 - 该网络将保护用户隐私和数据，同时使所有用户分享他们多余的带宽给有需要的访问，以换取经济收益。

密链网络将成为服务商和客户之间的去中心化市场，并参与创建和维护此基建。 服务商的费用将由消费者使用加密货币支付。

技术的研发，其功能将分为几个阶段以最小化风险。从早期经验中学习，并从附加技术（例如状态路由）的开发中受益。 所有去中心化的功能和维护将在第1期的第3阶段最后部分完成（见路线图）。

密链众筹的参加者将会得到相应代币，这将成为该网络中所有交易的基础代币。 密链部署后，我们的网络将为企业和社区的不同层面开发提供机会。 网络将开放给应用，使审查效果更差，使支付更简单高效，新的网络相关服务将会由密链基金会通过重用基建和协议开发实现。

密链网络中的VPN相关服务将在第1期的第1阶段后实现。 这一阶段的网络VPN服务将会改进现成的中心化虚拟私有网络服务。密链市场模式创建一个既具有竞争力又几乎无限扩展的VPN服务，其他实体（例如其他VPN提供商或应用开发者）可以从网络购买VPN服务，将其集成到它们的解决方案中。 这种竞争力来自网络的开放性，任何人都可以通过作为VPN服务提供商从而获得收益。 后续阶段将进一步改进和开发新的应用，在第3阶段

结束之前完成去中心化。

市场驱动力

我们每天的大部分时间都花在网络上，这样会造成更多的漏洞使我们的数据被窃取，被入侵，过滤或滥用。

研究显示这些是主要力量，正在为互联网隐私和安全解决方案创造不断扩大的市场：

1）政府立法

有一个明显的趋势，政府正在更多的侵入我们的私人生活。 随着我们的时间越来越多的在互联网上 - 这个趋势正越来越显著。

2）西方国家习惯了VPN服务

目前，很多位于东部，东南部的国家使用VPN。但近期政府政策变化之后，西方世界寻求互联网隐私解决方案的人数正在迅速增加。

3）网络威胁的风险增加

每年都有网络攻击的增加，人们从而意识到需要采取对应措施。 公司和个人倾向于投资和改变他们上网行为从而导致VPN市场的快速扩张。

4）自由职业者需要与企业服务器的安全连接

每年都有更多的工作由自由职业者完成。与企业服务器建立安全连接成为必须，但是对于小型企业来说，创建自己的VPN是一个有挑战性的成本。

美国国会推翻互联网隐私条例之后的*VPN*使用趋势图

牢记当前的世界形势和明显的趋势，越来越多的人越来越关心他们的隐私。 据研究报道，广告拦截器的使用量已经增长了40%以上（总共1.98亿月活跃用户）。 在最近联邦通信委员会（FCC）的法规更改后，在美国对隐私解决方案的搜索已经飞涨。

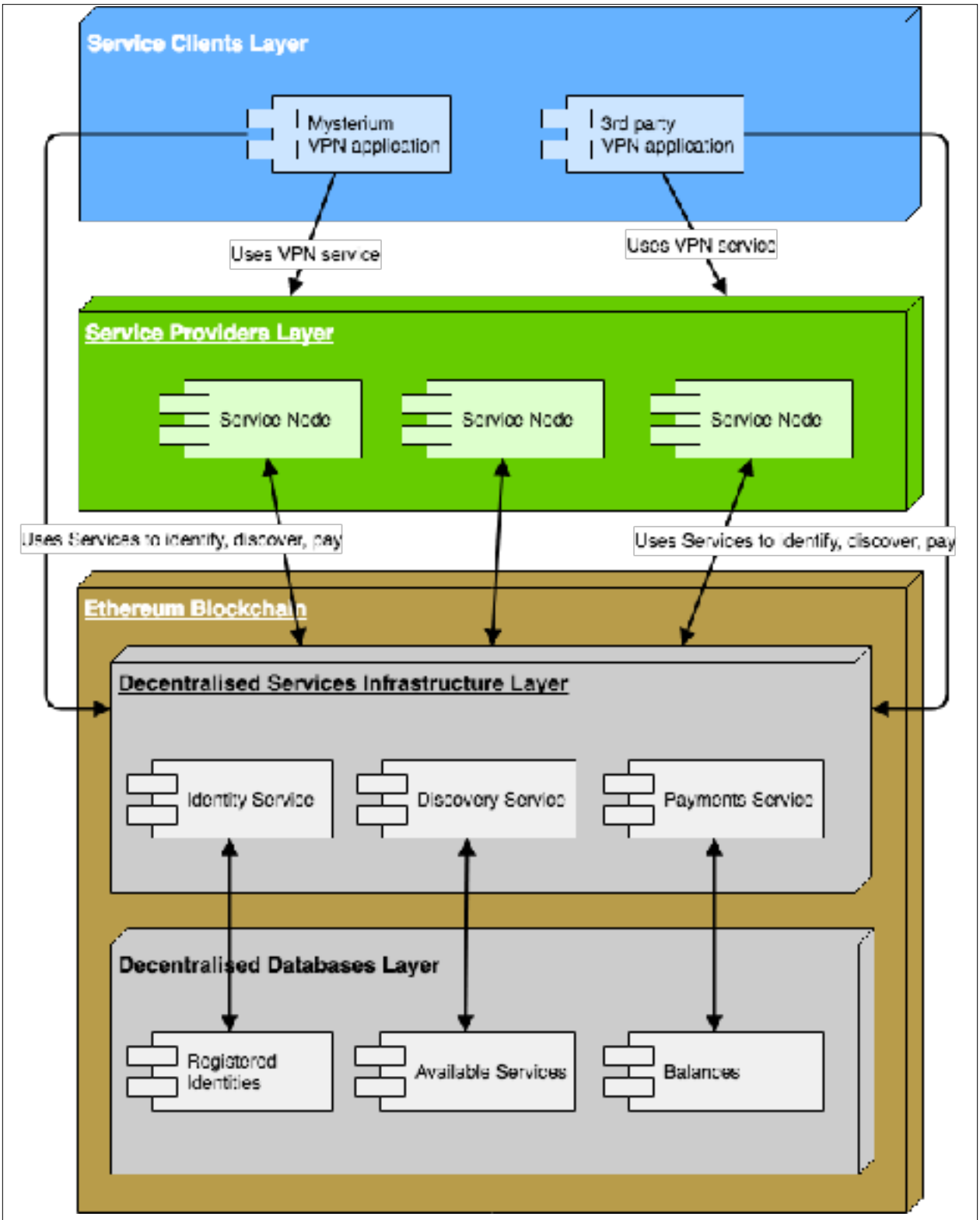
根据这个报告:

“预计到2022年底，全球VPN市场将达到1060亿美元，复合年增长率为13%。

VPN可用于向私有和公共网络如WiFi热点和Internet提供安全层。 在医疗保健，BFSI和电信行业运营的组织处理着非常敏感的信息，需要时刻保护，黑客主要针对这些行业，因为数据在黑市价格非常高。 一项研究显示，“目前，世界正在每分钟经历50多万次攻击”，随之而来的是由于高科技的发展。”.

