区块链3.0底层操作系统

基于多链技术的联盟+共有基础链
游戏场景化的区块链应用聚合平台

概 述

区块链技术发展至今，已有一千多个项目问世，涵盖从支付、金融、游戏、竞猜游戏到物联网等生活的方方面面。在可见的未来，会有越来越多的技术人员和科学家研发出更好的区块链产品，为大众提供更优质的服务，推动大量基于区块链技术的产品投入应用。但是，由于区块链在现实生活中存在渗透率尚低、缺乏贯通场景、不同链之间无法实现交互、用户无法找到入口级产品等问题，目前大众尚难以在日常生活中实际接触到这些基于区块链的产品与服务。

加密世界公链（CWV）是全球首条搭载混合共识、多链技术等二十多项区块链自主研发区块链专利技术的公链，是目前国际领先的融合公链。该链是基于 PBFT+DPoS+Raft 混合共识算法、结合了高性能联盟链和个人公有链的融合主链，能够支持不同区块链的共识， 通过利用侧链与其他区块链网络兼容，可以扩展和查询其他链中的数据。在承载十万级交易需求和更高性能需求的智能应用的情况下，依然可以保持安全高效的共识机制和分布式账本。

同时，加密世界公链（CWV）自带 SPEEDFORCE 快速交易传输网络，该网络类似于以太坊的闪电网络，但交易速度更快、能力更强，具有毫秒级的处理速度和理论上十万级的交易处理能力；带有开放跨链交易 API、智能合约、容器运行 sdk 和共享账本体系，是一个支撑区块链应用开发的开放平台。

CryptoWorld.Vip（加密世界）是基于加密世界公链（CWV）开发的首个入口级应用平台，是一个链接各种区块链技术的场景化虚拟世界。通过多链机制融合十万级 TPS 的主链，加密世界链是一个区块链 3.0 操作系统级别平台，它的使命是简化企业对区块链技术的采用，并将其集成到特定的业务应用程序和产品中。 通过加密世界公链，企业和个人都可以利用该平台快速创建自己的 DApp，管理自己的数字资产和构建专属的信用系统，通过利用该平台提供的基于区块链的业务工具，现代公司可以轻松地将其业务模型调整为具有区块链思维的新兴业务模型。

目录

1 项目背景

1.1 行业背景

我们正处于从工业文明迈向数字文明的进程中，要实现这一文明阶段的跨越演进，首先需要解决信任普遍缺失、权力不受制约和社会参与不足这“三大障碍”。互联网的诞生颠覆了人们传播信息的方式，是信息的去中心化，但并没有解决财富与价值在互联网上的转移问题。

区块链技术先天具有传递信任和价值、重构价值体系和秩序规则的能力。业界普遍达成共识，区块链作为一种全新的底层协议构建模式，将会成为继云计算、大数据和高级分析以来的又一个迭代性的重大创新技术，并成为现有互联网实现从信息互联网向价值互联网升级换代的核心推动力。

【来源：Statista, Blockchain.info】

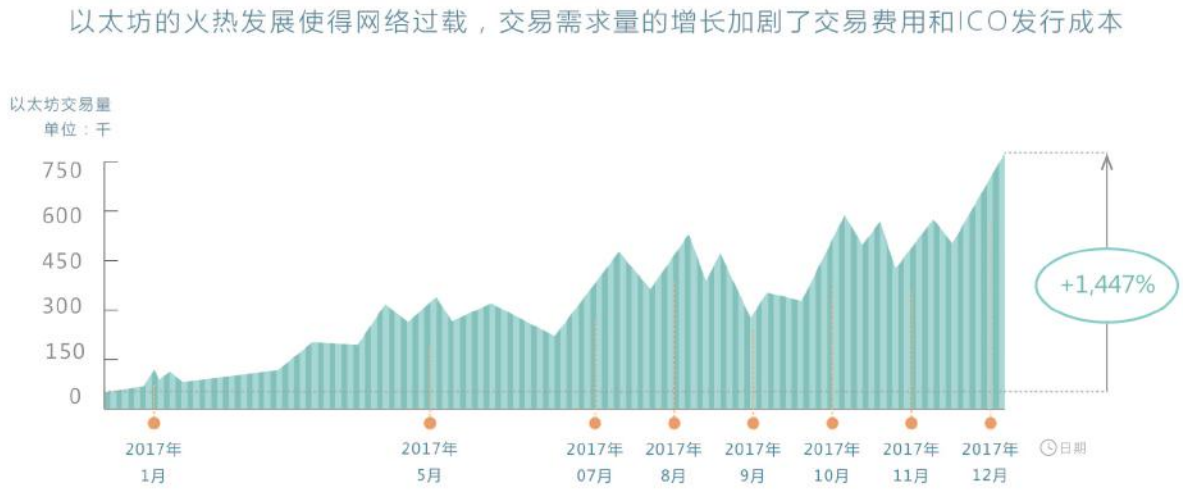
2016 年，区块链技术的真正价值开始被关注和挖掘，因此被称为“区块链元年”。2017 年，区块链实现了爆炸式增长，全球正在跑步进入“区块链经济时代”。2018 年，全球各行各业主动拥抱区块链，积极进行业务探索。在可预见的未来，区块链还将继续保持高速增长，但是许多区块链项目的开发周期长达两年以上，其在现实中的渗透度严重不足，缺乏可以体验和交互的场景。面对数量巨大的区块链项目，用户往往找不到其服务的入口。

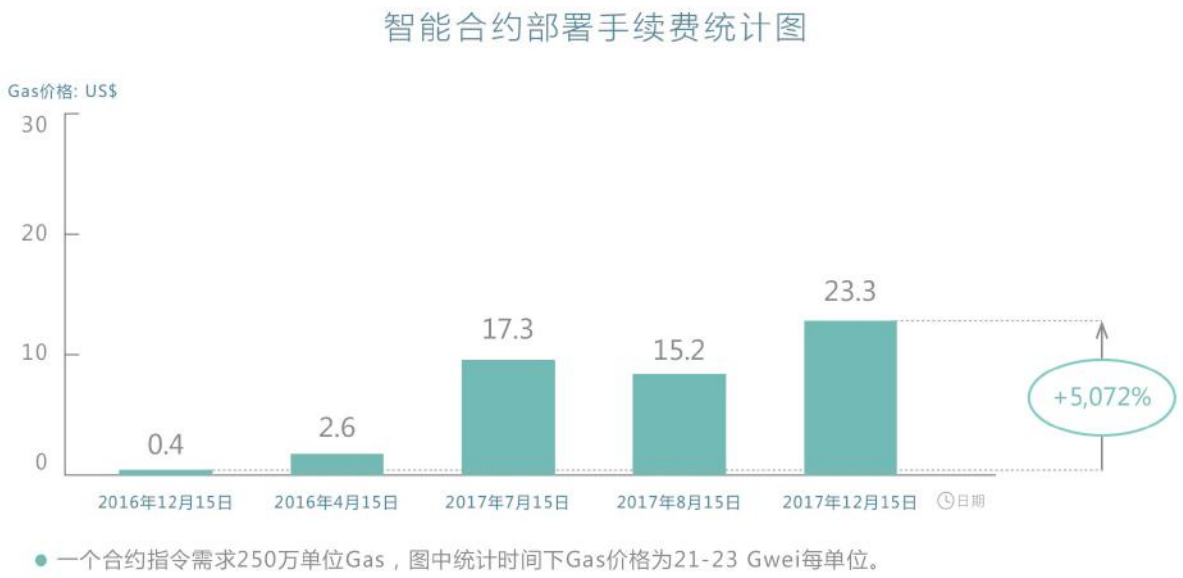
2019 年，区块链经济时代有望正式开启，黄金时代已经到来！加密世界-场景化价值虚拟世界将各式各样的区块链服务聚合在一个可视化的场景里，让区块链网络的价值得以场景化地集中展现。

1.2 **市场痛点**

1）现有主链交易处理速度与承载能力存在隐患

主链的交易处理速度成为目前限制区块链应用、用户体验的最大瓶颈。从最早 BTC 的 7 TPS，到 ETH 的 20 TPS，到 EOS 的 2,300 TPS，目前主流项目的交易处理速度远远无法满足蓬勃发展的区块链应用服务领域的要求。同时，随着用户规模的爆发式增长，对高并发交易的响应如果出现明显延迟与合约部署蜂拥大大增加，将对用户体验造成毁灭性打击。





【来源：安永】

近期一个活生生的案例是由加拿大初创公司 Axiom Zen 开发的一款基于以太坊(Ethereum) 区块链的养猫游戏 CryptoKitties，自 2017 年 11 月底上线便席卷整个虚拟货币世界。根据国外第三方网站 CryptoKitties Sales 的统计数据，目前该游戏的活跃玩家超过 25 万人，互不相同的虚拟猫接近 5 万只，截至 2018 年 3 月 6 日虚拟猫的总销售额将近

