农业生态链

基于区块链的农产品供应链系统及智能农业平台

Agricultural supply chain system and intelligent agricultural platform based on block chain

CNMC

农业生态链-基于区块链的农产品供应链系统及智能农业平台

摘　要

区块链是一个分布式数据库系统，具有公开透明，不可篡改等特点，区块链上流通着代币，代币以交易的形式传输价值，形成一个去中心化的信任网络。

区块链技术在快速发展，人们探索了区块链的很多应用，从最初的比特币支付和储值功能，发展至数字资产，数字身份等。

区块链技术在农业方面有重要的应用前景，认证溯源也是区块链的主要应用场景之一，利用不可篡改和时间戳的特性，在农产品苗等物品流转环节有所应用，在农业领域的应用目前还比较稀缺。

农业生态链既是一个农产品供应链系统，同时也是一个基于区块链的智能农业平台，大数据系统有助于科学生产，智能合约应用于农业有助于推动农业产业化发展。

农业生态链-基于区块链的农产品供应链系统及智能农业平台

1. 区块链发展历史

区块链（Blockchain）是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了过去十分钟内所有比特币网络交易的信息，用于验证其信息的有真实性并生成下一个区块。总体来说，这是一种通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案让参与系统中的任意多个节点共同维护并共享一段时间系统内全部信息交流的数据，通过密码学算法计算和记录到一个数据块（Block），并且生成该数据块的独特 ID 用于链接（Chain）上个数据块和校验，系统所有参与节点来共同认定记录是否为真。

1.1 比特币

区块链与比特币同时诞生于 2008 年，毫无疑问，比特币是截止到目前区块链技术最成功的一个应用案例。截至目前 8 年多的存续时间也佐证了区块链技术的可靠性。

比特币的诞生伴随着区块链的诞生，比特币是应用数学和金融领域的有效结合，是一个分布式数据库（P2P 特性），采用 POW 共识机制，数字签名采用椭圆曲线非对称密码系统。

1.2 点点币

PeerCoin，简称 PPC，名字取自 P2P 货币的意思，即点对点货币，因此被翻译为点点币。由 Sunny King 在 2012 年 8 月发布。PPCoin 的最大创新是其采矿方式混合了 PoW 工作量证明及 PoS 权益证明方式，PoS 采矿方式仅需普通电脑和客户端就能处理交易和维护网络安全，达到节能和安全的目的。

PPC 是从中本聪所创造的 BTC 衍生出来的一种 P2P 的电子密码货币，以权益证明（Proof of Stake，PoS）取代工作量证明（Proof of Work，PoW）来维护网络安全。在这种混合设计中，PoW 主要在最初的采矿阶段起作用。长远来看，PPC 网络的安全并不依赖能源的消耗。因此是一种清洁的密码货币。

1.3 比特股

比特股（Bitshare）首次采用了 DPOS 共识机制，进一步发展了区块链，将区块链发展带进 “二代币” 时代，同时实现了去中心化交易平台。比特股同样是一个新的基于区块链技术的开源软件。与基于工作量证明机制的比特币不同，比特股是基于权益证明机制的，这意味着它不需要矿工。

比特股软件用于发布去中心化自治公司（DACs），DACs 的理念是由比特股的创建者 Daniel Larimer 首次提出的。

1.4 以太坊

2013 年，加拿大小天才 Vitalik 发布了以太坊白皮书，经过一年多时间的开发，以太坊于 2015 年发布，以太坊试图打造一个图灵完备的世界计算机，在以太坊平台上不仅能流通货币，还能执行程序，构造智能合约。

简而言之，以太坊（Ethereum）是将比特币中的一些技术和概念运用于计算领域的一项创新。比特币被认为是一个系统，该系统维护了一个安全地记录了所有比特币账单的共享的账簿。以太坊利用了很多跟比特币类似的机制（比如区块链技术和 P2P 网络），来维护一个共享的计算平台，这个平台可以灵活且安全地运行用户想要的任何程序。本质上，以太坊的目标，就是将区块链技术所具有的去中心化、开放、和安全这三大特点，引入到几乎所有能被计算的领域。

2. 区块链应用探索

区块链在建立去中心化信用的尝试，已经不限于金融界，而被社会各个领域关注，特别是在中国目前一些中心性信用如“红会”，处于“塌陷”态势，区块链更能为社会管理提供一种全新的思路和技术选项。当前，区块链在物联网，知识产权，云计算，去中心化组织等领域都有新进展。

2.1. 数字货币

一般而言，数字货币（Digital Currency）分两类，一类指非密码货币（即数字黄金货币，如 e-gold，以及公司发行的货币，如 XRP），另一类即密码货币，也就是我们现在讨论的类似比特币的密码货币。使用密码货币有如下优势：

- 支付自由，无论何时何地都可以即时支付和接收任何数额的资金。无银行假日，无国界，无强加限制。比特币允许其用户完全控制他们的资金。
- 极低的费用，目前对比特币支付的处理不收取手续费或者仅收取极少的手续费。用户可以把手续费包含在交易中来获得处理优先权，更快收到由网络发来的交易确认。
- 降低商家的风险，比特币交易是安全，不可撤销的，并且不包含顾客的敏感或个人信息。

2.2. 数字资产

数字资产是指企业拥有或控制的，以电子数据的形式存在的，在日常活动中持有以备出售或处在生产过程中的非货币性资产。在我们生活中，你的钱在支付宝里直接消费就是常见的数字资产使用的一种方式，也就是电子支付系统，除此之外，我们经常用到的网络办公、网络炒股、在线读书或影音播放，都是在使用数字资产。股权通过数字资产形式进行分发。资产使用区块链数字资产有如下优势：

