ProducePay Chain

白皮书

摘 要

ProducePay Chain是基于区块链的点对点网络技术基础之上，是由美国知名农业支付应用ProducePay联合手游公司MachineZone合作推出。目前，ProducePay已经在美国掀起了农业金融变革风暴，并完成了数亿美元融资。MZ在整个全球游戏市场(包括主机、PC等所有平台)中拿走超过1%的市场份额，在全球手机游戏中占4%的份额，在所有游戏公司收入中将排入前15名。二者良好的发展前景，为智能农场开拓全球农业市场打下良好基础。ProducePay与MachineZone相辅相成，双方提供了在各自领域丰富的资源和技术，为PP在农业市场的多元化应用提供保障。项目自成立以来，坚持以理念创新、模式创新和技术创新为宗旨，扎根中国服务全球。ProducePay Chain将打造以水果农产品种植为基础的生态圈+生态链平台体系。

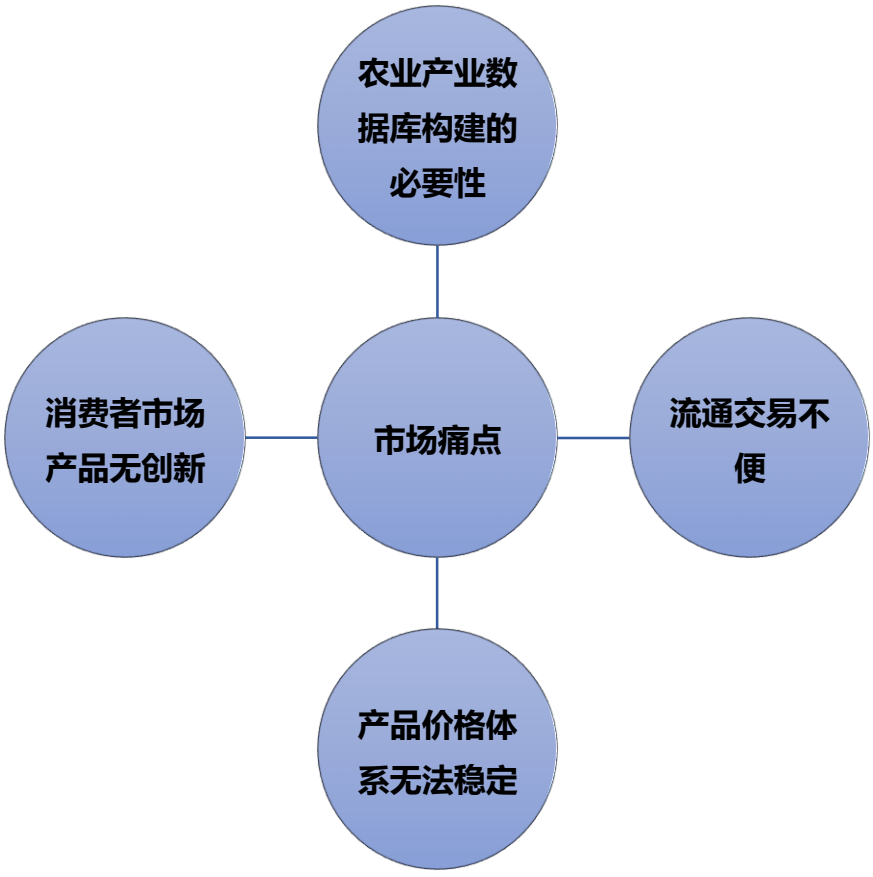
ProducePay Chain以实体经济为主导，以分享经济为补充，以现代企业管理体制为手段，发展持续服务型经济为目的的多元化项目机制。采取“线下企业实体农业概念+线上互联网O2O模式”并行，“实体经济+分享经济”并举，“实地运行管理+虚拟娱乐管理”相结合，达到企业健康持续稳步发展的目的。

区块链+大数据+生态农业的未来，给全球农业发展带来了良好的契机，使传统生态农业领域焕发生机。

行业分析

市场痛点分析

中国农业经济增长一直处于稳步提升阶段，农业市场潜力巨大，整个农业市场价值约为10万亿元人民币，相当于2014年全年GDP的六分之一，是一片正等待开发的蓝海市场。另外在2013年至2017年期间，农业收入增长一直维持在10%以上，这一良好的发展趋势正在刺激着农业经济的发展。然而，面对着庞大的市场，农业产业仍存在着一些痛点问题，主要表现在以下几个方面：



农业市场痛点

1）农业产业数据库构建的必要性

当前农业产业多粗放型生产，大多数农民仍使用最原始的农作方式，产量小，产品次，受自然环境影响大，导致农民身心俱疲。粗放型的生产模式直接阻碍了农业的发展，虽然B2B模式成为农业发展新方向，但是碍于资金问题、农民知识水平有限，B2B模式的引入仍然十分缓慢。而建立国际化的农业大数据集合库是解决此问题的首要方法。

2）农业交易全球化，但流通交易不便，造成资源浪费和重复执行等不必要程序

由于农业市场全球化进程的推进，频繁的以农产品为基础的交易推动了产业的发展，同时由于农业行业的特异性，尤其是季节、新鲜、保存问题，使得产品标的标记成为困难，仿佛置身商品交易的最初时期，以物换物的过程和价格标的极大波动，重复税收、重复检测的体制不但繁琐，而且造成农业资源的浪费。而统一一般等价交换制度标准成为解决此类问题的可靠方案。

3）产品价格体系无法稳定

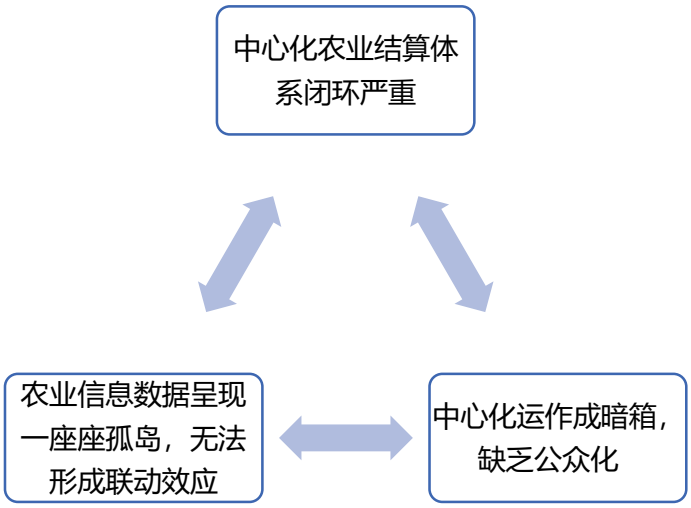
传统农业产业运作模式中，供需双方信息不畅，遇到需求量较大的时期，上游农作物种植商由于条件限制，供给难以跟上，导致上游一级市场农作物低价贱卖，下游最终市场消费者农作物价格飙升。另外，农产品的销售过程中，产品层层流转，从农产品种植到最终消费者购买，需要经过一级市场、二级市场、实体零售店等多个中间环节，不仅加大了转运过程中品质损坏的风险，也意味着中间的多级加价要由消费者买单。

4）消费者市场产品常年单一、无创新

对于消费者市场，存在着市场单一的弊病。随着社会经济的日益发展，居民的需求不仅仅满足于物质条件的满足、温饱的解决，而是更多的追求健康、生态、精神愉悦、便捷，虽然有部分企业已经在寻求生态农业，但是由于技术等问题，仍无法满足庞大的消费群体的多样化需求。

中心化结算体系存在明显弊端

就目前的发展来看，农业产业仍处在一个庞大的中心化平台之中，这种中心化的结算体系存在着如下明显的弊端：



中心化结算体系弊端

1）中心化农业结算体系闭环严重

农业产业经历了五千年的发展，由于新技术的应用以及消费者的刚性需求，仍处在高速的发展之中，但是不可否认，目前的农业结算体系都是中心化的交易平台，存在一些弊端。例如农产品受季节影响严重导致价格疯涨，农业产业上下游信息不对称等这些问题的存在都会影响产业利益相关者的交易体验，从而阻碍农业行业的蓬勃发展。

此外，传统的农业交流平台，所形成的社交圈是封闭且依赖于一个大中心化平台的，一旦交流平台中的用户因为某些原因离开平台，就会因此面临交际圈丧失、投资损失等风险。中心化平台运作，一切内容封闭化，对于各个利益相关者而言，虽然享有知情权，但是信息透明度极低，容易出现一言堂的局面，从而不利于行业的进一步发展。