牢记这些趋势（多个国家在互联网上的隐私政策变化后的需求，增加的网络犯罪，互联网事务和日益增长的对在线服务的依赖）恢复互联网上隐私的需求正在成为对个人自由和到商业安全的严重问题。 恢复隐私已成为全球清晰可见和全球化的趋势。 一旦开发完成 - 密链网络将帮助你恢复你的隐私，为你个人和商业生活时给予自由和安心。

平台分层



密链网络将由4个主要层级组成：去中心化数据库，去中心化服务基建，服务提供商和服务客户。

去中心化服务基建和数据库层

密链去中心化服务基建和数据库层提供基础智能合约以启动密链节在网络中识别他们自己，相互发现和在节点间发送微支付。

服务提供商层

密链服务提供商层由密链节点来充当VPN服务提供商。

服务客户层

密链服务客户层由密链网络客户应用组成。由密链和第三方服务提供商开发。

路线图

竞争者分析

以下表格对比了典型的VPN提供商，Tor网络和密链

	中心化VPN提供商	TOR 网络	密链
匿名	否	是	是
去中心化流量路由	否	是	是
端对端加密可能性	否	是	是
蜜罐风险	高	低	低
网络参与者激励	否	否	是
开源	否	是	是
速度	高	低	高/中
PSSA	否	否	是

资金细分

生成代币得到的资金将会用于开发和密链网络补益。以下是资金初步分配方案，以后可能更改。

核心开发 – 40%

核心开发将会开发本文档提到的技术。包括：密链节点网络，与VPN协议的集成，智能合约系统，支持的协议和服务，用户应用。。

运营 – 25%

这包括一个功能系统必要的开支。包括：托管和基建费用，工资，外包，管理和其它相关花费。

市场营销 – 25%

市场推广成本将会用在开发合作伙伴和直接客户当中。营销成本将大部分在直接的B2B销售当中。

法律法规 – 10%

这里有法律费用，用于保护隐私和抗衡审查。法律费用将在不同地区而不同。

开发路线图

整个开发分为第1期和第2期。每个阶段进一步拆分为几个阶段。

第1期

第1期组件：

- 发现机制 - 节点和客户之间智能合约

- 智能合约管理密链身份
- 支付机制状态路由和智能合约结清的组合
- VPN节点协议和库 －网络的“工作室”，提供VPN服务给客户
- 节点应用 －主流操作系统上建立原生节点应用，能够运行密链协议和提供VPN服务给客户
- 客户端应用 －允许用户以VPN用户身份连接网络
- 为第三方应用提供的网络接口

本期将以3个阶段完成。

第1阶段

第1阶段开发目标:

- 智能合约用于支付结清
- 密链节点V1.0 - linux版本
- 密链节点V1.0 - 3个主流操作系统的版本
- 密链客户端与3个主流操作系统的版本
- 密链中心服务器，用于节点发现，身份管理和微支付会计处理

第2阶段

- 密链节点V2.0 - 增加新协议，用于所有操作系统的开发，与新智能合约集成
- 密链客户端V2.0 -
- 智能合约，用于发现和身份管理
- 简单中心服务器 －仅用于微支付会计处理

Stage 3

第2期

第2期的目标是开发密链协议作为标准，能够“拆解”用户数据并将其发送到密链节点网络中 - 提供端对端加密。

更多第2期的细节将会在这个文档的最终版本中出现。

代币创建详情

代币（MYST) 将于2017年5月30日开始创建。

- 可以试用以太币，比特币及法币兑换MYST.
- 代币兑换顶格（软顶）为6百万瑞士法郎（CHF) , 这个数字在代币正式发售前可能会有变更
- 代币创建为期14天
- 如果在14天结束前到达顶格（软顶），将接受顶格后24小时内的捐赠，给错过MYST代币创建的用户额外的机会
- 最低预期是70万瑞士法郎，如果未达到，则退款。
- 代币创建将设置硬顶：一旦达到硬顶，代币创建自行停止，不再继续。硬顶额度将在代币创建前一周确定。

MYST 代币创建比例

- 软顶前, 1 CHF = 1.2 MYST.
- 软顶后 (24 小时自由投放), 1 CHF = 1 MYST.

其他 MYST代币

会有额外MYST代币生成，以用作：未来融资，基金会，奖励，顾问费用，以及种子轮代币。

未来融资用代币

一部分MYST代币将预留用作以后融资供密链第二阶段开发，但也有可能永远不增发，全凭未来显示状况而定。

未来融资预留数额如下：

- 如果首次融资2百万瑞士法郎，则50%预留用作未来融资
- 预留比例根据融资额度递减，知道融资额度达到6百万美元，预留比例递减到15%.

- 6百万美元之后，未来融资预留部分则固定在15%.

未来融资预留代币锁定期为12个月，到期发送到多重签名地址。

创始人，基金，奖励计划，及顾问

- 基金，奖励计划，顾问将拿到9%。 代币由基金的多重签名接收，用来奖励来自于各方的帮助贡献：早期节点运营方，奖励计划参与者，顾问，新员工等。
- 创始人将获取10%代币。锁定期12个月。

种子轮参与者

种子轮参与者将在代币创建开始后根据所投ETH/CHF额度按以下倍数获取代币。

- 1x if 2 million CHF (or less) is collected. 募集2百万瑞士法郎则为1倍（1比1）.
- 高于2百万CHF至6百万CHF区间 线性递增倍数，从1倍到5倍。
- 6百万及以上都为5倍。

代币创建结束后，代币结构示例

因为种子轮以瑞士法郎计价ETH，在此示例中1ETH相当于50CHF。

Contribution, in CHF	**2m**	**3m**	**4m**	**5m**	**6m**	**9m**
Contribution participants (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%

