

smartmesh.io
pr@smartmesh.io

THE
SMARTMESH
PROJECT

SMARTMESH 白皮书

PRODUCED BY
**SMARTMESH
FOUNDATION
PTE. LTD.**

SmartMesh

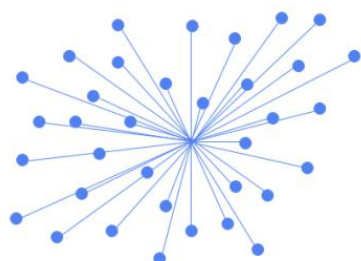
连接世界每一部手机的网络

如果网络今天才被发明，它一定会是一个连接手机的 P2P 网络，并且更安全，更便宜，更快。

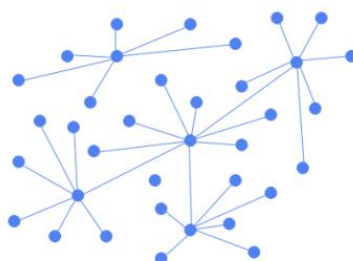
目录

1. 创世纪	3
2. 关于 SmartMesh	4
2.1 什么是 SmartMesh 协议	4
2.2 SmartMesh 的定位：移动 MESH 技术的先驱，专注技术、孵化生态	5
2.3 SmartMesh 第三方生态解决的问题	5
2.3.1 信息安全问题：点对点无网传输.....	5
2.3.2 网络拥堵问题.....	6
2.3.3 无网通讯.....	6
2.3.4 无网支付.....	6
2.3.5 普惠金融.....	7
3. VISION:一个全球化的 MESH NETWORK	7
4. TECH STACK	9
4.1 SmartMesh 架构	9
4.2 SmartMeshToken	10
4.2.1 SmartMesh 代币合约.....	10
4.2.2 签名授权代支付.....	10
4.3 SmartMesh 微支付	11
4.4 SmartMesh 无网支付	12
5. UNIVERSAL CONNECTIVITY ARCHITECTURE	14
6. SmartMesh 基金会	15
6.1 SmartMesh 决策委员会	15
6.2 SmartMesh 生态化中心	15
6.3 SmartMesh 技术开发中心	16
6.4 SmartMesh 市场营销中心	16
6.5 SmartMesh 日常管理中心	16
7. 团队成员	17
8. 发展路线	18
9. SmartMesh 分配细则	19

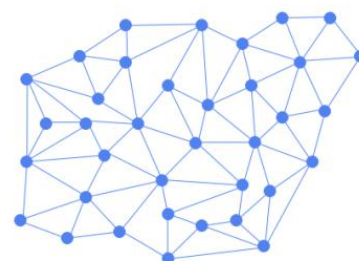
1. 创世纪



Centralised



Decentralised



Distributed

起初，人创造了互联网。

人看到互联网是好的。然而，在互联网上，人们不信任彼此。

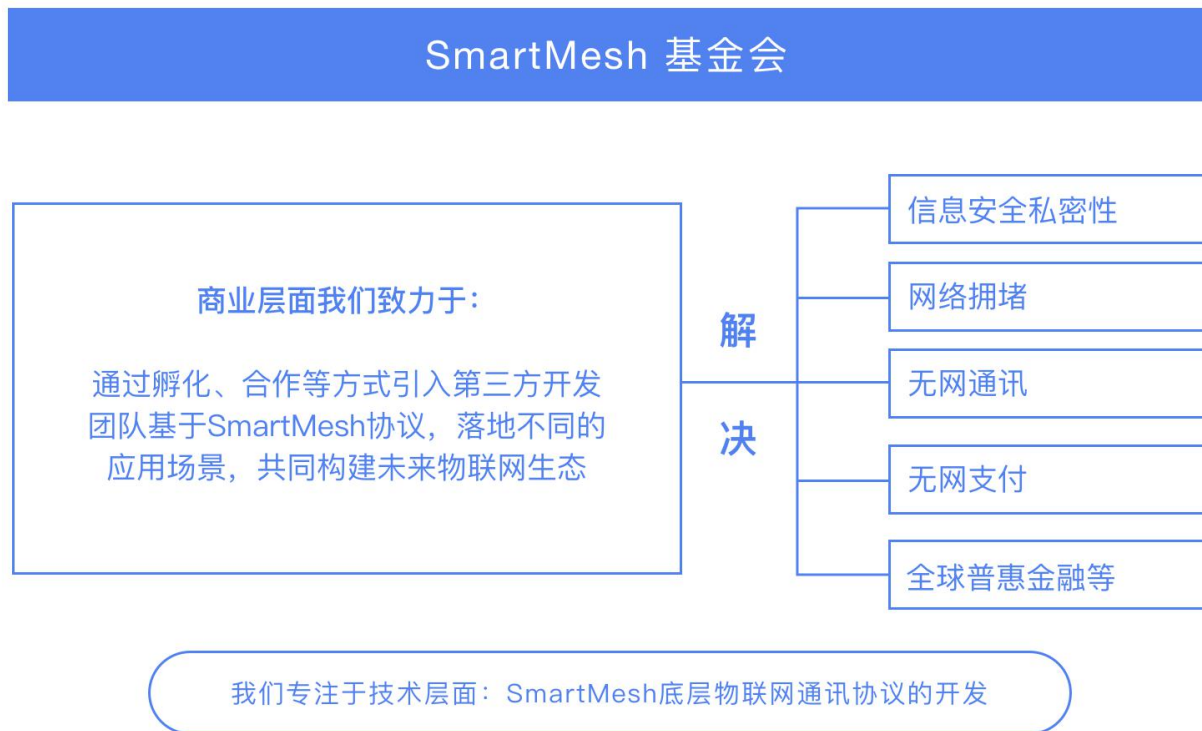
然后人创造了区块链。它可以让人们彼此合作，不需要相互信任。区块链是好的，但它很慢。

