InDex

下一代去中心化开放金融基础设施

目录

摘要

区块链和加密货币具有许多独特的属性，从比特币到 Libra，人们试图使用区块链技术，建设新的金融体系，解决金融服务包容性、可用性和信誉问题。这些属性包括：去中心化的分布式数据库，确保网络不受单一实体控制；开放访问和开源代码，允许任何能连接互联网的人参与其中；以及运用密码学的安全加密技术，保护数据和价值传输访问的安全；分布式共识机制，保证数据的一致性和可靠性。

我们认为，区块链技术自诞生之初就是为经济系统和金融系统服务的，应该专注于价值领域和金融领域，而不是其它。但现有区块链有限的性能和可扩展性，加密货币具有波动性，阻碍了区块链技术在金融领域的广泛使用。区块链技术这一伟大创新，需要经济与价值作为基础，金融应用实现飞跃。

去中心化金融 Decentralized Finance（DeFi）是未来区块链发展的方向。**InDex** 将专注于这一领域，创造一个更具包容性、可参与性和透明度的金融系统。

InDex 简介

InDex 的使命是为 DeFi 的市场参与者，包含金融市场技术开发者、金融市场机构、金融市场交易双方，建立下一代去中心化开放金融基础设施。InDex 由三个部分组成，它们将协同作用：

- 一个开放的，具备原子交换互操作性多链架构的智能隐私区块链;
- 一个围绕去中心化金融服务提供商、DeFi 项目，分布式应用的服务和生态系统;
- 一个独立的，去中心化的治理机制，激励和协调 InDex 的发展。

我们认为服务和生态系统的培育与建立，与 InDex 技术开发与实现，具有同等的重要性。InDex 引入节点和 Staking 奖励机制，用于激励去中心化金融服务商和开发者。在初期，InDex 通过基金会协调和提供服务和生态系统的培育和管理框架，并牵头进行能够产生积极作用的合作，为在 InDex 上孵化和开发 DeFi 项目和 DApp 应用提供支持。

InDex 生态系统的成员将包括分布在不同地理区域的金融服务提供商、金融机构、多边组织和学术机构。目前已加入的成员包括：

- 金融服务提供商：Digitizing Assets、Swarm Fund
- 区块链行业：UKEX
- 技术平台：KMD Labs、B.S. Labs
- 学术机构：澳大利亚迪肯大学

区块链是独一无二的，因为它们，允许以软件的速度尝试成千上万的治理体系和货币政策；在某些情况下，失败所造成的损失要小得多。我们有机会创造出截然不同的权力分配和制衡结构，并为我们自己规划想要的未来。

InDex 治理分为两个关键部分，激励和治理。激励机制将涉及记账、节点、Staking 等

多种方式，随时间推移 InDex 的不同参与者将提出对他们有利的演进变化。

由于所有组织和参与者不可能始终保持 100%的激励一致性，因此 InDex 的所有参与者围绕共同激励进行治理的能力，对 InDex 的演进变革至关重要。InDex 的治理机制主要是在链与离链两种治理方式，是 InDex 的一项重大课题。我们将与社群、技术平台和学术机构合作，对链上治理的模式和技术进行探索和实施。

无论是 InDex，还是服务和生态系统，以及持续演进的治理机制，InDex 都将开放性作为原则，任何用户、开发者或者机构，都可以使用 InDex 网络，在这个网络上构建产品、服务和应用，并实现增值。这是实现 InDex 使命的基础：建立下一代去中心化开放金融基础设施。

InDex Blockchain

框架设计

InDex 将金融产品的需求融入到区块链底层架构设计中，以符合 InDex 作为开放金融基础设施的定位，整个架构设计将遵循如下思路：

- 安全是金融的核心要素，针对此我们将增强权限管理、网络安全、隐私保护、监督/监管等能力；
- 实现高性能，满足大规模商业应用对于系统的高吞吐、高并发的性能需求；
- 提供由图灵完备的虚拟机，方便智能合约的构建和执行；
- 实现多链并存和跨链技术，解决跨链互操作性和资产流动问题。

至此，整个网络将会分为网络层、共识层和应用层，其中，网络层负责传播交易以及相关信息；共识层负责使节点能够就系统当前状态达成共识，保证分布式系统的一致性；Dapp

应用层：负责更新交易状态（即处理交易），这样，通过三明治结构的架构设计，满足了金融产品的基本需求。

同时，为了保证 InDex 网络的可扩展性（Extensibility）和可伸缩性（Scalability），功能组件将采用模块化设计，并提供了标准定义“DIC Module”，所有的模块都遵循这一标准定义，凡是遵循“DIC Module”的模块，都可以加载到整个网络中来。

目前，DIC SDK 提供有如下模块：

- Auth：多资产账户模型
- Bank：转账相关
- Crisis：系统经济情况处理
- Gov：治理
- Params：系统全局参数处理
- Slashing：对作恶者进行惩罚
- Staking：权益质押
- D-Oracle：去中心化神谕机

技术特性

dPoW 延迟工作证明机制

InDex 提供网络安全性的方式称为延迟工作证明技术（dPoW），它建立在当下最安全的区块链技术——工作量证明技术（PoW）之上，后者是比特币网络所使用的安全技术。从本质上讲，它利用比特币网络的哈希值来保护 InDex。这可以通过将指数区块链的备份存储到比特币分类账上来实现。

