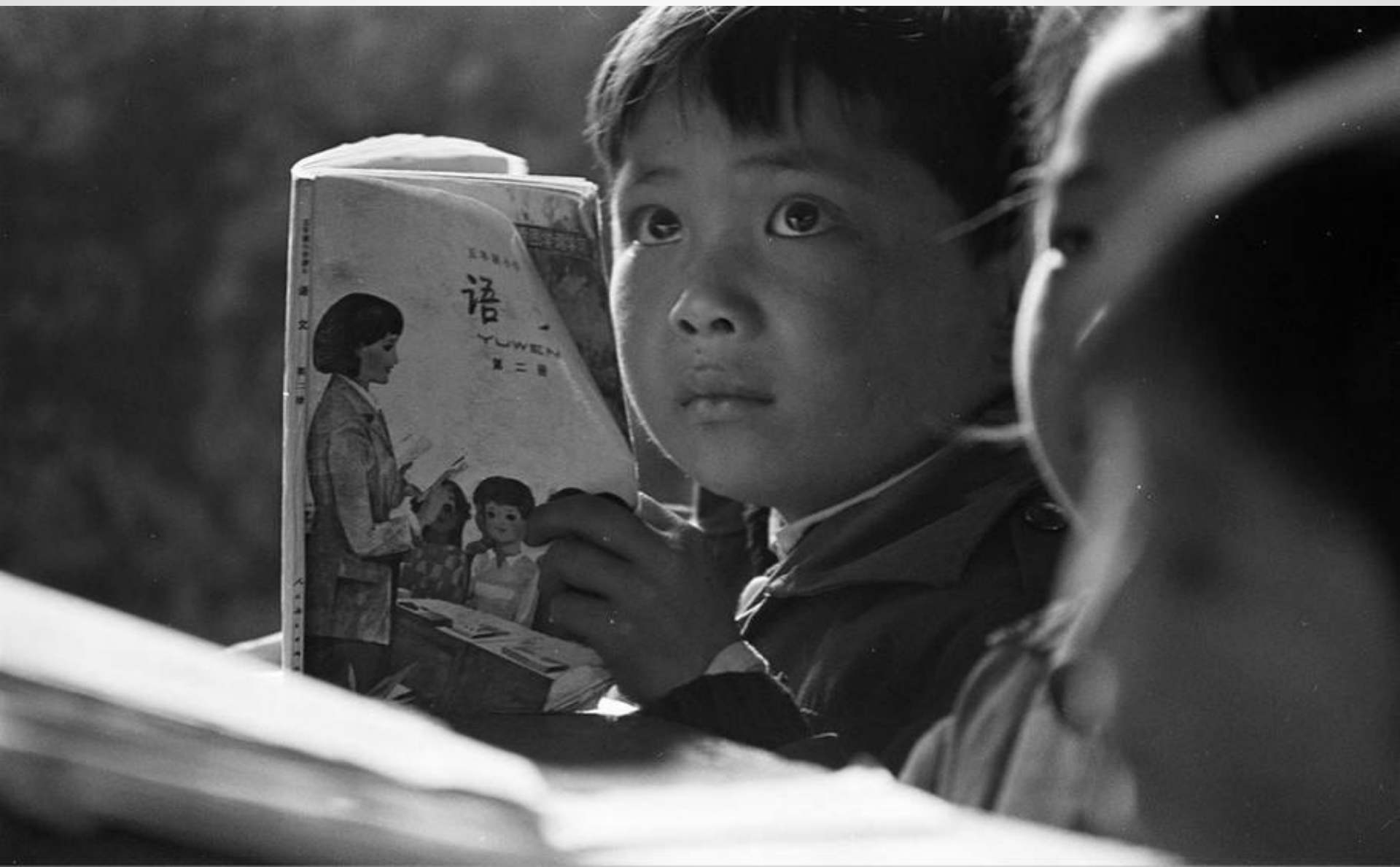


精准扶贫台账系统项目 技术方案

2017.12

一、贫困及扶贫



贫困现状

- 我国是一个幅员辽阔，人口众多的发展中国家。贫困问题作为当今世界最尖锐的社会问题之一，也广泛存在于我国社会中。
- 根据国家扶贫办**2015年10月12日**发布的数据，按照**2011年**确定的我国相对贫困的标准（农村人均纯收入**2300元**，接近世界银行**1.25美元/天**的标准），我国目前尚有**7017万**贫困人口。

精准扶贫

- 在“十三五”脱贫攻坚工作有关情况新闻发布会上，细化了精准扶贫和精准脱贫的基本要求与主要途径，包括了六个精准：
 - 扶贫对象精准
 - 项目安排精准
 - 资金使用精准
 - 措施到户精准
 - 因村派人精准
 - 脱贫成效精准
- 这六个方面，并非一件事情的孤立切面，而是统一过程的不同重点环节，彼此依赖和相互联系，其成效必须是相互验证的。

如何精准扶贫

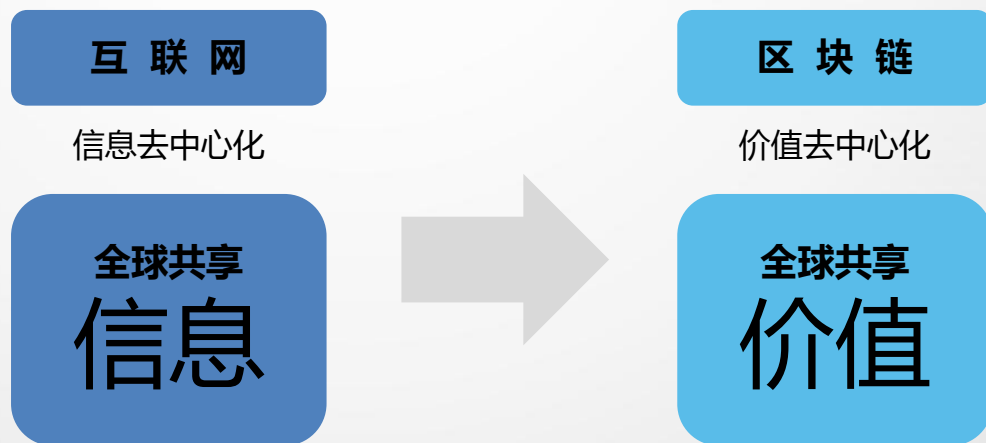
- 要在扶贫工作中做到六个“精准”，必须借助必要的技术手段，如果仅靠人力参与，成本较高而且也难以做到精准。
- 区块链，是脱胎于2008年出现的比特币技术的一种去中心化的、无需信任积累的信用建立范式。由于其去中心化属性，使人们看到了其提高社会整体运行效率，改变社会结构的潜质，所以自从其问世以来，众多产业和投资机构看好其在各方面的应用，目前其在金融，互联网等行业正在由设想发展出实际的应用和新的模式。而区块链能够准确，分布式地追踪，记录款项的产生和流动，且不可轻易篡改的特性，能够从技术层面解决目前政府扶贫工作中的一些问题，同时结合其他一些互联网技术，能够更好地提供将扶贫工作进行量化，并提供支撑起精准化工作的平台和框架。