然后人创造了 Lightning、Raiden 和 Plasma。它们让人们可以做事。但是没有网时人们不能工作。

然后人创造了 SmartMesh，SmartMesh 的灵说：让万物都连接起来，即使没有互联网。

SmartMesh 在没有互联网的地方连接起万物。从此万物总是连接在一起。

2. 关于 SMARTMESH



2.1 什么是 SmartMesh 协议

SmartMesh 是一个基于区块链的物联网底层协议，能让智能手机、车载设备等不通过互联网就可以相互连接的协议，SmartMesh 内置区块链轻节点，扩展雷电网络协议实现代币的无网微支付。基于区块链代币的激励，SmartMesh 可以自组织形成一个具有弹性、去中心化、能够自我修复的 Mesh Network，提供比互联网更高的近场速度和带宽，并且它通常是免费的。它有可能成为一个与现有互联网平行的网络。

2.2 SmartMesh 的定位：移动 MESH 技术的先驱，专注技术、孵化生态

在 Mesh Network 领域有很多先驱，但显然移动手机组成的 Mesh Network 是走在最前沿的。在全球领先的近场通讯领域，澳大利亚的 Serval 和中国的 NextApp，分别优化了 Wi-Fi Direct、Bluetooth、Bluetooth LE、ANT 和其他的无线协议以及上述的应用软件分别让安卓和 iOS 手机的近场通讯成为现实。

每个基于 Mesh Network 的通讯应用都实现了同样的事情：它们让你能够在没有 SIM 卡的情况下和其他人保持沟通。它们的用户场景可能稍微不同，有的侧重聊天，有的侧重研究，有的侧重社交，但他们一起拥有千万级别的用户群体。

基于已有的技术优势以及生态资源 SmartMesh 未来主要将会持续不断的对物联网底层协议进行深度开发，并且不断地整合全球顶尖的无网通讯公司，着力于制定全球物联网通讯的统一标准。同时 SmartMesh 基金会也会通过孵化与合作等方式不断地引入第三方开发团队基于 SmartMesh 协议不断的落地各种应用场景。

2.3 SmartMesh 第三方生态解决的问题

SmartMesh 构建了一张平行于国际互联网基于智能手机点对点直连的网状网络，让不该发往中心服务器的流量在局域网状网络里就完成通讯，节省流量资源，减少电力通讯的辐射与浪费，通过基金会构建生态让人与人、人与物、物与物的连接变得更加便捷简单，是无网通讯、无网支付、无网游戏的未来方向。

2.3.1 信息安全问题：点对点无网传输

大家有没有想过我们使用的所有的手机 APP 都有信息泄露的风险，为什么呢？因为我们所有的聊天记录，浏览习惯全部都在第三方服务器保存。美国的甜爹，Visa 这类的大公司都有过

很多次的客户资料泄露事件更更况一般的小公司。有了 SmartMesh 以后所有的信息传输只是点对点，从此就隔绝了第三方信息被暴露的风险。

2.3.2 网络拥堵问题

无论是在火车、地铁、飞机上、户外野营还是看比赛，在没有网络或数据阻塞的场合下，即使没有流量或无法接入网络，用户都可以向周边的人发送消息，在大型艺术、娱乐、体育活动现场都可以将精彩瞬间随时与外界分享，而且随着越来越多的设备加入网络，网络的质量会更好，速度会更快，填补了弹性社交最后一公里，让娱乐变的更精彩。

2.3.3 无网通讯

前段时间，联合国宽带委员会(以下简称“UNBC”)发布报告称，目前全球网民数量增长开始放缓，目前全球有 39 亿人口尚未接入互联网。当前互联网在发达国家的普及程度虽趋于饱和，但在全球最贫穷的 48 个国家，90%的人口尚未接入互联网。万万没想到，全球仍有 42 亿人上不了网，SmartMesh 将解救这些人，只要他们使用装有 SmartMesh App 的手机，就可以彼此连接，形成一个局域 Mesh，Mesh 连接的所有手机中，只要有一个手机连接了 Internet，在 Mesh 上所有的人都将可以使用互联网连接世界。

2.3.4 无网支付

成熟稳定的第三方支付平台在无网情况下不能工作，SmartMesh 基于 SmartMesh 支付点对点直连的网状网络，让每一部智能设备都能成为一个节点，形成密集覆盖的节点网络，打破传统支付模式，让支付变得简单。

