

# MediShares

全球区块链相互保障合约市场

白皮书

v 1.0.9

# 1 项目概述

## 1.1 项目背景

### 1.1.1 起源和演变

保险的最初模式，实际上是一种起源于海上的民间互助组织，最早在小渔村自发形成的。

在古时候，渔村中十条船出去打鱼，如果风浪导致船只失事，那么失事船员的家小就会面临无人抚养照顾的绝境，于是出海前就自发约定，每条船交一份‘份子钱’，用于事故船员家人的生活保障，这就是最早的民间互助组织。

但这一模式很难大范围推广，第一是渔村人员有限，第二随着船只变大货物增多，风险加大，有限的‘份子钱’，难以维持。

所以就有一群人跳出来让他们来专业从事这项工作。当然本质上他们是通过和参与者对赌获利。随着参与的人越来越多，国家发现这是一个资金密集度很高的行业，因此也具有极大的金融风险，所以不是人人都可以开办的，必须有相应的执照才可以经营这个很有“钱途”的事业。所以这就形成了我们近代的保险业。

### 1.1.2 保险市场

去年全球的保费收入 3.92 万亿美金，占全球经济总量的 5.7%，是一个市值规模巨大的市场。

中国全行业共实现保费收入 3.10 万亿元人民币，同比增长 27.50%，增速创新高，保险业资产总量 15.12 万亿元，成为世界第二大保险市场。

在中国庞大的人口基数下，保险整体市场规模绝对数字较大。但与之不相称的是，我国人均保费和保单量要远远低于发达国家的水平。由此，就产生了两个矛盾：一是保险渗透率与人们日益提高的生活水平不匹配，具体表现在人们的物质生活越来越丰富，却没有相应的风险应对方式；二是保险行业整体的机制和创新跟不上自身的发展速度，目前保险行业处在一个快速上升的通道，但整体的机制和创新仍比较落后。

### 1.1.3 健康风险加剧

健康风险和环境污染相关，未来二十年将是癌症剧烈爆发时期。2015 年 8 月，世界卫生组织发布的《世界癌症报告》是 6 年来首篇概述全球癌症情况的报告。警告未来将出现癌症病例大爆发的情况，中国的癌症在 2012 年的发病个案几乎占了全球一半，高居第一位，并预测 2035 年全球新癌症病例将增加近一半。在最新发布的《2015 中国肿瘤登记年报》中，每一分钟，全国就有 6 人被诊断为恶性肿瘤，有 5 人死于癌症。其中肺癌的发病率仍然高居榜首，其次为胃癌、结直肠癌、肝癌和食管癌。前十位的恶性肿瘤占了全部的 76.39%，其中女性乳癌发病最多。健康风险的加剧，医疗成本的不断提高将使得保险保障市场成为世界上每一个人的刚需。

## 1.2 传统模式的问题

### 加入门槛高

传统的保险模式，其资金效率低于 20%，有大量的资金用于支付保险代理薪酬和企业运营。

### 运营效率低

保险组织机构臃肿，整体机制跟不上市场发展，所以整体运营效率较低。

### 隐私保护问题

传统的加入过程中需要很多客户的个人身份信息，包括身份证和医疗病例等，这些存储在中心化数据库中的信息存在信息泄漏的风险。

### 拒赔概率高

保险规则和赔付执行流程主要由组织者制定、颁布和修改，其中也不可避免的包含人的主观因素，如何保证加入用户的利益，尤其是对规则进行修改时，是一个不得不重视的问题。

## 资金安全问题

传统的模式无法保证组织者始终不接触资金，没有专门的资金池，没有理财的模式，中心化的数据存储模式也无法确保所有支付记录可以查询，基本上它对于参与用户而言就像是一个黑匣子。

## 1.3 去中心化的优势

### 零门槛加入

无论加入和退出都是没有门槛的，任何人随时都可以加入和退出。而且在没有人生病的情况下，大家都不需要交任何费用，仅仅当有人发生大病等满足赔付条件的时候，每个参与的人才会缴纳费用。

### 身份认证

基于区块链的身份认证，高度隐私保护，同时数据经过严格加密，查看个人信息必须通过身份识别的智能合约，而只有拥有私钥的人才能授权别人查看自己解密后的身份信息。

### 资金效率高

几乎会员缴付的每一分钱全部都会用于保障使用，95%用于自动赔付，5%用于社区发展和奖励。

### 激励机制

任何组织和个人都可以基于智能合约模板发起一个共享保障合约，并因此获得 MediShares 平台的原生代币“MDS”。这将极大丰富未来保障的应用场景，满足很多目前无法获得保障的场景。

### 无资金池

基于智能合约锁定代币资金，作为系统的运营者不触及任何的资金，完全没有专门的资金池，更没有理财的模式。由于不接触资金，所以会规避绝大多数的法律风险，甚至系统本身也不会被认为具备保险公司的特征。

## 高效运营

基于机器数据源的赔付触发条件，解决主观判断赔付标准的问题。因为区块链智能合约不能修改的特性，赔付过程将通过锁定在智能合约上的代币执行，从而保障了承诺的赔付必定会得到履行。

## 全球市场

基于 MDS Token 的无国界流通特性，MediShares 市场对全球用户开放，并用区块链完成赔付和清算。

## 1.4 愿景

保险未来的样子？



我们认为保险的未来不是保险公司的摩天大楼，也不是貌似降低了一些成本的互联网电子保单，我们相信保险的未来就是“智能合约”，真正达到让保障的运营成本能够趋近于零。

而伴随的相互保障的智能合约化，必然会出现一个保障合约市场。

这正是 MediShares 想要做的事情！

我们希望用区块链技术改变相互保障行业生产关系，让保障回归本质，将利益分享给社区。

## 2 相互保障市场简介

### 2.1 互助的模式

互助保障是指具有同质风险保障需求的单位或个人，通过遵守公约、选择加入某互助计划，并缴纳费用形成互助金的形式成为会员，由该互助金对公约约定的事件发生所造成的损失承担互助保障责任，或者当互助会员发生死亡、伤残、疾病或者达到公约内约定的年龄、期限等条件时承担给付互助金责任的互助保障活动。

