

# ARC白皮书

(V1.3)



综合应用区块链，  
构建现实世界与区块链完美结合的商业生态链  
引领人类全面进入可信赖的数字化生活

ARC，开创应用价值的新纪元

2018.01.02

# 目 录

第一部分 开篇——价值应用概念.....	1
1.1 互联网技术革新必然趋势：价值应用.....	1
1.2 区块链技术发展趋势：应用领域急速扩张 .....	2
1.3 技术准备已经完成，开创价值应用时代 .....	4
第二部分 征程——价值应用的实现.....	5
2.1 总体描述.....	5
2.2 价值应用的硬件.....	5
2.2.1 什么是 MOP .....	5
2.2.2 MOP 区块.....	6
2.2.3 超高频射频芯片介绍.....	7
2.2.4 国际 MOP 芯片的优劣分析.....	8
2.2.5 价值应用 MOP 芯片的总体设计方案.....	9
2.3 价值应用的软件.....	12
2.3.1 艾瑞币（Agilereservecoin）的诠释.....	12
2.3.2 艾瑞币链（Agilereservecoinchain）的总体架构 .....	13
艾瑞币链底层.....	14
艾瑞币链核心层.....	14
艾瑞币链中间层.....	14
艾瑞币链应用层.....	14
2.3.3 艾瑞币链协议与 Agilereservecoincoin .....	15
艾瑞币链详细架构.....	15
艾瑞币母链.....	16
艾瑞币子链.....	18
区块结构.....	18

共识机制.....	19
字节费分配.....	21
Agilereservecoincoin.....	22
Agilereservecoincoin 的主要功能.....	23
2.3.5 艾瑞币链生态系统.....	25
技术环节.....	25
平台环节.....	26
应用环节.....	26
app 环节.....	26
系统的主要特征.....	26
系统的主要优点.....	27
多用户共识安全机制.....	27
2.4 应用场景：艾瑞币链项目在综合应用行业的系统解决方案 .....	28
2.4.1 传统综合应用制造困境解析.....	28
2.4.2 综合应用行业智能制造解决方案.....	29
2.4.3 综合应用行业智慧应用平台解决方案 .....	31
2.4.4 综合应用行业智慧 app 解决方案.....	32
第三部分 未来——价值应用改变世界.....	34
3.1 艾瑞币链项目阶段性规划.....	34
3.2 艾瑞币链项目的投资价值.....	36
第四部分 项目基金会.....	38
第五部分 团队简介.....	40
5.1 发起人.....	40
5.2 高级顾问.....	40
5.3 首席专家.....	40
5.4 团队成员.....	41
5.5 天使投资人.....	43
5.6 顾问团队.....	44
第六部分 参考文献.....	46
附录 A 文档修订记录.....	48

# 第一部分 开篇——价值应用概念

## 1.1 互联网技术革新必然趋势：价值应用

我们所处的时代，是新技术引领社会变革的时代。在信息互联网时代，人们的协作和交流突破了时间和空间的限制，世界成为一个整体互动平台。

近几年，互联网发展进入“互联网+”的新业态，这一阶段是知识社会创新2.0推动下的“互联网+各个传统行业”的经济社会发展新形态，为各行各业的改革、创新、发展提供了广阔的网络平台。

当前，信息化时代进入空前的重要发展阶段，互联网能够实现“物物相连”，这一阶段被称为继计算机、互联网之后世界信息产业发展的第三次浪潮：物联网时代。应用技术包含两层含义：其一，应用的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；其二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。

然而，从互联网，到“互联网+”，再到应用，所有阶段都未能解决信息传播的局域化问题（中心化）。在当前中心化构架下的应用很难完成真正意义的自主协作和有效交易，因为这种协作和交易的相关方往往是属于不同的利益主体，具有复杂和难以确定的信任关系。因此，目前的应用设备的协作和交易只能够在同一信任域下进行；即，协作和交易的设备必须由同一个应用运营服务商提供或者进行授权验证，这大大降低了应用应用的真正商业价值。

在这种情形下，我们提出“价值应用”，重点将区块链技术引入应用，解决应用发展过程中所面临的中心化问题。区块链是一种去中心化的交易记录存储技术，它基于密码学原理，凭借分布式点对点网络，实现有序交易记录的永久性存储，不可删除和篡改，公开并且可溯源，因此它被公认为迎接上述挑战的不二选择。在区块链的生态，人们不需要事先建立信任，便可以安全的

进行交易，因为每一笔交易都记录在区块链的“公共帐本”上，有据可查，它能完美解决互联网虚拟世界的信任和权益问题。价值应用的必然趋势如图 1.1 所示。

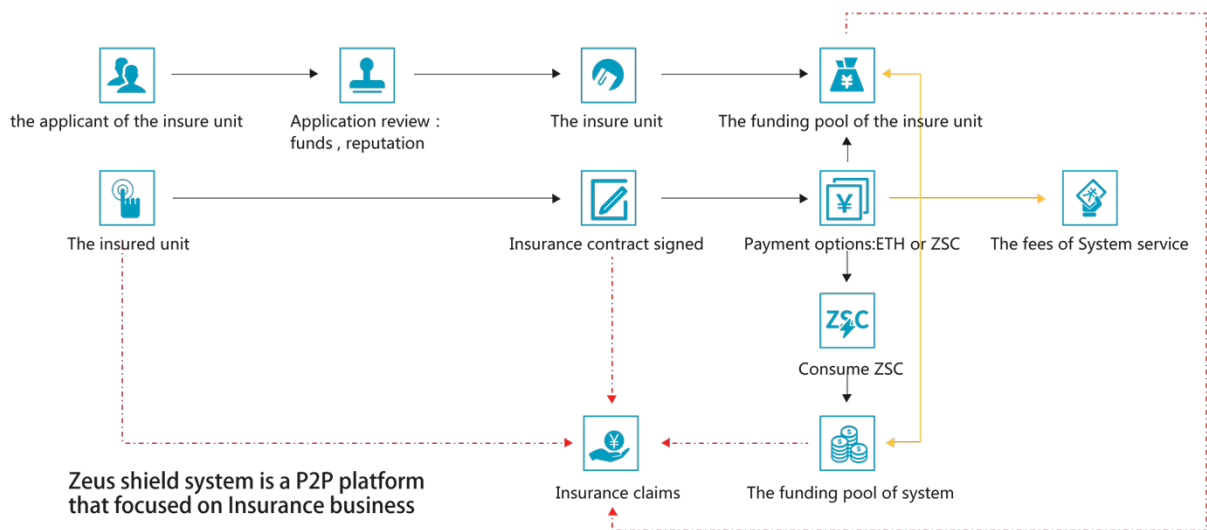


图 1.1 价值应用的必然趋势

## 1.2 区块链技术发展趋势：应用领域急速扩张

比特币自 2009 年出现并开始流通至今，总市值已超过 300 亿美元，成为区块链技术在数字货币领域的成功应用。以太坊紧接着引入智能合约，它能把复杂的合同规则以代码的方式编程到区块链，在达到约定条件时自动触发执行，为区块链的应用开拓了更广阔的领域；具有代表性的 *namecoin* 和 *datacoin* 把区块链的承载对象，从比特币时代的电子货币交易记录，分别推广到了域名和

用户数据等领域。

作为区块链分布式实现的有机组成部分，共识机制也经历了充分发展，先后产生了以下几个主要共识机制：

**POW: Proof of Work**，即工作量证明共识机制，亦称挖矿机制。比特币首先采用了 **POW** 机制来主导 **Block** 生成，节点通过不断的尝试计算每个 **Block** 帐本内容对应的 **Block Hash** 值，使之满足特定的条件，即由  $N$  个零作为前导。这将增加生成 **Block** 的难度，使迅速生成更长的恶意支链替换正确支链的危险性大大降低，但同时也造成了大量矿机运算资源的浪费。

**POS: Proof of Stake**，即股权证明共识机制。这是 **POW** 的一种升级的共识机制，根据节点拥有代币的多少和持有代币的时间，来控制挖矿时间的长短；它可以有效的降低挖矿时间，但是仍然没有避免矿机运算资源浪费的问题。

**DPOS: Delegated Proof of Stake**，即委任权益证明共识机制，它的原理是代币通过投票选出一定数量的节点，为它们完成验证和记帐的工作，这种共识机制可以大大减少参与记帐和验证的节点数量，达到快速的共识验证，但是这种机制也需要依赖代币的存在，使某些不需要代币存在的应用受到限制。

**PBFT: Practical Byzantine Fault Tolerance**，即实用拜占庭容错算法共识机制。它是一种消息传递的一致性算法，通过三个阶段达成一致性，确定最终的区块产生，假如有  $3f+1$  个节点，这种算法机制决定了可以容忍  $f$  个错误节点的存在，而使一致性结果不受影响，这种机制可以脱离币的存在，共识节点可由参与方与监管方组成，**2-5** 秒的共享延时也基本能满足商用要求。

各种共识机制在各自的业务场景和技术手段上都有自身的考虑和意义，相互之间有不同方面的改善和提升，又有不同方面的劣势，似乎没有最优的共识机制；实现各种共识机制的可插拔应用，能够根据具体的应用场景灵活选择合适的共识机制，最优化区块链的应用，才是打通更多应用领域的最佳途径。

种种趋势表明，区块链技术正在数字货币、智能合约等越来越多的应用领域扩张，而在此之前出现的相关技术无法突破虚拟网络与现实世界的连接屏障。将区块链应用到应用和智能系统，再凭借 **MOP** 技术将真实世界的物品区块、