2）中心化运作成暗箱，缺乏公众化

农业结算体系中心化运作，一切内容封闭化，对于行业利益相关者而言，虽然享有知情权，但是信息透明度极低，容易出现一言堂的局面。农业行业最大的特点就是中间商的层层流转哄抬了流向消费者的最终产品的价格。在农业结算交易平台，虽然有相关的产品信息，但是仅限于农产品的基本介绍以及标价，对于农产品的各个基本信息却无法得以求证。由于消费者无法实现产品溯源，这就变成了一个暗箱，外人无法探讨其中的操作，因此有失公平。

3）农业信息数据呈现一座座孤岛，无法形成联动效应

随着互联网的发展，信息不对称问题可以逐渐解决，但是仍然无法解决信用不对称问题。农业结算体系中心化，使得各个数据被分散在一座座孤岛里，这些数据无法联合在一起，不能刻画更加全面的交易行为画像。数据的分散也无法获得广而全的消费者行为轨迹，无法进行精准营销。

解决方案

从前述分析中可以看出，农业行业的前景及其广阔，但是问题也十分突出。

ProducePay Chain针对这样的背景，建立可以解决问题的全球化农业生态平台。ProducePay Chain项目致力于通过引入区块链技术，打造去中心化的生态平台，避免中心化带来的各种弊端，增强交易的安全性，保护用户的隐私，增强数据的可信度，杜绝私自篡改或者销毁相关数据的现象，为用户建立一个安全可信的平台机制。通过让生态内的用户持有基于区块链和智能合约的代币，享受平台内提供的各项产品与服务的物权，这些代币不仅可以用来购买平台内销售的农产品、水果，还可以享受生态观光旅游、养老等服务，也可以像真实货币一样使用，甚至兑换成法定的货币。通过ProducePay Chain的不断努力，可以为最终消费者带来前所未有的消费体验。

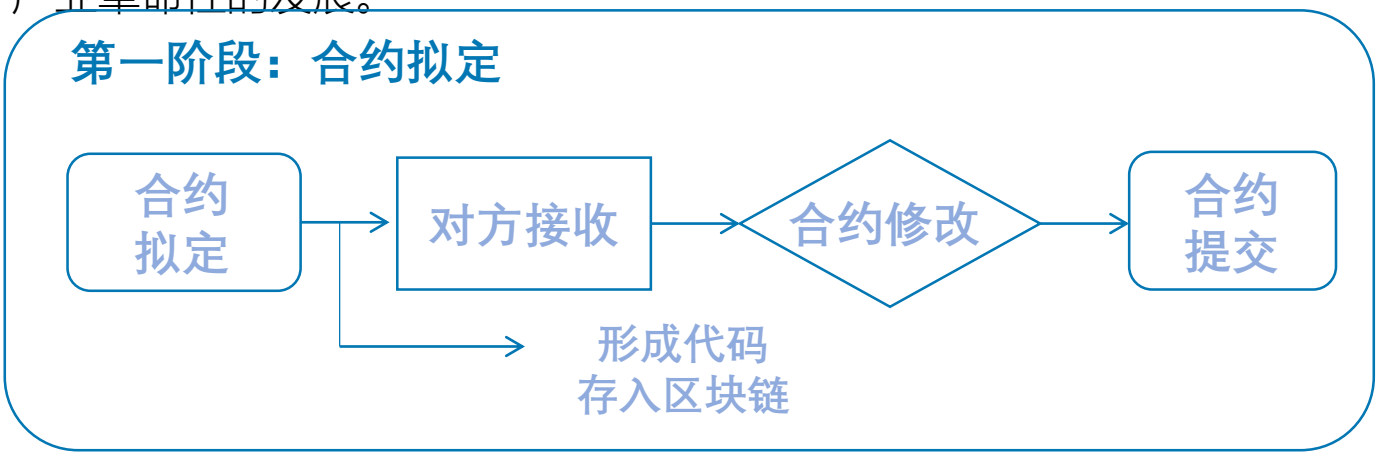
当更多消费者接入ProducePay Chain生态平台后，代币会因为稀缺性的增加而增加自身的价值。如此，便产生了一个公开、公平、民主、最具用户参与度、最具用户粘性的农业产业生态圈。

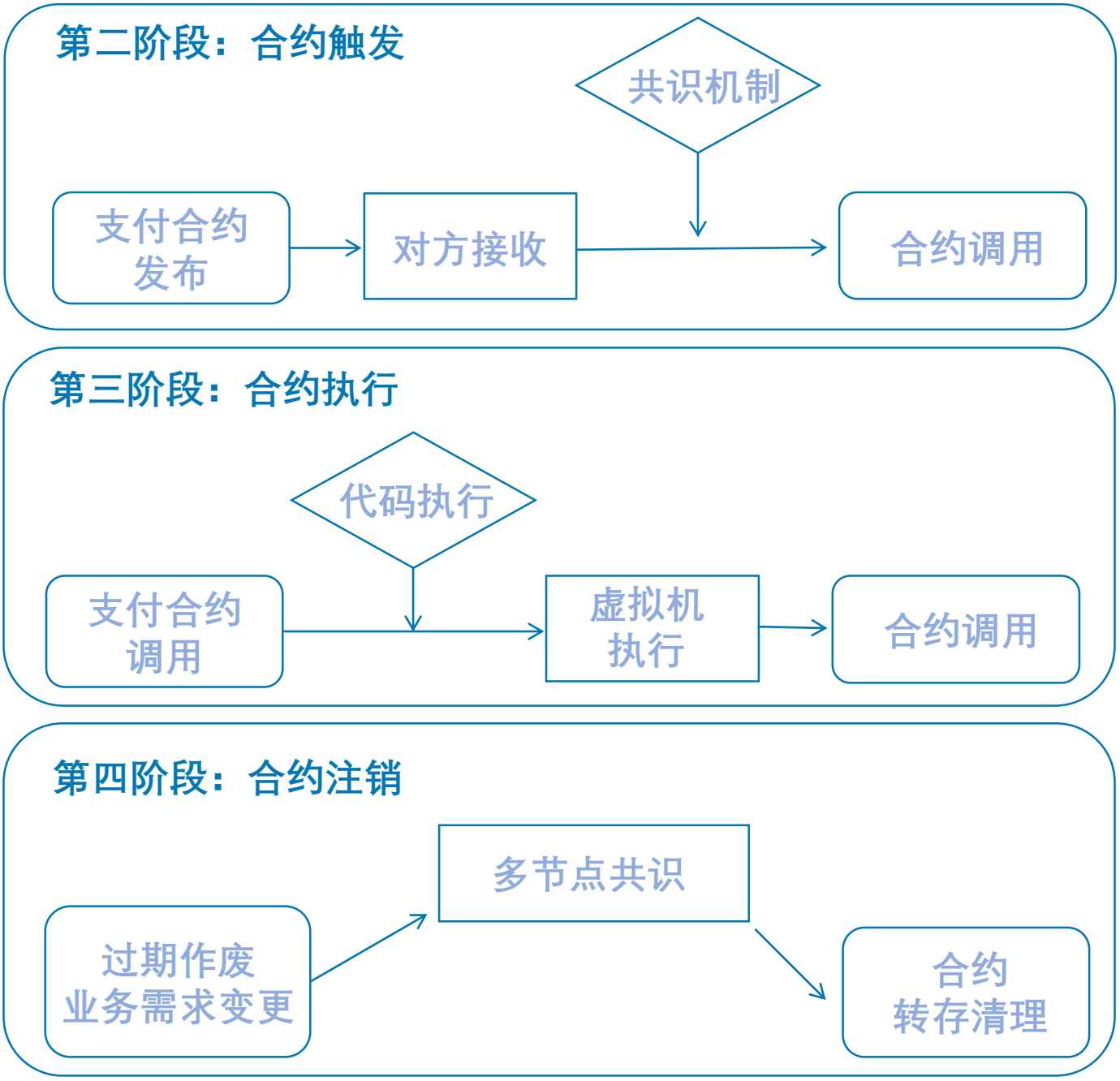
ProducePay Chain介绍

合约式结算的定义

合约式结算也称作合约式支付，合约式结算是一套以智能合约技术为基础，用数字形式为定义的结算承诺，所有参与结算的相关责任方要在上面达成协议，并在共识达成的条件下自动执行协议。智能合约必须要有数字化的货币参与，无论是数字货币还是与法定货币对应的数字化密钥，且资产必须联网。

ProducePay Chain不仅与比特币等基于区块链的结算系统相同，而且是一个基于区块链的电商结算合同系统。用户与用户间通过私钥对合同进行签名，从而完成代币的交易。实际上，ProducePay Chain可以被用于签署任意ProducePay Chain代币合同。如果合同的标的物是登记在ProducePay Chain区块链上的数字资产，那么ProducePay Chain可以自动在链上进行程序化交割执行；如果合同标的物为链外的资产，那么合同参与方自行执行即可。即便是后者情况下，ProducePay Chain也消除了签署、保管大量纸质合同的繁琐性，并用数字签名保证了合同的不可抵赖性。通过合约式结算模式，建立了完善的可信机制，推动了农业产业革命性的发展。