首次最低充值 10 元，并保持账户余额不低于 0 元，即可享有最高 30 万元人民币互助金额大病保障。真正实现小小零钱，大大保障，会员可以随时退出，形成了基于遵守会员互助计划公约之间的“助人助己”式互助。

互助的核心是公约，这也是为什么它能够通过智能合约实现的核心原因。



### 2.2 互助的市场规模

经过近 2 年的市场教育，大病互助模式逐渐被大众了解和接受，仅 2016 年一年，行业新增互助用户超过 1500 万，截止目前，互助整体用户规模已在 3500 万以上，至 2017 年底，互助用户规模有望达到 5000 万人。增量市场潜力巨大。

## 3 MediShares 平台

### 3.1 什么是 MediShares?

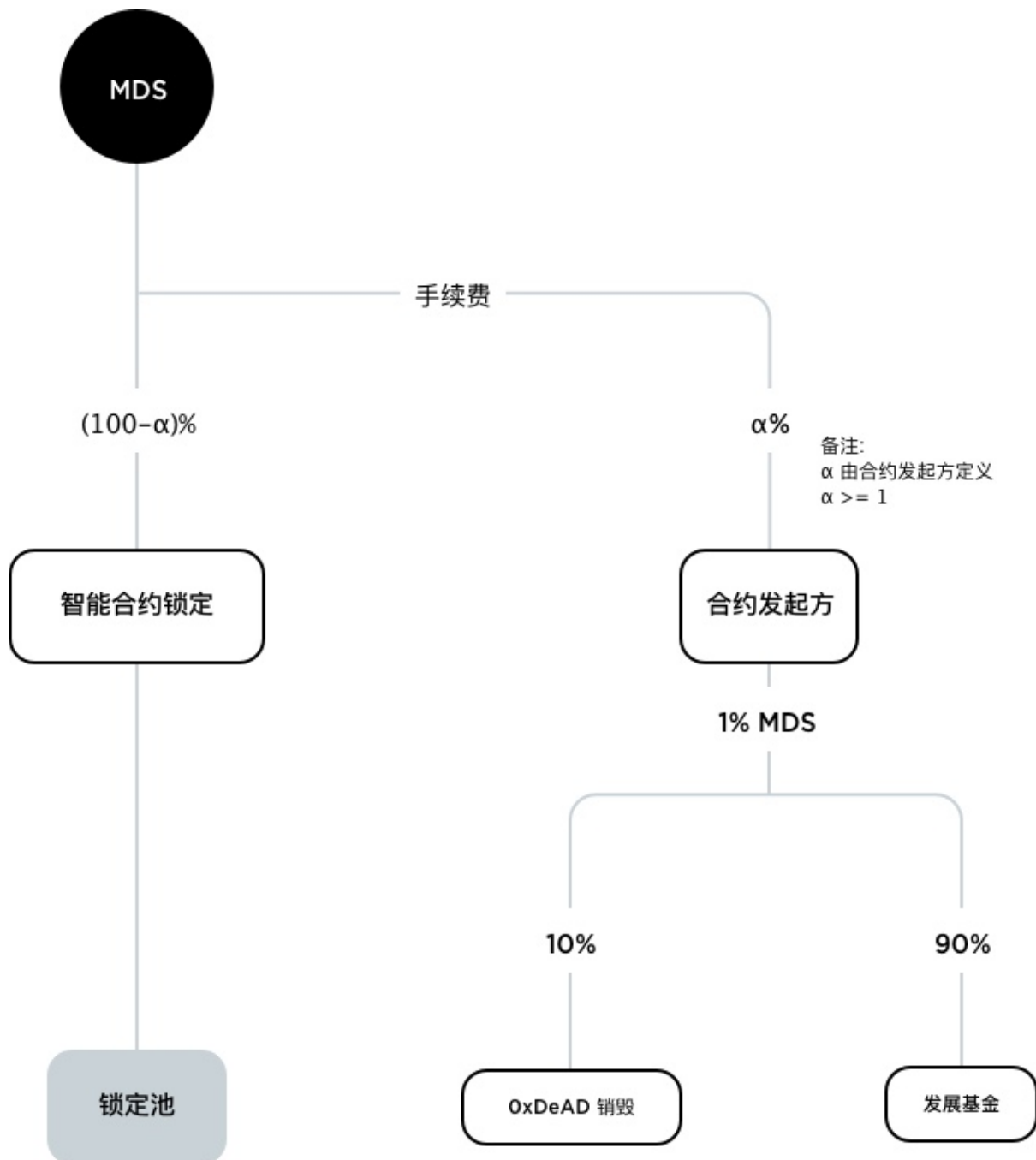
MediShares 是基于以太坊的、去中心化的、开源的相互保障合约平台，由新加坡的非盈利性机构 Medishares Foundation Ltd. (“Medishares 基金会”) 设计并开发。但开发完成后的 MediShares 平台并不由 Medishares 基金会拥有，而是由整个 MediShares 社区自治管理并运作，全球任何组织或个人均可以自由加入 Medishares 的开放式社区作为其中的成员。

世界范围内任何组织或个人都可以通过锁定 MediShares 的 MDS 获取平台上的相互保障合约的赔付资格，从而获得合约所指定的保障。

世界范围内任何组织或个人都可以通过 MediShares 平台和 MediShares 提供的智能合约模板发布相互保障合约，并从中获得 MDS 奖励。

## 3.2 功能模块

### 3.2.1 加入模块



(1) 用户通过将 MDS 发送到智能合约加入保障，合约发起方在创建合约是定义参数 α, α>=1。(100-α)%的 MDS 将由智能合约锁定。锁定的代币只有两种提出方式，一