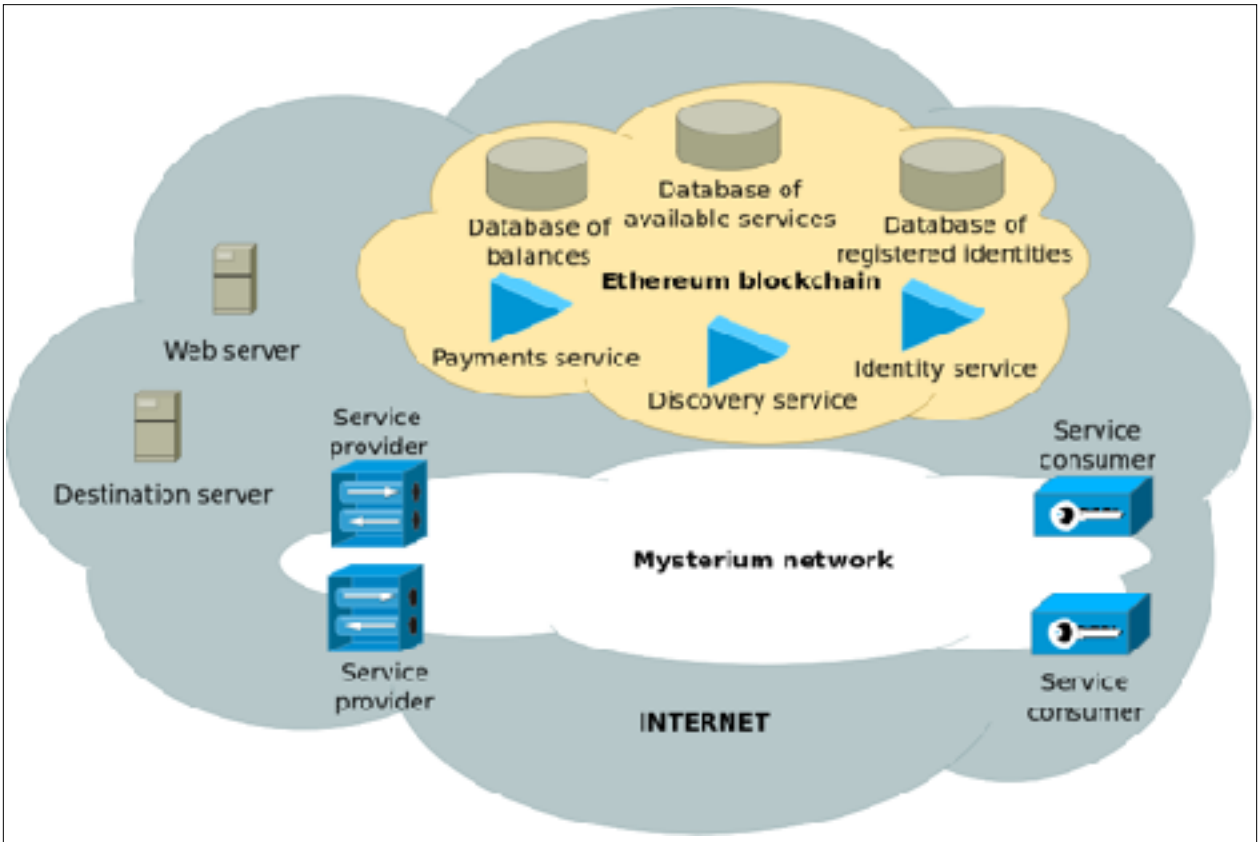
Seed Participants (locked)	3.40%	5.70%	7.70%	9.50%	11.40%	8.50%
II'nd Phase (locked)	50.00%	41.25%	32.50%	23.75%	15.00%	15.00%
Founders (locked)	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

密链体系架构

密链仍然在持续开发中。本章节部分内容将有更改。

技术蓝图

从鸟瞰图我们可以看到，VPN服务提供方发布VPN服务，用户从已发布VPN中选择合适的服务，并在事后付费。密链网络实现认证用户和服务提供者，发布及检索服务，进行结算。 密链网络本身在互联网上运行，并依赖以太坊网络实现抗审查分布式存储和结算。密链网络在服务和结算中通过注册帐号来实现限制性的信任机制。



密链鸟瞰图

任何在密链注册的用户都可以发布VPN服务（需要兼容密链网络协议）．发布之后，即可定价并确立支付条款．网络的其他用户可以根据条件（区域，价格等）检索合适的VPN服务，在查询结果中挑选服务提供者并连接使用该服务。VPN购买方和服务提供方可以互发信息讨价还价，询问技术细节以保证建立安全的VPN连接会话．在协商谈判中，VPN用户承诺为提前得到的服务付费，并在每次续期时进行更新。VPN提供方通过以太坊智能合约在服务期满时根据该支付承诺进行结算。 如果用户在密链网络账户余额足以结清支付承诺，对应金额将从用户账户转移到服务方账户。

主要模块

1. 以太坊 可以通过智能合约执行去中心化的代码，激活可靠的服务和支付。
2. 身份验证服务和已注册身份的数据库 确保用户和服务方之间得到验证。
3. 发现服务和可用服务的数据库提供发布可用的VPN服务和选择最合适的VPN服

务。

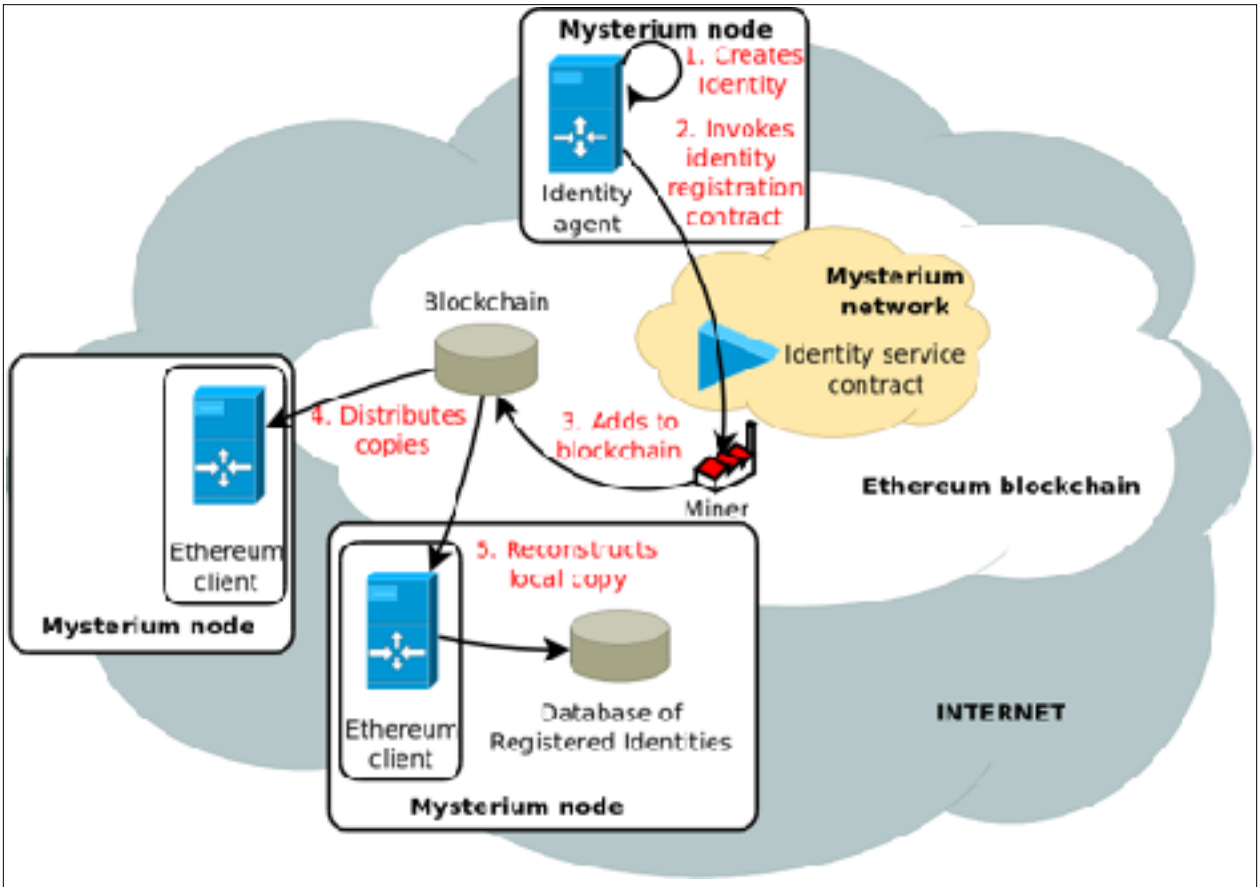
4. 支付服务和结余数据库 在服务中允许安全的以承诺为基础的小额支付。

服务配置

当一个用户（一个服务消费者）在密链网络中需要VPN供应方提供的VPN服务，他们必须先挑选一个符合他们需求的服务。当一个服务被挑选之后，客户端将开启一个对话框并提供身份信息给这个发布的服务。在对话期间，价钱可能会得到承诺并且VPN会话可能会得到配置。对话可以在现成消息频道或新建的频道中开始。对话将在其中一方停止接听另一方或任意一方断开网络连接后结束。