延迟工作证明（dPoW）的工作原理是，每隔十分钟，InDex 中一个块的块哈希被写入比特币区块链的块中。这个过程称为公证，它是 InDex 安全机制的支柱。InDex 的公证节点执行成功完成公证所需的技术工作。

InDex 实现 dPoW 的过程相当简单，虽然它提供了令人难以置信的高级别安全性，是一个优雅而简单得安全解决方案，整个过程可以分为 7 个步骤：

1）选择一个特定的比特币区块。由 InDex 上的公证节点进行区块的选择，完成后 InDex 全网络就该块的选择有效并准备进行公证这一事件达成共识。

2）选择哪些公证节点将参与公证。接下来，公证节点必须就哪些节点将参与公证而达成共识。每个需要公证的事务，都需要获得 64 个节点中签名中的 13 个签名，系统将随机抽取 13 个签名提供节点在签名前。

3）向 InDex 主链进行公证。一旦公证节点网络达成共识，哪 13 个节点将参与公证过程后，他们就可以在 InDex 链上创建交易。使用 OP_RETURN 命令，这个公证交易将会将第一步中选择的特定区块的哈希值保存到 InDex 网络中。

4）向比特币网络进行公证。现在，InDex 网络就哪个在比特币网络上的区块将会被公证达成了共识。使用在第三步中同样的处理过程，公证节点将会在比特币网络中执行一笔交易，然后存储 InDex 上的区块哈希值保存到比特币网络中。

5）返回公证结果到 InDex 网络。在比特币网络确认了上一步中所创建的交易，公证节点会广播这条信息在整个 InDex 网络中。这样，被用作公证的块和它之前所有块提供了完全不可变的性质，整个网络不接受删除或更改公证块的重组行为。

6）返回结果到每个 dPoW 保护链的公证。公证节点还向每个采用 dPoW 保护的网络通知公证已经完成。正如上一个步骤所述，一旦采用 dPoW 保护的网络得知块已经工作，那么该块和它之前的所有块都变得不可变。

7）重复整个 dPoW 的过程。InDex 的公证节点网络大约每十分钟重复整个 dPoW 过程，这为所有采用 dPoW 保护的链提供了全天候的比特币网络级别安全性。即使攻击者获得对网络的控制权，他们也无法重新组织已经公证的任何块。由于公证每 10 分钟发生一次，51%的攻击及不可行又无利可图。

公证过程至关重要，因为它保护 InDex 与比特币网络具有相同的安全级别。公证完成后，InDex 不能重新经过公证的区块。在该点之前完成的每个事务都受到 BTC 哈希难度的保护。因此，黑客需要攻破比特币网络，以便在它们破坏或改变 InDex 之前销毁公证的块哈希，显而易见的是，黑客攻击 InDex 至少要花费千万美元（按当下比特币网络）级别的成本，高昂的攻击成本，将使得黑客需要更多的思考，是否攻击。

智能多链技术

InDex 使用创新的多链技术解决了区块链可扩展性问题。在 InDex 平台上启动区块链的所有项目都可以获得本地和独立的区块链。在一条链上发生的事情不会影响生态系统中的其他链条。与此同时，我们生态系统中构建的所有区块链都具有与 InDex 主链相同的隐私和安全功能。

类比于现在互联网，我们为每个项目提供他们自己的高速互联网连接与他们自己的调制解调器和他们自己的路由器。没有共享基础架构。无论您的邻居有多少视频流，您的互联网都不会放慢速度。在 InDex 平台上推出的区块链也是如此。您的项目的性能表现永远不会被生态系统中其他项目的活动所阻碍。

这使得 InDex 与现有的其他区块链平台区别开来。没有其他区块链服务提供商提供这种级别的可扩展性和一流的安全性。虽然您被迫与其他项目共享基础设施，但一些区块链平台可以提供安全性。这增加了拥塞和交易费用，从而限制了可扩展性。

其他区块链平台提供独立的区块链，但在安全方面，您可以使用自己的设备。如果您使用工作证明（PoW）共识机制，这尤其麻烦，因为较小的项目通常没有足够高的哈希难度来保护自己免受 51%的攻击和其他攻击。没有安全性，可伸缩性似乎无关紧要。

智能多链支持凭借 18 种不同的参数，可以定制出数亿种不同的方案，这 18 个参数分别为：名称、区块时间、矿前供应、共识规则、区块奖励、隐私设置、区块奖励减小周期、奖励减小数量、奖励纪元。

智能多链技术提供了一种在区块链上运行程序和应用程序的极其强大而有效的办法。它具备三个特征：

1）图灵完备。支持 C / C ++，这意味着它允许使用图灵完备码。使用 Antara，任何程序或软件都可以编码为在您的智能链上运行。

2）没有 GAS 费用。多链模块没有 GAS 费用，无论执行模块需要多少流程，它都只需要支付一笔交易费用即可。

3）代码自定义化。经验丰富的开发人员可以编写自定义模块，创建更高级的模块进行远程调用。

InDex 是当下唯一为平台上构建的每个项目提供安全性和可扩展性解决方案的区块链平台。

Atomic swaps 原子交换协议

原子交换（Atomic swaps）是一种支持两种运行在不同区块链网络上的加密货币进行快速交换的技术，原子交换本质上是跨链点对点交易。

所谓交易的原子性（Atomic）是指一个单元，其中一个交易应该被认为是最小的，并且不能被分割的。

我们使用哈希时间锁合约来获得这样的一个特性。 哈希时间锁合约（HTLC）是比特币闪电网络的重要组成部分，它们同时也是原子交换的关键组件之一。顾名思义，它们基于两个关键功能：Hash-Lock 和 Time-Lock。

