



CDBC

区块链 4.0 生态系统

Focused Block Chain Infrastructure and  
Platform Layer Core Technology

1. 项目背景 .....	.....
.....	4

1.1 2019, 全球区块链高速发展年.....	.....
.....	4

1.2 区块链优势.....	.....
.....	5

1.3 区块链的价值: 机器信任、价值传递、智能合约.....	.....
.....	6

2. 行业痛点 .....	.....
.....	8

2.1 数据云存储的行业背景.....	.....
.....	8

2.2 数据云存储市场规模.....	.....
.....	8

2.3 个人云存储用户规模及预测.....	.....
.....	9

2.4 行业痛点.....	.....
.....	9

3. 项目介绍 .....	.....
.....	11

3.1 CDBC——链接金融, 旨为用户 .....	.....
.....	11

3.2 CDBC 生态体系.....	.....
.....	12

3.3 CDBC 的核心优势.....	.....
.....	13

4. 技术架构 .....	.....
.....	15

4.1 匿名通信技术——P2P.....	.....
.....	15

4.3 共识机制.....	.....
.....	18

4.4 抗量子攻击的哈希和签名算法.....	.....
.....	19

4.5 CDBC 的跨链结构.....	.....
.....	20

5.3 多区块链资产管理	24
6. 发行计划	26
7. 发展规划	27
.....	27
8. 技术团队	28
8.1 基金会	28
8.2 团队成员	28
附录	30
风险提示	30
免责声明	32

# 引言



随着进入“区块链3.0 时代”，最为炙手可热的词汇之一莫过于区块链技术。随后各式各样的“区块链+”的应用便如雨后春笋般涌现，区块链所代表的技术突破为各领域的创新带来无限的可能。当移动支付遇上区块链，又会产生怎样的火花呢？区块链技术又该如何为金融市场赋能呢？

随着大数据时代快速发展，数字货币交易市场比拼较量日渐激烈。一味停滞不前，就会淘汰出局。基于区块链技术的落地应用如火如荼的展开，各行业纷纷布局。目前区块链领域逐渐发展了一些产品方案和赋能实体经济，但真正落地并规范实施的应用稀缺。以“打造支撑各类链上应用的区块链4.0生态系统”为目标而诞生的CDBC，在诸多优秀项目中成功突围，受到广泛认可，与自身团队能力、战略规划有着密不可分的联系。

区块链技术作为对于传统支付模式、移动支付、交易体系数据建设中最好的技术方案。CDBC将区块链的独特优势发挥到极致，迅速推进区块链链上应用，形成基于区块链的完善行业生态体系，将广泛而深刻地改变人们的生活方式。

# 1. 项目背景

## 1.1 2019 · 全球区块链高速发展年

在过去的几年中，区块链因其巨大的应用前景而引发了世界性的关注，并成为一场全球参与竞逐的“军备”大赛。2019年区块链及相关行业加速发展，全球正在拥抱“区块链经济时代”，更多成熟应用加速落地。不可回避的是区块链将重新定义世界。

2019年，世界在变，你的认知亟待升级。

区块链（Block chain）是当下最为热门的新时代技术话题，集分布式数据存储、点对点传输、共识机制、加密算法等计算机技术于一体，被认为是互联网时代又一颠覆式创新。因其在数据存储和信息传输等方面具有巨大突破，很可能从根本上改变现有经济、金融的运作模式，甚至有可能在全球范围引起一场新的技术革新和产业变革。



简单来说，区块链是一台创始信任的机器，是实现互联网向价值互联网的基础设施。在区块链孕育而生的数字经济社会环境下，2018年群魔乱舞，归零币遍地，跑路潮无数。而2019年的区块链行业将打破在区块链热潮下天花乱坠的虚假口号，重塑信任价值，将会吸引越来越多投资者拥抱区块链。

## 1.2 区块链优势

### 不可篡改

不可篡改是基于“区块+链”（block +chain）的独特账本而形成的：存有交易的区块按照时间顺序持续加到链的尾部。一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。区块链系统的信息一旦经过验证并添加至区块链后，链上数据在每个网络节点中均有备份，且不会删除，导致攻击整个网络的成本代价极高，从而区块链网络中的数据具有难以篡改，且唯一可信等优势。