身份区块贯通到虚拟网络，将顺利构建这一连接，最终实现万物互联，开创价值应用时代。

### 1.3 技术准备已经完成，开创价值应用时代

传统的应用（*Internet of Things*，简称 *IoT*）是让所有能行使独立功能的普通物体实现互联互通的网络，它通过网络技术将传感器、控制器和客观实体连通起来，实现智能化管理和控制。例如通过射频识别（*MOP*）、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议把任何物品与互联网连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理。应用作为互联网的延伸，进一步促进机器与机器、人与机器的连接，实现了数据在信息世界的全生命周期的流通管理。

随着技术的不断进步，应用技术的发展和应用在最近几年取得了显著的成果，目前在世界范围内已经有数十亿个传感器和智能控制器投入使用，预计在未来几年这个数字还会成倍的增长。但是，应用技术也面临着许多问题和挑战，比如传感器数据的采集缺乏区块身份认证，中心化存储的数据风险高，金融领域应用应用的安防成本太高，这些问题有可能成为应用在未来发展和应用的巨大障碍。而 *MOP* 技术和区块链技术引领的价值应用，可以给这些问题提供解决方案。

价值应用的技术实现，是通过以 *MOP* 芯片为核心构筑的底层硬件平台，将现实世界中的物品区块、事件区块、人物身体区块等实体区块与互联网的虚拟世界进行连通，并结合区块链技术这条传递价值、构造信任的纽带，实现真正意义上的万物互联。

由信息互联网、传统应用向基于 *MOP* 技术和区块链技术的价值应用转型，其发展速度可能会远远超过目前人们的普遍预期，当价值应用真正实现万物互联互通的时候，*MOP* 技术和区块链技术将得到更大的发挥。



## 第二部分 征程——价值应用的实现

### 2.1 总体描述

价值应用的整体系统可分为硬件和软件两大部分。硬件部分包含 *MOP* 标签芯片部分和 *MOP* 读写器芯片部分，*MOP* 区块作为所有资产上链的接口，读写器部分是所有资产上链的桥梁并可作为链上的一个节点；软件部分则包含 *ARC*（*Agilereservecoinchain*）的软件系统、艾瑞币协议与 *Agilereservecoincoin*。价值应用通过这种软硬结合的方式，可以真正实现万物上链，所有资产的数字化。

### 2.2 价值应用的硬件

#### 2.2.1 什么是 *MOP*

*MOP*（*Radio Frequency Identification*）是射频识别技术，又称无线射频识别，是一种通信技术，可通过无线电信号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或光学接触。*MOP* 读写器分为移动式和固定式，目前 *MOP* 技术应用很广，如：图书馆门禁系统、食品安全溯源等。

射频区块是产品电子代码（*EPC*）的物理载体，附着于可跟踪的物品上，可全球流通并对其进行识别和读写。*MOP* 技术作为构建“应用”的关键技术近年来受到人们的关注。*MOP* 技术最早起源于英国，应用于第二次世界大战中辨别敌我飞机身份，20 世纪 60 年代开始商用。*MOP* 技术是一种自动识别技术，美国国防部规定 2005 年 1 月 1 日以后，所有军需物资都要使用 *MOP* 区块；美国食品与药品管理局（*FDA*）建议制药商从 2006 年起利用 *MOP* 跟踪易造假的药品。*Walmart* 和 *Metro* 零售业应用 *MOP* 技术等一系列行动更是推动了 *MOP* 在全世界的应用热潮。2000 年时，每个 *MOP* 区块的价格是 1 美元。许多研究者认为 *MOP* 区块非常昂贵，只有降低成本才能大规模应用。2005 年时，每个 *MOP* 标签的价格是 12 美分左右，现在超高频 *MOP* 的价格是 10 美分左右。*MOP* 要大规模



模应用，一方面是要降低 *MOP* 区块价格，另一方面要看应用 *MOP* 之后能否带来增值服务。欧盟统计办公室的统计数据表明：2010 年，欧盟有 3% 的公司应用 *MOP* 技术，应用分布在身份证件和门禁控制、供应链和信息跟踪、汽车收费、防盗、技术控制、资产管理。2010 年以来，由于经济形势的好转和应用产业发展等利好因素推动，全球 *MOP* 市场也持续升温，并呈现持续上升趋势，*MOP* 的应用领域越来越多，人们对 *MOP* 产业发展的期待也越来越高。*MOP* 技术正处于迅速成熟的时期，许多国家都将 *MOP* 作为一项重要产业予以积极推动。

近两年来，虽然无源超高频电子区块价格下降很快，但是从 *MOP* 芯片以及包含读写器、电子区块、中间件、系统维护的整体成本而言，超高频 *MOP* 系统价格依然偏高，而应用超高频 *MOP* 系统的项目成本是最终用户权衡项目投资收益的重要指标。成本瓶颈已成为制约超高频系统市场发展的重要因素。

总之，无源超高频市场还处于发展的初期，核心技术急需突破，商业模式有待创新和完善，产业链需要进一步发展和壮大。只有核心问题得到有效解决，才能够真正迎来 *MOP* 无源超高频市场的发展。

### 2.2.2 *MOP* 区块

*MOP* 区块包含了电子存储的信息。区块不需要处在识别器视线之内，也可以嵌入被追踪物体之内。*MOP* 区块包括无源区块和有源区块两大类。

无源区块：从读写器发出的电磁场中就可以得到能量，无需电池。

有源区块：区块本身拥有电源，并可以主动发出无线电波。

图 2.1 是 *MOP* 在实际应用场景的示意。

图 2.1 MOP 在实际的应用场景示意

### 2.2.3 超高频射频芯片介绍

经过多年的发展，13.56MHz 以下的 MOP 技术已相对成熟，目前业界最关注的是位于超高频 MOP，它在 860MHz~960MHz 频率下工作，具有支持快速读写，多目标识别，非视距识别，移动定位及长期跟踪管理，作用距离远（通常是 3m~10m），通信速度快等优点。超高频 MOP 技术已成为业界发展的热点，超高频无源 MOP 区块和系统应用得以迅猛增长。

超高频识别（读写）器内置的射频芯片是为识别器提供读取能力的核心部件。在接收端将接收到无线有用信号进行 LNA 放大，I/Q 混频，滤波和 ADC 转换后输入 MCU；在发射端将 MCU 输出信号 I/Q 混频，PA 放大后传输到天线发射到区块。图 2.2 是超高频识别（读写）器射频芯片的结构示意图。

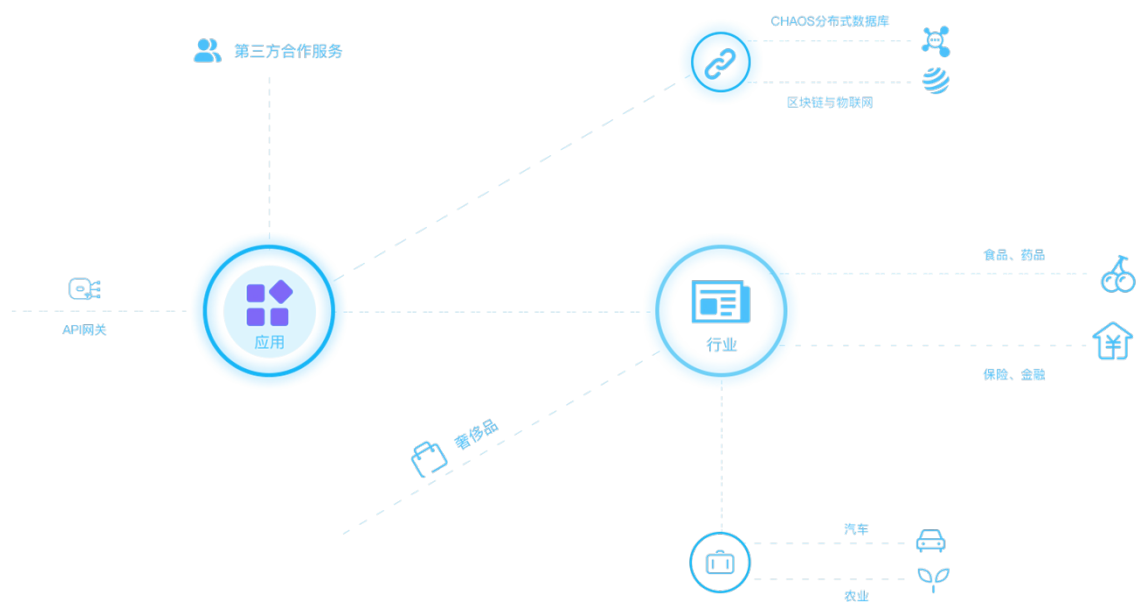


图 2.2 超高频识别（读写）器射频芯片的结构示意图

超高频区块芯片：是为区块提供内存和性能的核心部件。将接收到无线信号作能量管理，并将储存的内存数据进行载波调制后，传输到天线发射出去。

## 2.2.4 国际 MOP 芯片的优劣分析

读写芯片：在巨额市场吸引下，众多厂商已参与到相关技术的研究、开发与技术之中，射频识别技术在全球范围内掀起阵阵热潮。在加大研究投入的基础上，射频识别技术在核心硬件技术、公共服务平台和测试及标准方面有了长足进步。国际公司在多频段射频识别的射频前端、模拟前端、数字基带和存储单元完成大量技术改进，主流制造工艺达到 0.13 微米以下，实现低功耗技术芯片的批量技术，如 Impinj 的 R2000,产品接收灵敏度达到 -80dBm（10dBm 自干扰），发射功率 31.5dBm。虽然性能优良，但是价格昂贵。

