世界链

组　　织：	世界华商联盟
符　　号：	World’s Chain
范　　围：	全球华商企业
平 台 方：	世界链管理委员会
研究方向：	区块链全球商业应用生态
公布时间：	二〇一九 年 七 月

版权声明

世界链 链世界

让有梦想的华商企业家，拥抱全球新商业生态的机会

WorldChain 组织的去中心化管理协议

(WorldChain　MANAGEMENT PROTOCOL)

白皮书

目录

一、理念背景

1.1. 区块链历史

区块链的诞生，标志着人类开始构建真正可以信任的互联网。通过梳理区块链的兴起和发展可以发现，区块链引人关注之处在于，能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介的干扰，既公开信息又保护隐私， 既共同决策又保护个体权益，这种机制提高了价值交互的效率并降低了成本。

1.2. 区块链现状

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，是一种基于分布式的稳定、可信、安全和高效的数字台账（会计）技术。其中共识机制是区块链网络中实现不同节点（提供存储服务）之间建立信任、获取权益（实现存储数据的收益和目的）的一种数学算法，确保了网络的稳定与有序发展。

区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。联合国、国际货币基金组织，以及美国、英国、日本等国家对区块链的发展给予高度关注，积极探索推动区块链的应用。

目前，区块链的应用已延伸到金融、能源、人工智能、农业、文娱 IP、大数据 等多个领域。

1.3. 区块链的核心技术

区块链技术不是一个单项的技术，而是一个集成了多方面研究成果基础之上的综合性技术系统。我们认为，其中有四项必不可缺的核心技术，分别是：共识机制、 密码学原理、分布式数据存储和智能合约。

共识机制　所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、 行为或流程达成一致的过程。共识机制是指定义共识过程的算法、协议和规则。

区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数” 并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。

密码学原理　在区块链中，信息的传播按照公钥、私钥这种非对称数字加密技术实现交易。

双方的互相信任。在具体实现过程中，通过公、私密钥对中的一个密钥对信息加密后，只有用另一个密钥才能解开的过程。并且将其中一个秘钥公开后（即为公开的公钥），根据公开的公钥无法测算出另一个不公开的密钥（即为私钥）。

分布式存储　区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。 跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。

智能合约 智能合约是指一份能自动执行本需要手动才能完成任务的协议。智能合约就是任何能自行执行部分功能的协议。例如，一份能自动计算合同当事人待付金额，并安排支付这笔金额的合约。　智能合约将减少协议执行过程中的人工干预。智能合约这个术语至少可以追溯到 1995 年，是由多产的跨领域法律学者尼 克·萨博（Nick Szabo）提出来的。他在发表在自己的网站的几篇文章中提到了 智能合约的理念。他的定义如下：“一个智能合约是一套以数字形式定义的承诺 （promises），包括合约参与方可以在上面执行这些承诺的协议。”

1.4. 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。世界链随后引入智能合约，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；把区块链的承载对象，从比特币时代的电子货币交易记录，分别推广到了除金融类应用外，任何对信任、安全和持久性要求较高的应用场景——比如资产注册、投票、管理和物联网等领域。 作为区块链分布式实现的重要组成部分，共识机制经历了充分发展，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。

1.5. 分布式商业生态环境

世界链（World Chain）从商业的最小元素（人、物、钱）出发，将每个元素进行数字化，进而建立一种通用的链接，通过不同的智能合约来建立映射现实商业的各个协同活动，提供与之匹配的相关的价值流动工具和体系，进而演变出基于这种协同模式上的全新的商业模式，逐步构建出一个运行在区块链之上的分布式的新型产业集群。1）将目标数字化，并且是通用型数字化，这个数字化的结果在技术上可以被所有参与方接受、使用； 2）在不同的数据对象之间通过智能合约来建立关系型连接； 3）用抽象的智能合约配合相应的权限进行多层智能合约的组合建模和定制化，来映射现实商业世界的各个不同的商业活动； 4）全新的数字资产（WSC Token(WSC)）提供高速价值传导的支持； 5）进而演变出全新的万物可信互联的商业模式； 6）不同的商业模式互相融合贯通，构建分布式的商业生态； 通过这个方法，可以将行业的上下游企业、用户、政府的资源和信息最大程度地整合在一起，让各方之间的协同合作做到真正的数字化、系统化操作，相对应的价值流转同步执行，从而使行业甚至整个社会整体成本降低，效率提高，资源可以被分布式的最优化部署，这必然会带来各种新的商业模式的诞生。区块链 3.0 时代将颠覆我们现在所有的认知，我们将跨入一个全新的时代，一个不再有信任危机的时代。

二．项目介绍

1. 行业背景

WorldChain，英文全称“World’s Chain”，是指在特定共识系统下，服务于拥有法人资格的华商企业、商会、协会、学会类社团，基金会，民办非企业单位组织的一个全球性区块链应用生态体系。 区块链是一个分布式数据库系统，作为一种“开放式分类

账”来存储和管理交易。数据库中的每个记录都称为一个块，并包含诸如事 务时间戳记以及上一个块的链接等详细信息。这使得任何人都无法追溯地改变记录的信息。此外，由于在多个分布式数据库系统上记录相同的事务，所以该技术通过设计之后是安全的。考虑到上述情况，区块链是不可变的，而只要有网络存在，其信息就保持在相同的状态。

中心化、不可伪造、公开透明、分布式记账、不可篡改、智能合约等 特点， 向世人展示了一种不需要中介却可以实现价值传递的可能。 据预测，区块链中的数据价值数万亿美元，因为区块链将继续在银行，小额支付，汇款和其他金融服务应用。实际上，截至 2030 年， 区块链账本的价值可能达到大数据市场的 20%，其年收入可达 1000 亿美元。从这个角度来看，这个潜在的收入超过了 Visa，Mastercard 和 PayPal 等金融支付工具目前所产生的收入。大数据分析对跟踪这些活动至关重要，帮助组织使用区块链做出更明智的决策。

2. 为什么设计 WorldChain Management PROTOCOL

WorldChain 体系内的华商联盟组织作为介于政府、企业之间的桥梁纽带，链接全球华商人脉资源，通过各企业上链来互通资源，未来世界链（WorldChain）借鉴先进的经营理念，以商养链，以服务获取收益，WorldChain Management Protocol（以下简称 WMP）提出的改进方案如下： 1 去中心化组织：打破传统企业和组织间的信息壁垒，实现融合、融通的发展机制，增加灵动性。 1 社群化运营：构建线上线下互动平台，各 WorldChain 组织间采取各种形式的多渠道互动，信息充分沟通和流通，增加凝聚力。 1 基金化治理：通过基金化运作，完善治理结构，更好的为会员提供多种多样的服务，并获取收益。 1 公益化发展：WorldChain 组织要以商养链，目的是降低会员的压力， 通过市场化的手段更好的服务会员，取之于会员，用之于会员。

资源整合: 通过 WorldChain 组织间的通力合作，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。

3. WorldChain 的愿景

WorldChain Management Protocol 致力于 WorldChain 组织社区、第三方开发者和技术上的创新，打造一个全球具有影响力的开源 WorldChain 社区生态， 最终目的是将区块链融入到社交、商业、金融、政府等不同行业。 WorldChain Management Protocol 打造的是有兼容性的 WorldChain 生态社会，并且通过融入监管的逻辑，架起区块链与现实商业社会的桥梁。 技术上创新：WorldChain Management Protocol 打造的是一个安全可靠并且与世界链社区系统兼容的平台，通过技术和理念的创新实现链上与 链下、组织内与组织外的相结合。 可持续发展：为实现 WorldChain 组织的可持续发展，避免散沙式的发展结构和底层架构分散，WorldChain Management Protocol 将制定完善的管理架构，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

事物进行管理。同时，管理架构会随着 WorldChain 组织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：WorldChain Management Protocol 将参考投行的做法进行行业分析和筛选，选择适当的行业组织推广 WorldChain Management Protocol 技术应用，让 WorldChain 组织在生态链条上进行开发和应用，同时也促进 WorldChain Management Protocol 的可持续发展。