2.3.5 普惠金融

截止 2016 年，全球约还有 29 亿人没有银行账户，并且目前在移动支付领域基本上所有的产品都是基于有网的状态下实现的。SmartMesh 将会基于其底层通讯协议，构建起一个丰富的通讯和普惠金融的生态圈，来满足这如此巨大的需求。

3. VISION: 一个全球化的 MESH NETWORK

Mesh 的先驱面临着扩展的困境。首先，一个全球的 Mesh Network 需要全球的专家和精英聚合在一起来共同解决。其次，用户的激励也非常重要，因为密度不够的话 Mesh 的覆盖是有限的，产生不了网络效应。

所幸的是，今天，我们找到了解决问题的方法。区块链的自治社区精神让雷电网络和 SmartMesh 走在了一起。雷电网络的进展让微支付成为现实，SmartMesh 的扩展则让区块链可实现无网支付。这个聚合了世界级专家与精英的团队来一起实现这个共同的梦想。

我们倡议建立一个连接智能手机的 Mesh 网络，为共享自己手机节点的人提供代币支付。

SmartMesh 是一个节点市场，就像一个智能手机节点的 Airbnb。拥有智能手机的任何人都可以向其他节点发送短消息、照片或语音邮件，而且他们可以通过帮助传输这些数据来获得 Token。当然，传输的数据包都是加密的。

为了解决这样艰巨的任务，我们面对最大的挑战是建立一个可以在手机之间快速传输加密 Token 的微支付，让人们可以分享他们的节点，快速获得回报。这在原本的区块链上是做不到的。众所周知，区块链上交易的确认速度非常慢，不可能适用于手机节点。

比特币与区块链自诞生起一直存在若干技术问题：每秒只能处理 7 笔交易，每笔交易都要等 6 个块的确认才能视为有效。区块链的这种处理能力根本不能让人们把比特币当货币使用，更谈不到手机节点之间的微交易了。幸运的是，自 2015 年以来，我们拥有了以前的 Mesh

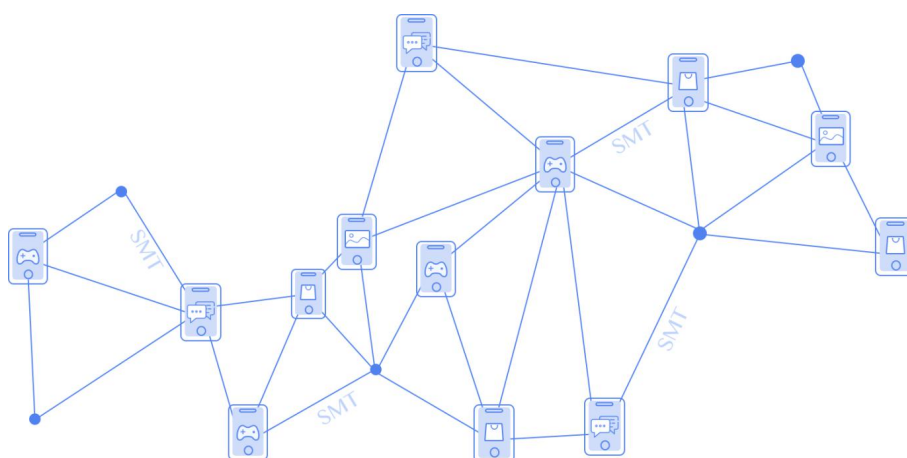
Network 项目所没有的新技术，即区块链。加密 Token 尤其是作为 off-chain 支付加速器的 Lightning 网络，Raiden 网络。

闪电网络 (Lightning Network) 提出以区块链为后盾，离链 (off - chain) 实现真正的点对点微支付交易，区块链处理能力的瓶颈被彻底打破，时延、最终性、容量，甚至隐私问题也迎刃而解。雷电网络则是闪电网络思想在以太坊上的实现，Plasma 则把闪电网络概念拓展到了支付之外的计算领域。