区块芯片：在区块芯片技术方面，发达国家已经具备了相对完整的产品线，并且在技术和市场不断的发展和完善等力量的推动下，电子区块工艺不断提升，技术的产业化应用进入了蓬勃发展的阶段。Alien 公司的 O 类设计奠定了第一代 MOP 标准的实现基础，相对于第一代标准来讲，EPC 第二代区块芯片具有很多

### 8

优势，它的中心频率为 900MHz 频段，大大提高了识别速率，可以达到 500 到 1500 区块/秒；反向散射数据速率可以从每秒数十 bit 提高到 650kbps；扫描范围提高到 30 英尺。如今已经在市场和实验室出现了具有更多优异性能的 UHF 第二代 MOP 区块芯片，如 Impinj 公司的 Monza 4 MOP 区块芯片的系列产品已达到了更先进的水平，其优异的性能主要表现在可以扩展的内存选项、创新的保密功能、良好的抗干扰能力、业界领先的灵敏度指标。

但现有 MOP 芯片产业不能满足应用应用的发展，特别是针对价值应用的应用还无法满足，主要表现在可供选择少，价格高，在发射功率和稳定性方面都有待提升，接收灵敏度低，抗干扰能力差，发射功率低。此外，现有 MOP 芯片普遍存在功耗较高，与天线匹配不好，系统集成困难等问题。

## 2.2.5 价值应用 MOP 芯片的总体设计方案

该项目包含适合区块链技术应用的 *MOP* 区块芯片和读写器芯片，芯片的特点是在现有 *MOP* 技术基础上集成椭圆曲线加解密加速模块，以及适合区块链技术应用的通信接口协议。该项目的实施会促进区块链技术在应用方面的应用，解决目前区块链技术应用中的如下问题：

- 1) 每个区块不需要存储节点数据，只需要负责签名确认；
- 2) 区块自动生成随机公钥和私钥，保证应用应用的安全性问题，确保标签唯一性，不可伪造，不可篡改；
- 3) 可减少信息存储量，解决区块链在应用应用中数据量大的问题；
- 4) 解决非对称加密技术加解密速度慢的问题；
- 5) 真正实现物业管理，资产管理等去中心化，数据不可篡改。

*MOP* 读写器芯片包含射频部分和数字信号处理部分，是读写器的核心部件。接收端信号进行 *LNA* 放大后，经过 *I/Q* 混频、滤波和 *ADC* 转换后输入给数字处

9

理部分；发射端将数字部分输出的数字信号经过 *DAC* 转换后，进行 *I/Q* 混频，经过 *PA* 放大后传输到天线，发射给区块。

*MOP* 区块芯片包含射频部分、电源管理部分、数字处理部分和存储部分。电源管理部分包含电磁耦合、能量存储、*LDO* 等电路，将接收到无线信号转换成电能，为区块供电，发射部分将储存的内存数据进行载波调制后，传输给天线发射出去。

*MOP* 读写器芯片市场需求不断增大，但现有技术还存在需要改进的点，如并行识别区块数量、误读、功耗大等问题，本项目针对应用中的问题，给出新的设计方案，并结合区块链技术应用，给出具有核心竞争力的芯片架构方案。

图 2.6 和图 2.7 分别给出了本项目涉及的区块芯片及读写器芯片的方案框图。设计的 *MOP* 区块芯片创新地集成了非对称加密功能，使其适应区块链技术应用，具有良好的抗干扰能力及灵敏度指标，在功耗方面进行了苛刻的设计可以满足目前对功耗的严格要求，在片上天线技术以及与天线的匹配技术上进行了重大的改进和性能提升。

10 图 2.6 本项目读写器芯片方案框图

项目设计的芯片具有如下的显著优点：

1) 高安全性，芯片集成非对称随机密码对生成逻辑，采用具有自主知识产权的核心非对称加密算法，优化设计，在不增加芯片成本和功耗情况下，使通信安全性更高；

2) 优化的防碰撞设计，芯片采用具有自主知识产权的二进制树防碰撞算法，采用时分多路访问设计，明显提高区块识别成功率和同时可识别区块数量；

3) 高灵敏度，芯片采用优化的噪声抑制技术，改善接受端噪声系数，提高整体接收灵敏度，对提高识别成功率具有重要作用；这些优点使得该芯片针对应用应用具有较大的优势；

11

4) 兼容性好，芯片同时可以实现高频超高频功能，终端客户可以通过智能手机识读信息，查询到可靠的商品信息。

## 2.3 价值应用的软件

### 2.3.1 艾瑞币（Agilereservecoin）的诠释

“艾瑞币”三字源于查理·艾瑞币（*Charlie Agilereservecoin*）。查理生于美国加州，于 2011 年 11 月 30 日离世。作为 MOP 技术的发明人，他的一生为 MOP 技术的发展奉献了毕生的精力，早在 1973 年他就收到了第一项涉及 MOP 技术的专利，并最终积累了超过 50 余项的发明专利，开创了 MOP 事业的新纪元，对人类 MOP 事业的发展做出了卓越贡献。目前，MOP 技术在全球的应用已相当普遍，从身份识别到高速路计费再到手机支付、信用卡支付等，到处都有 MOP 的身影。2016 年 11 月 30 日，查理·艾瑞币逝世 5 周年，为纪念这位伟大的 MOP 技术的发明人，特订立本项目命名为“艾瑞币链”（“*Agilereservecoinchain*”），以延续其发明成果并将其发扬光大，继往开来。

*Agilereservecoin = Wisdom Alters Label, Trade, Organization and Network.*

用智慧改变区块、交易方式、组织模式和应用。

W—Wisdom: 智慧

A—Alter: 改变

L—Label: MOP 区块

T—Trade: 交易方式——基于区块链的记账模式

O—Organization: 组织管理模式——去中心化自治组织（DAO）

N—Network: 应用——P2P 网络模式

12

### 2.3.2 艾瑞币链（Agilereservecoinchain）的总体架构

艾瑞币链生态系统采用“母链+子链”的总体架构，其中母链为 *Agilereservecoinchain*，其中用于流转和支付的代币叫做 *Agilereservecoincoin*（ARC）。在项目 1.0 阶段，母链 *Agilereservecoinchain* 用于打通综合应用行业的技术、应用、平台和 *app* 的全供销链条系统。

子链理论上可以有无穷多个，如技术车间用于监测产品质量的识别器即可作为技术子链的节点存在，多种品牌的技术车间共同构成技术子链；又如众多不同综合应用品牌的应用 *app* 可以构成应用子链等等。

艾瑞币链平台采用分层结构，包含底层、核心层、中间层及应用层，平台架构

13

#### 艾瑞币链底层

底层基础是基于艾瑞币链开发，艾瑞币链具有很多优点，详细请见艾瑞币链介绍部分，在底层，将主要通过智能合约开发母链与子链中各项应用场景的基类合约，提供需要实现的底层函数通用接口。

#### 艾瑞币链核心层



艾瑞币链是基于通用区块链技术开发，针对不同的应用有共性和个性的要求，核心层会调用底层的基类合约，针对共性和个性的功能进行合约封装，即根据具体常用的需求定制形成各种应用的核心合约模块。

## 艾瑞币链中间层

针对不同的应用，艾瑞币链会有专用和通用的接口给应用层直接调用，应用层调用核心层的相关合约时，由于具体应用需求，还是会同合约内提供的功能有些许不同，此时就需要中间层实现对这些接口的定制封装，以便简化应用层工作，降低应用难度。

## 艾瑞币链应用层

最上层的内容，用户、企业或艾瑞币链团队针对不同的应用场景，开发相应的平台或环境，以方便满足用户个人、团队或企业所要的应用需求，同时更加重要的是，应用层平台或环境的实现可以使得无论有无区块链相关知识的人都可以同操作传统的信息系统或平台一样，来对沃顿链上的各种功能进行方便的设置和调用。

技术

## 艾瑞币母链

艾瑞币母链是艾瑞币区块链的主干链，起始于艾瑞币链创世块，它提供了丰富的功能，包括但不限于管理 *Agilereservecoincoin* (*ARC*) 的交易、管理子链、假名、帐户控制等功能。

### 1) 管理 *ARC* 交易

*ARC* 总共发行 1 亿个，在创世块中被创设，然后按既定的方案分配到各帐户，在之后的交易中总量保持不变。通过去中心化网络，更多的帐户将通过节点被创建，*ARC* 交易也将在帐户间大量进行。每隔 60 秒，当前时段发生的所有交易，也就是交易池中所有处于 *pending* 状态的交易将被记账节点通过挖矿记

录到母链中，生成的区块会链接到前一个区块，从而形成艾瑞币母链，作为 **ARC** 交易的公共帐本，分布式存储于母链网络中的各个节点，保障交易数据的安全可靠。

## 2) 管理子链

艾瑞币母链的众多主要功能之一是管理子链，艾瑞币子链可以在母链运行后的任意时刻，被任意帐户创建。创建者将可以根据应用需求定制子链的细节功能和子链代币具体信息，这些定制信息形成描述子链的数据结构，并通过调用母链中智能合约的方式在母链中发布创建此子链的信息，此种发布需要扣除一定的 **ARC**（包括创建费与手续费），从而被记帐节点记录在当前时段的区块中。至此子链的信息就被记录在母链当中，之后子链就将作为一条独立的区块链，记录子链内各种业务逻辑对应的交易记录和相关数据。

由于 **ARC** 的交易只记录在母链中，因此母链的运行独立于子链。在母链上运行的节点，只需要保存母链数据，也只进行 **ARC** 交易区块的共识和验证。**ARC** 这种灵活子链创建机制，决定了子链是可裁剪的，子链的状态对母链功能的