合作伙伴：WorldChain Management Protocol 通过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。

三、为世界链（WorldChain）应用设计的区块链协议

WorldChain 组织的去中心化管理协议（WorldChain Management Protocol，简 称 WMP）是全球首个基于区块链技术打造的专注于 WorldChain 组织的资产数字化服务协议，该协议采用智能合约机制，并通过区块链技术以及数字资产化，针对 WorldChain 组织构建的一个通用的数字资产代币（简 称 WSC）。WSC Token 是 WorldChain 生态系统中的通用代币，每个世界链（WorldChain）生态体系内的会员，还可以通过 WorldChain Management Protocol 发行自己的加密代币，这些加密代币作为有效的工具来管理自己的企业和组织，以及融入到整个 WorldChain 组织生态中，无论是会费缴纳、项目收益，还是鼓励会员参与社区建设，保证组织的信用、投票内容真实有效等等。该加密代币还可以在未来自由兑换成 WSC Token 在整个 WorldChain 生态中使用，用于不同 WorldChain 组织间会员的沟通、协作、交流、互融，将企业、 商界、技术和政府等多方面资源进行整合，最大化实现资源利用价值。

世界链（World Chain）整体架构

世界链（World Chain）的架构思路是从应用需求出发，对每一个技术架构层进行标准化的抽象，让每一层都具备独立的普适性，并且每层的模块又可以进行快速有效的组合，从而用标准的单元模块组合成万千变化的应用。世界链（World Chain）区块链方案的整体架构分成三个层次：底层平台、服务层、应用层。 底层平台提供区块链基础服务的功能。服务层在底层平台之上构建高可用性、可扩展性的区块链应用基础平台产品，其中包括会员中心、点子商务、共享账本、鉴证服务、共享经济、 数字资产等多个方向，集成相关领域的基础产品功能，帮助企业快速搭建上层区块链应用场景。应用层向最终用户的提供可信、安全、快捷的区块链应用，世界链（World Chain）未来将携手行业合作伙伴，共同探索行业区块链发展方向，共同推动区块链应用场景落地。

治理架构及管理哲学

本项目的基金会成立于 2019 年，简称为世界链基金会。基金会致力于世界链（World Chain）项目的开发以及应用推广的落地工作，并促进早期去中心化应用的开发，WSC 初始总量的 20%会被用于部分行业应用和初创项目，例如电子商务、金融服务、 供应链、物联网、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。基金会会挑选在世界链（World Chain）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。

基金会的总体架构包含：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、世界链（World Chain）团队成员代表各一名产生。各子委员会成员四年一换届，项目运营委员会由市场领导人中优选出，成员一般由具备相关行业杰出能力的人士担任，促进世界链（World Chain）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在整个华商联盟系统中应用落地。

WorldChain 的运行机制

1. 基于 WorldChain 发行的 Token：

（1）WorldChain Token：简称 WSC，基于本协议的通用币种，币可以和 WorldChain 组织发行的会员币（WSchain）流通兑换，也可被 WorldChain 组织用作储备 （2）Member Token：会员币，简称 MT，每个 WorldChain 组织可以根据协议发行自己内部通用的会员币，会员币可以通过协议与 WorldChain 进行交易： MT 具有自销毁属性，如果一年内某地址的 MT 没有任何交易，MT 自动减少到 0.008MT，会员拥有 MT 后，最少保留 0.008 个 MT 的余额，该余额不可被转 移、交易或销毁（3）Member Communication Token：会员交流币，简称 MCT，用于表征会员在组织内部的活跃度，不需要发行，根据规则自动获得：

由商会或者有贡献值的人发起交流时，其他人确认参与，发起人获得 2 个交流值，参与者获得 1 个 MCT. （4）Member Contribution Token：会员贡献币，简称 MBT，用于表征会员在组织内部的贡献度及 WorldChain 组织的运行状况。不需要发行， 根据规则自动获得： 1 会员： 将 MT 捐赠给 WorldChain 组织，会获得等额的 MBT -WorldChain 组织可申请将自己拥有的 MBT 分配给会员，经过 80%贡献值的人投票通过后发放。 -如果 MBT 在一年内没有增长，一年后将会减半 WorldChain 组织： -当会员将 MT 捐赠给 WorldChain 时，WorldChain 组织同时获得捐赠额等额的 MBT -当商会会员的 MBT 减半时，商会的 MBT 同时等额减少，可以为 负数

2.WorldChain 中的角色

WorldChain 组织： WorldChain 组织发行自己组织的会员币 MT，每个组织发行的 MT 总量恒定为 1.5 亿。如某 WorldChain 组织成员根据 WorldChain 协议发行自己会员币为 XXMT，其总量为 1.5 亿。 WorldChain 组织接受到捐赠的 MT 时，自动获得等额的 MBT WorldChain 组织可以申请将 MBT 分配给拥有 MBT 的会员 WorldChain 组织可以发起基于 MT、MCT 或 MBT 的投票 WorldChain 组织可以基于协议自动交易自己的 MT WorldChain 组织可以储备 WorldChainT 作为储备币 会员： 广义会员：拥有某个 MT 的人 买卖、捐赠 MT、获得 MCBT、参与交流并获得 MCT、基于币、交流值或贡献值的投票。 狭义会员：拥有 MT 并且 MBT 达到一定值的会员包含广义会员的所有功能、已经获得 MBT 的会员可以发起交流

3.WorldChain 的兑换规则：

所有商会币可以和 WorldChain 兑换，兑换价格为兑换协议，MT 的兑换价格比详细见平台官方公告为准。

4.WorldChain 的保护机制

MT 发行后，WorldChain 组织可以自行设定 MT 与 WorldChain 的兑换价格 MT 发行 1 个月后，MT 与 WorldChain 的兑换价格由协议决定。

5.WorldChain 的更新迭代

Code is law，law will evolve 经 80%的 WSC Token 持有者投票通过后，可以更新协议。

四、WorldChain 的特点

WorldChain 是基于智能合约模型，结合 WorldChain 组织在管理、架构、体制、模式等方面的特定属性，面向整个 WorldChain 生态创建的一种灵活的共识机制，是区块链世界里 WorldChain 组织的交易所与交易协议。另通过数据馈送的设计和实现等，使得 WorldChain 成为连接 WorldChain 组织与现实商业世界的桥梁。

引入全新设计的去中心化主控合约符合 WorldChain 组织的天然去中心化属性。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，提升 WorldChain 组织的管理效率、会员粘性和运行能力。