我们构建 SmartMesh 的计划如下：

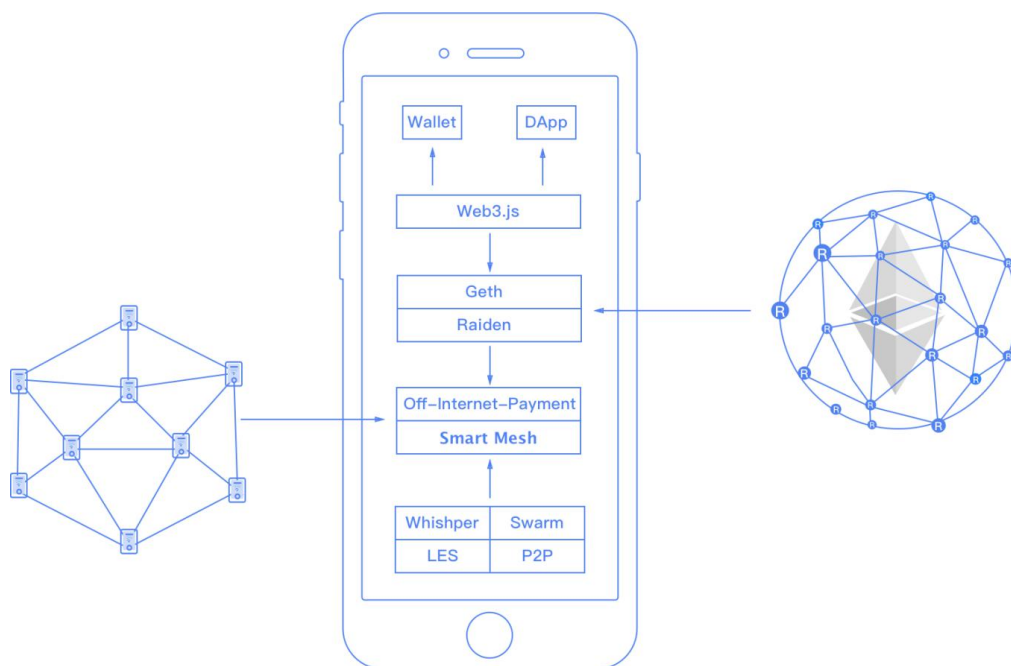
1. 建立奖励机制让人们得到奖励，这个基于区块链与代币来实现;
2. 为了让 Token 交易足够快，我们需要建立一个基于 Ethereum 的 Raiden Network 的微支付；
3. Raiden Network 速度很快，但它不能在无网的情况下工作。为了使 Raiden 能够在无网状态下工作，我们设计了 SmartMesh Extension，以便能够在手机上进行 off-internet 无网微支付；
4. 无网微支付准备就绪，人们就可以参与 SmartMesh，共享他们的节点并构建我们设想的全球 Mesh Network。

在下面的段落中，我们将在适当的技术细节中解释我们的项目愿景、历史、现状和未来，即使你不具有技术背景也应该能够理解。



4. TECH STACK

4.1 SmartMesh 架构



SmartMesh 是一个去中心化的兼容有网和无网两种情况的点对点分布式网络，目前基于终端的 LES 协议通过 Geth 连接 Ethereum 区块链。网络最上层的是去中心化应用，通过 Web3.js 和智能合约层进行交易，用户通过 Wallet 保管自己的私钥、转账、查询等功能，由 Swarm 实现共享存储空间、托管个人文件，Whisper 构建去中心沟通网络，通过雷电网络或 Plasma 支付 off-chain 交易，提升交易确认速度，或通过支票簿合约激励个人用户、提供个人存储空间及其网络资源。近场底层点对点连接基于 Wi-Fi、蓝牙、ANT 等协议，随着分布式 node 的增加，分布式网络将会越来越完善，最终构建一个世界的平行网络。我们相信 SmartMesh 具有的潜力远超无网（无互联网）聊天、无网数据传输和无网络支付的潜力。

4.2 SmartMeshToken

SmartMesh Token 是基于 Ethereum 的合约代币，简称 SMT。Ethereum 是一个开源的、公共的分布式计算平台，它提供了一个分布式的图灵完备虚拟机，支持运行智能合约。

SMT 用于激励 SmartMesh 节点分享者，并用来在 SmartMesh 生态系统中购买产品和服务。当用户将自己的智能手机节点共享到网状网络时，可获得 SMT 代币的奖励。用户在网络中停留的时间越长，在 SmartMesh 上聚集的 SMT 数字资产就越多。

4.2.1 SmartMesh 代币合约

SmartMesh Token Contract 基于 ERC20Token 标准。我们在 SMT 上实现了一些功能来支持 SmartMesh，其中包括签名授权代支付。

ERC20 代币标准已经在 Ethereum 社区赢得认可。大量知名的 Ethereum 应用程序均符合本标准，并已经证明 ERC20Token 标准是成功的。

4.2.2 签名授权代支付

基于 Ethereum 的智能合约在使用的时候需要消耗 Gas，这是 Ethereum 安全保障的措施之一，但是 Gas 需要以太币来支付，这就增加了普通用户使用去中心化应用(DAPP)的复杂度，为了使普通用户更加方便交易，我们开发了交易代理发送的功能，也就是可以由第三方来帮助普通用户支付 ETH 来支付 Gas 的消耗。

第三方代理发送交易的服务费需要使用 SMT 来支付，整个过程须由用户签名特定格式的消息进行授权后，才能由智能合约操作用户的资产。用户签名的消息最少包括代发人地址、服务费、资产变动声明等，也就是说整个过程完全由用户自己掌控，安全性无异于用户亲自用 ETH 发送交易。

4.3 SmartMesh 微支付

随着区块链技术不断的发展，PC 端的钱包应用暴露出了众多短板。设备体积影响随身携带，数据庞大个人无法完成同步，已无法满足市场用户的正常需求。

目前市场上已存在的轻钱包 App 依然是中心化服务，支付过程中，需要上传签名数据到服务端进行节点广播交易，一旦被攻击，就无法提供服务，存在很大的安全隐患。且在交易过程中需要经过其它区块的确认以及消耗 Gas，违背了区块链去中心化的思想，无法快速的完成微支付。

