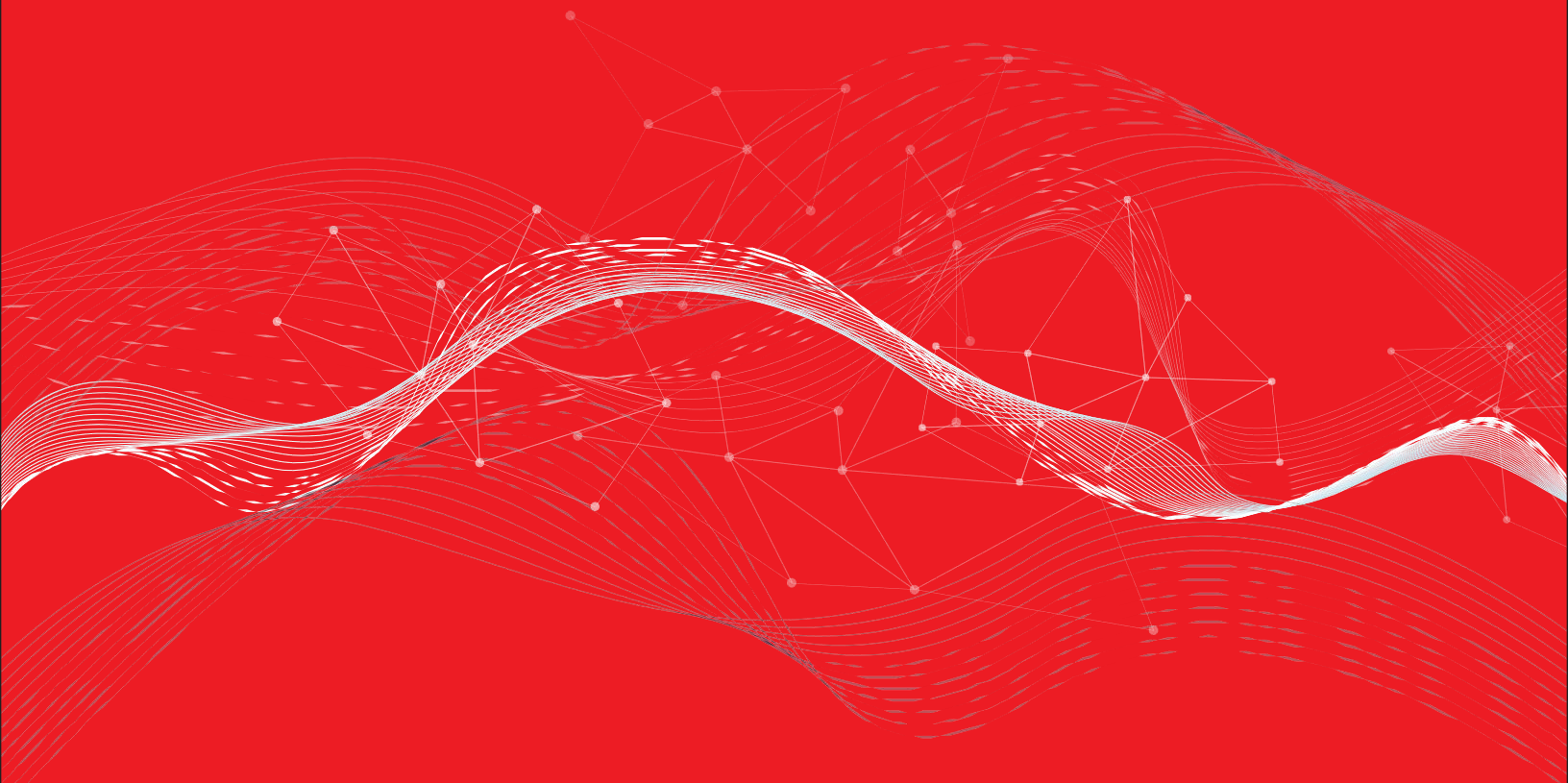




# **MEDIC COIN**



## 目录

介绍	1
特点	2
MEDIC COIN规格	2
Folding@home项目	6
MEDIC电子病历	8
MEDIC远程医疗应用	10
结论	10

## 介绍：

现在市场上充斥着这么多的硬币，为什么还需要另一种硬币？ Medic是一种独一无二的加密货币，它由一个活跃的开发者和发起人，慈善家组成的团队和许多附加产品来支持它。