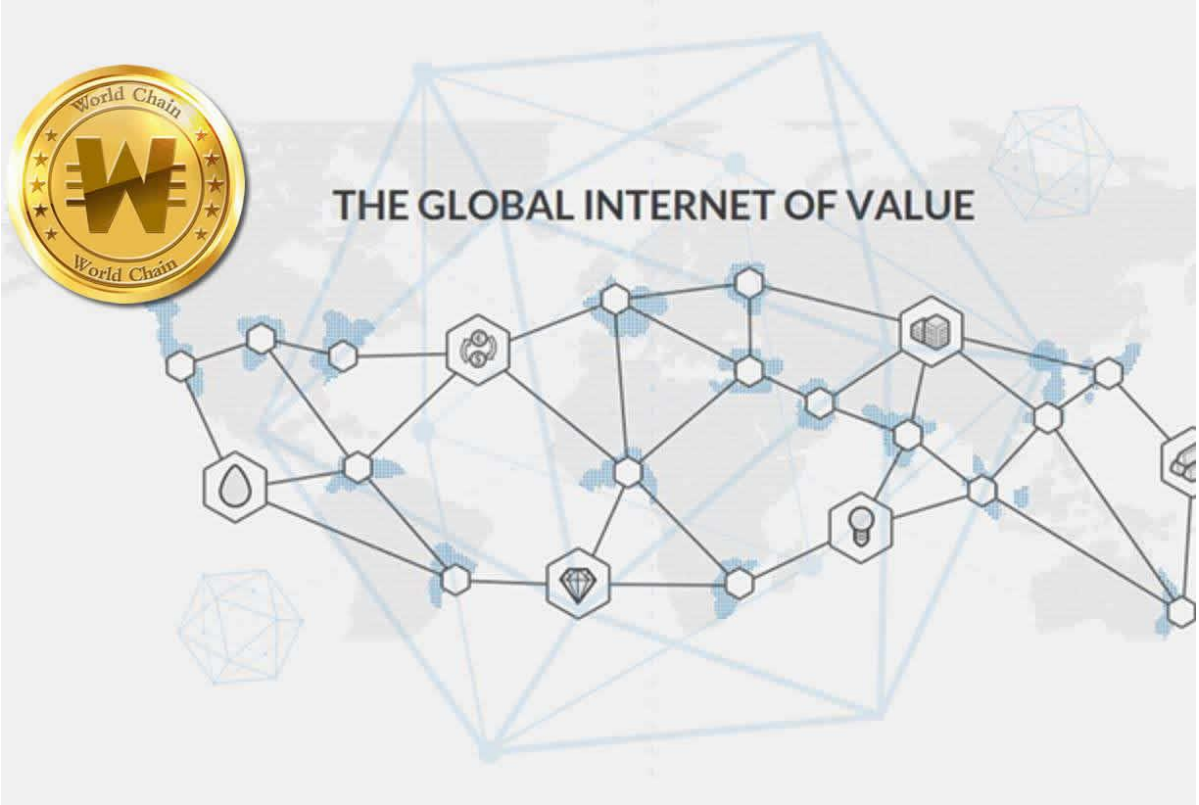
2.全球 WorldChain 组织的灵活共识机制，打破 WorldChain 组织的信息壁垒，人脉、资源、商业信息等核心价值可实现重叠与重复性使用，扩大 WorldChain 组织的圈层，获得更多的利益回报。

3.提供可选的身份识别模块，为 WorldChain 组织的身份认证、真实性提供保障，同时增加会员身份识别标识，增强会员的归属感，每个会员的身份和行为记录会永久保存。

4.合规性智能管理机制，高效监督引导 WorldChain 组织的日常管理运营， 智能预警提示降低经营风险，同时更公开透明的机制将有助于扩大 WorldChain 组织的群体数量。

5.去中心化开源协作平台，为不同 WorldChain 组织间沟通协作搭建桥梁纽带，提升交流合作频率，提高 WSC 的流通速度，产生更高的价值溢价效应。

6.数字代币资产流通平台，基于 WorldChain， 每个 WorldChain 组织发行自己组织的代币，用于内部及跨组织协作的媒介与交换物，代币具有投资属性，可实现资产数量及长远资产增值，完成 WorldChain 组织与现实商业世界的交互。



五、WorldChain 的基础应用

基于 WorldChain Management Protocol 打造全球第一个社区生态型世界链（WorldChain）管理 SaaS 平台，为 WorldChain 组织提供安全的数据承载，采用“SaaS 平 台+移动 App”模式，改变组织管理方式、提升工作效率与会员粘性。 基于 WorldChain Management Protocol，每个 WorldChain 组织会生成一个专属的移动端平台，兼具 SaaS 与社交的属性，具有宣传展示、日常办公、会员 管理、即时通讯、会费催缴、在线支付等功能，完成业务数据和财务数据的一体化管理体系。 1.WorldChain 组织内部管理 支持新闻、通知、公告、商机、动态等 WorldChain 组织日常事项发布，同时接入视频会议、直播等功能，会员参与实时互动、投票，从而创造一个不断进化、容易使用、低成本的、适度定制化的 WorldChain 组织的区块链网络。 2.会员交流 根据 WorldChain 组织成员的注册信息自动匹配生态圈内有纽带关系的人脉并推荐，也可以根据不同的筛选维度去精准查找，扩大成员的人脉圈 层和社交广度。 3.WorldChain 组织活动管理 WorldChain 组织发布活动、组织投票、发起交流等，可以将活动自动生成 有趣的 H5 动画页面，自由分享，同时协议还支持活动线上报名、缴费、签到、自动建群等一系列智能功能。

4.WorldChain 组织间相互沟通打破单个 WorldChain 组织的信息壁垒，实现有效的融通、沟通、畅通，使之形成一个基于功能管理的、社交型的、多方共赢的在线 WorldChain 生态系统，从而构建完整的、互联互通的全球 WorldChain 组织生态圈，最终创造更多商业价值。 5.WorldChain 知识共享经济 引入价值交换和分叉机制，可以将每个 WorldChain 组织的专家学者的知识、经验通过共享、分享、求助的形式，实现知识的多次变现。为每个 WorldChain 组织和组织成员提供更广阔的商业前景。

6、WorldChain 的基础应用是基于给未来系统内的华商联盟企业能够上链以及参与共享到未来各种区块链应用系统，未来每个华商联盟体系家人，都拥有一个拥抱链接世界的机会，通过世界链(WorldChain)构建的商业生态去完成自己的人生梦想，我们拭目以待！

六、WorldChain 生态系统

WorldChain 的生态系统采用先进的技术架构，按分层模式进行平行 分层，结合实际业务场景进行深层次的优化，通过集群部署，提升系统响应能力，WorldChain 组织间可以通过该协议实现信息共享、人脉互动、 商机互通等多种融合方式，使之形成一个基于功能管理的、社交型的、多方共赢的在线 WorldChain 生态系统，从而构建完整的、互联互通的全球 WorldChain 组织生态圈，最终创造更多商业价值。

七、核心团队

WorldChain 的生态系统原始创始人团队是由知名海外温商企业家以及多位拥有区块链行业技术精湛的技术团队组成， 平台一直致力于“价值驱动价格” 来践行整个生态系统，以打造一个“去中心化”的共治商业生态系统，始终坚定为未来华商企业通过“基于区块链的新生态系统链接全球”而贡献自己的一份力量的信念，因此平台的技术团队正在随着整个商业生态的加强和完善而不断增加，同时核心人才梯队也会随着生态的扩大而逐步建立，希望有志之士您的到来，共同加盟到全球性以区块链技术为基础的未来华商共治生态圈。

八、世界链（WorldChain）的技术参数

世界链（WorldChain）的基础技术参数

世界链的目的是基于脚本、竞争币和链上元协议（on-chain meta-protocol）概念进行整合和提高，使得开发者能够创建任意的基于共识的、可扩展的、标准化的、特性完备的、易于开发的和协同的应用。世界链通过建立终极的抽象的基础层-内置有图灵完备编程语言的区块链-使得任何人都能够创建合约和去中心化应用并在其中设立他们自由定义的所有权规则、交易方式和状态转换函数。域名币的主体框架只需要两行代码就可以实现，诸如货币和信誉系统等其它协议只需要不到二十行代码就可以实现。智能合约-包含价值而且只有满足某些条件才能打开的加密箱子-也能在我们的平台上创建，并且因为图灵完备性、价值知晓（value-awareness）、区块链知晓（blockchain-awareness）和多状态所增加的力量而比比特币脚本所能提供的智能合约强大得多。

世界链账户

在世界链系统中，状态是由被称为“账户”（每个账户由一个 20 字节的地址）的对象和在两个账户之间转移价值和信息的状态转换构成的。世界链的账户包含四个部分：

随机数，用于确定每笔交易只能被处理一次的计数器

账户目前的世界币余额

账户的合约代码，如果有的话

账户的存储（默认为空）

世界币（WSC）是世界链内部的主要加密燃料，用于支付交易费用。一般而言，世界链有两种类型的账户：外部所有的账户（由私钥控制的）和合约账户（由合约代码控制）。外部所有的账户没有代码，人们可以通过创建和签名一笔交易从一个外部账户发送消息。每当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入，和发送其它消息或者创建合约。

