一站式中小微企业链改服务平台

ZYChain

正元链商

白 皮 书

Zhengyuan Chain merchants Foundation 版本 v.2.0.1 2019/12/01

导语

区块链技术日新月异地改变着人们的生活，越来越多的企业开始着手研究或落地区块链应用，从中央到各级政府陆续出台有力措施鼓励区块链领域的技术创新和落地应用。

区块链技术的本质与核心是为人类服务，给人类提供更便捷的生活方式。我们觉得区块链应该回归本质，追求技术的发展，将区块链从“看不见摸不着用不到“转变成实际的商业应用底层技术，让人们可以更直观的体会到去中心化技术给人们带来的生活便利、安全、隐私、公平等特性，让人们感受到去中心化互联网技术的魅力；真正让中小微企业都用得上，用得起商业级别的区块链底层技术，从而践行区块链3.0生态应用体系的开创先锋！

ZYChain是一套支持多共识，数据库、执行器等可插拔，且易升级的区块链架构；创造性地支持分层的架构，主链负责交易清算，智能合约和虚拟机从主链上分离放到平行链上独立执行，多条平行链并存提升运算效率；同时平行链之间通过主链实现链间互联，为商业应用的开发提供了足够强大的技术支撑和稳定的性能保障。

ZYChain（正元公链）是 ZYChain Foundation（基金会）全力打造的简单稳定拓展性强的区块链公链系统；基于正元公链，中小微企业有机会构建丰富的针对特定场景的业务应用。

目录

第一章：行业现状及痛点

区块链应用场景已经从单一的数字货币领域延伸到社会的各个领域，除了金融服务业相对成熟以外，其他行业还处于刚刚起步阶段！

中小企业机制灵活，创新能力强，在解决就业岗位，缓解就业压力，保持社会稳定，促进地方经济发展方面，发挥了不可替代的作用；同时，中小企业贡献价值占据经济半壁江、提供大量就业机会！面临以下困局：

1、企业规模小，难以形成品牌

2、管理粗放，运营成本高

3、由于金融机构对中小微企业的评价缺乏正确的评估，造成融资难

4、技术含量低，产品缺乏核心竞争力

5、人才制约企业的发展

摆在传统企业，特别是中小微企业面前的，是一道难题：学习和开发门槛过高！

区块链作为新生技术，让传统企业认识到价值需要一定的学习成本，而想参与区块链的小微企业，却无法破解区块链开发周期长、成本高、人才稀缺、落地应用难的问题。

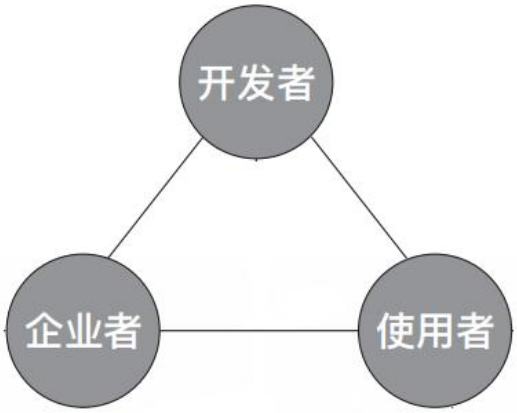
第二章：技术解决方案及原理

ZYChain公有链系统，是一条基于比特币和以太坊系统之外开发的主链，多链共识，多链并行及跨链原子操作构建的高速跨链资产流通公路。在ZYChain底层系统上可扩展多条平行公链，各条平行公链既可独立开发 DAPP，建设多样化的应用生态，又可实现多链间的跨链互换功能。在ZYChain上共享区块链大生态、交易时间、隐私保护、渐进节点共识以及提高信任的效率；在并发响应方面也同时做了大量的突破；再配合ZYChain快速的TPS指数，从而提高了ZYChain整体性能即吞吐量(Performance)让ZYChain的整体稳定性得到了进一步的技术支撑和保障，从而让正元公链成为真正落地的商业应用链；正元公链应用领域广泛，包括稳定币、社交网络、电子商务、资产数字化、债权上链、数据存证、合约游戏等不同的场景，满足金融/支付/电商/溯源/物流及更多产业的实体应用，切实将区块链技术运用在实体的各个领域中，真正地解决了区块链领域无法做到的高吞吐量痛点，极其方便地打造世界级的区块链基础设施。ZYChain将打造一个公链联盟，为各条平行公链提供基础服务。正元公链的核心会如比特币一样稳定，同时兼备灵活高效的扩展性，开发者可以在正元公链系统上建立强大的 DAPP 和多链的生态，为中小微企业的链改需求进行个性化定制，共同维护ZYChain生态的发展。

1. 通过区块链技术让企业的产品溯源上链，提升企业自身的公信力
2、让消费者参与企业的价值创造活动，减低企业的运营成本
3、通过链改来解决企业的现金流，提升企业的链值
4、通过链改服务，让企业更加聚焦产品的功效，提升核心竞争力
5、通过链改，进一步理顺企业的合作关系，形成更加平等、高效的人才机制来留住人才

第三章：ZYChain 全生态体系架构

ZYChain作为一种全生态底层开发平台，不仅仅是做公链及联盟链的开发，而是包罗万象的一个ZYChain新次元空间，在ZYChain的新次元空间里，用户/开发/企业形成了三位一体的生态闭环，同时配合ZYChain强大的公链及联盟链底层技术支撑，使这个新次元空间拥有了集社交/金融/全产业解决方案的一整套产业化区块链开发领域，未来ZYChain将不断丰富生态社区，打造一个区块链3.0跨时代的ZYChain新次元空间。



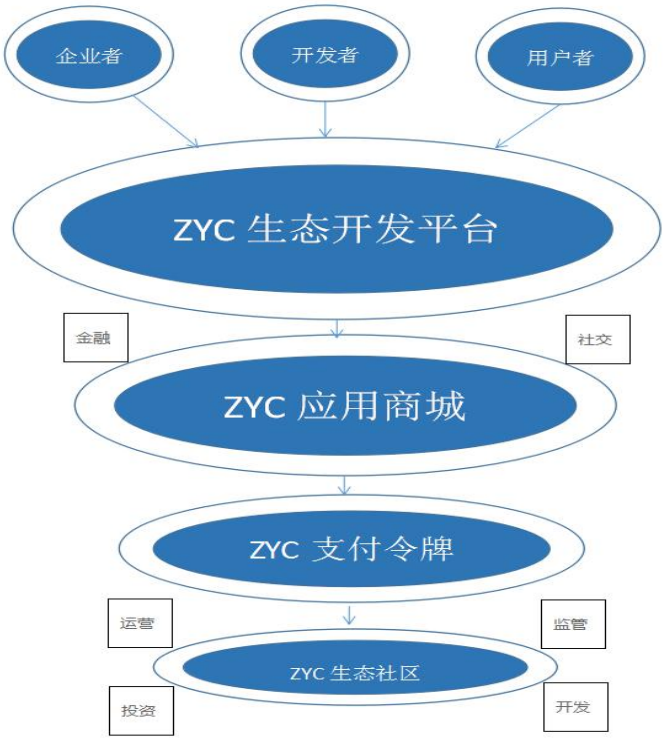
ZYC OS—Dapp应用—公链底层开发平台

ZYC OS生态操作系统，其中包含了ZYC STORE应用商城、ZYC公链联盟链底层开发，ZYC EXCHANGE交易系统，ZYC WALLET钱包，ZYC MAIL加密社交。

ZYChain生态系统中的核心应用包括社交/金融/支付/物流等全产业链的区块链应用+开发，同时会针对于数据上链/云端数据/溯源等产业提供ZYChain区块链解决方案。

开发社区—开发者、企业者、使用者三位一体生态闭环

简述：如图所示，我们将开发者、企业者、终端用户通过三个维度的链接形成了三位一体的生态闭环，且皆通过ZYC生态开发平台进行相应的开发及建设，在ZYC生态平台中有自有的社交以及金融体系，即ZYChain加密邮箱及ZYChain钱包，通过ZYChain区块浏览器进行ZYChain应用商店的部署，Developer、Company、User可以通过ZYC支付令牌进行相应的购买及奖励，在这个生态底层提供了集监管、投资、运营、开发多维一体的生态保障及机制。



生态商业架构图：

第四章：ZYChain 底层开发布局

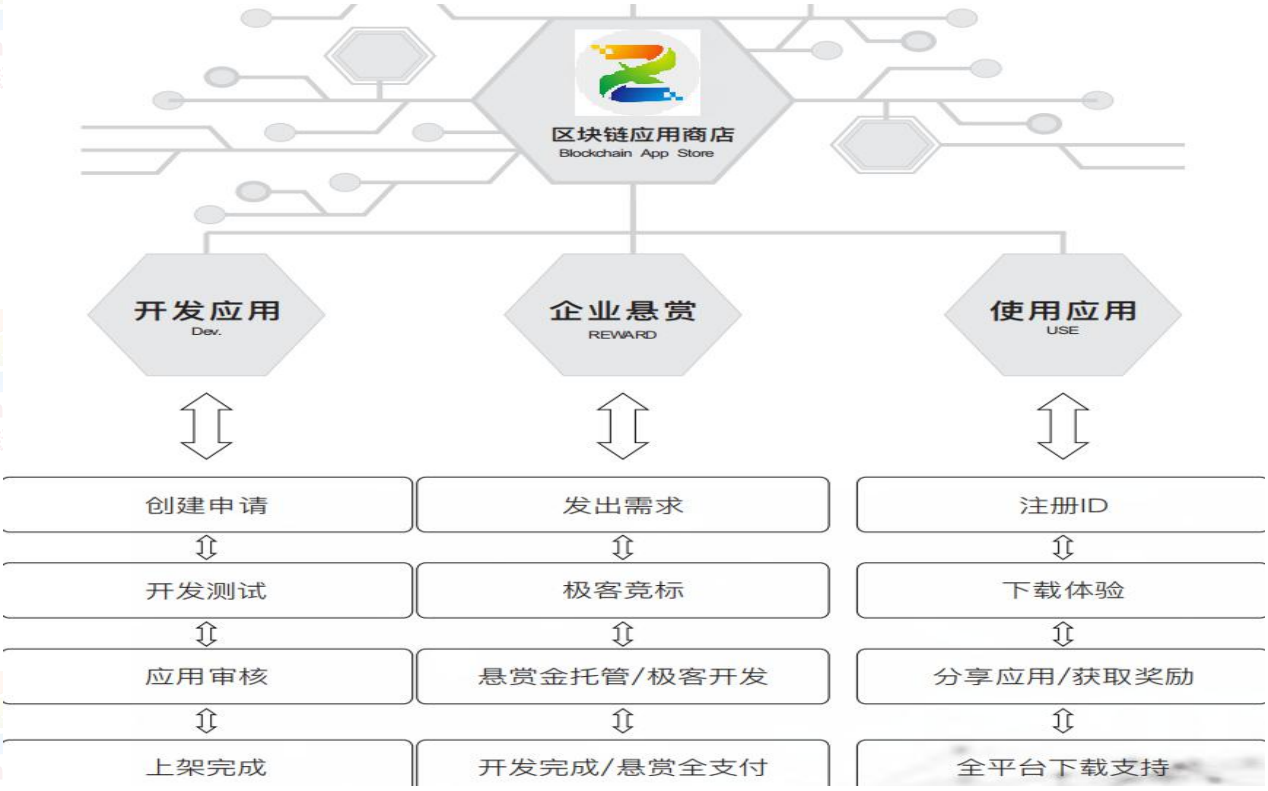
1、ZYChain生态社区账号

所有的开发者、企业者、用户者都会有属于自己的ZYChain生态账号（公钥+私钥+动态失效重验），通过ZYChain不同端口的账号可以进行相应的操作，相对应得会有三个不同得平台（D+B+C),未来ZYChain生态社区会不断壮大，那么生态社区的用户也会不断的增多，所以生态社区的账号也就成为了整个生态的ID身份证明。