身份验证服务

与互联网连接的软件代理（在这里叫做身份代理）代表数字身份。每个身份代理代表某个人来控制自己的身份。该软件代理是连接密链网络发布或使用VPN服务的功能实现部分（密链节点）。每个代理都能获取数字身份，能够通过使用与身份关联的密钥签名并解码所有通讯。一个节点可能有多个身份。通过生成密钥和公钥创建身份。通过公钥计算其keccak256哈希值得到的最后20个字节导出的唯一标示符来验证身份。通过在以太坊网络调用身份注册智能合约进行发布，使其他网络用户获悉其存在。合约中必须提供标示符和公钥。身份合约成功执行后，身份公钥即被矿工添加到以太坊区块链。至此，写入区块链的身份即称之为已注册身份。所有密链节点遵循区块链，读取新注册身份的交易，并维护着包含所有注册帐号交易信息的本地数据库。节点使用包含注册身份信息的本地数据库检索与其身份关联的公钥。节点使用该数据库检查从其他节点而来的通讯是来自可靠已注册身份并进行合理签名。



身份数据注册及复制

已注册身份信息

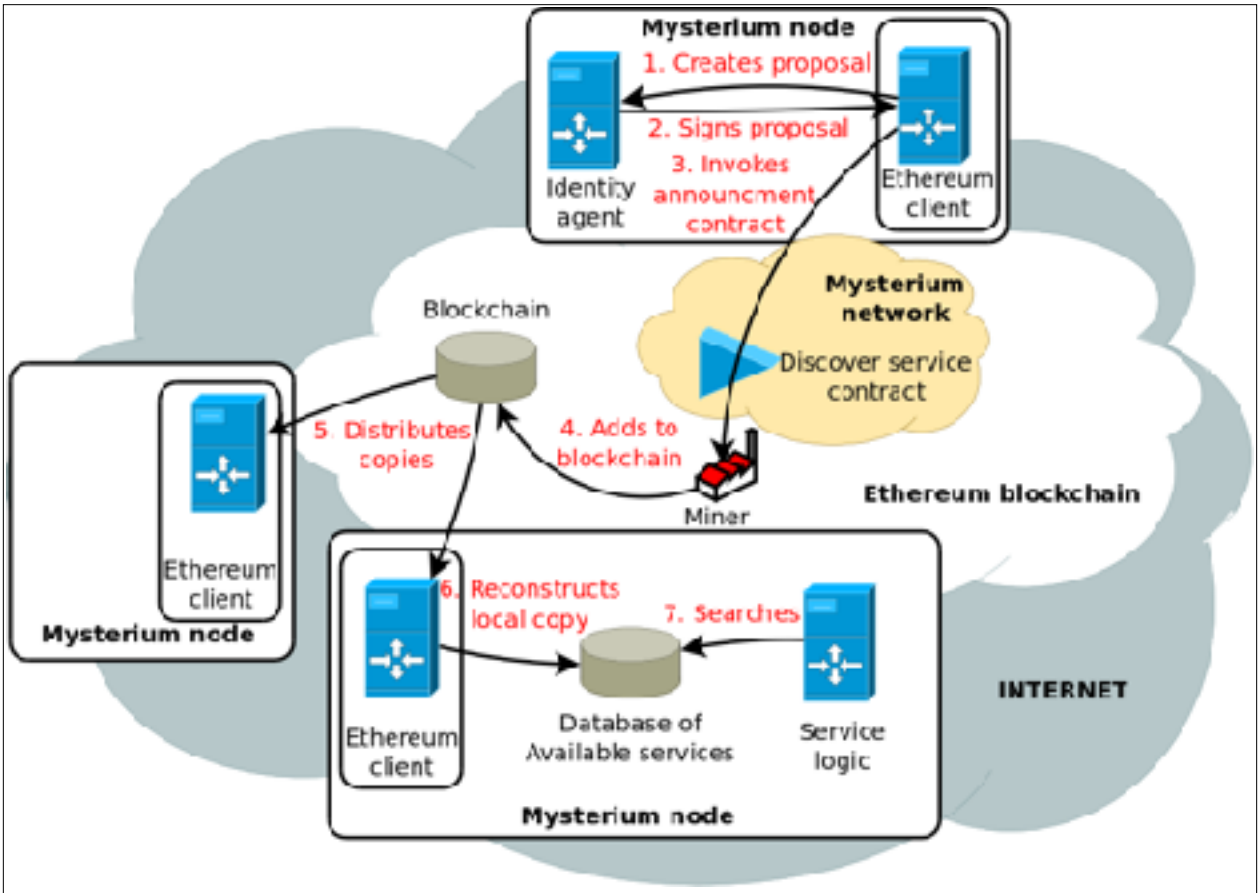
密链网络节点必须包含预设的金额（MYST）来成功调用身份注册合约并进行身份注册。该金额会定期根据MYST与法币值变化而进行调整。这种预设值使身份注册具有价值。身份注册具有一定成本可以防抛之不用（因为需要花钱）并且创建大量身份需要开销（减少利用信誉等级作恶）。我们把你的已注册身份看作是可重复使用的有益资源。重复使用身份进行支付结算，会留下支付记录，公开账户余额，并获取VPN提供方的信任。我们将在支付环节讨论风险与信任之间的关系。

加密机制

因为考虑到EVM的计算成本，以及运行长计算方面的局限性，实现身份注册的加密学机制将采用EVM本身的keccak256哈希算法，ECDSA签名验证，以及标识符恢复功能来实现。密钥对，及身份后的标识符与以太坊外部账号的加密学逻辑完全一致。密链的密钥对不能在以太坊主网使用。

服务查找

VPN提供方希望提供服务并获取收益，那就可以在网络中发布服务。提供方发布服务需要准备服务标书。编入格式版本，提供方描述，服务定义，连接节点的方法列表。服务提供方的身份代理签署该标书，并且节点在以太坊网络调用一个服务发布智能合约。矿工运行合约并把该标书加入以太坊区块链，即可被公众查看和拷贝。密链节点跟踪区块链，复制包含该标书的交易，记录出现该交易的以太坊区块数。节点随后从该交易中导出标书，并使用导出标书建立和存储含有网络上所有服务的本地数据库。节点可以检索本地数据库或者其他可信节点数据库寻找符合特定要求的服务。



*VPN*服务发布和检索查找

旧服务公告处理

加入区块链的标书将永存，但服务发布却不一定长期有效。为了去掉过期标书我们定义以下用户行为：用户将预定义区块前的所有标书进行放弃（比如60000块，大概需要十天），VPN提供方需要在旧标书被抛弃前重新发布服务。VPN服务提供方重新发布使用相同序列号的服务，所有网络用户用从区块链获取的新标书替换本地数据库存储的旧标书。这个简单的方法保障没有过期VPN服务淤积。

服务标书

如前所述，一个标书需要编入：标书格式版本，服务提供方描述，服务定义，以及联系节点方法。版本号实现标书格式扩展。服务提供方描述包括服务方身份及相关服务序列号。序列号可以在更新节点联系信息时候重复使用，但一旦任何参数变化（包括单价变化），就需要更新为一个新的值.