二、区块链



区块链是一种互联网底层的分布式数据库技术

- 区块链（Block-Chain）是指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，把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指纹用于链接（chain）下个数据块和校验，系统所有参与节点来共同认定记录是否为真。
- 区块链技术的开发和应用有望实现从信息互联网向价值互联网的转变。区块链通过构建P2P自组织网络、时间有序、本共识改的加密账本、分布式共识机制，从而实现去中心化信任。全网记账，共同公证，创造基于计算机算法而不依赖第三方的信任机制，实现价值的点对点传输。



区块链的技术特点

1

去中心化

数据的传输不再依赖某个中心节点，而P2P的直接传输。全网络的每个节点都遵循共识开源协议，自由安全传输数据。所有交易记录是对全网络公开的，每个节点都可备份。

2

去信任化

利用成熟的密码学来保障交易的不可欺骗性，建立各方的信任关系。参与整个系统中的每个节点之间进行数据交换是无需互相信任的。

3

稳定性
可靠性

系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

4

开放性

系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

5

交易公开透明，
不可篡改

区块链中所有的数据记录公开透明，对所有的参与方提供设计功能，并且数据不可篡改。这种技术不仅确保了数据的正确来源，也确保了数据在中间过程不被人拦截。



稳定

安全

低成本

区块链发展概述

- 国内：

2016年10月，工业和信息化部发布《中国区块链技术和应用发展白皮书（2016）》。

2016年12月，区块链首次被作为战略性前沿技术、颠覆性技术写入国务院发布的《国务院关于印发“十三五”国家信息化规划的通知》。

2017年1月，央行推动的基于区块链的数字票据交易平台已测试成功。

- 国外：

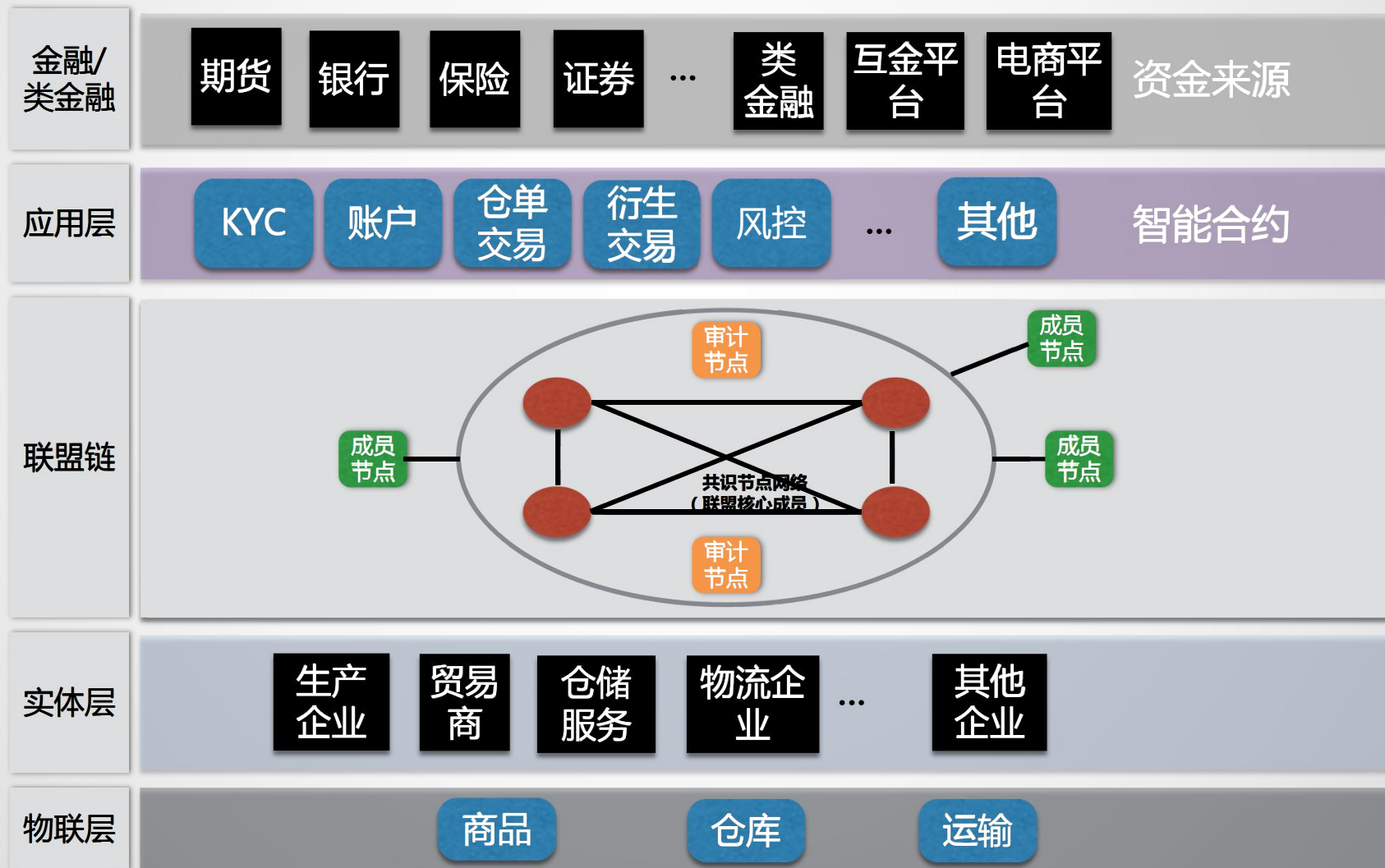
2016年1月，英国政府发布《分布式账本技术：超越区块链》白皮书，鼓励对区块链技术的深入研究。