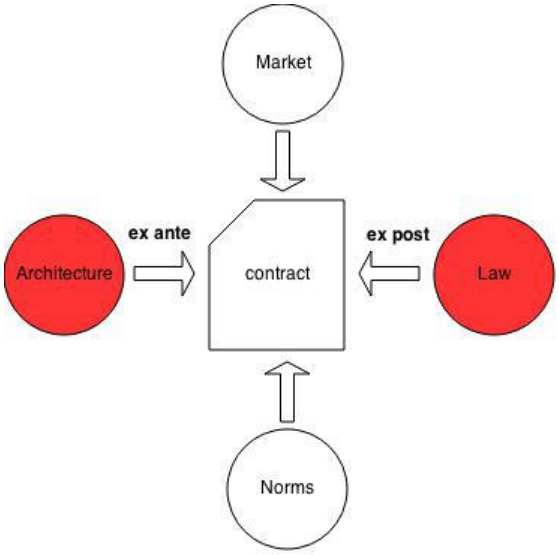
1) 去信任化。通过区块链的分布式系统，人与人之间的信任被转移到对机器的信任上。
2) 去中心化的特性。在现在，持有的股权想要转让要办理很多手续，找各种不同的部门才能办好，太浪费时间和金钱。而区块链技术如果加上电子合同就能改善掉这个问题。
3) 高度透明。我们最怕的不就是信息不透明，还有一些资产公示不完全么，应用区块链技术就能解决掉这个问题了。
4) 匿名化。我们经常一不小心就在互联网上进行“裸奔”了，我们的信息在某些不良的公司中被标价售卖，或者...我记得是有记者曝光过几百元查一个人所有记录的。

2.3. 数字身份

将我们活人映射进代码里，就变成了数字身份，在我们现行的经济活动过程中，国家通过法律手段获得建立了全民身份信息。又通过产权法等约定了财产和自然人之间的权益关系。在区块链里，先要构建数字身份认证服务，比如可以使用指纹等特有特征信息去构建，在这个基础之上才能发展智能合约，乃至物联网。

2.4. 智能合约

智能合约都是有独立的代码以规定合约的执行依据的，理论上，合约都需要一个仲裁平台，智能合约也不例外，不一样的是，智能合约的冲裁平台是区块链，而不是传统第三方机构。例如以太坊，借助图灵完备的虚拟机 EVM，完全无须第三方信任的代码便可让用户来构建智能合约，而 Rootstock 则是需要一个叫 50%信任制的仲裁联邦。这个仲裁依然不是活人去仲裁，也是代码。



此外，不可否认的是，智能合约必须被归类为与法律相关的行为。我们生活在一个被法律管理和控制的世界，所有可能的经济交易也被法律管理和控制。合约法只是组织经济交易的一种可能的工具。

3. 互联网+农业

3.1. 传统农业的发展瓶颈

传统农业是以土地为基本生产资料，以农户为基本生产单元的一种小生产。在现代农业中，农户广泛参与到专业化生产和社会化分工中，加入到各种专业化合作组织中，农业经营活动实行产业化经营。这些合作组织包括专业协会、生产合作社、供销合作社、公司加农户等各种形式，它们活动在生产、流通、消费、信贷等各个领域。而农民合作社作为新型农业

经营组织之一，在实际运营过程中却遇到不少难题，其中最突出的是土地大规模流转的困难。

国外经验表明，在工业化、城镇化快速推进时期，农业面临着容易被忽视或削弱的风险，必须倍加重视农业现代化与工业化、城镇化的同步推进和协调发展。当前，我国工业化、城镇化呈现快速发展态势，但农业现代化明显滞后，面临着一系列严峻挑战。经过总结分析，我国目前农业发展仍存在很多问题，主要表现在以下方面：土地特别是耕地资源不断减少；耕地质量退化；农业剩余劳动力过多；农产品生产成本不断上升，收益持续下降，农业的比较优势弱；水资源缺乏及污染等严重问题。

3.2. 互联网+农业发展现状

互联网+农业正处风口，吹来了机遇，也有挑战，当巨大发展与产业升级的机会迎面而来时，中国农业如何迎风起飞，落地执行，需要更多农业建设者们的冷思考和热处理。

当前我国农业产业链系统效率低下，农业现代化程度依然很低，产业链面临“内忧外患”。拥抱互联网也就成了农业未来的新出路，作为最传统的产业，农业被互联网改造的潜力最大。“互联网+农业”实现的是农业产业的跨越式发展，不再只是简单互联网接入农业，或者农业融合互联网，从而实现去中间化，提升效率等旧有模式，而是成功地将互联网与社会资本带入驱动农业发展的轨道中。一方面，“互联网+农业”促进专业化分工、提高组织化程度、降低交易成本、优化资源配置、提高劳动生产率。另一方面，“互联网+农业”通过便利化、实时化、感知化、物联化、智能化等手段， 为农地确权、农技推广、农村金融、农村管理等提供精确、动态、科学的全方位信息服务，正成为现代农业跨越式发展的新引擎。

3.3. 区块链+农业发展前景

因为区块链特性给大家提供很大的想象空间，所以目前已经有很多公司看到区块链在农业领域有广泛应用前景，便开始探索“区块链+农业”的应用。通过互联网及互联网身份标识技术，将生产商生产出来的每件产品信息全部记录到区块链中，就可以在区块链中形成每一件商品的真实生命轨迹。消费者通过自己的智能终端，可实时跟踪每件商品的动态，从而保证消费流程全透明。

区块链+农业实质是通过区块链技术构建自治溯源的封闭体系，实行“区块链+农业”的战略组合，打开“大数据农业”的新大门，对生产、流通、经营、金融服务、人才培养等农业产业链各环节进行深度改造，促进农业向信息化、科技化转型升级，优化农业供给侧，提升农业运营效率和质量。