如果没有展示相关的密钥数据，Hash-Lock 会锁定资金的使用。Time-Lock 能够确保智能合约只能在预定义的时间范围执行。因此，HTLC 的使用消除了中心化的需求，它们创建了特定的规则，从而防止原子交换被部分执行。

原子交换如何工作：

原子交换协议的设计方式可以有效防止交易对手间发生欺诈。我们假设 Alice 要将手中的 DIC 和 Bob 持有的 BTC 进行交换。

首先，Alice 将她的 DIC 存入合约地址，该地址类似于一个保险箱。通过该方式创建好安全防护后，Alice 还会生成一个用于访问它的密钥。然后，她与 Bob 共享此密钥的加密哈希值。请注意，Bob 这时候无法获得 Alice 的 DIC，因为他只拥有该密钥的哈希值，而并非密钥本身。

接下来，Bob 使用 Alice 提供的哈希值创建出另一个安全合约地址，用于存入他的 BTC。如果 Alice 要交换 BTC，Alice 需要使用与该地址相同的密钥，与此同时，她也需要将 DIC 的密钥展示给 Bob（借助于 Hash-Lock 的特殊功能）。这意味着，一旦 Alice 提出兑换 BTC，Bob 就能同时获得 Alice 手中的 DIC，该原子交换的交易流程也随之完成。

“原子”一词代表了交易的一致性，即交易要么完全成功要么完全不成功。如果任何一方在交易过程中放弃或未能按照预期执行，合约将被取消，资金将自动返还给其原所有者。

原子交换可以通过两种不同的方式进行：链上和链下。链上原子交换发生在任一种加密货币的区块链在线网络中（在上述案例中，是发生在比特币和 DIC 的区块链网络上）。另一方面，链下原子交换是发生在链下的。这种原子交换通常基于双向支付渠道，类似于闪电网

络中所使用的渠道支付。

跨链智能合约

InDex 的另外一项重大创新技术是跨链智能合约。简而言之，此功能允许不同区块链之间的价值转移，而无需进行交换或交易，这使得通过公证的 Merkle 树和使硬币供应保持恒定的燃烧协议的组合成为可能。

这项新技术创造了区块链互操作性，提供了两个主要优势。首先，如果基金项目在 InDex 上启动区块链，并且单链结构的性能不再足以处理该项目的需求，则可以创建其他链并与第一条链同步，来满足对于性能的需求，这是可能的，因为交叉链智能合约允许多个（或许多）区块链相互通信并作为单个链运行。

这意味着 InDex 生态系统内的所有项目都可以按需扩展，并随业务增长。随着项目需求的增加，可以随时添加更多链条，以便性能永远满足发展的需求。如果一条链不足以满足需求，且没有办法切割它，那么请再添加一条链；如果两个链还不够，请创建第三个链，等等。单个资产链集群中可以存在的链数没有限制。该技术适用于 InDex 生态系统内的所有项目。

其次，作为 InDex 的 MoMoM 扩展解决方案技术的结果，InDex 平台上的任何链都可以验证生态系统中任何其他链上发生的交易。此外，跨链智能合约允许在链之间无缝转移价值，而无需交易或交换。简单地说，一条链上的硬币被烧掉，而价值被允许出现在生态系统内的一个单独的链上。换句话说，它具备完整的区块链互操作性。

通常，实现跨链验证的执行步骤有五个步骤：

1）InDex 平台同步过程中第一步是采用多个块的 Mekle Roots 并将它们定位到 Merkle 树中用来创建新的 Merkle Root。

2）对于 InDex 平台上的每条智能链，重复这个相同的过程，从多个块的 Merkle Roots 中生成单个 Merkle Root。

3）使用 OP_RETURN 命令将来自所有智能链的独特指纹写入 InDex 账本中。

4）然后 InDex 生态系统中所有智能链的所有数字指纹都被便宜成另一个 Merkle 树。生成的 Merkle Root 充当主指纹。

5）最后，主指纹数据被公证回每个智能链的账本中，实现了顶尖的互操作性和可扩展性功能。

零知识证明

零知识证明（ZK-Proofs）早在区块链技术出现之前就已为人所知，但随着分布式账本的出现，进化出了一整套新的可用案例。

简单地说，零知识证明可以让您向验证者证明您知道某些事情，而不会泄露你发送的信息。举例来说，Anna 与 Carl 签署了一份智能合约，Anna 在里面放了 100DIC。并约定 Carl 必须完成一项特定任务，就可以得到智能合约里的 100DIC。

如果 Carl 要完成的任务属于多重机密任务，整个情况就会变得复杂。假设你已经和 Anna 签署了智能合约，获得报酬的条件是完成任务 A、任务 B，以及任务 C。现在你虽然已经完成任务，但是你不想透露关于这些任务的细节给竞争对手知道，因为这是公司机密，这时候就该 ZK-Snarks 出马了。ZK-Snarks 被部署在智能合约中，并提供你已经完成这些任务的证明，当然证明过程不会透露任何消息。这对于保护你个人和公司的隐私都有莫大的帮助。验证过程中 ZK-Snarks 也只会公开部分而不是全部信息，公开部分足够证明你的陈述。

零知识证明运作原理：

ZK-Snarks 由三种算法，G、P、V 组成。

G 是密钥生成算法，它接受的输入包含一个参数 “Lambda”（必须保密，在任何情况下都不能被公开），和一个程序 C。然后生成证明密钥 pk，和验证密钥 vk。这两个密钥都是公开的，任何需要使用的人都能取得。