合约式结算的四个阶段

ProducePay Chain与区块链的撮合

ProducePay Chain与区块链技术存在着充分的"合作空间"。当ProducePay Chain遇上区块链，会产生一个使用全新的加密认证技术和去中心化共识机制共同维护的完整的、分布式的、不可篡改的农业社区，通过ProducePay Chain发行的数字货币将所有用户长效地联系在一起。

1）从中心化到去中心化，点与点完成结算

区块链的真正价值在于促进各行各业的结算中心化机构之间达成共识、构建联盟，形成多个中心组成的结算生态圈，这样的生态系统突出中心的职能，大大简化了中心化机构运营成本。

2）从不信任到信任，结算信任危机成为过去式

区块链的去信任化特性，基于互不信任的原则，整个系统的运作是公开透明的，通过"签名"机制和利用"少数服从多数"的朴素方式，却能够从机制上保障信用。

3）从不安全到安全，打消用户信息担忧

首先，用户数据以块链结构存储，具有自校验性，篡改之后可以迅速发现。其次数据在多个节点都有相同的备份，即使某个节点上的数据被修改，也可以从其他节点上自动恢复过来，从机制上杜绝了黑客的数据篡改袭击。借助区块链技术，用户能够随时随地查看自己真实的资金池。

综上，将区块链用于农业的管理，是区块链技术日渐成熟的创新性运用。ProducePay Chain就是在这个信念下产生的新型区块链分布式农业生态系统。ProducePay Chain面向全球，力图为农业产业带来质的变化，使居民消费者都能够享受到ProducePay Chain带来的便捷、舒适、安全的服务，从而为人类的发展保驾护航。

ProducePay Chain的创新

1）进一步去中心化

在基于PoW共识机制的区块链中，需要第三方提供相应的算力将所有交易打包，并且第三方有收取手续费和选择打包的权力，由此出现了大量的拥有集中算力的矿场和矿池。在区块链行业中，很多类型的攻击都是针对矿场的，其主要原因在于区块链的算力已经在某种程度上集中。然而，DAG 的网络系统中不存在集中式的挖矿，用户之间相互验证也使其实现了进一步的去中心化系统。

ProducePay Chain验证过程中使用的PoC机制也能有效让整个网络趋于平衡，单纯的更多算力也不足以使某个用户节点在整个网络中掌握绝对权力，只有对网络有了贡献才会使节点用户拥有更多回报，而他的贡献在网络中体现出来的是对其他用户的服务与便利。

在ProducePay Chain平台中，区块链技术使得平台呈现出一个可持续的、公开透明的、无中心化的、安全可靠的、开放共识的协同生态平台。

2）智能合约的交互

“跨链”一直是区块链发展所关心的重要问题，“跨链”的意义在于实现互联互通，让各种链状结构有可能交织，从而更好地实现自身网络价值。而ProducePay Chain的DAG架构其本身就是一个网状结构，所谓“跨链”的实现只是简单的智能合约之间的交互，而且，我们所提出的时间戳和直系父辈就是新型交互式智能合约的重要技术和逻辑保障。

ProducePay Chain平台将面向用户提供足够丰富的智能合约模版，以便于ProducePay Chain代币的分配和激励的自动执行，同时也开放端口，让生态内的所有人均可以参与智能合约模版的设计和发行，并自行定义价格或激励条件，并和创始团队一样，通过用户的使用率来获得对应的代币激励，也就是无人使用的智能合约模版将无法获得收益，甚至是创始团队本身。

3）提高交易速度

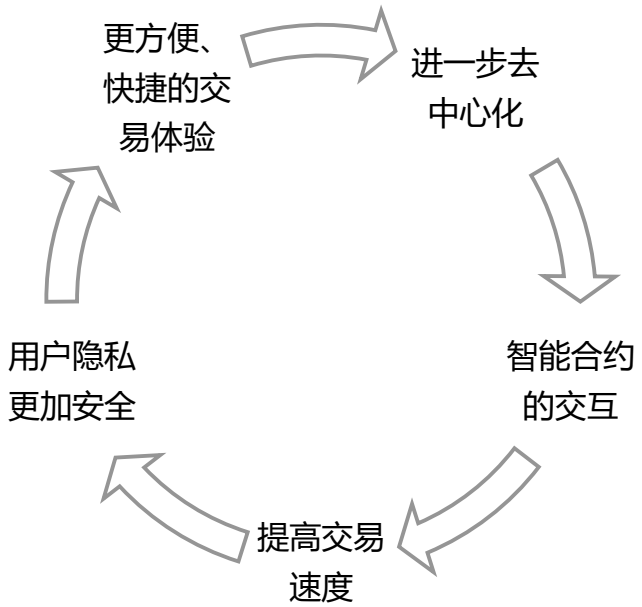
在ProducePay Chain结算平台上可直接使用ProducePay Chain发行的数字资产进行交易，实现跨所交易、跨所结算、不同币种和资产之间的存取。所有的结算都在ProducePay Chain系统通道中进行，同时还能全天候结算、实时到账、提现简便且没有隐性成本。

4）用户隐私更加安全

ProducePay Chain具有独有的隐私保护加密合约，通过安全多方计算可以实现隐私的原始数据完全隔离访问，实现了快速安全的数据分享服务。数据通过区块链的加密方式、身份验证、授权机制等技术存储于去中心化资源上，除了用户本人任何机构和个人都无法接触用户的原始数据。

5）更安全、方便、快捷的交易体验

ProducePay Chain中的分布式交易所提供去中心的撮合交易，避免了数据的丢失、篡改带来的损失，能够带来更加安全、方便的交易体验。ProducePay Chain代币作为整个生态的中心货币，连结了与其他币（其他数字货币、法币及数字资产）的交易、汇兑、流通信道，是贯穿整个生态的润滑剂，自身价值不可估量。



ProducePay Chain生态结构

商业逻辑

ProducePay Chain构建开放、平等、安全的农业链上平台，所有参与者都能够创造和分享ProducePay Chain上的价值。每个人在使用ProducePay Chain平台的时候给ProducePay Chain贡献了数据和资源，并能够获得应有的收益。

数据，是ProducePay Chain运行的基石，用户通过传感器、智能硬件、实体产业向ProducePay Chain云端上传实时数据，数据在ProducePay Chain上通过差分隐私技术进行安全加密，实现存储、解析和流通。

代币（Token），是ProducePay Chain网络中的权益凭证。用户上传及分享数据将获得ProducePay Chain代币；购买农产品、水果生态观光旅游、获得养老服务等都需要消耗ProducePay Chain代币。