2016年1月，美国存管信托和结算公司（DTCC）发布《拥抱颠覆——开发分布式账本的潜力，改善交易后的环境》。

2016年4月，欧洲数字货币与区块链技术论坛（EDCAB）为欧盟议会的政策制定者举办了一个集中讨论区块链的“博览会”。

链链区块链-总体架构

资配易推出了自己的区块链平台--链链区块链，有多项自主研发成果，已有多个项目在该平台上稳定运行了近一年时间。



链链区块链-BaaS基础平台

基于Hyperledger Fabric底层区块链平台建立BaaS（区块链即服务Blockchain-as-a-Service），为上层应用提供技术支撑。

Hyperledger Fabric是由Linux 基金会发起创建的开源区块链分布式账本项目，该项目的愿景是借助项目成员和开源社区的通力协作，共同制定并建立一个开放、跨产业、跨国界的区块链技术开源标准，让任何数字化的价值交换都可以被透过具经济成本效益且安全的方式进行交易及追踪。

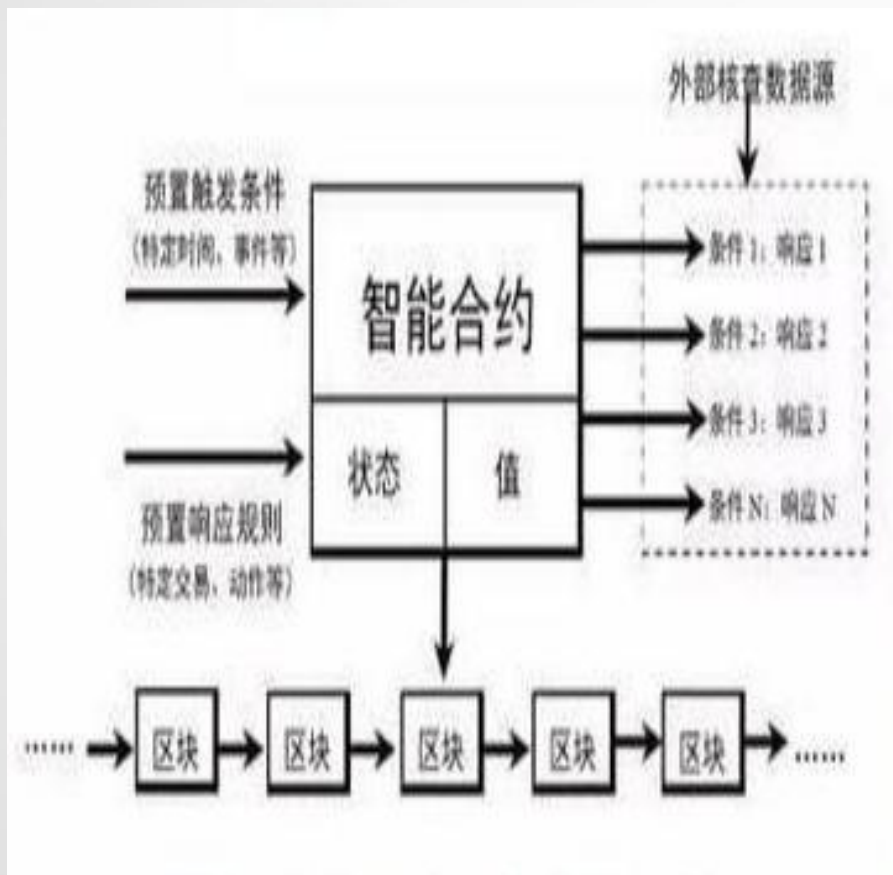
成员包括思科、IBM、英特尔、红帽等大型科技企业，以及摩根大通、富国银行、德意志交易所集团等金融机构，链链也是其成员之一。

共识机制PBFT

由于区块链是分布式的，既要保证各个节点的处理一致，又要容错（某节点故障或被攻击），所以需要一种共识算法保证各节点对处理能达成 共识，平台使用PBFT算法，极倔原始拜占庭容错算法效率不高的问题，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行。

