



ZZM白皮书V4.0

ZZM White Paper

目录

一、项目基本信息	3
1.1 项目概述、目标	3
1.11 项目背景	3
1.12 行业痛点	5
二、设计理念	8
2.1 ZZM 设计理念	8
2.2 应用场景	9
2.21 内容发行	9
2.22 周边商品交易	11
2.23 线上线下活动	12
三、项目商业价值体系	12
3.1 内生价值产生与使用	12
3.2 商业增值逻辑	13
四、项目方案	14
4.1 项目创新性与落地可能性	14
4.2 项目设计原则	15
4.3 项目创新性	16
4.4 特性	17
4.5 架构及组件设计	18
4.6 部分组件说明	20
五、Token 介绍和使用计划	27

六、项目治理机制	28
6.1 资金管理机制	28
6.2 基金会治理	29
七、团队介绍	29
7.1 核心团队介绍	30
7.2 合作伙伴介绍:	30
八、落地项目介绍与未来规划	32
8.1 已落地和将落地的项目	32
8.2 未来规划	32
九、风险与管控	34
法律结构与免责声明	34
风险披露	35

一、项目基本信息

1.1 项目概述、目标

1.1.1 项目背景

文化产业是指：文化产品生产和提供文化服务的经营性行业。文化娱乐产业是文化产业的重要组成部分，主要包括数字音乐、数字图书、数字视频、数字游戏等，在满足人民群众精神文化需求，扩大和引导文化消费，带动就业，促进经济发展等方面具有重要作用。

文化娱乐产业作为提升国家“软实力”的重要途径，受到了各个国家的高度重视。我国在《十三五规划建议》中指出，到 2020 年要让“文化产业成为国民经济支柱性产业”。2016 年，我国文化娱乐小众市场百家争鸣，电影、电视剧等细分市场的增速更是超过 30%。此外，科技发展引发渠道创新，消费升级为文化娱乐产业带来了重大投资机会。文化娱乐产业总体规模包含核心层、关联层、拓展层的细分市场，其中，核心层市场规模 2015 年约为 4500 亿元，年均复合增速在 25% 左右，预计 2020 年总体规模将达万亿级别。德勤在文化娱乐产业系列报告指出，在国家推出政策支持，互联网改进传统行业，和大量内外资本投入等利好情况下，中国文化产业正处于前所未有的“黄金时代”。在电影方面，中国已在全球票房增长速度中领先，并且预测在 2020 年将成为全球第一大市场。

前瞻产业研究院《文化娱乐产业投资前景与发展趋势分析报告》显示，

2013-2016 年国内文化娱乐产业投资一直保持向上增长态势，2016 年文化娱乐投资事件达到 668 件，并购规模和速度继续维持高热度。中投顾问产业研究中心梳理出产业中十大热点：电影、IP 经济、秀场娱乐、动漫、网络剧、音乐、网络文学，并对其市场规模进行了分析预测，见下图。

行业	市场规模
文化娱乐	文化娱乐产业总体规模包括核心层、关联层、拓展层的细分市场。其中核心层市场规模 2015 年约为 4500 亿元，年均复合增速在 25% 左右，预计 2020 年总体规模将达万亿级别
电影	2015 年中国电影产业规模首次达到 1000 亿元，同比增长 46%。预计 2020 年达到 1800 亿元
IP 经济	保守估计，未来三年内 IP 原生市场超过 150 亿，IP 衍生市场有望超过 2000 亿元
秀场娱乐	2016 年秀场娱乐市场规模高达 100 亿元，未来讲义 20%-30% 的速度增长，到 2020 将接近 250 亿
动漫	截止 2015 年底，动漫产业总产值已突破 1200 亿元，预计 2020 年将有望达到 4400 亿元
网络剧	网络剧已经爆发，2018 年市场空间可达 650 亿元
音乐	2015 年音乐产业市场规模约 2900 亿元，未来五年复合增速在 3% 左右，2020 年市场规模达 3300 亿
网络文学	2015 年网络文学市场规模达 70 亿，未来五年年复合率或达 20%，到 2020 年市场规模有望达 170 亿

“泛娱乐”是指文化内部各领域以及文化和其他领域之间的融合，特别是

基于互联网与移动互联网的多领域共生，打造明星 IP 的粉丝经济。随着近年来文化产业的快速发展，“泛娱乐”已经成为文化领域最受关注的商业模式。据前瞻数据库数据显示，2016 年中国“泛娱乐”产业总产值约为 4155 亿元，2017 年预计达到 4800 亿元。

2017 年全国居民在教育文化娱乐领域支出环比增长 12%，是居民消费各环节中增速最快的。随着文学、动漫、影视、游戏为核心的泛娱乐 IP，被互联网原住民的 80 后、90 后甚至更年轻的 95 后人群消费和传播，再加上国家政策的支持，加速了“泛娱乐”在社会中积极正面的舆论导向，群众对泛娱乐的消费已成为社会文化常态。



1.12 行业痛点

尽管文化娱乐产业目前处于“黄金时代”，但是其产业组织结构和产业要素存在着诸多不足，目前文化娱乐产业模式下版权侵犯、数据篡改、资源严重倾斜等问题制约着文化产业的发展。

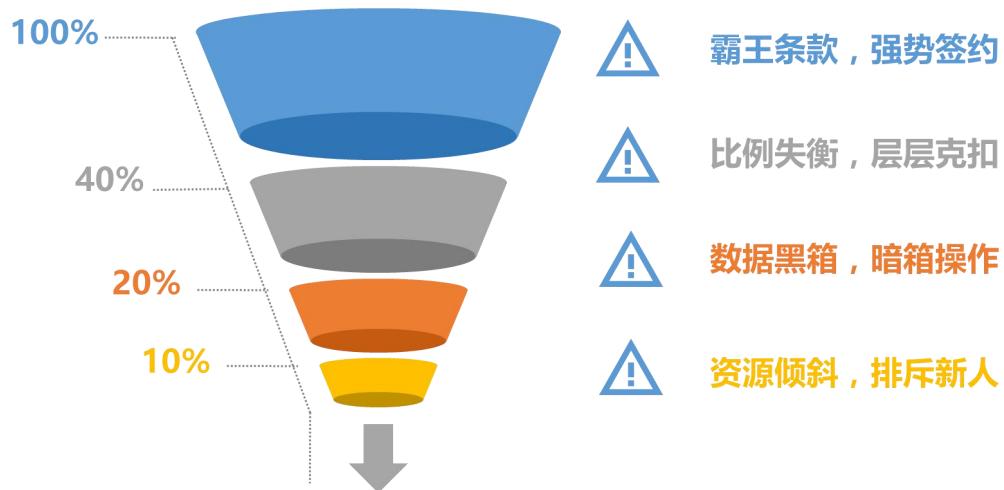
(1) 侵权问题积重难返

2014 年查处的广东省 “DJ020 网”，向公众提供未经授权的音乐作品达 62286 首；北京天盈九州网络技术有限公司未经权利人许可，通过其运营的凤凰网以及苹果智能移动客户端软件 “军事秘录合集” 和 “凤凰开卷” 传播，侵犯文字作品著作权；“人人影视网” 未经著作权人授权，组织他人将包括《地心引力》在内的 467 部影视作品的对白上传至网站，供用户浏览、下载和使用。侵犯著作权。网络音乐人的原创歌曲被各大音乐网站收录，用户随意下载，部分网站甚至用各种盈利方式利用原创歌曲盈利，但音乐人却完全不知情。这类侵权案例多如牛毛，但是由于互联网技术本身易复制、难追溯的特征和我国国民版权意识较弱，侵权问题屡见不鲜，难以根除。音乐、电影、电视剧、网络小说等内容产生者辛辛苦苦创作的作品，一旦上传到网上，几乎不可避免的会被他人盗用或免费使用。文化娱乐的起点是创意、核心是内容，版权问题极大损害了创作者的权益，抑制了创作者创作的动力，严重制约着文化娱乐产业的发展。