Medic采用了OpenEMR（开放式电子病历），使其对医生和患者更加有用。开发者将区块链技术引入到了OpenEMR种，使其更加的进步。通过Medic EMR形式的OpenEMR，患者和医生能够使用Medic硬币进行支付。

Medic团队正在努力设计一款基于智能手机的远程医疗应用，允许病人使用Medic硬币支付来咨询在线医生进行诊断。Medic远程医疗应用将与Medic EMR集成，为您提供更加强大完整的电子病历，保障您的健康。

Medic硬币允许您通过POW/POS/MasterNode的方式获得更多的硬币。基于Script算法的POW机制可以让你从每个找到的新区块中获得77个硬币。POS则可以让你赚取39.8个硬币。而Medic的Masternode拥有者可以从每个找到的新区块中获取159.2个硬币。除此之外，如果你帮助斯坦福大学的Folding@Home项目进行蛋白质折叠研究，找到治疗疾病的方法，你可以得到更多的奖励。

我们还有一个专业的营销人员队伍，他们的主要工作是对Medic进行推广，让更多的商家能够接受Medic的支付。他们之前在多个行业有着丰富的营销经验。

Medic硬币是独一无二的，我们努力做好事，让生活更美好。欢迎加入我们，帮助我们一起建立一个强大的社区，为Medic的发展打好基础。

## 特征：

每个POS区块奖励199个硬币，Masternode拥有者分享其中的159.2个硬币或80%的区块奖励。通过POS您可以从区块奖励中获得39.8个硬币或20%的区块奖励。想成为Masternode的拥有者，您需要199999个MEDIC硬币。一个钱包可以同时运行POS和Masternode。同时，您可以在一个钱包中拥有多个Masternode。

每个POW区块奖励77个硬币。每一个区块都会重新调整难度。最后的POW区块是99,999。同时，一旦斯坦福大学的Folding@Home项目开始允许您通过使用CPU/GPU来帮助科学家治疗老年痴呆症，糖尿病和先天性疾病时，您也可以从中获取硬币奖励。

## Medic规格：

名称：Medic Coin

简称：MEDIC

POW算法：Scrypt

困难调整：每个区块

最大区块大小：3MB

最大供应量：500,000,000MEDIC（5亿个）

出块时间：90秒

POS所需币龄：1小时

POW区块奖励：每块77个硬币

最后POW区块：第99,999区块

POS座奖励：199个硬币（80%Masternode/20%POS）

Masternode所需硬币：199,999 MEDIC

## DarkSend简介

DarkSend通过模糊您的资金来源提供真正的财务隐私。你钱包里的所有MEDIC都是由不同的“输入”组成的，你可以把它们看作是独立的硬币组合。DarkSend利用创新的流程将您的输入与其他两个人的输入混合在一起，并且不会让您的钱币离开您的钱包。你随时都可以控制你的钱。

## DarkSend过程

DarkSend通过将您的交易输入分解为标准的面额，这些面额分别是0.01MEDIC、0.1MEDIC、1MEDIC和10MEDIC - 类似于你每天使用的纸币面额。

然后，您的钱包向网络上特别配置的软件节点（称为“Masternodes”）发出请求，通知这些Masternodes您想混合某个面额。该过程中没有可识别的个人信息会发送到Masternodes，所以他们永远不知道你是谁。

当其他两个人发出类似的信息，表示他们也想混合某个面额并且使用相同的面额，一个多端混合开始。Masternode混合这些输入并指示所有三个用户的钱包支付现在转换后的面额（已经分解成标准面额）输入回自己。你的钱包支付给他人的硬币将会来自个不同的地址（称为变更地址）。

为了充分掩饰你的资金，你的钱包需要和Masternode重复这个过程多次。这个过程每完成一次，就被称为“回合”。每一轮DarkSend都会使你的资金源地指数化的模糊。

这个混合过程会在后台自动进行，不需要任何操作。当你想进行交易时，你的资金已经被匿名了，不需要额外的等待。

**重要提示：**您的钱包只包含1000个“更改地址”。每次发生混合请求时，您的一个地址就会被使用。一旦使用了当前的所有的地址，你的钱包就必须创建更多的地址。并且只有启用自动备份才能执行此操作。因此，禁用备份的用户也将禁用DarkSend。

*代码审查K. Atlas 2014*

## DarkSend技术细节（高级用户）

DarkSend是一款独特的分散式混合系统，这个系统被用于模糊化网路上的硬币交易地址。并且这主要是为了加强硬币的流通性，这是货币的属性，它可以让任何没有进入市场的硬币自动加入到交易中，减少了那些没有流通的硬币。如果没有DarkSend，随着网络的增长，没有交易历史的硬币将变得越来越有价值，因为它们很少参与到之前的交易中去。如果长期保持这种状况，那么某些硬币就有可能被列入“红名单”，如果在过去的任何时候被发现用于非法或有问题的活动，就会失去部分或全部价值。没有人愿意持有涉及非法活动的资金，但在DarkSend后，这些硬币重新进入流通，并传递给与先前的非法行为无关的新用户。我们通过实施DarkSend来解决这个问题，它是Medic Coin网络核心协议的一部分。