种是以互助均摊的方式扣除，另一种是用户主动申请退出保障合约。合约发起方需要从 $\alpha\%$ 中支付 1%MDS 的手续费，其中 10%直接销毁，90%用于平台发展基金。

(2) 如果锁定池中 MDS 余额小于最新均摊金额将失去保障资格，因此用户需要将持续充值 MDS 发送到智能合约进行锁定，保留保障的资格。

(3) 用户可以向智能合约发起区块链请求，将扣除手续费和均摊金额后的 MDS 退回钱包，同时退出保障。

(4) 加入模块支持两种不同的形式：个人和组织。个人形式包括用户为自己，也可以为亲友进行加入和续费充值。组织形式支持公司为员工批量加入的操作。

### 3.2.2 赔付模块



(1) MediShares 的赔付将通过 MDS Token 进行。因为其绑定数字资产的特性，会有比较好的抗通胀性，但同时也需要承担波动的风险。

(2) 一旦发生互助事件，申请互助的用户需要抵押一部分 MDS 用于引入平台认可的第三方公估机构对事件的真实性进行核实。

(3) 赔付模块包含两个关键系数：年龄系数和扣费系数。

年龄系数：不同年龄段的人群分摊的互助金也有所差异。

扣费系数：区分保障额度来保证公平性，疾病严重程度越轻，获得的保障额度越低。

### 3.2.3 赔付规则

(1) MediShares 的精算模型将与传统模型完全不同。保险精算模型的主要目的就是提高企业的利润率。通过采取更多复杂的保险模式才能让知情权严重不对称的客户们交出更多的保费。所以这样的精算模型目标和客户的利益是完全对立的。

(2) MediShares 中，通过缴纳保费和支付理赔的方式来获得利润率，这个基础已经不复存在了。那现有的精算模型就完全失效了，而新的精算模型将变成一种事后均摊的模型，能够让系统中每一个会员获得更公平的保障。这样的精算模型是和会员的利益完全一致的。

### 3.2.4 赔付数据采集模块

赔付数据采集主要包含两种方式：

一、可获取第三方可信数据种子的保障合约，如天气灾害保障，将通过 Oracle 直接触发智能合约进行分摊和赔付。

MediShares 将通过与另外几家区块链技术公司的战略合作，获得可信的 Oracle 数据，包括与 Delphy（天算）去中心化预测市场和 Scry（无域）全行业分类数据区块链协议。

二、不能获取第三方可信数据种子的保障合约，如大病互助保障，将通过理赔调查、结果公示的方式进行分摊和赔付。

(1) 申请互助的用户需要抵押一定数额的 MDS 作为真实性承诺，并支付公估机构的调查费用。调查结果将通过 DAPP 在社区公示一周，公示期间所有加入该保障合约的用户都可以成为监督人举报骗保行为。

(2) 当社区用户数足够大时，可以通过社区见证人机制取代公证调查步骤，进一步降低理赔成本。

### 3.2.5 社区见证人机制

MediShares 社区的任何一个人在缴纳一定的 MDS 资产押金后，都可以成为见证候选人，患者在提出救助申请后，智能合约会根据特定公开的随机算法（包括地理位置等综合因素考虑）提供优选见证人，选择见证人后，见证人需与患者见面，并审查相关信息，并将所有资料整理归档，签名确认，在赔付完成后将获得 MDS 奖励。

如果在后续流程中发现申请人造假，而见证人未能及时觉察，见证人押金将被没收，作为管理委员会运营资金。

见证人在经济利益的驱动下将为合约各方提供准确可靠的信息输入，可极大地保证合约的公平且有效执行。

### 3.2.6 社区监督人

任何人一旦发现有可能的欺骗情况，即可通过匿名的方式抵押一定的 MDS 资产，举报欺骗行为，管理委员会将负责介入调查，方式包括随机更换其他公估机构或者见证人，一旦查实，则举报的监督人将获得申请人抵押的 MDS 作为奖励；如果举报有误，则将举报人抵押的 MDS 资产作为管理委员会运营资金予以没收，上述的每一个流程都将在区块链上留下相应的 Hash 记录。

监督人在经济利益的驱动下，平衡了公估机构/见证人的权力，可有效降低公估机构/见证人合伙欺骗的行为，可更加有效地保证合约的公平执行。

### 3.2.7 风险防控

传统的保障模型中最大的风险来自系统组织者作弊。如果数据库控制者偷偷将患者放入数据库，而且私下收取费用，其他会员都无法察觉。因此如何进行自证是很大的难点，在过去往往需要通过政府部门背书，或者专业公司来审计。这其中不仅成本巨大，而且对于普通人来说也非完全透明。

MediShares 将在每个会员注册时，就把该名会员的信息加密后写入到区块链中，如果退出组织，也会写入到区块链中。并且在需要的时候，随时可以查询相应的信息。区块链信息一旦写入，全球没有任何国家或个人有能力更改。这是目前最牢不可破的自证方式。

### 3.2.8 合约市场

只有符合 MediShares 标准的保障合约才能在市场上架，这些标准包括且不限：

遵守 MediShares 的社区治理条例；

遵守 MediShares 统一约定的手续费标准；

可以通过 Oracle 或者 见证人/监督人机制 判定赔付结果。

### 3.2.9 合约发起方的权利和义务

权利：

合约发起方将获得加入保障合约时需支付的手续费的 40% MDS 作为奖励。

义务：

合约发起方除了需要支付创建保障合约的以太坊 Gas 外，还需要抵押一定数量的 MDS，一方面避免 MediShares 市场上有大量无效的保障合约，另一方面抵押的 MDS 数量将成为该保障合约在市场中的权重，权重高的合约将在市场中获得好的展示位置，从而吸引更多的用户加入。