(2) 中心化平台难言公正

网络作者为了将自己的作品上架销售，不得不借助阅读平台，与之签约。但是作者作为弱势群体，没有谈判话语权，往往不得与之签下霸王条款，例如后续作品必须优先在该平台发布、作品版权归于平台等。网络音乐会人将原创音乐放在平台上销售，但是销售数据不透明、推荐规则不透明，网络音乐人的收入完全依靠中心化的平台提供的数据。除此之外，平台与内容提供方的分成比例也去缺乏公允。传统唱片艺人是没有分成的，词曲作者每首歌的版税才 0.8 元，数字音乐的分成，一般唱片公司和音乐平台七三分（大牌歌手分成会

更高), 然后词曲作者和艺人再从唱片公司里抽成固定比例, 词曲作者抽成 16%, 艺人抽成 15-30%, 汗水与回报完全不成正比! 大公司对行业的垂直垄断令许多底层创意者和创作者无法得到展示才华的机会, 高度中心化的管理方法和机制导致平台方对成熟 IP、有名的创作者格外倾斜, 抑制了新 IP、新人才的成长, 还存在着侵吞创作者费用等违规操作。



(3) 原创者回报周期长

文化产业的创意者和内容创作者, 是需要付出大量的经历和时间的, 但他们却无法得到相应的报酬。例如, 一个有潜力的 IP 需要进行开发和 IP 共同成长, 形成一套特有的 IP 运营模式, 前端严格选品, 伴随 IP 一同成长, 运用产品/品牌思维定义内容, 用最短时间多渠道立体化的放大 IP, 最后帮助 IP 多渠道变现。IP 孵化、音乐创造、小说写作等均需要一定的周期, 在这个周期内往往创作者无法得到报酬, 导致文化娱乐产业的创作者的“收入真空期”特别长。这种根据结果给予报酬的方式, 大大提高了创作门槛, 一旦 IP 孵化失败或者作品不受市场欢迎, 这意味着一段时间的努力几乎白费。

二、设计理念

2.1 ZZM 设计理念

ZZM 团队利用自身行业经验和区块链技术，与诸多大型企业达成战略合作，致力于将区块链技术应用于文化娱乐产业，打造一个全球性文化娱乐数字平台，旨在解决目前文化娱乐业痛点，扶持新生代文化内容创造者，改变文化娱乐产业的组织结构，重构泛娱乐时代文化娱乐产业网络和运营模式。

ZZM 生态圈遵循区块链去中心化、公开透明、人人平等、人人参与的原则。利用区块链去中心化特征，保证平台上业务去中心化、透明执行，避免中心化管理的暗箱操作和霸王条款；利用区块链数字加密技术和可追溯特征，保证网络作者、原创音乐人、IP 孵化团队的版权不会被侵犯，利益不会受损；利用 ZZM 高流通性，避免了内容创作者的“收入真空期”。基于区块链进行实时的清算、结算和交割，费用实时到账，不会经过中间平台，安全可靠，并且手续费极低，节约资源，实现高效率低成本地完成一系列功能，这让 ZZM 在未来有了极大的发展空间。未来，在 ZZM 平台上，可以发起文化娱乐活动、影视作品、文学作品的众筹；购买 IP 周边商品和圈内的生态商品；发起粉丝线下活动，增强粉丝经济；打赏喜欢的明星、大咖、作品等；安全地、去中心化地存储身份、文字、影视作品等。

文化娱乐的起点是创意、核心是内容，利用区块链技术，能将文化娱乐价值链的各个环节进行有效整合、加速流通，缩短价值创造周期；可实现数字内容的价值转移，并保证转移过程中的可信、可审计和透明；基于区块链的政策监管、行业自律和民间个人等多层次的信任共识与激励机制，同时通过安全验

证节点、平行传播节点、交易市场节点、消费终端制造等基础设施建设，不断提升文化娱乐行业的存储与计算能力，助力文化娱乐跨入全社会的数字化生产传播时代。

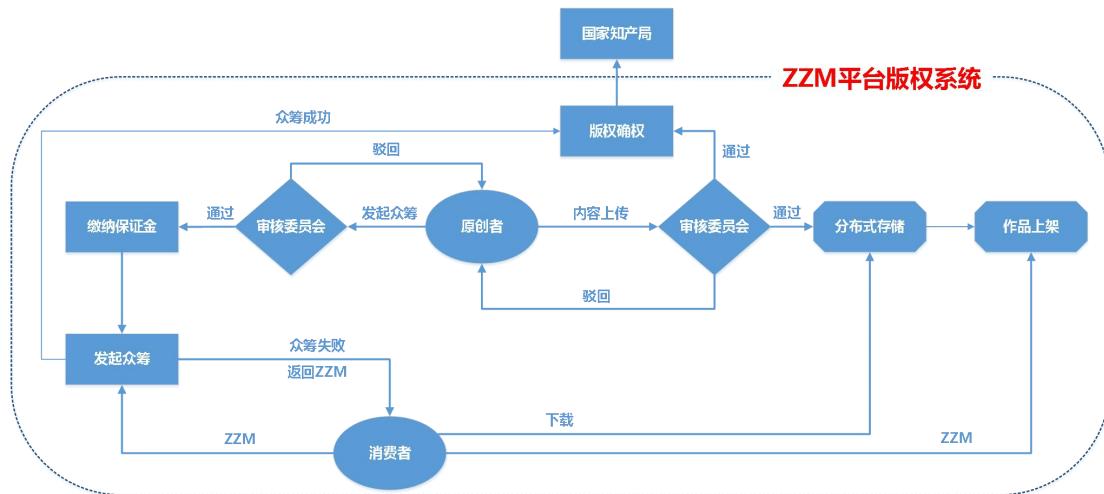


2.2 应用场景

ZZM 应用场景广泛且具有可行性，主要分为三大类：内容发行、商品交易、粉丝活动。

2.2.1 内容发行

在 ZZM 平台上，利用区块链特有的可信数据环境特性，所有的原创者，能够简单、快捷、低成本的完成原创声明、版权登记、和作品众筹，并且能将自己的创作内容上传到去中心化的存储系统，给原创者提供一站式的资产管理方案。



(1) 版权确权

ZZM 平台对于原创文化娱乐作品，IP 产权等提供版权确权的服务，通过去中心化的方式对版权加盖时间戳，数据是真实可靠的，能够保证版权的产生时间的真实性。未来，ZZM 确权信息会直接对接国家知识产权局，如果作者的作品被盗用，或者作品版权引起了争议，则可以直接通过区块中的时间戳来判定版权归属。