P 算法扮演证明者角色，需要三个输入：证明密钥 pk、公开的任意输入值 x，还有想证明的知识的陈述，这里我们用“w”代表。P 算法生成证明 prf，使得：prf=p(pk,x,w)

验证者算法 V 会返回一个布尔变量。布尔变量只会返回两种结果：为真（TRUE），或为假（FALSE）。验证算法同样需要三个输入：验证密钥 vk，公开的输入值 x，和证明 prf。

计算 v（vk，x ,prf）如果返回 TRUE，就说明证明者是对的，反之则返回 false。参数 Lambda 的值必须始终保密，因为任何人都可以使用它来生成假的证明。即使造假者不知道真正的陈述 w，这些使用 Lambda 生成的假的证明也会返回 TRUE。

零知识证明如何通过非交互的方式运作：

用离散对数的方式来说明：

Anna 想要向 Carl 证明，她知道一个值 x，使得对一个底数 g，可以得到 y = g ^ x

Anna 从 Z 集合中随机挑选一个数 v，并计算 t = g ^ v

Anna 计算 c = H (g, v, t)，H ( ) 是哈希函数。

接着，Anna 再计算 r = v – c * x

Carl，或是任何人，都可以检查 t = g ^ r * y ^ c

ZkSnarks 的功能实现:

实例函数如下：

```
function C(x, w)

{

return ( sha256(w) == x );
```

```
}
```

函数 C 需要输入两个参数，一个是公开的哈希值“x”，另一个是需要被验证的私密陈述“w”。如果 w 的 SHA-256 哈希值和 “x” 相同，则函数 C 返回 TRUE；反之则返回 FALSE。

Carl 如果作为验证者，他需要做的第一件事，是通过密钥生成算法 G 生成证明密钥 (pk) 和验证密钥 (vk)。

为此，Carl 还需要先生成一个随机数"Lambda"。如同前面说明的，Carl 必须非常小心地保管“Lambda”，因为只要 Lambda 被 Anna 知道了，她就能伪造正确的证明。

生成密钥过程如下：G(c,lambda)=(pk,vk)

两个密钥已经有了，接着 Anna 必须证明自己的陈述的有效性。她将使用证明算法 P 来生成需要的证明。她必须证明自己的陈述 w，在经过哈希运算（SHA-256）后，能得到输出 x。证明算法 P 产生证明的行为如下所示:prf=p(pk,x,w)

现在 Anna 已经有了证明（prf），她将把这个值交给 Carl 来进行 Zk-Snarks 的验证算法环节,v(vk,x,pr).

现在，vk 是验证密钥，x 是已知的哈希值，prf 是 Anna 交给 Carl 的陈述证明。如果验证算法返回 TRUE，则表示 Anna 是诚实的，她的确拥有私密陈述“w”；如果返回 FALSE，则表示 Anna 说谎，她并不知道“w”是什么。

下一步计划是什么?

在具备了性能充足，结构稳定的底层技术框架后，InDex 计划增加功能组件和金融生态应用，以完善创造一个更具包容性、可参与性和透明度的金融系统所需要的必备先决条件。

功能组件

Dapp 开发模块

目前 Dapp 模块开发门槛仍然较高，对于开发者而言不友好。InDex 的 Dapp 开发模块，通过提供完善的软件开发工具包（SDK），各项标准化数据接口开发以及统一的开发语言，降低学习曲线斜率。

一方面降低应用开发者的学习成本，另一方面可以使得开发者有更多的时间专注于应用的开发质量，从而提高 InDex 上 Dapp 生态的整体水平。

该开发模块由 InDex 技术团队负责开发并提供，是开源的，开发者可以在 InDex 的 Github 库中找到。

可编程金融模块

InDex 通过图灵完备的虚拟机和数量庞大的标准模块库，可以方便的按照用户需求进行特定需求的金融模块搭建，这是完全可定制化和高灵活度的解决方案。

这些开放的金融模块，使得地理和环境不再是唯一的先决条件。用户在财务协议方面也具有前所未有的透明度，在签订合同之前了解到每份合同的条款。同样的，金融协议将由智能合约仲裁，这些合约将始终按计划执行，从而消除系统中各类交易对手风险。

目前 InDex 的众多开发者正在尝试建立许多去中心化的基础金融模块。这些多层次金融网络的模块化，可编程性和成本效益将使个人能够达到之前所未有的，更为细致化的财务颗粒度。

金融生态应用

去中心化身份标识

区块链网络中并不要求账户或地址与真实信息进行绑定，但是，对于很多金融应用场景，按相关法律要求，特别是在反洗钱及反恐融资方面，身份认证是必须且必要的。传统方案中，我们进行身份认定时已经向平台方提供了身份信息，存在身份信息泄露的风险。因此，将结合生物识别技术和密码学算法，引入去中心化身份标识，将身份信息进行分布式的加密存储，确保用户身份数据隐私和安全，身份信息控制权重新交还给个人，个人可以做出是否公开、向谁公开等决定。InDex 身份认证协议将遵循 W3C 标准，同时也会寻求和 MicrosoftDID、Sovrin、uPort、CVC、Bloom 等身份认证类项目展开合作