3.4. 农业科技金融

农民贷款整体上比较难，主要原因是缺乏有效抵押物，归根到底就是缺乏信用抵押机制。由于区块链建立在去中心化的 P2P 信用基础之上，她超出了国家和地域的局限，在全球互联网市场上，能够发挥出传统金融机构无法替代的高效率低成本的价值传递的作用。当新型农业经营主体申请贷款时，需要提供相应的信用信息，这就需要依靠银行、保险或征信机构所记录的相应信息数据。但其中存在着信息不完整、数据不准确、使用成本高等问题，而区块链的用处在于依靠程序算法自动记录海量信息，并存储在区块链网络的每一台电脑上，信息透明、篡改难度高、使用成本低。因此，申请贷款时不再依赖银行、征信公司等中介机构提

供信用证明，贷款机构通过调取区块链的相应信息数据即可。

3.5. 区块链应用于农业领域的障碍

对于困扰着粮食和农业部门的各种问题，区块链技术听起来可能像一剂灵丹妙药。然而，真正应用起来还会存在很多问题，即使供应链中的所有各方都将不可避免地采用这种技术，而真正让不同的公司和组织都应用起来还会有一定距离。需要强调的是，所有各方的充分参与才是成功整合区块链技术的必要条件。

广泛的区块链应用有赖于一个可靠的互联网连接。在一些发展中国家，农户在没有宽带接入的情况下难以应用这一技术。安全问题可能是区块链应用需要克服的最大障碍。每次交易都成为存储的数据。一方面，区块链被认为是安全的，“牢不可破”的，但就那些围绕该技术开发的系统来说，这一点难以成立。比特币交易所的安全漏洞频频发生，而最近，在以太坊交易所的漏洞就导致了数亿美元的损失。

在区块链上，个人丢失密钥等因素可能造成不必要的延迟。在最坏的情况下，一个脆弱的密钥可能会威胁到整个链的安全，特别是在该密钥落入黑客手中的时候。

4. 农产品供应链系统

4.1. 需求分析

食品质量与诸如心脏病、肝炎、中风、糖尿病及癌症等慢性病有关系。通过改善食品质量，我们可以明显降低慢性病发病率。首先我们要回答一个问题：我们为什么吃质量不好的食品？问题出现在 3 个环节：生产、运输和销售。

食品生产发生在农场。农业通常面临高风险——自然灾害、减产、事故，等等——这些风险都会直接影响到产出。另一个问题在于食品运输的物流状况。现在的农业已经完全处于

生产者-分配者-消费者的巨大的链状模型中。大型的食品生产商通常能对位于发展中国家的食品生产进行管理，然后通过庞大的物流网络将食品销售到全世界。生产者们通常没办法将食品直接销售给消费者，而只能依靠分配者或商户来低价买。大公司因此可以以很低的价格大量买进食品。但这些食品通常并没有被完全消费掉。结果是造成食品的浪费和处理问题。花费能源和肥料来养殖并输送的食品却没有被消费掉，这是一个可憎的浪费。可以看出，整个食品供应链都可能出信任问题，

4.2. 解决方案

产品从生产到销售，从原材料到成品到最后抵达客户手里整个过程中涉及到的所有环节，都属于供应链的范畴。目前，供应链可能涉及到几百个加工环节，几十个不同的地点，数目如此庞大，给供应链的追踪管理带来了很大的困难。区块链技术可以在不同分类账上记录下产品在供应链过程中涉及到的所有信息，包括涉及到的负责企业，价格，日期，地址，质量，以及产品状态等，交易就会被永久性、去中心化地记录，这降低了时间延误、成本和人工错误。

农业产业化过程中，生产地和消费地距离拉远，消费者对生产者使用的农药、化肥以及运输、加工过程中使用的添加剂等信息根本无从了解，消费者对生产的信任度降低。基于区块链技术的农产品追溯系统，所有的数据一旦记录到区块链账本上将不能被改动，依靠不对称加密和数学算法的先进科技从根本上消除了人为因素，使得信息更加透明。

5. 智能农业平台

5.1. 农业大数据系统

农业大数据是融合了农业地域性、季节性、多样性、周期性等自身特征后产生的来源广泛、类型多样、结构复杂、具有潜在价值，并难以应用通常方法处理和分析的数据集合。农业大数据保留了大数据自身具有的规模巨大（volume）、类型多样（variety）、价值密度低（value）、处理速度快（velocity）、精确度高（veracity）和复杂度高（complexity）等基本特征，并使农业内部的信息流得到了延展和深化。大数据技术和农业相结合将赋予改变农业从田间到餐桌的整个链条，比如推动精细化农业、实现全程可追溯、打开企业“黑箱”推动并购重组等，“大数据+农业”或将重新定义农业。

农业生态链记录一切可以数据化的领域：从上游生产到中下游流通，再到销售终端，消费者分析和画像，农业将因为大数据变得不同。大数据使得种植过程更加科学，很多风险由此可以规避。结合已经非常成熟的 GPS 技术，生产活动进行之前，可以经由计算机做分析，并且第一时间将分析结果发送到农机或智能手机上。农民可以及时掌握田间各种因素的信息（比如土壤施肥情况等），分析作物的成长状况，以及帮助农民实现科学管理决策，判断化肥和杀虫剂的使用量和施用时机，提高效率避免浪费，从而实现增产。

5.2. 农业物联网发展基础

农业物联网，即通过各种仪器仪表实时显示或作为自动控制的参变量参与到自动控制中的物联网。可以为温室精准调控提供科学依据，达到增产、改善品质、调节生长周期、提高经济效益的目的。农业物联网一般应用是将大量的传感器节点构成监控网络， 通过各种传感器采集信息， 以帮助农民及时发现问题， 并且准确地确定发生问题的位置， 这样农业将逐渐地从以人力为中心、依赖于孤立机械的生产模式转向以信息和软件为中心的生产模式，从而大量使用各种自动化、智能化、远程控制的生产设备。

区块链技术为物联网提供了点对点直接互联的方式进行数据传输，整个物联网解决方案不需要引入大型数据中心进行数据同步和管理控制，包括数据采集、指令发送和软件更新等操作都可以通过区块链的网络进行传输。