服务定义包括：1.VPN服务种类定义；2. 服务提供方地域的大概信息；3.VPN服务通道流量来源大致区域；4. 每个会话带宽；5. 服务使用及计费方法，MB/MYST 或 秒/MYST.

服务类型

密链网络上将会有数种独特的VPN服务。IP隧道和Sock Proxy代理类型将首先实现。其他相关服务将一一添加。大概位置将根据接入点编入ASN和ISO 3155 Alpha-2国家代码。大概位置可作为快速查找特地VPN服务方的搜索条件，或进行精确到国家水平的查找。连接服务方节点信息列表是服务方节点支持的协议列表及协议的具体数据。该列表包含一些强制提供的信息，以便实现默认节点对节点协议，包含关联IP地址，port信息等。

节点可以支持多种VPN服务，每个服务类型按不同服务进行推广。节点长期保存发布的标书并认为有效。有效标书是服务方愿意以预设条约进行服务的标书。

服务选择

每个客户都可以在密链网络中自由选择不通的服务。一个VPN客户通过本地的或可信的远程数据库中搜索符合他们需求的服务：服务类型，服务提供地区，你的流量将从哪出现，测量单位，最高单价和提交的带宽。

所有符合需求的服务将会以价格从低到高排列，可以按照价格从低到高的顺序尝试建立服务连接直到功能对话框开启。客户可以选择使用在曾经用的服务商中被标记的优选服务商，即使其价格高于当前可选的最低价格。 当客户选择了一个服务后，下面的事件将会发生：一个连接客户与服务商节点的对话框将会弹出，一些承诺费用将会扣除，连接将会建立直到使用完毕。若对话框建立失败，下一个最佳服务商的对话框将会手动或自动建立。

密连客户端可以在选择服务商的过程中提供一系列的自动化协助。逻辑与界面可因客户端软件的不同实现而不同。远程数据库查询功能和信任机制仍未定义好，将会进一步研究和设计。

支付

密链网络将采用状态路由支付方法，它是基于信用的一种支付方式。这种方式有点类似支票支付。举一个简化的支票支付例子，一个银行账户持有人可以给另外一个人签发支票作为付款方式。支票上有签发人的姓名，收款人姓名，应付金额。这些信息由签发人书写并签字。在银行里，收款人可以用支票换取等额现钞。如果签发人余额不足以支付该款项，则银行拒付并退回支票。

密链网络中，以太坊上的智能合约就充当了银行的角色。所有密链用户都有一个智能合约管理的账户。用户在账户中存入代币（MYST）。当用户需要使用VPN服务，即可作出承诺：使用存款来购买服务方的VPN服务。VPN提供方收取付款。提供方向智能合约提出将一定金额从使用者账户转入提供方账户的请求。所有价值传输将被记录在册，余额信息记录在合约状态中。使用者也可以请求合约进行提现。

我们分阶段详述价值传输流程…

账户

我们要在以太坊上开发和部署智能合约，用来管理用户账户并进行价值传输。一个合约既可以存储所有密链账户的价值。所有合约执行交易被写入以太坊区块链。交易包括充值，支付结算和提现。使用软件的人都可以查询写入公共区块链的交易，并更新任何账户状态。例如服务提供商或许希望查询用户账户余额以确保用户有足够余额进行支付。

充值

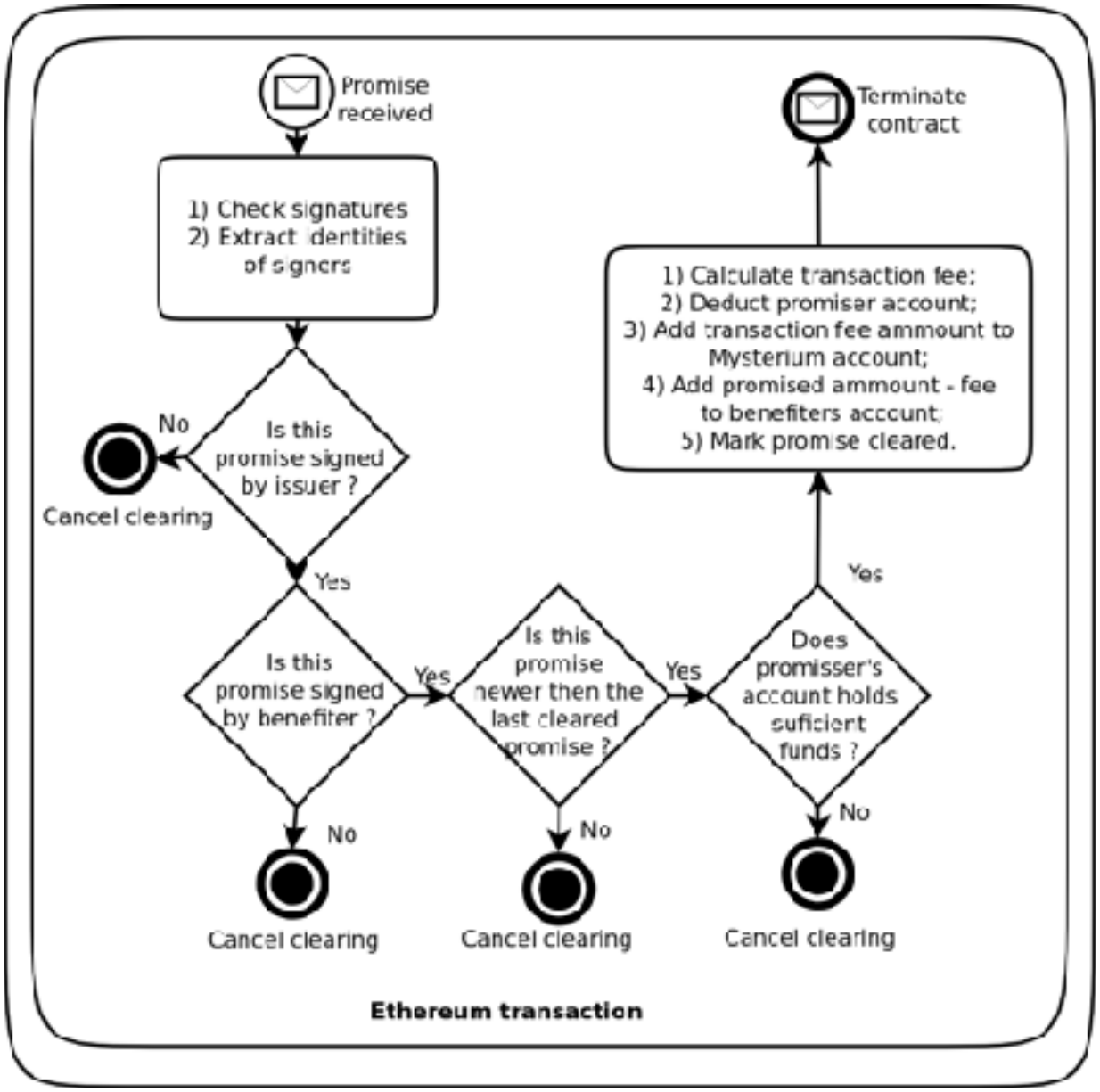
任何密链用户可以通过密链支付合约给账户充值MYST。为进行充值，用户需调用合约，提供收款账户标识符。成功执行合约即可将相对应价值MYST计入账户余额。