## DarkSend状态码

系统具有各种模式，使服务器能够跟踪混合池的当前状态。这些混合池是一次性使用，允许三个人同时使用它们。状态为空闲，排队，接受请求，促成交易，签署交易和传输事务。

用户通过连接到处于空闲状态的节点来启动DarkSend。然后Masternode将状态切换到“排队”并向网络发送消息，告诉其他用户目前可以进行混合。用户可以一次使用多个服务器混合，即所谓的多会话混合。这大大加快了混合的过程，但是这是以创建更多地址为代价的，因此需要更频繁的钱包备份。

## 模糊您的隐私

混合是将来自多个用户的多个交易结合在一起的过程，其中关于用户的所有个人隐私信息将从交易中移除。用户通过系统向自己发送硬币，而这些硬币永远不会离开用户的钱包。因此Masternode的操作是完全独立的混合过程。Masternodes只是作为交易的存储和签署的路径，允许用户以安全的方式和匿名的方式启动这个过程。

隐私是通过使用100, 10, 1或. 1的计价金额来实现的。在母节点上启动的每个会话仅包含一个单一的面额，例如具有10x100个Medic Coin输入和10x100个Medic Coin输出。用户单独签名他们的输入到集合输出，允许交易一旦完成并广播有效。

## 费用模型匿名

在混合软件的其他实现中，可以使用费用来分开事务并识别网络上的用户。在Medic网络上，通过允许节点播放无费用的交易的特殊类型的消息来避免这种情况。我们使用这种技术将交易的费用分开，所以使用DarkSend技术的每10笔交易只有一笔需要交易费用。这可以防止对DarkSend的定时攻击。

## DarkSend的阶段

当用户指定一些资金用作“现金账户”时，这个过程就开始了。然后，他们只需简单地告诉一个随机masternode他们想混合一个特定的面额，比如说100MEDIC。由于面额不包含关于用户最终想要混合输入的信息，所以在这一点上，主节点没有任何关于交易的信息。主节点接收到请求并向网络发出一条消息，表示它已经准备好混合这个面额，并且有一个用户正在等待。

此时，如果其他用户希望混合该面额的输入，则可以连接到托管其他用户事务的主节点。当三个用户在同一主节点排队时，下一个阶段“接受请求”被启动。

在这个阶段，所有的用户将他们的输入和输出发送到主节点，在那里它们被收集并存储到内存中，直到所有用户都已经识别出他们想要混合的输入/输出的完整列表。这个过程一旦完成，流程进入下一个阶段，“促成交易”。此时，Masternode会向用户发送一条消息，告知他们正在共同创建合并事务。所有输入都来自用户的钱包，所有的输出都直接发送回用户的钱包。在这个过程中所涉及的资金从来不会离开用户的钱包，从而可以将Masternode与用户的资金完全隔离。这就是DarkSend的过程为何能保持隐匿和安全原因，不会让用户的资金产生风险或让masternodes涉及到任何法律风险。一旦交易被批准，这个过程就进入下一个阶段“签署交易”。

用户只对其输入进行签名，然后将资金释放到所有输出。另外，投入和产出在这个过程中并不直接关联，因为投入是分开的，只是联系在一起。产出也是在一个单独的列表中，只是彼此相关。这意味着，所有的用户都在这个过程中交易。用户不仅自己付钱，其他人也在付钱。

当所有输入签名到所有输出时，交易将变为有效，主节点使用称为DSTX的特殊消息进行广播。网络将跟踪这些消息，允许Masternodes每n个小时提交一次DarkSend交易，而无需支付费用。

## 什么是INSTANTSEND ?

InstantSend是一个先进的服务，允许交易几乎在瞬间完成。有了这个系统，输入可以被锁定到特定的交易，并通过Masternode网络进行一致性验证。如果Masternode网络无法达成共识，则通过标准区块确认来进行交易验证。InstantSend能够解决双重支付问题，并且无需比特币等其他加密货币的漫长确认时间。