2、操作系统介绍

从互联网Windows,Linux的操作系统到移动端Symbian/Android/IOS的操作系统，人类无时无刻不在追求着综合体验感更优的操作系统，从区块链现阶段来看，单单将操作系统可能还谈不上，因为没有一个完整的体系是可以用完全去中心化的方式做出来的，相应的安装部署规划等都是需要借助完善合理的中心化管理模式去进行优化，这样才能形成一个实际意义上的操作系统，这样也能够更好的让用户作为个体体验到更优的操作感，在ZYChain操作系统中拥有先进的底层技术支持及足够的性能支撑，作为操作系统我们考虑到了个体的分散端口，我们把所有个体归纳成了三个端口即企业端用户端开发端，让彼此紧密的形成一个良性生态。

3、区块链应用商店



4、去中心化交易所

中心化交易所记账式交易、流程不透明、系统有漏洞，还存在各种隐患和风险，而且有违区块链去中心化的理念。而去中心化交易所的意义在于，用户掌握自己的资产，所有的交易都在区块链上进行，所有的交易记录都可查，交易过程由智能合约代码控制。

ZYChain去中心化交易所首先会消灭那些拉盘砸盘的做市商或者“市值管理”团队。在去中心化交易所进行交易，所有的挂单都需要上链，每一次交易都会被监控，这就意味着整个交易流程的公开透明。

ZYChain交易平台同时也为在ZYChain公链上开发的联盟链TOKEN提供了难上币的解决方案，“思路决定出路”，ZYChain在去中心化交易中要瞄准的不仅仅是让用户可以在钱包里交易主流的币种，而是能与通证模式结合，让钱包真正的融入生活。

ZYChain不仅仅志在要打造区块链行业的支付金融体系，更是要打造一个资产数字化的交易平台。对标的未来不仅可以交易项目的代币，有价值的数字资产都可以进行交易。ZYChain去中心化交易平台将领航数字货币交易领域的蓝海世界。

5、信用体系

为了让ZYC的生态开发平台更加的公平公正符合区块链去中心化思想的本质，即建立属于ZYChain的生态社区正在建立一个分布式的资产行为的数据分享平台，来解决这些痛点，这样每个生态平台上的节点用户，都会拥有自己的信用体系Background Check，信用体系即是配合监管机制同时又是对生态体系规划完善的重要工具，通过信用体系可以解决生态良莠不齐的痛点问题，改善了“纯去中心化”带来的诟病，让ZYChain的生态更加的透明安全。同时,ZYChain希望从重构信贷生态开始，基于区块链技术，把数据还原给用户、把报告还原给用户，并能输出标准化的金融服务，能让个人或机构等加入生态的各方轻松接入，实现信用自由流通

运用区块链去中心化的特点，ZYChain通过消解传统金融机构或者互联网金融机构在这个环节中形成的垄断地位，真正实现个人点对点交易。在目前的金融数据体系中，很多数据被污染过，甚至有中占比高达40%的造假数据参杂其中。在数据认证的过程中，需要不断地校验其安全性、再逐步将其落地应用。同时，ZYChain也会与众多身份识别和征信数据机构合作，在区块链上构建对应每一个人在真实世界中的信用状态，并且这种信用情况是分布式的。ZYChain真在开发一个针对C端用户的开源Dapp，用户可以通过这个Dapp查看和管理个人信用信息，同时，其他流量端也可以借此基于侧链和开放平台接口开发甚至是未来开放相应借贷数字资产的依据和评判标准。

6、资产登记

我们会对ZYChain平台上的所有用户资产进行进行验证，这实际上是一个非常大的工作量，甚至是有风险的，但我们会避开那些风 险的登记，以避免一些无聊的人试图通过各种各样的登记来获得不法的收益。实质上来说这种登记能够解决大多数时候的信任问题，这就已经值得我们去尝试了。

ZYChain 的目标是将真实的资产交易市场映射到区块链上来，并最终打造一个可信赖的环球社交网络。

7、集成支付

“Internet of Asset”在以传统的方式进行“确权”和资产登记时，往往需要填写大量的材料，手续非常的复杂繁琐。整体行业的管理和效率非常低，而且中间存在着大量的信息不对称。对于过去需要2-3个月甚至更久的共商消息变更，在ZYChain上只需要几秒钟就可以完成。在交易方面，ZYChain可以解决行业的“流动性不足”和“履约风险”问题。在交易环节中，资产上链后，由于信息透明可追溯，产品的开发者以及购买企业便完全透明，降低了信用成本。而“资产数字化”方式会使得资产的流动性得到显著的提高。同时“智能协议”可以在买卖双方定好协议后自动执行，可以有效规避“违约风险”。

8、ZYChain监管机制

区块链透明化、去中心化的特点，在政府、监管者甚至交易层面，都很难被完全接受。那么 区块链应该如何让政府和监管机构适当地参与到里面的监管，又不损害到商业机构的利益和避免 降低效率呢？总账可以按照规定规则来审计全部或部分总账分录。在与参与者合作中，审计员可以通过基于时间的证书来获得总账的查看，连接交易来提供实际的资产操作。利用了密钥的层级可以控制将给予审计员检查某些交易，某组 交易的审计权限，只披露给审计实体最相关的密钥来提供控制审计的可能性。不是系统的成员的 应用审计人员，可以给予被动的观察区块链数据的手段，同时保证给予他们只是为了与被审计应 用程序相关的交易。在记录、管理和同步受监管金融机构之间的金融协议，直接设计出负责监管 与监督观察作业的节点，监管者也在账本上，交易信息经由特定交易方来验证，不需由一大群与 该交易无关的验证者。

区块链的监管，在某种程序上是促进区块链的商业应用更好落地和提供合 规性的保护，但如果过度监管也可能毁掉区块链，需要把握好尺度。同时监管机构也应紧追创新 步伐，以开放和包容的态度进行有效的新形式的监管。 对比互联网技术的发展路径，我们发现不 论是区块链技术本身，还是基于区块链技术的应用， 都处于行业发展早期，有很多值得探索的方向。 因此我们希望可以构建一个全新的区块链生态系统，作为未来世界可选的互联网价值传输协 议的可选项，并把整个区块链行业的易用性向前推进一步，这也是我们设计多原链的原因。多原链致力于拓展区块链技术的应用边界和技术边界，使普通互联网用户能感受到区块链技术的价值,并构建一个全新的基于区块链技术的开发者和用户的生态系统。

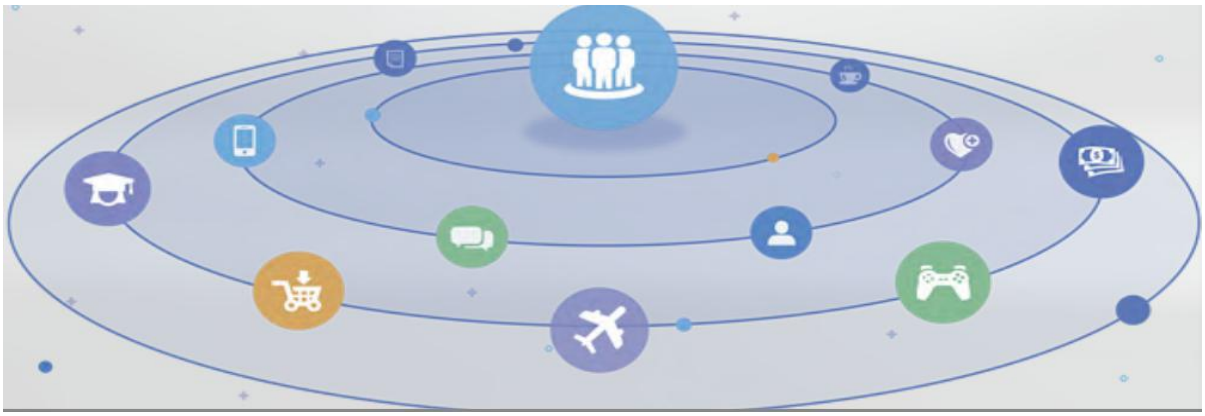
9、ZYChain安全体系

安全层面基于密码学理论中的对称与非对称双重加密算法基础上，融入了我们团队独创的不可逆四重加密（Token+公钥+私钥+动态失效重验重建）+独有核心算法，使合约传输、交易、数据更安全； 在公开性方面多原链实现了全网链+相关节点+订阅模式+智能甄别储存，加密传送隐私交

易至拥有解密私钥节点，交易哈希打包入块，隐私交易数据只在拥有解密私钥的相关节点上保存，相关节点先解密再执行交易，交易数据不会发送给无关节点；相关方有权利看到明文数据，其他无权看到明文数据，仅对密文数据真实性进行验证。另外，有订阅同一个通道的节点可以维护和分享同一个账本，形成一个个具有保密性的通讯链路。各账本之间批次隔离，形

成了一个个隐私的共识通道，完全杜绝了信息泄漏的可能。相比以太坊和EOS在隐私保护方面基于假名保护，且没有做更多的延展，优势明显。

10、ZYChain环球社交网络构建



互联网2.0已远，区块链3.0是否能颠覆Facebook,打造新型社交平台？

目前，占主导地位专属中心化的社交网络严格限制数据访问，阻碍第三方开发商拓展的问题。创业公司和独立开发者处于弱势地位，用户甚至处于被消费的处境。扭转这一趋势，构建全新的去中心化公平的社交网络的核心是加密通证（Crypto Tokens)----这是开放网络设计的新方式。

