

区块链服务网络BSN第一次开发者大赛

编号：25

作品名称：网购隐私宝：一种基于BSN的电商平台客户信息保护方案

所属行业：电商

作者：椰风海岸小分队（成员：李双杰、徐忱、李洲、马华伟、杜铮、王亚龙）

得奖情况：三等奖

声明：本作品的版权归作者椰风海岸小分队（成员：李双杰、徐忱、李洲、马华伟、杜铮、王亚龙）所有，仅供个人学习、研究使用。未经版权方许可，任何个人或组织不得将作品或相关章节、图片用于商业用途。如需商用，请提前与版权方联系并取得版权方许可，联系方式：15901379229、15901379229@163.com。如作品涉及侵权，请与大赛主办方联系，联系方式：contest@bsnbase.com。



www.bsnbase.com



中国移动
China Mobile

网购隐私宝：

一种基于BSN的电商平台客户信息保护方案

椰风海岸小分队

中国移动设计院

2020年02月

www.10086.cn

一 背景及必要性分析

二 信息化系统改造方案

三 效益分析

- 随着线上购物的普及，越来越多的消费者选择在电商平台进行购物，网购在给人们带来各种便捷的同时，也对公民个人信息安全带来极大影响。目前，网购成个人用户隐私泄露的重灾区，因信息泄露而被电信诈骗的新闻层出不穷、各种推销广告接踵而来，在人们不胜其烦的时候，还有可能导致经济损失。而造成这一切的重要来源就是网购中个人信息的泄露，如何在网购中保护个人信息安全越来越受重视，国家和相关方加大资源投入保护个人信息安全，但面临信息泄露容易而取证困难等问题。

网购个人信息获取容易，从平台到商家各个环节均存在信息泄露的诸多漏洞

国家加大信息安全保护力度，但打击犯罪面临取证困难等问题



- 面对当前高度开放和相对透明的互联网环境，当用户在应用各类网站和APP时，需要不断地通过个人信息进行认证、授权、登录等，而所有这些信息，包括姓名、身份证号、手机号、性别、年纪、家庭住址、购物信息等集合在一起，几乎可以描绘出一个用户的完整数字画像，也正是通过这些信息，才使得用户自由但毫无保护地驰骋在互联网世界。

1 账户注册/登录

- **电商平台：**以购物、物品置换等应用为主，代表为淘宝、京东、拼多多、闲鱼等；
- **社交媒体：**用于各类社交应用，如微博、微信、QQ、Ins等。



2 身份认证/识别

- **在线交易：**发生私人财产转移的应用，如电子银行的在线转账、消费，电商平台的付费、交易；
- **政务网站：**对接公共平台资源，如个人资格认证、身份确认等。



3 系统跳转/授权

- 在面对一些非主流应用，或者在使用某些小插件、小工具时经常会遇到需要通过授权个人信息才能进行系统间跳转的情况，而个人信息就在一次次跳转中被泄露。



4 权限确定/调整

- 在提升或开通某些权限时，其等级与所提供的个人信息量是正相关的，这也意味着在调整权限过程中需要非常注意安全防护等相关内容，而这一点却常常被忽略。



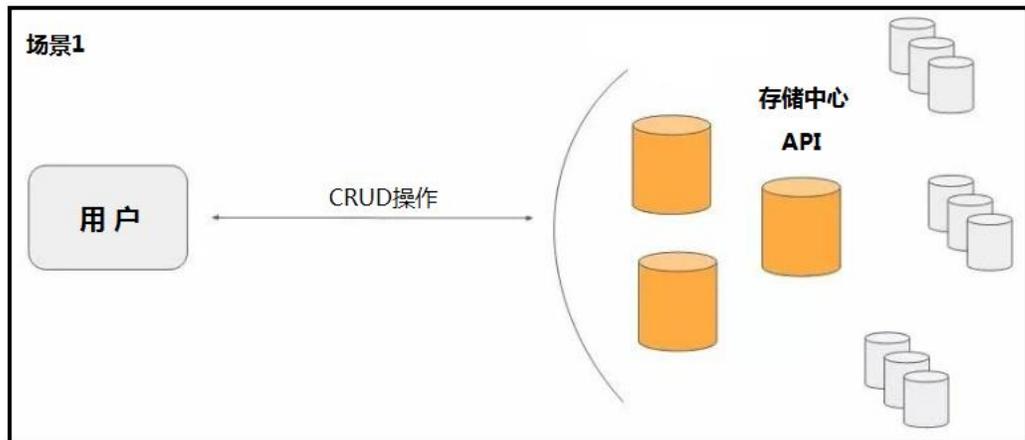
- 传统模式下，绝大多数应用都需要先进行注册，将个人信息录入其系统的数据库，作为后续认证、识别的基准。以电商平台为例，当前各大主流平台之间用户信息是相互隔离的，对于用户而言如果要查询个人交易记录必须分别登陆各个电商平台进行操作，因此对于信息流转而言，仅限于在某一个电商平台上进行信息流转，而无法进行电商间的信息流转。在一个电商内的信息流程大致分为以下几个环节：信息录入、数据调用、主体互动、信息确认、数据线上线下映射、闭环回执等。



对于当前这种系统运作的优势，包括：

- 流程简便、信息提取和使用的难度较低。各个电商平台仅需维护好自己的操作流程，在不同平台间赋予接口即可；
- 便于提高用户粘性。用户在各个电商平台间要不停重复前述各流程，往往选择对某一平台“从一而终”，降低了用户的知情权和选择权。

- 在当前这种信息流转模式下，各个电商平台仿若一座座信息孤岛一般，既重复了流程中的多个环节，又浪费了不少存储和算力资源。而用户则更是疲于应对个人信息的使用、更新和防护，随着各类应用的不断拓展，身上的负担也随之越来越重。