多币种钱包

钱包是用户存储个人数字资产的地方，账户是数字资产流动的起点和重点，在区块链网络中是整个金融网络的原点。因此，一个可靠、易用的钱包应用显得尤为必要。

InDex 网络由于本身支持智能多链技术，可以方便的在一个钱包内支持包括比特币、以太坊、EOS 等主流币和指数币（DIC）在内的多币种存储。

去中心化数据发布器

对于基于差异的金融智能合约，事实上通过“谢林点”协议将数据发布器去中心化是可能的。谢林点的工作原理如下：N 方为某个指定的数据提供输入值到系统（例如 DIC/USD 价格），所有的值被排序，每个提供 25%到 75%之间的值的节点都会获得奖励，每个人都有激励去提供他人将提供的答案，大量玩家可以真正同意的答案明显默认就是正确答案，这构造了一个可以在理论上提供很多数值，包括 DIC/USD 价格，柏林的温度甚至某个特别困难的计算的结果的去中心化协议。

通过这种去中心化的数据提交和验证的方式，完成了现实数据转换到链上数据的过程，解决了目前在区块链世界中预言机（神谕机）缺乏的问题，使用去中心化的投票认证方式，

以这种群体投票选择的手段，提供了数据输入的合理性和公允性，解决了用户无法完成线下数据输入到链上的问题。

加密资产金融服务

基于 InDex 的金融智能合约应用，可为用户的加密资产提供数字商业银行存贷业务、杠杆业务、以及其他金融衍生品服务。

将加密数字资产转入安全的 InDex 金融合约应用的金融账户：您的加密资产将由贝宝的合规加密数字资产托管合作方进行托管，安全可靠，同时用户立即获得无需信用审核的贷款额度，应用将通过智能授信模块，实时为您根据您的加密资产价值，提供相应的稳定币贷款额度。

用户可以选择不同币种和期限存币，以获取固定收益。应用的存币产品通过质押贷款生息，而非交易，安全有保障，无论加密货币市场行情好坏，您都可以赚取稳定数字资产收益。用户也可以申请贷款，实时到账。稳定币贷款将实时发放，可以即时提现使用。由合规托管机构管理超额的质押物，保证存币本息刚性兑付。

开放场外交易市场

OTC（场外交易市场，又称柜台交易市场），柜台交易是指在证券交易所以外的市场所进行的股权交易。英文全称 Over-the-Counter Market，中文翻译为柜台市场。和交易所市场完全不同，OTC 没有固定的场所，没有规定的成员资格，没有严格可控的规则制度，没有规定的交易产品和限制，主要是交易对手通过私下协商进行的一对一的交易。场外交易主要在金融业，特别是银行等金融机构十分发达的国家。针对数字资产的 OTC 交易是一种个人对个人的一种数字资产交易形式，平台只作为中间的担保方。但传统的数字资产 OTC 交易由于缺少监管也存在着被攻击、违反反洗钱规定和恶意欺诈的风险。

InDex 将帮助运行在本链上的应用实现基于金融智能合约和区块链技术的智能数字资产 OTC 交易，从而规避传统 OTC 交易所必须面临的风险。

去中心化交易所

传统的中心化交易所是由中心化平台进行撮合交易，由平台进行信任背书。而在去中心化交易所中，交易双方资产都存储在各自的账户里面。当彼此的订单撮合达成时，卖方调用去中心化交易所的智能合约地址，由智能合约完成买卖双方的币币交易，并返还给买卖双方。整个交易过程中，资产都存储在用户钱包，不需要充值到交易所中。只有当双方达成交易时，交易的数字货币才通过智能合约进行交换。因此中间过程没有第三方，安全性由智能合约来保障。

InDex 上的去中心化交易所允许人们在没有交易对手风险的情况下交易加密货币。该组件是开源的，交易功能可用于任何开发人员连接到去中心化交易所的任何硬币。InDex 将会提供全套的技术方案以供任何人使用。交易所组件完全实现了订单撮合，交易清算，和结算。订单匹配方面是通过原子交换协议来执行的。

广义预测市场

现代化的预测市场，是基于参与者的目标是基于对于某个未来事件尽可能做出最佳预测。这个时间可以是政治选举、明日天气甚至是一场球赛。通过在 InDex 上设置一个高度智能化和中立的神谕机，让一个公平、现代化的预测市场运行在 InDex 上成为可能。整个预测市场的市场价值超过万亿美元，在可预见的未来内，即使仅仅将部分预测市场的价值导入 InDex 生态中来，整个系统也将获得相当可观的价值流入和发展前景。

不管是有神谕还是有 Sherlin 币，预测市场都会很容易实现，带有 Sherlin 币的预测市场可能会被证明是第一个主流的作为去中心化组织管理协议的“Futarchy”应用。预测市场

的出现，同时打通了链上数据和链下数据的交换过程，满足了线上应用的数据取样问题。

一群交易者（真人和机器）买卖份额，基于未来事件的结果出价，这是对 InDex 上的预测市场的最佳描述。

去中心化矿池

大型矿池通过拥有巨大的算力，无形中握住了某条链的命脉，通过庞大算力的使用权利，天生具备给用户带来负面影响的潜力。一些比特币开发者甚至认为这个威胁太严重，必须紧急采取分叉，修改挖矿算法。如果成功，可以淘汰一批现有矿池。尽管很多人对于分叉很谨慎，担心股东不同意；可是这个方法可以阻止矿工滥用权力。

利用 InDex 的金融智能合约解决这些问题，可以在任何加密货币上部署去中心化矿池。去中心化矿池可以提供更加民主的流程，每个矿工可以发起交易。也就是说，该矿池决定交易是否通过的可能性更小。矿工加入矿池的原因是有可靠和稳定的薪水，但是挖矿垄断的风险更大。没有算力的矿工将很难发现区块并获得奖励。