创建去中心化的网络基础设施，它融合了专属网络中的开放式。通过分散式架构，不让单一公司把持数据的拥有权，进而提升用户的数据隐私权。

2）使用Tokens激励开放式网络参与者（包括用户，开发人员，投资者和服务提供商）。通过开发新的开放网络，通证可以帮助扭转互联网的中心化的趋势，从而保持互联网网络的可访问性，活力和公平性，并带来更大的创新。同时实现用户、创作者和平台之间的报酬平等。

3）社交控矿，奖励分润。当用户创造出好的内容，比如文章、音乐、照片等，被其他用户分享或者称赞，创作者就可以获得奖励。如果你不是创作者，但当你在ZYChain上看到不错的贴子，可以点赞或者转发，这时也会获得奖励。

4）ZYChain打造端对端的加密传讯功能，用户除了写博客之外，也可以传送即时通讯、视频、图片、表情符号给其他用户，而且通过区块链的安全设计，只有用户可以看到内容，减少内容外泄或者被黑的风险。

11、结合AI数据信息解决方案

ZYChain是一个数据采集存储的基础性公链，宗旨在通过结合区块链技术和AI技术，为所有行业提供一个大区块的数据存储空间和存储技术的跨链技术。ZYChain.AI存储整体为去中心化文件数据存储整体，宗旨为在大数据浪潮中的每一个个体或群体提供永久、稳定、安全的存储服务功能，并且与任何网页浏览器的浏览功能相通，真正做到无障碍在线数据调阅管理。在CM数据生态系统中，共有三种用户角色：数据上传方、数据需求方、数据整合方。独特的点在于每一名用户的身份并非固定不变的，而是随着自身需求不断变化。数据上传方作为整个生态体系的基石，数量最为庞大，通过上传一手数据以获得Token激励，同时主动分享自有数据同样可以使整体数据存储生态处于一个信息流动的状态，

有助于保持数据的有效性并推进数据更新。借助AI的精确性选择与即时数据分类筛选，能够极大地提升数据存储能力、提高分析速度。同样，人工智能地快速学习能力与程式化也使得其更具有普适化的市场应用价值，因此借助AI对现有的数据存储公链模型进行升级改造具有广大应用前景。

12、全网全端跨平台全行业应用

ZYChain独创的全网操作系统，兼容目前所有智能操作系统，利用ZYChain底层系统开发出来的应用可以在PC电脑、安卓iPad、手机，IOS系统iPhone、iPad、Mac等众多平台上进行全网全端运行，真正实现了全网全端跨平台应用。

在ZYChain 系统中，通过不同共识机制的引入和监管的需求，可以为众多行业发展需求也提供支持。例如多原链系统中，提供的基于Proof of Time 和Raft协议融合的共识机制，可以满足可信网络中，对区块链速度和容量的要求，通过基于区块链技术的主控合约和Oracle和DataFeeds的引入，也可以引入更多线下的因素。

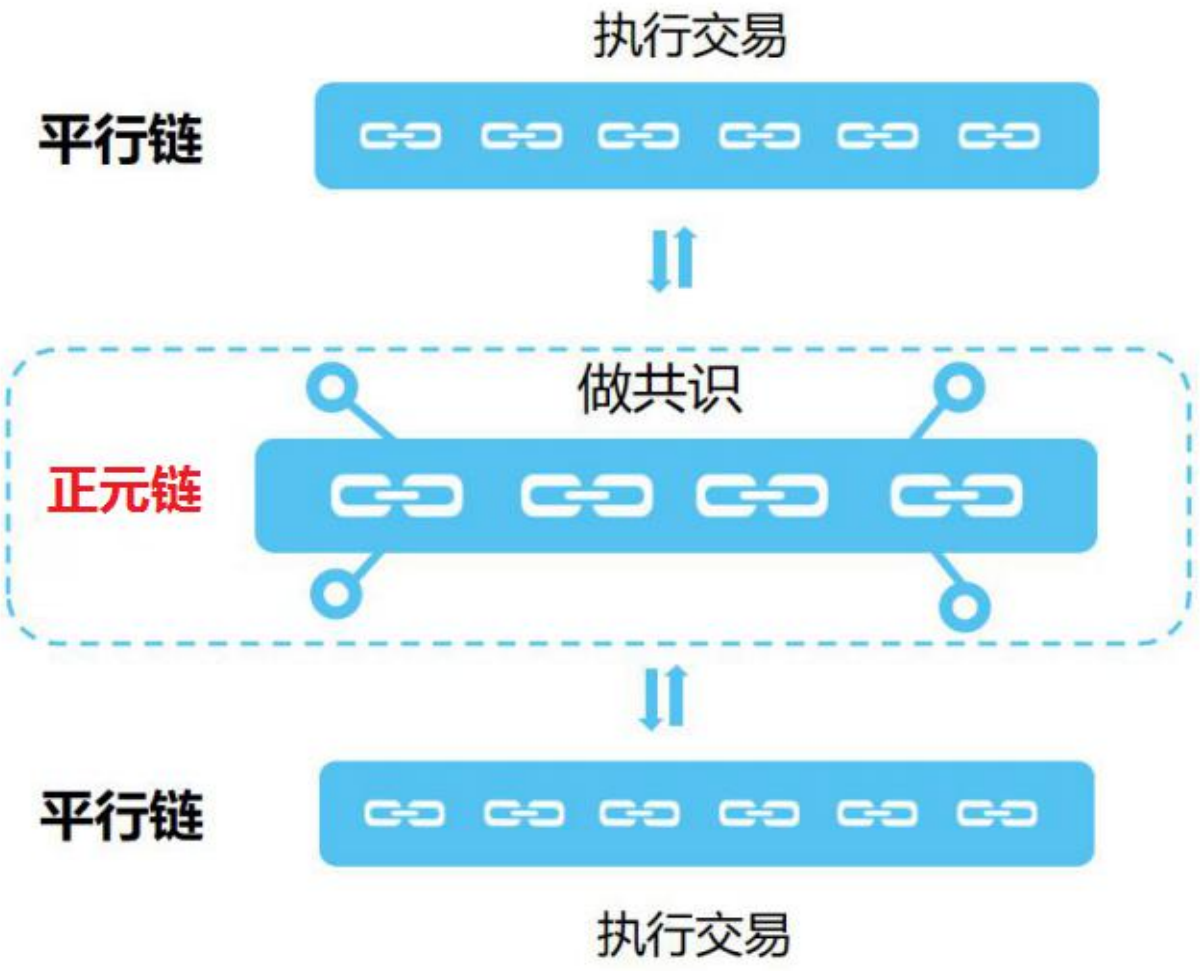
通过Identity和 Privacy的设计，可以符合金融行业的监管需求。在多原链系统中，可以支持多个行业的应用需求：例如金融业、物联网、供应链、社交和游戏、慈善、数字资产和股权等。

另外基于ZYChain的智能合约和主控合约，通过图灵完备的编程语言，可以实现更复杂商业逻辑的支持，并将支持更多的行业应用场景。

第五章：ZYChain系统的结构模块、功能及特点

系统简介：正元公链的模块化设计，是在对区块链的底层架构、应用开发的不同功能和需求进行分析的基础上，划分并设计出一系列功能模块，通过模块的选择和组合可以构成不同的产品，以满足市场的不同需求。

正元公链采用“从混沌走向秩序的开发模式”，方便开发者随时调整和扩充。从迭代和重构、以及系统的可拓展性等角度考虑，正元链将区块链的底层架构、不同应用开发的功能和需求纳入考量，对系统进行了模块化设计。包括mempool 的排队方式，加密签名的方式，共识的模式，RPC 的函数，命令行的命令，钱包的内在逻辑，数据库存储的方式等等，区块链核心的所有模块都可以定制



服务模块

客户端为用户提供了对账户，区块，节点和钱包的管理及查询功能，如新建账户，发送交易，生成随机种子，获取区块信息，获取钱包状态等。所有的交易都通过客户端，签名并加密后送入区块链。RPC 模块提供 RPC 接口给客户端，客户端通过 RPC 接口对区块链进行操作，比如创建账户，查询账户，发送交易，查询交易，查询区块信息等等。 Mempool 模块

交易缓存池,mempool 中存储从 RPC 接口来的交易,以及从 P2P 过来的交易。Mempool 的实现主要是解决共识模块的处理速度比 RPC 模块慢的问题

共识模块

正元公链主网的共识算法为 SPOS，一种支持上万人一起挖矿做共识的安全POS 算法。在正元公链生态中的平行公链也可拥有各自独立的前置共识，采用强一致性的拜占庭共识算法，并且引入了 DPOS 投票权的概念，超级节点必须将交易信息打包进区块，并且区块信息广播给其他节点，将交易信息储存在区块上，发挥共同治理社区的功能。

执行器模块

执行器是区块链的逻辑处理中心，执行器通过一个只读的数据库读取状态，并虚拟执行，执行结果只影响内存不会存盘。执行器的输入是交易，交易有多种类型，不同的交易对应不同的执行器去执行。

P2P 模块

P2P 模块连接各个节点，在全网广播交易，区块相关信息。

Blockchain 模块

Blockchain 模块主要负责接收来自共识模块的区块，存储到本地硬盘。

加密签名模块

负责交易的签名和加密，签名保证交易可以被回溯，加密保证交易信息安全。

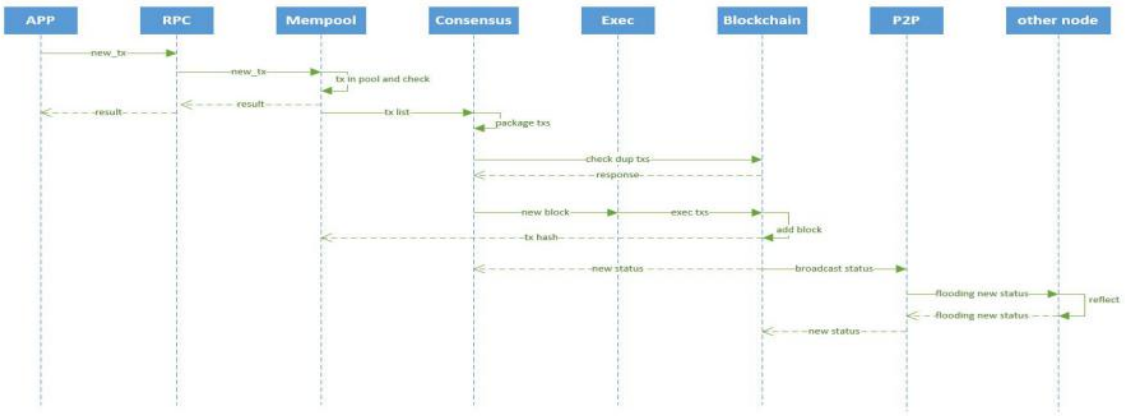
运行流程

(1) 客户端接收交易，签名并加密后，通过 RPC 模块送到节点的 Mempool 模块缓存。不同节点收到的交易通过 P2P 模块在网络内广播，保证所有节点Mempool 中的消息一致；

