量子链
Qtum

# QTUM BLOCKCHAIN ECONOMY WHITEPAPER

# 量子链区块链经济白皮书（草案）

量子基金會
foundation@qtum.org

# 目录

# 摘要

Qtum Blockchain （简称“量子链”或“Qtum”）致力于开发比特币和以太坊之外的第三种区块链生态系统，通过价值传输协议（“Value Transfer Protocol”）来实现点对点的价值转移，并根据此协议，构建一个支持多个行业（包括金融、物联网、供应链、社交、游戏等）的去中心化的应用开发平台（“DApp Platform”）。由于技术上的创新、治理结构完善、应用范围广，量子链将成为优于比特币和以太坊的公链：

- **从技术角度分析**，量子链具有强大的开发团队，通过引入 Identity、Oracle 和数据馈送（Data feeds）机制，并兼容比特币改进协议（Bitcoin Improvement Proposals） 的 UTXO 交易模型，实现了首个基于 IPoS（激励权益证明）共识机制的智能合约平台。在合规性方面，也符合不同行业的监管需求。

- **从治理角度分析**，量子链设立量子链基金会，致力于量子链的开发建设、治理透明度倡导和推进工作，促进开源生态社会的安全、和谐。通过制定良好的基金会治理结构，分别从代码管理、财务管理和公共关系等多个维度帮助管理开源社区项目的一般轶事和特权事项，从而确保量子链的可持续性、基金会内部管理有效性及募集资金的安全性。

- **从量子链应用角度分析**，量子链通过“去中心应用”和“主控合约”将链下因素引入，形成符合现实世界商业逻辑的区块链主控合约，支持多个行业、多种渠道，最终实现走向移动端策略（Go Mobile）。在量子链的生态系统中，我们将会与第三方开发者一起，从技术架构支持提供移动端的服务，包括：移动端钱包、移动端 DApp 应用、移动端智能合约服务。 我们也鼓励第三方的开发者加入我们，一起开发区块链的移动端服务，共同推动区块链技术的落地。

作为最有前景的区块链生态系统，量子链完美地结合了比特币和以太坊的优点，并解决了现有区块链系统的固有缺陷。量子链将持续通过基础平台的搭建，以及各产品的开发和商业化落地项目的发展和迭代，逐步形成区块链经济，提升行业效率，促进社会的高效协同发展。

量子链，定义区块链经济。

# 第一部分 量子链的设计理念

## 1.1 区块链出现的背景和意义

在比特币诞生之前，全球信息传递都是通过互联网的 TCP/IP（传输控制协议/因特网互联协议）协议来实现高速低成本的传输，但是随着互联互通技术的发展（互联网、物联网、VR/AR），人与物体、人与信息的交互方式更加多样化，更多的实体被数字化或者代币化，仅仅是信息的分享和传输并不能满足经济社会的发展，因此当实体被数字化或者代币化之后，人们越来越关注到价值转移以及如何点对点传输这些资产和价值。

在 2008 年 10 月 31 日，Satoshi Nakamoto 第一次发布了比特币的白皮书《比特币：一种点对点网络中的电子现金》，并提出了通过去中心化的比特币网络实现价值转移。在比特币体系中，全网参与者均为交易的监督者，交易双方可以在无需建立信任关系的前提下即可完成交易。区块链技术改变了我们获取和分享信息的方式，创造了一个新的分布式、点对点的生态社会。

在比特币网络出现之前，我们一直无法在不借助于第三方受信机构的情况下，通过互联网进行点对点的价值的转移和传输。比特币网络则是运行于信息高速公路上面的第一个 Value Transfer Protocol （“VTP 协议”）。在本白皮书中，我们也第一次归纳和提出了互联网应用层 VTP 协议的概念。

目前，随着区块链技术的成熟，区块链的应用场景不仅限于比特币和以太坊，量子链试图将区块链链上和链下相结合，形成第三个区块链的生态环境，进一步使用 VTP 协议实现点对点价值传输。

## 1.2 为什么设计量子链

自从 2009 年比特币代码开源以来，社区里面出现了很多代币和其他区块链项目，还包括致力于成为通用智能合约平台和去中心化应用平台的以太坊项目，但是区块链行业不论是从技术角度，还是行业应用角度都还面临着很多挑战。主要问题如下：

1. 缺乏新型的智能合约平台。比特币生态和以太坊生态由于缺少与现实社会的连结，使各行业的广泛应用受限；

2. 不同区块链平台之间的兼容性。比如基于 UTXO 模型的比特币生态和基于 Account 模型的以太坊生态无法兼容；

3. 共识机制本身缺乏灵活性。因为参与者的不同，在公有链中和联盟链中，对共识机制的要求不尽相同；

4. 缺乏对行业合规性的考虑。例如在金融行业要求的尽职调查，如背景调查和 KYC（“Know-Your-Customer”）部分，在现有的区块链系统中，难以实现；

5. 现有区块链系统具备很大的封闭性。目前大多数智能合约仅接受链上数据作为触发条件，缺乏与现实世界的交互。

我们希望可以构建一个全新的区块链生态系统——量子链，作为未来世界可选的互联网价值传输协议，并把整个区块链行业的易用性向前推进一步。

量子链是基于 UTXO 的智能合约模型，面向公有链灵活的共识机制，实现比特币和以太坊的兼容。另通过 Oracle 和数据馈送（Data Feeds）的设计和实现等，使得量子链成为区块链世界与现实商业世界的桥梁。

## 1.3 量子链的设计原则

针对区块链技术和行业应用局限性的各种问题，量子链提出的改进方案如下：

1. 引入全新设计的主控合约，通过链下数据和链上数据的共同输入作为触发条件，完成合约的执行；

2. 实现区块链技术之间的兼容性；

3. 面向公有链的灵活共识机制；

4. 增加对行业合规性的考虑，提供可选的身份识别模块；

5. 通过链下数据作为主控合约触发条件，实现与现实世界的交互。

除此之外，量子链在开发过程中还加入了模块化的设计和易用性的考量。为了便于开发和维护，将量子链分为三大模块，分别为量子链技术模块、量子链用户交互模块和量子链商业路径模块。

为了对应不同用户的操作系统和开发需求，同时也真正做到开源，我们提供不同版本的 Qtum 系统，另外还提供移动端的服务，鼓励第三方的开发者，与我们一起推动区块链技术在中国的落地，开发出普通互联网用户可以使用的区块链移动端服务。

## 1.4 量子链的愿景

量子链致力于通过社区、第三方开发者和技术上的创新，打造一个在全球具有影响力的开源社区生态，最终目的是将区块链融入到金融、社交、游戏、物联网等不同行业。量子链是有兼容性的生态社会，并且通过融入监管的逻辑，通过 Oracle 和 Data Feed 架起区块链与现实商业社会的桥梁。

**技术上创新**：量子链打造的是一个安全可靠并且与以太坊社区和比特币系统兼容的平台，通过技术和理念上的创新实现链上与链下相结合。

**可持续发展**：为实现量子链的可持续性发展，避免散沙式的发展结构和底层构架分化，量子链基金会将制定完善的治理架构，对一般轶事、代码管理、财务管理、薪酬管理和特权操作范围等事务进行管理。同时，治理架构会随着基金会和社区的发展不断更新，并引入监察和监督功能，规则制定和变更控制管理等。