央行推出的区块链数字票据交易平台就是基于PBFT算法。

链链区块链-智能合约

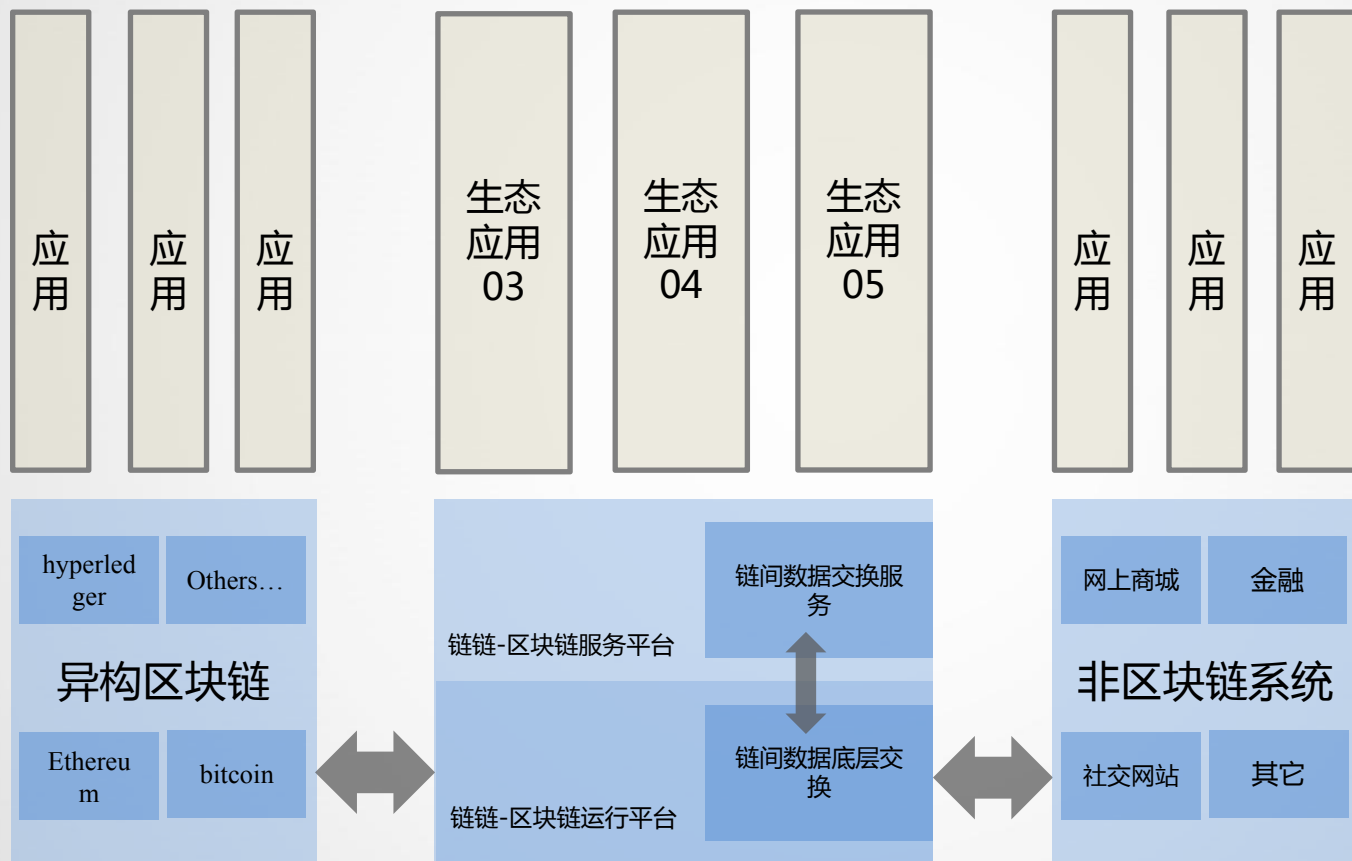


智能合约是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值

智能合约包括事务处理和保存的机制，事务及事件信息传入智能合约后，合约资源集合中状态会被更新，进而触发智能合约进行状态机判断，从而根据预设信息选择合约动作自动执行。

链链区块链-链间通信

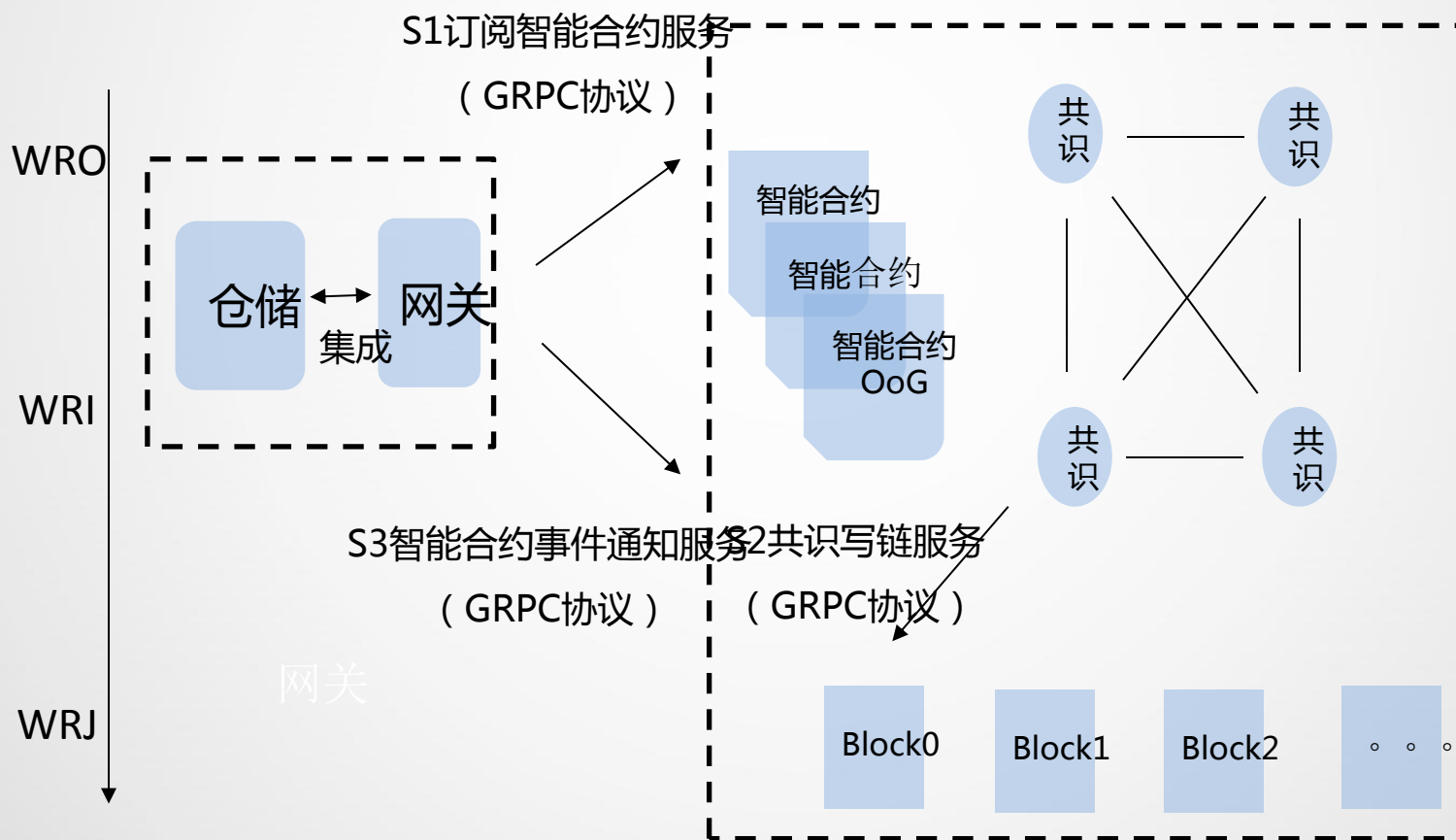
链链可以链接不同区块链系统（同构或异构）以及区块链和非区块链系统，使其可以进行一定的数据交互。