### 3.3 应用场景



### 3.3.1 大病保障合约

大病保障合约主要涵盖癌症等重大疾病的保障，通过理赔调查、公示、社区监督完成赔付，一般需要设定半年观察期。

任何一家公司或者平台都可以基于 MediShares 的智能合约模板发起特定的大病保障合约。

#### 痛点

数据显示中国人购买长期健康险的比例仍仅为 3%，而我们所面对的健康风险却不断升高，最主要的原因还是传统保障的费用太高。

#### MDS 应用

全球任何一个机构或个人，均可作为保障合约发行方在 MDS 平台上发起保障合约。在此方面，目前国内最大的互助保障平台众托帮已有意成为 MediShares 平台的保障合约发行方之一，使用 MediShares 平台来尝试发起互助保障合约。

众托帮的互助会员数已经超过 850 万，若加入 MediShares 社区作为其中一名成员，其丰富的互助社区运营和产品设计经验将为 MediShares 的初期发展带来帮助。

众托帮还会将其 2016 年就已申请的《基于区块链的互助保险和互助保障运行方法及系统》国家级发明专利分享给 MDS 的开源社区。



### 3.3.2 极限运动爱好者保障合约

极限运动已经成为追求城市生活以外刺激体验的一项重要活动，并受到越来越多年轻人的喜爱。

#### 痛点

以极限运动中的潜水为例，全球有大量潜水爱好者，但潜水作为死亡率最高的风险运动却没有相应的意外伤害保险产品。

#### MDS 应用

潜水爱好者组织（比如 PADI ）或者潜水爱好者社区成员可以通过 MediShares 创建潜水爱好者相互保障合约。



### 3.3.3 匿名疾病保障合约

根据中国卫生部数据，中国慢性病患者已超过 2.6 亿人，慢性病导致的死亡占总死亡人数的 85%。

#### 痛点

大量慢性疾病患者（如乙肝等）不愿意购买保险，因为担心可能会因此泄露个人隐私，丢掉工作。

#### MDS 应用

区块链的匿名疾病保障合约通过零知识证明等密码学方法能够很好的保护用户的隐私同时提供公平公正的保障。





### 3.3.4 豪车车主保障合约

仅以中国温州为例，五年之内共有 4353 辆保时捷上牌，302 辆玛莎拉蒂上牌，128 辆宾利上牌，84 辆劳斯莱斯上牌，34 辆兰博基尼上牌，24 辆法拉利上牌。