**商业应用**：量子链基金会将参考投行的做法进行行业分析和筛选，选择适当的行业推广量子链技术应用，让企业在量子链上进行开发和应用，同时也促进量子链的可持续发展。

**合作伙伴**：量子链基金会通过与合作伙伴的通力合作，将企业、商界、技术和政府等多方面资源进行整合，最大化实现资源共享，最高效利用资源，实现社会协同发展。

量子链基金会还将提供透明的财务管理，全面的代码管理并协助量子链进行商业落地。同时，基金会将保持高标准的诚信和道德的商业行为，遵守相关的法律法规。此外，量子链基金会将聘用第三方机构提供相关工作审计报告，合规治理和监督。

为进一步使量子链成为完全开源社区生态，量子链基金会最终将 80%的量子币发放给社区，用于商业应用、市场推广等帮助实现真实世界与区块链世界的结合，剩余 20%量子币奖励创始团队、早期投资者、顾问和开发团队。

从量子链的雏形阶段、开发阶段到正式推出，得到了包括创始团队、开发团队、行业专家、早期投资者、律师和咨询顾问等社会各界的大力支持。在此感谢以下为量子链区块链经济的发展做出卓越贡献的人员（部分名单）。

| | | |
|---|---|---|
| 帅初（联合创始人） | Neil Mahi （联合创始人） | Jordan Earls （联合创始人） |
| Anthony Di Iorio（投资人） | 陈伟星 （投资人） | Jeremy Gardner（投资人） |
| David Lee（投资人） | 沈波（投资人） | 徐明星（投资人） |
| 李笑来（投资人） | Jehan Chu（投资人） | 孙铭 （律师） |

# 第二部分　量子链技术特征

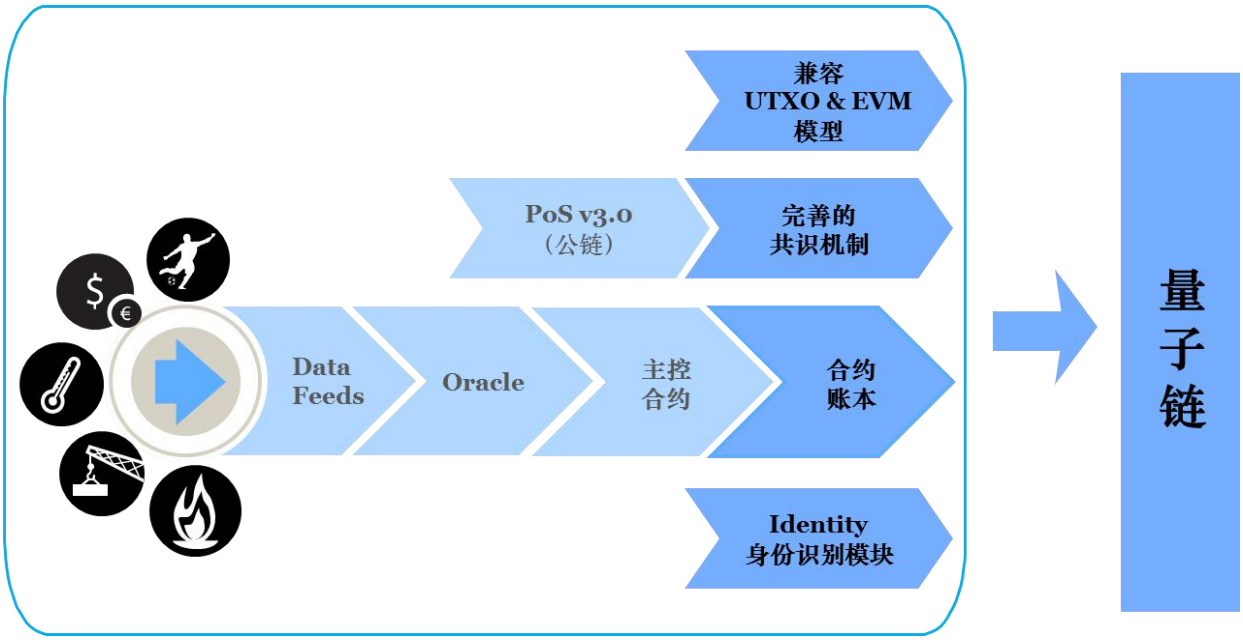
## 2.1 量子链概述

量子链致力于开发兼容比特币和以太坊的全新生态系统，并且以行业应用为导向，通过移动端 DApp 开发策略，把区块链的技术优势带给不同行业的应用者和普通互联网用户。

另外量子链更加注重智能合约的实际应用，将通过完善的 Oracle 和 Identity 模块的设计，并加入了数据馈送（DataFeeds）机制，使得传统互联网企业（金融、物联网等）应用区块链技术时满足相关合规性的要求。

除此之外，Qtum 还将重点开发去中心化应用，与第三方开发者一起，为普通用户提供移动端的去中心化应用，共同携手打造 Qtum 生态系统。

## 2.2 量子链模型




- **兼容 UTXO 和 EVM**

一方面，量子链采用了 UTXO 模型保证交易的连续性和可溯源性。另一方面，以太坊的智能合约均可在量子链上运行。因此，量子链完美的结合了比特币和以太坊的优点，并解决了两者的固有缺陷。

- **共识机制**

我们使用了 Proof of Stake 作为量子链的共识机制。在后续的开发过程中，我们计划在 POS 基础上添加激励措施和估计节点在线，并称之为激励权益证明共识机制（IPoS）。

- **合约账本**

在量子链中，合约账本存储了所有的量子链明文可读性强的合约内容，用户可以选择性地把自己感兴趣的合约代码和合约解释通过 P2P 的形式下载到自己的 Qtum 客户端。合约账本的构建，可以给 Qtum 系统中的合约带来更多的透明性、可读性以及可审计性。

首先，链下数据作为 data feeds 输入到量子链上，然后 Oracle 选择合适的数据触发智能合约。为了避免 The DAO 事件的再次发生，我们还在量子链中引入了监管者的角色。

✓ Data Feeds：
Data Feed 代表任何从链外取得的数据，比如汇率、GDP、某个城市的温度、比赛结果等。然后将数据输入到智能合约或者去中心化应用。

举个例子，当房间里的温度降到 10 摄氏度以下时，空调将自动转化为“制热”模式。这里，温度计上的读数就是链外数据。

✓ Oracle：
在 Qtum 系统中，Oracle 代表可信的特定的机构、实体、节点、公钥地址。 当有多个数据源时，Oracle 可以根据预先制定的规则选择合适的数据输入量子链。

✓ 主控合约：
在以太坊中，只有链上数据可以触发智能合约。在量子链中，我们引入了链下数据，与链上数据一起作为触发条件，完成合约的执行。这样的智能合约我们称之为主控合约。