### 隐匿安全

区块链系统中虽然所有的数据记录和更新操作过程都是对全网节点公开的，但其交易者的私有信息是通过哈希加密处理的，即数据交换和交易都是在匿名的情况下进行的。加密简单而言就是通过一种算法手段对原始信息进行转换，信息的接收者能够通过秘钥对密文进行解密从而得到原文的过程。区块链运用了许多成熟的加密算法来保证系统的可靠性和安全性。

## 开放性

基于区块链系统使用开源的程序、开放的规则和高参与度，除交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口了解区块链数据和开发相关应用，整个系统信息高度透明。

## 自治性

区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

## 分布式

区块链分布式的特征也称去中心化，是区块链最基本的特征。在传统的中心化网络系统中，对一个中心节点的破坏即可瘫痪整个系统，而对于区块链网络，由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护，此时攻击某个节点无法破坏整个网络。

## 1.3 区块链的价值：机器信任、价值传递、智能合约

产生的区块链，有什么价值呢？实际上这从区块链的特性上就可以得出结论：去中心化、交易点对点、不可篡改的特性可以实现机器信任；交易不可逆、信息加密的特性可以实现价值传递，此外信息点对点、不可篡改等还可以实现智能合约。

## 机器信任

比如在区块链上, 不存在一个第三方的中心机构, 而完全依靠点对点、不可篡改等交易机制保证双方信任。区块链技术不可篡改的特性, 改变了中心化的信用创建方式, 通过数学原理而非中心化信用机构来降低成本, 建立信用。

## 价值传递

区块链是第一个能够实现价值传递的网络: 一方面, 简单的价值传输, 让数字资产可以在区块链上自由流通; 另一方面, 发行代币, 让融资更加便利, 同时持有者还能享受整个生态的服务 (比如一种代币是基于一种区块链应用而产生, 拥有代币, 代表了拥有应用服务)。

## 智能合约

这一条款以计算机语言而非法律语言记录, 是指将电子合约与区块链技术结合, 当一个预先编好的条件被触发时, 智能合约执行相应的合同条款。



## 2. 行业痛点

### 1. 数据云存储的行业背景

云存储是在云计算(Cloud Computing)概念上延伸和发展出来的一个新的概念，是指通过集群应用、网络技术或分布式文件系统等功能，将网络中大量不同类型的存储设备集合起来协同工作，共同对外提供数据存储和业务访问功能。云存储是一个以数据的存储和管理为核心的云计算系统。简单来说，云存储就是将储存资源分享到一处存储空间，使用者可以在任何时间和地方，透过任意可连网的装置访问该空间。

### 2. 数据云存储市场规模

2016 年，云服务市场规模达到72.6亿美元，2017 年为97亿美元，市场空间巨大。



### 3. 个人云存储用户规模及预测

从个人云存储市场来看，用户规模接近20亿人，市场空间巨大。如此大的用户量也给网盘服务商提出了更高的要求，只有形成技术领先优势，提供更多个性化服务，以及资金实力雄厚的项目才能最终在市场的竞争中胜出。

### 4. 行业痛点

尽管传统云存储具有方便、快捷和成本相对较低等优势，但其本身的机制和存储方式依然存在诸多风险和隐患：

#### 1. 隐私泄露问题

云存储用户可根据自己的喜好随时将设备中的音频、视频等文件快速上传到网盘中，这样不仅可以节省移动设备的空间，还可以在需要时非常快捷的访问网盘中的内容。但实际上，网盘的管理员可以从服务端的平台中直接查看和删除用户上传的文件，鉴于这种管理机制，用户的隐私容易发生泄漏。

#### 2. 数据的覆盖性强，修复能力不够

云存储的多客户端数据一般以最后一次更新为准，其他客户端自动同步。当用户将文件更新保存过后，发现编辑有误，想返回修改前的文件版本时，可能会发现在不支持版本管理的云存储服务中文件副本已经被错误地更新。同样，误删的文件如果没有额外的备份，那么网盘中的数据将会永久丢失。

### 3. 服务器安全性不高

云存储服务器因其特殊的存储方式，早已经成为黑客入侵的首要目标。服务器上存储着大量的用户数据，对大用户群服务的信息劫持更是黑客们收入的重要来源，这就意味着服务器的安全直接影响着用户数据的安全。

### 4. 运营终止的风险

在当下的互联网环境下，云存储服务商提供面向公众的云存储服务，每年的资金投入在 7 千万美元以上，而对私提供的云存储盈利模式还尚不清晰。**IM** 和**Emai**的盈利模式已经成熟，所以相关厂商可以持续免费，而云存储的投入至少是前两者之和的十倍，厂商之间的服务整合和公约形成的首要问题是利益分配，因此服务商们也存在因经营不善而关停服务的可能。