41,375 ETH。[1]这样的火爆对以太坊的承载能力提出了巨大的挑战，该游戏一度占用了以太坊 25% 的算力，导致系统拥堵几近瘫痪，全网速度急剧下降，交易费大幅度增加。

虚拟货币用户规模的增长在 2017 年创造出前所未有的机遇，各类虚拟货币活跃钱包数量已超过 2000 万，用户基数的暴涨自然带来市场需求的激增。CryptoKitties 的成功让人意识到游戏可能是区块链技术最早期、最高频的应用场景，但以太坊的先天局限使其无法承载高并发、高频的游戏场景，因此许多项目方都在寻找性能更强大的区块链底层技术方案。

2）一般用户接触区块链应用服务的渠道匮乏

区块链项目数在 2017 年同样迎来爆炸式的增长，根据国外网站 ICOBox 的统计，2017 年全年共有超过 380 个项目成功进行了 ICO 募资，其中一半以上发生在第四季度[2]，这一增长势头在可预见的未来仍有望延续。

然而，目前区块链技术项目的火热仅仅局限在资本市场，绝大多数项目仍处于早期试验产品甚至构想阶段，开发周期大多长达两年以上，因此一般用户实际体验到这些能够颠覆性地改变日常生活的美好应用尚需时日。

即使这些项目顺利完成开发并上线运营，其在现实生活中的渗透度是否能够达到预期仍有待观察。同时，面对数量巨大并且仍在不断增多的区块链项目，不具有专业知识的用

[1] https://qz.com/1197978/ethereum-game-cryptokitties-is-launching-on-mobile-and-in-china/

[2] https://medium.com/icobox-io/cryptocurrency-and-ico-market-overview-for-2017-b82297996c22

户很难找到一个低门槛的服务入口。如果一般用户不能轻松地享受这些服务，再革命性的技术也不过是纸上谈兵。

3）场景交互及货币切换难以实现

当前众多区块链应用已经涵盖了以互联网、信息、金融、房地产、交通等为代表的日常生活的方方面面，未来也将会有更多更细化的使用场景。然而，不同的区块链项目与服务相对独立、彼此隔绝，大部分区块链项目尚未给普通用户提供一个易于上手、成熟可靠的场景交互解决方案，不同项目货币之间的兼容切换问题势必会影响用户体验的完整性与流畅性。

我们以最乐观的估计假设不同领域的众多区块链项目将成功开发并顺利落地，但如果一名用户在游戏平台需要消费 A 游戏币，参与体育竞猜又要另行准备 B 游戏币，享受金融服务还要切换成 C 平台币，与好友互动再要使用 D 社交币，这样四分五裂的区块链世界，究竟能为我们的生活水平带来多大程度的提升？归根结底，用户体验是评判一切服务高低优劣的准绳。毋庸置疑的是，区块链技术将给人们的生活带来革命性的突破与改变，但是如果没有一个入口清晰且可以无缝衔接各种场景的可视化应用，区块链技术之于现实生活的意义将大打折扣，整个行业的发展前景也会蒙上阴影。

1.3 解决方案

1）加密世界（CryptoWorld）

加密世界依托自主研发、性能强大的加密世界公链（CWV），旨在解决目前主链交易处理速度低与承载能力不足的问题，通过构建一个模拟资产经营平台，为一般用户提供一个体验区块链技术革命的入口和连通各区块链应用的可视化场景，并为行业内专业开发人员搭建一个无限扩充的开放平台。

2）加密世界公链（CWV）

加密世界公链（CWV）是由加密世界项目团队自主研发的底层区块链技术，是全球首条多链机制融合主链，采用了 PBFT+ DPoS+Raft 的混合共识算法，能够在维持安全高效的共识机制和分布式账本的前提下大幅提升区块链的读写吞吐量。同时，CWV 自带 SPEEDFORCE 快速交易传输网络，拥有十万级交易处理能力，大幅提升了主链承载能力，可以为用户提供更多具有更丰富交互体验的应用。此外，CWV 还带有开放跨链交易 API、智能合约、容器运行 SDK、共享账本体系等，构建出一个完整的支撑区块链应用的开发平台。

3）应用聚合平台（CryptoWorld.VIP）

加密世界将会构建一个规模庞大的应用聚合平台（CryptoWorld.VIP），前期聚焦游戏应用，伴随平台运营的成熟与用户规模的扩大，再逐步拓展至其他应用。

通过提供一个互联开发扩展框架，开发者可以将不同的应用嵌入加密世界体系之中，加密世界的生态系统也因此得到不断丰富，真正实现可持续发展。

模拟资产经营游戏平台作为首个入口级应用平台，以 1:1 映射的现实世界建筑空间为基础，通过将不同的虚拟建筑接入不同的区块链并赋予其各异的服务功能，构建出一个连通不同区块链项目的场景化服务平台。虚拟地产空间是加密世界的基本框架，也是整个加密世界核心世界观的主要载体，通过一个不断扩展场景应用的体系，真正为用户提供一个进入区块链世界的入口，可视化地体验众多区块链项目为现实生活带来的变革。

2 加密世界商业模式

2.1 加密世界详解

1）核心架构

加密世界是由底层加密世界链与各类智能合约开放平台组成的生态系统，在全新的模式下构建了以 Token 和容器 Docker 为核心的智能合约，为各类 DApp 开发商提供了一个更为友好的开放平台。

基于自主研发的区块链技术，加密世界实现了核心世界观系统及各种场景应用系统的去中心化运行。整个系统运行环境的各组成部分以容器 Docker 的形式被复制成多份，分散到不同地域、不同加盟服务器上进行多点灾备。一旦运行环境出现异常，加密世界会通过智能合约自动选出另一个性能最佳的服务器，并将其上的系统环境 Docker 运行起来，从而恢复

全部系统服务。

2）自主研发的底层区块链系统

加密世界使用具有自主知识产权的区块链核心引擎，构建联盟链与个人公有链结合的基础主链。区块链上的记账节点与验证节点分散在不同地域，归属不同算力提供者的服务器，构建出一个相互信任又彼此制约的区块链运行环境。

个人用户的计算机可以作为账本验证节点加入加密世界公链，为加密世界提供账本信息验证工作，作为回报获得平台代币 CWV Token。获得的 Token 既可用来在加密世界中购买房产、享受各类区块链服务等，更好地融入生态环境。也可在交易所将虚拟利益转化为现实世界的收益。 Token 激励机制将吸引更多专业、优质的服务器加入，推动生态环境可持续发

展。

底层区块链系统采用微服务架构，应用全栈异步处理方式，以 Actor 微内核方式进行多线程调度管理，搭建了一个高性能的引擎框架。同时，采用多链区块并发打包机制，实现交易的快速确认。此外，通过侧链对接技术实现加密世界公链与其它公链（如比特币、以太坊等）的对接，形成一个融合链网络，将其他外链区块链应用整合到加密世界中，并通过代币交换系统实现 CWV 与 BTC、ETH 及其它彩色币自由的自由转换，真正为用户提供无缝衔接的服务体验。

3）核心世界观系统

加密世界为用户提供了一个广阔、开放的虚拟世界，这个世界拥有自己特有的核心世界观，如虚拟地产构建规则、游戏规则、Token 体系规则、Dapp 分润规则等。所有规则均以智能合约的形式入链锁定并同步到每个节点服务器上，确保平台的公平公正。

4）用户访问门户

用户访问门户是指加密世界为用户提供的多种终端产品，如 iOS、Android、H5 等，是用户访问加密世界的入口。用户与加密世界的具体交互方式主要包括管理自己的虚拟资产、参与位于世界各地的场景应用（如游戏、资产交易中心等）、与其他用户互动、使用集合的各种区块链应用等。

5）模拟资产经营平台

CryptoWorld.Vip 是基于区块链的模拟资产经营平台，具有可视化、场景化的特点，是

加密世界首个落地项目。与网络游戏的完全虚拟化不同，加密世界基于区块链技术，在虚拟世界中提供现实世界的产品与服务，所有交易均以平台代币 CWV Token 结算，是沟通虚拟世界与现实世界的桥梁。很多虚拟地产拥有和真实世界相同的行业职能属性，如游戏厅、娱乐场、交易公司、广告公司（购买虚拟房屋广告位并进行广告投放）等。CryptoWorld.Vip 的宗旨是让用户在获得游戏娱乐体验的同时展现创意，在全新的数字世界里拥有一块属于自己的土地并构建自己的家园和事业，通过经营收益及平台分成获得真实世界的价值提升，真正体验一种全新的生活方式。

CryptoWorld.Vip 以游戏的形式将用户聚合在一起，并将不同的区块链应用与加密世界中的各种功能性虚拟建筑进行绑定，真正为用户提供一个进入区块链世界的总入口，以可视化地体验众多区块链项目为现实生活带来的变革。