- **Identity 身份识别模块**

正如我们所知，金融行业对数据的安全性和身份识别有更加严格的要求。我们在量子链上引入了第三方征信机构，通过 Identity 身份识别模块验证的客户，将获得更多的权限。

具体的技术特征和实现方式，请参考技术白皮书。

# 第三部分 量子链治理架构

## 3.1 量子链基金会的设立

量子链基金会（以下简称“基金会”）是 2016 年 11 月正式在新加坡成立的非营利性公司。量子链基金会致力于量子链的开发建设和治理透明度倡导及推进工作，促进开源生态社会的安全、和谐发展。

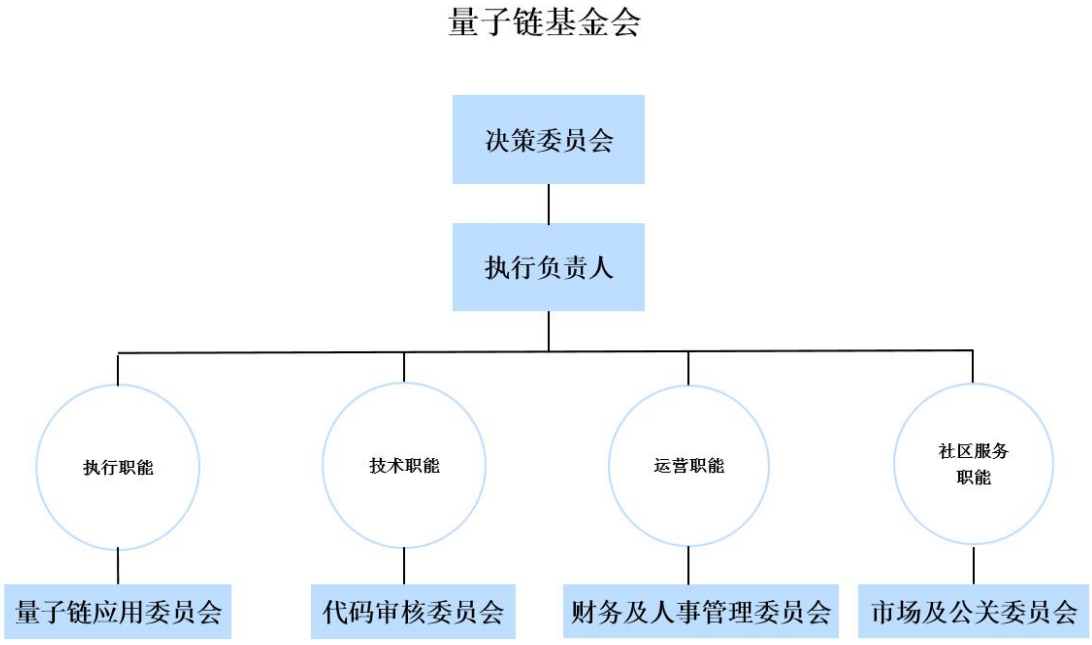
多次采取硬分叉的解决方式使得人们对以太坊、乃至区块链的去中心化理念产生质疑。为避免客户端出现交易不一致，或者其他有违区块链设计理念的事件再次出现，量子链基金会将通过制定良好的治理结构，帮助管理开源社区项目的一般轶事和特权事项。

量子链基金会治理结构的设计目标主要考虑开源社区项目的可持续性、管理有效性及募集资金的安全性。基金会由开发人员和职能委员会组成，组织架构主要由决策委员会、代码审核委员会、财务及人事管理委员会和市场及公共关系委员会组成。基金会成立初期，决策委员会由基金会主席帅初、量子链核心开发人员和私募成员组成，每期任期为二年。

## 3.2 量子链基金会治理架构

量子链基金会治理架构包含了针对日常工作和特殊情况的操作流程和规则。本节将详细介绍基金会各职能委员会的职责。

量子链基金会组织架构包括（如下图）：



- **决策委员会**

量子链基金会设立决策委员会，其职能包括聘任或解聘执行负责人以及各职能委员会负责人、制定重要决策、召开紧急会议等。决策委员会成员和基金会主席任期为两年，基金会主席不可连任。

首届量子链基金会决策委员会成员在区块链领域中具有丰富的行业经验，简要经历如下：

| 姓名 | 简要经历 |
|---|---|
| 帅初 | 量子链基金会主席，毕业于 Draper University（英雄学院）和中国科学院，之前就职于阿里巴巴，博士期间就致力于区块链技术的开发和研究，具备丰富的区块链行业的开发经验。 |
| Neil Mahi | Neil 拥有 ISCAE 的工商管理硕士，后来专攻计算机科学领域，拥有超过 20 年的软件开发经验和 4 年的区块链开发经验。此外，Neil 还曾是一名职业扑克玩家，精通四门语言。 |
| Jordan Earls | Jordan 十三岁开始编程，目前已经审核过超过 100 种数字货币的设计，并发现若干安全漏洞，是数字货币社区中值得信赖的知名成员。 |
| 沈波 | 沈波是分布式资本投资公司的创始人，专注于对区块链初创公司的投资。 |
| 孙铭 | 孙铭律师主要致力于并购、银行和信托、数字货币、区块链和分布式账本技术的法律咨询服务。 |
| David Lee | David 是硅谷 LeftCoast 的联合创始人之一，他主要从事分布式账本技术，大数据和机器学习等。 |
| 龚鸣 | 龚鸣撰写过大量的区块链相关的文章、资料。致力于推动区块链和分布式账本技术的发展。 |
| 方建凯 | 方建凯是分布式资本投资公司顾问，曾就职于万向区块链实验室，并担任市场及运营总监。 |
| 钱德君 | 钱德君是上海鼎利信息科技有限公司的联合创始人之一，主要致力于区块链技术落地应用的研究和开发。 |

决策委员会任期期满后由社区根据量子币币数和币龄计算权重进行投票选出 50 名社区代表，再进行投票选出 11 位决策委员会的核心人员，被选出的核心人员将代表量子链基金会做重要和紧急决策，并需在任职期间接受授信调查，并公开薪酬情况。

凡下列事项，需经过决策委员会以记名的投票方式进行表决，每名决策委员会成员有一票投票权，基金会主席有两票投票权。决策委员会做出决议，必须获得全体在任委员会成员的过半数通过：

- ✓ 修改基金会治理架构；
- ✓ 任免执行负责人及各职能委员会负责人；
- ✓ 制定重要决策；
- ✓ 决策委员会成员在任期内的任免，如成员违反职能范围、法律、行政法规、主动辞职等
- ✓ 紧急事件，如影响整个社区的事件、软件安全、量子链系统升级等