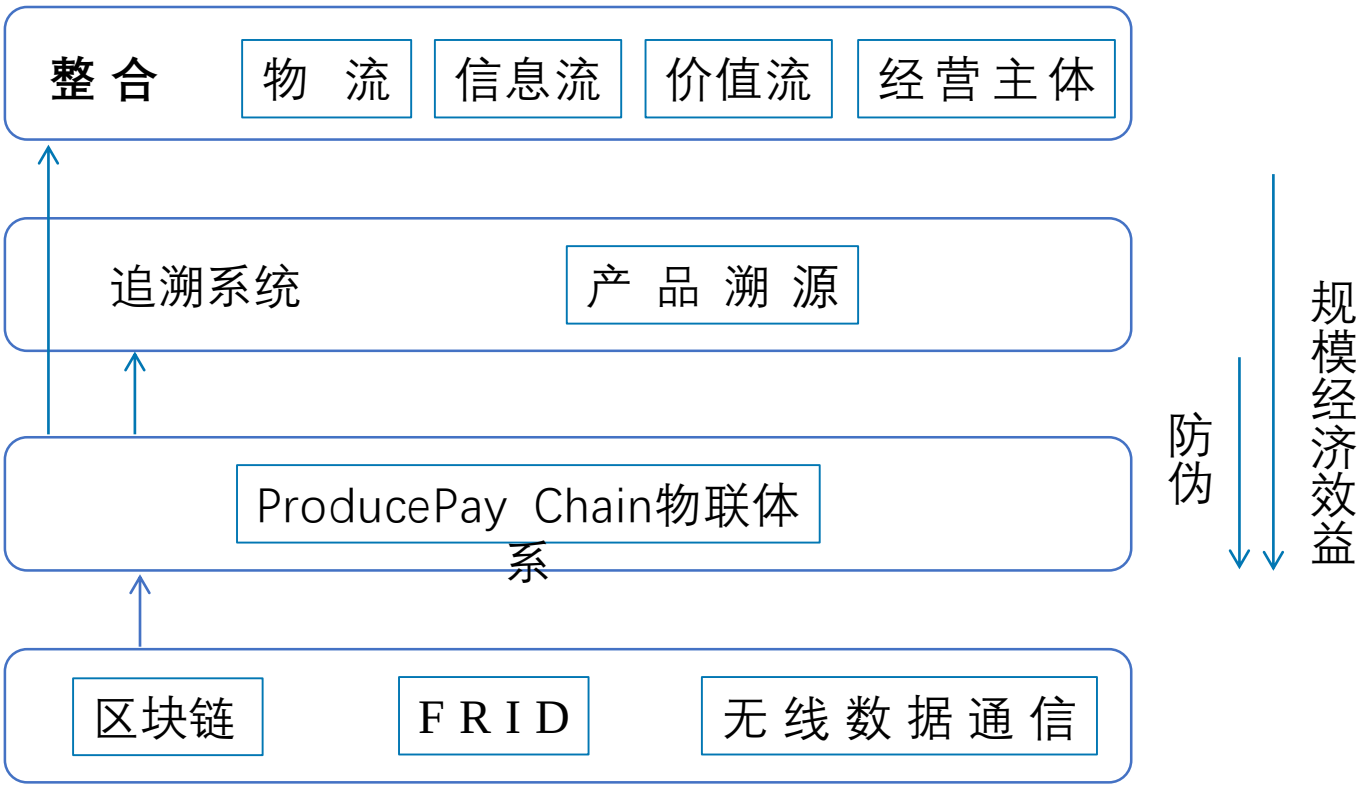
ProducePay Chain的核心为"线下企业实体农业概念+线上互联网O2O模式"并行，"实体经济+分享经济"并举，"实地运行管理+虚拟娱乐管理"结合，以达到项目健康持续稳步发展。

物联体系

农业物联是指基于区块链技术、RFID、无线数据通信等技术，构造一个覆盖实体产业的物联网。在这个网络中，实体产业与用户能够直接进行"交流"，而无需中间平台的干预。其实质是利用区块链技术对每一产品或服务进行溯源追踪，交易数据分布式储存不可篡改且永久保存、智能合约的自动性等特征，实现利益相关者的自动交易以及信息的互联与共享。

农业物联实质上就是对农业产业链进行整合，有助于提高产业集中度，扩大规模经济效应。ProducePay Chain打造的农业物联是指线下实体经济与分享经济、线上互联网O2O模式，农业产品销售为基础，覆盖休闲观光旅游娱乐、养老服务等各项目。其促进了农业产业链的各环节有机地连结在一起，然后根据社会资源状况和市场需求状况的变化，在产业链环之间合理配置生产要素，协调各产业链环之间的比例关系，从而产生协同效应和能量聚合，实现产业链效益的最大化。

农业产业链的整合强调物流、信息流、价值流以及经营主体的多重整合，同时也注重宏观视域内、区域内和跨区域的产业链整合，由此壮大了农业产业链的规模，并促进规模经济效益的发挥。在产业链整合过程中，生产资源由低效益行业（种植等）向高效益行业（农业休闲观光等）配置，提高了产业集中度，增强了企业的市场竞争力。



信息数字存储

1）数据来源

ProducePay Chain的数据来源主要来自用户的上传与每次交易的存储。一方面，ProducePay Chain借助于互联网形态与大数据等新兴技术，使用多变量和机器学习模型，该模型通过对用户不同的网络行为数据进行相关性分析，不断优化评估结果，使评估结果动态化。通过实时收集大量交易行为数据，借助区块链、云计算等手段提高平台服务的便捷性与精确性。

另一方面，用户可以进行个人数据的上传，形成个人资产数据库，并将资金流向及资产增值过程映射到区块链中的公有链上。随后，这些公有信息和私密信息成为用户财产，经用户本人同意后得以调用查询与检索。

2）数据安全

安全性是保障数据在网络中流畅运转的关键，基于区块链的的分布式存储让ProducePay Chain具备高度的安全性，ProducePay Chain对用户上传的数据、利用大数据模型收集的数据通过同态加密、差分隐私（differential privacy，DP）进行数据安全保护，并使用离散存储方式进行数据存储。这些数据由整个系统中具有维护功能的节点来建立共识，共同维护、不可篡改。

ProducePay Chain将农业数据与区块链协议绑定，进行信任认证，安全和管理的授权，让每个人可以管理自己的数据，把数据的控制权归还给用户自己，让每个数据的贡献者获利，消费者和企业能够在安全、平等、信任的前提下，共同分享数据、存储、算力等资源，构建开放的数据存储共享平台。ProducePay Chain上的数据只有拥有者或者授权者才能访问，数据的访问权限由用户设定的智能合约来确定。

3）数据提取

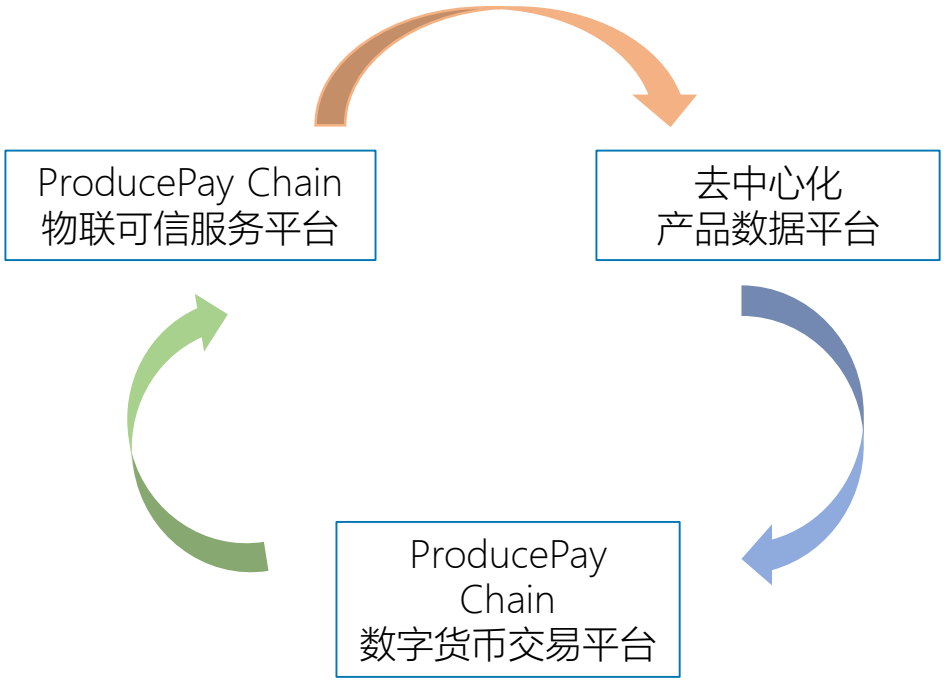
数据使用需要满足ProducePay Chain认证协议，并且经过所有者授权。ProducePay Chain上的所有参与者都可以成为数据提取方，包括普通消费者、ProducePay公司以及各联盟合作商等。

4）信息银行

消费者的数据是极其宝贵的资源，能够用于企业制定迎合消费者需求的产品与服务，有针对性的制定营销策略等多种用途，也是根据消费者生理状况种植恰当农产品的关键数据。用户产生的数据可在信息银行中得到安全的存放，也可进行交易，获得ProducePay Chain代币或者兑换相应产品与服务。

5）超级应用

超级应用是ProducePay Chain的核心模块，主要包括以下几种场景：



场景一：去中心化产品数据平台

基于代币经济理论，结合区块链的去中心化、不可篡改的特性，ProducePay Chain设计了应用场景一去中心化产品数据平台，通过产品数据的上传，有助于ProducePay Chain构建针对农业的大数据综合库，通过建立数据库，可以有效解决行业数据孤岛现象。而产品的上链需要经过ProducePay Chain理事团队的审核，严格保证了上链产品与服务的质量。

场景二：ProducePay Chain数字货币交易平台

ProducePay Chain搭建自有的数字货币交易平台，用户可以在该平台进行代币的投资与交易；ProducePay Chain还将所发行的代币在ICO交易所上币，消费者也可以通过交易所购买；ProducePay Chain创办的应用场景一产品数据平台中，也可以进行代币与农产品、旅游养老服务的交易。通过三种方式，用户可以随时互相交易或者消费服务，同时在交易所进行购买虚拟币、持有虚拟币。也许像比特币一样，ProducePay Chain代币也会实现九年间增值2000万倍。由于具有增值的可能性，因此持有ProducePay Chain代币也是一种投资行为，为用户带来稳定收入来源。