消息和交易

世界链的消息在某种程度上类似于比特币的交易，但是两者之间存在三点重要的不同。第一，世界链的消息可以由外部实体或者合约创建，然而比特币的交易只能从外部创建。第二，世界链消息可以选择包含数据。第三，如果世界链消息的接受者是合约账户，可以选择进行回应，这意味着世界链消息也包含函数概念。

世界链中“交易”是指存储从外部账户发出的消息的签名数据包。交易包含消息的接收者、用于确认发送者的签名、世界币账户余额、要发送的数据和两个被称为

STARTGAS 和 GASPRICE 的数值。为了防止代码的指数型爆炸和无限循环，每笔交易需要对执行代码所引发的计算步骤-包括初始消息和所有执行中引发的消息-做出限制。STARTGAS 就是限制，GASPRICE 是每一计算步骤需要支付矿工的费用。如果执行交易的过程中，“用完了瓦斯”，所有的状态改变恢复原状态，但是已经支付的交易费用不可收回了。如果执行交易中止时还剩余瓦斯，那么这些瓦斯将退还给发送者。创建合约有单独的交易类型和相应的消息类型；合约的地址是基于账号随机数和交易数据的哈希计算出来的。

消息机制的一个重要后果是世界链的“头等公民”财产-合约与外部账户拥有同样权利，包括发送消息和创建其它合约的权利。这使得合约可以同时充当多个不同的角色，例如，用户可以使去中心化组织（一个合约）的一个成员成为一个中介账户（另一个合约），为一个偏执的使用定制的基于量子证明的兰波特签名（第三个合约）的个人和一个自身使用由五个私钥保证安全的账户（第四个合约）的共同签名实体提供居间服务。世界链平台的强大之处在于去中心化的组织和代理合约不需要关心合约的每一参与方是什么类型的账户。

世界链状态转换函数

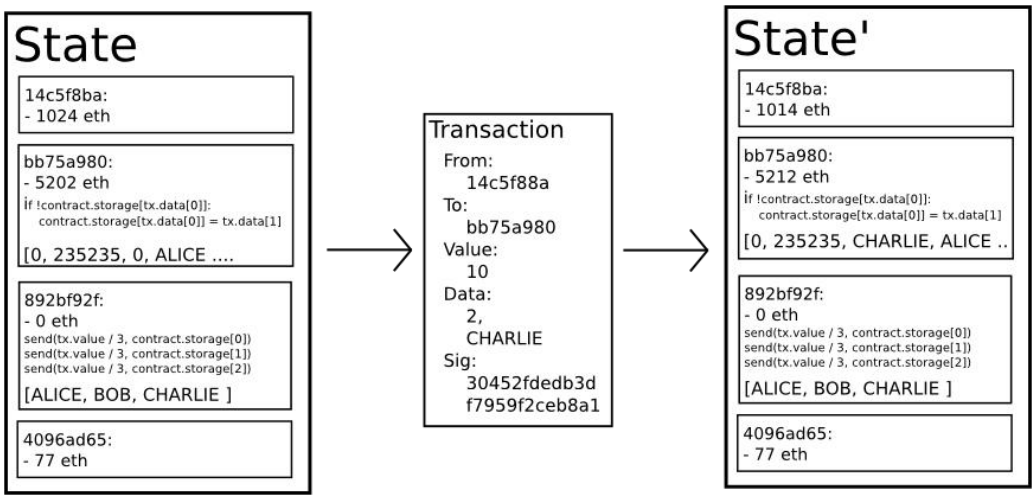


图 8-1

世界链的状态转换函数：APPLY(S,TX) -> S'，可以定义如下：

1.检查交易的格式是否正确（即有正确数值）、签名是否有效和随机数是否与发送者账户的随机数匹配。如否，返回错误。

2.计算交易费用:fee=STARTGAS * GASPRICE，并从签名中确定发送者的地址。从发送者的账户中减去交易费用和增加发送者的随机数。如果账户余额不足，返回错误。

3.设定初值 GAS = STARTGAS，并根据交易中的字节数减去一定量的瓦斯值。

4.从发送者的账户转移价值到接收者账户。如果接收账户还不存在，创建此账户。如果接收账户是一个合约，运行合约的代码，直到代码运行结束或者瓦斯用完。

5.如果因为发送者账户没有足够的钱或者代码执行耗尽瓦斯导致价值转移失败，恢复原来的状态，但是还需要支付交易费用，交易费用加至矿工账户。

6.否则，将所有剩余的瓦斯归还给发送者，消耗掉的瓦斯作为交易费用发送给矿工。例如，假设合约的代码如下：

```
if !self.storage[calldataload(0)]:
    self.storage[calldataload(0)] = calldataload(32)
```

需要注意的是，在现实中合约代码是用底层世界链虚拟机（EVM）代码写成的。上面的合约是用我们的高级语言 Serpent 语言写成的，它可以被编译成 EVM 代码。假设合约存储器开始时是空的，一个值为 10 以太，瓦斯为 2000，瓦斯价格为 0.001 以太并且 64 字节数据，第一个三十二字节的快代表号码 2 和第二个代表词 CHARLIE。的交易发送后，状态转换函数的处理过程如下：

1.检查交易是否有效、格式是否正确。

2.检查交易发送者至少有 2000*0.001=2 个世界币。如果有，从发送者账户中减去 2 个世界币。

3.初始设定 gas=2000,假设交易长为 170 字节，每字节的费用是 5，减去 850，所以还剩 1150。

4.从发送者账户减去 10 个世界币，为合约账户增加 10 个世界币。

5.运行代码。在这个合约中，运行代码很简单：它检查合约存储器索引为 2 处是否已使用，注意到它未被使用，然后将其值置为 CHARLIE。假设这消耗了 187 单位的瓦斯，于是剩余的瓦斯为 1150 - 187 = 963。

6.向发送者的账户增加 963*0.001=0.963 个世界币，返回最终状态。 如果没有合约接收交易，那么所有的交易费用就等于 GASPRICE 乘以交易的字节长度，交易的数据就与交易费用无关了。另外，需要注意的是，合约发起的消息可以对它们产生的计算分配瓦斯限额，如果子计算的瓦斯用完了，它只恢复到消息发出时的状态。因此，就像交易一样，合约也可以通过对它产生的子计算设置严格的限制，保护它们的计算资源。

代码执行

世界链合约的代码使用低级的基于堆栈的字节码的语言写成的，被称为“世界链虚拟机代码”或者“EVM 代码”。代码由一系列字节构成，每一个字节代表一种操作。一般

而言，代码执行是无限循环，程序计数器每增加一（初始值为零）就执行一次操作，直到代码执行完毕或者遇到错误，STOP 或者 RETURN 指令。操作可以访问三种存储数据的空间：

堆栈，一种后进先出的数据存储，32 字节的数值可以入栈，出栈。

内存，可无限扩展的字节队列。

合约的长期存储，一个秘钥/数值的存储，其中秘钥和数值都是 32 字节大小，与计算结束即重置的堆栈和内存不同，存储内容将长期保持。

代码可以象访问区块头数据一样访问数值，发送者和接受到的消息中的数据，代码还可以返回数据的字节队列作为输出。

EVM 代码的正式执行模型令人惊讶地简单。当世界链虚拟机运行时，它的完整的计算状态可以由元组(block_state, transaction, message, code, memory, stack, pc, gas)来定义，这里 block_state 是包含所有账户余额和存储的全局状态。每轮执行时，通过调出代码的第 pc（程序计数器）个字节，当前指令被找到，每个指令都有定义自己如何影响元组。例如，ADD 将两个元素出栈并将它们的和入栈，将 gas（瓦斯）减一并将 pc 加一，SSTORE 将顶部的两个元素出栈并将第二个元素插入到由第一个元素定义的合约存储位置，同样减少最多 200 的 gas 值并将 pc 加一，虽然有许多方法通过即时编译去优化世界链，但世界链的基础性的实施可以用几百行代码实现。