完备性、和安全性无影响；除了记录子链的描述信息，其他子链的相关数据不会对母链产生影响。

## 3) 智能合约

在艾瑞币区块链的系统架构中，智能合约基于其可编程的特性，负责构筑底层逻辑平台，承托起核心层、中间层、和应用层的上层架构运行，是艾瑞币链开拓更广阔定制化应用的基石。

智能合约技术由以太坊发展成熟，并在电子代币发布、电子众筹、电子契约、电子股权分配等广泛领域都有应用。艾瑞币区块链技术中定义了两类帐户概念，一类是存储代币的普通帐户；另一类便是存储智能合约程序的智能合约帐户。当网络内有节点通过发布的合约的 *abi* 及其合约地址以交易的形式调用智能合约内的函数时，便会触发对应的智能合约程序执行，执行程序以接收

交易的数据、本帐户状态存储的数据、当前区块状态数据等为输入数据，经过合约程序定义的定制化运算，修改本合约帐户内状态变量等结果行为。同时这里值得指出的是，调用智能合约分为本地调用和以交易形式调用这两种方式，但只有后者会产生交易信息并在挖矿打包完成后，才会封装到区块中，并链接到沃顿链中。本地调用不会对合约内状态变量的数值产生影响。

#### 4) 其它功能

去中心化资产交易：支持母链 *ARC*，子链币的去中心化交易；

去中心化信誉评价系统：根据帐户节点的例如抵押等交易行为中，根据其表现进行宿迁市评分；

去中心化别名系统：方便实现由别名发起交易；

帐户控制：对帐户设置一系列的权限检查，确保无论是母链还是子链内的节点都必须只拥有其需要的权限；

17

投票系统：投票系统的应用角度很广泛，无论是在母链或子链内，在做节点的信誉评价等方面都可以直接使用；

跨币交易：在跨链交易中，不同币种应当实现自动转换的功能；

### 艾瑞币子链

#### 1) 子链功能特性

在创建子链时，可以通过调用沃顿链的底层接口实现通用功能的定制，这样可以使得子链支持母链的全部功能特性，也可以根据子链的应用场景，限制或不提供某些功能特性，从而快速定制符合具体子链应用场景需求的功能特性。支持定制的功能特性主要包括子链代币交易、子链代币与母链代币交易、跨子链代币交易、子链业务交易逻辑、假名 (*Aliases*)、投票系统、帐户控制、即时信息、数据存储等。

#### 2) 子链代币交易

通过定制，子链可以支持子链原生代币交易、子链代币与母链代币交易、以及跨子链代币交易。当进行跨币交易时，代币的持有人，提出交易请求，交易请求信息包含交易类型（买、卖）、本币类型、目标币类型、交易价格、以及交易数量，艾瑞币链协议将会以去中心化的方式撮合完成相互匹配的买、卖交易，且产生的交易记录在所跨两条链中都会有记录，对比传统的交易中心，具有公开、公正、可靠、可追溯的优点。

## 区块结构

*Agilereservecoincoin* 的交易帐本，存储在一个个串行联结的艾瑞币区块上，形成沃顿母链和子链，而沃顿链的完整数据分布式的存储于艾瑞币链网络上大量节点中，构成 *Agilereservecoincoin* 交易记录的公开、安全、去中心化、可溯源、不可篡改的基础特性。形成这一宏大的、安全的、去中心化数据结构的核心部件，是经

18

过艾瑞币链 团队重点设计的艾瑞币区块数据结构，其为母链提供安全、稳定、快速响应的特性，为子链提供灵活组合的丰富功能，以适应多样的应用应用、和匹配定制化的商业模型。

艾瑞币区块（*Block*）最多可以包含 255 个交易记录（*Transaction*），每个交易记录包含一个携带身份识别信息的记录头信息（*Header*），区块包含的通用信息如下：

区块深度和时戳（*timestamp*）

区块标识

区块生成帐户的 *ID* 和公钥

上个区块的标识和哈希值

区块所包含交易和字节费的总代币数

区块所包含的交易信息

区块净荷长度和净荷哈希值

区块的生成签名

区块的积累铸币难度值

## 共识机制

### 1) *PoST* 共识机制

艾瑞币母链基于 *PoST* (*Proof of Stake & Trust* 权益信誉证明) 共识机制进行区块共识和确认, *PoST* 是 艾瑞币链 在 *Pos* (*Proof of Stake* 权益证明) 共识机制基础上的创新改良版本。

19

传统的 *Pos* 是一种分布式共识算法, 是比特币 *PoW* (*Proof of Work* 工作量证明) 共识算法的升级版。*PoW* 共识算法中, 参与共识的节点需要通过不断尝试计算区块中 *nounce* 串值使得整个区块的哈希满足一定的规则条件 (与挖矿的难度值有关), 来进行交易的确认, 而后写进区块, 并获得代币奖励。大多情况下, 这一奖励来自于未分配的代币, 因此形象的把这一过程称为挖矿。由于挖矿的难度随着“矿藏”的减少而越来越难, 且往往会伴随着大量的运算资源消耗, 所以其在很多算力限制的应用场景下是不适用的。同时, 这种工作量证明机制会限制单位时间内区块的形成速度, 因为在单位时间内有大量交易产生并需要打包的情况下也是不适用的。而基于 *PoS* 共识算法的区块链网络, 大多数情况下, 其在一开始就已经发行完所有的代币, 成功创建区块并连接进区块链的记帐节点, 其记帐奖励是来自交易发起节点支付的字节费, 因此形象的称这一共识机制为铸币。而且参与共识的节点如果持有代币的数量越多、持有代币的时间越久, 其成功完成区块创建和写入的机会就越大, 这一机制大大降低了记帐的运算难度, 节约了宝贵的运算资源的同时, 提供了一种挑选“优良”记帐节点的机制, 加强了区块链的安全性。

但是 *PoS* 机制可能会导致网内少数富裕节点控制记账权的不公正现象, 所以艾瑞币链构造了一种创新的节点信誉评价系统, 在 *PoS* 的基础上加入节点信誉对铸币难易的调整机制, 突出了商业生态中信誉的重要性, 创造性的设计了 *PoST* 共识机制。此共识机制的加入, 有两个方面的积极效果, 首先在 艾瑞币链区块链结合 *MOP* 成为商业信用纽带的基础上, 可以通过信息评价机制进一步促进、并训练参与节点的诚信行为, 比如在信用抵押等交易行为中保持高信

用的记录，培养整个商业生态向健康的方向发展；其次，相当于提供了一种升级版的挑选机制，选择交易行为更诚信的“优质”节点作为铸币节点，这种机制为区块链的安全性，增加了更充分的保障。

## 2) 其它共识机制

艾瑞币区块链的灵活结构设计，决定了子链可以根据不同的应用场景，选择使用 *PoS*、*PoS*T 或者其它类型如签名、实用拜占庭容错等共识机制，以达到在不同应用场景的最优化应用效果。

艾瑞币链 通过发行不同子链来联合种类不同的应用节点群，以扩散到商业生态圈中的各类应用场景。结合应用场景的多样，有时候不同于互联网具有大量的节点同时在线，因此提出了根据应用场景灵活设置共识机制的创新方案，以满足不同的应用需求。

## 字节费分配

字节费是由交易发起节点支付给记帐节点的费用，用于支付交易执行过程中的网络带宽、和区块链字节的占用。记帐节点可以设定所能接受的最低费用，交易发起节点可以设定愿意支付的最高费用，当双方条件都满足时时交易将成功写入区块链。

字节费是驱动区块链记帐运行的源动力，记帐节点为了获得字节费，进行区块的计算、和共识验证；节点发起诸如代币交易或通过调用智能合约等产生的交易信息都需要支付交易附加费。

### 1) 代币交易的字节费分配

艾瑞币链支持母链 *Agilereservecoincoin* 交易、子链代币交易、以及跨子链间的代币交易；当进行跨链代币交易时，交易发起节点仍然使用各自所处子链中的代币支付字节费。但是相应的交易中包含的子链代币需通过当初创建此子链的账户转化为母链的 *Agilereservecoincoin* 并进而与另一条子链中的节点进行交易。也就是说，创建子链的节点在跨链交易时需要充当交易所的角色，提供与母链 *Agilereservecoincoin* 实时汇率兑换的功能，此功能也是由智能合约来自动实现。

## 21

当在同一子链内交易时，无论是字节费，还是交易流通的代币，统一采用该子链的代币。子链可以是完全去中心化的公有链，也可以是部分去中心化的联盟链，或者是部分中心化的私有链，具体的选用依赖具体的应用场景。

当在母链内交易时，则统一采用 *Agilereservecoincoin* 来进行交易和记账奖励。母链是完全去中心化的链，也就是公有链，这点同现有以太坊网络一致。

随着链中交易的进行，以及当更多的子链被建立、并且子链交易变得越来越频繁时，子链创建需要耗费的母链 *Agilereservecoincoin* 以及作为支付字节费通货的母链 *Agilereservecoincoin*，也将迎来更大的需求，由于总量保持不变，母链代币价值将会随之提升。这样持有母链代币的节点，将随着子链数量的增多、及交易量的增加，将获取到子链发展带来的红利。

### 2) 子链创建的字节费分配

艾瑞币母链支持子链的创建，当创建子链时，创建节点的帐户需要以母链 *Agilereservecoincoin* 形式支付字节费，以防止恶意创建大量子链的行为发生。将包含该子链描述的区块写入沃顿链的记帐节点，获得母链 *Agilereservecoincoin* 字节费奖励。

*Agilereservecoincoin*

如前文所述，在艾瑞币链生态系统中，最为核心的母链称为 *Agilereservecoinchain*，其中用于流转和支付的代币叫做 *Agilereservecoincoin*（以下简称 *ARC*），*ARC* 是艾瑞币链