场景三：ProducePay Chain物联可信服务平台

ProducePay Chain对农业信息系统进行了整合共享，加快消除无效的产品或服务信息，促进供应链信息的整合共享，提升统一产业供销网络的支撑能力，推进接入统一的数据共享交换平台，建设起一个行业公共数据开放网站，落地完善全国农业产业数据信息共享工作，并开展农业产业信息资源编制，构建出一个产业信息的共享标准体系，开展"物联网+农业+娱乐+消费服务"，促进跨地区、跨时区、跨层级的农产品信息互认共享，实现农业大数据的共享和开放，通过共享数据来避免供应链方面的失信行为。ProducePay Chain将通过推动农业产业链的经营水平的不断提高，逐步构建起"物联网"式的全产业链条。

ProducePay Chain应用与价值

核心创新

1）产业架构

农产品及水果种植、名贵中药材种植产业、畜牧水产养殖产业、生态农业观光旅游产业、中高档养老产业。

2）经营核心

以农产品水果种植为重点，以不断完善农业观光旅游为亮点，以打造养老产业为后续保障，达到乡村振兴的目的。

3）运行机制创新

以实体经济为主导，以分享经济为补充，以现代企业管理体制为手段，发展持续服务型经济为目的的多元化机制。采取"线下企业实体农业概念+线上互联网O2O模式"并行，"实体经济+分享经济"并举，"实地运行管理+虚拟娱乐管理"相结合，达到企业健康持续稳步发展。

4）战略布局创新

ProducePay Chain已组建了重庆市第一家土地流转的专业合作社，并申报为重庆相关职能部门的项目试点，通过土地流转取得15000亩土地经营使用权，采取"公司+基地+农户"的组织形式，打造水果基地，实行分散联合经营与集中"统一技术标准、统一产品质量、统一销售渠道、统一分配利益"集约化产业链的经营模式，立足基地示范，幅射基地以外，以规划布局建设旅游产业，以品种布局突出旅游观光亮点，以经济支撑打造养老产业。

ProducePay Chain平台技术特征

分布式控制结构

ProducePay Chain的区块链根据系统确定的开源的、去中心化的协议，构建了一个分布式的结构体系，让价值交换的信息通过分布式传播发送给全网，通过分布式记账确定信息数据内容，盖上时间戳后生成区块数据，再通过分布式传播发送给各个节点，实现分布式存储。具体来说，分布式结构体现在3个方面：

1）分布式记账

ProducePay Chain平台上用户行为轨迹以及交易数据由多个节点进行记账，并且会验证其合法性，合法性的交易会被记录到所有用户的账本中，最大限度地避免了道德风险，并且不容易出现错误。

2）分布式传播

区块链中每一笔新交易的传播都采用分布式的结构，根据P2P网络层协议，消息由耽搁节点被直接发送给全网其他所有的节点。

3）分布式存储

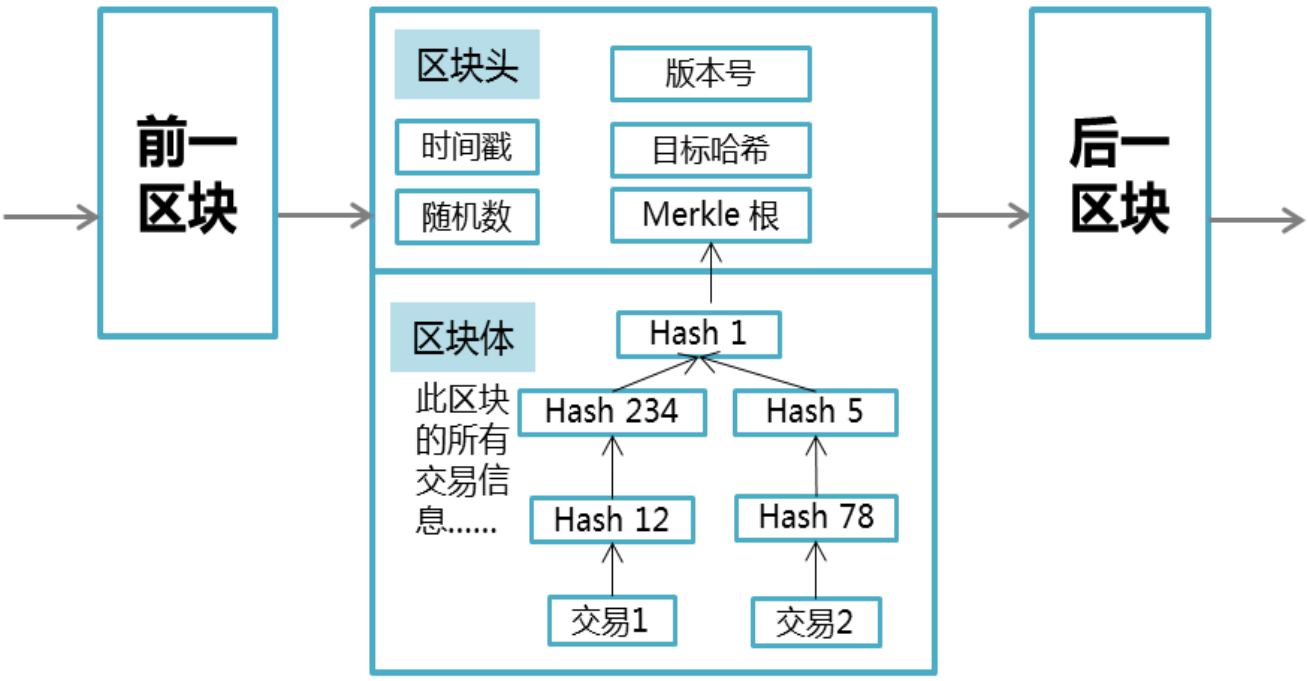
让数据库中的所有数据均存储于系统所有的电脑节点中，并实时更新。完全去中心化的结构设置使数据能实时记录，并在每一个参与数据存储的网络节点中更新，这就极大的提高了数据库的安全性。

综上，通过分布式记账、分布式传播、分布式存储这三大“分布”，系统内的数据存储、交易验证、信息传输过程全部都是去中心化。使用分布式交易所的方式进行撮合支付，买方挂单和卖方挂单缓存在区块链中。

当共识节点记账时，自动触发买卖挂单，将账单分布式传播到网络中，在51%以上的节点验证通过后，完成交易。分布式撮合交易支付的好处是每一笔交易都有据可查，每一笔交易都得到了最广泛节点的确认，在提高交易记录安全性的同时增加了黑客操纵交易盘的难度。

数据区块结构

区块链就是区块以链的方式组合在一起，区块链是系统内所有节点共享的交易数据库，这些节点基于价值交换协议参与到区块链的网络中来。每一个区块的块头都包含了前一个区块的交易信息压缩值，这就使得从创世块（第一个区块）到当前区块连接在一起形成了一条长链。由于如果不知道前一区块的HASH函数值，就没有办法生成当前区块，因此每个区块必定按时间顺序跟随在前一个区块之后。这种所有区块包含前一个区块引用的结构让现存的区块集合形成了一条数据长链。“区块+链”的数据存储结构如下图所示。



数 据 区 块 结 构

共识机制

区块链的价值锚点在于链条自身的消耗与产出。当区块链选择PoW（Power-of-Work， 工作量证明）作为共识机制时，每一次区块的生成消耗的算力都将成为其价值的基石。另外，在ProducePay Chain上，每个节点都具备解决现实环境问题的能力，并能对外提供农业行业的产品与服务。如果ProducePay Chain的每个节点能够参与共享工作的结算，整个区块链条就具备了现实的产出价值。因此，为保证区块链自身价值最大化，ProducePay Chain将默认选择基于PoW的共识机制。PoW的核心要义为：算力越大，挖到块的概率越大，维护区块链安全的权重越大。

但由于PoW具备交易速度较慢等显性缺陷，因此在平台中后续的数据链，其共识机制将被设计成模块化的，可以通过控制链参数进行配置，能够动态适用公链和私链的不同应用场景。平台将针对数据链本身的应用场景和交易情况，选择合适的共识机制，确保各个分布式节点通过算法取得数据的一致性。