5.3. 智能合约推动农业产业化

基于区块链技术的智能合约不仅可以发挥智能合约在成本效率方面的优势，而且可以避免恶意行为对合约正常执行的干扰。将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障存储、读取、执行整个过程透明可跟踪、不可攥改。

农业生产是个受多种因素影响的复杂过程，在种植之前，农民要决定耕种次序是什么、种什么作物、选哪种型号的种子，以及化肥、农药、施肥、灌溉的频率如何把握等诸多决定，

林林总总有四五十项之多，但是人很容易出错，一旦犯错，一年浪费了，沉没成本非常高。

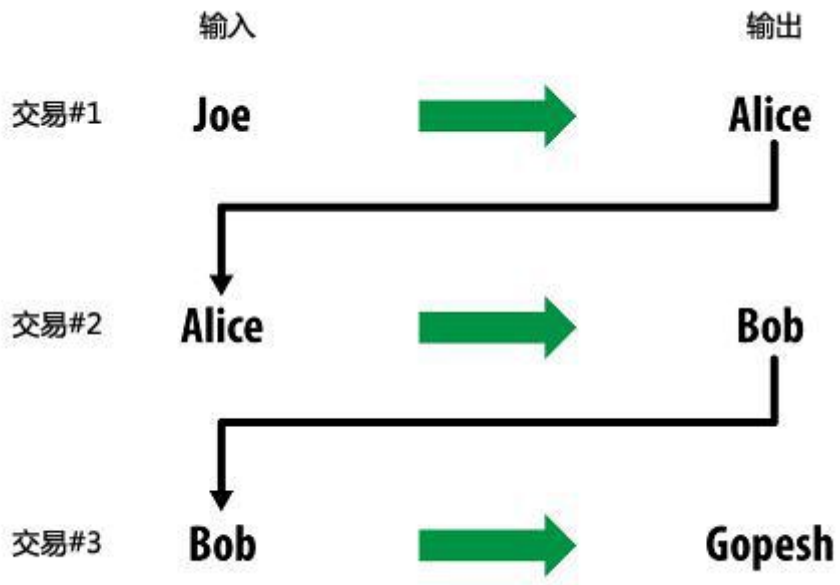
6. 技术实现方案

6.1. UTXO 设计

交易的输出会被创建成为一个包含这笔数额的脚本的形式，只能被引入这个脚本的一个解答后才能兑换。简单点说就是，Alice 的交易输出会包含一个脚本，这个脚本说“这个输出谁能拿出一个签名和 Bob 的公开地址匹配上，就支付给谁”。因为只有 Bob 的钱包的私钥可以匹配这个地址，所以只有 Bob 的钱包可以提供这个签名以兑换这笔输出。因此 Alice 会用需要 Bob 的签名来包装一个输出。


```
{
  "unspent_outputs": [
    {
      "tx_hash":"186f9f998a5...2836dd734d2804fe65fa35779",
      "tx_index":104810202,
      "tx_output_n":0,
      "script":"76a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac",
      "value":10000000,
      "value_hex":"00989680",
      "confirmations":0
    }
  ]
}
```


当 Bob 花费从 Alice 和其他顾客那里赚得的比特币时，他就扩展了比特币的交易链条。而这个链条会被加到整个区块链账簿，使所有人知晓并信任。我们假定 Bob 向在邦加罗尔的网站设计师 Gopesh 支付一个新网页的设计费用



6.2. 非对称密码系统

自从公钥加密被发明之后，一些合适的数学函数被提出，譬如：素数幂和椭圆曲线乘法。这些数学函数都是不可逆的，就是说很容易向一个方向计算，但不可以向相反方向倒推。基于这些数学函数的密码学，使得生成数字密钥和不可伪造的数字签名成为可能。比特币正是使用椭圆曲线乘法作为其公钥加密的基础算法。

在农业生态链系统中，我们用公钥加密创建一个密钥对，用于控制比特币的获取。密钥对包括一个私钥，和由其衍生出的唯一的公钥。公钥用于接收比特币，而私钥用于比特币支付时的交易签名。

公钥和私钥之间的数学关系，使得私钥可用于生成特定消息的签名。此签名可以在不泄露私钥的同时对公钥进行验证。

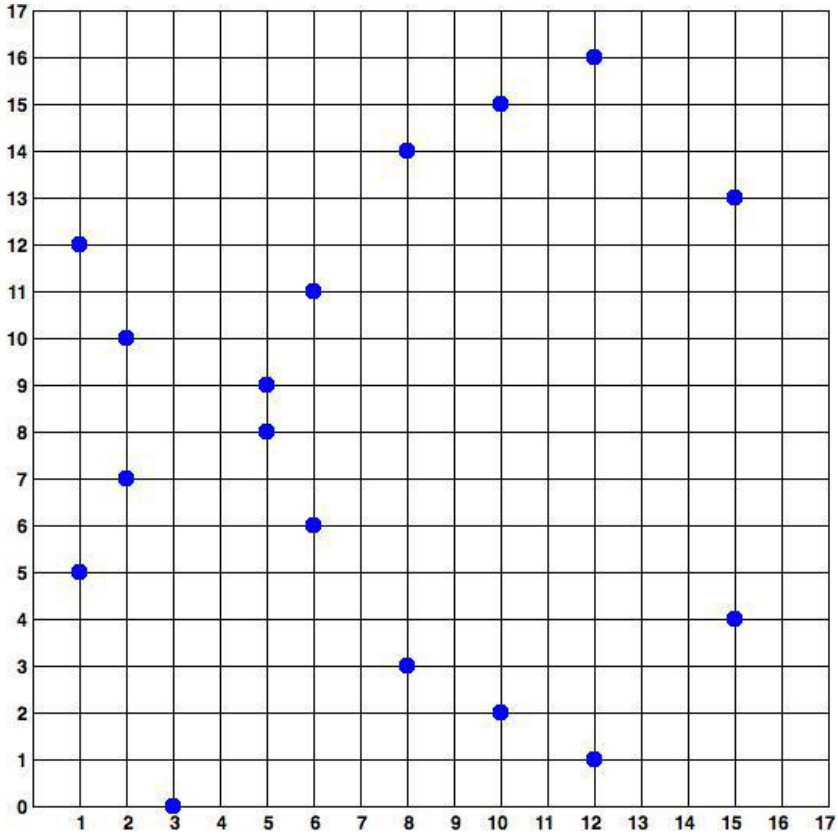
类似比特币，农业链采用 secp256k1 标准所定义的一条特殊的椭圆曲线和一系列数学常数。该标准由美国国家标准与技术研究院（NIST）设立。secp256k1 曲线由下述函数定义，该函数可产生一条椭圆曲线：