#### 痛点

豪车因为维修价格极高，大多数保险公司拒保，或者保险费用极高，湖南卫视《Top Gear》一季的经费都付不起测试一次 Ferrari 250 GTO 的保险费。

#### MDS 应用

豪车俱乐部或者车主可以通过发起豪车车主相互保障合约，将极大降低成本。



### 3.3.5 天气灾害保障合约

近些年，以极端高温、台风、旱涝等为主要表现形式的极端天气频率较往年有所增加。世界气象组织表示，导致全球频繁出现极端天气的主因，是温室气体排放造成的全球气候变暖。

#### 痛点

天气灾害在特定国家和地区内是非常小概率事件，但在全球范围则是时常发生的事件，而且有越来越多的趋势，很多家庭因此遭受巨大冲击。

#### MDS 应用

通过读取全球天气和地震相关数据接口，即可完成智能合约的自动触发，将实现真正意义上的全自动保障合约。



### 3.3.6 虚拟资产保障合约

MediShares 为虚拟资产类保障提供可能。

#### 痛点

随着虚拟数字资产越来越多的进入普通人的生活，对虚拟资产的安全保障需求也越来越强。

#### MDS 应用

用户可发起为交易所资产丢失等可能的风险设定的保障合约，一旦受到损失并提供可公示的证据，即可获得赔偿。



## 3.4 技术模块

### 3.4.1 系统架构



系统的核心组件包括：

以太坊

智能合约

DAPP

Oracle

IPFS

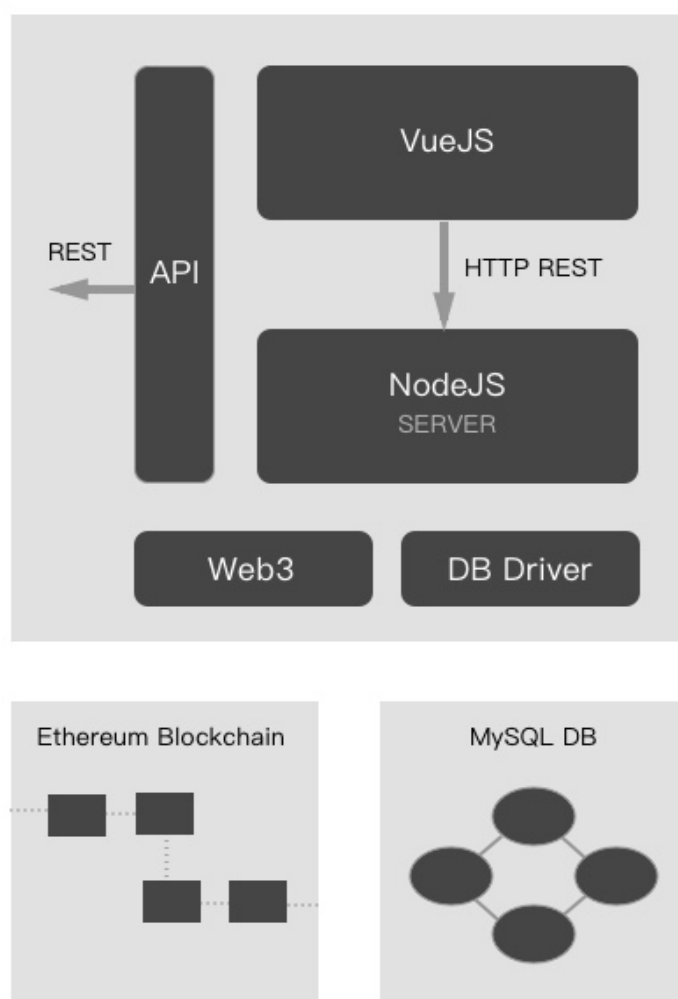
### 3.4.2 应用层 DAPP

DAPP 将提供一个基于 Web 的用户体验优秀的功能入口。

保障合约发起人可以在 DAPP 中创建保障智能合约并分享。

用户可以在 DAPP 中查看 MDS 余额，加入保障，接收通知等。

公示和投票板块完成社区治理相关的功能，公示文件和图片将通过 IPFS 保存。



DAPP 架构图

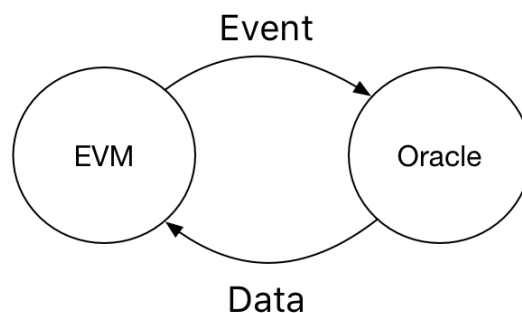
### 3.4.3 数据和 API 服务

MediShares 将开放部分数据和 API 接口给第三方公估和理赔机构，以及保障合约的发起人，从而提供将 MediShares 与第三方系统对接的可能，降低第三方公司的使用成本，同时也使得客户的隐私能够得到保护，避免数据泄露的危险。

### 3.4.4 Oracle

智能合约是在 EVM (Ethereum Virtual Machine) 中执行的，它是个封闭的环境，合约没办法由 EVM 内部向外界取得任何资料。Oracle 能够帮助智能合约取得 EVM 外部的信息，其实现原理是透过 Event 来跟外界 Oracle 联系，再由 Oracle 主动将资料抛回 EVM。

MediShare 的某些保障合约的赔付结果判定时需要用到 Oracle，另外通过交易所接口获取过去 24 小时稳定货币与 MDS 汇率并得到一个平均汇率用于进行稳定货币赔付时也会用到 Oracle。



### 3.4.5 隐私保护技术

匿名疾病相互保障合约需要更强的用户隐私保护，即在申请理赔前，所有加入保障的用户身份可验证但不可追溯输入的信息。

基于区块链的零知识证明 Project Alchemy 将被用于解决隐私保护的问题。

### 3.4.6 系统容量

随着用户数逐渐增长，系统需要满足大用户量的小额扣款需求，基于 POW 的以太坊公链可能会出现性能瓶颈，所以 MediShare 技术团队会持续关注新的区块链技术平台解决方案。其中主要的方向是以 Cosmos 为代表的侧链解决方案和以 EOS 为代表的 DPOS 公链解决方案。

## 3.5 盈利模型

MediShares 的核心价值是通过“人人为我，我为人人”的方式，将运营成本降到最低，每个人既是参与者也是受益者。而 MediShares 的价值将因为越来越多用户的加入，以 MDS 代币价值的形式体现。

## 4 MDS Token

### 4.1 MDS 的生成

MediShares 平台将在以太坊上正式上线运行时起，自动初始生成恒定总量为 20 亿枚基于以太坊智能合约 ERC 20 标准的 MDS 代币。作为 MediShares 系统的开发者，MediShares 基金会将作为全部 MDS 的初始拥有人。

### 4.2 MDS 的使用

MDS 是使用 MediShares 上保障服务的代币，也是 MediShares 市场的基础价值。不同的参与方（保障合约发行方、用户、管理团队）持有不同数量的 MDS，并根据需求进行良性流动和循环。

MDS 受智能合约的监管，实现了无资金池的保障权益锁定。

### 4.3 MDS 的用途

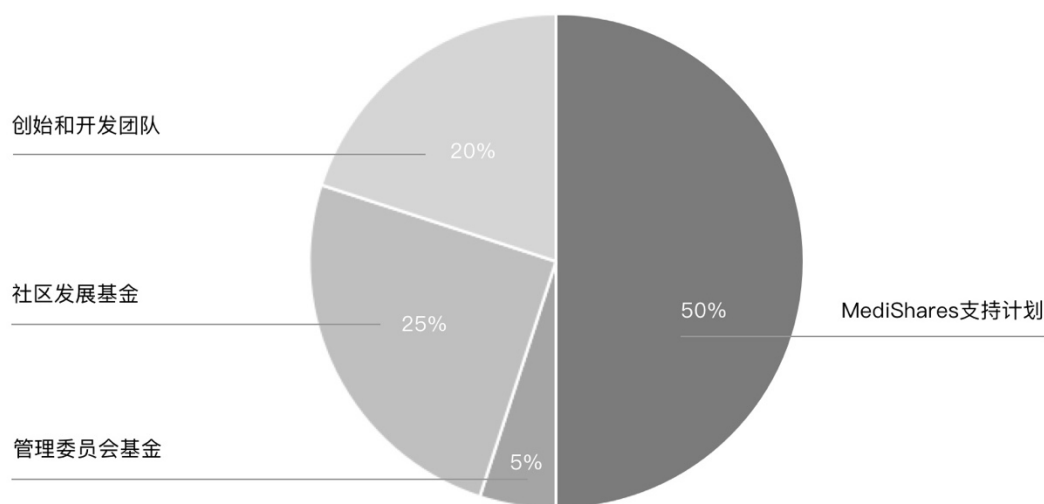
用户加入相互保障时，系统将收取一定比例 MDS 的手续费，一小部分平台手续费将会发送到一个没有任何人掌控私钥的地址直接销毁，任何人都可以通过以太坊区块链浏览器查询，以确保公开透明。

创建保障合约需要锁定一定数量的 MDS，合约市场会形成类电商的盈利模式，保障发起人需要通过锁定更多 MDS 获得比较好的排名和市场露出，从而带来更多用户加入和更多代币收益。