InDex 应用生态发展

与 InDex 一起发展

为了鼓励更多人的参与到 InDex 的生态建设的各个环节中来，我们分别对开发者、应用项目方、持币者进行了分别的基金和计划设立，旨在鼓励他们中的有突出贡献的个人或团队。

如果您是开发者，您可以参与到我们的测试网中来，在这里，你可以提前预览 InDex 即将采用的最新模块和配套的技术文档等，也非常期待您在社区中提出您的宝贵意见，以便

DAO 更好的把握前进方向。

如果您是持币者，希望您可以关注每次的 DAO 的动议和提案，关注整个社群的发展和建设，并提出您的意见和建议，整个社区都在期待您的反馈。

如果您是团队成员，希望能够在 InDex 上发行您自己的应用和项目，我们希望你可以和我们取得联系，以便我们了解您的想法和意图，以便我们给您提供必要的帮助和支持。

开发者基金

为了快速支持开发者，扩大 InDex 生态圈。解决优秀项目的资金短缺问题，特别设立开发者基金，用于支持开发者进一步研发和运营。

申请条件：

- 开发者向 DAO 申请，申请的内容需要包括，产品描述、成果展示（包括但不限于产品链接或者安装包 APK）；
- 需要申请者验证软件所有权；
- 审核标准：产品本身已经达到 DEMO 级别或者更高。
- 资金用途：用来支持申请者进一步的开发或者运营计划。

参与范围：开发者的项目领域包括但不限于基于区块链技术应用场景开发的以下几类：

- Dapps（涵盖金融、支付、游戏、货币、物联网、能源管理、社交通信等领域）；
- 查询、转换、协助开发等一些具有实用价值的优秀工具类应用；

雏鹰计划

区块链技术经过一段时间的发展，逐步得到了更多行业的关注和研究，很多传统企业都

尝试着将区块链技术融入到自身行业中来，解决一些基于数据的痛点问题，包括供应链、票务等环节。

为了区块链行业和 InDex 本身的发展，InDex 团队启动雏鹰计划，将会帮助对区块链技术和 InDex 感兴趣并做出尝试的公司或团队。

该计划将会予以区块链基础知识科普、技术支持和商业模式建议等方面的帮助，同时也将对评估结果较优的项目予以资金支持，起到孵化互雏的功能。

金融合规服务

InDex 作为开放金融基础设施，深知金融合规对于业务展开的必要性和重要性。根据 InDex 自身团队的实际情况，决定成立合规帮助小组，对所有在 InDex 生态上，需要合规建议的团队，予以技术、审计和法律上的帮助，该小组的成立，同时也表示了 InDex 一直以来所宣称和坚持的合规金融区块链上基础设施的初衷。

这些帮助服务是完全免费的，如果产生任何收益，都将捐赠给 DAO，以进一步推动 InDex 生态的发展。

InDex 的治理

InDex 的使命是创造一个更具包容性、可参与性和透明度的金融系统。为了实现这一使命，InDex 需要一个由多元化的独立成员构成的监督实体。

我们将这个监督实体称为 InDex 委员会，一家独立的非盈利性会员制组织，总部位于新加坡。一直以来，新加坡对于区块链技术的开放和支持的态度，是委员会选择在这里的主要原因。InDex 委员会旨在促进 InDex 区块链的运营；协调各个利益相关方（网络的验证

者节点）在推广、发展和扩张网络的过程中达成一致；以及管理储备资产。

InDex 委员会由 InDex 基金会管理，基金会由所有公证节点委派一名代表构成。InDex 基金会成员共同对网络和储备的治理制定决策。所有决策都将通过及机会做出，重大决定或技术性决策需要三分之二的成员投票表决同意。

通过委员会，公证节点得以与网络的技术方案和发展目标保持一致。在这方面，委员会类似于其他非营利性实体，以基金会的形式出现，管理开源项目。由于 InDex 未来的发展依赖于一个分散的、不断成长的开源贡献者社群，因此委员会是一个必要的媒介，就开发和采用什么样的协议或规范给予引导。

在该网络发展的最初几年，需要额外依靠一些角色来替委员会完成下列工作：招募担当公证验证者节点的创始人；为快速启动生态系统而进行筹款；设计和实施激励计划，从而推动 InDex 被广泛采用，包括向创始人发放此类激励奖金；以基金会名义建立社会影响力资助计划。

在未来的某个时间点，由于 InDex 的高度发展和组织状况的稳定，基金会会慢慢退出 InDex 的管理工作，将事务的决定权，决策的执行权和资产的控制权交还给社区，平稳，缓慢地将治理工作交还给社区，实现区块链最本初的社区自治结构。

技术研发路线图

目前，InDex 已经完成了基础的技术架构和模块的开发，DPoW 共识方式在测试网中运行状况良好，赋予了整个网络比特币网络级别的安全性能；具备图灵完备性和可扩展性的智能合约已经完成技术验证，包括作为通证经济底层的 Assets 合约，支持在无信任环节中即时支付的 Channels 合约，允许用户促进、管理其他区块链上资产标记化表示的

Gateways 合约，允许用户设立可继承的去中心化基金的 Heir 合约等等；已经完成了的零知识证明环节，允许用户在完全匿名的状态下，即外界无法观测到任何交易数据的情况下相信转账的可靠度，将自己的资产进行转移或交易；使用原子交换技术，实现了去中心化跨链资产交易的功能。