承诺发布

承诺是签发者承诺付款的二进制表示编码，包含签发方的标识符，承诺序列号，收款方（受益方）标识符，以及承诺支付金额。当用户需要支付时，可以发布新承诺，或者更新现有支付承诺，并发送给收款方。每个支付承诺都会被分配一个特有序列号，并且每增加一个新承诺，序列号随之增长。发布者和受益者之间必须确保序列号的唯一性。增加付款额度时承诺也随之更新，但其他组成参数保持不变。承诺受益方可以请求发布者停止更新承诺，并于下次支付时发布新承诺。每次承诺发送给受益方时，都经过发布者数字签名。接收到承诺后，受益方应当检查是否有效。有效的承诺含有发布者的数字签名，具有比上一次承诺更高的序列号，根据请求进行更新。

承诺结算

要收取支付承诺中的价值款项，必须进行支付承诺结算。用户对密链网络支付合约提出清算请求。在相同发布者和受益者交易对中，结算顺序序列号靠前的承诺优先于靠后的承诺. 发布给合约的清算请求需要包括: 来自于发布者的承诺，发布者的数字签名，受益方的数字签名。两者签名表示双方同意该笔价值传输。



支付承诺清算

当执行智能合约时，会检查封装的履约承诺是否被签发者和受益方正确签名。首先验证签名和从签名中抽取标识符，然后将抽取的标识符与承诺中设定的标识符做对比。如果承诺非签发者和受益方签署，清算会被取消。如若不然，清算继续进行，通过合约代码检查清算是否已经执行过。支付合约使用状态存储方式来存储上次已结算承诺序列号。该存储信息对每个发布者和受益方交易对都具有唯一性. 简单的对比序列号足以确定承诺是否在之

前已经结算。

如果出现已经结算过的情况，结算随之取消。如果未结算，检查支付发布者余额是否足以支付该笔款项。 如果余额不足，清算取消，但并不意味着承诺价值失效，受益方可以选择待发布者充值后再进行结算。最终，如果发布者账号余额足够支付，则清算完成。承诺中定义的价值从发布者账户扣除，计算出一笔小额转账费用计入密链网络，剩余部分计入受益方账户。然后一个支付承诺序列号存入合约状态，所有清算流程结束。调用支付合约时受益方或许要求，即使发布方账户余额不足无法完全履约，会有所损失的情况下，合约仍旧执行清算。

提现

密链账户持有人都可以将本人账户余额提现到任何以太坊账户。要进行价值传输的用户必须启动密链支付合约并提交签名请求。请求内包含账户持有人标识符，和外部目标地址。合约执行后，检查请求是否为账户持有人签名，账户中是否有足够余额完成支付请求。如果通过检查，对应价值完成传输。否则不予执行。

风险控制

支付承诺并不能保证支付履约。承诺中写入的金额并不局限于用户账户余额，可以是任意金额。所有被用户签名的支付承诺在清算前都有效。这就意味着如果用户给其他密链用户做了虚假承诺，其将无法再安全使用其身份。做了虚假承诺的发布者一旦充值，任何具有有效承诺的提供方即可获取对应金额。创建注册身份需要一笔费用，如果违约，身份即毫无价值。失去注册身份价值的代价可以防止用户发布虚假承诺。建议的支付方式应该仅限于交易金额是注册身份价值的一半。

所有支付合约的交易存储在以太坊区块链的公共账簿中，因此人人可以读取。每个人可以重建所有交易流水，查看所有注册身份余额，并且可以追踪所有支付承诺以及承诺中的序

列号。这就意味着任何人可以在接受你的支付承诺前查询你的余额并且浏览你的支付历史记录来评判你的信用度。

在清算交易成本方面也有风险和收益的平衡。通过智能合约进行支付有gas和交易费产生。有些服务提供方可能会选择禁止用户以更高额度更新支付承诺，并且在成本占履约的价值比例较高情况下尽快对承诺进行结算。其他服务提供方可能愿意承担高风险，允许积攒更多承诺价值，使清算成本占清算价值比例微乎其微。

接收到的支付承诺（还未被受益方签署）可以与其他用户分享，无需担心与之相关价值流失。与其他服务提供商分享对比接收到的支付承诺对于降低风险至关重要，可以预警防范余额不足的用户，以及向多个服务提供方做出大量虚假承诺的用户。