加入相互保障人数越多，智能合约锁定 MDS 越多，可流通量越少，供需比将逐渐下降。



## 4.4 MDS 公开售卖计划



MediShares 项目合计有数量为 20 亿的 MDS 代币，其中 50%属于 MediShares 社区支持计划。

剩余 MDS 分配方案：

5% 管理委员会基金，用于管理委员会的运维基金，逐年开放；

25% 社区发展基金，用于奖励对社区建设有贡献的合作伙伴，将逐年开放；

20% 创始和开发团队预留，分配给创始团队、早期贡献者和将来的团队成员，奖励其对社区的建设、产品设计和开发、社区运营所做出的贡献。作为团队激励，将在公开售卖一年后开始解锁，分四年逐步解锁，每年解锁 25%。

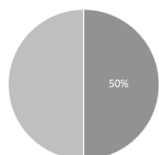
任何中国公民不得参与 MDS 的公开支持计划。

任何美国公民、永久居民或绿卡持有人将不得参与 MDS 的公开售卖计划，除非已经按照美国相关法律经认证后取得了合格投资者的资质。

## 4.5 项目预算

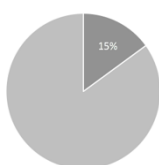
公开售卖的代币将全部用于 MediShares 平台开发、团队人员扩充、市场运营推广等有利于平台运营发展的用途。

以下是初步预算方案：



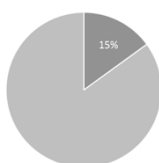
#### 核心开发 50%

这部分资金将用于底层架构、合约开发和界面开发，进一步提升用户体验，以及拓展后续新的功能。包括了人力和各种软硬件研发成本。



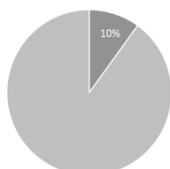
#### 安全性 15%

MediShare 团队将在安全性上持续投入，保证用户保障资金的安全。我们将计划一系列的安全审计，每一个新的主要功能的上线前都需要进行安全审计，然后才考虑在主网部署。



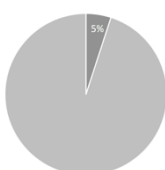
#### 运营 15%

为确保平台的高效、稳定运营，我们将招募专业的运营、客服、管理人员，打造高效的运营团队，提高平台的稳定性和可拓展性。



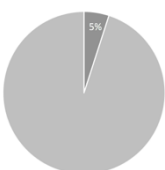
#### 市场营销 10%

这部分预算将用于进行社区建设活动，并通过传统的营销渠道让普通大众了解 MediShares。



#### 法律合规 5%

区块链是一个新兴行业，各国法律法规将对平台产生重大影响。合规性将成为 MediShares 平台成功的关键因素之一。所以我们针对可能出现的法律风险设置专门的预算，同时也将严格执行审计、会计流程，建立完善的法务流程，确保平台符合各类法律法规的监管要求。



#### 商业发展 5%

MediShares 的平台运营需要与各种有保障需求的组织达成业务合作关系，同时还需要与公估机构、数据机构合作。

## 5 发展路线图



## 6 MediShares 社区

MediShares 社区拥有在保险、互助、区块链技术等行业都有着长期丰富经验的专家组成，并且在推动行业发展中已经做出了巨大贡献，从而在行业中有着巨大的影响力。并且长久以来对行业都有着深刻的理解以及敏锐的洞察力，将是项目在未来能够进行高速发展的良好保证。

### 6.1 社区成员



#### 虞家男

上海交通大学硕士

众托帮 CTO，全栈开发者，连续创业者

多项区块链技术专利，心链创始人



#### 高寒歌

英国贝尔法斯特女王大学金融学硕士

原平安信托业务总监，兴业全球基金业务总监

第一财经公司与行业节目嘉宾



#### 龙格

北京师范大学硕士

互助保障模式鼻祖，保险产品精算专家

原华泰保险产品部高级经理



#### 郭馨芳

执业医师

原平安健康险高管

挂号网联合创始人

原 MERCER China Leader in Health Management

## 6.2 社区顾问



**沈波**

分布式基金创始人

BitShares 联合创始人



**李国权 David Lee**

新加坡管理大学教授

著名区块链投资人

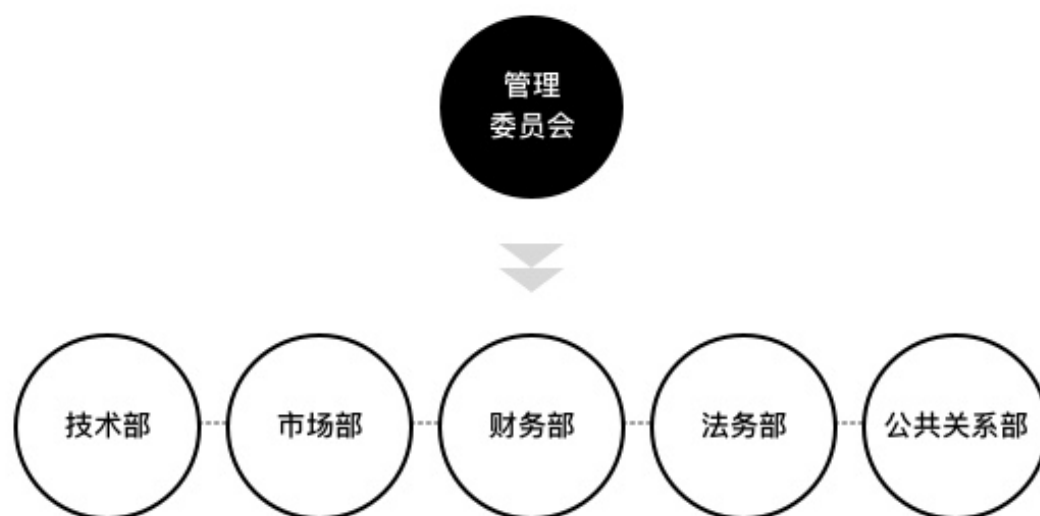


**乔克**

众托帮创始人，原中国平安高管，连续创业者

中国互联网协会理事，中国青年创业就业导师

### 6.3 组织架构



## 7 战略合作伙伴

### 7.1 业务合作伙伴

MediShares 的业务合作伙伴将包括医疗机构、互助机构、相互保险公司等机构。

### 7.2 区块链技术合作伙伴

Delphy 天算 — 去中心化预测市场

SCRY 无域 — 全行业分类数据区块链协议

InfoCorp — 东盟普惠金融区块链技术平台

Zhongtopia 众托帮 — 中国最大的互助保障平台

## 8 风险提示和免责声明

### 8.1 关于本白皮书

本白皮书只做交流之用，其中包含的信息或分析不构成购买提议或劝导。本白皮书不构成也不应被理解成为提供任何买卖的行为，或邀请买卖任何形式虚拟商品的行为，也不是任何形式上的合约或者承诺。