(2) 共识模块判断时间或交易数目等条件，向 mempool 中拉取交易列表。共识模块排除重复交易后，将交易列表打包进入区块,接着开始做共识；

(3) 共识完成后，共识模块发送区块给执行器模块来预执行,此时不写本地数据库。不同的交易类型进入不同的执行器，比如 coins 交易进入 coins 执行器。预执行完成后，共识模块再将区块送给 blockchain 模块；

(4) Blockchain 模块通过 P2P 网络将区块广播给其它节点，然后所有节点将区块存入本地数据库。



一、安全共识 SPOS

SPOS 即 Safe POS，它通过 Ticket 实现 POS 的安全挖矿逻辑。用户使用钱包账户中ZYC余额购票（挖矿权），一票对应一个唯一的 Ticket ID，同时拥有一份挖矿权；一个区块只能由一票挖出，

实际的挖矿几率各票均分（如全网有 N 张票，则一张票挖到矿的几率为 1/N）。

Ticket 挖矿流程如下所示：

钱包：定期检查账户中的 ZYC 余额来购买票，当满足购票条件后构造一条买票

交易发往区块链。

共识：它会一直尝试使用本地持有的票去打包区块，一旦打包成功，是表示对应的 Ticket 持有人挖矿成功，并获得对应的区块奖励。

智能合约：智能合约会把地址对应的票信息写入到区块链数据库，每一张Ticket 都对应有一个唯一的 Ticket ID，也会有一条数据记录在数据库。

恶意节点，试图分叉正元公链，或者任何系统能检测到的恶意行为，都可能会被惩罚，每次惩罚会损失 20%的资产。挖矿必须以正元链基金会发布的标准钱包进行，篡改挖矿行为，如果被系统自动判定为恶意，都会给矿工造成巨大的损失。

二、随机数支持

在区块链上为了体现公平性（针对游戏等应用场景），就需要一个不能被预测的随机数。目前的区块链大体有如下实现方案：

（1）合约中调用外部中心化的随机数发生器获取随机数；

（2）使用区块 hash 中的某些值作为随机数。

但是这两种方案都有非常明显的弊端，原因在于：

（1）区块链多节点之间智能合约执行结果是要求强一致的，如果合约从外部读取数据，是很有可能获取到不同结果的（比如网络原因导致有的节点读取正常，有的返回错误）进而导致分叉。

（2）区块的哈希可以被控制，导致随机数被控制。由于一些区块链系统没有提供很好的随机数算法，所以很多 DAPP 开发者会自己封装自认为完美的随机数算法导致随机数被预知。

正元公链实现了在随机数上的优化，在原来的随机数基础上引入了 VRF（Verifiable Random Functions）可验证随机函数逻辑，使得随机性进一步增强，以下是具体实现逻辑：

首先，用户使用钱包账户中的 ZYC 购买票（Ticket），10000ZYC 对应一票。钱包同时生成一个 randNum，哈希过后再结合钱包挖矿地址的私钥，票对应的 index（一次可以买多张票）等元素再做两次哈希，得到一个公开哈希参数（pubHash）：pubHash=hash(hash(privateKey:index:hash(randNum)))然后，新购买的票中包含这个 pubHash 以及 randNum 并存入区块链，这张票有 12 小时的成熟期，过了 12 小时才可以参与挖矿；接着共识算法从区块链中找到已经成熟的票（Ticket）开始打包，由于共识打包区块操作只在节点本地执行，所以它可以读取本地存储的私钥，算出一个私密哈希（privHash）并将这个参数放入到挖矿交易中：

privHash = hash(privateKey:index:hash(randNum))

最后，智能合约收到挖矿交易，对比 hash(privHash)和 pubHash 的值，两者一致挖矿交易成功，对应的节点获得挖矿奖励，否则挖矿交易执行失败。

VRF 关键术语

SK, PK: VRF 中使用的公私钥对，SK 为私钥，PK 为公钥

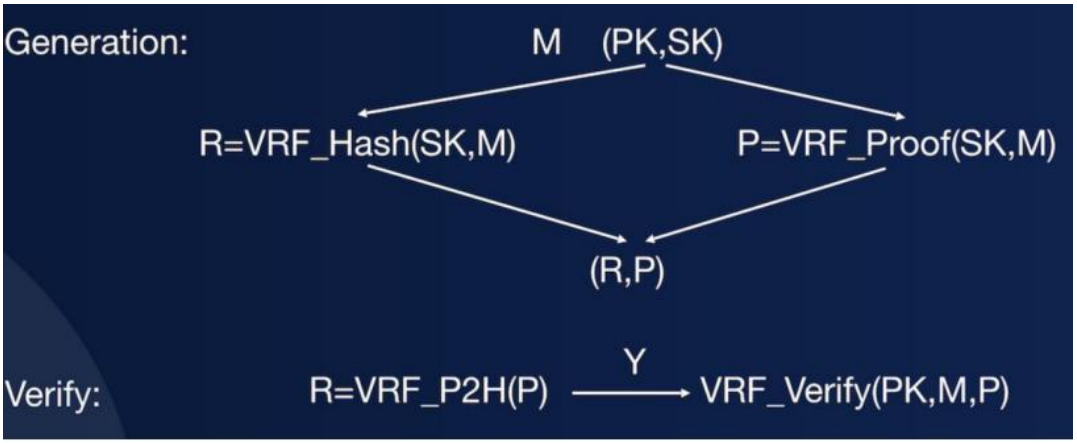
M: 输入数据

R：VRF 哈希输出

P：VRF 证明

Prover：证明者，拥有 VRF 公私钥 PK 和 SK

Verifier：验证者，拥有 VRF 中的公钥 PK



包括四个函数，分为两类

生成函数

R=VRF_Hash(SK,M)　P=VRF_Proof(SK,M)

验证函数

R=VRF_P2H(P)　　VRF_Verify(PK,M,P)

VRF 使用流程

(1) 证明者生成一对密钥，PK 和 SK

(2) 证明者计算 R = VRF_Hash（SK，M），P = VRF_Proof（SK，M）

(3) 证明者把 R，P，PK，M 递交给验证者

(4) 验证者计算，满足 VRF_P2H（P）= R 并且 VRF_Verify(PK，M，P）= True

即验证通过，否则验证不通过

ZYChain使用 VRF 实现随机性的流程

(1) SK 对应挖矿节点账户的私钥， PK 对应挖矿节点账户的公钥。

(2) 在 2020 年 ZYC 升级分叉的那个高度，挖矿节点先读取前一个区块中存储的 privHash 作为输入 M，并通过 VRF 生成函数分别计算出 R 和 P。

(3) 挖矿节点将 R 和 P 写入挖矿交易中，打包进区块并广播。

(4) 所有节点收到区块，在智能合约中通过 VRF 验证函数来验证正确性(满足 VRF_P2H（P）= R 并且 VRF_Verify(PK，M，P）= True 即验证通过，否则验证不通)

(5) 再往后的区块，读取前一个区块中存储的 R 作为输入 M 来计算 R 和 P。

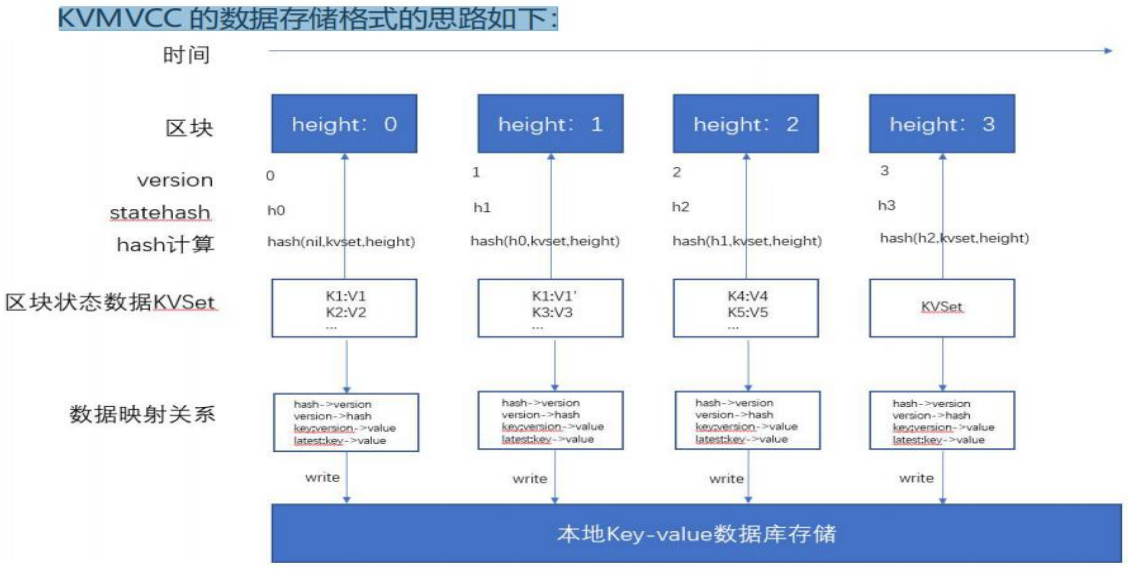
(6) 可以看出，当前区块引入的随机数，都需要依赖于上一个区块的随机值 R ，随机值更不容易控制，随机性大大增强。

因此，SPOS 共识的实现结合了随机数，由于一般情况下是无法预测其它节点的共识信息，所以也无法获取到它的共识随机数。并且系统设定私密哈希（privHash）不能提前泄露，就算有恶意矿工自己提前暴露，它对应的票也会被作废，同时本金会被冻结较长时间（2 天以上）。再加上系统设定票需要经过 12 小时的成熟期后才可以参与挖矿，以及在共识逻辑中引入 VRF 可验证随机函数的实现，每一个区块的随机值都依赖于上一个区块的随机数 R，随机性进一步增强。这些条件组合起来，系统的随机数几乎是无法被操控的。这样当开发者实现的 DApp 中需要保证公平随机时，就可以直接使用系统提供的这个安全的随机数了。

三、支持 MVCCKVDB 的存储方式

正元公链区块链率先创新实现了 MVCCKVDB（多版本 KV 数据存储），传统的区块链是以 merkle 树或是 MPT 树的形式来存储数据，每次数据的改变，树都会做一次重构，效率比较低下。 例如，对于一颗 20 层的默克尔树，查询一个叶子节点的数据需要进行 20 次读操作来完成，导致数据查询的效率仅为普通数据库的查询效率的 1/20，对于每秒能完成 10 万次读操作的系统，每秒仅能读取 5000 笔交易的数据，大幅限制了系统的读取性能。写数据时，同样要加载树型分支上的多个节点数据，并最终要在更新以后写入到磁盘，这里面的操作消耗也是比较大的。