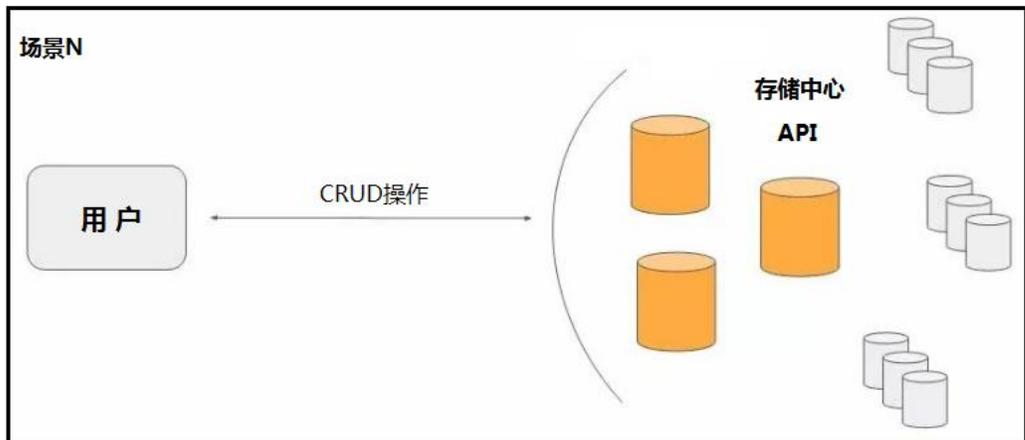


弊端1：信息繁复，资源浪费

不同平台需不断地注册、录入、更新和维护个人信息，且不同的电商平台之间还不能完全实现互通，无法仅靠简单的“一键授权”进行跳转。用户注册的登录账号越来越多，冗余信息量越来越大，而各个电商平台重复存储，造成资源浪费。

弊端2：通道闭塞，统计困难

从用户角度出发是对应多个电商平台的，但却无法实现平台间的信息叠加和交互。比如用户要按照时间查询年度消费记录，只能在不同消费账户下的不同电商平台分别进行统计后再进行汇总、统计、分析，操作十分不便捷。



弊端3：资料外泄，安全隐患

不论在那个电商平台，个人信息一旦录入均为明文显示，多种信息交织叠加（包括姓名、性别、身份证号、手机号、家庭住址等等），几乎可以描绘出一个用户的完整数字画像，而一旦这些信息被泄露（比如各种骚扰电话、销售电话、诈骗电话等），轻则对个人隐私曝光（甚至人肉），重则造成经济上的损失和精神上的打击。

- 在区块链去中心化存储的系统中，没有客户端和服务端，只有节点和对等节点，实现分布式存储。之后，将用户端和服务端端的存储数据进行上链，在这样的系统中，使用加密经济协议来保证存储系统所需的属性，并使用区块链来支撑这些协议。

优势1：信息去重，降低成本

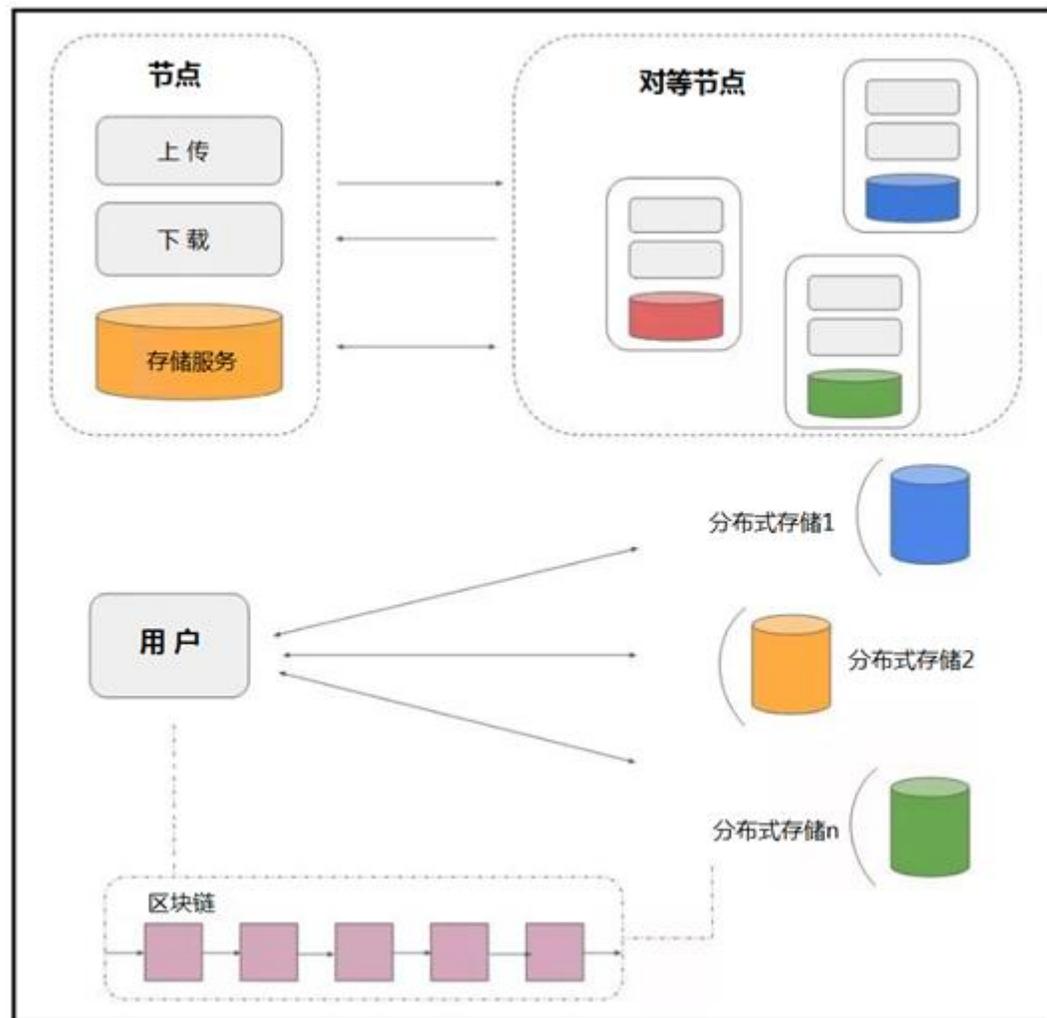
区块链技术对去除数据重复率的问题有良好的解决能力，通过数据去重能将成本降低5倍至10倍。同时，区块链存储能降低数据冗余率，从而降低成本。