### 3. 项目介绍

#### 3.1 Cloud Data Base Chain——链接金融，旨为用户

Cloud Data Base Chain公链(文中简称“CDBC”)正在构建一个通用、支撑功能完善、性能高、便捷、用户体验好、可扩展的基于增强 DAG 的用的区块链4.0生态系统。为云数据价值传输应用提链基础设施与平台核心技术算法和签名算法，独创双层共识和挖矿机，汇集于CDBC打造生态系统。



CDBC目标是为了补充（甚至是取代）目前统治互联网的超文本传输协议（HTTP），将所有具有相同文件系统的计算设备连接在一起。原理用基于内容的地址替代基于域名的地址，也就是用户寻找的不是某个地址而是储存在某个地方的内容，不需要验证发送者的身份，而只需要验证内容的哈希，通过这样可以让网页的速度更快、更安全、更稳健。

针对现有区块链基础设施普遍存在的实用化程度较低等问题，CDBC研发团队所提出现实可行的解决方案。采取公平分发机制，支持第三方资产发行、跨链通信、多链融合等功能，

链上链下数据映射机制，基于有向无环图(DAG) 和哈希网 (HashNet) 的新型增强数据结构。

在**CDBC**广泛应用后的世界，人们的任何行为和活动均可实现自动支付、自动评价、自动保存、自动判断合法性，人们可以自行选择一生的行为和活动是否保存。

随着人工智能的逐步演进，可以诞生具备个体完整意识、完全自主智能的虚拟人，人们将现实生活中的各种资产完全转移到链上后。代表一个个人类社会个体的虚拟人将和个体资产一起，永远在链上保存和演化下去，实现了人类社会的虚拟永生。这就是**CDBC**网和区块链完整结合后，现实世界和虚拟世界之间的信息映射和价值映射完全实现后的世界。

## 3.2 CDBC 生态体系

**CDBC**充分吸收现有区块链优秀项目的优点，专门解决它们的突出问题和技术缺陷，构建更加繁荣的应用生态体系。**CDBC**创新设计了链上链下数据映射机制，基于有向无环图(DAG) 和哈希网 (HashNet) 的新型增强数据结构，具有交易快速确认、抗量子攻击、节点匿名通信、交易匿名保护、高级智能合约、数据上链等区块链**4.0**的功能特性，并通过采取公平分发机制，支持第三方资产发行、跨链通信、多链融合等功能。

### 我们的目标：

- ◆ 解决数字货币的实际支付问题，让数字资产的管理变得更简单。
- ◆ 构建全球价值**CDBC**网，为价值传输应用提供基础区块链网络。
- ◆ 成为能为底层操作系统提供海量应用的底层公链。

- ✧ 构建遍及各行各业的自由化**CDBC**多维世界。

#### 我们的愿景：

- ✧ 用透明、自治化的数字货币便捷世界各地的**CDBC**使用者。
- ✧ 支持各类实际应用以公有链、联盟链、私有链等形式落地。
- ✧ 囊括所有数字资产，覆盖至全球各行各业、生活点点滴滴。

#### 我们的价值：

- ✧ 锚定最终价值从实际应用起航。
- ✧ 以消费模式为切入，用技术作价值流通。
- ✧ 形成基于区块链的完善行业生态体系。

### 3.3 CDBC的核心优势

**CDBC**面向的应用场景已经不限于区块链**1.0**背景下以比特币为代表的数字货币应用，不限于区块链**2.0**背景下，数字货币与智能合约相结合的金融领域，以及不限于区块链**3.0**在政府、健康、文化和艺术等领域上的应用尝试。

基于**CDBC**的区块链**4.0**公有链将多个行业的基础设施，形成基于区块链的完善行业生态体系，将广泛而深刻地改变人们的生活方式。

- ✧ CDDBC团队搭配及分工合理，技术研发能力强，市场推广能力强，场景落地能力强，能够确保CDDBC实现设计的各种特性。
- ✧ CDDBC团队作为技术提供方，目前已和多个有使用区块链技术优化和提升现有业务流程的公司合作，已将CDDBC基础设施用到多个实际应用领域和场景中，正在开发和实施。
- ✧ CDDBC团队正积极构建合作伙伴联盟，力争将CDDBC应用到尽可能多的行业和实际场景中去。
- ✧ CDDBC团队正积极构建开发者社区，在技术层面确保更多技术人才加入到CDDBC基础设施本身的改进优化和基于CDDBC的DAPP开发中来。
- ✧ CDDBC团队正积极打造区块链技术普及社区，推进区块链技术的普及工作。