确权之后，创作者可以建立一个智能合约，设定时间、使用或下载所需的 ZZM 数量。一旦其他人使用或者下载原创内容，自动向创作者支付预先设定的 ZZM。充分利用了区块链加密技术和智能合约的特性，保护了创作者的权益。

(2) 去中心化存储

ZZM 平台为原创者身份，创作的文字、影视作品等有价值的信息提供去中心化的存储服务，创新性地融合基于 IPFS 协议的去中心化的方案。

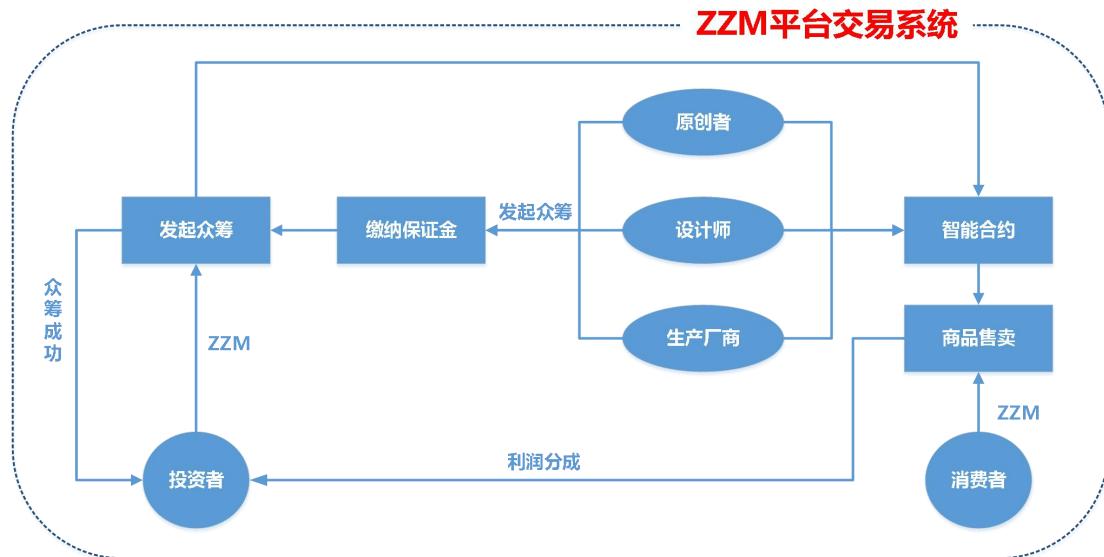
(3) 作品众筹

IP 孵化等项目具有时间长、前期投入成本高等特点。为了减少创作者的回报周期，降低其创作失败风险。ZZM 平台为原创者提供众筹服务，在歌曲创

作、小说创作以及 IP 孵化中，筹集一定量的 ZZM，提前出售作品的使用权，可以更加激励原创者毫无顾虑的进行创作，减少了作品不受欢迎的市场风险。

2.22 周边商品交易

由于文化作品的制作成本较高，制作方靠单一产品形态往往很难收回制作成本，故常借用泛娱乐领域成熟 IP 作为基础并向周边行业延伸。多数文化产业链围绕 IP，由核心——内容生产层作为上游，扩散——渠道发行层作为中游，周边——衍生产品层作为下游，依序构成。



原创者以自己的作品为 IP，与生产厂家和设计师合作，在 ZZM 平台上进行周边商品的销售。除此之外，由于周边商品前期生产所缺资金，亦可以通过平台众筹的方式来让用户参与，并将销售利润按一定比例回报给众筹者。由于所有的信息均上链，所有参与者、设计者、制造者和 IP 创造者均能够看到销售数额，通过编写智能合约来保证合同的及时生效，不需要担心毁约等问题。

2.23 线上线下活动

(1) 明星见面会

在 ZZM 平台上，粉丝可以通过 Token 支付方式购买自己喜爱的明星的见面或吃饭的机会，与其深入交谈。明星见面能够获得大量的 ZZM，可以将募集的 ZZMToken 用于生产周边商品。

(2) 明星时间购买

可以通过 ZZMToken，购买明星时间。例如，可以在 ZZM 平台上，找到女朋友喜欢的明星，给予其一定的 ZZMToken，让其录一段生日祝福视频送给女朋友。

(3) 小鲜肉众筹

明星能够发行专属彩色币，赠与支持自己的粉丝。粉丝即可以将其收藏，也可以在 ZZM 平台上兑换相应的明星周边商品。

(4) 粉丝打赏

用户可以用 Token 对喜欢的明星、大咖、影视作品、文学作品作者进行打赏，基于区块链进行实时的清算、结算和交割，费用实时到账，不会经过中间平台，安全可靠，并且手续费极低，节约人力资源，实现高效率低成本地完成一系列功能

三、项目商业价值体系

3.1 内生价值产生与使用

ZZMToken 是 ZZM 生态圈唯一的原生资产，总发行量 2 亿，永不增发。

ZZM 全部预挖，并放入“项目扩展”资产中进行冻结。

ZZM 的最小单位是 10^{-8} ，即小数点后八位小数，类似于比特币的设计。

ZZM 能够在 ZZM 生态圈内使用和交易，ZZM 并不是一种数字货币，准确来说，ZZM 是 ZZM 生态圈内的一般等价物和 ZZM 团队股权，持有 ZZM 能够按一定比例获得 ZZM 生态整体收益。ZZM 是由椭圆曲线数字签名算法（ECDSA）保障的数字资产，能够在 ZZM 生态圈内用于资产交易、众筹、发起活动等功能。

ZZM 的价格不会锚定任何法定货币或者加密货币。在 ZZM 生态圈内的交易、押金等均以 ZZM 进行支付。依靠 ZZM 才能使用生态内各种功能，包括但不限于用于链上转账、作品发布、版权确权等。除此之外，持有 ZZM 能对 ZZM 生态圈内部治理和重大技术发展演变（分叉、更新等）做出表决。ZZM 是 ZZM 生态圈系统内承担一般等价物和经济成本承担者，因此 ZZM 是 ZZM 生态圈内的必不可少的核心要素之一。

3.2 商业增值逻辑

ZZM 是第一个以区块链技术为基础的文化娱乐产业平台，未来的应用场景非常之多，且具备落地的现实条件。每增加一个应用场景，ZZM 团队会将该场景产生的利润回购 ZZM，然后把回购的 ZZM 应用于下一个场景，如下图所示。随着应用场景增多，ZZM 生态圈参与者会呈爆炸式增长。根据梅特卡夫定律，ZZM 网络的价值会呈指数增长，而 ZZM 数量为 2 亿个且恒定不变，因此 ZZM 会越来越有价值。



ZZM 对接一个项目时，会根据项目的规模，解冻“项目扩展”资产中的部分 ZZM 投放市场流通，当对接的项目成功运作并形成成熟的生态圈时，ZZM 团队回购一定比例 ZZM，并将其放入“项目扩展”资产中继续冻结，对接下一个项目时，继续重复该步骤。当对接项目不断落地，“项目扩展”中的资产将使用完毕，ZZM 将形成有数字内容发行、周边商品交易、线上线下活动发起的多维度闭环生态体系。生态体系越丰富，所需的 ZZMToken 流通量越多，根据货币需求数量论，ZZMToken 的价格也会随之水涨船高。