6）外链应用互联扩展开发框架

加密世界提供了一套完整的互连桥接开发框架，在该框架下开发者可以利用侧链技术将其他主链、公链上的 DApp 融入到加密世界生态体系之中，并在模拟资产经营游戏平台上以可视化、场景化的形式展现出来。同时，开发框架下设有 Token 跨链兑换中心，用户可以在此完成 CWV Token 与其他 Token 之间的兑换，真正实现外链应用服务与加密世界体系的无缝对接。

7）区块链场景应用发布平台

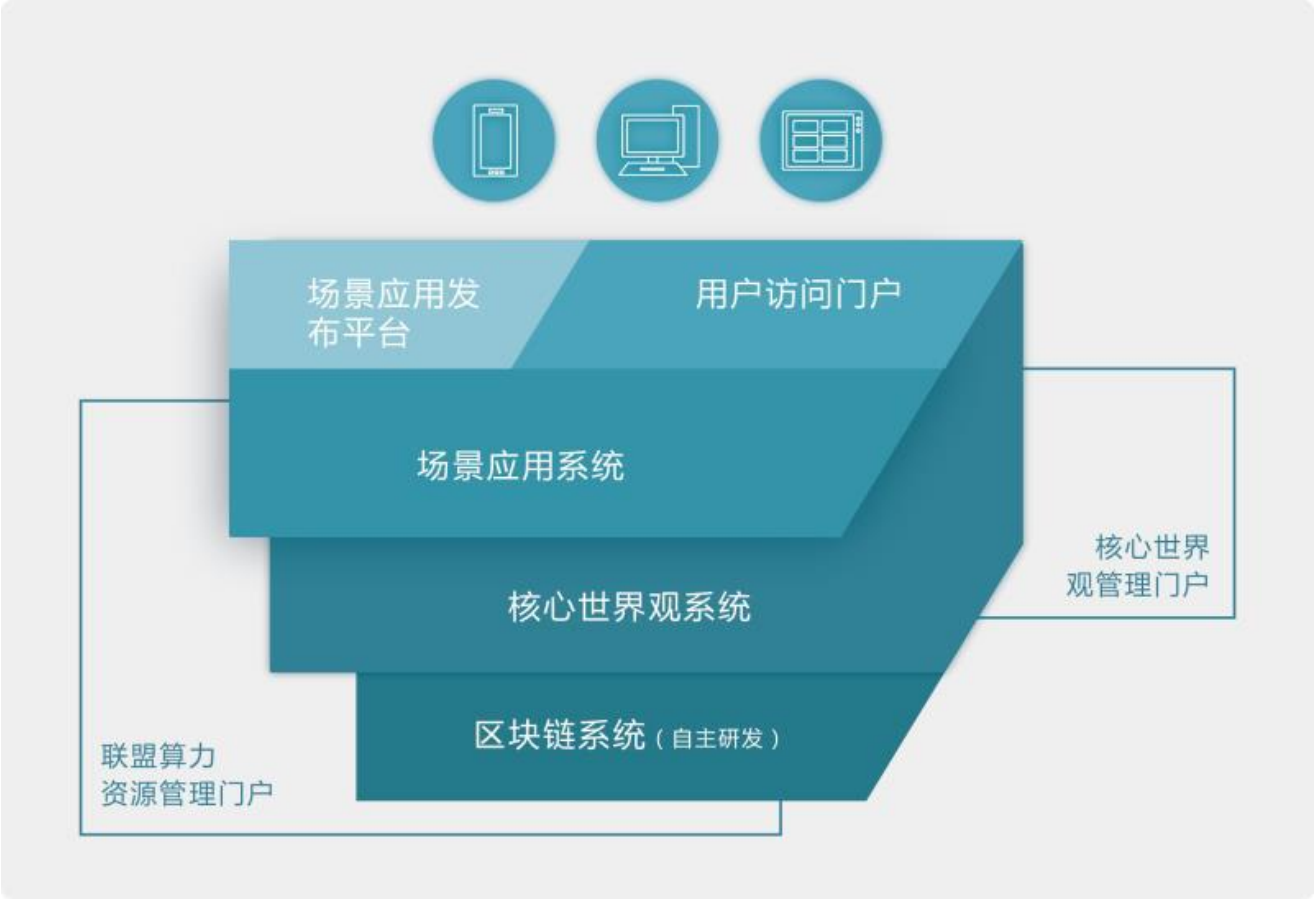
加密世界公链为开发者提供丰富的开发扩展框架，以便其为加密世界开发各种行业职能

应用（即：场景应用），并通过场景应用发布平台将自己的场景应用发布到业务承建市场中。

场景应用一旦发布成功，虚拟地产的业主可以在业务承建市场中选择购买/租赁相应场景应用 DApp，为自己的虚拟房屋添加相应的场景应用服务属性。加密世界中的其他用户可以在其中进行相应的场景活动，如游戏、广告投放等。

开发扩展框架将提供如下功能：

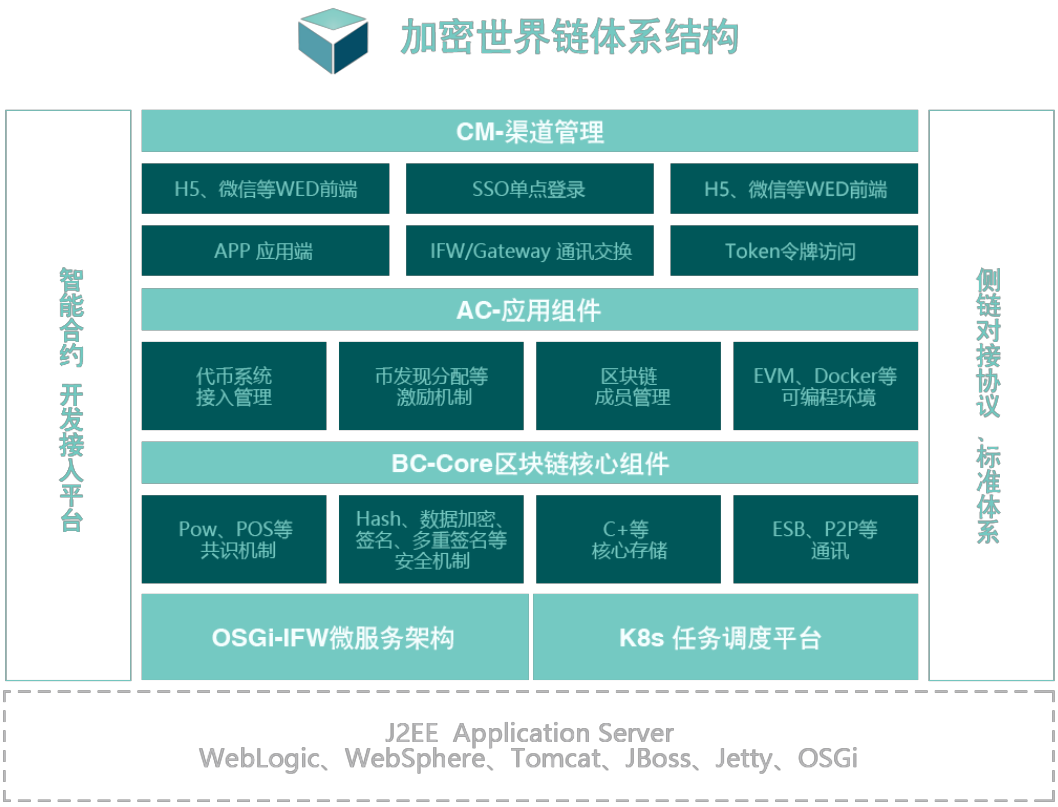
- 区块链浏览器
- SDK 开发工具包，支持 Java / Kotlin、.NET C# / VB、JavaScript / Typescript、Python、Go
- 智能合约编译器与 IDE 插件
  - C# / VB.Net / F#，Visual Studio
  - Java / Kotlin，Eclipse
  - C / C++ / GO
  - JavaScript / TypeScript
  - Python / Ruby