## FOLDING@HOME项目和MEDIC

一旦完成了POW的最后一块，Folding@Home项目就会开始让您通过CPU/GPU进行蛋白质折叠相关的计算，从中你可以获得MEDIC。当您做其他事情时，Folding@Home软件依然可以保持运行。当你忙于日常活动时，你的电脑正在努力帮助我们治愈癌症，老年痴呆症，帕金森病，亨廷顿病等疾病。

## MEDIC EMR

### 区块链快速审查

区块链从本质上说是一种新型的数据库技术，经过优化以解决一系列独特的任务。历史上，数据库已被用作中央数据库，以支持事务处理和计算。但是，由于各种技术和安全问题，数据库很少在组织之间共享。区块链是一个共享的，分布在各方的交易数据库，旨在增加透明度，安全性和有效性。区块链是将交易（在两个或多个政党之间）的数据库（跨多个位置或节点复制的数据库的副本）分成块（每个块包含交易细节，如卖方，买方，价格，合同条款和其他相关细节），通过将公共交易细节与两方或更多方的独特签名相结合，由整个网络通过加密进行验证。如果编码的结果对于所有节点来说都是相同的那么这个块将被添加到先前已经产生的区块后面（只要该块被验证），这样该事务就具备了有效性。如果块是无效的，则节点的“一致性”将在不一致节点中进行纠正。

区块链交易比传统的中心化数据库具有以下优势：

**安全性：**区块链依靠加密来验证交易，方法是验证交易涉及的各方的身份。这确保了未经相关方同意，“虚假”交易不能被添加到区块链上。每次将交易添加到区块链时，执行称为“散列”的复杂数学计算，计算取决于交易数据，交易涉及的各方的身份以及先前交易的结果。当前区块的状态取决于先前区块，确保交易不会被恶意更改。如果以前的交易数据发生了变化，它将影响当前的“哈希”值，使这个区块产生错误。

**透明性：**就其性质而言，区块链是一个分布式数据库，在多个节点之间维护和同步 - 例如，由多个交



易方进行频繁交易。另外，交易数据必须在各方之间保持一致才能被添加到区块链中。这意味着通过设计，多方可以访问相同的数据 - 因此区块链相对于依赖多个“隔离”的传统数据库系统显着提高了透明度。

**有效性：**从概念上讲，使用区块链维护数据库的多个副本似乎不会比单一的集中式数据库更有效。但是，在大多数现实世界的例子中（包括我们在资本市场上研究的几个案例），通常存在一些拥有相同交易信息的重复数据库。在许多情况下，与同一交易有关的数据是有争议的，因此需要在各组织之间进行费时费力的对账程序。跨组织使用区块链等分布式数据库系统可大幅降低手动对帐的需求，从而节省大量成本。此外，在某些情况下，区块链可以提高组织跨区域需求，从而消除了跨多个组织重复同一请求问题。

## HIPAA法规和合规指南

在讨论其实施之前，有必要讨论有关1996年健康保险可移植性和责任法案（HIPAA）的问题。其中有几个主要规则，包括云计算准则，隐私和安全规则。本文的主要目的不是要对HIPAA法案进行分析。在讨论相关应用的时候，将明确讨论法案与实施相关的问题。

### 隐私规则

根据Medic EMR业务模式，遵守“隐私规则”是必要的。因为这涉及到私人健康信息的传输和存储。在这种情况下，隐私规则是指使用电子表格转移其工作的其他医疗机构之间的健康计划，医疗保健计划。受HIPAA规则影响的另一方是代表其行事的服务提供商。谈到代理商（也称为商业伙伴（BA）），坚持商业伙伴合同（BAC）至关重要。多年来，HIPAA对上述协议都提出了严格的要求。

从最初的调查来看，有一些优点，包括授权使用这些信息的要求，可用信息和私人信息的定义。可用的健康信息被定义为提供个人身份的健康信息，其中没有可以用于个人识别的信息。当涉及可识别个人信息的时候，需要注意一些问题。例如，在使用或披露可用的健康信息方面没有限制。在这种情况下，这些信息不能提供个人身份，甚至不能提供合理的基础信息来识别个人身份。分辨可用和私人信息的界限是非常重要的。