区块链和挖矿

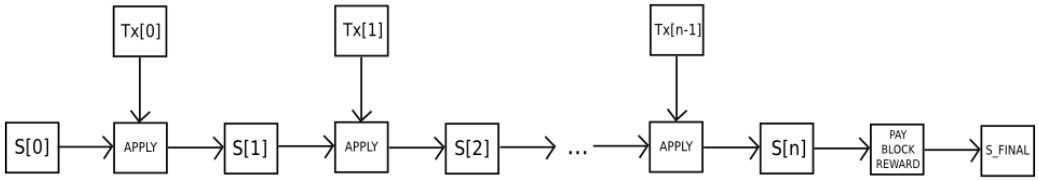


图 8-2

虽然有一些不同，但世界链的区块链在很多方面类似于比特币区块链。它们的区块链架构的不同在于，世界链区块不仅包含交易记录和最近的状态，还包含区块序号和难度值。世界链中的区块确认算法如下：

1.检查区块引用的上一个区块是否存在和有效。

2.检查区块的时间戳是否比引用的上一个区块大，而且小于 15 分钟。

3.检查区块序号、难度值、 交易根，叔根和瓦斯限额（许多世界链特有的底层概念）是否有效。

4.检查区块的工作量证明是否有效。

5.将 S[0]赋值为上一个区块的 STATE_ROOT。

6.将 TX 赋值为区块的交易列表，一共有 n 笔交易。对于属于 0……n-1 的 i，进行状态转换 S[i+1] = APPLY(S[i],TX[i])。如果任何一个转换发生错误，或者程序执行到此处所花费的瓦斯（gas）超过了 GASLIMIT，返回错误。

7.用 S[n]给 S_FINAL 赋值，向矿工支付区块奖励。 8 检查 S-FINAL 是否与 STATE_ROOT 相同。如果相同，区块是有效的。否则，区块是无效的。

这一确认方法乍看起来似乎效率很低，因为它需要存储每个区块的所有状态，但是事实上世界链的确认效率可以与比特币相提并论。原因是状态存储在树结构中（tree structure），每增加一个区块只需要改变树结构的一小部分。因此，一般而言，两个相邻的区块的树结构的大部分应该是相同的，因此存储一次数据，可以利用指针（即子树哈希）引用两次。一种被称为“帕特里夏树”（“Patricia Tree”）的树结构可以实现这一点，其中包括了对默克尔树概念的修改，不仅允许改变节点，而且还可以插入和删除节点。另外，因为所有的状态信息是最后一个区块的一部分，所以没有必要存储全部的区块历史-这一方法如果能够可以应用到比特币系统中，经计算可以对存储空间有 10-20 倍的节省。

应用

一般来讲，世界链之上有三种应用。第一类是金融应用，为用户提供更强大的用他们的钱管理和参与合约的方法。包括子货币，金融衍生品，对冲合约，储蓄钱包，遗嘱，甚至一些种类的全面的雇佣合约。第二类是半金融应用，这里有钱的存在但也有很重的非金钱的方面，一个完美的例子是为解决计算问题而设的自我强制悬赏。最后，还有在线投票和去中心化治理以及给体系内的华商联盟企业上链这样的完全的非金融应用。

代币系统

链上代币系统有很多应用，从代表如美元或黄金等资产的子货币到公司股票，单独的代币代表智能资产，安全的不可伪造的优惠券，甚至与传统价值完全没有联系的用来进行积分奖励的代币系统。在世界链中实施代币系统容易得让人吃惊。关键的一点是理解，所有的货币或者代币系统，从根本上来说是一个带有如下操作的数据库：从 A 中减去 X 单位并把 X 单位加到 B 上，前提条件是(1)A 在交易之前有至少 X 单位以及(2)交易被 A 批准。实施一个代币系统就是把这样一个逻辑实施到一个合约中去。

用 Serpent 语言实施一个代币系统的基本代码如下：

```
def send(to, value):
    if self.storage[from] >= value:
        self.storage[from] = self.storage[from] value
```

self.storage[to] = self.storage[to] + value

这从本质上来说是本文将要进一步描述的“银行系统”状态转变功能的一个最小化实施。需要增加一些额外的代码以提供在初始和其它一些边缘情况下分发货币的功能，理想情况下会增加一个函数让其它合约来查询一个地址的余额。就足够了。理论上，基于世界链的充当子货币的代币系统可能包括一个基于比特币的链上元币所缺乏的重要功能：直接用这种货币支付交易费的能力。实现这种能力的方法是在合约里维护一个世界币账户以用来为发送者支付交易费，通过收集被用来充当交易费用的内部货币并把它们在一个不断运行的拍卖中拍卖掉，合约不断为该世界币账户注资。这样用户需要用世界币“激活”他们的账户，但一旦账户中有世界币它将会被重复使用因为每次合约都会为其充值。

金融衍生品和价值稳定的货币

金融衍生品是“智能合约”的最普遍的应用，也是最易于用代码实现的之一。实现金融合约的主要挑战是它们中的大部分需要参照一个外部的价格发布器；例如，一个需求非常大的应用是一个用来对冲世界币（或其它密码学货币）相对美元价格波动的智能合约，但该合约需要知道世界币相对美元的价格。最简单地方法是通过由某特定机构（例如纳斯达克）维护的“数据提供“合约进行，该合约的设计使得该机构能够根据需要更新合约，并提供一个接口使得其它合约能够通过发送一个消息给该合约以获取包含价格信息的回复。

当这些关键要素都齐备，对冲合约看起来会是下面的样子：

1.等待 A 输入 1000 世界币。.

2.等待 B 输入 1000 世界币。

3.通过查询数据提供合约，将 1000 世界币的美元价值，例如，x 美元，记录至存储器。

4.30 天后，允许 A 或 B“重新激活“合约以发送价值 x 美元的世界币（重新查询数据提供合约以获取新价格并计算）给 A 并将剩余的世界币发送给 B。 这样的合约在密码学商务中有非同寻常的潜力。密码学货币经常被诟病的一个问题就是其价格的波动性；虽然大量的用户和商家可能需要密码学资产所带来的安全和便利，可他们不太会乐意面对一天中资产跌去 23%价值的情形。直到现在，最为常见的推荐方案是发行者背书资产；思想是发行者创建一种子货币，对此种子货币他们有权发行和赎回，给予（线下）提供给他们一个单位特定相关资产（例如黄金，美元）的人一个单位子货币。发行者承诺当任何人送还一个单位密码学资产时。发还一个单位的相关资产。这种机制能够使任何非密码学资产被“升级“为密码学资产，如果发行者值得信任的话。 然而实践中发行者并非总是值得信任的，并且一些情况下银行体系太脆弱，或者不够诚实守信从而使这样的服务无法存在。金融衍生品提供了一种替代方案。这里将不再有提

供储备以支撑一种资产的单独的发行者，取而代之的是一个由赌一种密码学资产的价格会上升的投机者构成的去中心化市场。与发行者不同，投机者一方没有讨价还价的权利，因为对冲合约把他们的储备冻结在了契约中。注意这种方法并非是完全去中心化的，因为依然需要一个可信任的提供价格信息的数据源，尽管依然有争议这依然是在降低基础设施需求（与发行者不同，一个价格发布器不需要牌照并且似乎可归为自由言论一类）和降低潜在欺诈风险方面的一个巨大的进步。

身份和信誉系统

最早的替代币，域名币，尝试使用一个类比特币块链来提供一个名称注册系统，在那里用户可以将他们的名称和其它数据一起在一个公共数据库注册。最常用的应用案例把象“bitcoin.org“（或者再域名币中，”bitcoin.bit“）一样的域名与一个 IP 地址对应的域名系统。其它的应用案例包括电子邮件验证系统和潜在的更先进的信誉系统。这里是世界链中提供与域名币类似的的名称注册系统的基础合约：

```
def register(name, value):
    if !self.storage[name]:
        self.storage[name] = value
```

合约非常简单；就是一个世界链网络中的可以被添加但不能被修改或移除的数据库。任何人都可以把一个名称注册为一个值并永远不变。一个更复杂的名称注册合约将包含允许其他合约查询的“功能条款“，以及一个让一个名称的”拥有者“（即第一个注册者）修改数据或者转让所有权的机制。甚至可以在其上添加信誉和信任网络功能。