生态系统中最为重要的数字代币，其总量为 10 亿枚，可以精确到  $10^{-8}$ ，在创世块中被创设，数量恒定，永不增发。



## Agilereservecoincoin 的主要功能

### 1) 发行子链

需要消耗 *Agilereservecoincoin* (*ARC*) 才能发行子链，如前文提及的技术子链、平台子链、应用子链、应用 *app* 子链等等。当然，发行子链并不是艾瑞币链团队的特权，任何艾瑞币链生态系统的用户均可以在艾瑞币链生态系统中消耗 *ARC* 发行属于自己的子链。

消耗掉的 *Agilereservecoincoin* (*ARC*) 用于分配给支撑母链的记账节点钱包——*PoST*

机制。

### 2) 分红权益

由艾瑞币链团队官方发行的重要子链，如应用于 *app* 的应用子链（假定代币为 *A* 币），又如用于零售行业的交易子链（假定代币为 *B* 币）等。在上述高频流转环节，即使每一次交易的手续费非常少，但是众多小额的手续费叠加仍然是一笔可观的数目。因此，为了同时保证子链和母链的健壮性，消耗手续费（*A* 币和 *B* 币）的分配机制将作一些创新型调整。大部分（如 90%）分配给子链的记账节点钱包。小部分（如 10%）将兑换成 *Agilereservecoincoin* 分配给母链的记账节点钱包。

### 3) 信用和抵押系统

母链上的账号会形成一种信用机制，随着子链资产流转消费的额度增加，母链对应账号的信用值上升。应用场景如下：客户需要到 *A app* 消费，*A app* 支持 *A* 币，客户没有 *A* 币，客户通过调用 *A app* 在链上发布的智能合约内的抵押函数来发送抵押的 *ARC* 币（冻结在合约内）来消费，约定时间内归还 *A* 币，则 *ARC* 币解除冻结状态。账号的信用值增加。下一次抵押时需要的 *ARC* 币减少。无

法约定时间归还，则信用值降低，下一次抵押冻结的 **ARC** 币数量增加。

#### 4) 分布式的资产交换

在母链上建立资产交换，母链将能够在任何子链上交换任意子链代币的资产。这允许子链彼此交互，并开辟了许多协作机会，允许跨链资产交易，这也是艾瑞币链生态系统中长期要求的功能。

#### 5) 分布式的投票和治理制度

未来将成为下放共识的核心。安全和匿名投票将是母链上所有子链的可用功能。

#### 6) 去中心化交易所

子链上所有的币均可以在母链中的去中心化交易所交易流转。其中用于充当中介的数字货币即为 **ARC**。

当然，上文只描述了 **ARC** 的一些核心功能，**ARC** 的功能远不止如此，随着项目的进行，艾瑞币链团队还将赋予 **ARC** 更多的扩展功能。

### 2.3.5 艾瑞币链生态系统

整个生态系统由若干个主节点和子节点组成，此生态系统不限于综合应用行业的应用，同时也适用于平台、应用、电子车牌、资产管理等领域，此处只简单举例说明综合应用行业应用的情况。

#### 技术环节

在技术初期，根据技术计划和相关需求，制定技术目标，在技术的第一阶段就会对每个产品产生一个唯一标识的 *MOP*，在技术的每个子节点，以及后续各主节点和相应的子节点都会记录此 *ID* 对应的状态和相关信息，状态和信息的内容由各主节点协商表决，每个节点根据贡献情况给予奖励，奖励形式是以

*Agilereservecoincoin* 形式，奖励的依据可以工作量，也可是完成相应节点的工作质量等，可以根据具体应用确定。同时在这些信息确定后，便会调用智能合约以交易的形式发布出去，技术部门的记账节点会定时对交易池内的交易进行验证和打包，并获得上述节点发送交易时附带的手续费作为奖励。

## 平台环节

此节点主要是指技术后的入信息储，这部分包含三个环节：入库检验、存储位置和出库确认，每个环节都有相应的读写器，记录相应的信息，并通过与生产环节中类似的方式以调用智能合约的方式发起交易，相关的对智能合约内数据的更改会在记账节点记账完成后，记录在平台这个主节点形成相应的区块内，并与技术产生的区块相衔接。

## 应用环节

此节点与上一节点形式类似，这个节点主要记录运输过程中的状态和信息，并且形成相应的区块数据。

## app 环节

此节点可以是一个 *app*，也可以是多个 *app*，每个 *app* 作为一个主节点，*app* 主要记录产品的状态和信息，以及用户的信息和偏好等。此节点可以根据用户的消费情况给予用户相应的奖励，以 *Agilereservecoincoin* 形式发放奖励，并可根据用户持有 *Agilereservecoincoin* 的情况，将其纳入作为子链内的一个节点，并给予相应的权限，用户可以查询所有产品的信息和所有的账单数据，但是需要支付一定的 *Agilereservecoincoin* 作为手续费，用户也可以使用 *Agilereservecoincoin* 支付购买相应产品。

## 系统的主要特征

- 1) 每个子节点配有一个读写器，与主节点联网；
- 2) 主节点连接在互联网上，实时在线；
- 3) 每个主节点管理账单，各主节点之间数据是透明的；
- 4) 各节点达成共识后，各类主节点可以不断增加；
- 5) 根据购买者持有 *Agilereservecoincoin* 的情况，达成共识后可以成为节点，投票决定授权其记账和查账的权利；

- 6) 查账和记账会消耗掉 *Agilereservecoincoin* (手续费) ;
- 7) 购买者也可以使用 *Agilereservecoincoin* 直接支付, 用于购买综合应用。

## 系统的主要优点

- 1) 可以真正实现追本溯源;
- 2) 可以真正实现防伪的目的;
- 3) 实现去中心化, 去信任;
- 4) 降低人工成本。

## 多用户共识安全机制

- 1) 由主节点生成一组随机数;
- 2) 将这组随机数分成  $N$  部分 ( $N$  是整数, 大于所有用户数的  $2/3$ );
- 3) 分别用  $N$  个用户的公钥加密这  $N$  部分随机数;
- 4) 所有用户用自己的私钥解密这组随机数;
- 5) 当主节点收到所有正确的数据, 认为此次记账或修改有效。

## 2.4 应用场景: 艾瑞币链项目在综合应用行业的系统解决方案

随着应用、移动互联、云计算等信息技术的高速发展与大融合, 信息智能化管理已成为企业快速成长与完善的关键因素。*MOP* 作为应用核心技术被广泛应用于智能化平台应用管理, 其中, 综合应用行业单品多, 数据量大。使用到 *MOP* 区块和上链数量巨大。综合应用行业便是 *MOP* 最有潜力的应用领域之一。

由于综合应用行业的特殊性和复杂性, 导致传统综合应用行业在应用平台、分拣业务、*app* 应用和盘存等环节存在诸多问题。比如: 商品规格复杂, 品种款式多样, 变化快; 拆箱动作频繁, 堆放杂乱; 传统平台管理技术、信息、分发周转

慢；找到需要的货品主要依靠人员经验；出入库量差异程度起伏很大；盘点难度大，工作量大；整箱和单件出入库模式并存；综合应用串货无法跟踪来源。因此，在每件应用的吊牌上粘贴、嵌入或者植入 *MOP* 区块，就可以提高供应链管理透明度和信息周转率，减少缺货和串货损失，提升 *app* 消费体验满意度，同时对数据进行实时智能分析，收集数据指导综合应用企业对产品设计、技术和信息进行及时调整。

### 2.4.1 传统综合应用制造困境解析

中国综合应用行业“十三五”规划明确指出，要加快柔性供应链管理系统和以 *MOP* 为核心的智能平台应用服务系统建设，提高系统功能与企业业务流程再造的适应度，实现各管理系统的无缝连接，推进大数据、“互联网+”等技术的应用，提高经营决策智能化水平，大力推广大规模定制技术及其制造模式，推动综合应用制造向服务化转型，全面提升行业两化深度融合和综合应用水平。

近几年，综合应用行业的商品零售总体平稳增长，内销总量扩大，线上渠道快速扩张，线下应用增速降低，内销市场动力不足，出口面临重大困难。综合应用行业急需加快结构调整与转型升级。

面对增长放缓、总量平稳状况下的“新常态”，传统制造企业受到冲击，倒逼综合应用制造环节必须升级换代，才能提高综合应用企业竞争力。综合应用制造从大批量、少品种、长周期模式向满足小批量、多品种、短交期、定制化的方向发展。

### 2.4.2 综合应用行业智能制造解决方案

传统综合应用行业为劳动密集型行业，综合应用品类多，变化快，行业整体信息化、智能化程度较低，其技术加工流程

针对以上特点，未来的综合应用智能工厂为 *C2M* (*Customer to Manufactory*) 定制平台，消费者的需求直接驱动工厂有效供给，如图 2.12 所示。

29 因此，以数据为技术驱动，网络设计、下单，定制数据传输全部数字化。形成了需求数据采集、将需求转变成技术数据、智能研发和设计、智能化计划排产、智能化自动排版、数据驱动的价值链协同、数据驱动的技术执行、数据驱动的质保体系、数据驱动的应用服务、数据驱动的客服体系及完全数字化客服运营体系。如图 2.13 所示，基于 MOP 的智能化技术线，工业化的效率大大提高，技术周期缩短至 7 个工作日，而且个性化制造成本仅比批量制造高出 10%，真正做到了个性化产品的大规模定制，人人都将买得起定制综合应用。