正元公链借鉴了数据库设计中的 MVCC 理念（Multi-Version ConcurrencyControl 多版本并发控制），设计了独创的 KVMVCC 的数据存储格式，用于改善 MAVL 或者 MPT 结构中存在的低效的问题，更好的满足区块链数据增长到一定规模后的保持较高的数据读写性能。



Hash 计算：

statehash=hash（prevstatehash，KVSet，height），包含了前一区块的状态 Hash 信息，本区块的状态数据 KVSet 信息，本区块的高度信息（也就是版本信息）。

有以下对应关系会被存储到每个节点的数据库中：

hash->height(version)

height(version)->hash

key:height(version)->value

lastest:key->value

数据查询：

根据 statehash 可以查找到对应的 height（version），根据 height 可以查找到对应高度时，具体 key 值对应的 value 值。

数据验证：

对于特定高度 height 的 KVSet，可以根据前一区块的 hash 值 prevstatehash、KVSet、height 进行 Hash 运算，如果 hash 值相符，则数据未被篡改，否则，数据被改动或者数据有误（高度有误，或者 KVSet 数据有误）。

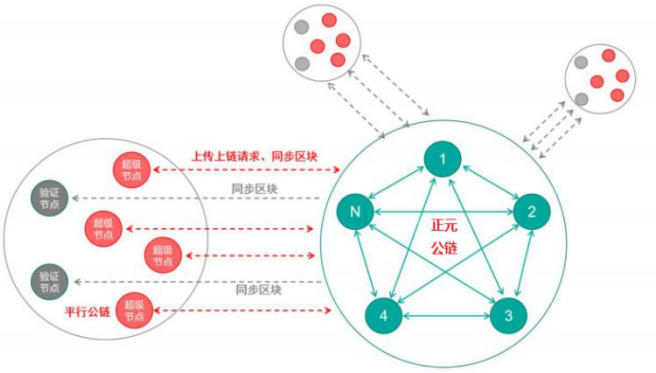
对于最新版本数据的维护：

特别的，当对于最新区块的 key、value 值进行存储时，同时保留（新增key）或者更新（已经有历史版本的 key）key:latest->value 的映射关系到本地 key-value 数据库中存储。当需要获得最新的批量数据时，可以根据 latest前缀（可以自定义）来批量查询最新数据。由于通常的 key-value 数据库可以很好的支持前缀匹配查询，查询效率会比较高，远高于默克尔树存储结构的查询。

四、EVM WASM JSVM 三类虚拟机的支持

EVM 是以太坊智能合约虚拟机，用 Solidity 编写智能合约，正元公链兼容以太坊上的合约。EVM 的部署方式为，通过正元公链提供的接口将智能合约部署到正元公链的 EVM 虚拟机中，也可以通过接口调用 EVM 合约来执行智能合约。 WASM ，用 C++编写智能合约，正元公链兼容 EOS 上的合约。 WASM 的部署方式为通过正元公链提供的接口将智能合约部署到正元公链的WASM 虚拟机中，也可以通过接口调用 WASM 合约来执行智能合约。JSVM，用 Javascript 编写智能合约，Javascript 开发者众多，可降低区块链开发门槛。JSVM 的部署方式为，通过正元公链提供的接口将智能合约部署到正元公链的 JSVM 虚拟机中，也可以通过接口调用 JSVM 合约来执行智能合约。

五、平行公链



正元公链的平行公链其实就是独立的应用链，这些链共享正元公链的 SPOS 共识，从而实现低成本部署极具公信力的公链系统。平行公链拥有自己独立的钱包和服务，例如发行数字资产等。只要保证正元公链的安全性，即可保证正元公链生态系统中其它平行公链的安全性。随着平行公链的增加，正元公链节点也将迅速增多，并且更加分散，DDOS 攻击力也会减弱，就可以保证正元公链生态的安全。

在正元公链生态的基础上，结合开放平台的 API 和 SDK 就可以开发独立逻辑、容易升级的平行公链，这就像安装 Windows 系统一样简单，可节约巨大成本，各行业机构不必再为区块链底层基础设施研发消耗庞大的人力物力。

在正元公链上可开发多条平行公链，各条平行公链既可独立开发DAPP，建设多样化的应用生态，又可实现多链间的跨链互换功能。现在市面上的交易所大部分都是中心化的。特点主要就是为了提升效率和方便，所以是必要牺牲一部分的安全性。随意很容易被黑客攻击，对安全性要求非常高。所以能做到这一　安全性能要求的交易所也很少。中心化的交易所在体现形式上主要分为两种形式，资产控制和系统管理。

六、超级节点

为了提升区块链的性能，平行公链一般采用 DPOS（股份授权证明机制）共识，即在链上选拔出数个付出算力和宽带支持的超级节点，这些超级节点必须将交易信息打包进区块，并且区块信息广播给其他节点，将交易信息储存在区块上，发挥共同治理社区的功能。一条公链成功与否，其中一个重点衡量指标就是其链上的节点数。超级节点机制可以帮助平行公链快速建立链上生态，并依靠各个超级节点的运营、维护，促使平行公链生态变得更加繁荣，实现一个更加稳定、强大、去中心化的区块链系统。同时，平行公链运营方可设立平行链基金会，通过基金会对超级节点的各类token 激励机制、运营手段，促进超级节点的能动性和积极性，并通过 token的回购，交易手续费等方式，促进平行公链健康且可持续的发展。

七、一键 Token

以电子数据形式存在的资产被称为数字资产。区块链技术的运用，使数字资产拥有去中心化、去信任、可追踪朔源的特点。正元公链主要实现了资产数字化、一键 Token 的功能，同时也支持所有平行公链上发行各自的唯一 Coin 和多种 Token。

用户可在正元公链及所有平行公链上登记资产，实现资产数字化。一些流动性不足的资产，诸如房产、黄金、大宗商品、积分、白条等，可以通过数字化、证券化，增加流动性，实现价值的转移。

用户可通过填写表单一键发行 token，无需编写代码，也不用担心代码的错误对正元公链网络产生影响。同时 token 名字在同一条平行链上具有唯一性，避免了生态内数字资产的重复和混淆。

八、钱包找回

正元公链及平行公链，均预设钱包找回功能，解决了私钥丢失而导致数字资产损失的问题。当用户因遗失钱包或者存储设备突然损坏引起的私钥丢失，可以通过低权限的备用私钥（自己保存或者托管给信任的机构/人）找回自己的数字货币，找回指令并不会立刻转移数字资产，而是会在预告一段时间后生效，所以若备用私钥被冒用，用户也可及时发现，并用原私钥将数字资产转移到安全钱包，避免损失。

九、隐私支持

区块链技术不可篡改、分布式的特质，的确能够避免用户的隐私被中心化机构掌握从而导致被贩卖、被黑客攻击等的问题，但公开透明的账本，却让海量用户数据在链上曝光，隐私问题依旧如空中楼阁，没有得到根本解决。打个比方，原来在淘宝上购物，现在去中心化，不通过淘宝交易，甲乙双方直接邮寄。虽然没有淘宝掌握这两者交易的数据，但是他们交易数据被记录在区块链网络上，任何人都可以查看。

基于账户和 UTXO 混合模型，正元公链实现了区块链隐私交易系统，在使用UTXO 系统的同时，保留了账户体系，加入环签名和一次性地址，让账户在隐私和公开之间自由流转，同时具备不可追踪性和不可连接性。

(1) A 生成随机数 s，并计算 h = hash(s)，将 h 发送给 B；

(2) A 生成 HTLC，超过时间设置为：2 小时，如果 2 小时内 B 猜出随机数 s，则取走 1BTC，否则 A 取回 1BTC；这里 A 用 h 锁住 BTC 合约，同时 B 也有相同的 h。这样 A 和 B 都有相同的锁 h，但 A 有钥匙 s；

(3) B 在以太坊里部署智能合约，如果有谁能在 1 小时内提供一个随机数 s，让其 hash 值等于 h 则可以取走智能合约中 20ETH；

(4) A 调用 B 部署的智能合约提供正确的 s，取走 20ETH；

(5) B 得知 s，还有 1 小时时间，B 可以从容兑现 A 的 HTLC 的 1BTC。

一旦超时，交易失败，符合原子性。

Hash Locking 极大地提升了正元链生态网络的交易处理能力。交易双方若在区块链上预先设有支付通道，就可以多次、高频、双向地实现快速确认的交易支付；双方若无直接的点对点支付通道，只要网络中存在一条连通双方的、由多个支付通道构成的支付路径，闪电网络也可以利用这条支付路径，实现双方之间资金的可靠转移。

十、锁仓合约

用户可以使用锁仓合约冻结一部分资产，按规则定期解冻给相应的受益人，适用于分期付款，员工激励，遗产分配等应用场景。

功能提供以下 3 类操作

（1）创建定期解冻合约：创建时指定所要支付的资产类别和资产总量，以及定期解冻的形式。

（2）受益人提币：受益人提走解冻了的资产。

（3）发起人终止合约： 发起人可以终止合约的履行。

解冻的形式目前支持两种

（1）固定数额解冻：根据指定的时间间隔，解冻固定数目的资产。

（2）按剩余量的固定比例解冻：根据指定时间间隔，按剩余量的固定比例解冻，这种方式，越到后面解冻的越少。

十一、多重签名

正元公链系统最多可支持 32 个独立私钥控制多重签名账户，用户可以自由定义每一把私钥的权重，最终可以由权重来判断能不能发起交易，保证账户的安全。并且同时可以预防某把私钥丢失，账户金额无法找回的情况。如：有一个钱包设置了 3 把私钥，但每把私钥被授权的票数不同，张三、李四、王五三个人，王一的私钥可以有两票权重，如此当王一发起交易时，他只需要张三或李四任一人的私钥签名，就可以成功发起交易，反之如果只有张三和李四两个人发起交易，但是王一没有签名，他们俩总共只有两票，就无法发起交易了。

十二、支持预言机功能

预言机实现了区块链和真实世界的链接，预言机是一种可信任的实体，它通过签名引入关于外部世界状态的信息，从而允许确定的智能合约对不确定的外部世界做出反应。预言机具有不可篡改、服务稳定、可审计的特点。预言机合约发布数据分为三个步骤：

（1）发布数据发布事件（告知全网，将有某个事件的结果于未来公布，并分配唯一的事件 ID，如果事件未发生，可以进行撤销）。

（2）预发布结果（数据提供者预发布时间结果，如果被审计发现结果有问题，可以撤销）。

（3）发布结果（预发布结果经过审计后，最终全网发布，不可篡改，可审计追溯）。

其他合约（比如竞猜合约）可以使用上述步骤 1 中的事件 ID 和具体事件来开展（竞猜）活动，当步骤３结果公布后，竞猜合约根据事件 ID 对应的结果来触发合约完成竞猜结算，实现了无人干预的客观、可信、可审计、可追溯的公平竞猜。