去中心化存储

在过去的几年里出现了一些大众化的在线文件存储初创公司，最突出的是 Dropbox，它寻求允许用户上传他们的硬盘备份，提供备份存储服务并允许用户访问从而按月向用户收取费用。然而，在这一点上这个文件存储市场有时相对低效；对现存服务的粗略观察表明，特别地在“神秘谷“20-200GB 这一既没有免费空间也没有企业级用户折扣的水平上，主流文件存储成本每月的价格意味着支付在一个月里支付整个硬盘的成本。世界链合约允许去中心化存储生态的开发，这样用户通过将他们自己的硬盘或未用的网络空间租出去以获得少量收益，从而降低了文件存储的成本。

这样的设施的基础性构件就是我们所谓的“去中心化 Dropbox 合约“。这个合约工作原理如下。首先，某人将需要上传的数据分成快，对每一块数据加密以保护隐私，并且以此构建一个默克尔树。然后创建一个含以下规则的合约，每 N 个块，合约将从默克尔树中抽取一个随机索引（使用能够被合约代码访问的上一个块的哈希来提供随机性）， 然后给第一个实体 X 以太以支撑一个带有类似简化验证支付（SPV）的在树中特定索引处的块的所有权证明。当一个用户想重新下载他的文件，他可以使用微支付通道协议（例如每 32k 字节支付 1 萨博）恢复文件；从费用上讲最高效的方法是支

付者不到最后不发布交易，而是用一个略微更合算的带有同样随机数的交易在每 32k 字节之后来代替原交易。

这个协议的一个重要特征是，虽然看起来象是一个人信任许多不准备丢失文件的随机节点，但是他可以通过秘密分享把文件分成许多小块，然后通过监视合同得知每个小块都还被某个节点的保存着。如果一个合约依然在付款，那么就提供了某个人依然在保存文件的证据。

去中心化自治组织

通常意义上“去中心化自治组织（DAO, decentralized autonomous organization）”的概念指的是一个拥有一定数量成员或股东的虚拟实体，依靠比如 67%多数来决定花钱以及修改代码。成员会集体决定组织如何分配资金。分配资金的方法可能是悬赏，工资或者更有吸引力的机制比如用内部货币奖励工作。这仅仅使用密码学块链技术就从根本上复制了传统公司或者非营利组织的法律意义以实现强制执行。至此许多围绕 DAO 的讨论都是围绕一个带有接受分红的股东和可交易的股份的“去中心化自治公司（DAC，decentralized autonomous corporation）”的“资本家”模式；作为替代者，一个被描述为“去中心化自治社区（decentralized autonomous community）”的实体将使所有成员都在决策上拥有同等的权利并且在增减成员时要求 67%多数同意。每个人都只能拥有一个成员资格这一规则需要被群体强制实施。

下面是一个如何用代码实现 DO 的纲要。最简单地设计就是一段如果三分之二成员同意就可以自我修改的代码。虽然理论上代码是不可更改的，然而通过把代码主干放在一个单独的合约内并且把合约调用的地址指向一个可更改的存储依然可以容易地绕开障碍而使代码变得可修改，在一个这样的 DAO 合约的简单实现中有三种交易类型，由交易提供的数据区分：

[0,i,K,V] 注册索引为 i 的对存储地址索引为 K 至 v 的内容的更改建议。

[0,i] 注册对建议 i 的投票。

[2,i] 如有足够投票则确认建议 i。

然后合约对每一项都有具体的条款。它将维护一个所有开放存储的更改记录以及一个谁投票表决的表。还有一个所有成员的表。当任何存储内容的更改获得了三分之二多数同意，一个最终的交易将执行这项更改。一个更加复杂的框架会增加内置的选举功能以实现如发送交易，增减成员，甚至提供委任制民主一类的投票代表（即任何人都可以委托另外一个人来代表自己投票，而且这种委托关系是可以传递的，所以如果 A 委托了 B 然后 B 委托了 C 那么 C 将决定 A 的投票）。这种设计将使 DAO 作为一个去中心化社区有机地成长， 使人们最终能够把挑选合适人选的任务交给专家，与当前系统不同，随着社区成员不断改变他们的站队假以时日专家会容易地出现和消失。一个替代的模式是去中心化公司，那里任何账户可以拥有 0 到更多的股份，决策需要

三分之二多数的股份同意。一个完整的框架将包括资产管理功能-可以提交买卖股份的订单以及接受这种订单的功能（前提是合约里有订单匹配机制）。代表依然以委任制民主的方式存在，产生了“董事会”的概念。

更先进的组织治理机制可能会在将来实现；现在一个去中心化组织（DO）可以从去中心化自治组织（DAO）开始描述。DO 和 DAO 的区别是模糊的，一个大致的分割线是治理是否可以通过一个类似政治的过程或者一个“自动”过程实现，一个不错的直觉测试是“无通用语言”标准：如果两个成员不说同样的语言组织还能正常运行吗？显然，一个简单的传统的持股式公司会失败，而象比特币协议这样的却很可能成功，罗宾·汉森的“futarchy”，一个通过预测市场实现组织化治理的机制是一个真正的说明“自治”式治理可能是什么样子的好例子。注意一个人无需假设所有 DAO 比所有 DO 优越；自治只是一个在一些特定场景下有很大优势的，但在其它地方未必可行的范式，许多半 DAO 可能存在。

进一步的应用

1.

储蓄钱包。 假设 Alice 想确保她的资金安全，但她担心丢失或者被黑客盗走私钥。她把世界币放到和 Bob 签订的一个合约里，如下所示，这合同是一个银行：

2.

Alice 单独每天最多可提取 1%的资金。

Bob 单独每天最多可提取 1%的资金，但 Alice 可以用她的私钥创建一个交易取消 Bob 的提现权限。

Alice 和 Bob 一起可以任意提取资金。 一般来讲，每天 1%对 Alice 足够了，如果 Alice 想提现更多她可以联系 Bob 寻求帮助。如果 Alice 的私钥被盗，她可以立即找到 Bob 把她的资金转移到一个新合同里。如果她弄丢了她的私钥，Bob 可以慢慢地把钱提出。如果 Bob 表现出了恶意，她可以关掉他的提现权限。

3.

作物保险。一个人可以很容易地以天气情况而不是任何价格指数作为数据输入来创建一个金融衍生品合约。如果一个爱荷华的农民购买了一个基于爱荷华的降雨情况进行反向赔付的金融衍生品，那么如果遇到干旱，该农民将自动地收到赔付资金而如果有足量的降雨他会很开心因为他的作物收成会很好。

4.

一个去中心化的数据发布器。 对于基于差异的金融合约，事实上通过过“谢林点”协议将数据发布器去中心化是可能的。谢林点的工作原理如下：N 方为某个指定的数据提供输入值到系统（例如 WSC/USD 价格），所有的值被排序，每个提供 25%到 75%之间的值的节点都会获得奖励，每个人都有激励去提供他人将提供的答案，大量玩家

可以真正同意的答案明显默认就是正确答案，这构造了一个可以在理论上提供很多数值，包括 WSC/USD 价格，柏林的温度甚至某个特别困难的计算的结果的去中心化协议。

5、云计算。EVM 技术还可被用来创建一个可验证的计算环境，允许用户邀请他人进行计算然后选择性地要求提供在一定的随机选择的检查点上计算被正确完成的证据。这使得创建一个任何用户都可以用他们的台式机，笔记本电脑或者专用服务器参与的云计算市场成为可能，现场检查和安全保证金可以被用来确保系统是值得信任的（即没有节点可以因欺骗获利）。虽然这样一个系统可能并不适用所有任务；例如，需要高级进程间通信的任务就不易在一个大的节点云上完成。然而一些其它的任务就很容易实现并行；SETI@home, folding@home 和基因算法这样的项目就很容易在这样的平台上进行。