四、项目方案

4.1 项目创新性与落地可能性

- 利用区块链技术，解决当前文化娱乐产业痛点，重构文化娱乐产业链
- 多种区块链技术集成应用：多重签名技术，同态加密技术，IPFS 协议
- 数个大企业支持的落地项目

ZZM 团队是有着丰富的行业从业经验和行业资源优势，目前，ZZM 理念收到了众多企业的热捧，许多公司提前与 ZZM 达成战略合作。

- 陕西中资文化产业发展有限公司
- 一托（中国）集团控股有限公司
- VK—百男大秀全球时尚品牌
- 秒偶社交电商平台

4.2 项目设计原则

➤ **开源透明**

区块链底层技术和使用的加密方式将会采取开源模式，由社区进行维护管理。

➤ **面向行业**

zzm 将专注于文化、娱乐行业，根据场景的需要进行适配调整。

➤ **社区维护**

zzm 将会以社区的方式进行代码的提交和维护，初创团队作为治理委员会负责日常的管理运营。

➤ **安全高效**

zzm 将融入多种密码学机制，并且将密码学机制设置成可插拔的，并纳入防量子计算的机制，为日后海量的数据提供持续的安全保障。

➤ **监管审计**

提供 CA 权限节点，满足监管方监管审计要求，满足业务合规要求。

➤ **性能可靠**

通过多链结构、跨链协议、性能优化、配置参数调整及高效的应用设计，可以达到场景下多用户、多企业的参与要求。

➤ **多链架构**

底层架构均衡考虑了系统性能、安全、可靠性可扩展性，引入状态通道，实现不同联盟之间的数据安全隔离及权限访问控制，提供丰富的合约模版。

4.3 项目创新性

➤ 改进型的莱特币底层技术

以莱特币底层技术为基础进行开发，用脚本型语言 Python 进行实现，减少后期维护的成本，提高版本迭代效率

➤ 松耦合设计

zzm 针对的场景用户量和数据量庞大，不同用户和数据之间的交互逻辑复杂，为了减少不同层级组件交互的损失以及日后升级的必要，我们将整个系统进行松耦合设计。

➤ 快速交易

数据缓存加速服务，由 RAFT 中的选举算法选举出高速交易节点，交易结算几乎是实时的，从而提升了交易效率，大大提高了资产利用率。

➤ 简易的交易规则设计

通过面向用户的操作页面进行智能合约编辑，普通用户也能够在区块链中嵌入预设计好的交易规则，轻便化地使用智能合约。

➤ 通道设计

提升交易的隐私性，当场景中的企业用户需要交易匿名，zzm 会提供专门的通道，由随机选择的节点进行哈希索引的存证，在保证隐私性的同时满足安全的原则。

➤ 链外存储设计

面对海量数据进行中心化与去中心化想结合的存储方式，在保证信息不可篡改的同时保证数据处理的效率，提升用户体验。

➤ 便捷的私钥管理

传统的私钥管理会降低用户体验，引入主控交易和自控交易机制，普通用户可以使用账户和密码进行登录。

➤ 多链机制

zzm 针对 C 端用户使用了公有链技术，针对联盟企业使用了联盟链技术，不同种类的链之间通过跨链协议、公证人机制（Notary schemes）、哈希锁定（Hash-locking）、侧链等方式进行交互。

4.4 特性

- 商业级的平台性能和能力
- 高定制化的智能合约的执行能力
- 高度自我进化和完善能力
- 高度的安全性
- 母链+N 侧链多链结构
- 高效跨链通信体系
- 高运算效率，芯片级加速能力
- 操作系统级别的结构优化
- 产业联盟企业服务器群（Industry Alliance Enterprise Server Group, IAESG）

4.5 架构及组件设计



用户层

用户层是面向用户的入口，通过该入口，执行与客户相关的管理功能，维护和使用区块链服务，也可通过该层将区块链服务输出到其他资源层，提供对跨层区块链服务的支持。

服务层

服务层提供统一接入和节点管理等服务，为用户提供可靠高效的服务能力。

网络层

基于点对点组网机制、数据传播机制和数据验证机制等，与操作系统、网络、

存储、计算等资源共同建立基础设施云服务，并提供多节点的身份认证和管理。

在各个服务场景间形成链间通信网络，建立交互协议。

激励层

价值度衡量、钱包、账户等集成到 ZZM 体系中，建立一套激励机制，激励记账和诚信节点，并惩罚不遵守规则的节点，促进整个体系的健康发展。

核心层

核心层是区块链系统的核心功能层，包含了共识机制、同态加密、加密、摘要与数据签名等模块。此外，根据应用场景的不同，可以有选择地添加能自动执行预设逻辑的智能合约模块。

合约层

负责记账节点的排序服务，提供对合约脚本的解析功能，合约类型的管理，并且加入状态通道，负责智能合约的匿名可控，设置安全容器运行合约，保障合约的安全性。

基础层

负责基础的存储，运用 LevelDB 和文件系统长期保存区块链和系统整体状态的数据集，对节点账本进行维护，针对上层的哈希签名做硬件加速，并制定核准校验协议保护数据安全。性能调优及 IO 处理，从软硬件两方面来提高系统的并发。

4.6 部分组件说明

用户管理

负责所有区块链参与者的身份信息管理，包括维护公私钥生成、密钥存储管理以及用户真是身份和区块链地址对应关系维护等，并且在授权的情况下，监管和审计某些真实身份的交易情况。对数字资产等金融交易类的应用，还提供了风险控制的规则配置，以保证系统交易安全。

注册登记

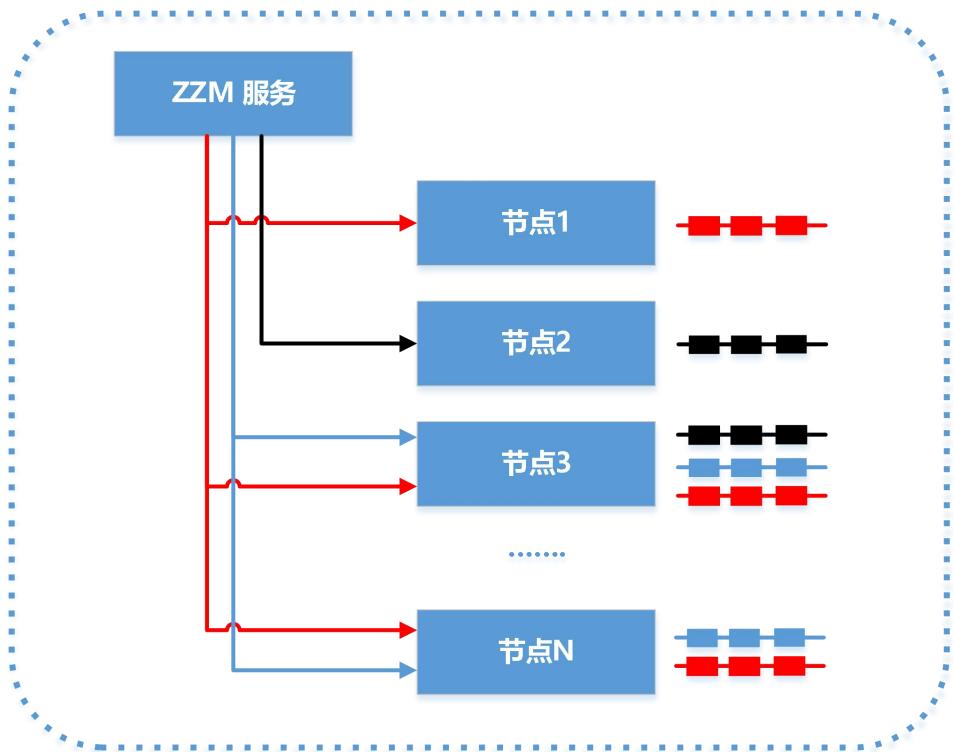
针对场景内的联盟链节点进行注册管理，登记企业的信息，提交企业的公钥的功能，完成证书登记，信息统一注册登记管理，满足治理委员会 KYC 和 AML 等要求。