链链区块链-链间通信网关

链链使用链间通信网关与交换机技术实现链接区块链和非区块链系统。

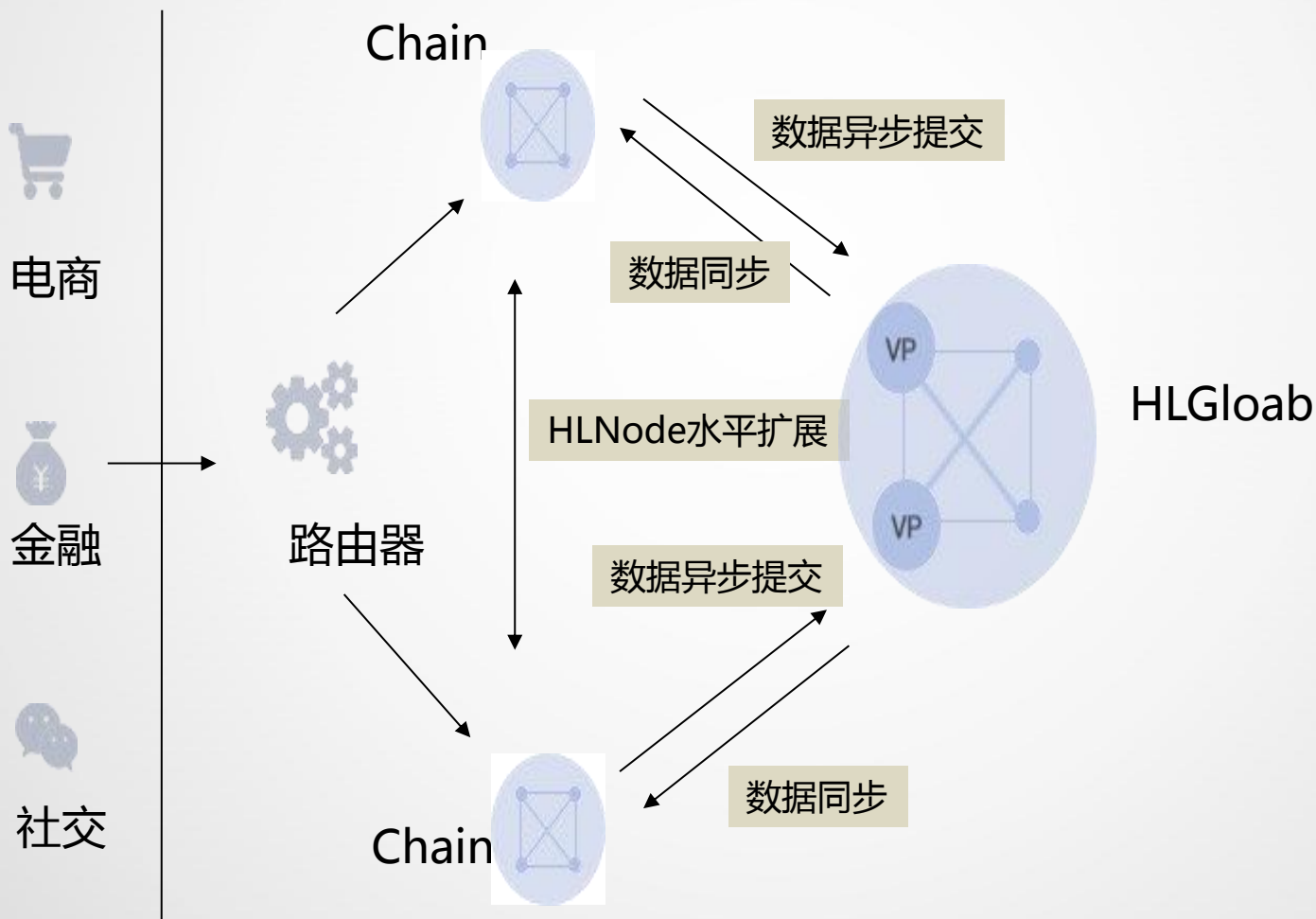
链间通信网关与交换机，链接起中心化与去中心化系统，链间通信使用标准化协议，安全可靠。