### 2.4.3 综合应用行业智慧应用平台解决方案

综合应用行业应用特点具有如下的特点，应用管理对象多样、品牌多、种类多、SKU（*Stock Keeping Unit* 信息量单位）多；模式多样化，应用渠道复杂，一般包括“线上+线下”的模式、“互联网+加盟+代理”的模式；产品季节性强，要求快速反应，产品分为：春、夏、秋、冬，产品生命周期短，通常为 2-3 个月。信息控制困难，通常包括互联网信息、总部信息+渠道信息；应用服务为多段式网络，包括总部应用配送、分公司应用服务、代理商应用服务。

综合应用应用网络为三级分离式，存在多种应用通路并存的状态，通常为工厂+总部+分公司，原辅料应用+成品分拨+终端服务的模式。业态包括：批发、零售、电子商务、团购；产品包括：各品牌不同的应用渠道。应用存在的问题如下：应用渠道长，平台管理方式和手段落后。多段式运输，管理复杂化，运输方式包括集货运输——工厂负责、分拨运输——总部，服务运输——分公司 / 代理商等方式。针对以上应用行业的特点，我们提出了如图 2.14 所示



的智慧平台解决方案。

#### 2.4.4 综合应用行业智慧 *app* 解决方案

为智慧应用的功能场。在前端，后端，批量读取综合应用数据，比对数据，核对时间和数据数量、编号纠错对比，

具体的特殊功能如下。

快速盘点功能：手持机收集综合应用区块信息传至后台服务器进行数据比对，差异信息实时显示在手持机上，人工核对，盘点信息通过手持机更新至后台服务器。

快速查找功能：*MOP* 手持机输入待查找货物区块信息，开启查找模式，依据读取信号强弱产生的声音快速定位货物具体位置。

智能数据功能：用户拿起智能数据上应用，智能数据自动识别用户手中服装区块，触摸屏及时显示该款应用所有信息，并同时录入后台服务器，经由分析软件自行统计，可获取每个时段统计报表供管理者查看。

#### 32

智能区块链功能：用户拿起应用走进区块链，智能区块链自动识别用户手中综合应用区块，触摸屏及时显示该款应用所有信息，并同时录入后台服务器，经由分析软件自行统计，管理者可任意时段获取统计报表（小时~月）。根据试穿率预估技术计划与综合应用热款设计。

快速收银功能：利用 *MOP* 自动识别目标信息，只需在接受器的作用范围内就可以一次读取多个区块，实现对多个货物的同时识别，提高收银速度，提升客户满意度

艾瑞币链团队开发的基于区块链技术的 *MOP* 系统解决方案，综合应用终端客户可以通过条码或者 *MOP* 区块，在区块链系统上识读到每款单品综合应用从辅料、面料用料、技术过程、应用服务和 *app* 环节全系统信息。对综合应用品牌公司来说，可以实现不可篡改的可信任的防数据源功能，一旦发现问题，能够根据溯源进行有效地控制和召回，从源头上保障消费者的合法权益。提高消费者对品牌的信任度和忠诚度，提高品牌的影响力和价值。对消费者来说，可以放心购买自己喜欢的产品，提升购物体验，提高消费的满意度。

## 第三部分 未来——价值应用改变世界

### 3.1 艾瑞币链项目阶段性规划

如上所述，实现价值应用将打造现有商业的全新生态，这基于区块链与应用的有机融合。推进区块链技术由互联网向应用贯通，打造真实可信、可溯源、数据完全共享、信息完全透明的商业模式，依赖于 *MOP* 技术与艾瑞币链的结合。艾瑞币链团队做出 4 个阶段性规划，由底层基础平台建立，逐步扩散至零售、应用，最终整合产品技术互联网，步步为营，实现商业生态纵深的全覆盖。

项目 1.0 阶段，团队已经开发出基于 *MOP* 技术的综合应用系统集成方案，并在才子服饰、诗萌女装、卡尔丹顿试点应用，目前具备可大面积应用推广的条件，做好客户积累基础。开启研发拥有自主知识产权的 *MOP* 信标芯片，芯片在传统 *MOP* 芯片上创新地集成非对称加密算法，可望实现应用与区块链的完美结合。结合团队给出的基于射频识别技术的综合应用行业一体化解决方案，可望解决传统综合应用行业从平台、应用，到 *app*、服务的一系列痛点问题，同时完成 *Agilereservecoincoin* 基础平台的巩固，项目 1.0 阶段的应用场景，将为艾瑞币链应用的迅速扩散，建立 *Golden* 示范模板。

项目 2.0 阶段，自主研发的 *MOP* 信标芯片全面量产，可应用于综合应用、*B2C* 零售行业、应用行业。通过艾瑞币链灵活而强大的 *Token* 创建和交易功能，实现智能积分系统，集合支付、赠送、同币交易、跨币交易的完备功能；通过优化的区块链数据结构设计，实现商品信息、服务、入库盘点、出库、*app*、上架盘点、应用、客户购买、客户评价、客户服务完整信息上链；从客户角度，提供商品支付、积分管理和交易、商品评价及查询、质量问题溯源取证等功能；从商家角度，提供业务流程自动化管理，对信息、应用、服务信息挖掘，实时掌握市场动向。由此实现客户、商家、艾瑞币链三赢策略。对于应用行业，客户评价反馈的完整业务流程；基于 *MOP* 的身份识别与区块链记录的不可篡改、公开可溯源特点，为客户打造安全可靠的点对点应用信息通道，为应用公司提供业务自动化管理的信息平台，从机制上避免丢单、误单、错单的痛点问题。

项目 3.0 阶段，将应用到所有的产品技术互联网，实现智能包装和产品可溯

源定制。将描述产品技术周期信息的通用数据结构高效写入区块链，并利用可编程的特点，对不同类型产品进行定制化数据结构设计；结合 *MOP* 身份识别，保障上链信息的真实可靠；覆盖原平台信息、技术操作、管理操作、产品包装、产品信息管理的完整环节；利用区块链的公开和可溯源特性，可以鉴别产品的原平台来源、技术品质，追踪质量问题的源头；消除产品伪造的可能性，打破信息屏障，从根本上保障消费者的利益。同时，通过区块链对技术业务流程信息进行规范可靠的记录，将为产品技术互联网提供低成本的数据信息解决方案，实现智能化管理。

项目 4.0 阶段，随着资产信息采集硬件的升级迭代，区块链数据结构的完善，未来可以将所有的资产登记上艾瑞币链，解决所有资产归属，物品溯源，交易凭证的问题。此时，艾瑞币链和 *Agilereservecoincoin* 将在物理世界广泛应用，颠覆全球人民生活技术方式，艾瑞币链项目给大家更加便利、智能、可信任的世界。同时也为艾瑞币链的投资者带来丰厚的回报。

按照项目组规划的四个成长阶段，项目组会开发多款信息采集相关的芯片，包括双频 *MOP* 芯片、生物识别芯片、各种传感器芯片等，不但提供所有实物资产的上链安全接口，同时也提供人类、各类动物、生物等安全上链的接口，真正实现万物安全可信赖的联网、汇总、数字化，彻底改变人们的生活方式，给人类生活带来更多的便利，艾瑞币链的应用范围将逐步拓展到人们生活的每个场景。

### 3.2 艾瑞币链项目的投资价值

1) 创新模式：艾瑞币链项目拟研发拥有自主知识产权的 *MOP* 信标芯片，可望实现应用与区块链的完美结合。研发的芯片将绑定 *Agilereservecoincoin*，创造基于艾瑞币链的应用应用智能生态圈，践行区块链技术向应用的拓展，*ARC* 必将成为时代变革的领导者；

2) 市场空间：万亿级别的市场，艾瑞币链已经具备可以迅速落地的应用方案，适用于综合应用行业的技术、平台、应用、*app* 等全流通领域。团队成员在服装行业及电子行业多年的从业经验及积累的客户资源，将为项目的落地提供极为便利的条件。后续还可望应用于电子车牌、资产管理等众多领域；

3) 高频应用：艾瑞币链搭载在 *MOP* 硬件系统上，解决区块链商业应用的瓶颈，也即链下的实体资产如何快速高效安全上链的问题。因此，艾瑞币链属于低门槛、高频率运用的商业生态链，会有广泛的应用群体和非常高的知名度；

4) 生态网络: 艾瑞币链要建立自己内容的应用生态链, *Agilereservecoincoin* 作为这一生态网络的母链唯一代币, 将在广泛的商业领域中流通, 具有极高的价值存储、价值流转、积分交易、商品支付媒介等功能, 随着 *MOP* 信标的不断普及和网络需求的不断扩大, *Agilereservecoincoin* 的需求也在不断提升, 因此, *Agilereservecoincoin* 的早期投资者必将随着艾瑞币链的发展壮大, 获得丰厚的回报。

5) 获利机制: *ICO* 发行的 *Agilereservecoincoin* 是艾瑞币母链代币, 随着母链及各子链的发展壮大, 艾瑞币链系统协议机制决定, 作为母链代币的 *Agilereservecoincoin* 将从各个层面获得发展红利, 并反哺艾瑞币区块链系统更加健壮和安全, 这是一个互恰的良性循环。

## 第四部分 项目基金会

本项目的基金会成立于 2017 年, 称为艾瑞币链基金会。基金会致力于 *ARC* 项目的开发以及 *MOP* 应用推广的落地工作, 并促进早期去中心化应用的开

发, *ARC* 初始总量的 20% 会被用于部分行业应用和初创项目, 例如金融服务、供应链、应用、区块链等, 包括项目战略规划、项目扶持、项目推广和代币置换。基金会会挑选在艾瑞币链上开发的去中心化应用, 并基于应用上的实际用户数量提供奖励。