## 4. 技术架构

作为一个基于区块链的完善行业生态体系, **CDBC**为整个区块链技术生态提供了完备的发展体系和技术架构。**CDBC**本身的区块链技术是经过普遍证实, 并通过长期实践考验的概念来设计, 代表着区块链技术根本性的进步。更重要的是**CDBC**为整个区块链技术生态提供的基石作用具有里程碑式的意义。

### 4.1 匿名通信技术——P2P

**CDBC**底层通信网络采用P2P 架构, 以及加入节点间匿名访问机制来确保信息服务的隐私保护性。



P2P是peer-to-peer 的简称, 又称为点对点技术, 是没有中心服务器、依靠用户群节点进行信息交换的对等式网络。

区别于传统的C/S中央服务器结构, P2P网络中每一个用户节点即是客户端, 又是服务端, 能同时作为服务器给其他节点提供服务。

P2P 网络的特点如下:

可扩展性在P2P网络中, 用户可以随时加入、离开网络。而且随着用户节点的加入, 系统整体的服务能力也在相应的提高。例如P2P下载中, 加入的用户越多, 则P2P网络中提供的资源就越多, 下载速度就越来越快。

## 健壮性

由于P2P不存在中心化服务器，天生就具备耐攻击和高容错的特点。即使网络中某个节点被攻击或下线，也不影响整个系统的正常运行。因为P2P网络中每个节点都可以充当服务端的角色。

## 高性价比

采用P2P结构的网络，可以有效地利用互联网中大量分散的普通用户节点。充分利用这些普通节点中闲散的CPU、带宽、存储资源，从而达到高性能计算和海量存储的目的。

例如BitTorren就充分利用P2P技术优势，简单而有效地实现了下载压力的分担，从而提供一个高性价比的服务。类似的还有SIA 网盘。

## 隐私保护

在P2P网络中，由于信息的传输分散在各个节点之间，而无需经过中心服务器。这样就减少用户隐私信息被窃听和泄露的风险。

## 负载均衡

由于P2P网络中，资源分散存储在多个节点上，而每个节点又都可以充当服务器的角色。当某个节点需要获取资源时，只需要向相邻节点发送请求即可，很好地实现了整个网络的负载均衡。

## 4.2 数据结构——DAG&HashNet

**DAG**当前的代表项目，最知名的无疑是**DAG**三架马车——**IOTA**、**Byte ball**、**Nano**，作为最新的分布式账本主力竞争技术，**CDBC**在第一阶段采用基础**DAG**结构存储交易数据。

**DAG**（**Directed Acyclic Graph**）即为「有向无环图」。有向无环图中的交易验证机制也和区块链不同，它是由后一笔交易来对前一笔交易进行验证。也就是说你如果想进行一笔交易，就必须要验证前面的交易（具体需要验证几个交易，则需要根据具体的规则而确定）。

发起者一边提交自己的交易，一边验证别人的交易，以此编织着一个去中心化网络，如果一笔交易没有被后面的交易验证，它也就失去了在整个体系中的合法性。这样的交易验证机制，使得**DAG**可以并发地进行多笔交易，最终组成了一种树状的拓扑结构图，这种树状结构极大的提升了整个系统的扩展性和交易速度。

与传统区块链相比，**DAG**具有以下独特优势：

### 更快的交易速度

与区块链技术不同，**DAG**技术最大的特点是没有区块，系统不需要定时出块，这也就明显的加快了交易速度，也实现了同时容纳海量并发交易。并且在**DAG**中参与交易的人越多，交易确认的速度也就越快，这个独特优势对于**DAG**的后续快速发展是非常有利的。

### 无交易费用或者极低的交易费用

在DAG系统中是没有矿工这一角色的。系统的一致性是由交易本身来维护，即每笔交易发出时都需要验证之前未确认的交易，并立刻广播至全网，从而形成互相联系的数据网络。通过这种方式，交易和验证同步进行，网络能够有效保持去中心化。DAG通过把交易确认环节直接下放给了交易本身，因此也就有可能实现无手续费交易了。