安全加密算法

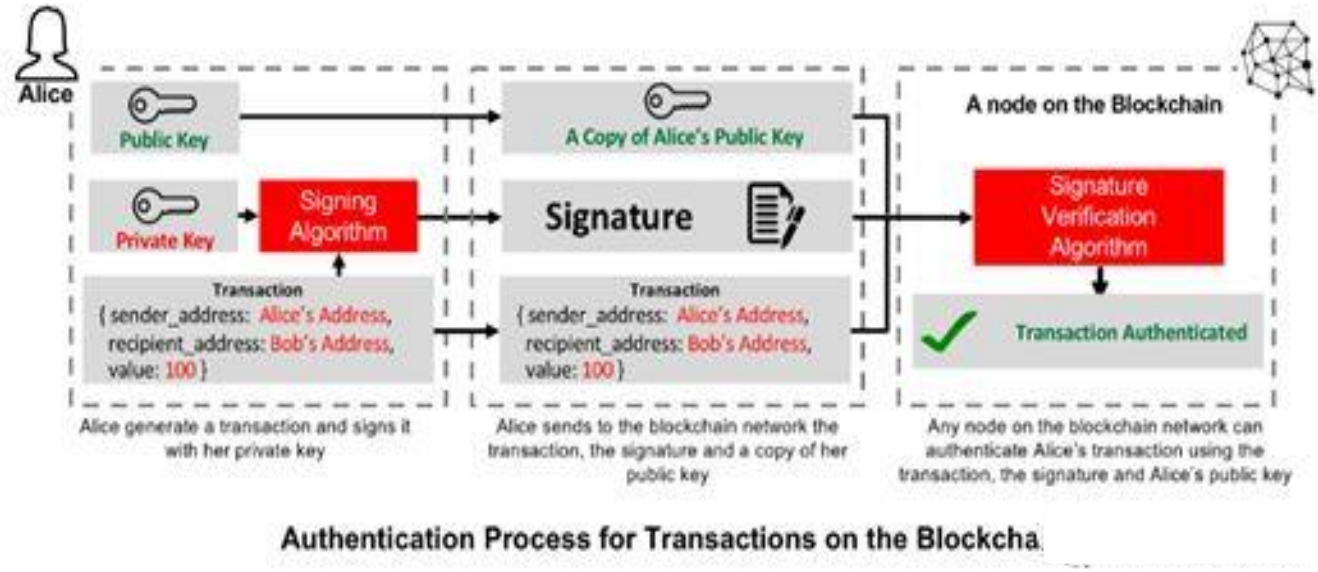
ProducePay Chain选择符合国内和国际标准的加密机制，对农业数据进行加密，用户间的交易数据和交易信息仅交易双方和有相应权限的用户可以查看。

1）对称加密

对称加密是最快速、最简单的一种加密方式，加密（encryption）与解密（decryption）用的是同样的密钥（secret key）。对称加密通常使用的是相对较小的密钥，一般小于 256 bit。密钥的大小既要照顾到安全性，也要照顾到效率，是一个trade-off。

2）非对称加密

非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，公钥（public key）和私钥（private key）。私钥只能由一方安全保管， 不能外泄，而公钥则可以发给任何请求它的人。非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。



非对称加密技术

3）私钥（private key）

非公开，是一个256位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

4）公钥（public key）

可公开，每一个私钥都有一个与之相匹配的公钥。ECC公钥可以由私钥通过单向的、确定性的算法生成，目前常用的方案包括：secp256r1（国际通用标准）、secp256k1（比特币标准）和SM2（中国国标）。ProducePay Chain控制链与初始数据链选择 secp256r1作为密钥方案。

5）哈希算法

通常哈希算法是指安全散列算法SHA，该算法是美国国家安全局设计，美国国家标准与技术研究院（NIST）发布的一系列密码散列函数，包括SHA-1、SHA-224、SHA-256、SHA-384和SHA-512等变体。目前比特币采用SHA-256 算法。除PoW外，其余哈希算法均指SHA-256。

加密机制

1） ECDSA加密算法

基出于安全考虑，区块链系统中，每一个在网络中广播的交易和区块都需要经过签名和签名验证的处理过程。ECDSA,即桶圆曲线数字签名算法，是目前行业中应用最为成熟和广泛的数字签名算法，但纯软件实现方法在通用计算机平台上，只能做到每秒上千次，远达不到性能需求。BOE加速引擎内嵌ECDSA模块，将大幅提离签名验证速度。

2）随机数生成器

各节点间进行数据传辅时，需要通过密钥交换理立加密通道，处理过程中采用了硬件随机数发生器，使得密钥交换的随机致种子完全不可预测，从而保护加密通道的可靠性。

3）数据分片

在高TPS情况下，节点间网络传输数据置巨大，远超当前网络基础设施的承受力，造成数据同步异常缓慢。BOE加速引擎采用了区块数据分片广播处理技术，每个区块分片中都含有完区块头部，便于将新产生的区块尽快广播到所有节点，实现区块链的快速收敛。

4）网络性能

ProducePay网络中，能够成为高贡献值节点的条件之一是能为系统提供网络带宽。BOE技术基于硬件实现了节点连接的流置统计，共识算法能够通过BOE技术计算出某个节点提供的网络带宽数据。

5）并发

ProducePay网络中，BOE加速引擎可实现大并发连接，并同时维持支持超过10,000条TCP会话，可并行处理10,000条会话，这将大大降低分布式网络层级数。专用并行处理硬件将接管由传统软件串行处理能力，例如交易数据广播，未验证Block全网关闭、交易确认广播等。其对会话的响应速度以及会话维护数量军事通过计算平台节点处理器性能的百倍以上。

P2P协议

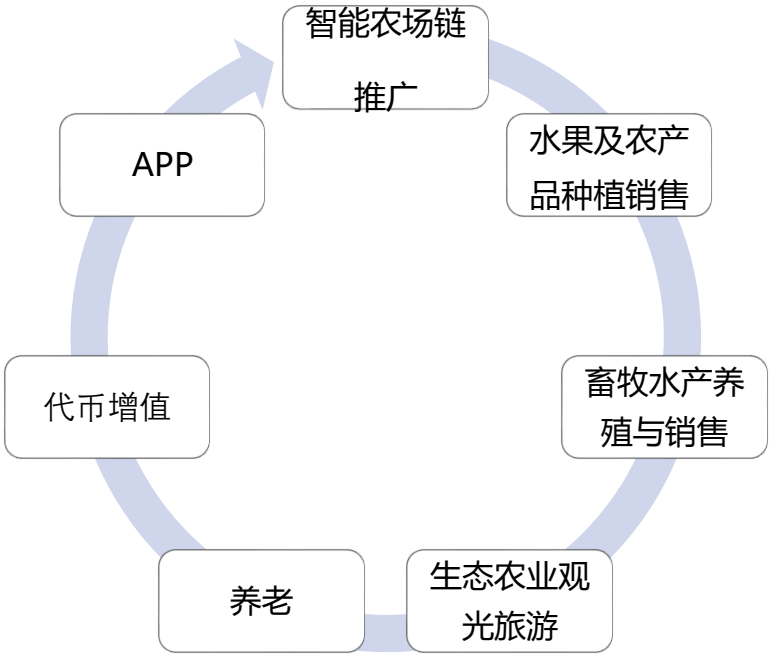
ProducePay Chain上，每个节点（客户端）均采用P2P协议进行消息广播交互。对于ProducePay Chain的数据区块，采用的P2P协议是标准的加密货币协议，该协议的核心特点是引入“幽灵“协议。而ProducePay Chain的控制区块则采用标准的P2P协议，不支持“幽灵“协议。

ProducePay Chain的客户端通常工作于守护状态。该状态下，客户端执行的工作包括：　（1）调用网络守护进程维护连接及定期发送消息；（2）获取当前区块信息以及关联区块信息；（3）获取工业制造参数，并对工业制造参数按照标准模型分析，确定是否提交更新的参数。

ProducePay Token体系

结算币

在我们设计的生态圈平台中，拥有ProducePay Chain代币的用户，就拥有了代币的所有权与处置权，可在法律规定的范围内任意处置代币。当用户在平台中通过处置代币而获得一些产品或服务，就获得了所接受服务或所购买产品的所有权与使用权。具体产品服务如下图所示：



ProducePay Chain代币结算体系

红利币

代币（Token）经济设计的核心理念，是把原来体系中耗散的交易成本集约起来，用技术手段把收益分散到体系内每一个参与者，使系统整体摩擦力不断下降，从而代币内在价值不断上升。

ProducePay Chain发展规划

初期规划：进入中国市场，平台搭建

ProducePay Chain目标于全球国际市场，但中国作为最大的发展中国家、人口最多的国家，对农产品的需求极大。因此，项目初期在中国运行。

日期：2019年——2022年（3年打基础）

1) ProducePay Chain实体对接初期发展规划

1.建立绿色经济作物基地

规划旱地和坡地约2600亩为绿色种植基地。以绿色水果种植、绿色干果繁育、优质药材种植为主，配套种植高端苗木，充分利用畜禽项目中养殖场产生的沼液、有机肥。

2.建立高质量的中药材种植基地

规划未来种植发展规模采取"公司+农户"模式，种植面积达5000亩以上，生产总值达10亿元以上，2—3年时间就能达5000亩以上种植规模，种植措施采取"以短养长，以长求效"的经营方针，以短期药材和育苗及畜牧养殖的对外销售回笼资金来实现扩大规模。