基金会的总体架构, 决策委员会下辖技术开发委员会、财务及人事管理委员会、项目运营委员会三个子部门, 分别负责技术开发战略的制定和实施监管; 财务制度的制定和执行监管; 项目总体运营及市场推广的决策及执行等事务。决策委员会成员四年一换届, 成员一般由各个子委员会推荐两名代表, 加上项目投资方代表、社区代表、艾瑞币链团队成员代表各一名产生。各子委员会成员四年一换届, 成员一般由具备相关行业杰出能力的人士担任。

### 艾瑞币链基金会的总体架构

基金会提倡透明高效的运营理念, 促进艾瑞币链生态体系健康发展。治理结构主要以项目管理的有效性、可持续性和资金安全性为主着眼点。基金会的使命就是推进区块链技术由互联网向应用贯通, 将把 *ICO* 募集的资金投向以下几个方向:

1) 拟研发带自主知识产权的 *MOP* 信标芯片, 芯片采用自主知识产权的非对称加密算法, 可实现应用与区块链的完美结合;

2) 通过 *ARC* 灵活而强大的 *Token* 创建和交易功能，实现智能积分系统，集合支付、赠送、同币交易、跨币交易的完备功能；

3) 通过优化的区块链数据结构设计，实现商品信息、服务、入库盘点、出库、*app*、上架盘点、应用、客户购买、客户评价、客户服务完整信息上链，实现客户、商家、*ARC* 三赢策略；

4) 凭借匹配多场景的区块链数据结构，打造安全可靠的点对点应用信息通道，为应用公司提供业务自动化管理的信息平台，从机制上避免丢单、误单、错单的应用痛点问题；

5) 将应用到产品技术互联网，实现智能包装和产品可溯源定制。

以上项目展开将为用户提供便捷的数据查询追溯、分析处理、管理交易接口，为商家提供智能化管理接口，结合机器学习、人工智能的深度应用，最终实现技术、应用、*app*、应用和服务的全供销链条的智能生态圈。

## 第五部分 团队简介

### 5.1 发起人

*ROGER LIM*（意大利联合发起人）：意大利籍，非鹰科技创始人&*CEO* 中国最早期的区块链参与者之一

*Ismail Malik*（英国联合发起人）：*ICO CROWD & BlockchainLab CEO*  
欧洲最顶尖的区块链及数字货币专家

*Tsukikawa Yuu*（日本联合发起人）：日本区块链发展推动者  
早期比特币投资人

*Walter Komarek*（欧洲联合发起人）：马耳他最大的通讯公司 *Forbesfone*  
的 *CEO*、主席和管理合伙人

## 5.2 高级顾问

金锡基(应用)：韩国籍，韩国电子行业的领军人物，工学博士（毕业于美国明尼苏达大学），韩国高丽大学教授，曾任职于贝尔实验室、美国霍尼韦尔公司，担任过韩国三星电子公司副总裁，集成电路设计领域的资深专家，*IEEE* 高级会员，韩国电气工程师学会副会长，韩国半导体科学家及工程师协会主席。发表学术论文 **250** 多篇，拥有发明专利 **60** 余项。

朱延平（区块链）：中国台湾籍，工学博士（毕业于台湾成功大学），台湾云端服务协会理事长，中兴大学资讯管理系主任。曾获得台湾教育部青年发明奖，台湾十大资讯人才奖。多年来对区块链的应用有着深入的研究，带领区块链技术团队开发系统应用于健康大数据和农业溯源项目。

## 5.3 首席专家

莫冰（应用）：中国籍，工学博士（毕业于哈尔滨工业大学），韩国高丽大学研究教授，中山大学特聘研究员，应用专家，集成电路专家，中国微米纳米技术学会高级会员，*IEEE* 会员。发表论文 **20** 多篇，申请发明专利 **18** 项。

40

**2013** 年开始接触比特币，比特时代、韩国 *korbit* 最早的用户之一。**2013** 年作为韩国高丽大学的技术负责人，与三星集团合作完成“基于对等网络的多传感器数据交互及融合”项目。致力于将区块链技术与应用相结合，打造可真正商业化应用的公共链。

魏松杰（区块链）：中国籍，工学博士（毕业于美国特拉华大学），南京理工大学副教授，网络空间安全工程研究院核心成员，硕士生导师。区块链技术专家，研究领域为计算机网络协议与应用、网络与信息安全，发表论文 **20** 多篇，申请发明专利 **7** 项。在美国期间，曾经就职于谷歌、高通、彭博社等多家高科技公司，担任研发工程师和技术专家职务，具有丰富的计算机系统设计、产品开发和工程项目管理经验。

## 5.4 团队成员

李海东：毕业于 *KOREATECH*(韩国理工大学)机械工程专业，风险投资专业博士，韩国成均科技股份有限公司理事，三星 *SDI* 下属加热元器件制造商 *NHTECH* 中国

部经理，在韩博士生联谊会经济组组长，韩国 *korbit* 最早的用户之一，数字货币资深玩家。

刘辉于：工商企管专业，美国阿姆斯特壮大学 *BBA* 学位，天宇国际集团有限公司总裁，中国制衣辅料行业领军人物，中国知名教导型企业家，2008 年 *CCTV2* 频道《赢在中国》创业栏目参与者，2013 年开始接触比特币，对数字货币和去中心化的管理思想有强烈兴趣和深入研究，在市场调研、渠道建设、商务合作、商业模式方面有丰富的实战经验。

肖途：厦门大学 *MBA*。十余年电子产品及系统开发工作经验。历任诺基亚研发经理，产品经理，微软硬件部门供应链总监。2015 年创办厦门致联科技有限公司，开发的智能化系统和方案在各工业品牌企业、品牌综合应用企业成功推广应用。

41

*Dr Frank Wang*: 国家 *CSC* 专项留学人员，美国高丽大学工学博士、融合化工系统研究所研究教授，美国成均科技股份有限公司 *CEO*，美国工业协会会员，其研究成果曾发表在世界顶级期刊《自然·通讯》上并参

与编写应用工程专业系列教材《应用导论》。目前的研究方向涵盖区块链技术与智能医疗技术相结合的交叉学科。

赵海明：成均馆大学化工导电高分子专业博士，韩国 *BK21th* 导电高分子项目核心成员，韩国京畿道传感器研究所研究员，韩国 *NCTECH* 环保科技有限公司研究员，中华总商会副会长，韩国成均科技股份有限公司理事，数字货币早期玩家。

刘才：工学硕士，具有十二年超大规模集成电路设计与验证经验，对 *MOP* 芯片设计全流程、*SOC* 芯片架构、数模混合电路设计等具有丰富的实际项目经验，包括算法设计，*RTL* 设计，仿真验证，*FPGA* 原型验证，*DC* 综合，后端 *PR*，封装测试等。曾带领团队完成多款导航定位基带芯片，以及通信基带芯片的开发，完成过 *AES*、*DES* 等加密模块设计，曾获得卫星导航定位协会科技进步一等奖。精通区块链底层共识机制的原理和相关非对称加密算法。

杨锋：工学硕士，曾工作于中兴通讯，人工智能专家，集成电路专家。十二年超大规模集成电路研发、架构设计、验证经验；五年人工智能，遗传算法



方面研究经验。曾获得深圳市科技创新奖；对 *MOP* 技术、区块链底层架构、智能合约、各类共识机制算法原理和实现有深入的研究。

郭建平：工学博士（毕业于香港中文大学），中山大学“百人计划”副教授、硕士生导师、*IEEE* 高级会员。集成电路领域专家，在 *IC* 设计领域已发表 40 多篇国际期刊/会议论文，申请中国发明专利 16 项。

黄锐敏：工学博士（毕业于德国弗莱堡大学），硕士生导师，华侨大学电子系讲师，集成电路领域专家，主要研究数字信号处理的电路和系统实现，长期致力于数字信号处理技术方面的研发。

42

郭荣新：工程硕士，华侨大学通信技术研究中心副主任。十多年嵌入式系统的软硬件设计开发经验，长期致力于应用领域的 *MOP* 和区块链技术的研发。

李帅：工学硕士，研究方向为网络安全、区块链接入认证技术。主持完成的区块链分布式认证作品荣获“2016 年全国密码学技术竞赛”决赛一等奖。

黄鸿泰：工学学士，五年 *WEB* 前后端开发经验，长期致力于应用平台和教育信息化平台的开发，2011 年开始接触比特币，早期显卡挖矿参与者。对虚拟货币及区块链技术有浓厚的兴趣。

戴闽华：工商企管专业，美国阿姆斯特壮大学 *BBA* 学位，资深财务专家，曾担任天宇国际集团有限公司副总裁、财务总监，13 年财务工作经验，对制定并实施企业战略、经营计划等政策方略，实现企业的经营管理目标及发展目标具有非常丰富的实际经验。

刘东欣：中欧国际工商学院 *MBA*，美国西北大学凯洛格（*Kellogg*）商学院访问学者，战略管理咨询专家，投融资专家。目前的研究兴趣在于区块链技术对金融领域的影响和改革。

## 5.5 天使投资人

宋国平：医学博士，韩国中华总商会会长，北京海外联谊会理事，平安国

际株式会社代表，东方徐福抗衰老中心代表，塑美美容整形株式会社代表。

薛蛮子：著名天使投资人，UT 斯达康创始人。拥

有 40 年的资本市场投资经验，经历多次波澜壮阔的市场变幻，留下多个经典案

例，其中包括中芯国际、招商证券、丹霞生物等。丹霞生物被投中评为 2016 年投资十大成功案例之一。

严小铅：卡尔丹顿服饰股份有限公司董事长，深圳市汕尾商会常务副会长。

林敬伟：广州久赢投资管理有限公司董事，创始合伙人，中山大学高级财务会计研究生班，EMBA 毕业；二十七年大型央企海内外工作经历，超过十五年大型央企上市公司董秘、财务总监、副总经理经历，长期主管企业上市、资本运作、投融资及财务管理工作，具有丰富的资本运作及财务管理经验。具有董事会秘书、上市公司独立董事资格。