2.2 加密世界公链详解

1）核心架构

加密世界公链（CWV）是一个开创性地结合了 PBFT+ DPoS+Raft 混合共识机制的多链机制融合基础主链，采用更完善的技术架构。

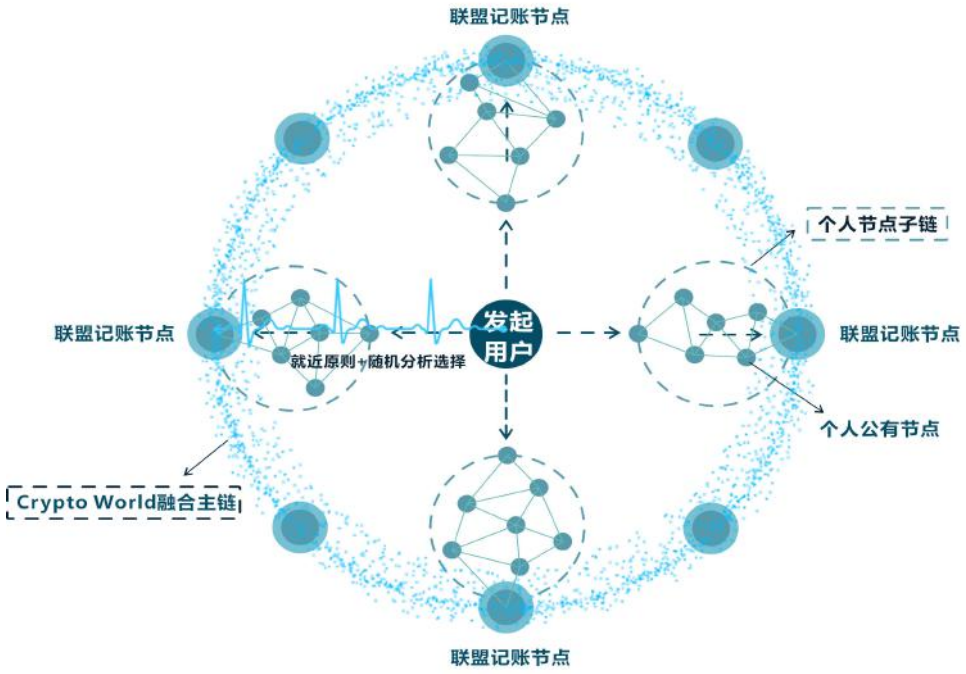


2）多链机制融合基础主链

i. 联盟节点+多条个人公有链融合的基础主链，其承载能力可以支持具有更多交互需求、更高体验要求的应用。系统对新加入的节点实行审查机制，确保资源提供方的设备性能符合要求。

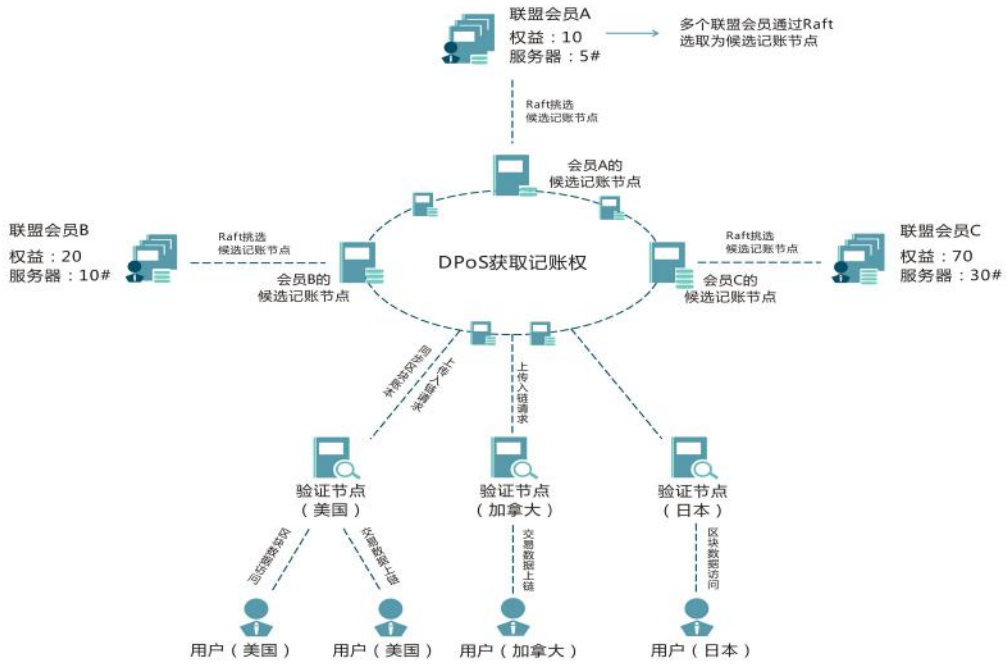
ii. 将传统的记账功能与查阅功能分层，随机入链，就近访问。由联盟负责记账，个人节点则负责审核查阅，在实现去中心化的同时保持高效运营。同时，联盟会根据设备性能选出核心会员，保证平台整体的稳定性。

iii. 自带更快速的“类雷电网络”SpeedForce，具备毫秒级交易处理速度与十万级交易处理能力。



3）PBFT+ DPoS+Raft 混合共识机制

在节点通讯 P2P 层采用了 PBFT 共识算法，使得节点网络数量可以达成一致（投票）；使用 Raft 算法使得由同等网络或者同一个 IDC 机房的几台服务器共同构成一个超级节点，通过强一致的 Raft 算法，对交易执行，合约运行提供任务分发共识；最后，在消息广播确认和成块机制上，提出了一种改进的随机 DPoS（Delegated Proof of Stake）算法，实现秒级出块，块级别的拜占庭算法 PBFT，可以对分叉进行检测和回滚。该算法将会大幅度提升 TPS，并且能够抵抗 1/3 作恶节点。链上我们提出了基于智能合约仲裁（Sanction）的机制，可以在区块链链治理上，提供一个更好更高效的解决方案。



4）PoW 真随机挖矿智能合约

在很多应用中都需要引用随机数作为公平性的依据。尤其是在游戏过程中随机数的生成是游戏公正性和可玩性的基础。比如加密世界里的虚拟房产抽选，扑克类的发牌次序、筛子的掉落机率；抽奖类的中奖率、游戏装备的掉落概率、野怪的掉落，剑圣的每一刀是否暴击，牛头人是否能打出粉碎等场景均依赖于随机数产生机制。在计算机世界有一个宝典一般的金句：“程序里没有真随机”。计算机生成的随机数都是用一套固定算法生成的，而不是真正意义上随机生成的数字，只要随机种子是相同的，那生成的随机数也是相同的。比如说 Python 的 numpy 中的 random 可以设置种子的参数，从而使得生成的两组随机数是一模一样。

CWV 中的采用了一套独有的真随机生成技术，通过在遍布全球组的区块链节点服务器中预制随机合约调用现场噪音收集模块，将全球各地的现场噪音片段收集到加密世界主链

中，然后通过真随机算法计算出随机种子，供加密世界中的游戏使用。由于全球真实世界的噪音是千变万化，没有规律可遵循，在加上加密世界自有的随机算法，从而产生真正的随机数。

5）技术架构独特优势

2.3 游戏应用研发

加密世界游戏团队会开发各类应用类小游戏，如足球竞猜对应 2018 年世界杯，第一款足球竞猜游戏会在 2018 年 6 月之前推出。此外，还将开发基于区块链的“竞猜”游戏，利用区块链的去中心化运行特点确保游戏的公平公正性，为用户提供极具娱乐性的模拟现实体验。用户通过加密世界的 CWV 代币参与游戏活动，并将游戏结果记入区块链中。竞猜游戏应用会陆续覆盖各种传统种类，包括比大小、德州扑克等。“竞猜”游戏经营权由第三方合作伙伴提供。

3 区块链核心技术

3.1 共识算法

加密世界的底层区块链系统采用 PBFT+ DPoS+Raft 混合共识的方式，在节点通讯 P2P 层采用了 PBFT 共识算法，使得节点网络数量可以达成一致；使用 Raft 算法使得由同等网络或者同一个 IDC 机房的几台服务器共同构成一个超级节点，通过强一致的 Raft 算法，对交易执行，合约运行提供任务分发共识；最后，在消息广播确认和成块机制上，提出了一种改进的随机 DPoS（Delegated Proof of Stake）算法，实现秒级出块。

互联网数据中心（IDC）是专门提供网络资源外包以及专业网络服务的企业模式，帮助

互联网业内分工细化。其主要服务包括整机租用、服务器托管、机柜租用、机房租用、专线接入和网络管理服务等。广义上的 IDC 业务，实际上就是数据中心所提供的一切服务。客户租用数据中心的服务器和带宽，并利用数据中心的技术力量，更好地满足自身业务发展对软、硬件的要求，搭建自己的互联网平台，享用数据中心所提供的一系列服务。

加密世界公链实现了所有节点以内网的方式同时在一个 IDC 中心达到毫秒级的同步和共识。通过 IDC 局部竞选出来的节点，将以 S_i 的权益身份参与下一轮的投票及挖矿。从概率算法层面，相同权益下每个节点的挖矿概率是相等的；在不同的区域内部，代表的权益越多，成功挖矿的概率就越大。因此，这样的设置可以激励各矿工节点提高区域内部的网络质量，相互促进从而提高效率，形成系统发展的良性循环。

1

参与投票的概率为：$P_i = \frac{1}{N_i} * Et$，

其中 Ni 为第一层的节点个数，Et 为进行一次选举轮询的时间间隔。

2

DPoS的权益算法为：$hash\left(hash\left(B_{prev}, Pi\right), Ni, t\right) \leq \frac{bal(A)*M}{D}$