在既定的项目发展规划上，下一步正在实现包括用以实现 DAICO 经济行为的 PIP（Public Interest Project）、解决开发人员创建和共享解决方案的动态库问题的 Antara 框架等组建正在开发中。

路线图：

2019 年第三季度	实现主网上线，挖矿软件和钱包同步上线； DPoW 共识机制部署； 开放金融资产标准（FRC-20）设立； 第一款应用项目上线，多币种钱包上线；
2019 年第四季度	基于零知识证明技术的匿名交易模块上线； 完成闪电网络的开发并接通相对应的第三方移动钱包； 应用开发文档库建立； 应用开发大赛的举办和开发者基金设立
2020 年第一季度	基于聚合数据的 Oracle 模块上线； 锚定各国法定货币的稳定币模块上线； 官方移动端钱包上线
2020 年第二季度	多重签名功能上线； 原子交换技术模块上线；

	去中心化交易所完成原型开发
2020 年第三季度	智能多链技术模块上线； 即时小额支付模块上线
2020 年第四季度及以后	基于 Dilithium 的数字签名方案添加到 InDex，完成抗量子级别安全性能升级； 升级其他技术模块，吸收和规划其他先进技术模块

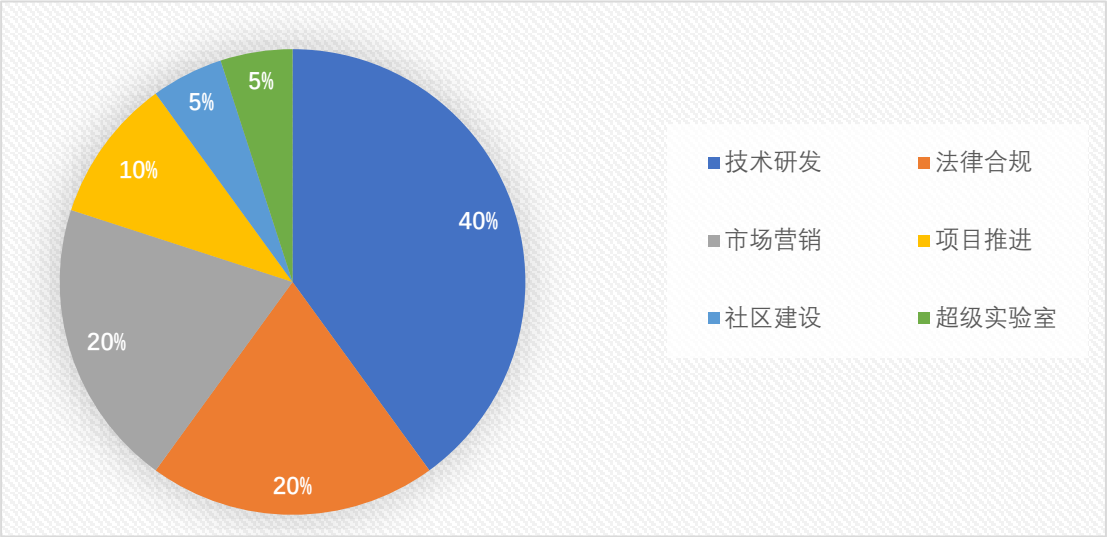
网络基础设定

Digital Index Coin，简称：DIC，是在 InDex 上所有应用场景下使用的交易媒介和流通价值符号。指数币是 InDex 上的燃料，用于支付交易费用、合约执行费用等。

- 总供应量：31 亿枚
- 区块奖励：360 DIC
- 奖励分配：创始团队 20%、节点（Master Node）30%、矿工 50%。
- 区块间隔时间：60 秒
- 减半周期：2 年（前四年）
- 减半机制：初始年产出总量的 6%，第三年起年产出量为总量的 3%，第五年起年产出为总量的 1.5%，并持续按照总量的 1.5%持续产出。

资金使用计划

创始团队所获得的 20%区块奖励将按照以下比例进行分配使用：



团队

技术团队

InDex 的技术团队来自于全球多个国家的区块链技术、密码技术、金融科技和软件工程的专业人员。同时，与包括 B.S. labs. 和 KMD labs 等机构在内的全球多个技术团队展开紧密合作进行技术研发。InDex 的技术研发基于成熟的开发团队和众多成熟技术，从而降低技术开发风险。

技术合作伙伴

KMD labs.

由参与 Komodo 公链开发的全球顶尖的区块链技术专家组成，CryptoConditions 智能合约、原子交换等区块链科学底层技术开发具有非常丰富的经验。

B.S. labs

成立于 2016 年，是由密码技术、金融科技和软件工程等领域的专家和教授组成的资深区块链研发实验室。B.S. labs. 参与了 zenpool 在内的多个区块链项目的研发工作。

管理/顾问团队

Daniel Santos

Token Advisors 创始人兼首席执行官，也是全球董事会的加密货币战略家和区块链顾问。目前，Token Advisors 在 Santos 先生的带领下，为亚洲，澳大利亚，北美和欧洲的客户提供区块链咨询服务。他本人拥有在花旗集团（伦敦），Renaissance Capital（莫斯科）和渣打银行（新加坡）等知名金融机构中超过 15 年的工作经验。

Denis ZNAMENSKIY

应用数学博士，曾担任 ALGOCHAIN 首席技术官，区块链及算法执行官，ZIPQUANT 首席技术官，研究中心负责人。拥有量化团队，对冲基金和初创公司的管理技能。 对区块链技术，人工智能，资本市场，数值方法的数学专业知识具有深刻的理论和实践理解以及强大的分析能力。