3.建立畜禽生态养殖基地

搞好现有养殖项目的基础上，扩大种猪和育肥猪生产规模，采取公司+基地+农户的生产经营模式，选择最佳位置和有条件的养殖（养殖小区）、农户参于畜禽养殖其中生猪养殖，至2022年力争实现年生产无公害商品猪10万头，新建散养牛场1个可容纳2千余头的放养，及懒兔养殖基地2个，年出栏1万余只等其他畜禽逐步扩增，建设成无公害成规模性的商品畜禽养殖基地。

4.建立乡村体验式旅游基地

利用生态养殖、绿色种植所形成的"绿色、环保、原生态"的乡村自然景观，发展"农村农耕生活体验营"的大农村体验旅游项目

5.可产生较好的社会效益

预计影响和带动劳动力上万人，村民超万家，增加每户村民年收入3-5万元以上。同时大大拉动了其他相关产业的发展。

2）ProducePay Chain平台早期实现路线

我们采用大数据、区块链的模式，构建世界级分布式数字货币生态系统，建立便捷、舒适、安全的农业消费平台。ProducePay Chain计划依托数据挖掘分析和机器学习技术，撮合消费者和企业快速完成交易，帮助消费者享受到更便捷、更安全的以农牧业产品为基础的，覆盖生态观光旅游、养老的各项精致的服务。

我们前期工作的重点是完成ProducePay Chain平台的上线与Token代币的销售，因此必须要进行ProducePay Chain平台的推广适用，比如利用百度、微信推广等方式扩大ProducePay Chain的影响力；完善数字交易系统并持续推广；探讨在平台和子系统中启动人工智能计划，并择机、择类开发完成初步版本的人工智能。

中期规划：辐射全国

日期：2022年——2026年（5年见成效）

基本思路：符合中国的政策、民情及社会现况，充分利用资源优势，促进农业生态循环经济，达到可持续经济发展。

发展规划：以水果、农产品经济为支撑，做好生态农业产业，畜牧养殖业，发展生态农业观光旅游业，打造养老产业。

并对接国外虚拟货币，采用区块链技术打造成P2P电子现金系统，用来实现一个可去中心化，并确保交易安全性可追踪性的数位货币体系，最终将公司推向国际市场并打造国际上市企业，达到实体与虚拟货币点对点币对币交易和资本市场互为依托相互促进的多元化企业。

未来规划：全球化发展

日期：2026年——2033年（8年达目标）

ProducePay Chain的目标在于以中国市场为起点，开拓全球市场，打造全球优质农业产业资源共享，以大数据为之根本，持续性整合全球农业产业链。

未来，我们不仅仅发展本企业的实体产业，我们还将通过产业联盟的方式，在全球广招合作伙伴，实现ProducePay Chain全球化生态体系的建立。我们会通过努力，对接全球1000多家企业纳入产业联盟之中，为全球消费者带来最为便捷安全可信的产品与服务，增加全球用户对生态体系的粘性。另外，ProducePay Chain将接入多类应用，组织多语言平台，进行全球化产业生态协同运作，打造一个万亿级全球化生态圈。

ProducePay Chain商业盈利模型

ProducePay Chain是一个基于区块链、能够贯穿整个农业行业的共赢生态，新商业模式下必将激发出更大的经济潜能，推动整个行业的技术进步、合作联合、共赢共利。

在新的商业模式下，ProducePay Chain上每个环节的节点，都将最大化经济权益，挤压出传统农业产业冗余的消耗，建立起效率更高、更公平、更稳健的盈利模型。

用户

用户是ProducePay Chain的核心，是ProducePay Chain的生命。ProducePay Chain坚持以"为人民服务，满足人民生活、精神所需"为目标愿景。有用户的存在，才可以真正驱动ProducePay Chain平台，从而让整个平台活跃起来。

企业

NO.1 ProducePay农业公司位于加利福尼亚州洛杉矶市。是为农户和农产品经销商提供在线交易和金融服务的知名农业软件公司。其运作理念彻底解决了农户回款难的问题。通常，农户在把农产品卖给经销商后要等很长一段时间才能收到回款，增加了农户的金融成本和金融风险。Produce Pay则为其会员农户提供提二天回款的服务，除此之外，Produce Pay还为农户提供销售预测、寻找销路和匹配经销商等服务；对于经销商用户，Produce Pay不仅提前帮经销商预付了货款，还帮助经销商匹配更多的货源。目前，ProducePay已完成数亿美元融资，其良好的发展前景，为智能农场开拓全球农业市场打下良好基础。

NO.2 MachineZone 手游公司成立于2008年(前身是Addmired)。MZ在整个全球游戏市场(包括主机、PC等所有平台)中拿走超过1%的市场份额，在全球手机游戏中占4%的份额，在所有游戏公司收入中将排入前15名，足以挑战传统的EA、动视暴雪等老江湖的地位。MachineZone仅用两款产品就成为美国第一大手游公司，专注于Real-Time技术，并且推出了自己的实时技术平台，将自己在大型在线游戏中积累的技术能力进一步应用到其他领域。其核心理念：凭借验证过的游戏原型，通过不断换皮，以及自己在流量运营上积累的能力快速变现。MachineZone的目标不是要创造出非凡的游戏产品，而是在用金融行业的手段经营游戏产品。MachineZone的运作理念充分注入智能农场，平台提供多项游戏功能可供娱乐+理财。

原料提供

原料的提供需要不断的优化，ProducePay Chain通过提供代币奖励吸引更多的原料商入驻平台，从而获得规模经济优势，提升议价能力，降低成本消耗，为ProducePay Chain积攒更多的资金用于平台的设计、智能应用的开发等。

政府农业管理部门

农业涉及民生，不可能回避政府的角色。而ProducePay Chain其链条透明的特性，可以助力政府农业管理部门更好地管理农业产业，监测农业大数据，做出快速、灵活的农业资源调配与管理。

ProducePay Chain团队构成

运营机构

为确保ProducePay Chain项目的公开和透明，ProducePay Chain通过设立最高决策机构——决策委员会进行管理。决策委员会下设业务委员会、技术委员会、综合事务委员会以及社区发展委员会，管理机构将由开发人员和职能委员会组成。决策委员会成员每届任期为两年，首届决策委员会成员由核心团队成员、区块链行业知名人士、法律专家和早期投资者组成，后续的决策委员会部分成员由社区选举产生。

运营监管

为了保证平台高效、透明、健康的运行，必须要对整个平台的活动进行监管。由于区块链技术的应用，平台所产生的各种数据都会被记录且无法篡改，因此一方面ProducePay Chain平台可以自行内部监管，自主互信；另一方面，平台设置ProducePay Chain自治委员会，对投资者社区大会负责，负责对其行使管理和监督的职能，两重监管保证平台以及平台利益相关者的利益。自治委员会每年根据所持代币的数量和币龄进行换届。

此外，理事会要设立审计、法律、财务等顾问，以报告、新闻的形式进行定期与不定期信息披露。理事会主要负责人的联系方式必须公开，接受各方的联络与监督。此外，理事会通过监督与报告双向通道，欢迎可再生资源协同平台用户、使用者、投资者共同参与管理、监督运营，对平台运营过程中的问题、重大危机、欺诈、舞弊等问题进行举报，同时必须确保举报人的信息保护。

运营团队

运 营 团 队 结 构 图

决策委员会职能包括聘请和解聘执行负责人以及各职能部门负责人、制定重要决策、召开紧急会议等，决策会员会成员每届任期为两年。

首届ProducePay Chain决策委员会成员在区块链领域或大流量领域具有丰富的行业经验，简要介绍如下：

1）决策委员会

决策委员会任期满后由社区所有持币成员根据所持有的ProducePay Chain代币数量和币龄计算权重进行投票，选出不超过9位的奇数位决策委员会核心成员，被选出的核心成员将代表ProducePay Chain社区做重要与紧急决策，并需要在任职期间接受授信调查并公开薪酬情况。

2）执行负责人

执行负责人由决策委员会选举产生，负责ProducePay Chain社区的日常运营管理、下属委员会的工作协调、主持决策委员会会议等。执行负责人定期向决策委员会汇报工作进展。