$y^2 = (x^3 + 7)\}$ over (F_p)

或

$y^2 \bmod p = (x^3 + 7) \bmod p$

上述 *mod p*（素数 p 取模）表明该曲线是在素数阶 p 的有限域内，也写作 F_p，其中 $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$，这是一个非常大的素数。



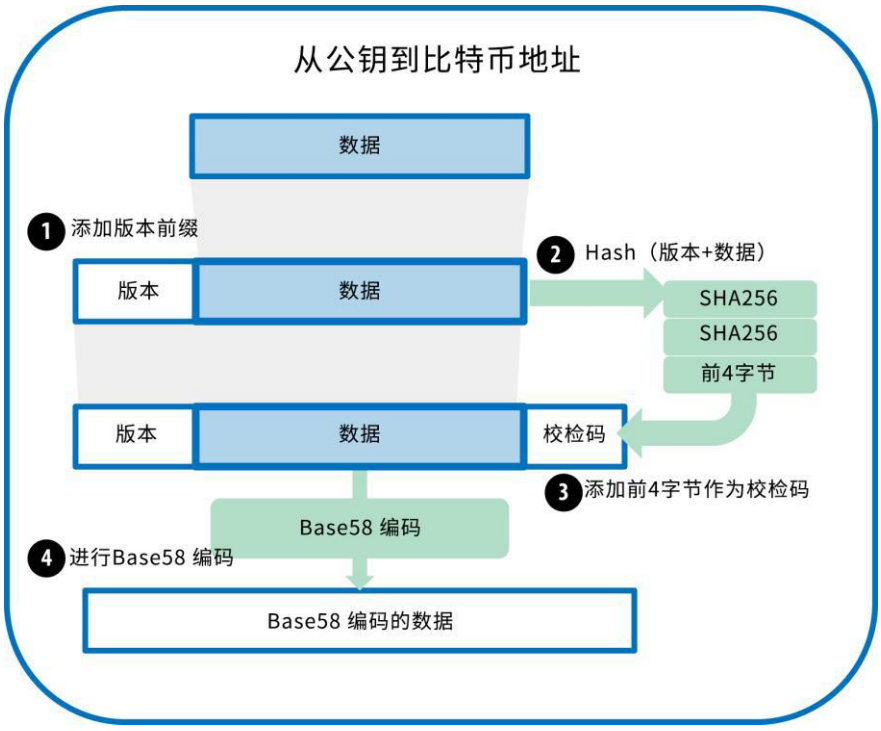
因为这条曲线被定义在一个素数阶的有限域内，而不是定义在实数范围，它的函数图像看起来像分散在两个维度上的散点图，因此很难画图表示。不过，其中的数学原理与实数范围的椭圆曲线相似。作为一个例子，上图显示了在一个小了很多的素数阶 17 的有限域内的椭圆曲线，其形式为网格上的一系列散点。而 secp256k1 的比特币椭圆曲线可以被想象成一个极大的网格上一系列更为复杂的散点。

6.3. 从私钥到地址的演变

我们并非直接使用公钥作为账号或地址，而是要经过一系列转换，这个设计也提现了中本聪天才的设计。

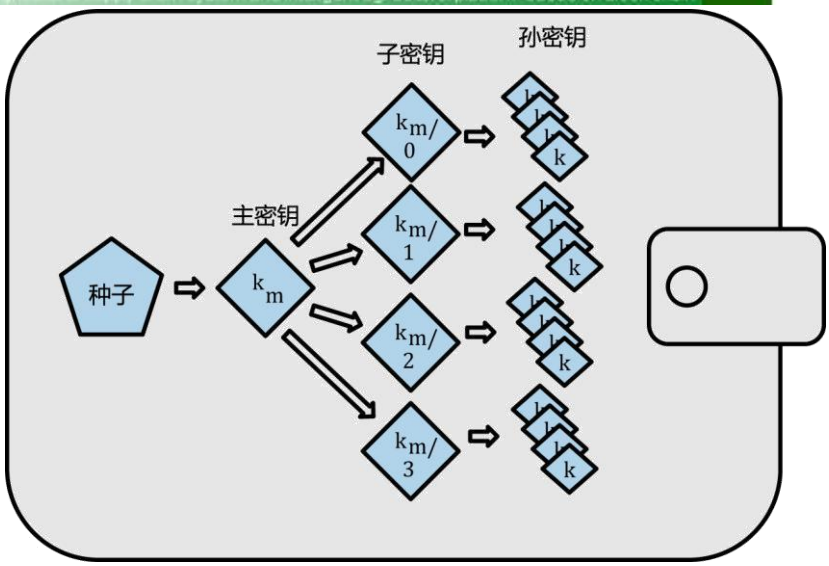
为了更简洁方便地表示长串的数字，许多计算机系统会使用一种以数字和字母组成的大于十进制的表示法。Base64 使用了 26 个小写字母、26 个大写字母、10 个数字以及两个符号（例如“+”和“/”），用于在电子邮件这样的基于文本的媒介中传输二进制数据。Base58 不含 Base64 中的 0（数字 0）、O（大写字母 o）、l（小写字母 L）、I（大写字母 i），以及“+”和“/”两个字符。简而言之，Base58 就是由不包括（0，O，l，I）的大小写字母和数字组成。