优势2：节省空间，减小压力

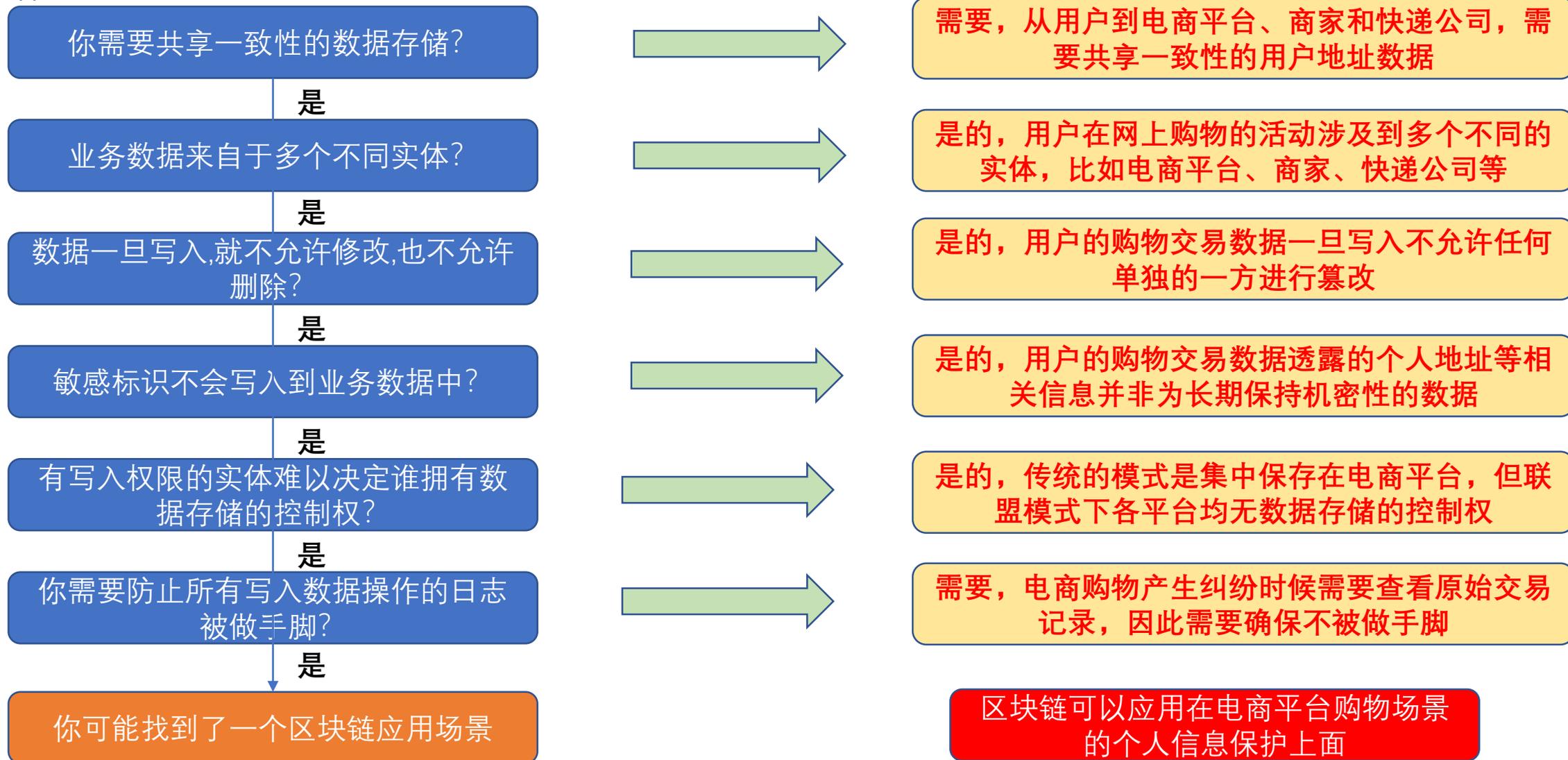
通过采用同构多链架构进行分区，并将不同的分区交给不同的节点集群来保存，这样单个节点保存的数据量就大大减小，有效降低了单节点的存储压力。此外，数据内容被分布式存储后可通过计算数据的摘要返回一个哈希序列实现唯一标识，并对该哈希序列进行上链，可大大减少上链压力和存储空间。

优势3：信息加密，安全防护

区块链存储的技术核心就在于分布式架构技术和密码学技术，用户的个人信息和各个平台上的执行过程，被加密后分成若干片，分别保存在不同节点上，读取的时候，只要把部分切片组合到一起，就能还原出整个原文件，由此保证了即便在有节点不在线的情况下，仅凭其余在线节点，也能还原出整个文件。同时，任何一个单一节点，看到的都是文件碎片，无法还原出其真实意义，保证了安全性。