## 医疗基础设施调查

如今，处方人员可以使用称为电子处方的系统以电子方式传送处方。根据国际移民组织报告“国家卫生保健质量和差距报告的未来方向”，如果处方医生开始采用卫生信息技术作为工具，则可以改善护理质量并降低药物的成本。在处方，描述，管理和病人监护阶段发生的医疗错误可以通过电子处方的采用来减少。

根据各种研究，通过消除手写处方也可以减少用药错误。通过消除这种传统的方式，药房和药房之间的通信时间也减少了。此举也可以避免药品不良事件发生而带来高成本。在一年中，美国的不良药物事件达到约38万至45万。这导致每年额外花费35亿美元。

在电子处方的许多方面，临床决策有大量的计算机化工具，旨在改善病人的护理。临床决策支持包括计算机提醒，药物选择，剂量，过敏和许多其他相互作用的关键点。一旦处方被放置在系统中，病人就会避免这些错误。

## 开源活动

在医疗领域，开源与同行评审相媲美。通过软件代码，用户可以公开测试，试用，试用和批评软件。与其他EMR不同的是，该软件中，用户可以改进，定制和学习编码。通过这种方式，医生们也可以学习许多其他的相关知识。通过开源，我们（病人和医生）对我们使用的工具有了跟多的了解。我可以在没有通过GitHub上课的情况下训练自己的代码能力。

最后，开放源码可以保证不需要支付昂贵的牌照费或入场费。在这种情况下，任何人都可以加入。通过这个社区，可以讨论病人和医生之间共同感兴趣的问题。对于那些想从头开始开源的人来说是一个重大问题，我已经把你覆盖了。尽管开发了许多电子病历，本节重点介绍了医疗电子病历。EHR主要解决了患者可以控制其健康信息的隐私问题。

## MEDIC电子病历

Medic EMR是OpenEMR的一个分支。我们分出OpenEMR并提供支持，并将其与Medic融合在一起，以创建Medic Coin生态系统。医疗电子病历，如OpenEMR，将会使用2次认证。用户将可以从Medic EMR和OpenEMR中获得希望。以下是Medic EMR成为OpenEMR网络后能提供的一些丰富功能。

## 功能丰富的解决方案

在社区中，我们充满活力的志愿者和贡献者十多年来一直维护着OpenEMR的关键功能。拥有超过30种不同语言的支持，多种定制和全面的数据分享。此外，需要帮助用户可以利用我们的志愿者支持网络以及10多个国家的30多家供应商获得帮助。

### 调度

高级时间安排允许诊所创建重复事件，由检入触发的自动化工作，以及患者提醒。

### 电子处方

在系统中输入处方，并将其以电子方式发送到病人的药房。

### 医疗帐单

以标准化方式导出结算数据，包括X12。

### CMS报告

只需点击几下即可生成有意义的CMS使用报告

### 实验室整合

将实验室订单自动发送到实验室，并自动将结果整合到病人的病例中

### 临床决策规则

使用临床决策规则引擎导航复杂的患者算法，以确保为患者提供最高的护理质量。

### 高级安全

HIPAA友好的，细致的访问对象控制和标准的散列密码加密有助于保护您的做法免遭入侵

### 多语言支持

提供30多种语言，并可定制添加更多。

Medic EMR是一个具有区块链功能的开源EMR。随着Medic支付系统的整合，患者可以到医院就诊。医生可以奖励Medic的患者，以控制他们的血压和糖尿病。制药公司可以向Medic Coin的使用医生支付数据挖掘费用。

## MEDIC智能手机医疗应用程序

根据Grandview公司的研究。到2025年全球远程医疗市场预计将达到1131亿美元。市场的主要驱动因素包括慢性病的发病率上升和自我照顾需求的上升。而且，随着互联网应用的不断深入，虚拟医疗和医疗集中化需求将不断增加，这样可以节约许多成本，这是远程医疗市场发展的关键成功因素之一。

虚拟医学是通过减少急诊室访问量和住院率，从而增加市场增长来实现的。远程医疗市场是根据产品和地区划分的。该服务是各个提供商在同一平台上进行通信的主要渠道，从而集中了所有可用的数据。

Medic Phone与Medic EMR集成，为病人提供一整套完整的医疗记录解决方案。Medic Phone是Medic Coin生态系统的一部分。通过Medic Phone，医生可以接受Medic币进行在线访问。

## 结论

Medic Coin的成功对世界至关重要，因为它是独一无二的，并且有潜力有力量去做更多的好事，让生活更美好。Medic Coin的拥有者在享受Masternode奖励的同时，也正在为更好的社会做出贡献。