### 8.2 免责声明

除本白皮书所明确载明的之外，MediShares 团队和 MediShares 基金会不对 MediShares 或 MDS 作任何陈述或保证（尤其是对其适销性和特定功能）。任何人参与 MDS 的公开售卖计划及购买 MDS 的行为均基于其自己本身对 MediShares 和 MDS 的知识和本白皮书的信息。在无损于前述内容的普适性的前提下，所有参与者在 MediShares 项目启动之后按现状接受 MDS，无论其技术规格、参数、性能或功能等。

MediShares 团队和 MediShares 基金会在此明确不予承认和拒绝承担下述责任：

- (1) 任何人在购买 MDS 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；
- (2) 任何人在购买 MDS 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取 MDS；
- (3) 由于任何原因 MDS 的公开售卖计划被放弃；
- (4) MediShares 的开发失败或被放弃，以及因此导致的无法交付 MDS；
- (5) MediShares 开发的推迟或延期，以及因此导致的无法达成事先披露的日程；
- (6) MediShares 源代码的错误、瑕疵、缺陷或其他问题；
- (7) MediShares 平台或以太坊区块链的故障、崩溃、瘫痪、回滚或硬分叉；



- (8) MediShares 或 MDS 未能实现任何特定功能或不适合任何特定用途；
- (9) 对公开售卖所募集的资金的使用；
- (10) 未能及时且完整的披露关于 MediShares 开发的信息；
- (11) 任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥（尤其是其存放 MDS 钱包的私钥）；
- (12) MDS 的第三方众筹平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或歇业；
- (13) 任何人与第三方众筹平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；
- (14) 任何人对 MDS 的交易或投机行为；
- (15) MDS 在任何交易所的上市或退市；
- (16) MDS 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制；
- (17) 本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

### 8.3 风险披露

MediShares 基金会相信，在 MediShares 的开发、维护和运营过程中存在着无数风险，这其中很多都超出了 MediShares 团队和 MediShares 基金会的控制。除本白皮书所述的其他内容外，每个 MDS 购买者还均应细读、理解并仔细考虑下述风险，之后才决定是否参与本次公开售卖计划。

每个 MDS 的购买者应特别注意这一事实：尽管 MediShares 基金会是在新加坡共和国设立的，但 MediShares 和 MDS 均只存在于网络虚拟空间内，不具有任何有形存在，因此不属于或涉及任何特定国家。

参加本次公开售卖计划应当是一个深思熟虑后决策的行动，将视为购买者已充分知晓并同意接受了下述风险。

### **(1) 公开售卖计划的终止**

本次 MDS 公开售卖计划可能会被提前终止，此时购买者可能由于以太币的价格波动以及 MediShares 基金会的支出而仅被部分退还其支付的金额。

### **(2) 不充分的信息提供**

截止到本白皮书发布日，MediShares 仍在开发阶段，其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了 MediShares 最新的关键信息，其并不绝对完整，且仍会被 MediShares 基金会为了特定目的而不时进行调整和更新。MediShares 基金会无能力且无义务随时告知参与者 MediShares 开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让购买者及时且充分地接触到 MediShares 开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

### **(3) 监管措施**

加密货币正在被或可能被各个不同国家的主管机关所监管。MediShares 基金会可能会不时收到来自于一个或多个主管机关的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何关于本次公开售卖计划、MediShares 开发或 MDS 的行动。MediShares 的开发、营销、宣传或其他方面以及本次公开售卖计划因此可能受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家之中现有的对于 MediShares 或本次公开售卖计划的监管许可或容忍可能只是暂时的。在各个不同国家，MDS 可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，MDS 可能被禁止交易或持有。

### **(4) 密码学**

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明）可能给基于密码学的系统（包括 MediShares）带来危险。这可能导致任何人持有的 MDS 被盗、失窃、消失、毁灭或贬值。在合理范围内，MediShares 基金会将自我准备采取预防或补救措施，升级 MediShares 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的，MediShares 基金会将尽力迎合密码学和安全领域的不断变化。

#### **(5) 开发失败或放弃**

MediShares 仍在开发阶段，而非已准备就绪随时发布的成品。由于 MediShares 系统的技术复杂性，MediShares 基金会可能不时会面临无法预测和/或无法克服的困难。因此，MediShares 的开发可能会由于任何原因而在任何时候失败或放弃（例如由于缺乏资金）。开发失败或放弃将导致 MDS 无法交付给本次售卖计划的任何购买者。

#### **(6) 众筹资金的失窃**

可能会有人企图盗窃 MediShares 基金所收到的公开售卖所获资金（包括已转换成法币的部分）。该等盗窃或盗窃企图可能会影响 MediShares 基金会为 MediShares 开发提供资金的能力。尽管 MediShares 基金会将会采取最尖端的技术方案保护众筹资金的安全，某些网络盗窃仍很难被彻底阻止。

#### **(7) 源代码瑕疵**

无人能保证 MediShares 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能，暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害 MediShares 的可用性、稳定性和/或安全性，并因此对 MDS 的价值造成负面影响。公开的源代码以透明为根本，以促进源自于社区的对代码的鉴定和问题解决。MediShares 基金会将与紧密 MediShares 社区紧密合作，今后持续改进、优化和完善 MediShares 的源代码。