链链区块链-链间通信交换机

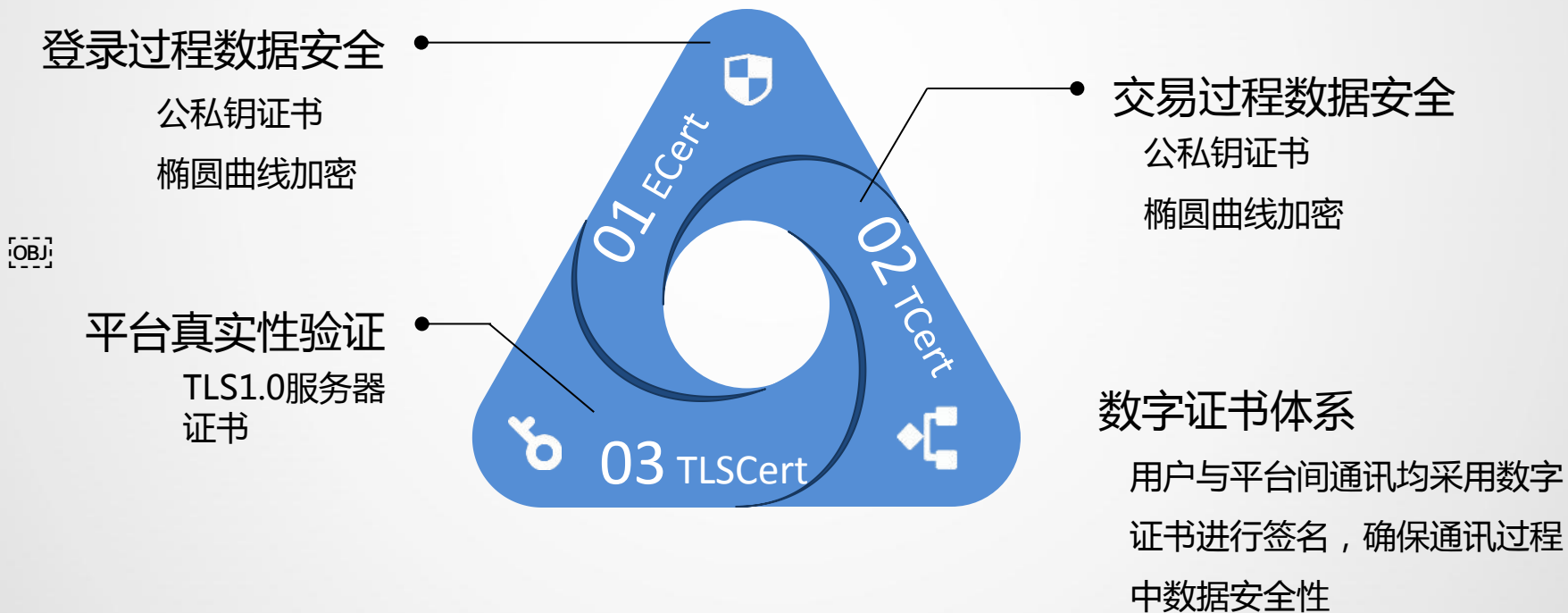
链链使用链间通信网关与交换机技术实现链接区块链和非区块链系统。

链间通信网关与交换机，链接起中心化与去中心化系统，链间通信使用标准化协议，安全可靠。



链链区块链-安全体系

使用公私钥证书以及椭圆曲线加密技术，实现登录过程、交易过程的数据安全，用户与平台间通信均采用数字证书进行签名，确保通讯过程中数据安全性。



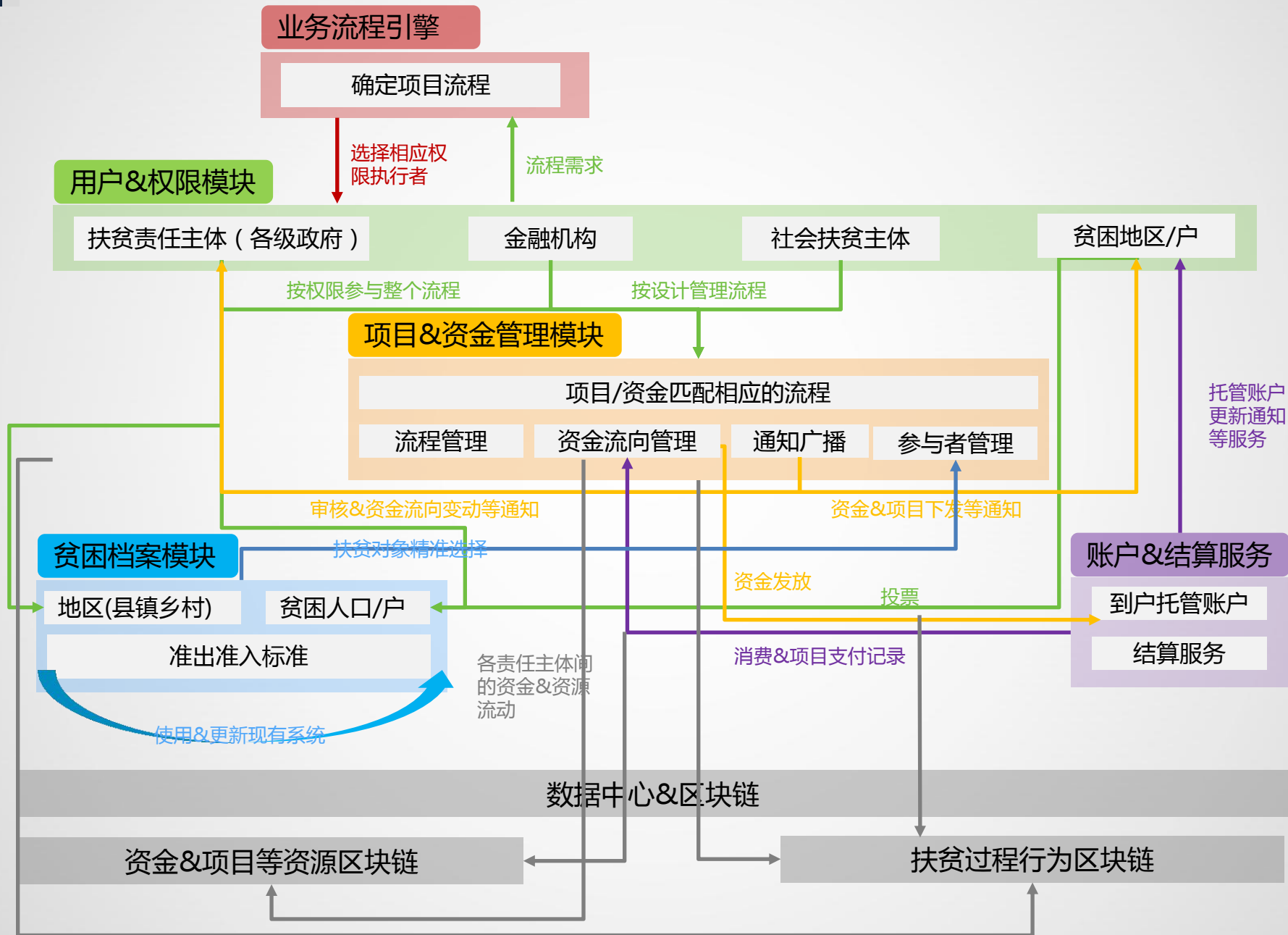
三、整体技术方案



系统框架



模块及功能



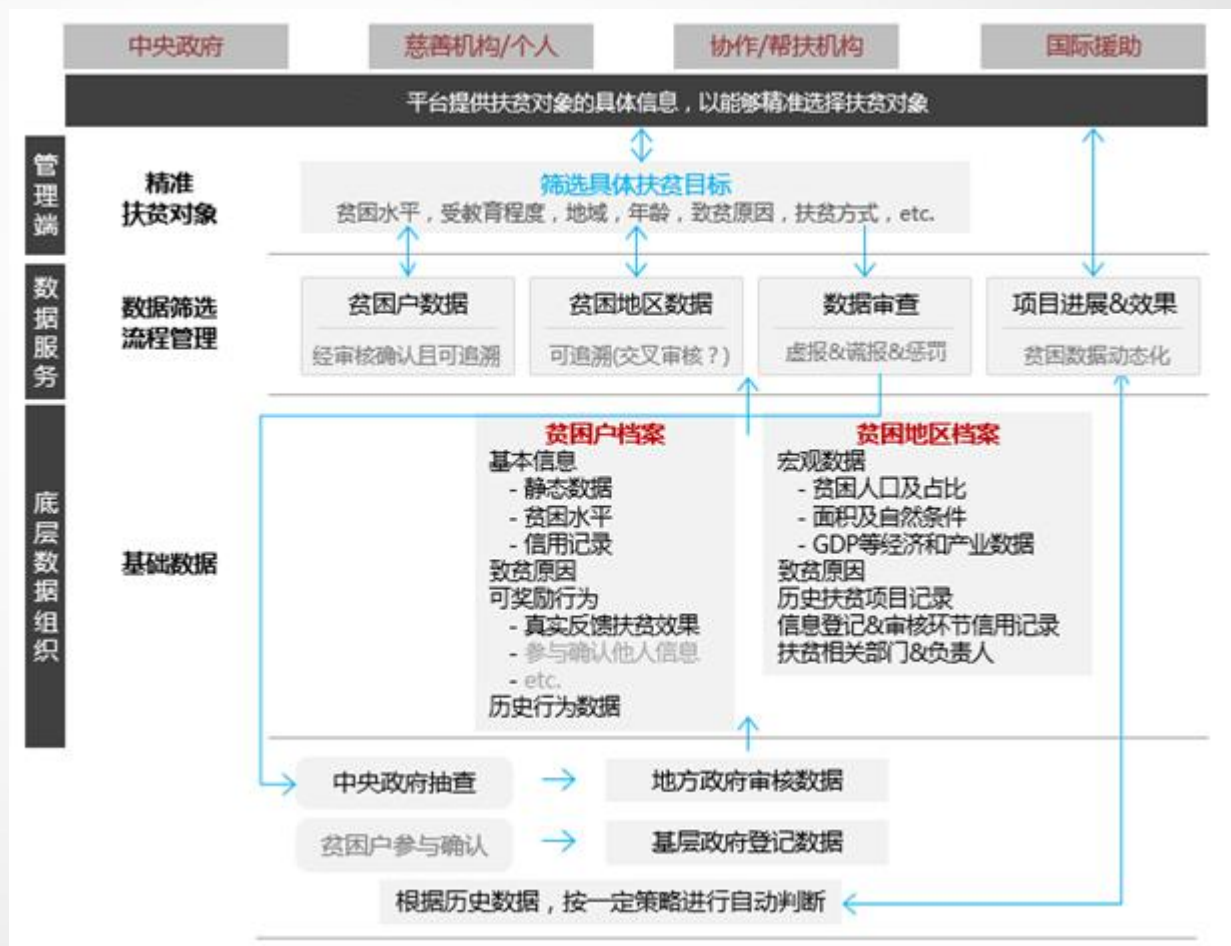
扶贫对象精准

现存问题

目前扶贫工作中，存在着大量虚报假冒现象。原因在于扶贫信息的收集、更新、维护等管理工作，都集中在了地方政府手中，即过度中心化，造成信息本身的信用度下降。

解决方案

区块链技术本身就贯穿着去中心化的思想，系统会在区块链底层技术的指导思想基础上，保留中央政府，地方政府和各权力机构等作为整个系统网络中的中心节点。



项目安排精准

现存问题

目前扶贫工作中，鉴于人力原因，一般都会有扶贫工作组，从上往下进行一层层地抽查，无法细致入微的关注每个细节，所以项目安排很难精准，必须依赖一定的技术手段。