其中D为挖矿难度：$D = \frac{1}{T}\sum_a bal(A)*Si$ ，取决于 Si 子集中的投票权益总数。

3

因此每个节点可以挖矿的概率为：$P\left\{T = \left(T_i * S_j\right)\right\} = r_i / \sum_{j=1,k=1}^{M,N} r_j * s_{k,}$

3.2 **区块形成机制**

为解决区块容量不足的问题，加密世界的共识分析方法引入了随机相关性分析，对默克尔树进行了优化。默克尔树(Merkle Tree),通常也被称作哈希树(Hash Tree)，顾名思义，

就是存储 hash 值的一棵树。Merkle 树的叶子是数据块(例如，文件或者文件的集合)的 hash 值。非叶节点是其对应子节点串联字符串的 hash。

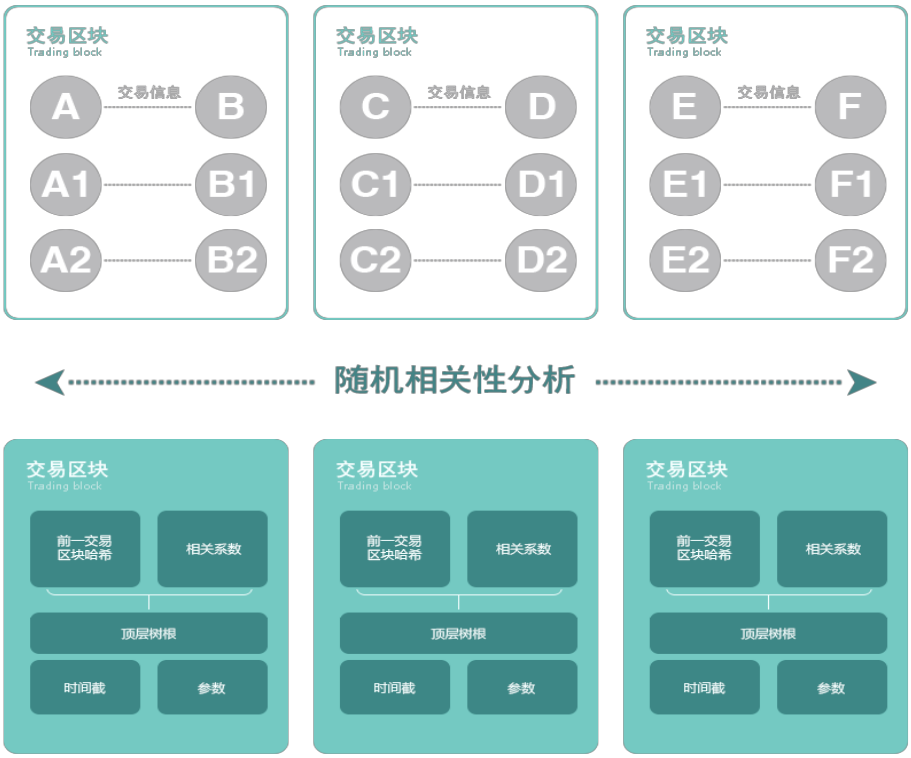
每个交易区块包含前一交易区块的哈希函数，每当有新的交易信息产生，通过随机相关性比对将交易信息按一定顺序连接在默克尔树中。交易区块中的相关因子能够为交易信息记录提供支撑，引导默克尔树的形成。当大量交易信息集中出现时，相邻交易区块随机相关性最高，通过构建相邻正相关模型可以使共识分析更加高效地进行，形成一条完整的相互制约彼此共识的交易链。

基于随机相关性分析的区块形成机制通过筛选录入信息缩短共识周期，提高交易区块的利用率与稳定性。同时，克服了共识机制下交易区块产生速度的局限性，避免哈希碰撞匹配交易区块的繁琐过程。此外，通过随机相关性分析可以检查网络中可能存在的待确认交易信息的有效性。

如下图所示，一种基于区块并发执行算法的记账方法，包括以下步骤：

- 在至少两个交易区块中分别进行交易操作，将交易信息存放在相应区块中。
- 对至少两个交易区块中的交易信息进行随机相关性分析、比对和排序，形成正相关默克尔树结构。
- 在至少两个交易区块中，前一个交易区块在交易过程中获得交易信息正相关默克尔树，并通过前一个交易区块的哈希结构执行后一个新生成交易区块的交易操作。新生成的交易区块中产生的新交易信息通过随机相关性比对进行交易区块之间的关联，使

至少两个交易区块形成一条完整的交易区块链，从而完成交易共识。



3.3 **智能合约**

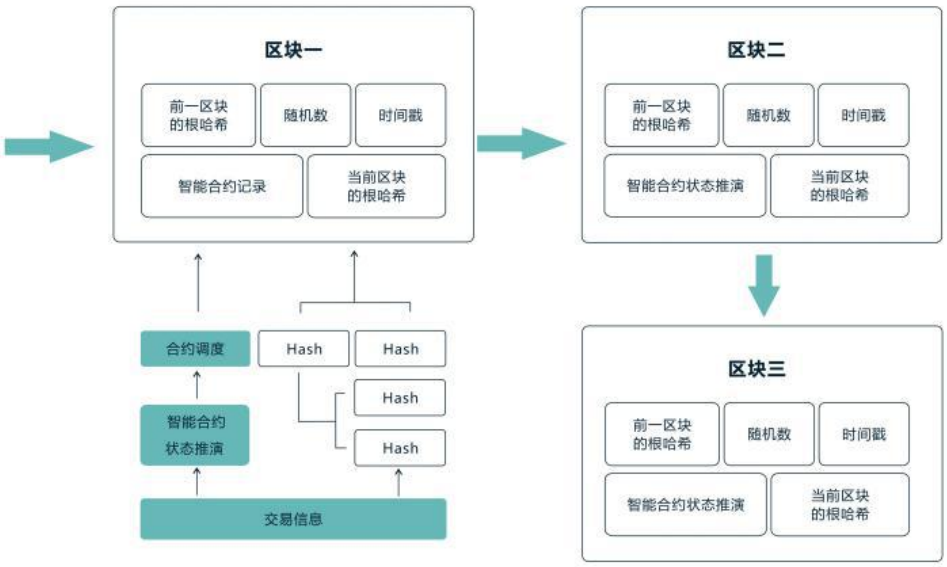
基于区块链智能合约的流程调度系统在传统区块链模型中增加了状态推演模块，该模块是一个函数式的过程，利用角色模式并充分利用多核机制，在进程及线程调度上具有吞吐量高、线程切换快等优势。

加密世界采用以分布式任务队列为工作项节点，并以流程状态及前后关联性记录作为存储的广义流程调度管理方法，能够在多任务、多机构和多角色的集中业务处理领域充分利用分布式缓存、无状态的函数式等技术，减少整个交易流程的系统损耗，为系统提升线性扩容能力，实现高效调度。同时，通过关联式的交易信息记录管理，避免账本管理过程中容易出现的复杂度高、耦合度高、扩展性差、难以维护等问题。

同时，加密世界在合约层提供 Docker 的运行封装以保证流程可以在区块链的任意节点上运行。DockerFile 是 Docker 封装的规范，加密世界在 DockerFile 基础上提供了智能合约的扩展和协议 BC-SMARTC，包括 UTXO 模型、Account 模型下地址之间的 Token 指令集、有限状态机 FSM 的流程定义等。不同的应用可以定义不同的 FSM 状态流程，极大地丰富了合约的流程处理方式。

基于区块链的账本交易执行主要包括根哈希、随机数、时间戳、智能合约记录等几个方面，具体过程包括：

- 以链式结构进行交易信息传递，只需要描述交易区块的节点连接、传输方向与流转条件，就能设计出交易流程并进行交易记账，简单直接。交易信息通过哈希运算形成哈希树，通过进行信息比对实现节点同步。
- 对于根哈希的形成，在最底层把交易信息分成小的数据块，与相应的哈希对应，之后逐层向上把相邻的两个哈希合并成一个字符串。通过运算这个字符串的哈希可以得到一个子哈希，直到最顶端形成这个区块的根哈希。
- 在 P2P 网络下载前，先从前一区块获得可信的根哈希，由此检查当前区块所生成的根哈希。如果当前区块的根哈希是损坏的或者虚假的，就从其他源获得另一个根哈希，再检查，直到获得一个与可信树根匹配的根哈希。



3.4 **随机合约**

随机数算法在当今世界的有着非常广泛的应用，金融、机械制造、IT 网络等等各行业均有使用。这也促使人们对随机数算法进行更加深入的研究，甚至有提供随机数服务的真随机数网站，利用大气噪声或者某种不可预测的大范围的随机源产生随机数。而对于实际应用当中应该使用什么样的随机数算法需要根据系统的不同要求而不同。对于比较简单的需求，比如网站的随机验证码，使用操作系统自带的伪随机算法就可以满足要求。对于银行密码或数据加密，随机数的要求很严格甚至非常苛刻，一旦出问题有可能导致很大的损失，可以采用硬件真随机算法。