### 无需挖矿，减少了资源浪费

根据 Power Compare 的研究，全球用电量的0.13%的正在被用于了比特币挖矿。而DAG中是没有矿工这个角色的，不会产生大量的哈希运算，也就节省了大量的社会资源，这对整个世界的运行是非常重要的。

HashNet 是一种有向无环图（DAG），是由无数个顶点和连接顶点的有向边组成。HashNet为维护大型公共分布式分类账的计算和交流困难提供了一种新颖的解决方案。关键的创新是高效的异步分布式共识协议，适当设计有向无环网络结构。

## 4.3 共识机制

CDBC采用POP（Proof of Powers）共识算法，通过以过去获取权利记录的量为参考，历史记录量越多获取记账的权利越大。在过去1000个记录块中，信用记录次数越多者，将拥有更大概率获得在下一个块中记录信息的权利。在一定时间内，谁先推算出满足目标值的Hash，谁就可以先得到记账的权利，并且此时会影响到获取下一个块获得记录权利的难度。在未来一定时间内，如果没有下一个块被计算出来，而此时拥有更大权利的节点推算出同样高度的块，

则认为权利大的节点的块是最长链。但这种机制，并不是一直是权利大的节点，持续获取记录权利：其他节点（权利较小的）想要获取记录资料的权利就只需要提升算力，使得推算速度增加，获取当前的记录权利难度减小；权利大的节点，不一定能在其他已提升算力的节点之前获取到记录的权利。

## 4.4 抗量子攻击的哈希和签名算法

### 哈希函数

哈希函数（Hash Function）是加密算法哈希算法中广泛应用的一种函数，也称为散列函数或杂凑函数。哈希函数作为公开函数，可以将任意长度的消息  $M$  映射成为一个长度较短且长度固定的值  $H(M)$ ，称  $H(M)$  为哈希值或者消息摘要（Message Digest）。哈希运算是一种单向密码体制，即一个从明文到密文的不可逆映射，只有加密过程，没有解密过程。

它的函数表达式为： $y = H(x)$ ，同时哈希函数具有碰撞阻力、隐秘性、谜题友好三个特性，它们各有侧重，但又相互贯通。

Hash 函数  $H$  将可变长度的数据块  $M$  作为输入，产生固定长度的 Hash 值  $h = H(M)$ 。称  $M$  是  $H$  的原像。因为  $H$  是多对一的映射，所以对于任意给定的 Hash 值  $H$ ，对应有多个原像。如果满足  $x \neq y$  且  $H(x) = H(y)$ ，即两个不同的输入  $x$  和  $y$  产生相同的输出  $H(x) = H(y)$ ，则称为碰撞。如果对于哈希函数  $H(x)$ ，没有人能够找到碰撞，则称该函数具有碰撞阻力。

隐秘性指的是当输入  $r$  选自一个高阶最小值的概率分布，在给定  $H(r||x)$  条件下确定  $x$  是不可能的。简单的说，就是无法从输出得到输入。设  $y = H(x)$ ，如果我们知道  $y$ ，很难迅速找到满足符合条件的  $x$ ，则称哈希函数  $H(x)$  具有隐蔽性。隐蔽性意味着几乎不可能找到其反函数  $x' = H'(y)$ ，

实际上满足条件的 $x$ 应该多个，这里隐蔽性要求哪怕1个也找不出来。这是因为上面提到的哈希函数单向性，对于给定的Hash 值，在 $2^{128}$ 次哈希计算量下是不可行的。

如果对于任意 $n$ 位输出值 $y$ ，假定 $k$ 选自高阶最小值分布，如果无法找到一个可行的方法，在比 $2$ 的 $n$ 次方小很多的时间内找到 $x$ ，保证  $H(k||x) = y$ 成立，那么我们称哈希函数 $H$ 为谜题友好。在搜索谜题这个应用中，我们将建立一个搜索谜题，该谜题是一个需要对庞大空间进行搜索，才能找到解决办法的数学问题。简单来说，就是要求具有随机性，任意输入可以得到固定位数的输出，很难找到输入和输出之间的任何关联性，哪怕是稍微调整输入，得到的输出都具有随机性，除了通过调整输入内容进行“暴力试算”，没有其他更好的办法。

## 数字签名算法

哈希算法可以保证交易数据不被篡改，但是无法保证对数据和摘要同时的替换攻击，同时也不能保证交易数据的不可否认性。数字签名算法涉及到公钥、私钥和钱包等工具，它有两个作用：