此外，当有下列情况之一时，执行负责人应在 5 个工作日之内召集决策委员会举行临时会议：

- ✓ 基金会主席认为必要时；
- ✓ 三分之一以上决策委员会成员联合提议时；
- ✓ 执行负责人提议时

决策委员会会议应由委员会成员本人出席。因故不能出席的，可以书面委托委员会其他委员代表出席。未委托代表的，视为放弃在该次会议上的投票权。

**• 执行负责人**

执行负责人由决策委员会选举产生，负责基金会的日常运营管理、各下属委员会的工作协调、主持决策委员会会议等。执行负责人定期向决策委员会汇报工作情况。

**• 量子链应用委员会**

量子链应用委员会负责筛选适合的行业，将量子链技术应用到行业中，从而实现商业落地。

**• 代码审核委员会**

代码审核委员会由量子链开发团队中的核心开发人员组成，负责底层技术开发、开放端口开发和审核、各产品开发和审核等。此外，各产品的开发人员每周召开项目追踪会议，沟通项目进展及需求。代码委员会成员每日了解社区动态和热点，在社区中与 Token 持有者进行沟通交流，并且不定期举办技术交流会。

**• 财务及人事管理委员会**

财务及人事管理委员会负责项目募集资金的运用和审核、开发人员薪酬管理、日常运营费用审核等；目前日常的账务处理暂时外包给第三方。

- **市场及公共关系委员会**

市场及公共关系委员会的目标是为社区服务，负责量子链技术推广、量子链产品推广、开源项目的推广和宣传等。此外，委员会还负责对外公告管理。若发生影响基金会声誉的事件，经内部审核评估后，统一由委员会进行公关回应。

## 3.3 量子链团队

量子链拥有一个非常有经验国际化团队，团队成员具有多年的区块链行业、密码学和虚拟货币社区的经验。量子链项目开发团队共有 17 位核心开发者，由帅初带领。至今已完成 Qtum 原型的开发。量子链主要团队成员及经历如下：

| 姓名 | 简要经历 |
|---|---|
| **帅初** | 帅初毕业于英雄学院，拥有中国科学院计算机科学博士学位，曾就职于阿里巴巴集团，目前致力于区块链技术的开发和研究，拥有丰富的区块链行业开发经验。 |
| **Neil Mahi** | Neil 拥有 ISCAE 的工商管理硕士，后来专攻计算机科学领域，拥有超过 20 年的软件开发经验和 4 年的区块链开发经验。此外，Neil 还曾是一名职业扑克玩家，精通四门语言。 |
| **Jordan Earls** | Jordan 十三岁开始编程，目前已经审核过超过 100 种数字货币的设计，并发现若干安全漏洞，是数字货币社区中值得信赖的知名成员。 |
| **Caspal OuYang** | Caspal 是一名经验丰富的 web 开发者，曾就职于百度。Caspal 拥有超过 21 枚亚洲魔方比赛金牌和 29 项国内魔方记录保持者。曾是魔方 4*4、5*5 盲拧和 3*3 足拧的中国区冠军。 |
| **Baiqiang Dong** | Baiqiang 曾就读于北京大学物理专业，之前供职于金山软件和猎豹移动。 |
| **Mike Palencia** | Mike 是区块链开发者、爱好者，2013 年投身于区块链行业，并参与多个加密货币项目的开发工作。Mike 参与开发了 Proof-of-concept 平台、区块探索者、线上钱包和最大的代币挖矿池之一。 |
| **徐小龙** | 徐小龙毕业于中国科学院，曾就职于微软和腾讯，拥有丰富的软件开发经验，热衷于区块链技术和开发。 |
| **Time Markov** | Time 拥有 C、C++、Qt、QML 开发领域超过 9 年的经验，致力于跨平台应用的开发。在区块链开发超过一年的经验。 |
| **Alexei Dulub** | Alex 是大数据、区块链技术和系统安全的全栈开发人员。Alex 曾参与了 blockverify.io 和 OmniBazaar 等项目。 |
| **Brett Fincaryk** | Brett 曾在 1999 年至 2004 年担任 Linux 系统管理员工作，2005-2014 年就职于一间 Linux 桌面支持公司。2013 年年中，开始进入区块链行业，2014 年加入了 Qtum 大家庭。 |
| **Roman Asadchiy** | Roman 是一名高级全栈开发人员，在构建分布式区块链解决方案方面拥有超过 3 年的经验。 此外，他还是比特币、以太坊和智能合约方面的专家。 |
| **John Scianna** | John 从 2012 年开始关注比特币，并于 2013 年加入了比特币社区。John 曾是一名记者、比特币矿工，并在多家比特币初创公司，包括 BoinPip、DC-based 区块链倡导组织和数字商务部。 |

## 3.4 量子链基金会人力资源管理

量子链致力于打造全球最具影响力的开源社区生态，为确保技术层面的开发顺利和基金会运营持续有效，有别于传统企业和其他非盈利组织的人员招聘过程，基金会将招聘最顶尖的开发人员和管理人才。

**人员招聘**

招聘人员按照“竞争、择优、经验”的原则，进行两人以上的面试、背景调查（如工作履历、商业利益等）、录用审批、试用期制度等。

基金会部分管理职能如财务、法务、税务等将采用外包形式，需经过基金会财务及人事管理委员会和基金会主席同意，签订人力资源外包服务协议。

量子链作为开源社区，不仅招聘专职开发人员，还会聘请业界知名的技术顾问，相关的聘请和薪酬支付均需要经过决策委员会、基金会代码管理委员会和财务及人事管理委员会审批，并签订合作条款。

**绩效考核**

决策委员会人员每年进行绩效考核，主要内容包括基金会资金运营、基金会管理情况和社区协调工作等，每年进行尽职调查并采取轮岗制，由社区投票结果选取下一届决策委员会成员，连任不得超过 3 届。

由于基金会开发人员来自不同国家，开发人员分为全职和兼职，因此基金会制定了薪酬管理和绩效考核制度的政策。开发人员需定期报告自己的工作进度及交流开发进程，由代码管理委员会对其进行绩效考核。此外，每年将持续进行尽职调查。

## 3.5 量子链基金会的风险评估及决策机制

量子链基金会为制定和完善风险管理体系和制度，要求每年就量子链可持续性进行安全评估，评估内容包括项目质量、项目进度、项目应用，例如智能合约和简单合约应用、威胁识别分析，管控措施评估分析，风险界定、处置等阶段。

基金会将根据事件特性，例如事件影响程度、影响范围、影响代币量和发生的概率进行分级，按照优先级进行决策，对于优先级高的事件，尽快组织基金会相关委员会进行决策。事件类型主要分为管理类事务和代码类事务：

对于基金会普通管理类事务，由基金会成员进行会议商讨，最终由 财务及人事管理委员会和基金会主席共同决定。

对于开源社区的代码问题和筹集资金的使用问题，决策通常采取成员投票机制。社区中每个成员根据所持量子币的数量和币龄绝对投票权重，通过基金会投票系统进行投票，投票结果将有导向性作用。决策委员会具有决定权，而社区投票结果将作为参考。

对于紧急事件（例如影响整个社区的事件、软件安全，系统升级等）的决策，由代码审核委员会审核后提交至决策委员会，决策委员会通过投票表决，采取特权机制落实到社区中。基金会将通过投票机制避免分歧的产生，若产生分歧，由决策层人员的量子币数量和币龄决定投票权重。