目前大部分计算机产生的随机数使用的是梅森素数旋转随机算法(Mersenne Twister random number Algorithm MT19937) ，1997 年开发的，基于有限二进制字段上的矩

阵线性递归，这是一个伪随机数发生算法。

如何结合区块链的方式，通过挖矿原理，提供真随机数，需要一套智能合约的方式来执行，保证区块链能否产生真随机数。

通过挖矿的智能合约方式，采用约瑟夫环随机方法，在区块链上提供真随机的算法。使用挖矿技术把每记录 ID 切成 n 片，随机放入 n 个随机切片文件中，存放的顺序及规则由数据库存储，切片文件以 M 张记录为一组，每个切片文件使用加密算法加密存储，加密密钥是提供随机资源的公钥 。

每次随机矿产生时，首先解密随机切片文件结合数据库存储信息组成完整记录号序列，然后根据上次区块链的保存参数，生成 k（20）个随机队列，每个随机队列充满 a（50000）个记录数据，准备好为客户端返回 ID 数据。

客户端请求数据时，根据请求参数按照约瑟夫环算法随机从 K 个随机队列中抽取一张随机 ID 返回。一旦队列中的数据不足满队列的 20%（M 张）时，系统按照规则从随机序列中抽取数据充满队列。

约瑟夫环需要的参数数组存储在区块链中，客户端请求随机序列时，利用系统自带随机数（或 MT 算法）随机一个参数，系统根据这个参数公钥地址中取得约瑟夫环参数，进而在随机队列中取得数据。

具体设计目标如下：

1) 随机序列要保证 5000 亿（50 亿/年 x1000 年）以内随机数据不重复。

2) 支持至少 10 万张/秒取数据速率。

3) 保证数据安全，没有被窃取、篡改可能。

4) 切片文件加载记录序列时间不超过 1 分钟。

约瑟夫环是一个数学的应用问题： 已知 n 个人（以编号 1，2，3...n 分别表示）围坐在一张圆桌周围。从编号为 k 的人开始报数，数到 m 的那个人出列。他的下一个人又从 1 开始报数，数到 m 的那个人又出列。依此规律重复下去，直到圆桌周围的人全部出列。

其数学推导公式为：f [n] = (f [n-1] + k)%n, n>1

随机数获取在获取数据的时候会用到约瑟夫环。我们随机规定系列的 n、k、m 值存放在区块链中，获取数据的请求带有使用第几个 n、k、m 值的索引，这个索引值是随机的，根据这个索引从当前区块里面去的这组 n、k、m 值，从而在随机队列中取得要获取的记录数。

约瑟夫环可以使取得的数据随机性更好，由于个人节点提供的真随机作为加密保存参数，可以保证即使知道了随机队列中的数据，也不能计算出本次请求到底会返回哪个记录。

3.5 **代币激励模型**

在联盟共治层上，加密世界联盟提供基础的 BC 交易记账服务，联盟成员提供成熟的网络和应用资源，每个区块链节点服务器可获取交易手续费收益。

假设S为每个区块所有交易的CWV总量，参与记账的节点一共分得U%（=0.01%，万分之一）个CWV。争得记账权的主节点M从中获得M%（=80%）奖励，其他节点如果完成80%确认，依次均分剩下的（1-M%）CWV。

具体计算公式为：$$P=\begin{cases} S*U*M & if from Master \\ S*U*\frac{(1-M)}{N}*80\% & if from follows \end{cases}$$

在合约执行层上，联盟成员节点以及其他满足一定计算能力的节点提供游戏合约执行的加速服务，每个游戏节点服务器可以获取游戏中的服务费和收益。

假设GameFees为游戏合约中规定的本次开局所能赚取的房间费，BonusRatio为游戏结束后的分红比例，但需要开局者先提供Allowance作为质押，若执行失败则扣除奖励给下一个合约执行者。

具体计算公式为：$$P=\begin{cases} -A & if throw errors \\ S*BR+GF & if game end \\ S*BR+GF+n*A & if game continues n times, n \geq 1 \end{cases}$$

4 代币发行计划

4.1 用途

为了激励加密世界的建设者和参与者，更好地推动整个数字世界的良性发展，加密世界将发行平台通行的原生 Token ——加密世界币 CWV，其用途包括但不限于：

1）购买资产：用户可以从官方平台购买加密世界中具有定价的资产，也可通过成熟的交易市场购买其他用户的资产。

2）购买物品：购买加密世界中游戏厅内的筹码，或者其他虚拟物品。

3）奖励回馈：对有贡献的用户和管理团队进行激励。

4.2 价值

加密世界币 CWV 是唯一在整个加密世界体系中都通行的 Token，作为一种支付媒介，对用户参与平台生态不可或缺。同时，随着加密世界用户数量增长，以及整个加密世界经济体系的持续发展，加密世界币 CWV 的价值也会相应提升。

4.3 获取方式

用户获取加密世界币 CWV 的方式包括但不限于：

1）参与私募支持加密世界项目，使用 ETH 兑换获取；

2）参与加密世界的经济体系建设，获取激励；

3）发布优质内容，获取其他用户的打赏；

4）从第三方交易平台买入；

4.4 代币分配方案与资金使用计划

本次发行 CWV 共计 100 亿枚，永不增发。具体分配比例如下：

1）私募发行：面向加密世界生态的早期投资者、主要参与者、行业合作伙伴、商业客户，分配比例占整体的 40%。根据参与的阶段不同，分为：早期基石 6%、基石 5%、早鸟 29%。私募发行部分仅面向特定购买者开放，筹集币种为 ETH，总值不超过 40,000 ETH。

2）基金会：用于奖励项目推进过程中不断加入的优秀人才及重要的合作伙伴为加密世界生态建设所做出的贡献，分配比例占整体的 20%。

3）研发团队：用于奖励研发团队和早期支持者，他们在加密世界的诞生和早期成长过程中的辛勤付出直接支撑起了整个生态构想与产品规划，因此将获得一部分 CWV 将作为回馈，分配比例占整体的 15%。研发团队部分包含锁仓承诺，本部分 CWV 将在预售结束后全部冻结，锁仓 24 个月。第一次解锁在募资完成的 3 个月后，其后每个季度解锁部分不超过团队持币总量的 12%。

4）项目运营：分配比例占整体的 25%。其中：

i. 战略发展和社区运营占 15%：将用于战略合作支持、组织管理、社区建设等，不断完善社区生态体系并推进加密世界整体发展

ii. 市场推广占 5%：将长期用于加密世界的媒体推广与社群运营

iii. 挖矿与节点奖励占 5%：将作为平台激励基金，针对个人用户挖矿以及联盟节点、游戏节点的早期构建，每天分配一定数额的 CWV 作为奖励。后期通过平台运营收益分成作为节点奖励。