## **(8) 无准入许可、分布式且自治性的账本**

在当代区块链项目中，有三种流行的分布式账本种类，即：无准入许可的账本、联盟型账本和私有账本。MediShares 底层的分布式账本是无准入许可的，这意味着它可被所有人自由访问和使用，而不受准入限制。尽管 MediShares 初始时是由 MediShares 基金会所开发，但它并非由 MediShares 基金会所有拥有、运营或控制。自发形成的 MediShares 社区是完全开放、无中心化且无准入门槛即可加入的，其由全球范围内的用户、粉丝、开发者、MDS 持有人和其他参与者组成，这些人大都与 MediShares 基金会无任何关系。就 MediShares 的维护、治理以及甚至是进化而言，该社区将是无中心化且自治的。而 MediShares 基金会仅仅是社区内与其他人地位平等的一个活跃成员而已，并无至高无上或专断性的权力，哪怕它之前曾对 MediShares 的诞生做出过努力和贡献。因此，MediShares 在发布之后，其如何治理乃至进化将并不受到 MediShares 基金会的支配。

## **(9) 源代码升级**

MediShares 的源代码是开源的且可能被 MediShares 社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对 MediShares 的运行或 MDS 的价值造成重大不利影响。

## **(10) 安全弱点**

MediShares 区块链基于开源软件并且是无准入许可的分布式账本。尽管 MediShares 基金会努力维护 MediShares 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入 MediShares 的核心基础设施要素之中，对这些弱点或缺陷 MediShares 基金会无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的 MDS 或其他数字代币丢失。

## **(11) “分布式拒绝服务”攻击**

以太坊设计为公开且无准入许可的账本。因此，以太坊可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 MediShares 系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入以太坊区块链的区块之中，或甚至暂时无法执行。

## **(12) 处理能力不足**

MediShares 的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过以太坊区块链网络内届时节点所能提供的负载，则 MediShares 网络可能会瘫痪和/或停滞，且可能会产生诸如“双重花费”的欺诈或错误交易。在最坏情况下，任何人持有的 MDS 可能会丢失，以太坊区块链回滚或甚至硬分叉可能会被触发。这些事件的余波将损害 MediShares 的可使用性、稳定性和安全性以及 MDS 的价值。

## **(13) 未经授权认领待售 MDS**

任何通过解密或破解 MDS 购买者密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意获取 MDS 购买者所购买的待售 MDS。据此，购买者所购买的待售 MDS 可能会被错误发送至通过购买者注册邮箱或注册账号认领 MDS 的任何人士，而这种发送是不可撤销、不可逆转的。每一 MDS 购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性：(i) 使用高安全性密码；(ii) 不打开或回复任何欺诈邮件；以及 (iii) 严格保密其机密或个人信息。

## **(14) MDS 钱包私钥**

获取 MDS 所必需的私钥丢失或毁损是不可逆转的。只有通过本地或在线 MDS 钱包拥有唯一的公钥和私钥才可以操控 MDS。每一购买者应当妥善保管其 MDS 钱包私钥。若 MDS 购买者的该等私钥丢失、遗失、泄露、毁损或被盗，MediShares 基金会或任何其他人士均无法帮助购买者获取或取回相关 MDS。

## **(15) 通胀**

可能会由于采纳 MediShares 源代码补丁或升级（这将由 MediShares 社区决定而不是 MediShares 基金会决定），导致 MDS 数量发生增加。由此产生的 MDS 供应量通胀可能导致市场价格下跌，从而 MDS 持有者（包括购买者）可能遭受经济损失。MDS 购买者或持有者并不能被保证会由于 MDS 通胀而获得赔偿或任何形式的补偿。

#### **(16) 普及度**

MDS 的价值很大程度上取决于 MediShares 平台的普及度。MediShares 并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，MediShares 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部 MDS 需求可能具有投机性质。缺乏用户可能导致 MDS 市场价格波动增大从而影响 MediShares 的长期发展。出现这种价格波动时，MediShares 基金会不会（也没有责任）稳定或影响 MDS 的市场价格。

#### **(17) 流动性**

MDS 既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的货币，也没有任何硬资产或其他信用所支持。MDS 在市场上的流通和交易并不是 MediShares 基金会的职责或追求。MDS 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 MDS 持有者处兑换或购买任何 MDS，也没有任何人士能够在任何程度上保证任何时刻 MDS 的流通性或市场价格。MDS 持有者若要转让 MDS，该 MDS 持有者需寻找一名或多名有意按共同约定的价格购买的买家。该过程可能花费甚巨、耗时长并且最终可能并不成功。此外，可能没有加密货币交易所或其他市场上线 MDS 供公开交易。

#### **(18) 价格波动**

若在公开市场上交易，加密货币通常价格波动剧烈。短期内价格震荡经常发生。该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 MDS 交易的二级市场，MediShares 基金会对任何二级市场

的 MDS 交易不承担责任。因此，MediShares 基金会没有义务稳定 MDS 的价格波动，且对此也并不关心。MDS 交易价格所涉风险需由 MDS 交易者自行承担。

## **(19) 竞争**

MediShares 的底层协议是基于开源电脑软件。没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用 MediShares 的源代码和/或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台、虚拟机或智能合约从而与 MediShares 竞争，或甚至赶超或取代 MediShares。MediShares 基金会对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台与 MediShares 产生竞争关系。MediShares 基金会在任何情况下均不可能消除、防止、限制或降低这种旨在与 MediShares 竞争或取代 MediShares 的竞争性努力。

## 9 支持文档和链接

### 9.1 重要信息

官网: <http://www.medishares.org>

Github: <https://github.com/MediShares>

### 9.2 社交网络渠道

Facebook: <https://www.facebook.com/MediShares-1971171169832807>

Twitter: <https://twitter.com/MediShares>

微博: <http://weibo.com/MediShares>

微信公众号: MediShares

### 9.3 联系

E-mail: [reg@medishares.org](mailto:reg@medishares.org)