地址的生成过程如图示：



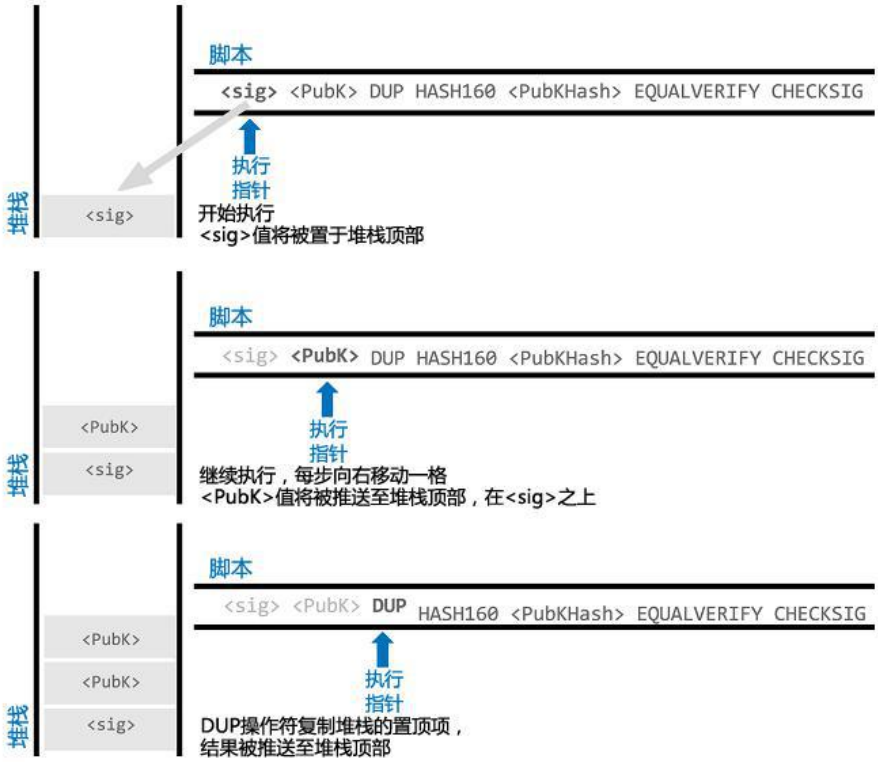
6.4. 分层确定性钱包

确定性钱包被开发成更容易从单个“种子”中生成许多关键的钥匙。最高级的来自确定性钱包的形是通过 BIP0032 标准生成的 the hierarchical deterministic wallet or HD wallet defined。分层确定性钱包包含从数结构所生成的钥匙。这种母钥匙可以生成子钥匙的序列。这些子钥匙又可以衍生出孙钥匙，以此无穷类推。这个树结构表如下图所示。



6.5. 脚本系统设计

借助比特币，农业链脚本语言基于基于栈语言，因为它使用的数据结构被称为栈。栈是一个非常简单的数据结构，它可以被理解成为一堆卡片。栈允许两类操作：入栈和出栈。入栈是在栈顶部增加一个项目，出栈则是从栈顶部移除一个项目。



脚本语言通过从左至右地处理每个项目的方式执行脚本。数字（常数）被推送至堆栈，操作符向堆栈推送（或移除）一个或多个参数，对它们进行处理，甚至可能会向堆栈推送一个结果。例如，OP_ADD 将从堆栈移除两个项目，将二者相加，然后再将二者相加之和推送到堆栈。

6.6. 共识机制

中本聪很清楚建立一个支付系统的信用必须解决防止“重复支付”问题，也就是不能造假币。中心化的信用系统是靠国家机器防止造假币。“比特币”怎么办呢？中本聪的伟大创新是给每一笔交易“盖时间戳”（timestamp）。每十分钟一个区块，把这十分钟的全网交易都正确的盖上时间戳。问题是谁来盖呢？中本聪并没有假设互联网上都是雷锋，他同意亚当.斯密的观点：市场上的人是贪婪的。他让所谓自称“矿工”的人去竞争这十分钟一个区块的记账权，竞争的规则就是正确记账的同时要去解 SHA256 难题，谁能证明自己的计算机算力最快，即工作量证明机制（Proof-Of-Work，POW）。其原理如下：

SHA256D(nVersion,hashPreBlock,hashMerkleRoot ,nBits,Nonce)<MAXTARGET/Diff

其中，左边式子括号里的参数为区块头的字段，分别表示版本号，前一个区块 id，交易默克尔树根，难度值，随机值。MAXTARGET 为最大目标值，常量；Diff 代表难度，全网难度一致。MAXTARGET/Diff 即通常所说的当前目标值。

很显然，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。相对其他共识机制而言，POW 逻辑简单，容易实现，容错达 50%，其安全有严格的数学论证。

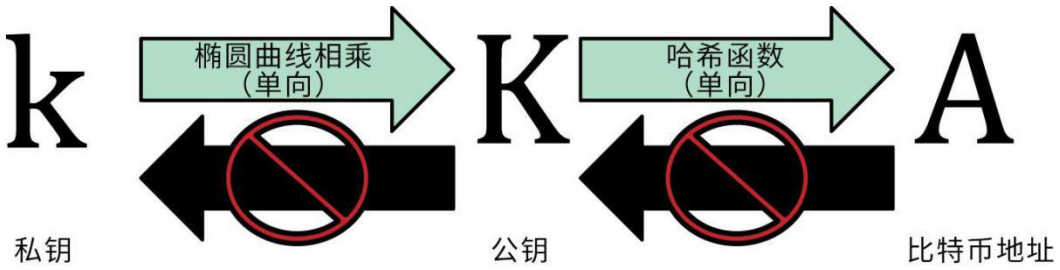
POW 并非完美，其中被指责最多的主要有两点，一是浪费能源，二是风险和收益博弈必然导致联合挖矿，而大算力矿池可能会对系统的去中心化构成威胁。于是有了权力证明机制（Pfoor-Of-Stake，POS），其原理如下：