- 一、证明消息确实是由信息发送方签名并发出来的，保证不可否认性。
- 二、确定消息的完整性。 数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用哈希算法对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性并保证信息的不可否认性。

## 4.5 CDBC 的跨链结构

人类社会的发展历程经历了原始单部落模式，到多部落模式，到不同文化生境，再到不同体制的国家。互联网的发展也是经历了单机时代，多机简单互联，多机局域网，再到各种异构的局

域网互联，然后到上世纪末的全球PC互联网，再发展到今天的移动互联网。区块链的发展，从最初1.0时代以比特币为代表，发展到2.0时代以集成了智慧合约的以太坊为代表，再到今天各种多链（跨链）区块链产品。



## 单链结构

经典的区块链网络，比如比特币网络、以太坊等都是采用单链结构，所有的事务和交易都是在一条链上进行。单链结构的优点是交易和共识流程比较简单，在区块链发展早期能够很好地满足用户需求。但是随着区块链技术的发展和市场对区块链的需求不断增强，单链架构逐渐暴露出很多无法解决的痛点：

### ✧ 整体输送量和性能存在瓶颈

比特币有7TPS以及需要6个区块的确认机制，以太坊间隔也需要10-20秒，这些都严重阻碍了日益增长的区块链业务发展需求；

## ✧ 链内业务相互干扰

单链架构很容易由于个别业务的繁忙而造成整个系统拥堵，比如最近风靡一时的数位加密猫 **Crypto Kitties** 就使得整个以太坊网络变得拥挤不堪，很多正常的交易都得不到及时处理和确认；

## ✧ 封闭的网络结构

无法实现不同链之间的跨链交互，无法满足多平台之间的业务交互需求。多链结构为克服单链结构的局限性，多链结构被提出，主要形态有多条平行链，主/侧链等，部分满足了业务多样化的需求，但在灵活性和定制化上还存在不足。

对于多条平行链，各条链的功能通常是预先设定好的，难以满足快速变化和多样化的业务需求，同时如何在多条链上共享计算和资料资源也没有得到很好的解决。

对于主/侧链结构，可以根据业务的增长和变化而派生出不同的侧链，但侧链的共识与主链耦合比较紧密，主链有可能成为新的中心和瓶颈。

# 5. 与区块链结合的 CDBC 多领域生态应用

## 5.1 构建分布式一体化社交生态



在**CDBC**平台，全球任何一个地方的用户都可以无国界相互联系和生意上的往来，并通过**CDBC**的 TOKEN进行交易和兑换成法币。

任何对由强认证、高隐私、弱关系，强个性用户构成的社交网络感兴趣的个人与组织均可考虑加入到**CDBC**生态中，参与生态建设。

**CDBC**承诺在恰当的时候开源认证、隐私加密、**CDBC**钱包等底层协议、代码、模块，对于系统的开发者只要满足相关的协议，对于APP开发者只要内嵌了**CDBC**模块即可连接到**CDBC**区块链网络中。**CDBC**也会协助生态上的其他组织编写链上智能合约，加速DAPP开发进程。

**CDBC**会开放全网分析平台，欢迎第三方组织（如广告）直接使用**CDBC**的数据以及有价值的分析结果，直接定位到最有价值的用户；同时也欢迎第三方组织提供服务（如：金融、娱乐、电商等），创造价值。

第三方个人或组织需采用**CDBC**，依据链上提供或者消耗的实际资源，采用细粒度计价的方式交易，类似于云计算计付费的方式。任何组织和个人均以区块链节点的方式接入区块链，不享有任何特权。

## 2. 金融交易应用

CDBC金融应用板块拥有数字银行、法币交易（OTC）、现货/币币交易、合约交易、杠杆交易、猜涨跌、量化交易等一站式服务体系，而其发行的CDBC代币则主要用于交易服务手续费、平台功能拓展、多项权益，支付系统支持跨境支付、站内支付、站外支付三种跨区域，实现生态价值回报等，支撑跨纬度的支付方式。



## 3. 多区块链资产管理

### 一站式管理

CDBC通过一个钱包应用里统一管理多种数字货币，不仅支援比特币、以太币等主流资产的存储和管理，也支援以太坊、Achain、Kchain 等智慧合约平台的标准协定，快速增加基于各平台发行的代币，在减轻用户管理负担的同时，也为新项目提供钱包服务支援，让项目团队更专注于核心服务。

