



---

## 目录

一、区块链发展现状.....	4
二、UDO 定位和目标.....	5
2.1 UDO 区块链服务.....	5
2.2 UDO 设计原则和目标.....	5
三、技术优势与系统安全.....	6
3.1 产品技术优势.....	6
3.1.1 高可用.....	7
3.1.2 灵活部署.....	7
3.1.3 快速接入.....	7
3.1.4 自适应 UPOS 共识算法.....	7
3.1.5 海量高速存储.....	8
3.1.6 跨链交易.....	9
3.2 UDO 系统安全.....	9
3.3 快速创建业务.....	13
3.3.1 创建区块链网络.....	13
3.3.2 创建智能合约.....	13
四、UDO 技术架构.....	15
五、UDO 应用场景.....	19
5.1 商品溯源.....	19
5.2 供应链金融.....	20
5.3 电子发票系统.....	21

---

5.4 旅游场景.....	22
5.5 精准扶贫.....	26
5.6 租房领域.....	28
5.7 区块链可信数据共享方案.....	30
5.7.1 医疗信息共享.....	32
5.7.2 农村金融信息共享.....	34
5.8 区块链在政务领域的应用.....	35

---

## 一、区块链发展现状

区块链是一种共享账本技术, 实质是由多方参与共同维护一个持续增长的分布式数据库, 也被称为分布式共享账本(Distributed Shared Ledger), 其核心在于通过分布式网络、时序不可篡改的密码学账本及分布式共识机制建立彼此之间的信任关系, 利用由自动化脚本代码组成的智能合约来编程和操作数据, 最终实现由信息互联向价值互联的进化。

最早关于区块链的描述出现在 2008 年由 Nakamoto 所撰写《Bitcoin: A peerto-peer electronic cash system》中, 重点讨论了比特币系统, 区块链被描述为用于记录比特币交易的账目历史。在比特币系统成功运行多年后, 部分金融机构开始意识到, 作为比特币运行的底层支撑技术—区块链—实际上是一种极其巧妙的分布式共享账本技术, 对金融乃至各行各业带来的潜在影响甚至可能不亚于复式记账法的发明。2014 年前后, 业界开始认识到区块链技术的重要价值, 并通过智能合约技术将其用于数字货币外的分布式应用领域; 2015 年,《经济学人》(Economist)杂志在封面介绍区块链为创造信任的机器, 即区块链可以在没有中央权威机构的情况下, 实现在分布式商业网络里多方参与的双边交易中的去中介化。

当前全球区块链产业生态发展迅猛, 产业链层次逐渐清晰, 无论从底层基础架构和平台, 还是细分产业板块的区块链应用, 以及风险资本投资都已初具规模。区块链技术的分散式存储、信息公开透明、不可篡改、强安全性、可追溯等特点,

---

可以完美解决共享经济发展过程中出现的信息不对称、交易成本高等诸多难题。

区块链技术可以重构信用机制，在全球范围内改变商业模式和交易规则。

## **二、UDO 定位和目标**

### **2.1 UDO 区块链服务**

UDO 构建了自主知识产权的区块链应用体系，研发了具有高安全、高性能、高扩展的区块链基础服务平台，秉持“自主创新、开放分享”的理念，为各领域的区块链应用提供全方位的解决方案，帮助客户在 UDO 上快速、高效的搭建企业级区块链行业应用，减少客户在区块链部署、运维、管理、应用开发等方面的挑战，实现业务快速上链，最终推动区块链应用场景落地，打造基于区块链的商业生态圈。

UDO 能够针对特定的业务需求，将区块链与传统 IT 技术、物联网、大数据、云计算、人工智能等进行融合，UDO 目前已取得多项技术突破和创新，在性能、扩展性、安全和运维等方面形成一系列技术特色和优势。UDO 的应用场景已服务于金融、税务发票、电子病历、电子商务、公益等领域；在房产租赁、旅游服务、现代农业、数字版权、数据安全等多个领域也积累了丰富的技术经验。未来，UDO 将搭建一个更为开放安全的区块链基础设施，与企业共享，打造通用型数字化开放平台，构建新一代价值流通网络。

### **2.2 UDO 设计原则和目标**

---

## 设计原则——

**合作、开放、共享：**UDO 专注于区块链底层技术和平台服务能力搭建，开放内部服务能力，与行业伙伴合作共享，打造一个标准统一、可行性强的区块链应用生态圈，推进区块链场景落地，帮助客户实现商业目标。

**简单普适：**在开源组件基础上部署企业级分布式区块链系统并非易事，UDO 在注重自主创新的同时，也注重区块链商业场景落地的可行性、可操作性。UDO 自主创新 UPOS 共识机制，拥有高性能主网及模块化的特性，让企业不必配置专业的区块链开发团队，就能快速高效地设计和部署自己的区块链网络，帮助企业实现自动化配置、部署商用级区块链应用，这将极大程度改变区块链落地的进程。此外，UDO 提供区块链服务全流程托管，让客户简单使用区块链系统，专注于上层应用的创新和开发。

## 设计目标——

UDO 旨在用区块链技术推动行业的创新成长，为企业提供区块链基础设施、一站式行业解决方案和安全、实用的区块链服务，让企业在 UDO 上快速搭建基于自身业务的高安全、高性能的区块链系统，通过可视化的管理，提高企业使用区块链的效率，有效降低运营成本。