6.点对点赌博。任意数量的点对点赌博协议都可以搬到世界链的区块链上，例如 Frank Stajano 和 Richard Clayton 的 Cyberdice。最简单的赌博协议事实上是这样一个简单的合约，它用来赌下一个区块的哈稀值与猜测值之间的差额, 据此可以创建更复杂的赌博协议，以实现近乎零费用和无欺骗的赌博服务。

7.预测市场。 不管是有神谕还是有谢林币，预测市场都会很容易实现，带有谢林币的预测市场可能会被证明是第一个主流的作为去中心化组织管理协议的“futarchy”应用。

8.链上去中心化市场，以身份和信誉系统为基础，比如未来华商联盟优秀企业为核心的商业生态。

费用

因为每个发布的到区块链的交易都占用了下载和验证的成本，需要有一个包括交易费的规范机制来防范滥发交易。比特币使用的默认方法是纯自愿的交易费用，依靠矿工担当守门人并设定动态的最低费用。因为这种方法是“基于市场的”，使得矿工和交易发送者能够按供需来决定价格，所以这种方法在比特币社区被很顺利地接受了。然而，这个逻辑的问题在于，交易处理并非一个市场；虽然根据直觉把交易处理解释成矿工给发送者提供的服务是很有吸引力的，但事实上一个矿工收录的交易是需要网络中每个节点处理的，所以交易处理中最大部分的成本是由第三方而不是决定是否收录交易的矿工承担的。于是，非常有可能发生公地悲剧。

然而，当给出一个特殊的不够精确的简化假设时，这个基于市场的机制的漏洞很神奇地消除了自己的影响。论证如下。假设：

1.一个交易带来 k 步操作, 提供奖励 kR 给任何收录该交易的矿工，这里 R 由交易发布者设定， k 和 R 对于矿工都是事先（大致上）可见的。

2.每个节点处理每步操作的成本都是 C (即所有节点的效率一致)。

3.有 N 个挖矿节点，每个算力一致(即全网算力的 1/N)。

4.没有不挖矿的全节点。

当预期奖励大于成本时，矿工愿意挖矿。这样，因为矿工有 1/N 的机会处理下一个区块，所以预期的收益是 kR/N , 矿工的处理成本简单为 kC. 这样当 kR/N > kC，即 R > NC 时。矿工愿意收录交易。注意 R 是由交易发送者提供的每步费用，是矿工从处理交易中获益的下限。 NC 是全网处理一个操作的成本。所以，矿工仅有动机去收录那些收益大于成本的交易。 然而，这些假设与实际情况有几点重要的偏离：

1.因为额外的验证时间延迟了块的广播因而增加了块成为废块的机会，处理交易的矿工比其它的验证节点付出了更高的成本。

2.不挖矿的全节点是存在的。

3.实践中算力分布可能最后是极端不平均的。

4.以破坏网络为己任的投机者，政敌和疯子确实存在，并且他们能够聪明地设置合同使得他们的成本比其它验证节点低得多。 上面第 1 点驱使矿工收录更少的交易，第 2 点增加了 NC; 因此这两点的影响至少部分互相抵消了. 第 3 点和第 4 点是主要问题；作为解决方案我们简单地建立了一个浮动的上限：没有区块能够包含比 BLK_LIMIT_FACTOR 倍长期指数移动平均值更多的操作数。具体地：

blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR - 1) + floor(parent.opcount * BLK_LIMIT_FACTOR)) /EMA_FACTOR)

BLK_LIMIT_FACTOR 和 EMA_FACTOR 是暂且被设为 65536 和 1.5 的常数，但可能会在更深入的分析后调整。 回复

计算和图灵完备

需要强调的是世界链虚拟机是图灵完备的； 这意味着 EVM 代码可以实现任何可以想象的计算，包括无限循环。EVM 代码有两种方式实现循环。首先， JUMP 指令可以让程序跳回至代码前面某处，还有允许如 while x < 27: x = x * 2 一样的条件语句的 JUMPI 指令实现条件跳转。其次，合约可以调用其它合约，有通过递归实现循环的潜力。这很自然地导致了一个问题：恶意用户能够通过迫使矿工和全节点进入无限循环而不得不关机吗？ 这问题出现是因为计算机科学中一个叫停机问题的问题：一般意义上没有办法知道，一个给定的程序是否能在有限的时间内结束运行。

正如在状态转换章节所述，我们的方案通过为每一个交易设定运行执行的最大计算步数来解决问题，如果超过则计算被恢复原状但依然要支付费用。消息以同样的方式工作。为显示这一方案背后的动机，请考虑下面的例子：

一个攻击者创建了一个运行无限循环的合约，然后发送了一个激活循环的交易给矿工，矿工将处理交易，运行无限循环直到瓦斯耗尽。即使瓦斯耗尽交易半途停止，交易依然正确（回到原处）并且矿工依然从攻击者哪里挣到了每一步计算的费用。

一个攻击者创建一个非常长的无限循环意图迫使矿工长时间内一直计算致使在计算结束前若干区块已经产生于是矿工无法收录交易以赚取费 用。然而，攻击者需要发布一个 STARTGAS 值以限制可执行步数，因而矿工将提前知道计算将耗费过多的步数。

一个攻击者看到一个包含诸如 send(A,self.storage); self.storage = 0 格式的合约然后发送带有只够执行第一步的费用的而不够执行第二步的交易（即提现但不减少账户余额）。合约作者无需担心防卫类似攻击，因为如果执行中途停止则所有变更都被回复。

一个金融合约靠提取九个专用数据发布器的中值来工作以最小化风险，一个攻击者接管了其中一个数据提供器，然后把这个按 DAO 章节所述的可变地址调用机制设计成可更改的数据提供器转为运行一个无限循环，以求尝试逼迫任何从此金融合约索要资金的尝试都会因瓦斯耗尽而中止。然而，该金融合约可以在消息里设置瓦斯限制以防范此类问题。 图灵完备的替代是图灵不完备，这里 JUMP 和 JUMPI 指令不存在并且在某个给定时间每个合约只允许有一个拷贝存在于调用堆栈内。在这样的系统里，上述的费用系统和围绕我们的方案的效率的不确定性可能都是不需要的，因为执行一个合约的成本将被它的大小决定。此外，图灵不完备甚至不是一个大的限制，在我们内部设想的所有合约例子中，至今只有一个需要循环，而且即使这循环也可以被 26 个单行代码段的重复所代替。考虑到图灵完备带来的严重的麻烦和有限的益处，为什么不简单地使用一种图灵不完备语言呢？事实上图灵不完备远非一个简洁的解决方案。为什么？请考虑下面的合约：

C0: call(C1); call(C1);C1: call(C2); call(C2);C2: call(C3); call(C3);...C49: call(C50); call(C50);C50: (作一个图灵机的步计算和记录结果在合约的长期存储)

现在，发送一个这样的交易给 A，这样，在 51 个交易中，我们有了一个需要花费 2^50 步计算的合约，矿工可能尝试通过为每一个合约维护一个最高可执行步数并且对于递归调用其它合约的合约计算可能执行步数从而预先检测这样的逻辑炸弹，但是这会使矿工禁止创建其它合约的合约（因为上面 26 个合约的创建和执行可以很容易地放入一个单独合约内）。另外一个问题点是一个消息的地址字段是一个变量，所以通常来讲可能甚至无法预先知道一个合约将要调用的另外一个合约是哪一个。于是，最终我们有了一个惊人的结论：图灵完备的管理惊人地容易，而在缺乏同样的控制时图灵不完备的管理惊人地困难- 那为什么不让协议图灵完备呢？

货币和发行

世界链网络包含自身的内置货币世界币，世界币扮演双重角色，为各种数字资产交易提供主要的流动性，更重要的是提供了了支付交易费用的一种机制。为便利及避

免将来的争议期间（参见当前的 mBTC/uBTC/聪的争论），不同面值的名称将被提前设置：

1: 伟

10^12: 萨博

10^15: 芬尼

10^18: 以太

这应该被当作是“元”和“分”或者“比特币”和“聪”的概念的扩展版，在不远的将来，我们期望“以太”被用作普通交易，“芬尼”用来进行微交易，“萨博”和“伟”用来进行关于费用和协议实施的讨论。