授权审核

根据定制的授权要求，自动审核参与方提交的信息及公钥。审核完成后，按照证书生成规则，提取相应信息和公钥信息进行证书签发。授权审核设定有监管特殊权限的证书生成规则。

状态通道

平台服务的通道管理功能可根据业务场景构筑独立的业务链，它允许参与方以区块链节点的形式加入该业务链，共享业务链数据。区块链节点可通过通道管理功能加入多个业务链，且各个业务链的数据（链、业务）相互隔离。并支持多链结构，使不同业务相互隔离运行在同一平台，加强隐私保护，降低系统构筑的成本，提高设备利用率。



动态组网

zzm 平台可以通过链通道识别节点，在服务不暂停的前提下，可以允许动态调控网络节点加入或推出业务链。

智能合约

负责合约的注册执行升级以及注销。用户通过某种编程语言编写智能合约，智能合约会根据用户的逻辑自动或者由其他合约触发，实现自动化执行。

负载均衡

能够均衡应用程序的流量，将前端并发访问转发给后台多台云服务器，实现业务水平扩展，通过故障自动切换，及时地消除服务的单点故障，提升服务的可用性，并且让 ZZM 上的 DAPP 或场景应用能够拥有良好的用户体验。

服务组件

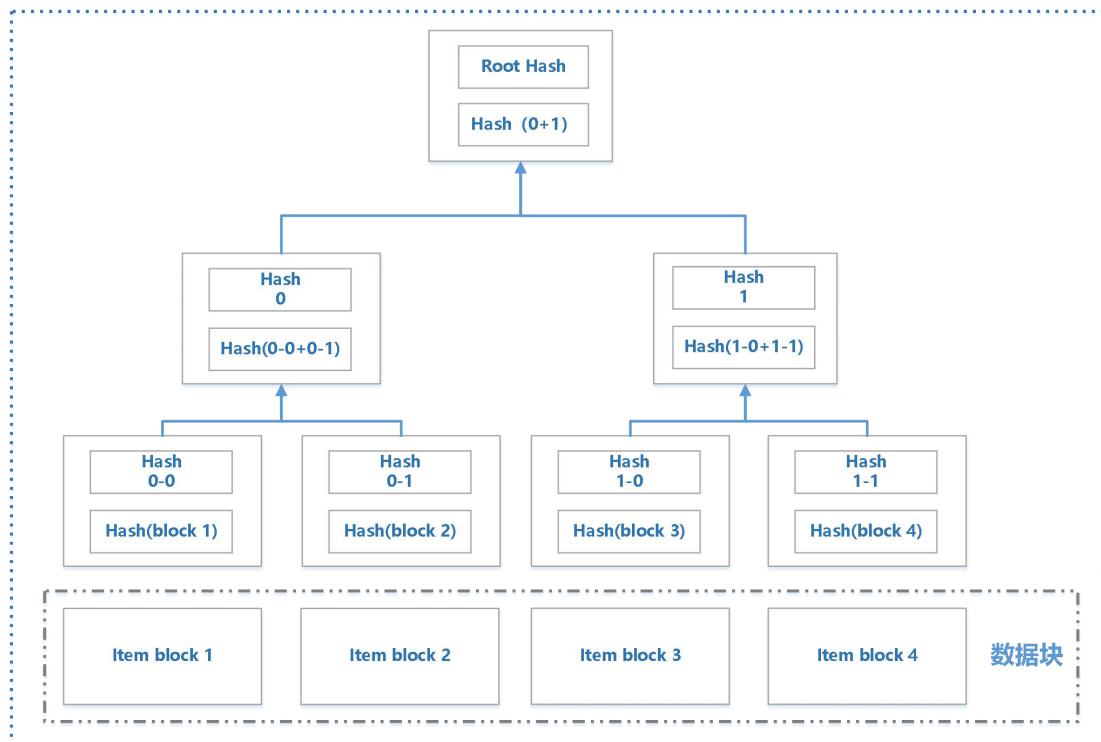
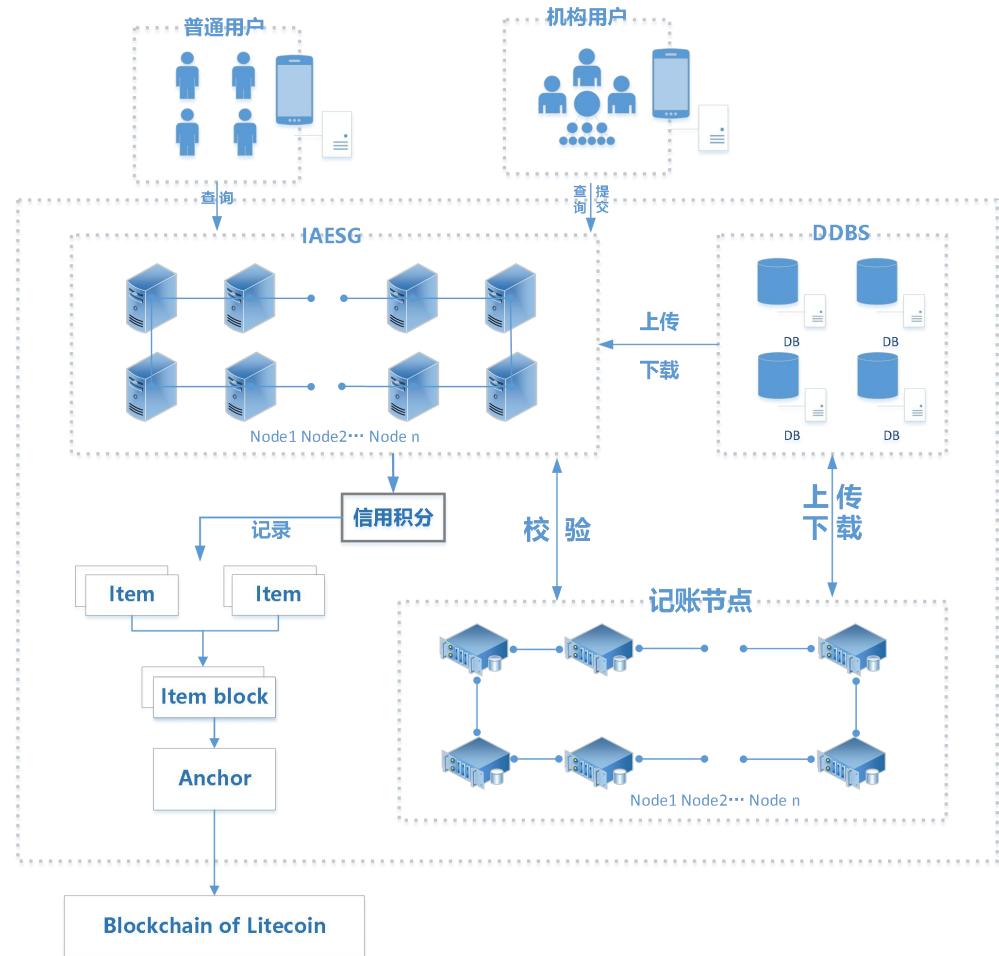
针对企业及个人开发者，均能够提供创建账户，资产数字化、获取区块的区块高度、创建与查询交易信息、链的实时通知等功能。现阶段可通过 SDK 实现