## 去中心化服务

**CDBC**坚持区块链的核心要义，为用户提供去中心化的数字货币存储方案，钱包金钥和所有类型货币的位置私密金钥信息都存储在使用者本地系统里。同时**CDBC**提供便捷的金钥备份方案——用户只需进行一次备份，记下多个单词，保存到安全的地方。

## 多重安全保障

除了让用户完全控制钱包金钥，**CDBC**还针对不同规模的数字资产管理，提供多重签名技术保障和两步授权验证，使用者可以选择在转账交易时进行手机验证码、指纹、活体等验证方式，全方位保证数字货币资产安全。

## 多语言支援

**CDBC**将支持中、英、日、韩等主流数字货币市场多种语言，为打造世界级应用扫清语言障碍。



## 6. 发行计划

CDBC全球发行10亿。

### 分配方案

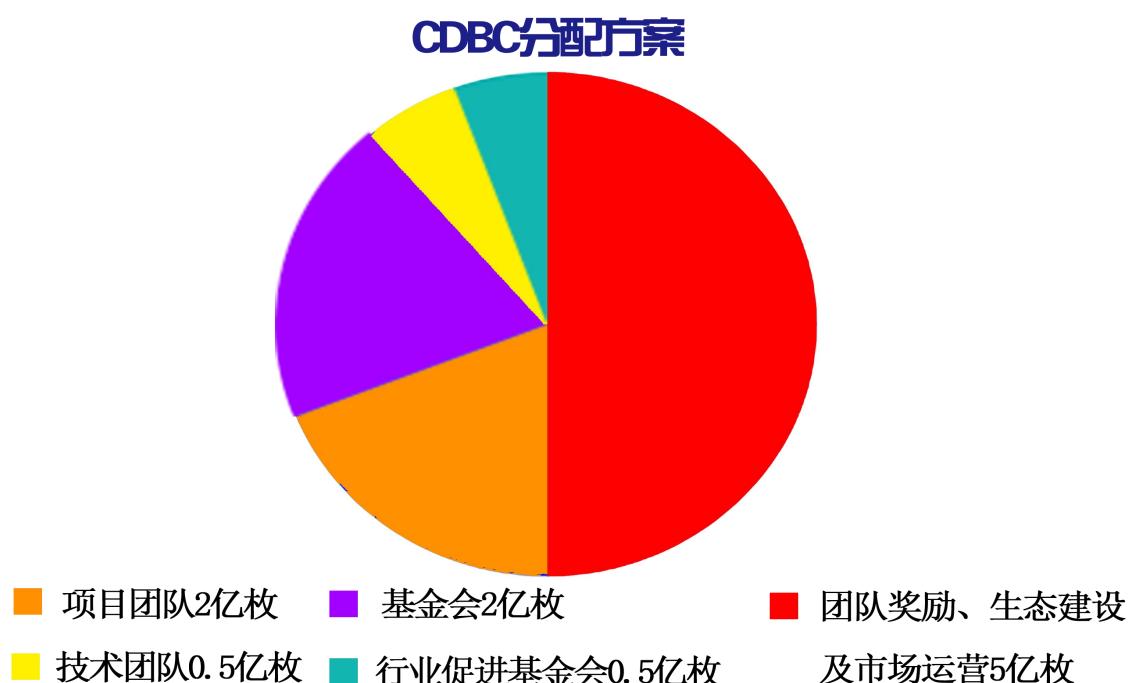
项目团队20%: 2亿枚

基金会20%: 2亿枚;

行业促进基金会5%: 0.5亿枚

技术团队5%: 0.5亿枚

团队奖励、生态建设及市场运营50%: 5亿枚



## 7. 发展规划

第一阶段，完成CDBC公链开发  
(已完成)