## 3.6 量子链基金会日常运营机制

量子链基金会日常运营主要分为代码管理、财务管理、人力资源、市场推广及法务事项。基金会将通过以下各项控制活动对日常运营进行管理，但各项控制活动不仅限于此：

| 控制目标 | 控制活动 | 控制所有人 |
|---|---|---|
| **代码管理** | | |
| 开源代码管理 | 底层架构代码为开源代码，存放在Github，由核心开发小组成员拥有修改审批权限。 | 代码审核委员会 |
| 源代码修改 | 提交人修改源代码，由核心开发小组审批后完成修改。 | 代码审核委员会 |
| 代码开发及修改 | 代码开发及修改人员需经过核心开发小组审批，授予权限后进行开发及修改。 | 代码审核委员会 |
| 代码测试 | 代码编写或修改后需要经过测试并汇总测试结果，确保测试结果无异常。 | 代码审核委员会 |
| 代码审核 | 代码由专人审核，通过自动或者人工方式审核代码，验证无误后在社区发布公告。 | 代码审核委员会 |
| 代码上线 | 代码上线之前由代码核心开发人员审核。 | 代码审核委员会 |
| 漏洞修复 | 当代码出现漏洞时，由开发人员进行修复和测试，经过代码审核委员会审批后上线。 | 代码审核委员会 |
| 应急演练 | 定期和不定期对代码的开发环境和测试环境进行应急演练，由代码审核委员会负责计划和实施。 | 代码审核委员会 |
| 代码修改权限 | 对于非公开的产品代码，由代码审核委员会授予修改代码的权限，申请审批后方可操作。 | 代码审核委员会 |

| 控制目标 | 控制活动 | 控制所有人 |
| --- | --- | --- |
| **人力资源** | | |
| 招聘 | 招聘人员需经过两人或以上人员面试，经过独立评价后形成招聘记录。最终由相关委员会进行审批。 | 财务及人事管理委员会 |
| 背景调查（尽职调查） | 对关键开发人员和关键岗位的招聘，需要经过尽职调查后方可录用，并留存调查文档。 | 决策委员会 |
| 专业服务外包 | 专业服务（财务、法务、税务等）外包经过财务及人事管理委员会评估审核后选定服务方，并签订外包协议。 | 财务及人事管理委员会 |
| 工资薪酬 | 决策委员会人员的工资薪酬应当披露；核心开发人员和管理人员的工资薪酬应当由决策委员会成员审核；其他人员工资薪酬应经过各委员会审核。 | 决策委员会 |
| **市场推广** | | |
| 推广渠道的新增 | 由PR委员会对新增推广渠道进行调研，包括渠道的方向、可延伸性和推广力度。经过调研后审批确定新增的推广渠道。 | 市场及公共关系委员会 |
| 推广服务合同签订 | 新增推广服务或者渠道，需要经过 PR 委员会审批后签订合作协议。 | 市场及公共关系委员会 |
| 推广文案的编写及审核 | 推广文案需要经过独立人员审核后方可发布。 | 市场及公共关系委员会 |
| 危机公关处理 | 当出现紧急事件，需要有 PR 委员会商讨公关处理，由决策委员会同意后方可对外披露。 | 市场及公共关系委员会 |
| **财务管理** | | |
| 预算审核 | 每年制定基金会运营预算，由财务负责人审核。 | 财务及人事管理委员会 |
| 合同的拟定与审核 | 由独立法务人员对合同条款进行审核。 | 财务及人事管理委员会 |
| 合同的签订 | 合同条款经过审核后，由决策委员会审核，审核后方可签订合同。 | 决策委员会 |
| 收入审核 | 基金会的收入来源主要是私募和量子币公开售卖，由财务人员进行核准并记录，由独立人员进行对账。 | 财务及人事管理委员会 |
| 支出审核 | 基金会所有支出需经过财务及人事管理委员会审核，并做好相关账务处理。 | 财务及人事管理委员会 |
| 账务处理 | 账务处理应由财务及人事管理委员会负责人审核，并且每月形成财务报告。 | 财务及人事管理委员会 |
| 资金对账 | 实物资金与资金账每月应当进行对账，由基金会财务及人事管理委员会授权人 | 财务及人事管理委员会 |

| 控制目标 | 控制活动 | 控制所有人 |
| --- | --- | --- |
| | 员审核。 | |
| 披露事项 | 定期披露基金会募集的资金如何使用，基金会的发展情况应定期向社区汇报。披露事项需经过决策委员会审批。 | 决策委员会 |
| 合作外包条款的签订 | 基金会部分职能外包，由财务及人事管理委员会的审批后签订外包协议。 | 财务及人事管理委员会 |

量子链基金会每年会接受外部机构对基金会募集资金的使用情况、利润、成本和潜在债务等进行评估和审计。

## 3.7 量子链基金会的经济

量子链基金会的财务管理团队分为日常财务管理和数字货币的管理。日常财务管理将外包，包括开发人员的差旅费、人员工资、房屋租赁、日常费用等；数字资产的管理由决策委员会授权人员负责，包括钱包管理、数字资产的到账、与其他数字货币的兑换、数字货币的兑现等。