- 按照美国国土安全部科学与技术理事会绘制的区块链应用场景流程图的分析结果，区块链可以用于电商平台购物场景的个人信息保护。

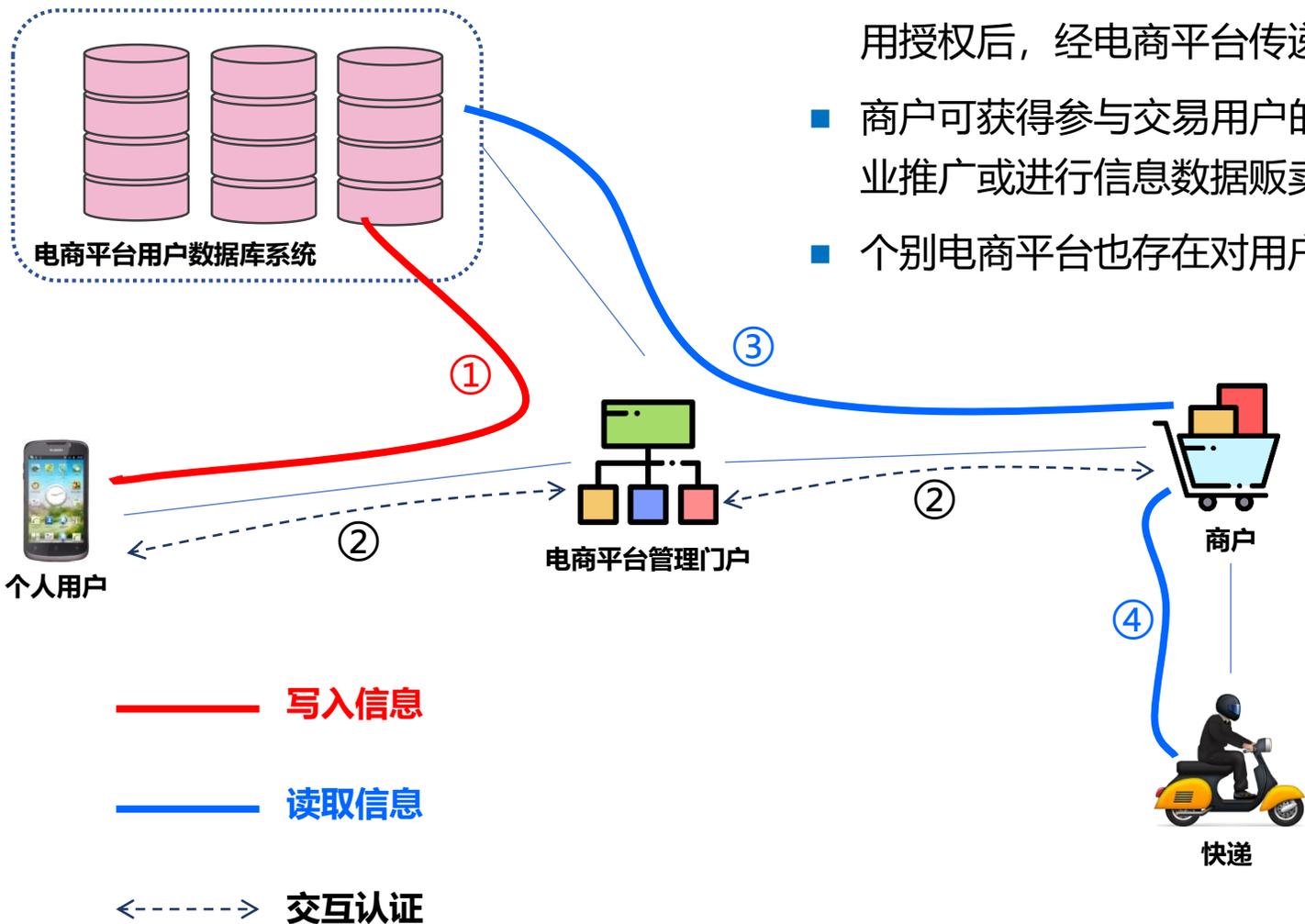


一 背景及必要性分析

二 信息化系统改造方案

三 效益分析

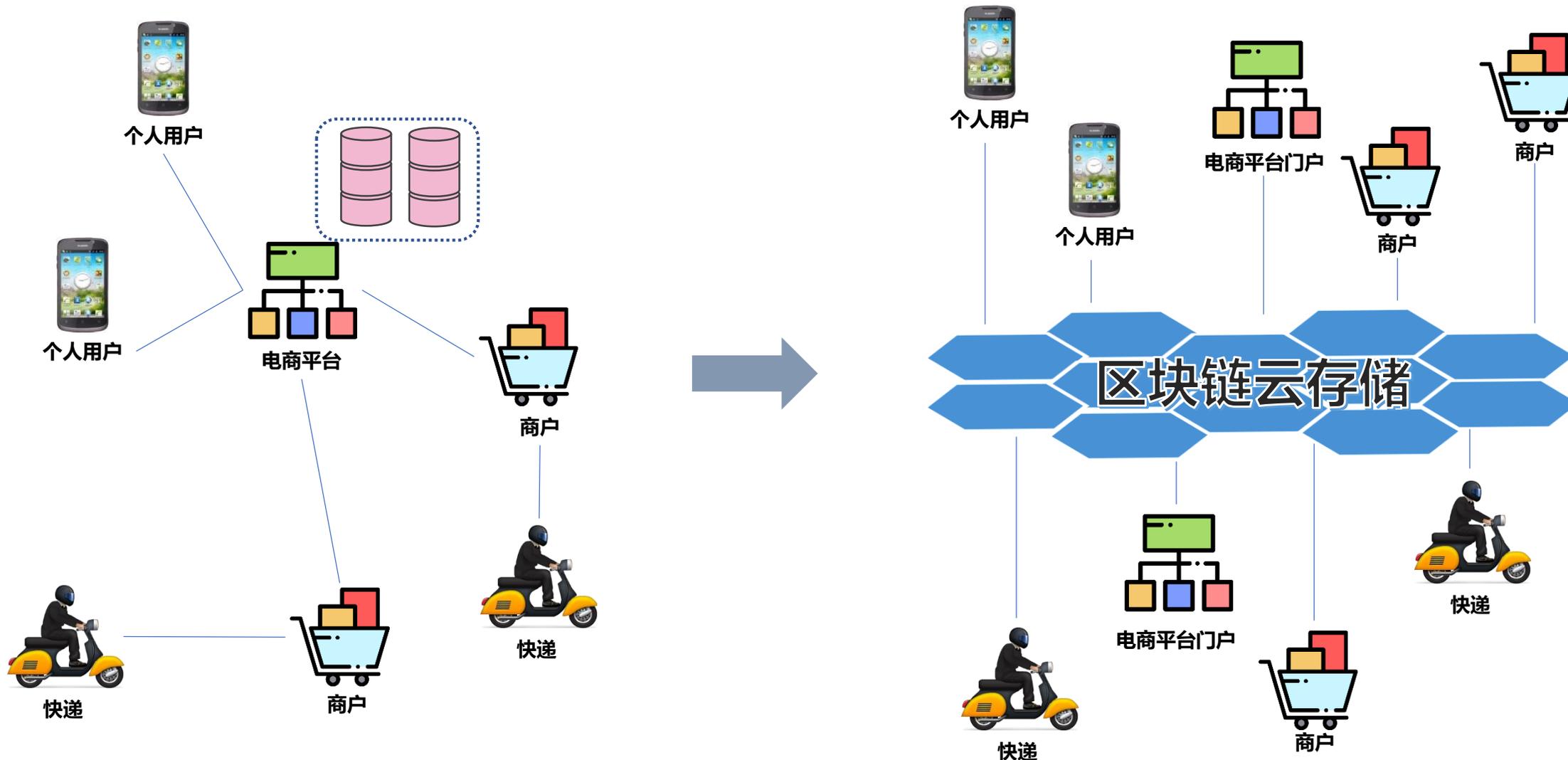
■ 现有电商平台运行模式下，用户通信地址信息的存储、读取流程



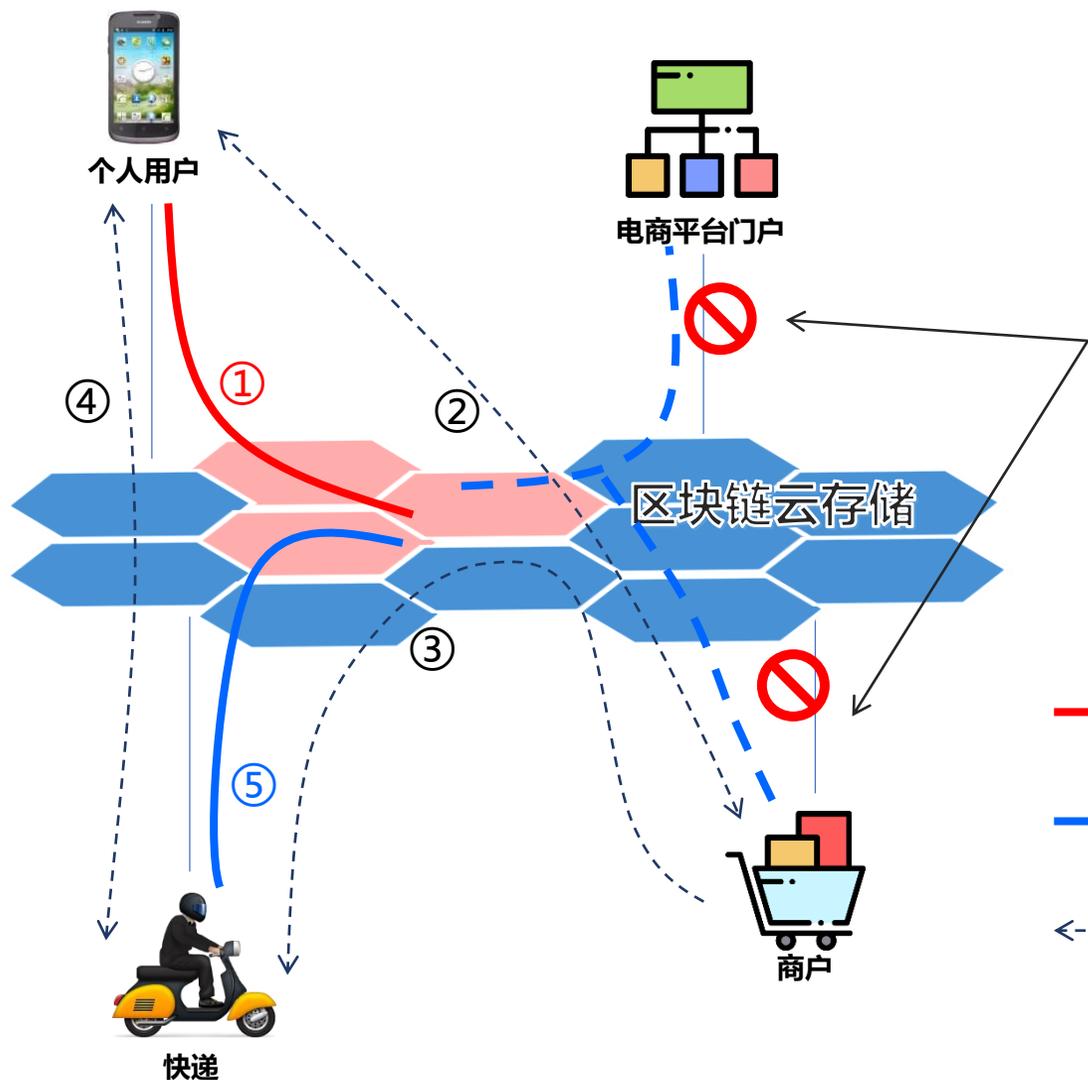
- 电商平台普遍采用中心化的数据存储方式，用户数据统一存储，在获得用户使用授权后，经电商平台传递给商户，商户启动物流流程
- 商户可获得参与交易用户的全量通信地址信息，不论是进行基于自身利益的商业推广或进行信息数据贩卖等行为均对用户造成侵害
- 个别电商平台也存在对用户信息的管理漏洞，造成用户隐私数据泄露

- ① 用户通过平台门户录入地址信息，由平台数据库统一存储
- ② 商户经平台联系用户，获取数据调用许可
- ③ 获得许可后，商户访问平台数据库获取用户指定的收货地址信息
- ④ 商户将收货地址信息发送快递公司