整理并发布新版白皮书，构建  
多维生态应用渠道

第二阶段，完成并完善CDBC  
公链生态初步建设

CDBC将促进社群的发展，为第三方  
提供智能合约确立相关路径

第三阶段，打造支持 各类链  
上云服务应用的区块链4.0生  
态系统，提供多元化云存储服  
务

CDBC生态系统接入，各类公链应  
用成功落地

# 8. 技术团队

## 1. CDBC基金会

**CDBC**基金会是非营利性组织，基金会通过设立相关部，致力于**CDBC**的研发，对**CDBC**的开源、社区建设、特性建议的审议等进行管理；同时致力于项目本身的财务、团队建设、对外关系等，使得项目更好的运行。

## 2. 团队成员

**CDBC**团队拥有多年深耕数字货币市场经验，以下是团队成员介绍：

姓名	背景
Luois Cheung	CTO，博士。主要研究方向为分布式计算技术，共发表高水平论文30余篇，撰写专著4部。主持和参与高级别科研项目10余项。一直从事P2P系统架构设计，对双层结构对等计算拓扑有深度的认识。
Roger Michey	首席架构师，博士。主要研究方向为分布式计算，共发表高水平论文20余篇。在分布式系统的可扩展性、可靠性以及弹性优化处理方面有深刻认识，对区块链底层技术和工作原理有深刻理解和实际操作经验。

Jason Loong

**CDBC** 安全事业部负责人，计算机科学与技术博士。致力于区块链以及网络安全的研究，在智能合约等方面有多年的研究基础。主持和参与包括国家自然科学基金、国家级科研等科研项目10余项，曾发表SCI、EI学术论文30余篇。

Andy

**CDBC**生态建设负责人，计算机技术博士。研究方向为机器学习与智能信息处理等，从事大型信息系统与分布式应用实践，具有丰富的产品研发和系统设计经验。较早开始区块链的研究，对区块链的应用与生态构建具有深刻认识，曾发表高水平论文20余篇。

Storm Zhang

工学硕士、高级程序员以及区块链技术专家，在IBM（International BusinessMachines Corporation）的系统科技部以及新浪工作多年，具有丰富的Hadoop 及Map Reduce 开发经验。2012年接触比特币，熟悉加密货币原理，交易所钱包的存储对接方案，目前专注于智能合约和区块链应用方。

# 附录

## 风险提示

在**CDBC**的开发、维护和运营过程中存在着各种风险，这其中很多都超出**CDBC**开发者所能控制的范围。除本白皮书所述的其他内容外，请参与者充分知晓并同意接受了下述风险。

### 市场风险

**CDBC**价格与整个数字货币市场形势密不可分，如市场行情整体低迷或存在其他不可控因素的影响，则可能造成**CDBC**本身即使具备良好的前景，但价格依然长期处于被低估的状态。

### 监管风险

由于区块链的发展尚处早期，在全球没有有关募集过程中的前置要求、交易要求、信息披露要求、锁定要求等相关的法规文件。并且目前政策会如何实施尚不明朗，这些因素均可能对项目的发展与流动性产生不确定影响。区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则 **CDBC**可能受到其影响，例如法令限制使用，**CDBC**有可能受到限制、阻碍甚至直接终止**CDBC**应用和发展。

### 竞争风险

当前区块链领域项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。**CDBC**项目是否能在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、战略规划等方面挂钩，也受到市场上诸多竞争者的影响，存在面临恶性竞争的可能。

## 人才流失的风险

**CDBC**汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链的资深从业者、具有丰富经营的技术开发人员。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**CDBC**整体受到负面影响的可能性。项目技术风险密码学的加速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给 **CDBC**平台，这可能导致**CDBC**的数据丢失。项目更新过程中，可能会出现漏洞，漏洞发现后会及时修复，但不能保证不造成任何影响。目前未可知的其他风险除了本白皮书内提及的风险外，此外还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其它风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。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，理性参与。



## 免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在**CDBC**及其相关公司中出售股票或证券的任何买卖建议、教唆或邀约。本文档不赞成也不理解为提供任何买卖行为，也不是任何形式上的合约或者承诺。鉴于不可预知的情况，本白皮书列出的目标可能发生变化。虽然团队会尽力实现本白皮书的所有目标，所有购买**CDBC**的个人和团体将自担风险。文档内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。本文档仅供主动要求了解项目信息的特定对象传达信息使用，并不构成未来任何投资指导意见，也不是任何形式上的合约或承诺。

注：

- a. 本项目涉及的**CDBC**是一个在交易环节中使用的虚拟数字编码，不代表项目股权、收益权或控制权。
- b. 由于数字货币本身存在很多不确定性(包括但不限于：各国对待数字货币监管的大环境、行业激励竞争,数字货币本身的技术漏洞)，项目将有一定的风险。
- c. 虽然团队会努力解决项目推进过程中可能遇到的问题，但未来依然存在政策的不确定性。大家务必在支持之前了解区块链的方方面面，在充分了解风险的前提下理性参与。团队将努力实现文档中所提及的目标，但基于不可抗力的存在，团队不能做出完全承诺。