我们的支付解决方案给出足够的信息来评测风险。也给了用户降低清算风险及提高清算成本之间权衡的自由。

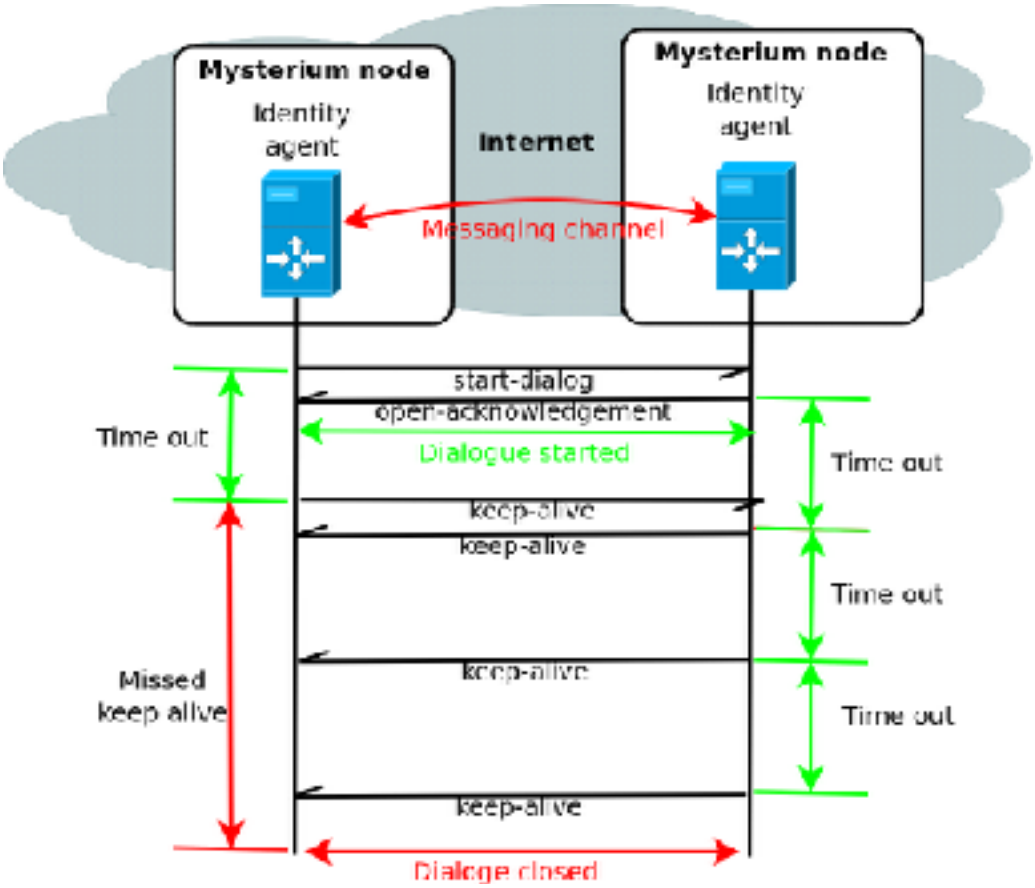
通信通道

通信通道使节点交互信息。有多种通信通道，每一种都采用不同的协议和通讯机制（直接的点对点，中心化服务中继，P2P Overlay中继）。节点间对话可以在任何双方参与的通信通道方式中进行。密链网络客户端会设定和支持一种默认通道方式及相关通讯协议。将会添加其他通道方式，以有效对抗实时网络中的审查手段。通信通道可提供不可靠数据报通讯界面。有些通信通道模式会采用传递信息路，从而需要做好保障通讯数据安全的措施。通道中发送的每条信息都由发送方签名并使用椭圆曲线加密法加密. 这种保护信息方式可避免窃听危险，但仍有暴露通讯双方身份的危险。

对话

对话机制打造了两个身份（节点）之间通讯用来实现支付的信息和建立服务会话。在任何一个时间点，两个身份间只能存在一个对话。尝试建立新对话，则上一个对话结束，新对

话建立。通过对失帧信息采用简单的肯定应答机制，从而在非可靠通讯通道中提供可靠的信息传输.



对话生命周期

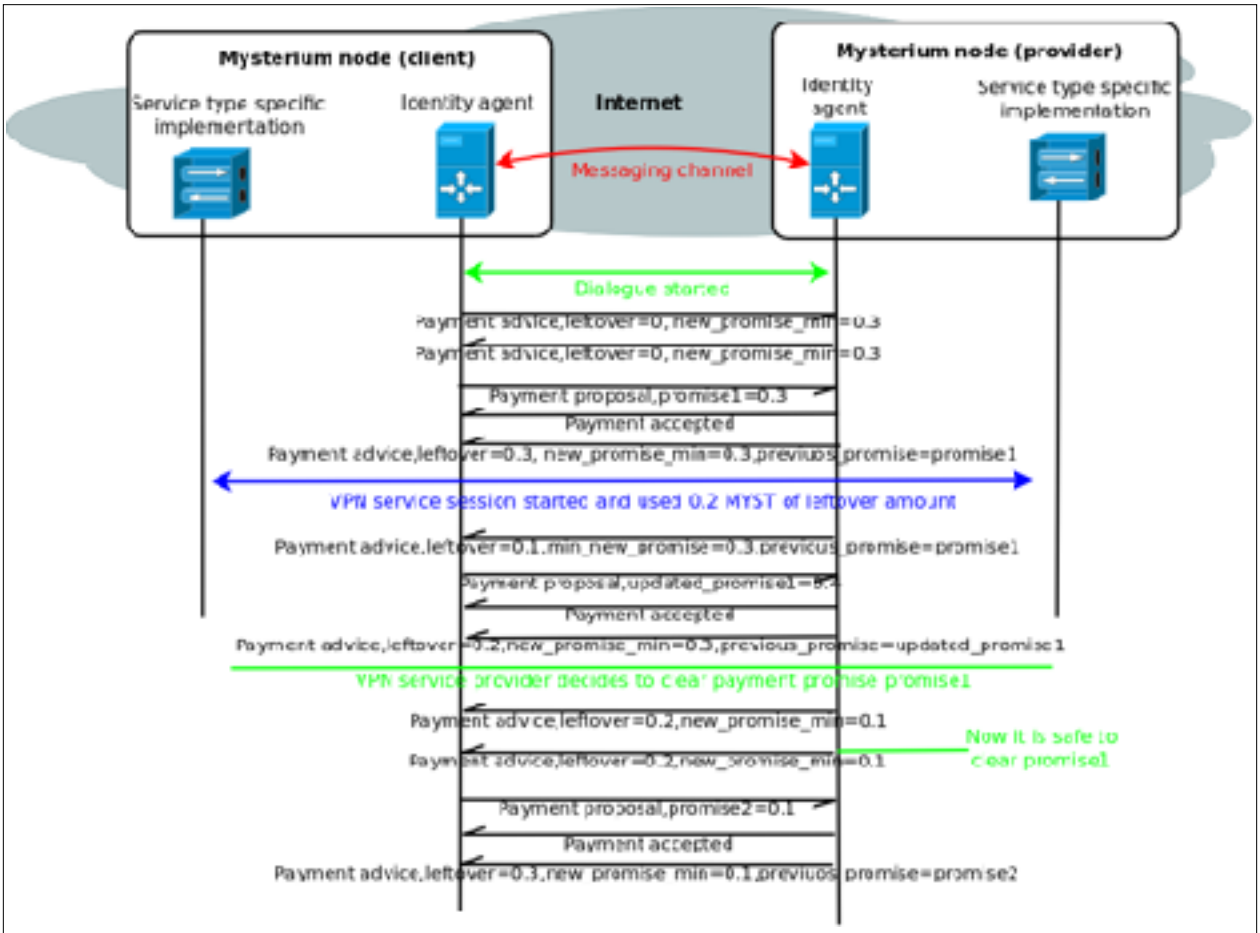
当一方身份要求另一方身份开始对话，另一方接受对话建立请求时，对话即开始确立。为保持对话，需要定期进行信息交互。如果一个节点没有相关有意义信息发送，则可以发送keep-alive信息。身份代理监视上一个对话信息接收时间，如果长时间没有信息接收则关闭对话。一个身份可以通过忽视远端身份发来的信息而终结现有对话。

支付机制

身份代理在节点存储状态信息。状态中记录与之成功建立对话的身份。记录数据包括：节点接收到但并未用于支付对应服务的MYST数量，从对方节点接收的最后一个支付承诺和所有未结算承诺列表。选择存储状态信息可以使VPN服务提供方降低支付承诺结算成本。对话建立之后，双方身份尝试查找远程身份的状态信息，每个身份代理向对话对方发送支付建议。支付建议是双向发送，因为身份关系是对等的，也有双方身份同时使用对方提供服务的可能。

支付建议包括已经收到但还未用于支付的MYST，对新发布支付承诺的支付条款描述，以及可选的请求对已发送支付承诺进行更新而非重发新承诺。有些服务提供方可能会因为测试目的选择免费提供服务。这就需要通过告知对方第一次使用其服务只需要有高于零的余额即可实现。支付条款要显示远程节点能接受的支付承诺中最低MYST额度。