解决方案

首先是依赖贫困人口和贫困地区的数据档案，来做项目安排初次决策时候的数据依据；然后是借助平台的广播效益，通过基础技术设备，链接项目相关人群，将信息层层传递造成熵增益的现象，用减少信息流通环节的方式，进行了一定程度的改善；最重要的是，借助项目参与者的反馈，能够为后续的决策，再提供依据，这样能够让整个扶贫流程形成一个有着丰富的正负反馈的自循环体系，并能够保持一定的中立性。



资金使用精准

现存问题

在资金使用范围层面，目前较为普遍地存在扶贫资金被挤占和挪用的情况；而在资金使用效率层面，地方政府多会选择短期见效快，回报高的项目，容易在减少贫困人口的问题上避重就轻。

解决方案

结合精准扶贫中，对资金使用的范围和效率方面的要求，系统在两个部分使用区块链技术实现，一是扶贫资源（包括扶贫资金）的去向追踪和记录上，二是对扶贫数据登记审核的流程中。



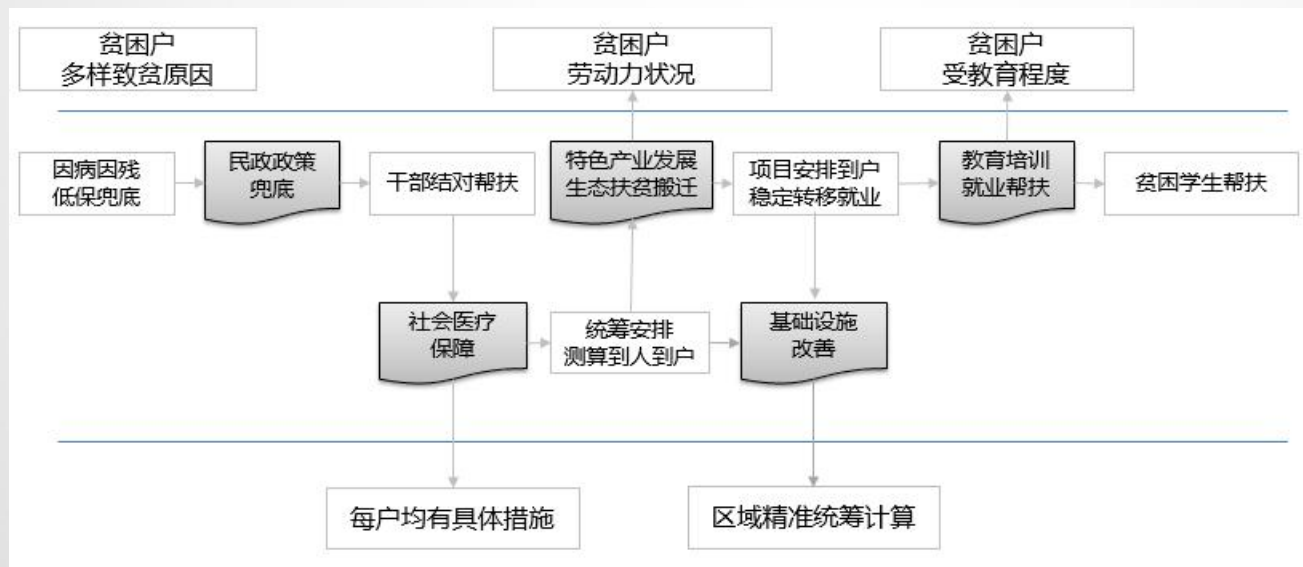
措施到户精准

现存问题

目前扶贫工作中，由于贫困户和贫困地区本身的数据档案暂时还没有建立起来，尤其对于贫困户本身的致贫原因，劳动力状况等信息，采集难度大更新困难。这就造成了，扶贫项目和计划，无法具体到每一个贫困户每一个人，无法精准的措施到户。