十三、去中心化 C2C 交易

传统中心化交易方式，仰赖平台做信用背书，以保证交易真实可靠，但也暴露出个人隐私和资产被盗的风险。个人无法掌握自身信息，但在正元公链网络中，个人交易信息分散式地储存在所有节点上，任何人都可以公开检阅，形成多中心化的数据储存模式。跳过中心化平台直接进行个人和个人之间的交易，交易效率较高。在正元公链系统中，每个节点都具有高度自治的特征。任何一个节点都可能成为阶段性的中心，但不具备强制性的中心控制功能。节点与节点之间，会通过网络形成非线性因果关系，实现去中心化、开放、扁平、平等的系统。

相较于集中式的交易，由于监管客户资金需要遵守管理机构的相关规定，需要跨越很多障碍。通过这种方式来进行交易的用户，必须遵守集中式交易服务商的各种规则且支付相应的费用。正元公链的 DEX（Decentralized Exchange)去中心化交易规则能解决这方面的问题，实现既便捷又安全的交易。正元公链实现 DEX 去中心化交易的方式有两种:比特币跨链支持(BTC Relay）和Hash Locking。

十四、比特币跨链支持（BTC Relay）

使用 BTC Relay 指的是在正元公链上置入 BTC 轻钱包，从而实现DEX 去中心化交易。轻钱包（Simplified Payment Verification）指的是简单支付验证。中本聪在论文中简要地提及了这一概念，他指出：不运行完全节点也可验证支付，用户只需要保存所有的区块头（block header）就可以了。用户虽然不能自己验证交易，但如果能够从区块链的某处找到相符的交易，他就可以知道网络已经认可了这笔交易，而且得到了网络上多少个节点确认。BTC Relay 指的就是把比特币区块头拷贝到正元公链上，在正元公链上虽然无法验证交易，但是能够从比特币的某处找到相符的交易，就可以得知网络已经认可了这笔交易。采用这种方式，可以撮合任何有交易意向的双方进行交易，交易保证会在 6 小时内完成。整个过程交易双方信息都是匿名的，无需第三方担保。

十五、跨链原子交易

正元公链在跨链交易上采用 Hash Locking（哈希锁定）的方法，可以用非常简单的方式实现跨链原子交易。原子互换就是在利用正元公链的脚本语言来构建智能合约，授权进行跨链交易。哈希锁定起源于闪电网络的 HTLC（Hashed TimeLock Contract），它的实现过程如下，以 20ETH 和 1BTC 的原子交换过程为例：系统管理上就是为了使用网站流量。中心化交易所通常将储存数据和支持基础设施的服务器外包给云服务，这样托管服务器就是在单个源中进行分配。所以安全性能上就会有损失，黑客只需要通过中央入口通道，就可以对交易所进行攻击。因此中心化的交易所在安全性能上有损失，同时也会存在很多的安全问题，用户将数字资产放在交易账户中，一旦黑客攻击就会损失严重。同时，中心化交易所依赖于中心化信用背书，涉及到的安全风险有：内部运营风险、商业道德风险、资产盗用风险。

综上所述，正元公链ZYChain具有安全性高、拓展性强、速度快等特点，非常适用于中小微企业的链改开发需求。

第六章：链商钱包的功能及特点

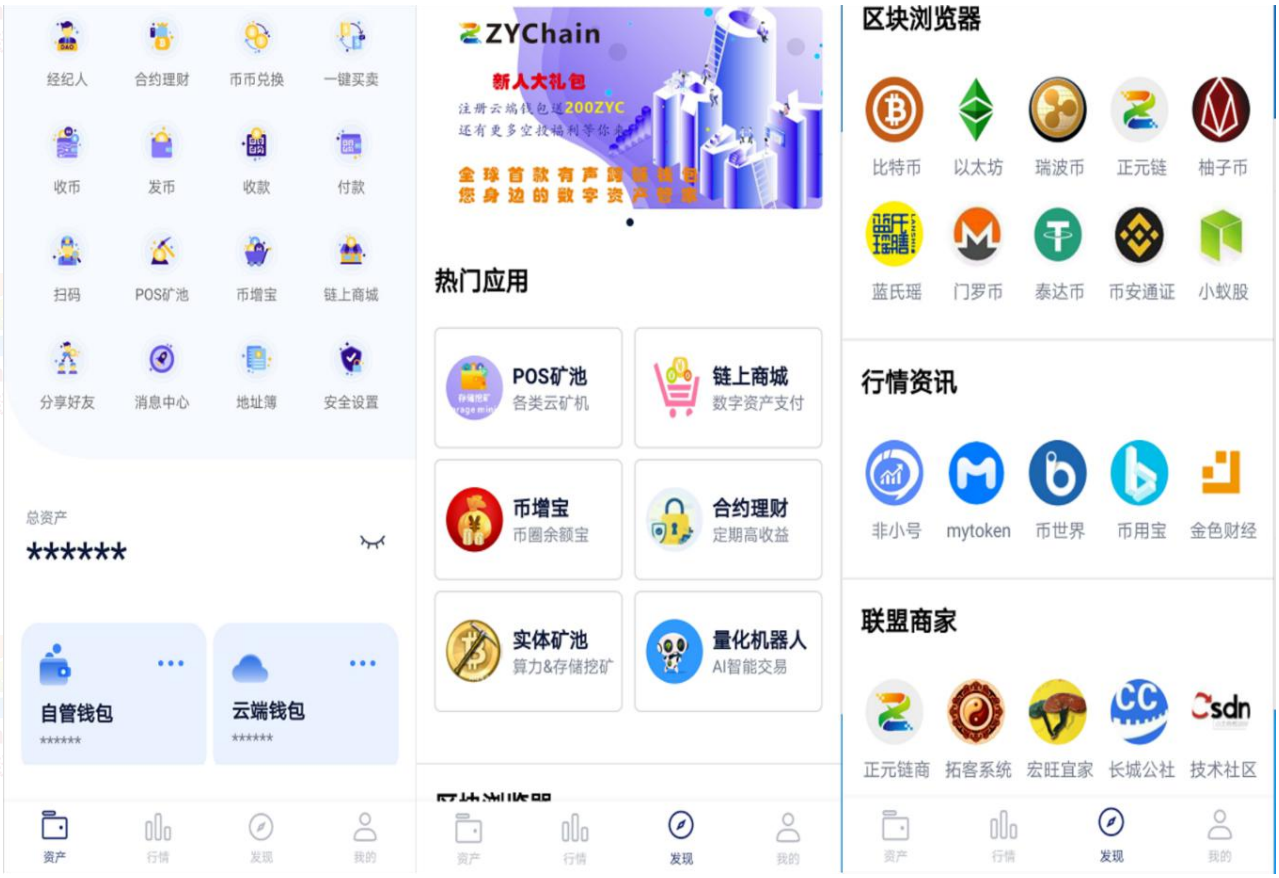
链商钱包是区块链领域全球首款有声跨链钱包，具有资产自管、资产共管、云端钱包等多项功能；供商家、企业、个人免费使用，共建开放的生态平台！

更具有以下几大特点：

一、收款到账智能语音提醒　　二、更人性化的中英文助记词

三、钱包秘钥找回功能　　四、双重PIN设置让资产更安全

五、一键消费、娱乐、理财功能　　六、 多签名共管钱包与币币兑换



链商钱包十大功能让更多人轻松使用，更安全、更便捷、更丰富

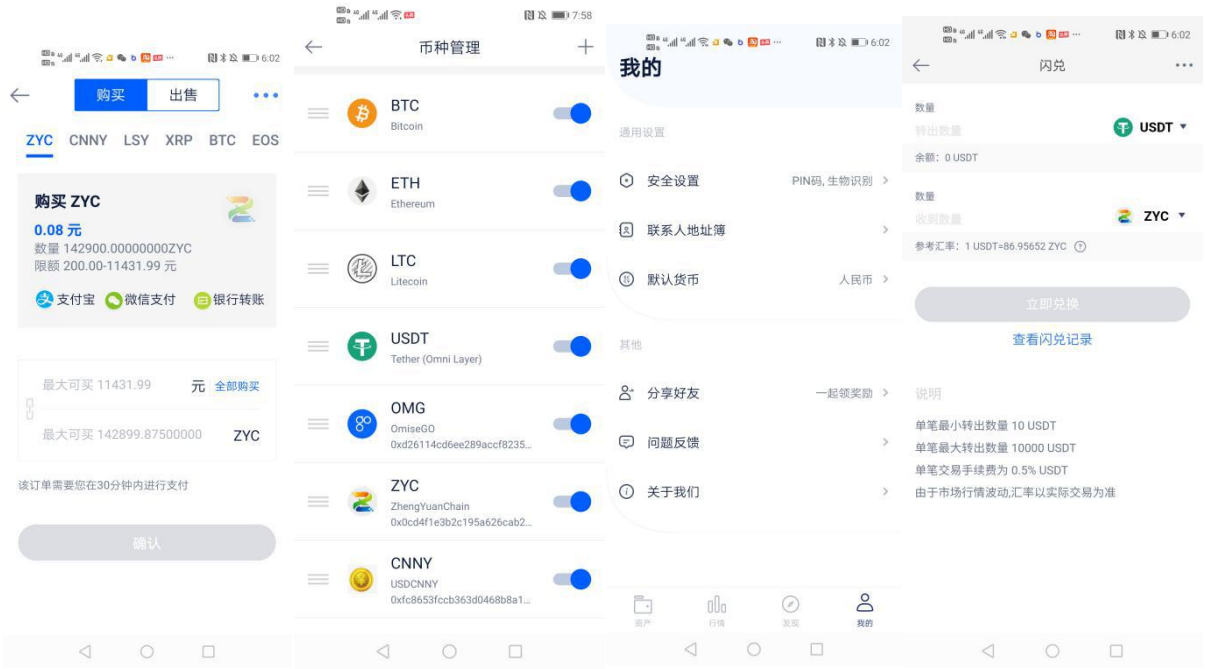
1、存储多链数字资产　　2、理财挖矿有收益

3、消费、购物和娱乐　　4、实时行情展示

5、一键买卖功能　　6、币币兑换功能

7、一键上链服务　　8、经纪人推广收益

9、内置STO交易所　　10、社交、建群直播打赏



第七章：企业链改服务

基于ZYChain底层开发的商用区块链公链系统，正元链商为中小微企业提供链改一站式服务，包括链改商业模型设计及拓展商业生态；软硬件技术开发及全程孵化服务。

我们先来看目前大家习以为常的链改，其本质上是币改。即通过帮助企业写白皮书，发行ERC20代币，上交易所或者通过ICO来融资。这种方式最大的问题在于对于币的估值是拍脑袋的，或者出于一些非法的目的。我们所提出的新链改，其核心是围绕可信数据，进行合理的估值。可信数据具有4个特点，第一是不可篡改的数据，第二是全流程数据，第三是通过哈希存证的文件，第四是多方维护的数据库。