接入、信息隐私保护、价值传递、存证方面的 BaaS 服务，满足生态链上的不同应用平台的接入需求。

数据安全设计

经过对场景的调研与思考，我们发现，小规模的服务商、公司所产生的流量较小，产生的数据较小，另一方面传统的文娱场景的数据中心建设也不够完善，没有很强的数据处理能力，所以我们设计了两套联盟服务器集群，配合莱特币底层技术使用，并且加入跨链机制，可以有效地利用当前文娱场景下原有的数据库实现去中心化、安全、快捷可追溯的数据共享。此外，很多数据本身数据量比较庞大，比如图片、视频、影视作品等等，这类数据将使用所有者的公钥加密存储再分布式数据库中，为了保证记录内容可信、未篡改，模型记录所有的数据的摘要并采用分层机构存储。将数据哈希值存放在 Item 结构中，再计算出每个 Item 的哈希值存放在 Item 块结构中，这样做可以有效地减少搜索空间，加快用户对记录的校验速度。

如图所示，数据块由多个 Item 块构成，层层计算哈希值，会得到这一数据块的 Merkle 根，每 1 分钟进行一次。由于莱特币底层区块链结构采用 POW 机制，需要数分钟生成一个区块，所以在模型中每 10 分钟冻结数据库，由于 IAESG 中代表提交生成的 Merkle 根到莱特币区块链中，形式类似于提交一笔莱特币交易，这样可以实现真正意义上的不可篡改，因为公有链参与的节点更多，更开放，更具有公信力，每个 Item 块都存储 Item 的哈希值以及一个头部信息，这样不仅利于每个块再点对点网络的传播，也减少了数据校验的成本。每条数据包含三个信息：数据所有者公钥、元数据、数据摘要。



共识流程

下面是 IAESG 的具体工作流程：

步骤 1：用户提交请求，并提交公钥作为标识

步骤 2：某代表节点接受请求

步骤 3：某代表节点广播已接受请求

步骤 4：用户提交记录，如果不希望公开数据，使用公钥对数据进行加密

步骤 5：当值的代表节点根据用户公钥将记录添加入 Item

步骤 6：当值的代表节点广播 Item 确认信息，并将需要处理的大文件存入

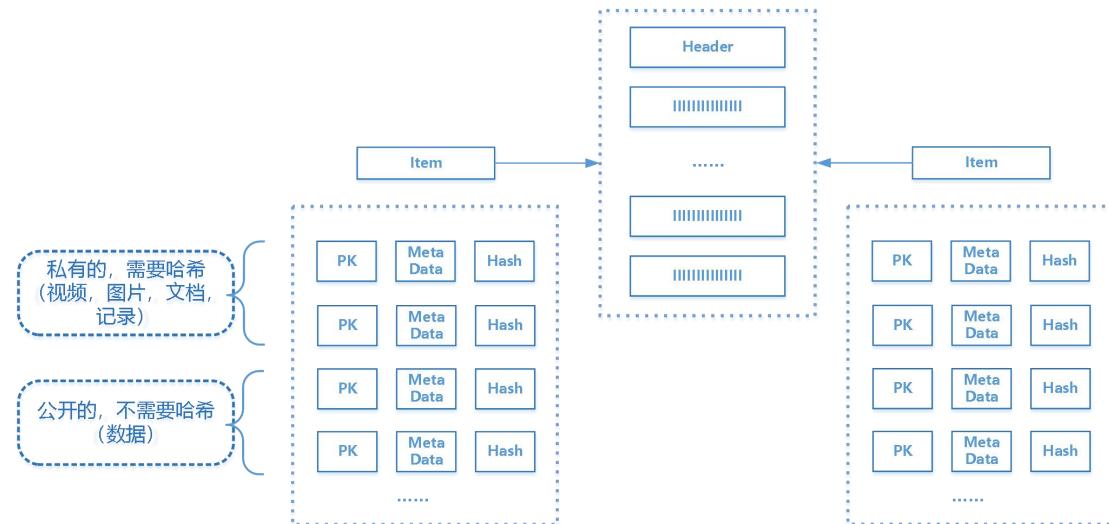
分布式数据库

步骤 7：校验代表节点对记录进行校验，其他节点更新数据

步骤 8：每隔 1 分钟检验一下 Item block 的数量，达到 10 个则组成一个数据块，并计算该数据块的 merkle 根

步骤 9：每隔 10 分钟将所有新生成的数据块的 merkle 根锚定到比特币区块链

步骤 10：返回步骤 1



数据共享与访问设计

数据所有者将数据加密存储在分布式数据库中，模型采用密码学中代理重加密（Proxy reencryption）机制来实现对数据访问控制和共享。因为模型基于区块链技术是一个去中心化的应用场景，没有可信的第三方也就不存在传统重加密场景中的唯一的代理角色。IAESG 中的任何节点都可以充当代理完成重加密的操作，作为报酬可以获得相应的 ZZM Token，代理协议设置如下：

1. 生成随机矩阵，选择安全系数 q 、 n 。
2. 生成公钥私钥对：公钥 $pk = P$, $P = R \cdot A$, 其中 R , S 是高斯参数，则私钥 $sk = S$
3. 加密算法：