何红连：华尔顿投资事业部总监、注册会计师，厦大 MBA 毕业。曾任美亚柏科投资中心部经理，目前带领华尔顿投资团队在应用和集成电路等领域进行调研，投资布局。

## 5.6 顾问团队

李钟吉：株式会社 BSM 代表理事，韩国碳素融合委员会，活性炭委员会委员长。

高尚台：韩国电子新闻社编辑局副局长，KInews 新媒体与新产业局局长。

刘晓为：哈尔滨工业大学教授，博导，973 首席专家。总装微纳米技术专家组成员；总装军用电子元器件型谱系列专家组成员；电子学会敏感技术分会力敏专业委员会副主任；东北微机电系统（MEMS）技术联合体副秘书长；《传感器技术》编委；黑龙江省政协委员。

苏岩：南京理工大学教授，博导，中国造船工程学会船舶仪器仪表学术委员会副主任委员，中国仪器仪表学会船舶仪器仪表分会副理事长，中国仪器仪表学会微纳器件与系统技术分会常务理事，江苏省仪器仪表学会常务理事，总装专家。

张岩：工学博士，教授，博导。现任哈尔滨工业大学（深圳）电子学院副

院长，数字集成电路设计及嵌入式系统领域专家。

马萍萍：厦门大学经济学硕士，七匹狼创投总经理。

彭先德：资深律师，广东文品律师事务所合伙人，二十余年司法实践经验，公司法、投融资法律事务专家。

傅克：毕业于河南财经政法大学，广东瑞霆律师事务所资深律师，中国注经验。

肖光坚：高级会计师，税务师，高级经济师，深圳市三明商会秘书长，深圳联杰会计师事务所合伙人，十余年上市公司财务顾问，资深财务专家。

ARC 代币总计 10 亿枚代币 ( *Agilereservecoin*coin<ARC> ) 。

发行额度：5 亿 剩余 5 亿挖矿产出

私募 41%=2.05 亿枚

第一期：1 亿枚 1BTC= 200000 1ETH=18000

第二期：1 亿枚 1BTC= 150000 1ETH=14000

公募 9%=4500 万枚

公募：4500 万枚 1BTC= 120000 1ETH=11000

企业投资人 23%=1.115 亿枚

开发团队 5%=2500 万枚

技术发展 12%=6000 万枚

实地推广 10%=5000 万枚

、

其中的分配计划如下：

比例	分配方案	明细
41%	<u>Agilereservecoin</u> (ARC) 私募售卖	<u>Agilereservecoin</u> (ARC) 私募售卖获得的收入将会用于 ARC 基金会的运营，包括开发、市场、财务和法律咨询等。
9%	公募投资人	公募投资人是在行业内外有很大影响力的大咖，不管是从技术还是商业拓展上都会对 ARC 项目有很大的指导和帮助。
23%	企业投资人	企业投资人指在 ARC 构建的分布式商业生态系统中的企业及为这些企业客户或者最终用户服务的服务提供商；这些企业投资人会把未来 <u>Agilereservecoin</u> (ARC) 在其商业活动中的使用作为重点开拓目标。
5%	创始团队、开发团队	创始团队、以及开发团队在 ARC 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 <u>Agilereservecoin</u> (ARC) 作为回报。
12%	持续经营及技术发展	维持 ARC 团队之后的持续经营和发展
10%	商业落地推广	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，用于唯链技术的行业应用，真正实现商业落地。

- 数字资产投资。持续经营过程中，ARC 基金会将分配大约 5%到 10%的资金/或数字资产，对区块链行业进行投资，例如对初创企业的孵化、天使投资以及对新兴科研技术的投入等。

在建立生态的过程中，ARC 基金会将作为 ARC 底层架构的提供者，收到一定部分的数字资产或资金。例如社区参与者、企业等为购买 ARC 使用的 Agilereservecoin (ARC) 等，以及基金会作为技术倡导者，提供技术分享和授权使用获得

## 资金使用预算

如前述，ARC 基金会对资金的使用主要包括日常运营、技术开发、商业拓展以及再投资等。主要的分类如下表所示：

使用分类	比例	明细内容
技术开发	50%	主要包括对初始团队的奖励、招募专家及开发人员、技术专利及知识产权保护等一系列活动
商业开发	35%	ARC 商业拓展与培训、技术交流与分享、定期刊物发表、联盟创建或参与等
再投资	10%	对区块链新技术和新团队的投资或吸纳等
日常运营	5%	基金会日常后勤管理、交通及办公、财务及报告的需求等。

## 天使投资人

阎焱	<p>软银赛富投资基金首席合伙人，软银亚洲信息基础投资基金总裁。软银亚洲信息基础投资基金曾给投资人带来 97% 的年回报率，是 2001 年以来全世界投资回报最高的基金之一。2009 年 12 月 15 日，《福布斯》中文版杂志“2009 福布斯中国最佳创业投资人”榜单，阎焱居首。</p> <p>分布式资本管理合伙人；BTS 创始人之一</p>
沈波	<p>以太坊和瑞波的早期有力推动者和投资人，参与投资和帮助推动了全球三十多个区块链项目，传统金融的资深人士，在证券、对冲基金和投资银行等行业拥有超过 12 年的丰富经验。</p> <p>Qtum 发起人</p>
帅初	<p>毕业于 Draper University(英雄学院)和中国科学院，之前就职于阿里巴巴集团，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。</p> <p>UT 斯达康创始人，中国社会科学院及美国加州大学伯克利分校硕士</p>
薛蛮子	<p>华尔街知名华人投资家、著名天使投资人</p> <p>他投资过的项目有 PCPOP、汽车之家、雪球财经等。曾担任美国纳斯达克上市公司 UTSTARCOM 的副主席、亚洲最大的光纤光缆公司 Asia Pacific Wire and Cable Company 及 8848 (www.8848.com)、美商网 (www.MeetChina.com)、中华学习网 (www.ChinaEdu.net) 等国际知名企业董事长。</p> <p>著名财经双语主播，艾问传媒创始人，赛富亚洲基金投资合伙人</p>
艾诚	<p>曾任中央电视台驻纽约财经评论员、世界银行国际金融总公司投资顾问；哈佛大学肯尼迪政治学院公共政策硕士、北京大学国际传播系硕士；获选《福布斯》杂志“30 位 30 岁以下亚洲人物” (Forbes 30 Under 30 Asia) 和世界经济论坛全球杰出青年。</p> <p>清华大学 i-Center 导师，清华大学博士研究生</p>
韩锋	<p>万向区块链实验室丛书主编，DACA 区块链协会秘书长，亦来云联合创始人</p> <p>韩锋老师主编了国内首本区块链书籍《区块链新经济蓝图及导读》，合编了《区块链：从数字货币到信用社会》一书。曾多次给中国银联，IBM（中国），思科以及融通基金、鹏华基金、景顺长城基金、深圳证券通信、中国证券登记结算等金融相关机构，全国各高校讲授区块链与未来应用等专题。</p>
马治国	<p>西安交通大学法学院博士生导师，陕西哲学社会科学重点研究基地——知识产权研究中心主任，前法学院副院长、律师、仲裁员、知识产权司法鉴定人。</p> <p>Bytom 比原链联合创始人，巴比特执行总裁。曾任朗讯贝尔实验室资深工程师，全球最大的比特币交易所 OKCoin（币行）副总裁。成功领导过 OKCoin、OKLink</p>
段新星	<p>等多款区块链产品的研发及运营工作。著作有《区块链：重塑经济与世界》《区块链开发与实例》，2017 年 5 月加入巴比特，任执行总裁。</p> <p>万达网络科技集团先进技术研究中心总经理</p>
季宙栋	<p>国内资深区块链专家、数字资产研究者 担任工信部区块链产业发展论坛副秘书长，先后参与工信部白皮书编写和有关标准发布，撰写有《区块链开发指南》等专业书籍。</p>

David Park	ICOGuide 联合创始人, Cointrade 首席营销官, 负责 ICOGuide 推广营销和区块链技术研究。在北美深造多年并获得伊利诺伊大学厄巴纳香槟分校广告学学位。
	David 是数字货币早期参与者, 精通线上线下推广营销, 将营销推广与数字货币产业完美融合。
Alex Kotenko	欧洲金融科技独角兽 BlockEx CTO 欧洲最权威的区块链专家之一, 比特币支付系统 XBTerminal Ltd 创始人。
Sergei Chmel	ICOSHARK 对冲基金管理合伙人, Le Genepi Cosmetics 创始人, 私募基金投资
Bruce Elliot	顾问, Virtown.ru 联合创始人和首席执行官。 Boston Multi Family Office 主管, Cube Limited 战略主管, Microgaming Systems 营销和商务拓展总经理。
Cameron Chell	连续创业者, Business Instincts 集团联合创始人和首席执行官。Slyce Draganfly Innovations, Raptor Rig, ColdBore Technologies, UrtheCast, ASP Industry Consortium, Engyro 和 FutureLink 联合创始人。
Stefano Schiavi	SCAL 首席投资顾问, Brilliant Already 首席技术官, Dev Bootcamp 软件开发工程师, Violet Jade Holdings 期权交易员。在博洛尼亚大学学习法律, 擅长算法设计与分析

所有版权: [www.agiLereservecoin.com](http://www.agiLereservecoin.com) ARC