第一个特点数据无法篡改与删除，第二个特点全流程数据，我稍微扩充一下。大家都知道比特币可以通过任何一个账户往前查，最终查到这枚比特币是从哪一个矿工那里挖出来的，也就是coinbase账户。这个追溯到的过程就是数字货币的流程，如果是一枚假币，我们是不可能在比特币网络上追溯到整这种通过全流程数据的查询来确保最终数据的可信性，是一种通用方式个流程的。通过这个，我们可以比较容易的理解，全流程数据对于数据的可信性非常重要。

在供应链金融领域，为什么银行能够对那些提供了完整的单据、发票、票据的业务提供金融支持呢？其原因就在于在供应链上这些数据都被证实可信，而这种可信来源于两种，一种是上传这些数据的主体是可信的，比如那些银行以及大型企业，另一种则是来源于从技术上面确保不可篡改的数据。后者更需要全流程的数据，而能确保全流程数据可信的技术手段就是区块

链，所以区块链技术在那些没有主体信任为基础和背书的应用场景中，能够提供全流程的可信数据，进而对接金融机构进行金融服务，这才是区块链技术运用于供应链金融的刚需场景。

关于可信数据的第三个特点，哈希存证的文件，我们可以参考Ipfs加区块链的用法，通过Ipfs保存文件后，我们可以获得这个被保存文件的哈希指纹，这个哈希指纹是定长的，有64字节，128字节等等，区块链将这些哈希指纹保存在链上，用于对原始文件进行指纹比对，一旦原始文件发生改变，哈希指纹就无法匹配成功，于是就证明了这个文件已经被篡改。可信数据的第四个点特点：多方维护的数据库，应该是最重要的特点，我经常会被问到，区块链和服务器到底有啥差别，答案就是服务器上是单方维护，而在区块链上可以多方共同维护数据库。这种多方共同维护的机制决定了链上数据的可信度更高。正是这种高可信的数据，才为产生这些数据的基础业务提供了增信。也就是区块链技术并不在强主体信用的应用领域有任何优势。我们经常听到，银行在区块链应用上，基本上都是POC项目，为什么会这么尴尬呢？因为银行的供应链金融业务是基于核心企业的主体信用，他们对于区块链技术没有刚性需求。只有可信数据才能真正的为普通企业提供供应链金融，为中小企业业务增信，这个是我过去三年来不断探索出来的一个重要结论。

那么为什么可信数据又能够成为资产呢？对于企业资产最经典的定义是指由企业过去的交易或事实形成的，由企业拥有或者控制的预期会给企业带来经济利益的资源。在这里我们可以看到企业的资产，源于流程，源于交易，源于事实。再来看看固定资产的定义，固定资产按其来源，可以分为购置的、建造的、无偿或有偿获取的、置换取得的、盘盈的以及接受捐赠的等等。

可以发现，无论是固定资产还是通常的资产，他们都是由一段段历史合成的，这段历史发生在交易当中，发生在过户当中，发生在流程当中，如果我们去买二手房，这个房子在房产交易登记中心没有任何的历史记录，你敢买吗？因此通过全流程的可信数据，我们可以得到可信的资产。这个也是我们所提出的新链改的核心概念，即数字资产来源于全流程的可行数据，而不是拍拍脑袋或者画一个大饼产生的，新链改的前提是对于企业业务，企业资产进行全流程的记录，并且这种记录并不是由企业单方面实施，而是由企业和企业的合作伙伴共同来维护，从而建立可行数据。基于这些可信数据，以及对于这些可信数据价值的评估，我们才能够发行所谓的数字资产。我这里把我们研究所得到的5种类型简单分享如下：

1、流程型：进销存管理、ERP系统、OA系统、订单管理、业务台账、物流管理、仓库管理、智能制造等

2、契约型：合同、确认函、报价、投标、存证等

3、权益型：不动产登记、知识产权登记、票据、单证、数字资产、大数据所有权等

4、价值流通型：应收应付帐管理、抵押/借贷管理、数字货币、去中心化交易所、游戏道具与积分等

5、民生政务型：政务流程管理、食品溯源等

我们根据这些类型做了非常详细的分类，整理出了140多个可以使用的场景，并把这些场景进行高度的抽象，开发区块链产品。

我们希望通过ZYChain系统，能够为企业打造可信数据，可信流程，可信资产做出一定的贡献，当数据流程以及资产都可信了之后，企业自然而然就能够对接金融应用，或者说他不需要对接那些金融机构，也会嗅着这些数据的味道，闻风而至。

2019年Q4正元链商和蓝氏瑶（实业）集团达成全面战略合作。正元链商坚信有实体经济背书的应用场景才有价值，而其对于实体经济的赋能优势才得以体现。依托区块链赋能实体经济所演化的应用场景能够帮助现有实体经济企业适应新一代数字信息化市场经济的发展需求，实现商业模式创新，挖掘新型有效市场，创造经济价值。

第八章：ZYC生态通证

正元公链打造的是一个分布式商业平台。它的组织边界（所有者、生产者、消费者）是模糊的。

这三个角色有可能是融合的，一个人可能是生产者也可能是消费者，同时也可能是所有者。比如说在一个公链上面，有人在上面发了段视频，他是生产者。同时呢，他也会看别人发的视频，他也是消费者。另外，因为他要消费这个公链上的视频，他需要购买Token. 而这个token 随着公链的发展，价值上升了。从收益本质上讲，他也是所有者之一。这样，就能最大程度的调动Token

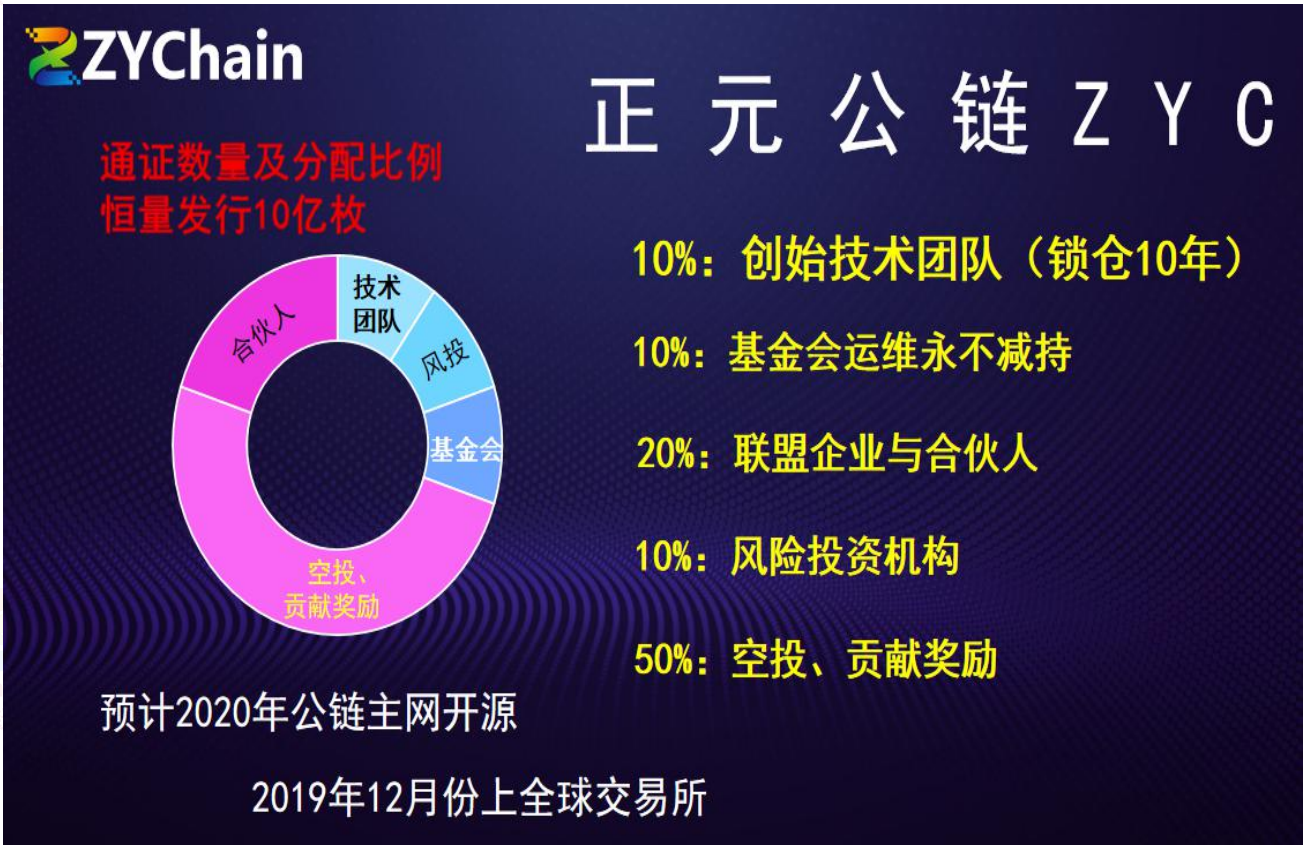
持有者创造力。同样，Token 可以应用于闲置资源兑换，物物交易或者物品租赁，用户在“ZYChain”可以租出转让二手资源或者闲置资源，使用者支付Token 给提供者，而使用者也将获得一定的Token 奖励。无论是购买、点赞、好评或者打赏，这一切都是由Token 来进行激励的。从经济角度出发我们发行了ZYC，上线平台会以国际一线交易平台为准，我们推出了ZYC，未来因为ZYC多维度的价值空间（社群、生态、应用、技术）会对ZYC的经济价

值做出一定的刺激和持续的增值，作为一种价格稳定的交易媒介通过快速的交易撮合，商家得到了价格稳定的法币，用户使用了数字资产进行消费。

从生态市场来看，ZYChain是一个具有自我造血能力的区块链项目，其从定义上就超越了“链”这一概念而是成为了真正的一个底层生态开发平台，从三个不同的端口（开发端、用户端、企业端）实现了三位一体的生态战略，彼此之间相互依靠相互发展，从而真正的实现了生态平衡的理念，通过再ZYChain上面的不断开发从而吸引到不同的开发者，持续的良性循环，形成真正意义上生态发展。