SmartMeshApp 是一个真正去中心化移动节点微支付钱包，SmartMesh 在智能手机上使用 LES 部署的 Geth 节点来验证和同步块头。Light Ethereum Sub-protocol 简称为 LES，是 Ethereum 的子协议，目的是在轻客户端(如智能手机等)中保持 Ethereum 某些特定部分有关当前状态的高安全性的执行。

同时 SmartMeshApp 结合 Raiden 网络技术，可以快速的完成微支付交易。Raiden 网络是一种建立在 Ethereum 基础之上的状态通道技术，它增强了 Ethereum 区块链的处理能力。其基本理念是用户可以在链下交易签名信息，而不是所有的交易都放到区块链上处理。

Raiden 网络通过 Ethereum 网络中的点对点支付与保证金存款保留了区块链系统所具备的保障机制。

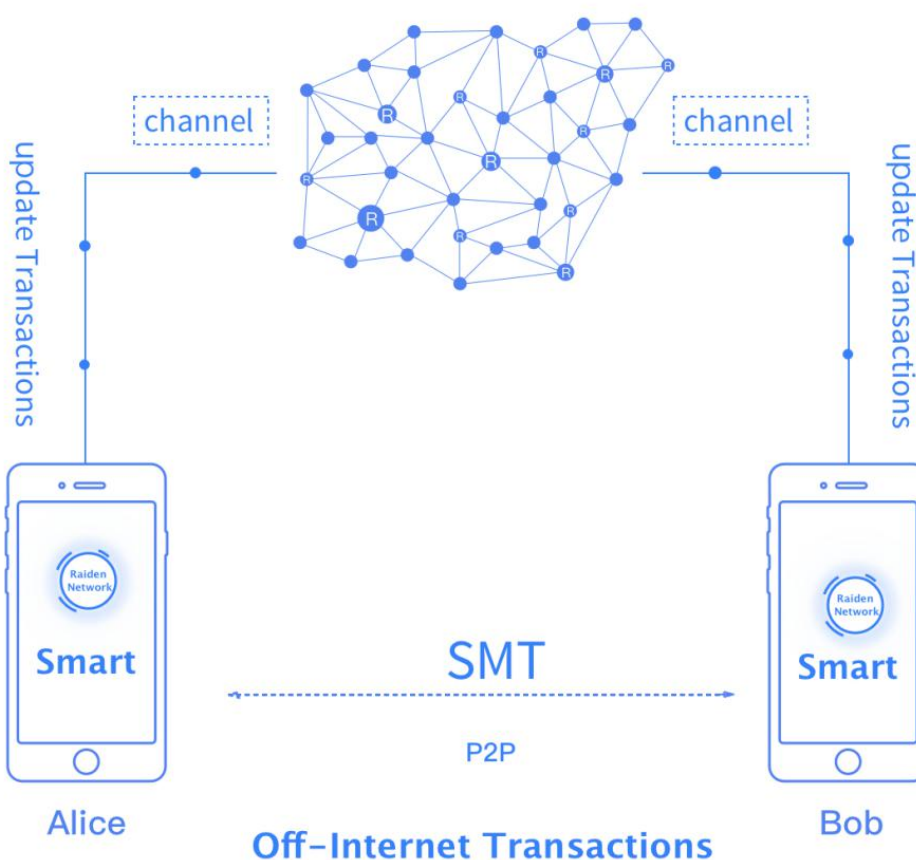
Raiden 网络具有可扩展性、快速交易、保密、互操作性、费用低、小额支付等优势，每秒可能有百万次传输，1 秒内确认和终止转账，交易费用可能比 on-chain 交易费用低 7 个数量级。更低的交易费用，使得 SmartMesh 可以有效地进行微支付。

基于此，可以对 Swarm 及 Whisper 扩展构建的分布式 P2P 网络进行激励，完善共享存储空间及网络资源共享和分布式 Whisper 协议组成的消息网络应用场景，组成一个完整的生态。

4.4 SmartMesh 无网支付

生活在移动支付盛行的时代，在无数先驱和先烈的探索下，无网支付依旧是无法攻克的难题。在无网或弱网场景下，任何第三方支付平台用户之间均无法正常完成支付交易。SmartMesh 让无网支付首次可以实现。

SmartMesh 无网微支付是基于 Raiden 网络扩展的 SmartMesh 支付协议，SmartMesh 用户之间通过手机 WiFi 或其他直连信号，P2P 传输签名加密交易信息，进行无网支付。



Alice 和 Bob 首先通过 SmartMeshApp 在互联网上建立 Raiden Network 双方通道，并各自质押一定的资产。在没有网络情况下使用 SmartMesh 无网微支付：