解决方案

系统，依赖基础数据的组织，可以为扶贫项目的措施到户，提供精准化的框架和服务。如下图所示。



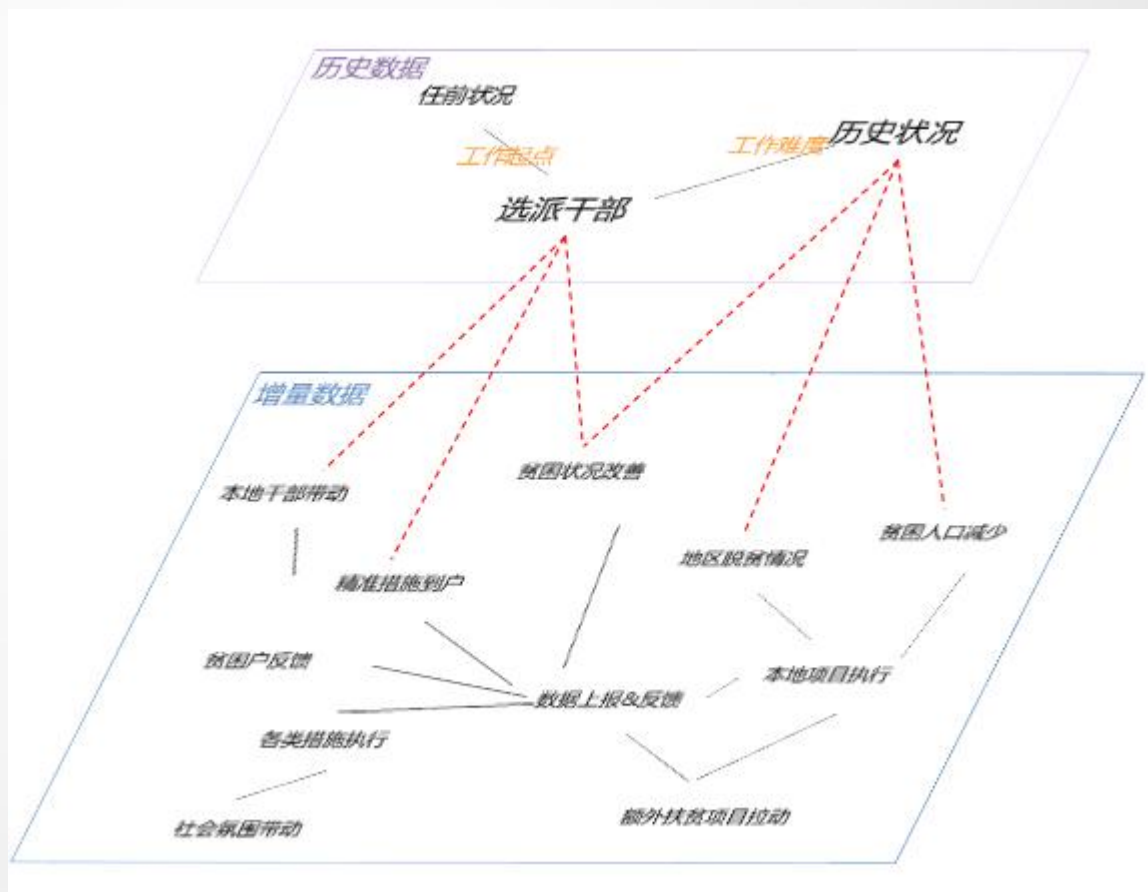
因村派人精准

现存问题

由于贫困人口较多的地区，一方面会造成外来干部较少，干部团队人员本地化严重，本地裙带关系严重，而基于贫困环境下，干部团队的平均素质不会太高。扶贫工作没有强硬有力的执行者，再合理再精准的扶贫政策和项目，也无法达到预期的效果。

解决方案

系统基于底层数据组织，可以非常容易地组织出某个扶贫干部，在任职之前的一些工作成绩，并能够通过横向对比，为其工作能力的评估提供数据参考。



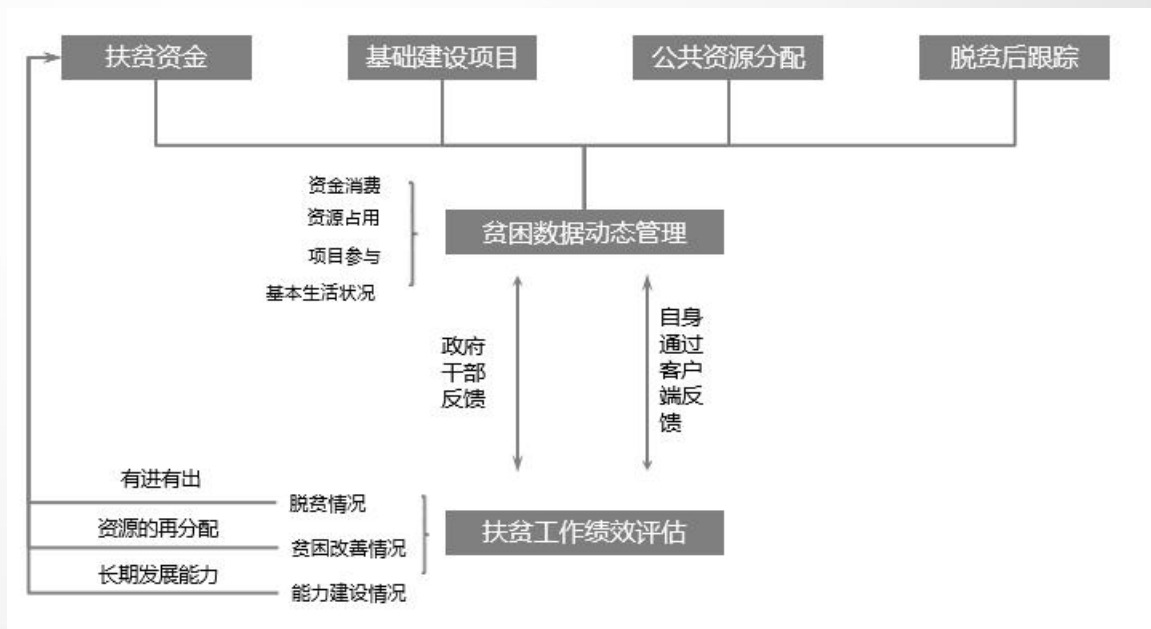
脱贫成效精准

现存问题

在当前的扶贫工作模式中，某个贫困户在采取某些措施，投入某些项目之后是否脱贫，完全是依赖基层干部的走访和提交材料来完成登记和判断。这就造成了，在脱贫结果导向压力不大时，出于对政策利好的追逐和依赖，不愿意摆脱贫困的帽子；而在脱贫结果导向压力变大时，出于行政压力，往往存在着谎报瞒报情况，让真正的贫困户“被脱贫”。

解决方案

区块链技术在本文中，会记录每个扶贫项目及每笔资金的具体流向，也会记录扶贫过程参与者的每一次行为，且一旦提交无法更改。这样就能够实现，对贫困地区、贫困户当前情况的动态管理，并能够通过横向对比判断其数据的真实性。



多谢指导！