正元公链打造自己的ZYC Pay体系。在ZYChain平台上有一个市集功能，用户可以在平台上买卖东西、做众筹，并使用ZYC 作为交易。

生态通证ZYC作为ZYChain底层系统的技术燃料，不仅能在ZYChain生态系统中进行流通，而且体现了持有者的身份权益。



发行机制

为了适应未来区块链的应用落地和生态扩展，正元链采用SPOS发行机制。预计在 2020 年区块链 3.0 版本主网上线，并同步完成ZYC 的映射。

正元公链主网每 15 秒生成一个区块，每个区块产出30 个ZYC，其中27个ZYC 由矿工获得，另外3个ZYC 进入发展基金。

第九章：发展历程及未来规划

未来规划

2019年Q4，完成正元公链底层架构的设计和开发，同时链商钱包、链上商城上线;引进全球五家以上的数字资产交易所，孵化十家以上的中小微企业上链，建立区块链领域的平行公链联盟，逐步完善链商生态圈。

2020年，去中心化STO交易所 BETA 上线公测

2021年，白云易道国学院正式成立

2022年，正元链商集团正式组建完成，市值将达到千亿元以上

前期：区块链商业应用开发时代3.0目前处于前期，上图是我们的规划与时间架构，由官方团队为开发主力，满足客户开发需求。客户只需付相应数量的ZYC令牌作为开发酬劳，即可完成区块链+商业应用的开发，实现基于区块链的商业想法或创意的技术落地。开发完成后，ZYChain官方团队将公布应用开发技术细节，并制作成开发案例， 免费共享给全网及其他开发团队学习。

中期：随着开发订单数量的上升，官方团队将逐步无法匹配订单需求量。我们将 根据官方技术团队承载的开发量上升情况，部署1500平米孵化园，邀请传统IT领域的高水平中、小型外包开发团 队免场地费入驻并免费进行培训指导， 并提供海量区块链+开发需求订单。

后期：根据悬赏开发订单的数量上升情况， 我们将在开发过程中提前向政府申请或竞标一块土地作为大型孵化园，容纳更多的大中小型外包团队进场，并提供海量区块链+开发需求订单。

第十章：发起人及运营团队

正元链商由国内首个IPFS矿场创始人、国内知名品牌创始人、上市公司创始人，澳洲知名证券交易所持有人联合发起。团队成员有数十家区块链交易所搭建的经验，具有极强的创新能力，同时诚聘国际知名区块链专家和法律、经贸、管理专家组成强大的专家顾问团，为整个项目的健康运营保驾护航。

正元链商发起人：贵妃

CCTV【影响力对话】嘉宾

道家五术传承人易学研究者

湖南睿蜂堂养生品牌创始人

国家首批区块链技术咨询师

币发集团矿交所联合发起人

长城公社区块链联合创始人

正元链商集团总架构设计师

（1）许基云（顾问）

澳泽商学院主席

澳洲宝泽资本执行董事

澳洲杰出华人经济领袖

亚太证券交易所大股东

（2）施道明（顾问）

圣贤国学大师

九成思想创始人

深圳圣贤智慧发起人

币发矿交所创始人

（3） 储雨花 （发起人）

国家注册会计师

九怡康集团市场总监

雨花养生品牌创始人

币发矿交所投资人

（4）蓝生（发起人）

广西讲师协会副会长

演说万能公式导师

广西大学生创业导师

著名演说家投资人

（5）贺一（发起人）

心灵幸福学创始人

国家级心理咨询师

人生设计教练导师

获杰出青年企业家

（6）卫东兴（发起人）

北京大学金融管理硕士

互联网技术牛人

长城公社联合发起人

币发矿交所联合发起人

（7）安焕庭（发起人）

蓝氏瑶集团执行总裁

电子商务行业协会副会长

中国西部研究与发展促进会

经济贸易常务副理事

（8）刘豪（发起人）

著名经济学博士

曾任农行行长

自律训练营导师

专业投资分析牛人

（9）朱桂珍（发起人）

广西邀约女王

百万团队销售精英

优秀讲师兼主持人

珠珠女侠自媒体发起人

（7）高光初（发起人）

广西一加八车行董事长

曾获十大杰出青年企业家

汽车金融信贷领域专家

八十年代的千万富翁

（8）蒋林旺（发起人）

广西科技种养大王

荣获广西省劳模称号

宏旺宜家品牌创始人

桂林银行股东投资人

（9）杨驿麟（发起人）

全脑潜能训练导师

时代脑咖联合发起人

区块链领域投资人

币发矿交所投资人

第十一章：基金会自治方案

ZYChain发展基金中的每一笔支出，都需要得到社区决策组织的投票表决。决策组织由“基金管理委员会”、“社区发展委员会”、“技术开发委员会”组成。

(1) 基金管理委员会主要负责生态应用布局、发展基金的管理、公示等任务；

(2) 技术开发委员会主要负责底层系统及应用 DAPP 的维护、开发和规划；

(3) 社区发展委员会主要负责统筹线上、线下社区的宣传推广、建议反馈等。

ZYChain社区建设的中流砥柱则是社区合伙人和社区志愿者，在所有社区成员中择优选择有能力、有实力、有精力、有责任心的“四有成员”担任，主要负责ZYC 的运营推广等工作的执行。

因此，ZYChain社区合伙人，也是社区发展委员会的候选人员，历届社区发展委员会成员都将在社区合伙人中投票选出，进一步参与发展决策和治理，共同分享ZYChain生态发展红利。

链上投票

正元公链将打造一套链上投票合约，旨在提供一种公平、公正、公开的社区发展自治系统，参与投票治理的角色主要有社区决策组织以及全体持票人（部署钱包挖矿，10000ZYC=1 票），提案投票需将一定量ZYC转入发展基金。

链上投票系统将于 2020 年第季一度上线第一个版本，主要功能包括社区决策组织成员的选举、发展基金专项经费审批、投票系统参数调整。

全体持票人主要负责：

(1) 定期在社区合伙人及现任社区发展委员会成员组成的候选人中，投票选举下一届社区发展委员会成员；

(2) 定期在开发者社区及现任技术开发委员会成员组成的候选人中，投票选举下一届技术开发委员会成员；

(3) 由超过 50%的持票人投票，并在指定有效投票的区块高度区间内，得票率超过 50%即可认为该社区决策组织成员为合法；

(4) 对已经通过社区决策组织投票，并进入公示期的重大项目，有投票否决权利；

(5) 对投票系统某些参数进行调整的投票，一旦通过，则投票的判断以新参数为准。

发展基金日常所需经费支出由社区决策组织投票决定。针对某一提案，投票须遵循以下规则：

(1) 提案需要按要求填入项目相关信息，包括项目地址、第一阶段提案 hash、上一阶段提案 hash（针对项目多阶段提案）、项目阶段性简述（md 格式）、承包人、项目经费、经费细则（md 格式）、收款地址等；

(2) 三分之二以上社区决策组织成员参与投票，并在指定有效投票的区块高度区间内，得到三分之二以上成员的赞成票，说明该提案投票初审通过。接下来根据项目需要支出的金额（系统参数）大小，决定是否需要公示期；

(3) 若小于等于系统金额，则不需要进入公示期，社区决策组织投票通过之后即可执行；

(4) 若大于系统金额，则社区决策组织投票通过之后，进入公示期，公示期期间（大约一周的区块高度），全体持票人可以对该项目投否决票，当积累超过三分之一的否决票，则该提案视为不通过；

(5) 根据每个不同阶段完成的情况，追缴上一阶段的金额，开始阶段预付一定金额，最后一个阶段支付尾款，尾款的控制由社区决策组织进行把控。

(6) 社区决策组织成员可以对提案进行评论，评论将以交易的形式提出并且与提案相关联，显示到提案区，参与评论的截止时间以实际提案结束投票高度为准

因此，ZYChain 社区合伙人，也是社区发展委员会的候选人员，历届社区发展委员会成员都将在社区合伙人中投票选出，进一步参与发展决策和治理，共同分享ZYChain生态发展红利。

第十二章：风险与免责声明

尊敬的ZYChain社区成员，在您持有 ZYC，以及使用 ZYC 的过程中存在以下诸多风险，请务必知悉并认同。

(1) 管辖和执法行动的风险在许多司法管辖地区，ZYChain 以及其他区块链科技组织所相关的法律政策尚不清楚或并未落实。无法预测如何、何时或是否有监管机构会针对ZYChain这样的科技和它的应用采取已有的或推出新的监管政策。这类监管行为可能会对 ZYChain系统产生各种负面影响。如果监管行动或法律或法规的变化使其在此类管辖范围内经营是非法行为，或难以在必要的监管许可下进行商业活动，基金会（或其附属机构）可能在该司法管辖区停止经营。基于与大量专业的法律顾问咨询讨论以及针对数字货币的发展和法律架构上的持续性分析，基金会对 ZYC 的销售表示谨慎态度。因此，对于大众销售，基金会需要经常性调整销售策略以尽可能避免法律风险。

(2) 市场竞争的风险

存在以下这种可能，即一种可替代的网络科技出现，其使用和ZYChain系统相同或类似的代码和协议来搭建类似的设施。正元链系统可能需要与这些替代性技术展开竞争，从而对ZYChain系统产生负面影响。

(3) 团队成员退出的风险

正元公链系统的发展依赖于现有的技术团队和专家顾问的继续合作，他们在各自的领域知识渊博、经验丰富。任何成员的退出可能会影响到正元公链系统的平台或其未来的发展。

(4) 发展失败的风险

因为各种各样的原因，正元公链系统的发展存在无法按照计划继续推进的风险，包括但不限于某种数字资产或虚拟货币或 ZYC 的价格下降，不可预见的技术困难，以及系统经营发展所需资金的短缺。

(5) 安全的风险

黑客或其他恶意的团体或组织可能会以各种各样的方式试图干扰ZYChain系统，包括但不限于恶意攻击、拒绝服务攻击、共识基础攻击，Sybil攻击，洗钱和欺诈。此外，还存在一种风险，第三方或基金会成员或其分支可能有意或无意引入某种漏洞，从而对 ZYChain系统的核心基础设施产生威胁，并对ZYChain系统产生负面影响。

(6) 其他风险

除了上述风险，还有其他的风险（如特别设置了 token 购买协议）与您的购买，持有和使用 ZYC 有关，包括那些基金会无法预测的各种情况。这种风险还可能会演化成各种无法预期的情况或上述风险的组合。您应该对基金会及其附属机构做出充分的尽职调查，在购买 ZYC 之前，需要理解正元链系统的总体框架和愿景。

第十三章：官方信息

基金会：ZhengYuanChain foundation limited

官方网站：www.zhengyuanchain.io

官方新浪微博：zhengyuanchain

微信公众号：zhengyuanchain

公司企业邮箱：zhengyuanchain@3113vip.com

开源地址：https://github.com/zychain

币用社群地址：http://www.biyong.net.cn/people/zhengyuanchain