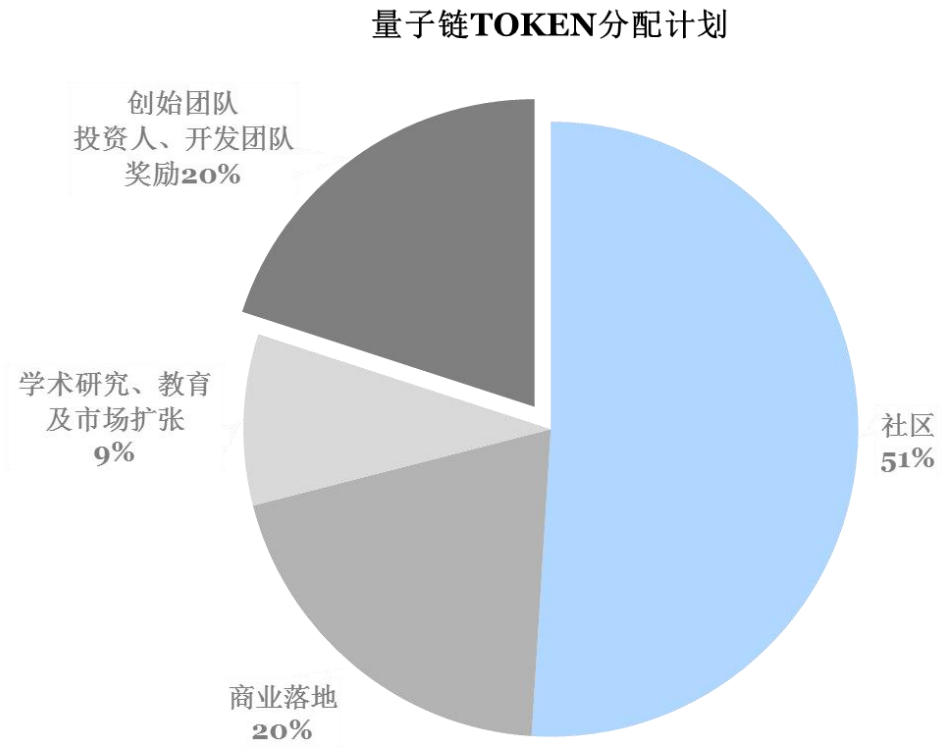
- **资金来源**

量子链基金会在开发初期不会产生大量收人， 主要收入来自于私募和量子币公开售卖，参与者需要使用量子币获取量子链和 DApp 的使用权。

- **量子币分配计划**

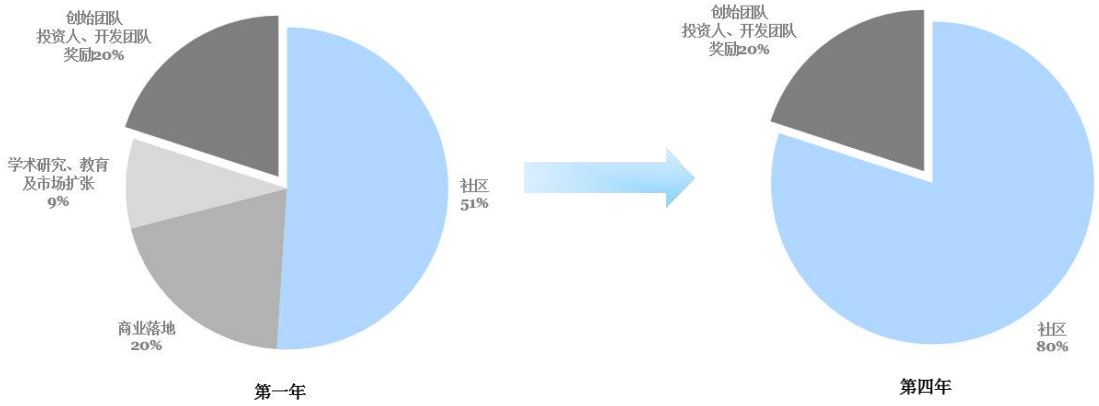
量子币的分配计划如下：最终 80%的量子币将分发给社区，20%分配给创始团队、私募投资者和开发团队（详见图一）。

| 比例 | 分配方案 | 明细 |
| --- | --- | --- |
| **51%** | 量子币公开售卖 | 量子币公开售卖获得的收入将会用于量子链基金会的运营，包括开发、市场、财务和法律咨询等。 |
| **20%** | 创始团队、私募投资人和开发团队 | 创始团队、私募投资人以及开发团队在量子链的发展过程中做出了人力、资源、物力以及技术的贡献，因此以发放量子币作为回报。 |
| **20%** | 商业落地部署 | 筛选合适的行业，进行行业中的战略部署、项目扶持和代币置换，用于量子链技术的行业应用，真正实现商业落地。 |
| **9%** | 学术研究、教育及市场扩张 | 用于支持量子链相关的学术研究、开发人员的教育材料、提高对量子链技术的意识以及向其他开源社区进行贡献。 |




图一

基金会计划将 29%（商业落地 20%；学术研究、教育及市场扩张 9%）分阶段逐步分配给社区，在三到四年后最终全部量子币投放于社区（详见图二），使量子链真正实现开源的社区生态。这部分量子币的运用将每年向社区公布并提供财务报告。




图二

| 比例 | 用途 | 钱包地址 |
| --- | --- | --- |
| **10%** | 商业应用 | 待公布 |
| **10%** | 代币兑换 | 待公布 |
| **9%** | 学术研究、教育及市场扩张 | 待公布 |

- **资金使用的限制条款**

量子币的使用本着公开透明的原则，根据上述分配原则和钱包地址进行使用，由托管机构监督数字资产的流向并定期分享给社区。

公开售卖收入的使用原则：

- ✓ 超过 50 个 BTC，需要经过财务及人事管理委员会审批；
- ✓ 超过 100 个 BTC，需要经过决策委员会审批。

- **财务规划和执行的报告**

每季度由财务及人事管理委员会制定财务规划并对上一季度的财务执行情况进行总结，形成财务报告提交至决策委员会审核。

- **数字资产管理**

属于量子链基金会的数字资产由财务及人事管理委员会授权人员负责，每天做交易记录，采取多重签名确保资产的安全性和准确性。所有收取的法币，及时转为数字货币，并存入数字钱包。基金会资产不得存于个人账户。

- **数字钱包管理**

基于独立性原则，量子链基金会的钱包采取 3/4 多重签名。若增加签名，须经过财务及人事管理委员会。大额的代币进行冷存储；小额的代币使用多重签名的方式。

- **量子币的发行及管理**

量子链对应的量子币是量子链和 DApp 的使用权。初次发行总量的 51%，总量固定。

- **披露事项**

每年基金会将向社区披露量子链的开发情况、公链的运营情况、量子币的使用情况以及基金会的运作是否符合治理章程。

## 3.8 其他事项及法律事务

- **法律事务**

  量子链基金会在新加坡成立，若出现需要寻求法律意见的事项，需要通过当地律师予以确认。

- **免责条款**

  量子链基金会目标转变为非营利组织，链上用户获取的是量子链的使用权。购买者应明白在法律范围内，量子币不做任何明示或暗示的保证，并且量子币是“按现状”购买的。此外，购买者应明白量子币不会在任何情况下提供退款。

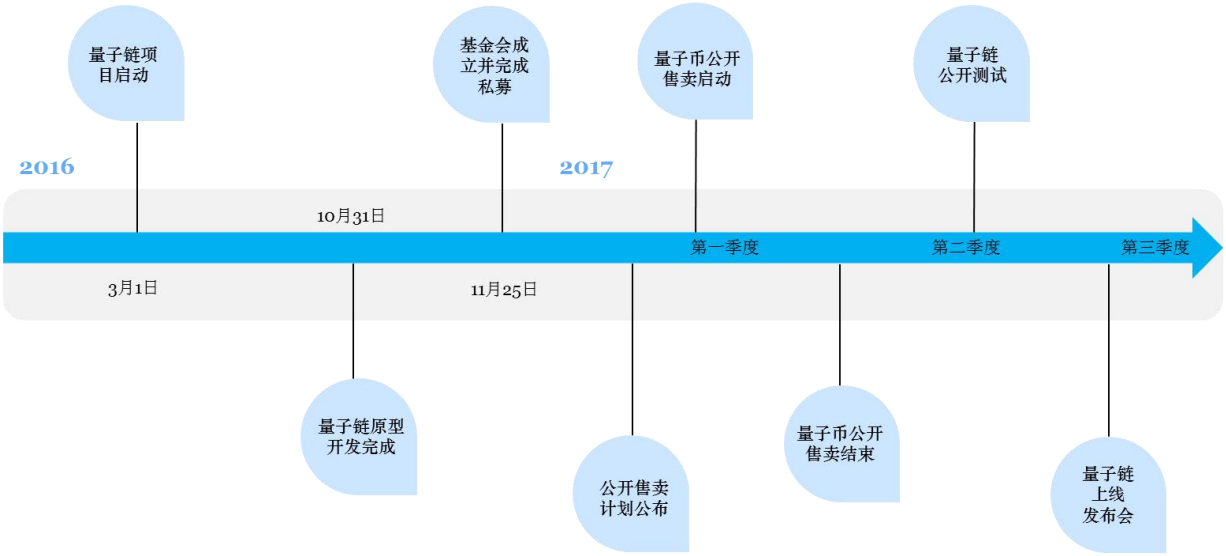
- **争议解决条款**

  当出现争议时，有关方面应依据协议通过协商解决。如协商解决无法解决，可通过法律解决。

# 第四部分 量子链实施及迭代

## 4.1 量子链上线的时间规划

*量子链项目时间表*




量子链项目的主要时间节点包括:

- 量子链项目启动：2016 年 3 月帅初、Neil 和 Jordan 作为联合创始人正式启动量子链项目；
- 量子链原型开发完成：2016 年 10 月，开发团队完成了量子链原型的开发；
- 基金会成立并完成私募：量子链基金会于 2016 年 11 月在新加坡成立了非营利性公司，并得到了超过一百万美金的种子轮投资，部分投资人包括快的打车创始人陈伟星、以太坊早期参与者 Anthony Di Iorio、OKCoin CEO 徐明星、BitFund 创始人李笑来和分布式基金合伙人沈波；
- 公开售卖计划公布：公布公开售卖计划，包括售卖目标、售卖期间、售卖方式和奖励等；
- 量子币公开售卖：根据公布的公开售卖计划，通过合作渠道进行公开售卖；
- 治理章程完成：在 2017 年第二季度发布正式治理章程发布；
- 量子链公开测试：在 2017 年第二季度发布公开测试网络；
- 量子链正式上线：量子链平台将于 2017 年第二季度到三季度正式上线。

## 4.2 量子链项目公开售卖计划

量子链的用户需通过消耗持有的量子币来获取量子链的功能，尤其在量子链上运行分布式应用需要支付和消耗一定量的量子币。

量子币将会在量子链正式发布时全部产生，由量子链基金会持有。

量子币公开售卖的具体规则和信息将会通过 Qtum 官网网站进行公布。

参与量子链售卖不是零风险的。详细内容，请参阅 PROSPECTUS 第五章“风险因素”。

募集对象的具体权利义务请参见 PROSPECTUS：Chapter III& Chapter IV。

## 4.3 量子链的未来迭代规划

作为区块链技术，会面临各种挑战和机遇，量子链的未来迭代包括两部分，一是代码本身的迭代；二是商业应用上的迭代。

- **量子链底层架构的迭代**

当量子链代码本身出现漏洞，通常采取系统升级。出现漏洞需要经过代码委员会进行分析、测试和审核，提交至决策委员会报备。当出现以下重大漏洞（不限于）采取系统升级：

- ✓ 影响用户资金
- ✓ 重大安全问题
- ✓ 影响系统安全

当出现较小的漏洞时，直接由代码委员会进行补丁。

- **商业应用上的迭代**

量子链将会是完全开源的项目，量子链系统希望通过技术上的创新、理念上的创新将区块链与现实链接起来。因此在商业应用的时候，量子链基金会会选择合适的第三方合作，进行行业和应用的迭代。由第三方供应商主导，量子链提供相应技术支持。

# 第五部分 量子链应用

## 5.1 去中心化应用

区块链技术的一大特点就是去中心化，而量子链系统致力从技术层面全面支持去中心化应用，量子链开发不同模块，提供适用于不同系统和不同用户的开发平台，简化开发者的准备工作，从而实现快速开发。另外通过移动端策略的引入，将不同的 DApp 想法产品化，使普通互联网用户可以真正分享到区块链技术带来的价值。

面向不同行业的 DApp 应用，可以把区块链技术带给更多的用户和行业。例如去中心化的社交、去中心化的存储和去中心化的域名服务、去中心化的计算服务等，通过激励机制的引入，将更深层次利用共享经济的理念，改变现有的 APP 市场和商业模式。

## 5.2 多个行业的支持

在量子链系统中，通过引入支持行业共识机制和监管的需求，可以为行业发展需求也提供支持。

例如，Qtum 系统可以满足可信网络中，对区块链速度和容量的要求，通过基于区块链技术的主控合约和 Oracle 和 Data Feeds 的引入，也可以引入更多线下的因素。通过 Identity 和 Privacy 的设计，可以符合金融行业的监管需求。

在 Qtum 系统中，可以支持多个行业的应用需求：例如 金融业、物联网、供应链、社交和游戏、慈善、数字资产和股权等。另外基于 Qtum 的智能合约和主控合约，通过图灵完备的编程语言，可以实现更复杂商业逻辑的支持，并将支持更多的行业。

关于 Qtum 的应用和行业支持，可以参考第六部分应用场景。

## 5.3 移动端策略

目前区块链技术开发更多停留在 PC 用户端，只有真正实现区块链移动端服务，才能使普通互联网用户也加入到社区中，从而推动区块链技术在中国的落地。

在量子链的生态系统中，我们不仅全面支持并推动移动应用战略，而且我们将会与第三方开发者，一起为用户提供移动端的服务，包括：移动端钱包、移动端 DApp 应用、移动端智能合约应用等服务。

量子链开发团队计划建立 DApp Store，将区块链技术与现有的互联网产品和数字货币进行融合，例如微信、云计算等。Qtum 已经发布的社区项目包括“春邮”和 BiSMTP 协议，宗旨是让每个 email 成为虚拟货币钱包。

# 第六部分 应用场景

**场景一: 区块链技术应用于智能合约**

Augur 是一个开源的、去中心化的预测市场平台，于 2015 年在以太坊上发布。Augur 使用了区块链技术执行智能合约。

在 Augur 平台上，任何一个人可以在任何地方都可以为自己感兴趣的主题（比如，2016 年美国大选谁会获胜）创建一个预测市场，不需要任何中心化的批准。作为回报，该市场的创建者将从市场中获得一般的交易费用。Augur 平台的另一个重要特性是可以减少诈骗和对手方风险：平台上的货币交易通过智能合约进行严格的监管，分布式 Oracle 系统可以确保没有人能对事件提出不真实的结果。

Augur 系统内部使用一种名为信誉（“REP”）的代币。当事件发生后，众多 REP 持有者对事件结果进行报告。而比特币和以太币用于市场的投资。

因此，Augur 使用分布式 Oracle 技术，允许智能合约在其上运行，建立了一个无需信任任何个人和组织的、高度自治可信的平台。

**场景二: 区块链技术应用于产品管理**

在区块链上使用唯一的 ID，并将此 ID 与商品结合，通过跟踪商品，供应链中各方之间的沟通和合作以及政府机构的监督来创建一个透明的供应链，以解决与假冒产品有关的问题。

2016 年 11 月，一个基于区块链的产品管理平台 Vechain（“唯链”）发布。唯链可以为用户提供商品资产管理、追踪溯源、防伪校验和增强消费体验。通过在区块链上放置唯一 ID 并使用近场通信（“NFC”）芯片，射频识别（“RFID”）标签或快速响应（“QR”）代码嵌入每个产品，方便验证这些商品的真伪。 VeChain 为不同企业提供了一个轻松创建、管理、维护和更新共享数据的机会。