SHA256D(nStakeModifier + txPrev.block.nTime + txPrev.offset + txPrev.nTime + txPrev.vout.n + nTime)< bnTarget * nCoinDayWeight

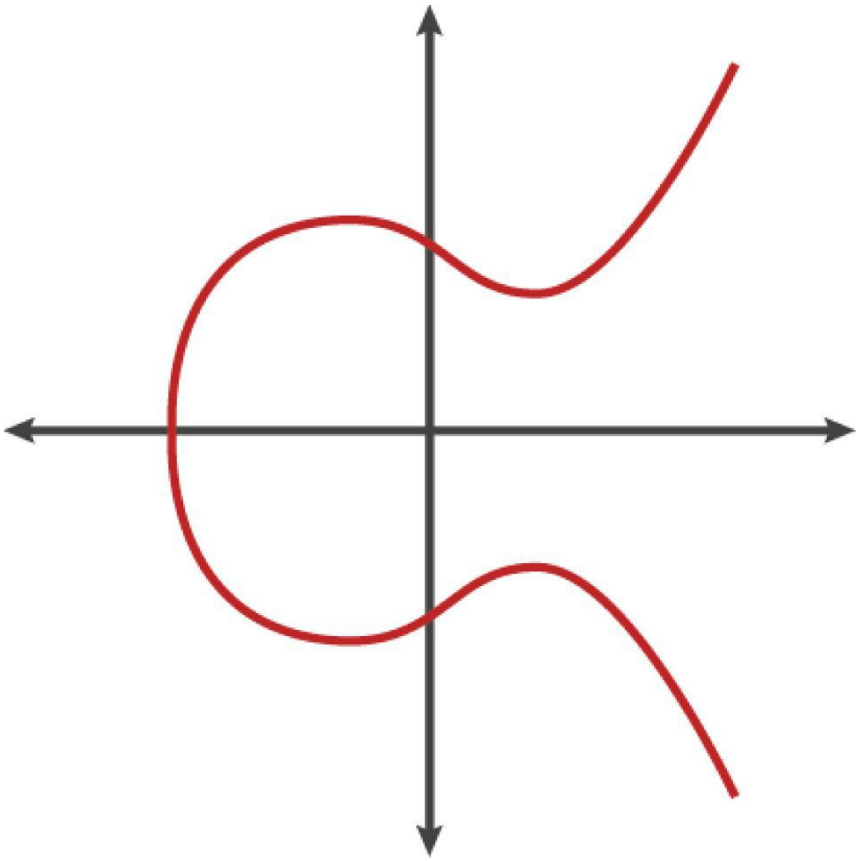
式子的每一个参数都有明确的设计目的，总体是为了实现挖到块的概率和余额成正比，并且同时具备随机性。Coinstake 结构图如下：

6.7. 私钥和公钥

自从公钥加密被发明之后，一些合适的数学函数被提出，譬如：素数幂和椭圆曲线乘法。这些数学函数都是不可逆的，就是说很容易向一个方向计算，但不可以向相反方向倒推。基于这些数学函数的密码学，使得生成数字密钥和不可伪造的数字签名成为可能。比特币正是使用椭圆曲线乘法作为其公钥加密的基础算法。



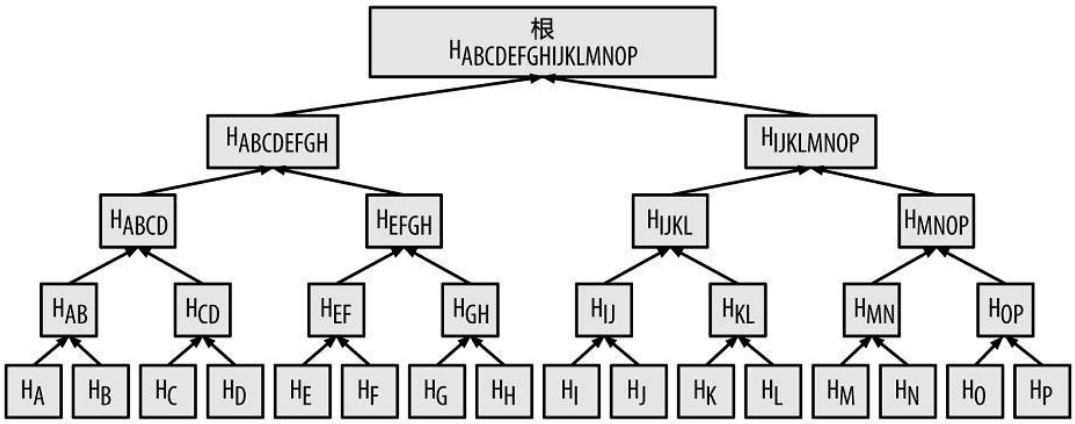
私钥就是一个随机选出的数字而已。一个比特币地址中的所有资金的控制取决于相应私钥的所有权和控制权。在比特币交易中，私钥用于生成支付比特币所必需的签名以证明资金的所有权。私钥必须始终保持机密，因为一旦被泄露给第三方，相当于该私钥保护之下的比特币也拱手相让了。私钥还必须进行备份，以防意外丢失，因为私钥一旦丢失就难以复原，其所保护的比特币也将永远丢失。



通过椭圆曲线算法可以从私钥计算得到公钥，这是不可逆转的过程：K = k * G 。其中 k 是私钥，G 是被称为生成点的常数点，而 K 是所得公钥。其反向运算，被称为“寻找离散对数”——已知公钥 K 来求出私钥 k——是非常困难的，就像去试验所有可能的 k 值，即暴力搜索。在演示如何从私钥生成公钥之前，我们先稍微详细学习下椭圆曲线加密学。