- 将中心化数据存储方式转换为区块链云存储方式，屏蔽信息传递中间环节，数据端到端直达



去中心化区块链云存储方式，用户通信地址信息存储、读取流程

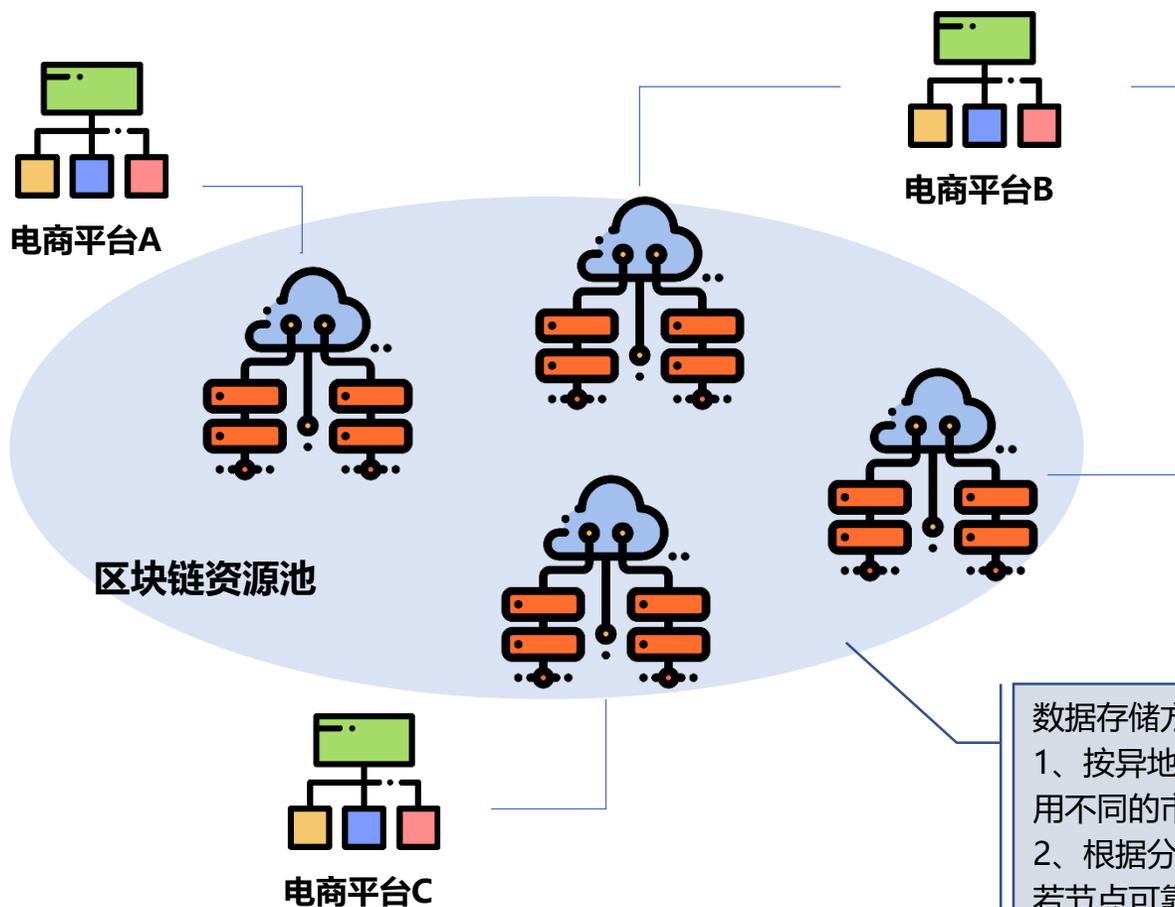


- 用户通信地址信息无需转手直达快递公司，平台和商户不能获取用户具体的通信地址，减少数据暴露机会，切断用户数据链条，保障用户隐私数据不泄露
- 根据运费计算和商用数据需求，可对平台和商户开放用户收货地址部分非涉密信息（省、市级信息），保障电商交易体系正常运转

- ① 用户通过区块链门户录入地址信息，由区块链云存储数据库存储
- ② 生成交易后，商户申请用户许可，准备进入调取用户通信地址流程
- ③ 商户向快递公司发送快递需求和用户ID信息
- ④ 快递公司向用户发送提取通信地址信息的申请并获得用户许可
- ⑤ 快递公司通过区块链云存储获取经用户授权的收货地址信息

— 写入信息
— 读取信息
← - - - - - → 交互认证

- 由参与联盟链的电商平台搭建区块链资源池硬件平台，根据联盟定义的智能合约架构体系进行数据配置和资源池运维管理

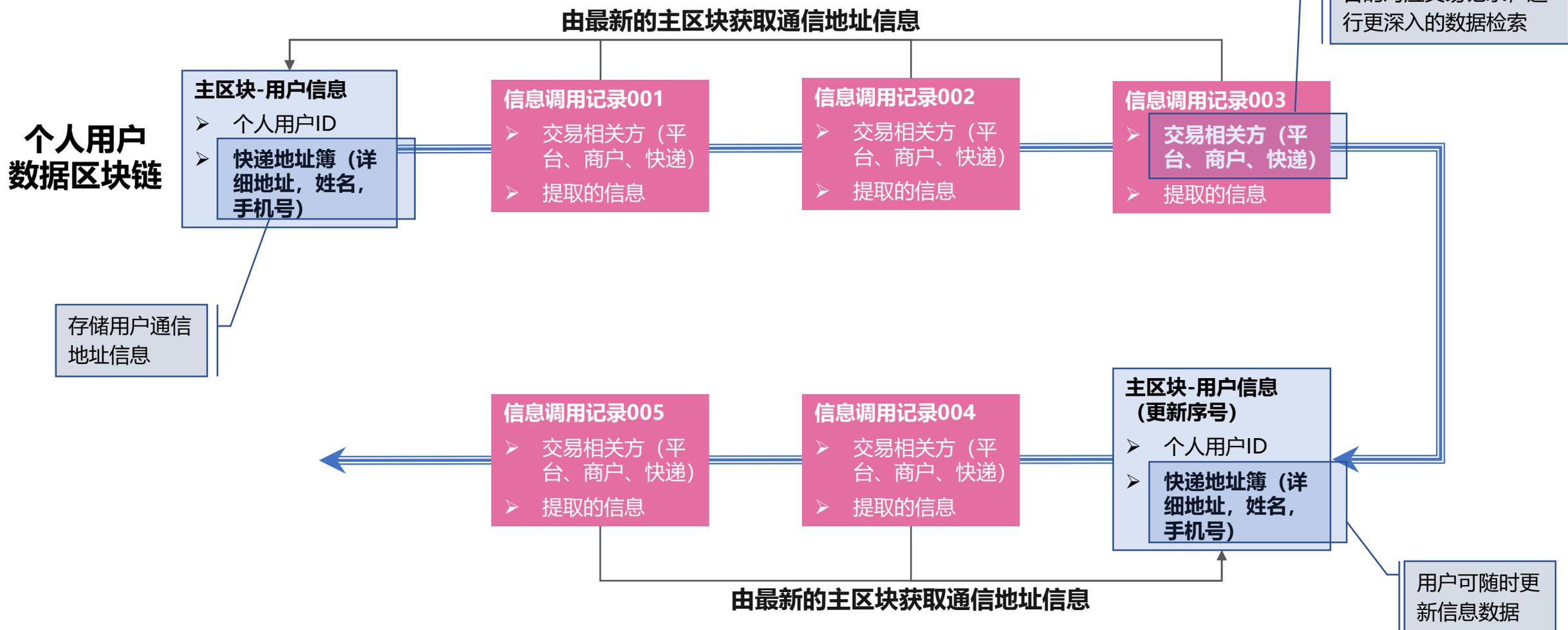


- 电商平台共同组建联盟链，并贡献硬件资源池提供云存储及计算资源
- 存储及算力资源可参考投入与收益相匹配的原则进行分摊
- 所有链内个人用户的地址簿信息均通过区块链云存储保存
- 区块链共识机制：采用电商平台轮流记账方式

