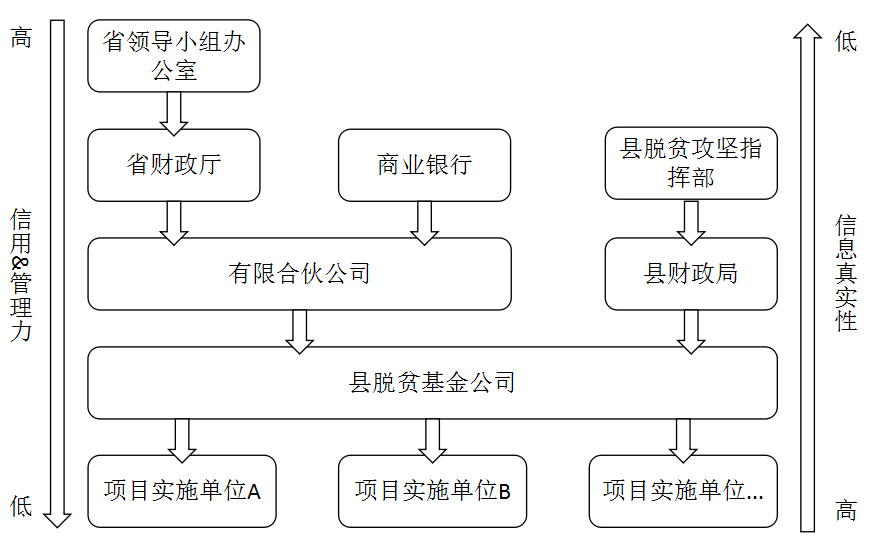
4.1 痛点分析

扶贫业务涉及的资金总体规模巨大，为了强化对资金的管理，达到提高使用效率，降低资金风险的目标，传统的做法是增加中间层级，级级加码，层层沉淀。但是，人心不古，虽然有行政层级上的上下关系，但是从每级的角度上讲，其需求是不一样的，从最高级省政府来讲，是想看到资金能更好的被利用，更多的贫困人口能够受到帮扶；往下中间层，更多的是想能不能把这笔扶贫资金留在他这里，做一些对自己有利的事情，比如弥补财政的赤字，做一些投资等；在最下层，这些钱是天上掉下来的馅饼，能不能真正用到扶贫上，另当别论。因此，虽然在行政上看是至上而下的，但是在需求上分析，是对立的。总结问题如下：

* 人为设置的信用可达性屏障
* 管理力度的急剧衰减
* 无法实时了解到扶贫转款账户变动的明细信息
* 无法及时了解到账务是否不平
* 无法保证上链信息的真实性



4.2 解决方案

4.2.1 方案介绍

为了解决以上存在的问题，创造性的提出基于区块链的解决方案，该方案分三步走。

1. 组织结构扁平化

区块链是一种新型的信息共享模式，将同一业务（生态）体系下的不同实体建立一个可追溯、可追责、低成本、可信任的系统。信息的透明，可追溯，是最高级最想看到的，同时也给下级徇私舞弊提出来警醒。而全网信息共同记录、共同检查、共同维护，体现了平等与开放，每一个参与者都是主人翁，极大的提高了下级参与者的积极性和责任意识。区块链的使用，可以消除上下层级之间约束和限制，使得组织结构扁平化，信息的传递也因此更加流畅。

1. 上下层级信用可达

在系统内，通过省政府的强信用背书发行“数字汇票”

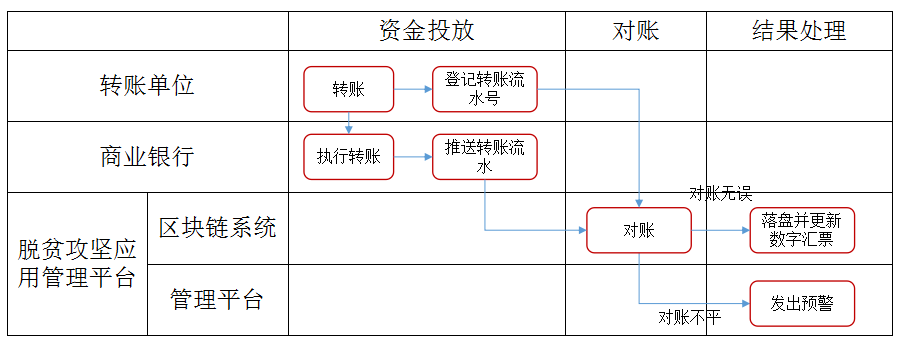
发起资金筹集计划时，参与各方核对该计划是否符合财政文件、项目合同等信息，达成共识，参与各方按照约定，进行资金的拨付和还款，由省政府强信用背书，生成“数字汇票”。

“数字汇票”实质上运行在区块链上的根据资金划拨、流转业务需求定制化的智能合约，具有如下特点：

* 发行时，约定使用条件，确定资金用途、流转路径、兑现范围等约束条件，固化资金的使用方向。
* 流通时，按照发行时约定的约束条件使用，且流通过程受参与各方共同监督。
* 承兑时，采用以链上信息为准的原则（区块链上信息更安全，更透明），当使用场景符合要求时，由对应的银行账户向受付对象发起现金转账。
* 数字汇票只在脱贫攻坚应用管理平台体系内部闭环流转。