6.8. Merkle 树

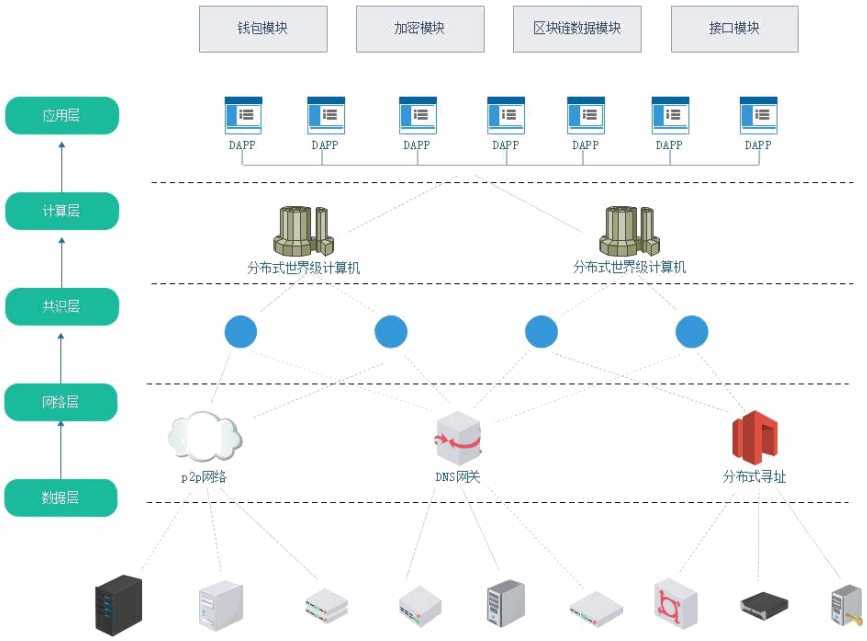
Merkle 树是一种哈希二叉树，它是一种用作快速归纳和校验大规模数据完整性的数据结构。



这种二叉树包含加密哈希值。在比特币网络中，Merkle 树被用来归纳一个区块中的所有交易，同时生成整个交易集合的数字指纹，且提供了一种校验区块是否存在某交易的高效途径。生成一棵完整的 Merkle 树需要递归地对哈希节点对进行哈希，并将新生成的哈希节点插入到 Merkle 树中，直到只剩一个哈希节点，该节点就是 Merkle 树的根。在比特币的 Merkle 树中两次使用到了 SHA256 算法，因此其加密哈希算法也被称为 double-SHA256。

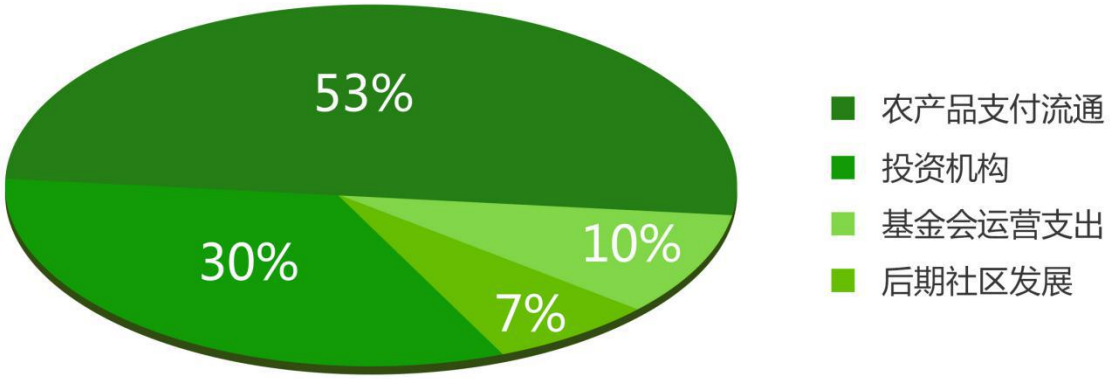
6.9. 系统分层架构

农业生态链采用五层架构模式，这种模式最大优点是将服务、接口和协议这三个概念明确地区分开来：服务说明某一层为上一层提供一些什么功能，接口说明上一层如何使用下层的服务，而协议涉及如何实现本层的服务；这样各层之间具有很强的独立性。其原理图如下：


钱包模块
加密模块
区块链数据模块
接口模块
应用层
计算层
共识层
网络层
数据层
DAPP
DAPP
DAPP
DAPP
DAPP
DAPP
DAPP
分布式世界级计算机
分布式世界级计算机
p2p网络
DNS网关
分布式寻址

7.分发机制

农业生态链发行总量为 3.8 亿其中 5 千万枚已永久锁死，只剩 3.3 亿，共有四部分组成。



1）农产品支付流通

用于农业产业生态系统产品，买卖支付工具。

2）投资机构

用于激励投资机构。

3）基金会运营支出

作为基金会各项运营支出。

4）后期社区发展

维护社区持续良性的发展。

8.开发单位

北京华联集团香港分公司——香港中鸣集团

9.风险提示

农业生态链内置代币简称为 CNMC，虽然基于区块链的数字资产已经非常安全，由强大的密码学能保证私钥能掌控一切，但其实还有一个更大的风险存在。私钥数据文件丢失的情况时有发生。用户必须非常注意不要剑走偏锋，这样不至于会搞丢 CNMC 币。

假如你有比特币，并且经常会将所有的币放在一个钱包里，那你就需要注意了，应该将风险分散到不同类型的比特币钱包。审慎的用户应该只留一小部分（或许低于 5%）的 CNMC 在一个在线的或手机钱包，就像零用钱一样，其余的部分应该采用不同存储机制分散开来，诸如电脑钱包和离线（冷存储）钱包等，CNMC 将提供多终端钱包。

当持有的 CNMC 为集体时，你该考虑采用多重签名解决方案。多重签名需要多个签名才能支付，从而保证资金的安全。多重签名的密钥应存储在多个不同的地方，并由不同的人掌控。打个比方，在企业环境中，密钥应该分别生成并由若干公司管理人员持有，以确保没有任何一个人可以独自占有资金。多重签名的地址也可以提供冗余，例如一个人持有多个密钥，并将它们分别存储在不同的地方。