代币分配方案

30% 产品研发
加密世界链开发/智能合约SDK优化及游戏开发/产品设计/专利研发等

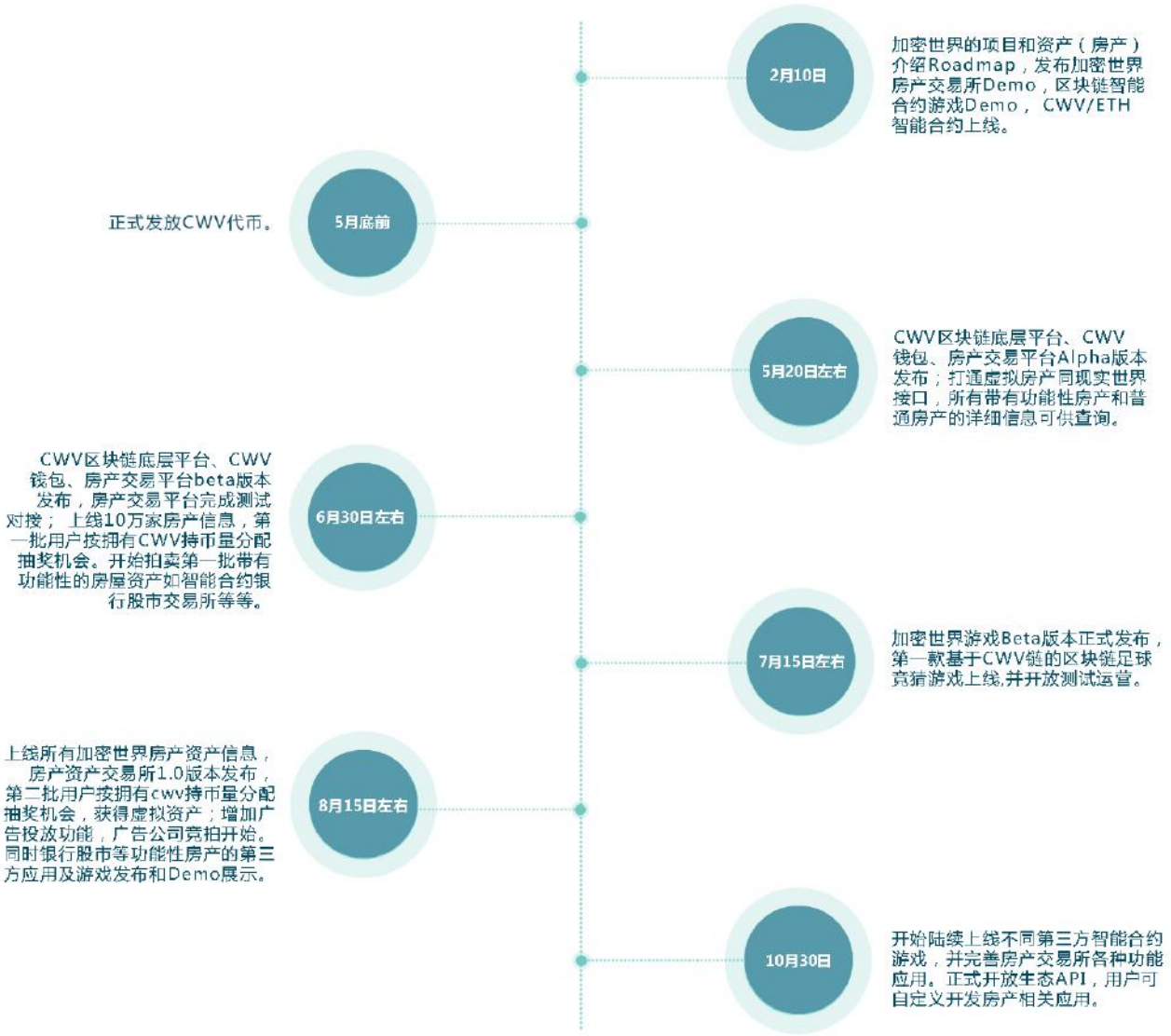
15% 运管管理
投入初期联盟链节点服务器及游戏服务器/公司运营

30% 商业发展
协助DApp商业化发展，最大限度挖掘其商业价值

15% 市场营销
搭建品牌/市场宣传/跨领域合作等营销活动

10% 风险备用
预备应对不可预知的各类风险

5 发展路线图


2月10日
加密世界的项目和资产（房产）介绍Roadmap，发布加密世界房产交易所Demo，区块链智能合约游戏Demo，CWV/ETH智能合约上线。
5月底前
正式发放CWV代币。
5月20日左右
CWV区块链底层平台、CWV钱包、房产交易平台Alpha版本发布；打通虚拟房产同现实世界接口，所有带有功能性房产和普通房产的详细信息可供查询。
6月30日左右
CWV区块链底层平台、CWV钱包、房产交易平台beta版本发布，房产交易平台完成测试对接； 上线10万家房产信息，第一批用户按拥有CWV持币量分配抽奖机会。开始拍卖第一批带有功能性的房屋资产如智能合约银行股市交易所等等。
7月15日左右
加密世界游戏Beta版本正式发布，第一款基于CWV链的区块链足球竞猜游戏上线,并开放测试运营。
8月15日左右
上线所有加密世界房产资产信息，房产资产交易所1.0版本发布，第二批用户按拥有cwv持币量分配抽奖机会，获得虚拟资产；增加广告投放功能，广告公司竞拍开始。同时银行股市等功能性房产的第三方应用及游戏发布和Demo展示。
10月30日
开始陆续上线不同第三方智能合约游戏，并完善房产交易所各种功能应用。正式开放生态API，用户可自定义开发房产相关应用。

6 治理架构

6.1 设立基金会

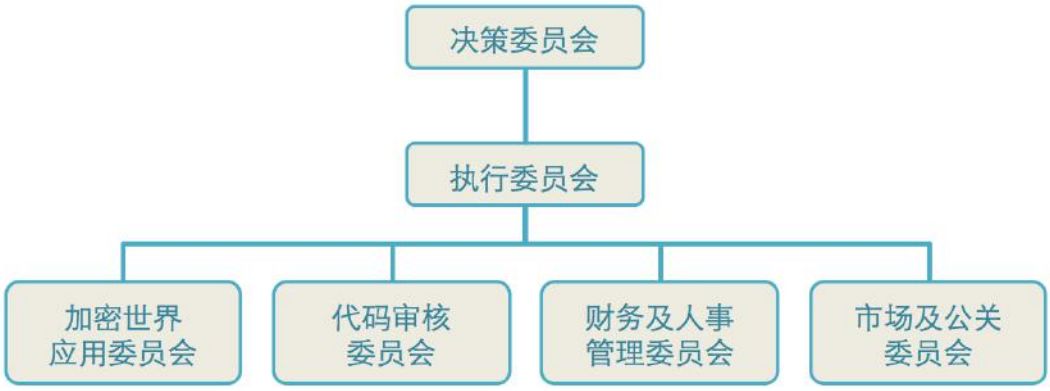
为更好地实现国际化的战略目标，同时考虑到政策法规方面的需要以及日常运营管理的效率，加密世界的决策及管理主体——加密世界国际基金会 CryptoWorld Foundation（以下简称“基金会”）将会设立在新加坡。基金会将致力于加密世界平台的系统开发工作与透明治理建设，以保证项目在最大程度上按照既定的计划推进，同时促进开源生态体系的安全、和谐发展。

6.2 基金会治理架构

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，由决策委员会、执行委员会及 4 个基层委员会组成。

决策委员会是基金会的最高决策机关，负责进行项目方向性的重大决策并统筹协调项目整体运营。首届决策委员会由 5 名核心创始成员组成，任期 4 年。5 名成员在区块链领域具有丰富的工作经验与独到的行业洞察，有能力在十分关键的项目初期高效地建立起初步生态体系，为项目的后续发展打下坚实基础。首届决策委员会任期届满后，由社区根据各用户持有加密世界 CWV Token 的份额和年限，按照一定权重综合计算，选举出 50 名社区代表，再从这 50 名社区代表中最终选举产生 5 名第二届决策委员会成员，以此类推。

对于项目日常运营管理，将由执行委员会代为行使决策权。执行委员会下辖加密世界应用委员会、代码审核委员会、财务及人事管理委员会以及市场及公关委员会，这 4 个基层委员会分工合作、相互配合，保证项目日常运营管理的效率，共同推进项目的安全高效发展。



6.3 交易安全及财务审计

1）交易安全

用户交易安全对加密世界的健康、可持续发展至关重要，基金会将给予最高优先级的重视。加密世界将通过区块链共识、智能合约等底层技术及数字签名、终端用户加密钱包等安全手段确保用户账户及资金安全；完成数据存储、网络、平台等资源的高效整合，将数据、应用、交易等各个组成部分集成到加密世界公链中，提供金融级安全保障；与最受信任的第三方交易平台和技术专家合作，携手构建并不断优化安全交易网络环境。

2）财务审计

基金会及其成员承诺恪守商业行为准则与社会道德规范，遵守相关法律法规及行业自律原则，时刻以最高标准要求自身。同时，基金会将定期邀请国际知名第三方审计机构对资金使用、成本支出、利润分配等情况进行审计和评估，并充分公开审计和评估结果，最大限度保障早期投资机构、个人投资者、平台用户、合作机构以及其他利益相关方的知情权与商业利益。

7 团队与合作伙伴

7.1 核心团队

James Sung CEO

James是一名美籍台湾的资深市场营销专家，同时也是央视评论员。拥有十年以上中美及全球市场运营经验，曾多次受邀CCTV，CNBC分享营销经验，与全球知名媒体CNN，BBC，TechCrunch等视频和网络媒体分享报道并发展合作关系。他在跨境贸易、技术营销和公共关系管理方面有着18年的经验。他拥有国际化的视角，曾在50多个国家开展业务，与一些创业公司和腾讯、T-Mobile等财富500强公司都曾合有过合作。

Denis Kaizer CTO

Denis 是拥有超过7年的开发经验的Dapp架构师、Solidity编程语言专家。早期区块链技术爱好者，多次公开演讲、参与编程马拉松评审。Denis是国际Solidity编程语言社区知名的开发者，俄罗斯区块链技术社区的领头者之一。曾参与多个国际区块链项目，开发智能合约，设计代币经济模型。发表学术文章《去中心化的Oracle网络声誉评估系统》将于2018年夏天刊登。编程马拉松大赛获奖经历包括：加拿大ETHWaterloo 2017的获胜者之一，ETHWaterloo是由以太坊基金会举办的基于以太坊的编码马拉松大赛，获得以太坊创始人Vitalik Buterin和Storj所颁奖项；获得Qtum举办2017 Blockchainhack Russia比赛优胜。