Wynn Ho

Wynn 在连续投资和业务顾问领域有超过 25 年经验。通过对许多国家/地区的各个行业的投资积累了丰富的经验，能快速评估和做出准确的决策。曾担任 Cold Storage Singapore，Lion Group Sdn Bhd 高级职位，高科技公司 Pacasa Holdings 的首席顾问；

ET Energy 区域总监；Zheng Cheng Power 首席顾问；PWR Holdings Pte Ltd 首席执行官。

Sky Qiushuo

新加坡、澳大利亚、英国注册会计师，KPMG 高级审计师以及特许财务咨询师，新加坡海外基金会实体设立早期从业者，促成大量初创团队在新加坡的合规化运营，其中包括多个市值在前 100 的项目。

风险提示

是指由于全局性的共同因素引起的收益的可能变动，这种因素以同样的方式对所有的证券的收益产生影响，例如相关政策风险等。同时，系统性风险还包括一系列不可抗力因素，包括但不限于自然灾害、计算机网络在全球范围内的大规模故障、政治动荡等。

团队内风险

InDex 汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链领域的资深从业者、具有丰富经验的技术开发人员等。团队内部的稳定性、凝聚力对于 InDex 的整体发展至关重要。在今后的发展中，不排除有核心人员离开、团队内部发生冲突而导致 InDex 整体受到负面影响的可能性。

项目统筹，营销风险

创始团队将不遗余力实现白皮书中所提出的发展目标，延展项目的可成长空间。目前 InDex 已有较为成熟的商业模型分析，然而鉴于行业整体发展趋势存在不可预见因素，现有的商业模型与统筹思路，存在与市场需求不能良好吻合从而导致盈利难以可观的后果。同时，由于本白皮书可能随着项目细节的更新进行调整，如果项目更新后的细节未被支持 InDex 的参与者及时获取，或是公众对项目的新进展不了解，参与者或公众因信息不对称而对项目认知不足，从而影响到项目的后续发展。

技术风险

首先，本项目基于密码学算法所构建，密码学的迅速发展也势必带来潜在的被破解风险；其次，区块链、分布式账本、去中心化、不同意篡改等技术支撑着核心业务发展，InDex 团队不能完全保证技术的落地；再次，项目更新调整过程中，可能会发现有漏洞存在，可通

过发布补丁的方式进行弥补，但不能保证漏洞所致影响的程度。

黑客攻击与犯罪风险

在安全性方面，单个支持者的金额很小，但总人数众多，这也为项目的安全保障提出了高要求。电子货币具有匿名性、难以追溯性等特点，易被犯罪分子所利用，或受到黑客攻击，或可能涉及到非法资产转移等犯罪行为。

目前未可知的其他风险

随着区块链技术与行业整体态势的不断发展，InDex 可能会面临一些尚未预料到的风险。请参与者在做出参与决策之前，充分了解团队背景，知晓项目整体框架与思路，合理调整自己的愿景，理性参与支持。

免责声明

本文档仅做传达信息之用，文档内容仅供参考，不构成在 InDex 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。

此类邀约必须通过机密备忘录的形式进行，且必须符合相关的证券法律和其它法律。本文档内容不得被解释为强迫参与支持计划。任何与本白皮书相关的行为均不视为参与支持，包括要求本白皮书的的副本或向他人分享本白皮书。

所有参与者均为自愿支持 InDex 平台的发展，在参与之前对 InDex 进行了清晰必要的了解。InDex 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。在开发过程中，平台可能会进行更新，一些实现方式可能随着项目的进展可能会发生变化，我们会在新版的白皮书中进行调整。我们会在官网更新白皮书，请参与者务必及时获取新版本，根据更新内容及时调整自己的决策。

InDex 明确表示，概不承担参与者因为依赖本文档内容、文本信息不准确之处，以及本

文导致的任何行为而造成的损失。团队将不遗余力实现文档中所提及的目标，然而基于不可抗力的存在，团队不能完全做出完成承诺。指数币作为 InDex 的官方代币，是平台发生效能的重要工具，并不是一种投资品。拥有指数币不代表授予其拥有者对 InDex 平台的所有权、控制权、决策权。指数币作为在 InDex 平台中使用的加密代币，均不属于以下类别： a) 任何种类的货币； b) 证券； c) 法律实体的股权； d) 股票、债券、票据、认股权证、证书或其它授予任何权利的文书。指数币的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何价值， 团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。

InDex 平台遵守任何有利于区块链技术及其应用健康发展的监管条例以及行业自律声明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查的所有信息必须完整准确。

InDex 平台明确向参与者传达了可能的风险，参与者一旦参与支持，代表其已确认理解并认可细则中的各项条款说明，接受本平台的潜在风险，后果自担。

结语

以上是对 InDex 生态系统的全面阐述，我们希望通过所有的利益相关者的努力，努力创建一个更为完善、更为可靠、更为易用的去中心化开放金融基础设施和一个高度发达的自治结构的社区。

DeFi 最终是要实现将一切资产 Token 化，自由地在全球市场进行全年不间断交易，并通过发达的互联网网络，重构信任和金融体系，让更多的人，无论他们身处何地，都可以便捷地享受现代化的金融服务，真正的实现普惠金融，通过智能合约自动执行，无需第三方的

托管和审核，没有身份歧视，任何一个人都可以参与的金融体系。