数据存储方式：

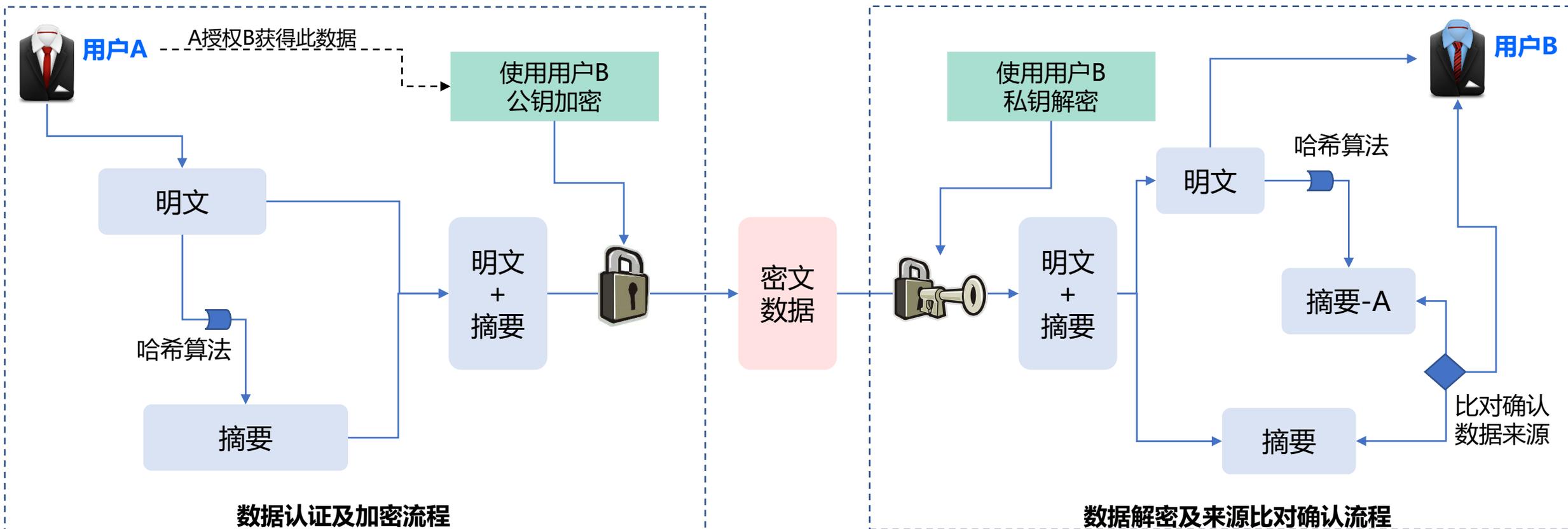
- 1、按异地容灾原则设定存储节点，节点间距大于100公里，使用不同的市电引入，物理隔离的传输管道
- 2、根据分布式存储原则，数据被拆分、加密存储于多个节点，若节点可靠性有较高的保障，建议存储在3个节点，兼顾安全性与成本

- 个人用户生成区块链数据，主区块存储用户通信地址信息，快递公司等相关方调用数据的行为被记录在区块链中；链内电商平台交易均调用此数据，减轻个人用户数据维护工作量
- 在个人数据检索等方面有丰富的可扩展性



■ 区块链云存储交互信息的来源认证和加密原理

- ✓ 各类用户对区块链云存储数据的读、写操作，以及用户之间的请求与授权，均要求进行消息数据来源认证和加密保护，确保消息真实性和安全性
- ✓ 采用非对称加密及利用哈希算法确保用户数据前后一致性的工作方式，具体消息传递流程如下：

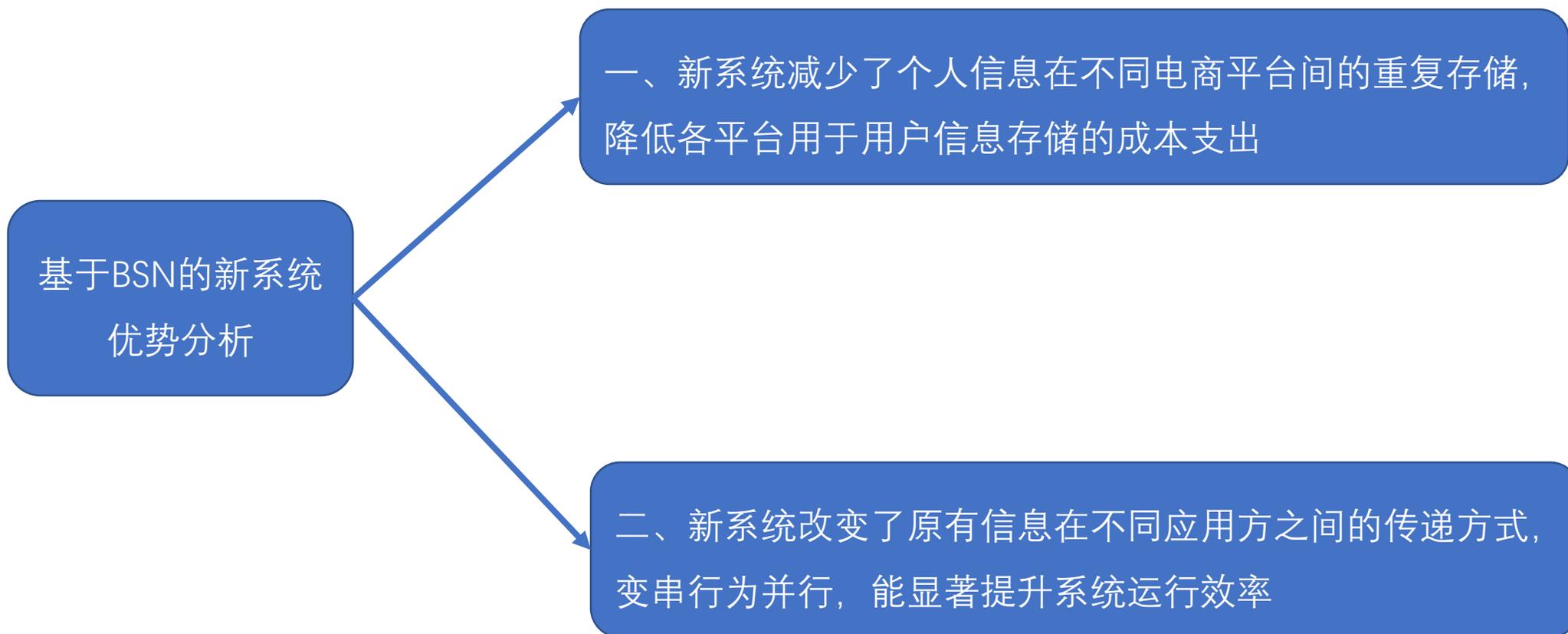


一 背景及必要性分析

二 信息化系统改造方案

三 效益分析

- 相对与传统的电商平台信息系统，基于BSN的新信息系统不仅能够实现个人信息保护，还能够减少个人信息在不同电商平台间的重复存储，降低各平台用于用户信息存储的成本支出，同时新系统改变了原有信息在不同应用方之间的传递方式，变串行为并行，能显著提升系统运行效率。