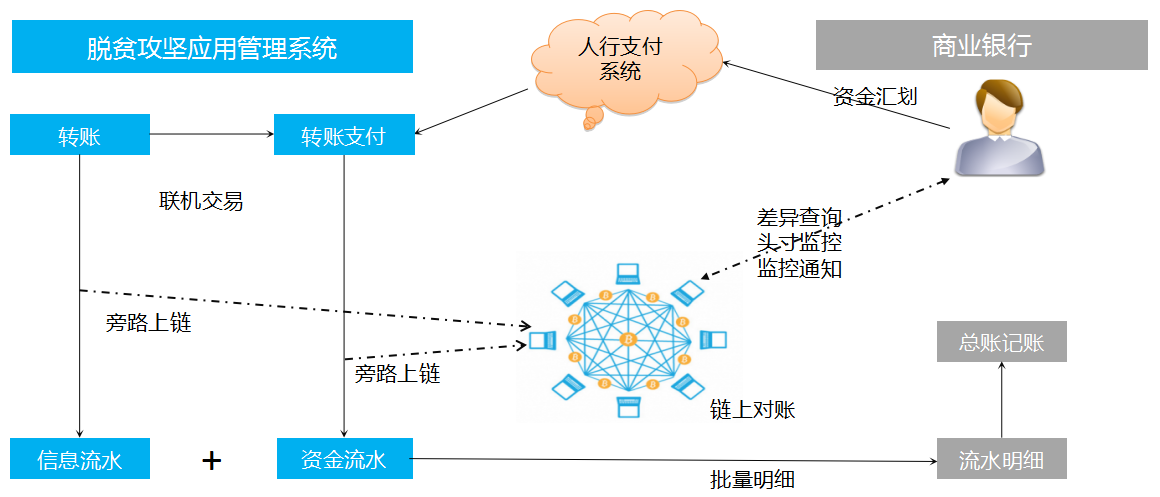
1. 实时对账

“数字汇票”就好比一部严格完善的法典，规定了方方面面。但是，如何让人们都按照他规定的去做呢？即如何保证每级部门都如实、按时得将相关款项下拨下去呢？也就是如何保证上链数据的真实性问题。比特币、以太坊等公有区块链大多采用经济制衡的手段，囚徒困境的策略，即作恶的获利要远远低于准守规则的获利。但是，这样往往会照成资源的浪费和弱一致性的达成，即还是会导致作恶，只是作恶的成本较高。结合扶贫基金业余的特点——“政府主导、企业主体、市场运作、风险可控”，即这一个在政府管制下的系统，因此，要想做好对中间环节的管控，就要充分发挥强信用单位的作用。在入口处，使用省政府的强信用对“数字汇票”的真实性进行背书。由此及彼，中间环节，使用商业银行的强信用对拨款信息的真实性进行背书。具体的做法如下：



1. 转账单位根据“数字汇票”上的信息（转账金额、拨款账户、收款账户、转账截止时间）在规定的时间内向规定的收款账户转账。转账完成后，根据银行转账回执，在基于区块链的脱贫攻坚应用管理平台上登记转账流水号，转账流水号直接发送到区块链系统的对账智能合约。
2. 商业银行执行转账，并将转账流水推送到平台，转账流水直接发送到区块链系统的对账智能合约。
3. 区块链系统的对账智能合约根据转账本门登记的转账流水号，获取商业银行推送过来的转账流水，根据“数字汇票”的信息，核对转账金额、拨款账户、收款账户、转账截止时间是否合法，如果有不合法之处，将不合法信息推送到管理平台，发出预警。如果对账无误，则落盘数据，并跟新“数字汇票”。

4.2.2 架构介绍



4.2.3 合约设计

实现功能：

* 实时流水对账，准实时发现对账差异。

触发时机：

* 每条交易流水和资金流水上报都会调用该合约的接口。

运行逻辑：

* 流水对账智能合约每收集到一条流水就会存储并执行对账逻辑(根据业务流水号、转账金额、拨款账户、收款账户、转账截止时间进行对账)，对平的流水就会实时清除，不平的流水根据发生时间判断，超过一定阈值(10分钟)，就认为是对账差异，需要进行告警和后续处理。



4.2.4 安全原则

1. 链上和链下之间的数据传输全部是加密，数据在机房会进行非对称加密，并且以https发送到区块链节点。区块链节点会进行ip白名单鉴权后，再进行解密。
2. 链上节点互相之间的数据传输全部是加密，节点间建立连接时会协商出一个加密密钥，密钥分段存放在内存。任意两个节点协商出的密钥都不相同。每次重新建立连接都会协商出一个新的密钥。
3. 链上节点数据加密存储落地，交易(区块)数据存储在本地磁盘是对称加密的，密钥存放在内存，密钥密文存储在磁盘。每次重启进程时需要拿密钥密文去密钥管理系统换回密钥明文，再进行数据解密。

4.3 总结

通过使用区块链技术，将原本自上而下的层级限制扁平化，消息指令得以通过点对点的方式传播，变单方管理为“可视化”公开管理，全程穿透，公开透明，实时监管，扫除了原来层层加码、层层沉淀所造成的信用可达性屏障，管理力度得以增强。通过“数字票据”的形式对资金进行数字化处理，两头见“钱”，中间采取“数字汇票”+智能合约的流通模式，即中间步骤“有数无钱”，开端使用省政府的强信用对“数字票据”背书，保证“数字票据”的真实性，中端使用商业银行的强信用对转账背书，保证转账上链信息的真实性，同时区块链为“数字票据”提供了安全、可信的运行流转环境。在这样一个结合了完善规章制度和先进科学技术的闭环系统中，扶贫资金得到了最大化的保障！