$$c = () = ()$$

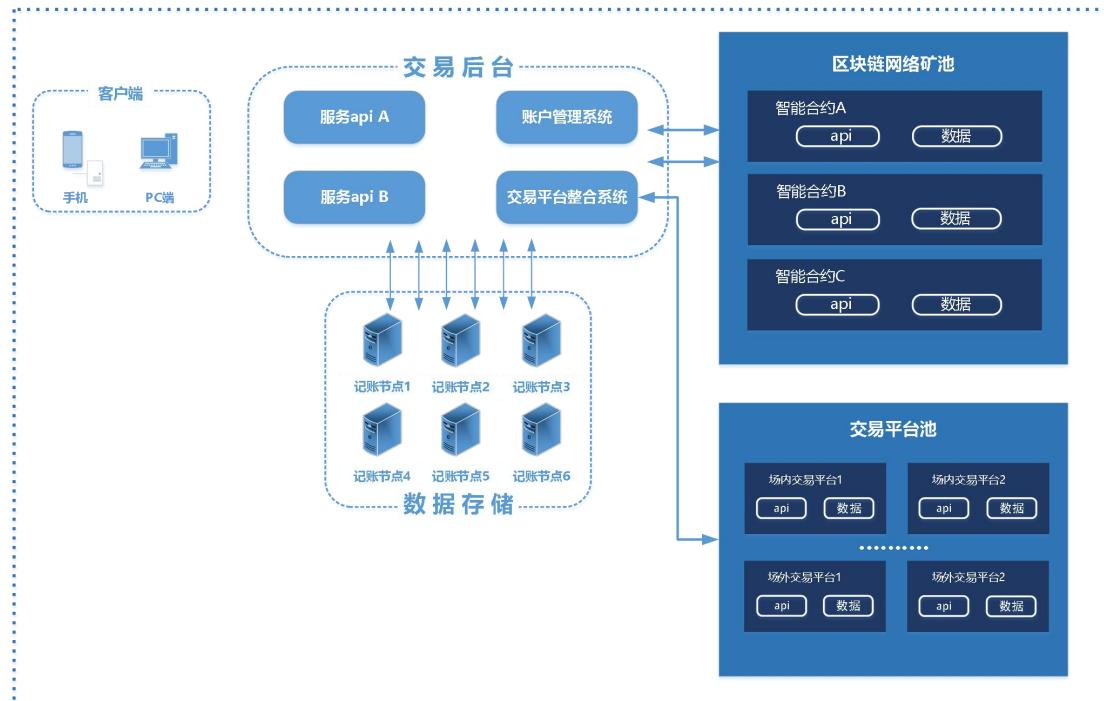
其中是误差参数

4. 解密算法：
 $M = S +$, 根据与 0 的距离远近判断取 0 还是 1
5. 重加密密钥生成算法：

其中， X 是随机矩阵， E 是噪声。

6. 重加密算法：
其中，选择误差分布

彩色币发行架构

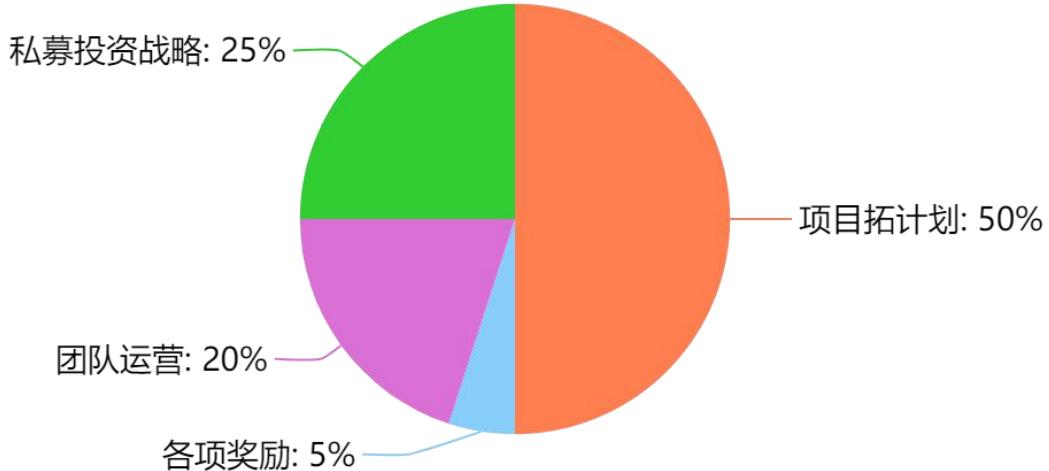


五、Token 介绍和使用计划

Token 名称	ZZM	运营主体	ZZM 新加坡基金会
算法	SCR2.0	发布日期	2017.11.27
发行总量	2 亿	市场流通量	3000 万
现有用户规模	3000-5000 人	官网地址	www.zzmnb666.com
钱包下载地址	http://www.zzmnb666.com/download/zzm-wallet.exe		
源代码	http://39.106.36.203/index.php		

Token 售卖计划总量:2 亿枚 Token, 具体分配计划是:

- 其中 50%用于项目拓展计划
- 25%用于私募投资战略
- 20%用于团队运营
- 5%用于各项奖励



六、项目治理机制

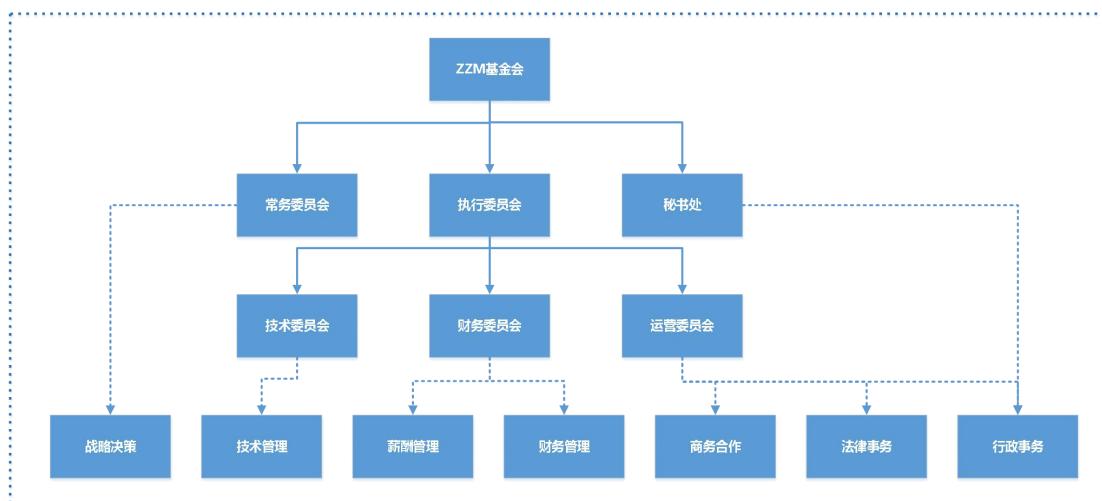
6.1 资金管理机制

募集到的资金应根据透明、可审计和效率原则进行保管和经营。筹集的 BTC 和 ETH 分别被多重签名钱包保管，并受公众的审阅。对于安全问题，这些多重签名钱包的私钥是由五位值得信赖的个人控制。钱包执行任何付款，都需要这五个人的同时签名。通过募集收到的资金将不会用于开发方的股东分红或利

润分配。而会全部用于 ZZM 的开发、维护等技术工作以及生态系统建设（例如投资培育链上的各类应用等）。

6.2 基金会治理

ZZM 是一个去中心化的国际区块链社区，在海外设立 ZZM 基金会来保证 ZZM 社区和资金的管理、运作。ZZM 基金会由基金会常务理事会、基金会执行委员会和秘书处组成。常务理事会人数是 11 个，每年按照一币一票的原则由社区投票选举产生，主要是负责制定 ZZM 未来的发展方向、发展战略以及重大事件决策。执行委员会由技术委员会、财务委员会、运营委员会组成，分别负责 ZZM 平台技术开发、财务管理、商务合作与运营。秘书部共 7 人，由技术委员会、财务委员会以及运营委员会按照 3：2：2 的比例组成，主要工作是协调各委员会的工作。



七、团队介绍

7.1 核心团队介绍

李金龙——ZZM 团队核心

区块链后起之秀，ZZM 创始人之一，毕业于山东大学经济学院金融系，在校期间就多次受邀参与电商平台研讨会，毕业后先后从事过互联网行业、金融行业、电商平台运营，2015 年受邀参加“2015 百家企业金融峰会”后深受启发，转型研究区块链，对区块链有非常深切的热爱，目标将区块链应用于文娱行业并落地。