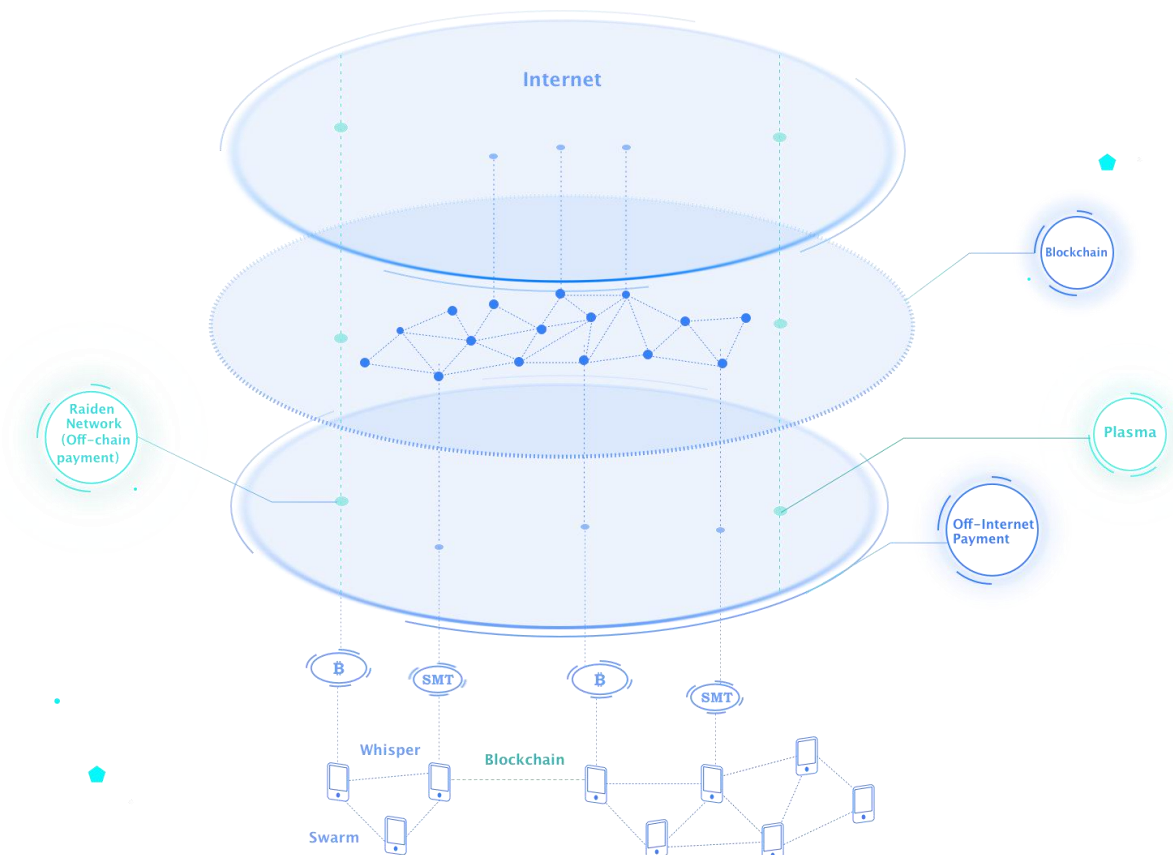
- Alice 和 Bob 通过手机 SmartMeshApp 建立无网连接。
- Alice 支付给 Bob 5 Tokens。

- Alice 把签名加密交易信息无网点对点传输给 Bob，双方存储加密交易信息。
- 待有网络时，Alice 和 Bob 把加密交易信息同步到 Raiden Network 节点上，进行交易验证通道内进行交易结算。
- 如果 Alice 关闭交易通道，Alice 向区块链上合约提交一个双方签字的 UpdateTransaction 报文，合约将等待 Hold Period 时间。期间如果对方 Bob 能够提交一个 Sequence Number 更高的 UpdateTransaction 报文，合约将没收 Alice 质押在通道中的全部资产并转移给 Bob。如果直至等待超时 Bob 也没有异议，合约将按照报文内容在区块链上完成转移支付并关闭通道，反之亦然。

雷电网络相比闪电网络，引入了较闪电网络 HTLC (Hashed Timelock Contract) 更为通用的 “Smart Condition” 。当发生争议时，只需向区块链上智能合约出示最新版本的 UpdateTransaction 报文，并请求智能合约对报文中的 Smart Condition 予以处理，就可以强制执行合约。如果没有争议，以上这一切都不会出现在 Ethereum 区块链上，增强了隐私，又提升了性能。