VeChain 还为在供应链上运行的各方的不同 IT 系统之间建立了连接。通过唯链的 APP，消费者可以直接查看所购商品在上游每个节点的信息，并能写入自己的数据。此外，唯链还能用于商品资产管理和用户体验等应用场景。

**场景三: 区块链技术应用于物业估值**

区块链技术透过分布式分类账技术，建立及传送完整、加密的资料，有助提升资料的可追踪性，确保资料准确无误。

中国银行（香港）（“中银香港”）是香港主要上市商业银行集团之一，在 2016 年 11 月 28 日宣布正式推出物业估值区块链技术，并成功透过该技术与物业估价公司完成首宗物业估值。

区块链技术帮助银行精简验证估值报告流程，节省成本；物业估价公司也无需再提供纸质本的物业估值报告，有助推动无纸化绿色金融。

目前，中银香港与两家物业估值公司合作。为扩大区块链的应用，中银香港将邀请其他估值公司及银行同业参加，以丰富区块链内的物业估值资料。同时，香港金融管理局大力支持了此次物业估值区块链服务的推出。中银香港希望为金融科技在金融业应用带来更多创新概念和应用案例，令金融机构及消费者同时得益，促进银行界金融科技的发展。

除了物业估值按揭流程外，中银香港将继续积极探讨及研究，把区块链技术应用于其他领域，包括贸易融资、电子证件管理以及跨境支付等。

**场景四: 区块链技术应用于移动数字汇票平台**

区块链技术的安全性、透明性、无法篡改和不可抵赖性等特性，可以用于解决移动数字汇票真实性和信息不透明等问题。

2016 年 11 月 11 日，中国浙商银行在旗下微信公众号发文称明年一月将推出基于区块链技术的移动数字汇票平台。通过移动数字汇票平台，企业与个人客户可以在移动端签发、签收、转让、买卖、兑付移动数字汇票。

一旦落地，浙商银行推出的移动数字汇票平台将成为国内首个采用区块链技术实现核心银行业务的实际应用，提高客户资金管理效率并降低使用成本。

**场景五: 区块链技术应用于证券交易**

2016 年 11 月 29 日，德国央行 Deutsche Bundesbank 无论从实力还是规模上都是欧洲央行体系（“ESCB”）最有影响力的成员，公开了区块链证券结算原型。

德国央行与德国证券交易所（“Deutsche Borse”）共同发起证券和股票交易市场原型，这是两家机构首个合作成果，只是改变原型，还不能实际推广。该产品为中央机构发行的数字货币和数字证

券交易和转移提供结算技术支持，兼顾交易和支付流程；计划是两个月之后进一步开发原型，分析这种区块链应用的技术性能和可扩展性。

**场景六: 区块链技术应用于物流管理**

2016 年 11 月初，欧洲最大港口鹿特丹港、荷兰银行、代尔夫特理工大学和荷兰国家应用科学研究院等组成区块链物流研究联盟，宣布共同探索区块链在物流领域的作用。

未来两年，联盟成员会联合测试物流和共同信息共享应用。代尔夫特理工大学指出，该项目会联合荷兰经济事务部的独立区块链项目，可以为联盟的测试项目提供开元基础设施。联盟成员不会单独探索区块链技术在物流行业的作用，项目核心是探索实际应用。

# 附件 1 专业术语

1. 比特币：比特币是一种加密数字货币，在 2009 年由化名的开发者中本聪（Satoshi Nakamoto）以开源软件形式推出。
2. 以太坊：以太坊是一个有智能合约功能的公共区块链平台。
3. 价值传输协议: 用于基于互联网的价值传输。
4. Internet of Things: 物联网。物联网是互联网、传统电信网等信息载体，让所有能行使独立功能的普通物体，如物理设备、汽车、建筑等实现互联互通的网络。
5. Oracle: 根据预先设定的判断条件，对输入数据进行筛选，选择最适合的数据作为数据输入。
6. Data feeds: 数据馈送，为区块链提供数据链下数据来源。
7. PoS: 权益证明共识机制。根据每个节点所占代币的比例和时间，等比例的降低挖矿难度，从而加快找随机数的速度。
8. UTXO: 未花费交易输出。比特币网络中使用的交易模型。
9. 智能合约：智能合约是由时间驱动的、具有状态的、运行在一个复制的、分享的张本质上的、且能够保管账本上资产的程序。
10. 代币：除了比特币以外的数字货币。
11. PoW：工作量证明共识机制。一方（通常称为证明人）提交已知难以计算但易于验证的计算结果，而其他任何人都能够通过验证这个答案就确信证明者为了求得结果已经完成了大量的计算工作。
12. 公有链：公有链是任何人在任何地方都能发送交易且交易能获得有效确认的、任何人都能参与其中共识过程的区块链。
13. 以太坊虚拟机: 以太坊虚拟机设计运行在点对点网络中所有参与者节点上的一个虚拟机，它可以读写一个区块链中可执行的代码和数据，校验数据签名，并且能够以半图灵完备的方式来运行代码。它仅在接收到经数据签名校验的消息时才执行代码，并且区块链上存储的信息会区分所做的适当行为。
14. 激励权益证明共识: 在权益证明共识中加入了激励措施，和估计节点在线。
15. 硬分叉: 区块链发生永久性分歧，在新公式规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会产生。
16. DAO：分布式自治组织。通过一系列公正公开的规则，可以在无人干预的和管理的情况下自主运行的组织结构。
17. 图灵完备语言：一个能计算出每个图灵可计算函数（Turing-computable function）的计算系统被称为图灵完备的。一个语言是图灵完备的，意味着该语言的计算能力与一个通用图灵机（Universal Turing Machine）相当，这也是现代计算机语言所能拥有的最高能力。

# 参考文献

[1] https://en.bitcoin.it/wiki/Category:History
[2] https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle.pdf
[3] https://github.com/bitcoinbook/bitcoinbook
[4] https://github.com/ethereum/wiki/wiki/White-Paper
[5] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, https://www.bitcoin.org/bitcoin.pdf
[6] 《区块链社会 解码区块链全球应用与投资案例》 龚鸣 2016
[7] David Johnston et al., The General Theory of Decentralized Applications, Dapps, 2015, https://github.com/DavidJohnstonCEO/DecentralizedApplications
[8] Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, http://ethereum.org/ethereum.html
[9] Paul Sztorc, Peer-to-Peer Oracle System and Prediction Marketplace, 2015, http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf
[10] PriceFeed Smart Contract, 2016, http://feed.ether.camp/
[11] Nxt, 2013, http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt
[12] http://chainb.com/?P=Cont&id=2863
[13] http://chainb.com/?P=Cont&id=2856
[14] http://www.bochk.com/dam/bochk/desktop/top/aboutus/pressrelease2/2016/20161128_01_Press_Release_SC.pdf
[15] http://tech.sina.com.cn/i/2016-08-09/doc-ifxutfpf1573966.shtml

# 版本变更记录

| 版本 | 日期 | 作者 | 更改内容 |
| --- | --- | --- | --- |
| 1.0 | 2017 年 2 月 9 日 | 量子链基金会 | 首次发布 |
| | | | |
| | | | |