Noah Zerkin 首席科学家

美国资深技术专家，长期专注于嵌入式平台、惯性传感器、空间数据参照和分析；新颖用户交互设计的操作计算系统。曾为美国宇航局NASA工作，为其设计了大量的行为照明装置，发明了虚拟现实接口技术专利，设计了用户医疗领域研究设备的原型，并为美国宇航局成功设计了飞行模拟器。

Alex He

Alex在软件开发和项目管理方面有着15年的经验，完成过多个企业级大型项目。他是一名全栈开发员和架构师，专长于Linux, Oracle数据库和现代网络服务构架。Alex也是一位PMP认证的项目经理。
Alex拥有新加坡国立大学的电气工程师学士学位和计算机研究生学位。

Tim Harvie

Tim是一位经验丰富的市场营销、管理专家，拥有多年的国际市场和组织领导经验，对于亚太市场拥有超过三年的积累。2016年起接触数字货币的买卖与管理，积累了北美数字货币市场营销经验。Tim专注于公司各部门的联通与整体运营，确保项目按计划与预算顺利执行；对用户市场拥有极高的敏感度，通过对其数据的分析，确定公司产品与服务的需求，计划、领导产品的优化与开发。他善于通过与技术部门的直接协作，推动了公司应用项目的发展。

7.2 早期基石投资人

玉红

SeeU & QYGAME 创始人，区块链三点钟发起人。2008年创办趣游，2013年出售给360，后任360高级副总裁。2015年创办QYGAME，2016年创办SEEU短视频社交平台；投资方面，2010年天使投资了天神娱乐，已在A股上市，目前市值190+亿；早起参与投资了七酷网络，于2014年与上市公司世纪华通完成重组实现上市。

Neo Wang

Neo Wang拥有超过14年互联网经验，知名连续创业者与天使投资人，曾就读于德国明斯特FH Muenster大学。参与创立并服务于国内知名智能穿戴硬件、消费升级设备、电子音乐垂直网站、社交网络、团购网站等创业项目。在中国移动互联网、大数据、人工智能及物联网领域有着深厚的人脉，并获得国内外诸多媒体和业内的认可，被科技媒体联合评为2013青年创想家、美国格理集团智能穿戴领域专家。

Roy Li

著名的安全专家和物联网专家，物联网操作系统Ruff.io创始人，区块链三点钟联合发起人，复旦大学硕士生导师。Ruff.io是有极客创始人出资，景林资本和山行资本联合投资。

Grace Fan

BrinkAsset CEO，RUFF体系BD负责人。互联网连续创业者，有多年产品销售与市场推广经验。物联网区块链深度爱好者，负责多个物联运营项目。加拿大不列颠哥伦比亚理工大学工商管理系。

林坦

毕业于Rose-Hulman Institute of Technology，曾就职于Amazon，Google(Kifi)，前互利科技CEO，现策源创投VP。

程野

Consensus Capital共识资本管理合伙人，曾投资过uber，唱吧，凡普金科等企业。

李媛媛

链氪资本创始人，CEO，聚焦区块链投资孵化，深度整合国内及海外优质区块链资源，探索区块链技术应用。目前投资的项目包括Vechain、Ruffchain、Alphacat、Crypterium、Qash、Ddex、Sot、Intchain、Comsa、Dta、Ether delta、Bnktothefuture、Aichain、Red、Iost、Fluz、Penta等项目。

7.3 顾问

王峰

火星财经发起人，蓝港互动集团（HK.8267）创始人，极客帮创投合伙人，曾任金山软件高级副总裁。他一手创办的区块链先锋门户火星财经上线仅26天，获A轮融资，估值1.5亿元；打造王牌栏目《王峰十问》对话薛蛮子、帅初、曾鸣、陈伟星、朱啸虎等行业意见领袖，成为2018年初现象级传播事件。他拥有逾20年的互联网从业经验，曾获《财富》“中国 50 位商业先锋”等荣誉。

蒋波

长岭资本的合伙人。2012年任思颐投资(NEA)执行董事管理在华投资。曾任阿里巴巴集团产品和技术管理重要职位，组建了支付宝的移动支付团队；管理雅虎中国所有通讯及社区类产品宾夕法尼亚大学沃顿商学院MBA学位Palmer Scholar荣誉获得者，清华大学计算机学士学位。

王斗

极客资本创始人，区块链机器人发明人。技术极客，社群运营家。曾在IBM，摩托罗拉，惠普和硅谷高科技公司担任总监十余年。在加拿大教授互联网技术和数字货币，并参与投资多个数字货币项目。

李岩

李岩 国内最大自媒体联盟Wemedia创始人CEO，福布斯三十岁以下创业人物，北京创业领军人才。

孔华威

致公党员，高级工程师 中科院计算所上海分所所长，起点资本合伙人。曾任张江科投首席科学家、曙光信息产业集团VP等，是科技部火炬创业导师，发起ITALK沙龙、IC咖啡等创新组织，上海大数据产业联盟秘书长，参与投资芯原微电子、七牛云存储、中晟光电、睿励科仪、黑子科技、鸢鼎信息等。

高阳(Sunny)

SegmentFault思否 CEO，思否区块链技术社区创始人，中国最大的黑客马拉松组织者，杭州青年企业家协会唯一的 90 后理事会员，中国 90 后青年企业家社群发起人，2014 年入选福布斯中国 30U30 创业者。中国第一家天使投资平台 AngelCrunch 创始成员，超过 10 年互联网行业创业、投资、媒体、游戏等跨界的从业经验。

7.4 投资机构

7.5 合作伙伴

8 风险提示与免责声明

8.1 风险提示

政策风险 截至本白皮书上线，各国政府均尚未出台一套完整的针对区块链项目及 ICO 融资方式的法律体系，未来不能完全排除各国明令禁止 ICO 融资的可能性，由此可能导致投资者出现损失。

监管风险 截至本白皮书上线，数字资产交易领域尚不存在强有力的监管主体，对于欺诈、恶意操控、散布虚假信息等违背商业道德的行为尚不存在处罚条例，请投资人在了解目前投资者保护措施尚不完善的基础上进行投资决策。

市场风险 数字资产市场整体被高估会导致投资风险的加大，请投资人谨慎决定是否投资，同时避免设定过高的期望回报。此外，在市场整体低迷时，也可能出现即使项目推进顺利，加密世界在代币价格上依然被低估的情况。

技术风险 区块链、分布式账本、去中心化、不同意篡改等底层基础技术的顺利成长构成加密世界核心业务发展的前提，目前不能完全排除上述技术在未来发展过程中因达不到预期而无法落地，或遭受黑客攻击而被证明存在根本缺陷等情况的可能性。

竞争风险 当前区块链领域项目众多，市场竞争压力巨大。加密世界团队会尽最大努力推进开发，尽早从诸多项目中脱颖而出，但也可能受到市场上恶性竞争的影响，导致项目推进受阻。

安全风险 本次筹资金额大，加之电子代币的匿名性、不可追溯性等特性，容易成为不法分子的犯罪目标，目前不能完全排除受到黑客攻击，或涉及非法资产转移等犯罪行为的可能性。同时，目前无法准确预估量子计算机的发展，未来可能出现因计算机性能激增使密码破解能力大幅提升，而导致加密世界币丢失的情况。

统筹风险 加密世界汇聚了一支热情、实力与经验兼备的人才队伍，但在未来不排除核心成员离开、团队内部发生冲突而使加密世界的开发工作受阻的可能性。

发展风险 目前尚不能对加密世界平台是否能获得大量个人或组织的认可及参与作出承诺，公众及外界开发人员对发展相关分布式应用的兴趣会影响平台的发展。

其他风险 随着区块链技术与虚拟货币行业的发展及项目开发的推进，加密世界可能面临目前尚无法预料的不确定性风险。本项目团队会尽最大努力规避或应对，但无法保证这些风险不会对本项目造成影响。

8.2 免责声明

文档性质 本白皮书仅作为传达信息之用，文档内容仅供参考，不构成任何投资买卖建议、邀约或教唆，不构成任何合约或承诺，团队对未来可能出现的任何投资损失概不负责。

代币性质 加密世界币是平台发挥效能的工具，并非投资品，团队并未作出任何增值承诺。投资者拥有加密世界币不代表被授予平台的所有权、控制权或决策权，不具有任何形式的法律约束效力。

投资前提 加密世界平台默认参与的投资者已达到年龄标准，具备完整的民事行为能力，已充分了解本项目及投资环境可能存在的风险，签订的合同基于自愿原则并且真实有效。加密世界对投资者因违背上述事项而发生的问题概不负责。

信息更新 本白皮书涉及的行业分析数据等来源于互联网，仅供参考之用，不保证准确性与实时性；涉及的项目内容可能会随着项目的推进而不定时更新，本项目团队届时将通过在网站上发布公告或上线新版白皮书等形式将更新内容公布于众，投资者自行承担因未能获得最新信息而可能造成的任何后果。