Alice 和 Bob 通过无网交易时，双方存储加密交易信息，有网络时双方进行 Raiden 网络同步验证，保证交易的安全性，不可篡改。

5. UNIVERSAL CONNECTIVITY ARCHITECTURE

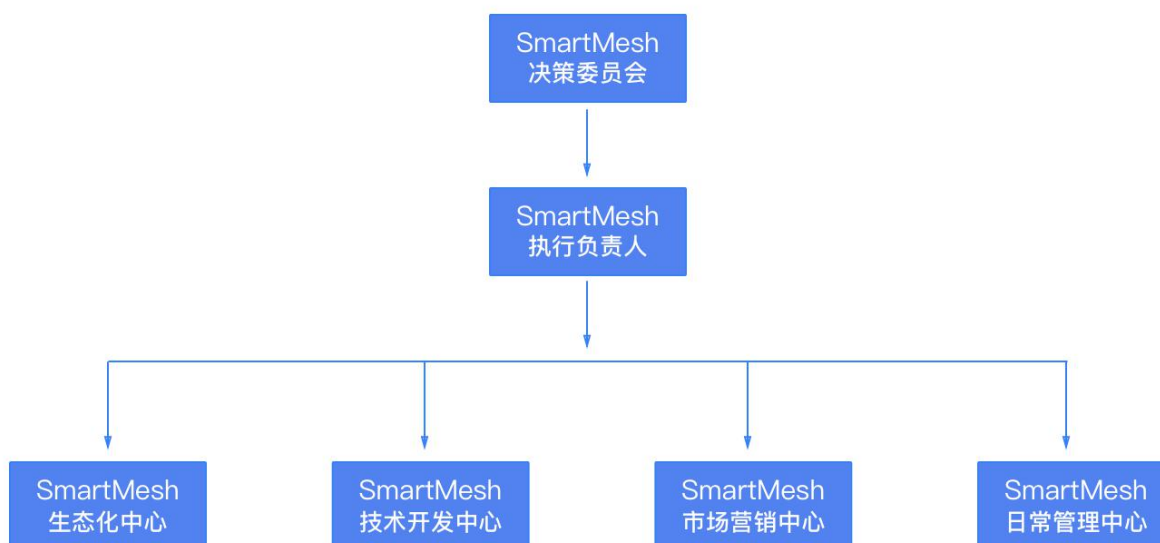


SmartMesh 构建了一张平行于互联网的 Mesh Network。每个智能手机都像是一个 SmartMesh，星星之火，可以燎原。随着 SmartMesh 的增多，手机的智能节点将会开始自行组网，手机内的应用会智能的选择每个 Packet 是该走互联网还是走 SmartMesh。区块链最初只存在 PC 电脑固定节点中，现在移动轻节点技术让区块链延伸至手机端成为现实，让人们在有网和没网的情况下都可以随时交易数字货币，SmartMesh 无网支付让数字货币在没有互联网的情况下也可以进行交易。

对未来网络通信而言，国际互联网和 SmartMesh 相互补充，SmartMesh 未来将会承载大量本地流量，它将成为最优化的普适连接。

6. SMARTMESH 基金会

SmartMesh 基金会



6.1 SmartMesh 决策委员会

SmartMesh 决策委员会负责重大事项的管理与决定，包括聘任与解聘执行负责人及各中心负责人，制定重要决策。决策委员会成员任期三年，可以连任。委员会设主席一名，具体事宜待定。首届决策委员会成员将由 SmartMesh 创始团队及投资人商议产生。

6.2 SmartMesh 生态化中心

生态化中心负责探索 SmartMesh 与行业结合应用的可能性，进一步实现商业落地。促进教育、电商、社交等领域，实现人工智能、跨境交易、互联互通、价值共享。

6.3 SmartMesh 技术开发中心

技术开发中心负责底层技术开发、测试、上线、审核等。SDK 支持市面上的通用语言，提供各个领域的技术支持并适当提供开源代码。

6.4 SmartMesh 市场营销中心

市场营销中心负责 SmartMesh 技术推广、SmartMesh 产品推广、SmartMesh 相关产品推广。

6.5 SmartMesh 日常管理中心

日常管理中心包括财务、法务、人事、行政等管理。财务负责基金的使用和审核；法务负责各类文件的审核与拟定，防范可能存在的各类法律风险；行政和人事负责人员、薪酬等人事工作以及日常行政工作。

7. 团队成员

王启亨

SmartMesh 创始人，国际区块链应用联合会主席 (International Blockchain Application federation)，领团科技董事长&CEO，亚杰商会 AAMA Blockchain 委员会轮值主席，世界无网通讯与社交领域领导者。

Kraken Yu

全球工程副总裁

原柏林/英国欧洲数字货币支付交易所首席战略官

Ashton Addison

首席市场策划师，EventChain.io 的首席执行官与创始人，领导者、企业家、自 2013 的区块链技术爱好者。

Leo Yao

Mesh 网络研发副总裁

原华为 Mesh 网络产品线负责人

Maxim Prishchepo

区块链架构师，Integral LLC 创始人兼首席执行官，Maxim 是两家革新性的 IT 公司的创始人和首席执行官。

8. 发展路线

2017

Q4

- SmartMesh iOS 和 Android 版 轻钱包开发
- SmartMesh iOS 和 Android 版 无网通讯 1.0

2018

Q 1

- SmartMesh iOS 和 Android 手机区块链轻节点开发
- SmartMesh iOS 和 Android 手机节点钱包开发
- SmartMesh iOS 和 Android 手机无网支付 1.0