■ 区块链改造方案带来的收益：

个人用户：

- ✓ 对电商平台和商户屏蔽个人通信地址信息，保护个人隐私
- ✓ 采用统一接口的通信地址录入，简化了信息录入和修改的操作，简化个人数据维护工作

电商平台

- ✓ 电商平台仅提供通用存储及算力资源，减少数据库建设成本及维护成本，降低OPEX
- ✓ 借助分布式云存储架构优势，提升用户数据安全性

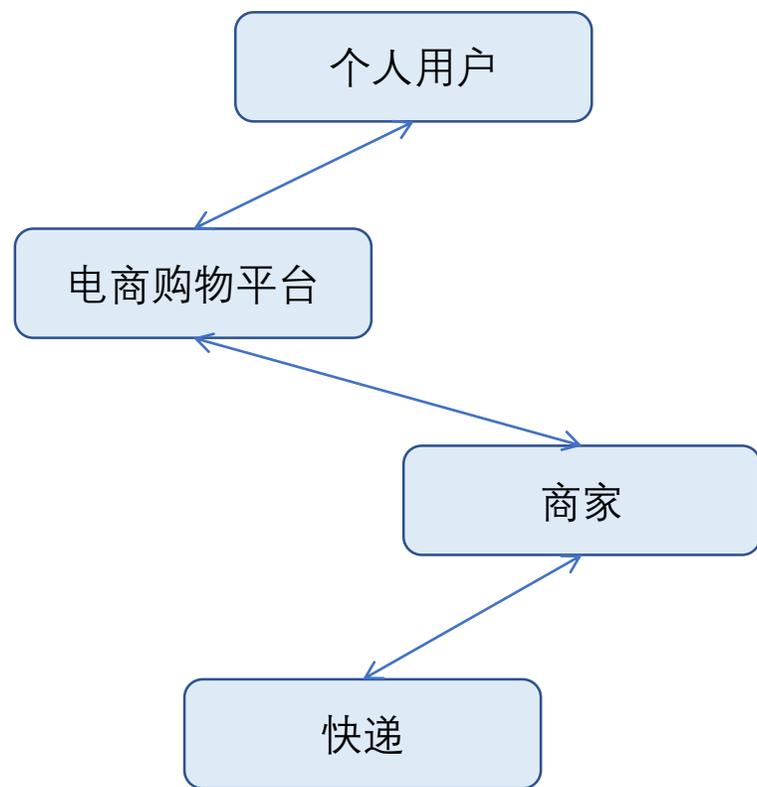
■ 基于BSN的新系统存储计算

据艾媒咨询数据统计，2019年移动电商用户规模预计达到7.13亿人，假设这些用户全部使用“网购隐私宝”，每用户基础数据量为4KB，每用户每年的购物记录100条，每条购物记录在“网购隐私宝”中存储数据量为1KB。

- ✓ 网购隐私宝用户基础数据量为 $7.13\text{亿} \times 4\text{KB} = 2.7\text{PB}$
 - ✓ 网购隐私宝每年的购物记录数据量为 $7.13\text{亿} \times 100 \times 1\text{KB} = 68\text{PB}$
 - ✓ 网购隐私宝一年数据量大约为70PB
- ## ■ 区块链云存储与电商平台自有数据库存储方式的资源需求对比
- ✓ 目前电商平台用户注册数据存储量对于电商平台存储系统来说占比很小。
 - ✓ 但随着加入区块链云存储的电商平台数量越多，云存储相对于传统存储方式的硬件资源需求优势越明显

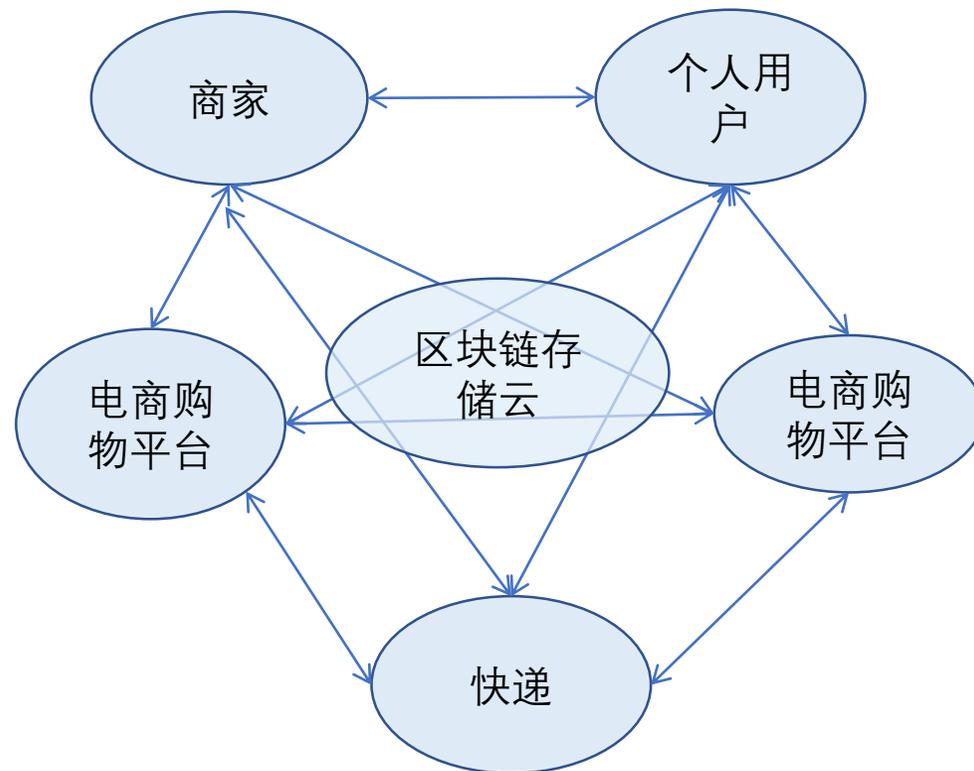
- 基于BSN的新系统改变了原有信息在不同应用方之间的传递方式，变串行为并行，能显著提升系统运行效率。

传统电商平台系统信息传递流程（串联，相互独立）



信息中转，效率低、安全性差

基于BSN的新信息系统传递流程（并联，相互连接）



信息直达，效率高、安全性强

- 1、提升运行效率
- 2、减少运维成本
- 3、防止数据造假
- 4、便于数据获取
- 5、提升容错能力
- 6、加强信息保护



中国移动
China Mobile

谢谢!

www.10086.cn