威廉·杰弗森·克林顿—ZZM 发起人

出生在美国纽约，毕业于纽约大学，美国著名经济学家，早期比特币布道者，参与过众多项目投资，其中包括以太坊、瑞波等。

李站——ZZM 运营总监

ZZM 项目运营总监，韩国金融学硕士，有着丰富的留学经历及国际视野。2013 年回国创业，成立了一托（中国）集团控股有限公司，同时是一托三大品牌创始人，山东鲁商联盟会副会长，一托梦慈善公益发起人。2015 年初入币圈，并在随后的两年时间内参与了区块链投资，项目运营及高峰论坛举办，有着丰富的区块链项目运营经验，有着丰富韩国的区块链社区及交易所合作渠道，致力于推广 ZZM 价值传播。

7.2 合作伙伴介绍：

➤ 陕西中资文化产业发展有限公司

在中国电影衍生品市场处于空白的情况下，陕西中资影视致力于将传统电影衍生品产业发展成为“电影+电影衍生品+院线+景区地产文化旅游”的综合

电影生态产业链，携手西安电广传媒股份有限公司依托西京影视文化平台，开启中国电影衍生品之路。

➤ 一托（中国）集团控股有限公司

一托是山东省首家以房屋资产管理为入口的一站式创业生活服务平台。集团旗下有涉及物业、资产管理、招商运营、商务服务、房地产中介、装饰装修、财务代理、人力资源、汽车租赁、电梯于一体的十大业务。

一托旗下有三大品牌：一托梦想寓专门为有梦想的创业者提供写字间租赁服务；一托青春寓专门为追求梦想在外地打拼的年轻人提供公寓租赁服务；一托自由寓专门为旅游爱好者提供旅游目的地酒店式公寓租赁服务。

一托的五年目标是将一托打造成山东省最大最专业的资产管理集团公司；一托的十年愿景是将一托打造成世界知名的创业生活服务平台。

➤ VK一百男大秀全球时尚品牌

百男大秀，集合中国各个民族、各个区域、各个领域、各个年龄层从 5 岁到 65 岁有生活态度的中国男人生活方式集合平台。来自中国 12 个男士领域的集合，包括企业家、创业家、新闻媒体、运动员、美业造型、童模、56 个民族大叔、KoL 红人、中国超模、健身教练空少、设计师、艺术家、艺人、主持人和各领域意见领袖等。其中耳熟能详的有：任达华，陈冠希，外婆家的 UNCLE 吴国平。更多人员来自新加坡，台湾，美国，日本，北京，上海，杭州，广州，深圳和香港的本身有生活态度男人。多角度，多风格，全面展示中国男性国际水准的全新魅力，由此启发，扩散，落地到更多男性身上。

➤ 秒偶社交电商平台

秒偶是一个定位于社交的电商平台，发行人的时间在“秒偶”上线后，用户可以通过购买的形式持有宝贵的时间资源，将虚拟的个人时间转化为直观呈现的可变通资产。用户可以手持时间约见红人，也可以通过交易、兑换发行人提供的沟通机会、知识、周边、共享体验等方式，对时间资源进行投资和支配。

八、落地项目介绍与未来规划

8.1 已落地和将落地的项目

- ZZM 在秒你 APP 里可购买知名作家出版的书籍。
- ZZM 在 11 月 19 号与具有中国维密之称的 VK 国际时尚服装品牌一同举办了 VK—百男大秀西安站，可用 ZZM 购买 VK 服装。
- 美国秒你影视文化娱乐有限公司将在 2018 年 1 月将自己的购买明星 APP 开发完毕并落地，该 APP 里聚集来自全球的明星、名人等，同时他们的时间只能用 ZZM 购买。该 APP 将成为 ZZM 生态圈重要部分。

8.2 未来规划

ZZM 从概念提出、测试链上线、PC 钱包开发完成、收集钱包对接完毕；从中国社区的建立，到美国、韩国社区的建立；从 11 月 3 号参加秒你电商平台发

布会到 11 月 19 号联手 VK 国际时尚品牌打造 VK—百男大秀西安站；从一百多个最初支持者到现在上万名社区成员。2017 年 ZZM 从概念测试到落地应用，并且在接下来的半年时间里，砥砺前行，完善 ZZM 社区，加速 ZZM 底层技术成熟，搭建 ZZM 的生态。下为 ZZM 的发展规划：



未来，ZZM 将会：

-
- (1) 与美国秒你影视文化娱乐有限公司合作，让 ZZM 真正落地应用，开启 ZZM 支付明星碎片时间，建立 ZZM 第一个回购系统。
 - (2) 建立 ZZM 美国社区
 - (3) 进入韩国，上韩国交易所同时建立韩国 ZZM 社区
 - (4) 在新加坡建立 ZZM 基金会
 - (5) 上线主流交易平台
 - (6) 打造更多 ZZM 的回收系统建立 ZZM 生态

九、风险与管控

法律结构与免责声明

任何人参与 ZZM 代币购买均基于其自己本身对区块链的知识和 ZZM 白皮书的信息。

ZZM 开发方在此明确不予承认和拒绝承担下述责任：

- (1) 任何人在购买金 ZZM 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；
- (2) 开发的推迟或延期，以及因此导致的无法达成事先披露的日程；
- (3) 源代码的错误、瑕疵、缺陷或其他问题；
- (4) 任何参与者泄露、丢失或损毁了数字加密货币或 Token 的钱包私钥
- (5) ZZM 的第三方众筹平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或歇业；

-
- (6) 任何人与第三方众筹平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；
 - (7) 任何人对 ZZM 的交易或投机行为；
 - (8) ZZM 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制；
 - (9) 本白皮书披露的任何风险因素，以及与该风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

风险披露

参加代币购买应当是一个深思熟虑后决策的行动，将视为参与者已充分知晓并同意接受了下述风险：

- (1) 因法律政策变化或政府行动，导致 ZZM 无法正常开发或使用，或者导致 ZZM 被禁止持有或使用的风险。
- (2) 因密码学的发展或者量子计算机的商用化，导致基于密码学的货币不再具有足够安全性（比如私钥易被破解）的风险。
- (3) 源代码基于社区要求而进行升级或修改，因此导致无法预测的风险。
- (4) 在运转时被“分布式拒绝服务”攻击或其他类型的攻击的风险；
- (5) 任何人持有的 ZZM 币被盗窃、遗忘或灭失的风险；

参考文献：

- [1]. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2009.
- [2]. Technical report by the UK government chief scientific adviser[Online],available:<https://www.gov.uk/government/uploads/system/uploads>

- ds/attachment data/file/492972/gs-16-1-distributed-ledger-technology.pdf,
February 21, 2016
- [3]. 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,(04):481-494.
- [4]. 郑金宇. 区块链技术对银行业的影响、展望及监管挑战[J]. 银行家,2016,(07):11-13.
- [5]. Zyskind G, Nathan O, Pentland A S. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]. IEEE Security and Privacy Workshops, 2015. 2015: 180-184.
- [6]. 贵阳市人民政府办公室. 贵阳区块链发展和应用[R]. 贵阳:贵州人民出版社,2016:18.
- [7]. 工信部. 区块链参考架构[M]. 2017.
- [8]. 杰弗里·摩尔. 跨越鸿沟[M]. 机械工业出版社, 2009.
- [9]. Furlonger D, Valdes R. Hype Cycle for Blockchain Technologies and the Programmable Economy, 2016[OnLine],available:<https://www.gartner.com/doc/3392717>, July 27, 2016