3）业务委员会

业务委员会负责社区整体的设计规划，以及引入相关的合作伙伴等。

4）技术委员会

技术委员会由核心开发人员组成，负责底层技术开发和审核、产品开发和审核等。技术委员会定时召开项目追踪会议，沟通需求和项目进展。技术委员会成员需要了解社区动态和热点，在社区中与业务参与者以及ProducePay Chain持有者进行沟通，并且不定期举办技术交流会。

5）综合事务委员会

综合事务委员会负责项目募集资金的使用和审核、开发人员薪酬管理、日常运营费用支出和审核等。

6）社区发展委员会

社区发展委员会的目标是为社区服务，负责ProducePay Chain产品和服务的推广、开源项目的推广和宣传等。委员会负责所有社区公告的发布和媒体的合作事宜。

7）ProducePay Chain的财务管理

ProducePay Chain决策委员会承诺将所有募集的代币用于社区发展和建设。

8）ProducePay Chain的审计

由于ProducePay Chain代币的特殊性，现有的各种形态的公司和机构事实上都难以在现有制度下进行监管。为了确保ProducePay Chain平台的治理工作以及代币使用的公开透明，ProducePay Chain决策委员会将聘请专业的审计机构进行审计。

ProducePay Chain发行计划

通证经济分配方案

种子轮销售份额 20% of tokens

种子轮销售价格 $0.01

种子轮销售截止时间 31/01/2018

种子轮销售所募金额 $6,199,200

战略销售份额 19.49% of tokens

战略销售价格 $0.02

战略销售截止时间 31/05/2018

战略销售所募金额 $24,548,832

私募销售份额 8.36% of tokens

私募销售价格 $0.02

私募销售截止时间 31/07/2018

私募销售所募金额 $15,498,000

公募销售份额 8.38% of tokens

比例	数量	分配方案
20%	180,000,000	种子轮
19.49%	175,410,000	战略轮
8.36%	75,240,000	私募
15%	135,000,000	团队配额
9.65%	86,850,000	顾问份额
19.13%	172,170,000	项目储蓄
8.38%	75,420,000	初始流通

种子轮销售情况

于 2018 年 1 月完成，以大约 $0.01 美元/PP 的价格售出总供给代币的 20.0%，筹得约 $180 万美元。

战略轮销售情况

于 2018 年 5 月完成，以大约 $0.02 美元/PP 的价格售出总供给代币的 19.49%，筹得约 $360 万美元。

私募销售情况

于 2018 年 7 月完成，以大约 $0.02 美元/PP 的价格售出总供给代币的 8.36%，筹得约 $150 万美元。

应用场景

1）智慧大数据

目前大数据的发展仍然面临许多问越。众所周知，如何保陳用户的隐私倍患是限制大数据 发展的关铤问越。大纖实际案例说明，即使无害的数据，一旦被大屋采集，也存在S3个人隐 私的风险。此外，大数据在存储、处理、传辅等过程中，也可能遇到潜在安全风险。而实现大 数据安全与隐私保护，单纯以技术手段限制服务商采集用户倍息，是极其困难的事。

为了挖掘数据共享的潜在价值，我们需要更好的解决方案来管理数据安全。集中式IT系统 在效率方面提供了优势，然而頻繁的数据泄露、透明度缺失以及数据的不完整性，亟需分布式 共识机制来弥补缺陷。区块链是一种分布式账本，其提供了可溯源、不可篡改的记录。基于区块链的技术可为固有安全的健康IT生态系统提供优化的解决方案，ProducePay通过智能合约对数 据进行采集、使用、授权等，保证数据的纯净性。通过ProducePay营造一个良好的生态图，利用区块链数据来构建智》大数据，未来将大大提升数据的安全性、除私性和可用性。同时，对公 有链上数据的授权传埔使用、查询交易费用，可通过收取ProducePay代币的方式解决。

2）区块链游戏

2017年全球游戏市场规横达到1090亿美金，正处于爆发式增长长阶段。

目前，除了免费游戏「F2P（Free-to-P丨ay）Gamesj外，线上游戏的商业揆式主要分为两种：用户付费购买游戏体验时长、用户付费构买虚拟游戏商品等增值服务。

虚拟游戏商品由中心化的服务商提供，出于商业目的，中心化的服务商通常会限制游戏内商品的转让，用户仅能在其专有平台上使用，而不能流通。对于有需求的用户而言，可能会在游戏环境之外发起虚拟游戏商品的交易。由于信思不对称等原因，交易流程繁琐，且用户可能遭遇欺诈。对于中心化的服务商而言，开发管理虚拟游戏商品的平台耗时费财，fi接禁止用户间的交易则更为容界。在此过程中，用户的虚拟游戏商品可能丢失、被没收或被更改，而用户却不具备对于虚似资产的追索权。此外，线上游戏可能也有一套封闭的经济系统，存在生产、分配、交换、消费等坏节，同现实世界一样，无法避免通胀通缩等问提，如果将虚似游戏商品存储在区块链上，以ProducePay为代表的加密数字货币取代游戏发行商提供的虚拟游戏货币，那么完全不需要游戏发行商及GooglePay、AppStore这样的中心化机构，虚似游戏商品即可便利地在用户之间流通。同时，去中心化的虚拟游戏货币产出方式和共享账本的交易流程将一定程度上消除游戏内的不透明性及通胀现象。此外，虚似游戏资产亦可走上证券化的道路。

ProducePay通过软硬件体系架构设计，稳定定支持百万级并发。可在线上游戏领域有广泛的应用。

风险提示

在ProducePay Chain项目的开发、维护和运营过程中存在着风险，这其中很多都会超出开发团队的控制。除本白皮书所述的其他内容外，请参与者充分知晓并同意接受了下述风险：

市场风险

ProducePay Chain代币的价格与整个数字货币市场形势密不可分，如市场行情整体低迷或存在其他不可控因素的影响，则可能造成ProducePay Chain代币本身即使具备良好的前景，但价格依然长期处于被低估的状态。

监管风险

由于区块链的发展尚处早期，在全球没有有关募集过程中的前置要求、交易要求、信息披露要求、锁定要求等相关的法规文件。并且目前政策会如何实施尚不明朗，这些因素均可能对项目的投资与流动性产生不确定影响。而区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则ProducePay Chain可能受到其影响，例如法令限制使用、销售数字金币有可能受到限制、阻碍甚至直接终止ProducePay Chain应用的发展。

竞争风险

当前区块链领域项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。并且随着信息技术和移动互联网的发展，其他应用平台的层出不穷和不断扩张，ProducePay Chain将面临持续的运营压力和一定的市场竞争风险。

人才流失风险

ProducePay Chain聚集了一批在各自专业领域具有领先优势和丰富经验的技术团队和顾问专家，其中不乏长期从事区块链行业的专业人员以及有丰富互联网产品开发和运营经验的核心团队。核心团队的稳定和顾问资源对ProducePay Chain保持业内核心竞争力具有重要意义。在今后的发展中，不排除有核心人员离开，核心人员或顾问团队的流失，可能会影响平台的稳定运营或对未来发展带来一定的不利影响。

核心协议相关的风险

ProducePay Chain目前基于某个特定的链开发，尽管团队会挑选目前最安全稳定的区块链作为基础设施，但该链发生的任何故障，不可预期的功能问题或遭受攻击都有可能导致ProducePay Chain以难以预料的方式停止工作或功能缺失。

系统性风险

软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分风险依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害。

无法预料的其他风险

基于密码学的数字金币是一种全新的技术，除了本白皮书内提及的风险外，还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其他风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。

免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成ProducePay Chain平台及其相关公司中出售股票或证券的任何买卖建议、教唆或邀约。本文档不组成也不理解为提供任何买卖行为，也不是任何形式上的合约或者承诺。

鉴于不可预知的情况，本白皮书列出的目标可能发生变化。虽然团队会尽力实现本白皮书的所有目标，所有购买ProducePay Chain的个人和团体将自担风险。文档内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。

本文档仅供主动要求了解项目信息的特定对象传达信息使用，并不构成未来任何投资指导意见，也不是任何形式上的合约或承诺。

ProducePay Chain明确表示不承担参与者造成的直接或间接的损失包括：

1）参与者一旦参与ProducePay Chain代币分发计划，即表示了解并接受该项目风险，并愿意个人为此承担一切相应后果。项目团队明确表示不承诺任何回报，不承担任何项目造成的直接或间接损失。

2）本项目涉及的代币是一个在交易环节中使用的虚拟数字编码，不代表项目股权、收益权或控制权。

3）由于数字货币本身存在很多不确定性（包括但不限于：各国对待数字货币监管的大环境、行业激励竞争，数字货币本身的技术漏洞），我们无法保证项目一定能够成功，项目有一定的失败风险，本项目的代币也有归零的风险。