更新承诺的请求包括上次未结清承诺的备份。支付建议在以下时候由节点发送：a) 尾款与前述金额发生超过10%变动； b) 尾款达到0; c) 服务提供方决定结清最后一笔收到的支付承诺; d) 服务提供方接收新的或者更新支付承诺。在对来自于对方最后支付承诺进行清算前，服务提供方需要发送支付建议通知对方，并且确保清算前成功抵达。通知须要避免对方发送更新版的支付承诺的同时，之前的承诺版本已被送往清算。

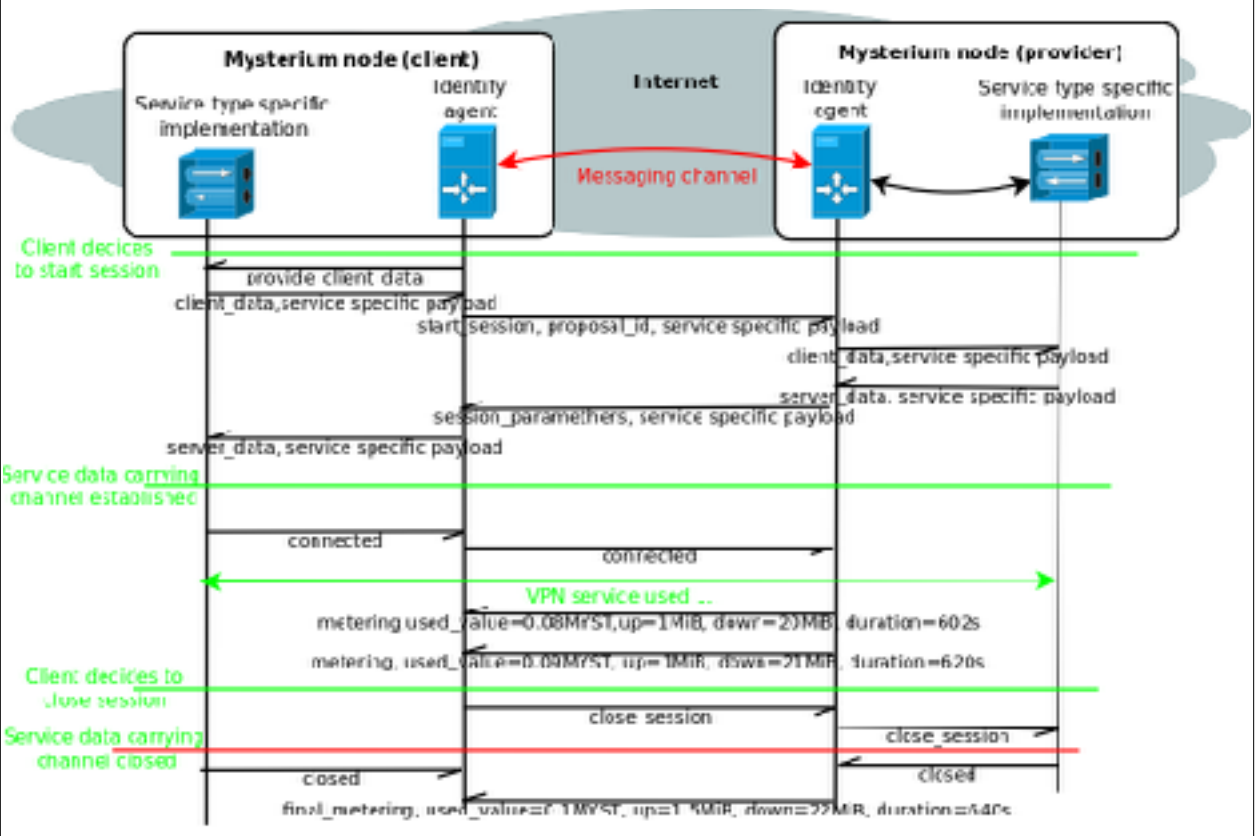


通过支付承诺提前支付

为了更简单的讲解，我们来设想一个身份正使用对家身份（服务提供方）提供的VPN服务。为了提高被服务提供方跟踪的尾款（余额），用户必须发送支付提议。支付提议是发给对方的一个信息，其中包含支付承诺。服务提供方接收到支付提议后，需要认可该提议为有效。如果支付提议不可接受，则发送负面响应。负面响应也要给出拒绝原因。客户应使用服务提供方而来的支付建议，如建议中有可选项，可对现存支付承诺予以更新。如果没有建议可选项，在下一个支付提议中必须有新的支付承诺。客户可以选择忽视建议，发送包含可被对方接受，具有足额以太币承诺的支付提议。

服务会话

要成为一个有用的VPN服务工具，必须要有针对用户应用的接口，和用来提供节点的数据承载通道。接口因服务类型而不同。如果选用IP隧道服务则表达为IP接口，如果选用安全套接服务，则为对本地IP地址的套接侦听。数据承载通道用来承载用户应用产生的流量，并且因具体应用而不同。密链网络将支持很多VPN服务模式，因此发送给服务会话的信息必须有足够大的灵活度承载应用特定类沟通信息。使用某个服务，节点就必须要支持该VPN服务类型。支持方式或来自于节点内置功能或来自于节点软件插件。在同一对话里可以同时开启一个或多个会话。 如果一个对话结束，服务提供方将终止所有会话。



会话生命周期

开启服务会话，客户需要请求建立会话。请求必须含有用来发现服务的标书，一个用于相

关回应的ID，和应用特定类数据。应用特定类数据应当由VPN服务客户端提供。接收到请求后，服务提供方接受或者拒绝。如果出现会话拒绝情况，需提供拒绝理由。如果接受打开通道，需附上会话ID，和服务提供方提供的应用特定类数据。

客户应使用来自于服务提供方的应用特定类数据尝试建立数据承载通道并报告给节点。客户端节点发送一条信息来确认成功建立会话或者失败。如果会话成功，服务提供商的节点就开始发送周期计费信息。计费信息包含此次会话总MYST费用，双方发送信息量，以及会话时长。如果未使用量降至零，服务提供方会通知节点终止会话。客户也可以发出终止会话请求。一旦会话终止，将会发送最后一条计费信息。

为符合对话语义，在对话创建和终止过程中，需要有一个特定服务软件实现提供节点使用的功能。当被节点询问，该实现需提供应用特定类信息，服务提供方节点在提供应用特定类数据前可能需要这些信息。然后该软件实现接受来自于服务提供方的应用特定类数据，尝试建立会话。成功创建会话或失败后，该软件实现将会话创建结果向节点通知。VPN服务类型实现必须根据来自节点的请求才能终止会话，如果会话被服务提供方终止，则需要通知节点。

尽管我们的例子使用了客户端-服务器类型的连接方式，实际上软件实现可以选择任何通讯模式来传递应用信息。

会话参数谈判模式限于客户端-服务器间交换服务实现特定类数据。任何附加的谈判模式应当在特定服务代码中实现。

联系方式

可以通过访问我们的接触我们 https://mysterium.network/