Q 3

- SmartMesh 无网通信 2.0 多跳算法的优化实现
- SmartMesh 无网社交功能
- SmartMesh 无网支付协议扩展

Q 2

- SmartMesh 手机雷电网络轻节点开发
- SmartMesh 手机微支付开发

• Q 4

- SmartMesh Token 激励机制
- Swarm 扩展协议
- Whisper 扩展协议

2019

Q 1

- SmartMesh Android SDK 封装
- SmartMesh iOS SDK 封装

Q 3

- 优化多跳 Mesh 网络性能
- 制定手机网络芯片 P2P 新标准

Q 2

- 优化智能手机点对点驱动程序
- 启动厂商对手机点对点网络驱动程序升级计划

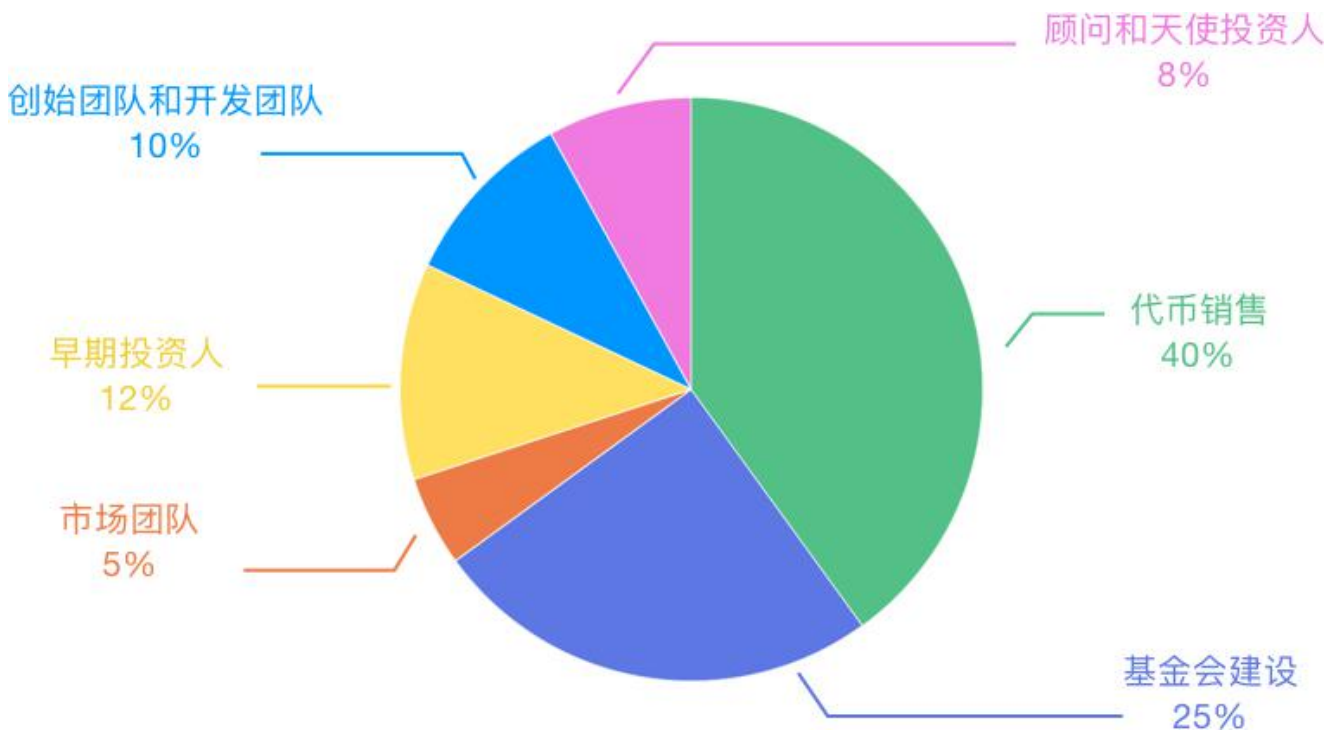
Q 4

- 构建 SmartMesh 生态

9. SMARTMESH 分配细则

SmartMesh Token，以下简称为 SMT。SMT 是一种基于 Ethereum 实现的合约代币。

SmartMesh 总共发行 3,141,592,653 SMT，其分配计划如下：40%将用于代币销售；25%用于基金会建设；12%用于早期投资人；10%用于创始团队和开发团队；8%用于天使投资人和顾问；5%用于市场团队。



比例	分配方案	明细
4%	顾问	SmartMesh 的顾问，锁定期为 1 年，第二年起每 3 个月解锁 25%
4%	天使投资人	SmartMesh 的天使投资人 (锁定期 1 年)
5%	市场团队	用于 SmartMesh 市场的推广运营
10%	创始团队和开发团队	在 SmartMesh 的创建初期和发展过程中做出了人力、资源以及技术的贡献，SMT 作为奖励进行发放。 (锁定期 2 年)
12%	早期投资人	过去数年投资者对开发团队投入的资金支持的回报。确保现在 SmartMesh 开发团队拥有的技术、知识产权、专利等能力或资产。例如“Translation on Demand”等美国专利或者知识产权，将转移至 SmartMesh 项目。 (锁定期 1 年)
25%	基金会建设	作为 SmartMesh 的备用金，用于后续项目开发，项目扶持，硬件成本及推广运营。
40%	代币销售	用于 SmartMesh 后续开发、市场推广、项目运行。

※ 无论任何时候，用户无权从 SmartMesh 基金会获得股息或利润的任何分配，且不应期望从获得代币中获得利润。

官网地址：smartmesh.io

©版权所有 2017 SMARTMESH FOUNDATION PTE. LTD.