发行模式如下：

通过发售活动，世界币将以每 BTC 1337-2000 以太的价格发售，一个旨在为世界链组织筹资并且为开发者支付报酬的机制已经在其它一些密码学货币平台上成功使用。早期购买者会享受较大的折扣，发售所得的 BTC 将完全用来支付开发者和研究者的工资和悬赏，以及投入密码学货币生态系统的项目。

0.099x （x 为发售总量）将被分配给 BTC 融资或其它的确定性融资成功之前参与开发的早期贡献者，另外一个 0.099x 将分配给长期研究项目。

自上线时起每年都将有 0.26x（x 为发售总量）被矿工挖出。

发行分解

永久线性增长模型降低了在比特币中出现的财富过于集中的风险，并且给予了活在当下和将来的人公平的机会去获取货币，同时保持了对获取和持有世界币的激励，因为长期来看“货币供应增长率”是趋于零的。我们还推断，随着时间流逝总会发生因为粗心和死亡等原因带来的币的遗失，假设币的遗失是每年货币供应量的一个固定比例，则最终总的流通中的货币供应量会稳定在一个等于年货币发行量除以遗失率的值上（例如，当遗失率为 1%时，当供应量达到 30x 时，每年有 0.3x 被挖出同时有 0.3x 丢失，达到一个均衡）。

Group	At launch	After 1 year	After 5 years
Currency units	1.198X	1.458X	2.498X
Purchasers	83.5%	68.6%	40.0%
Reserve spent pre-sale	8.26%	6.79%	3.96%
Reserve used post-sale	8.26%	6.79%	3.96%

Group	At launch	After 1 year	After 5 years
Miners	0%	17.8%	52.0%

除了线性的发行方式外，和比特币一样世界币的的供应量增长率长期来看也趋于零。

挖矿的中心化

比特币挖矿算法基本上是让矿工千万次地轻微改动区块头，直到最终某个节点的改动版本的哈希小于目标值（目前是大约 2190）。然而，这种挖矿算法容易被两种形式的中心化攻击。第一种，挖矿生态系统被专门设计的因而在比特币挖矿这一特殊任务上效率提高上千倍的 ASICs（专用集成电路）和电脑芯片控制。这意味着比特币挖矿不再是高度去中心化的和追求平等主义的，而是需要巨额资本的有效参与。第二种，大部分比特币矿工事实上不再在本地完成区块验证；而是依赖中心化的矿池提供区块头。这个问题可以说很严重：在本文写作时，最大的两个矿池间接地控制了大约全网 50%的算力，虽然当一个矿池或联合体尝试 51%攻击时矿工可以转换到其它矿池这一事实减轻了问题的严重性。

世界链现在的目的是使用一个基于为每 1000 个随机数随机产生唯一哈希的函数的挖矿算法，用足够宽的计算域，去除专用硬件的优势。这样的策略当然不会使中心化的收益减少为零，但是也不需要。注意每单个用户使用他们的私人笔记本电脑或台式机就可以几乎免费地完成一定量的挖矿活动，但当到了 100%的 CPU 使用率之后更多地挖矿就会需要他们支付电力和硬件成本。ASIC 挖矿公司需要从第一个哈希开始就为电力和硬件支付成本。所以，如果中心化收益能够保持在(E + H) /E 以下，那么即使 ASICs 被制造出来普通矿工依然有生存空间。另外，我们计划将挖矿算法设计成挖矿需要访问整个区块链，迫使矿工存储完成的区块链或者至少能够验证每笔交易。这去除了对中心化矿池的需要；虽然矿池依然可以扮演平滑收益分配的随机性的角色，但这功能可以被没有中心化控制的 P2P 矿池完成地同样好。这样即使大部分普通用户依然倾向选择轻客户端，通过增加网络中的全节点数量也有助于抵御中心化。

扩展性

扩展性问题是世界链常被关注的地方，与比特币一样，世界链也遭受着每个交易都需要网络中的每个节点处理这一困境的折磨。比特币的当前区块链大小约为 20GB，以每小时 1MB 的速度增长。如果比特币网络处理 Visa 级的 2000tps 的交易，它将以每三秒 1MB 的速度增长（1GB 每小时，8TB 每年）。世界链可能也会经历相似的甚至更糟的增长模式，因为在世界链区块链之上还有很多应用，而不是像比特币只是简单的

货币，但世界链全节点只需存储状态而不是完整的区块链历史这一事实让情况得到了改善。

大区块链的问题是中心化风险。如果块链大小增加至比如 100TB，可能的场景将是只有非常小数目的大商家会运行全节点，而常规用户使用轻的 SPV 节点。这会增加对全节点合伙欺诈牟利（例如更改区块奖励，给他们自己 BTC）的风险的担忧。轻节点将没有办法立刻检测到这种欺诈。当然，至少可能存在一个诚实的全节点，并且几个小时之后有关诈骗的信息会通过 Reddit 这样的渠道泄露，但这时已经太晚：任凭普通用户做出怎样的努力去废除已经产生的区块，他们都会遇到与发动一次成功的 51%攻击同等规模的巨大的不可行的协调问题。在比特币这里，现在这是一个问题，但 Peter Todd 建议的一个改动可以缓解这个问题。

近期，世界链会使用两个附加的策略以应对此问题。首先，因为基于区块链的挖矿算法，至少每个矿工会被迫成为一个全节点，这保证了一定数量的全节点。其次，更重要的是，处理完每笔交易后，我们会把一个中间状态树的根包含进区块链。即使区块验证是中心化的，只要有一个诚实的验证节点存在，中心化的问题就可以通过一个验证协议避免。如果一个矿工发布了一个不正确的区块，这区块要么是格式错，要么状态 S[n]是错的。因为 S[0]是正确的，必然有第一个错误状态 S[i]但 S[i-1]是正确的，验证节点将提供索引 i，一起提供的还有处理 APPLY(S[i-1],TX[i]) -> S[i]所需的帕特里夏树节点的子集。这些节点将受命进行这部分计算，看产生的 S[i]与先前提供的值是否一致。

另外，更复杂的是恶意矿工发布不完整区块进行攻击，造成没有足够的信息去确定区块是否正确。解决方案是质疑-回应协议：验证节点对目标交易索引发起质疑，接受到质疑信息的轻节点会对相应的区块取消信任，直到另外一个矿工或者验证者提供一个帕特里夏节点子集作为正确的证据。

去中心化应用

上述合约机制使得任何一个人能够在一个虚拟机上建立通过全网共识来运行命令行应用（从根本上来说是），它能够更改一个全网可访问的状态作为它的“硬盘”。然而，对于多数人来说，用作交易发送机制的命令行接口缺乏足够的用户友好使得去中心化成为有吸引力的替代方案。最后，一个完整的“去中心化应用”应该包括底层的商业逻辑组件【无论是否在世界链完整实施，使用世界链和其它系统组合（如一个 P2P 消息层，其中一个正在计划放入世界链客户端）或者仅有其它系统的方式】和上层的图形用户接口组件。世界链客户端被设计成一个网络浏览器，但包括对“WSC” Javascript API 对象的支持，可被客户端里看到的特定的网页用来与世界链区块链交互。从“传统”网页的角度看来，这些网页是完全静态的内容，因为区块链和其它去中心化协议将完

全代替服务器来处理用户发起的请求。最后，去中心化协议有希望自己利用某种方式使用世界链来存储网。

世界链（World’s Chain）

链接全世界华商，构建数字化商业！

致力于全球的

“ 自治的网络 · 协作的未来 · 共赢的生态 ”

聚焦链上复杂数据和交互，面向复杂商业协作关系

世界链网络的实现将带来全球华商生态区块链化，

世界链网络将实现全新的共识激励机制和升级力，

世界链网络让每参与者从数据安全中发挥创新力！