## 三、技术优势与系统安全

### 3.1 产品技术优势

---

根据“合作、共享、简单普适”的设计原则，UDO 打造的商用级区块链基础设施具备以下几方面的技术特色和优势：

### 3.1.1 高可用

UDO 全链路实现高可用设计，包括区块链节点、服务管控等，确保业务连续性。

此外，UDO 节点弹性能力和节点故障自动恢复能力强，从架构上保障了区块链系统的高可用。

### 3.1.2 灵活部署

UDO 实现底层链的部署方式，可以根据客户需求部署在不同的区块链节点，参与共识的节点在不同的区块链中运行，既实现应用系统相互隔离又最大程度实现区块链的去中心化或多中心化，满足不同企业和用户对区块链系统的部署要求。

### 3.1.3 快速接入

UDO 在用户业务开发方式、部署方式上做了大量的兼容性设计，实现各种场景、各种开发习惯的用户以较低的代价、较快的速度对接到区块链上来，满足多种用户习惯的接入方式。UDO 提供丰富的应用开发框架，用户可以基于这些应用开发框架进行业务开发，也可以直接基于 UDO 底层进行开发，UDO 基于客户业务进行全程设计和服务。

### 3.1.4 自适应 UPOS 共识算法

UDO 基于自主创新的共识机制 UPOS，为应用开发者提供可持续创造区块链的开发平台。UDO 平台拥有模块化结构，可支持 POS、DPOS、PBFT 等多种共

---

识算法，在分析各共识机制的协议性能和资源使用的基础上，对共识过程中的协议进行了针对性的改进，形成新的自适应共识机制 UPOS。

UPOS 为高性能区块链设计灵活的底层结构，支撑去中心化应用的巨量增长，采用 MAB 的机制及抢夺释放的机制，保证了更强的公平性。UPOS 设计足够的激励让节点升级硬件，并采用固定顺序节点产块，提升网络性能，块与块之间间隔是固定的，这样创建了一个兼具高吞吐量和更佳稳定的区块链网络，最终能支持高性能业务运行。

高效自适应的 UPOS 共识算法，保证了共识完成即交易确认，并且对交易确认过程中的其他环节，如签名算法、账本存储方式等进行了优化，实现了秒级确认交易。此外，UPOS 引入了信用评价，配合简化的一致性协议促进系统进入良性循环；修改检查点协议，使节点能动态的加入、离开系统，提高系统灵活性。

### 3.1.5 海量高速存储

UDO 采用主侧链存储策略，主链存储关键数据，侧链存储查询数据，侧链出现任何安全问题不会影响到主链，这样能有效的降低主链负担，提高主链的扩展能力，降低升级带来的系统性风险。

此外，UDO 结合以太坊平台的特征，构建一种基于智能合约的可信存证机制，主要包括集中化数据统一处理、认证数据分布式存储与高效动态取证等内容，以实现电子数据在以太坊上的存证交易与还原验证，保证数据的真实唯一、可溯源



---

与防篡改。

### 3.1.6 跨链交易

UDO 采用链路由的形式实现区块链的分片，提高区块链系统的交易处理能力。相较于一条单独的区块链系统，链路由系统可以通过连接多条子链的方式大幅度提升交易处理能力。交易的请求通过链路由的分配进入不同子链，可以有效规避针对一条子链的集中请求，此外，在链路由上部署同构子链的不同节点数的集群，对于同构链而言，多节点数量的集群会有相对较高的安全性，少节点集群的处理速度则更快。UDO 根据节点数量，地理位置，业务分类等不同需求，部署不同的链路由集群，根据路由规则，将不同需求分发到合适的集群之中处理，为用户提供更高质量的区块链服务。

### 3.1.7 通用型区块链数据库

UDO 设计出完整性的区块链数据库方案，从商业化的角度解决了传统数据库上链的问题，对数据库编程开发者友好兼容，让大量的生态开发者快速转移至新的分布式数据库上。在成本上远远低于传统的 RDS、NOSQL 等数据库，帮助更多的开发者减少巨大的成本。

## 3.2 UDO 系统安全

### 身份认证（零身份自治）

UDO 对区块链行业贡献公用的区块链零身份证明，包括个人、组织、AI、设备等，基于 IPFS，通过智能合约部署全球共享的去中心化自治的区块链零身份数

---

据库,能够查询到任何一个区块链身份在 UDO 生态里的一切活动。只要在 UDO 平台通过自治手段注册到指定智能合约,就可与其它任何智能合约交互的用户共享有效身份信息并直接进入(钱包提供自动登陆功能)和使用其它一切区块链 Dapp,而不需要再注册和手动登陆。

与其它区块链身份认证相比,零身份源于去中心化自治原则,完全由用户自主决定如何进行管理。它能够与智能合约交互,赋予智能合约在应用时的高度安全性;能最大程度地保护用户的匿名性,使区块链数据不再关联隐私属性而可以完全公开透明,从而大大提高区块链智能合约应用的安全可靠性,极大地保护用户的资产和社交资源,有效防范智能合约欺诈以及不良黑客作恶,提升区块链的应用效率。

## 交易保密、安全

UDO 基于零知识证明的隐私保护机制,即“私钥、公钥、地址”三位一体构成身份匿名,以确保用户身份完全被用户自己所掌控,提升交易的保密性和安全性。

公用的区块链零身份自治框架符合比特币对于隐私隔离的设计,通过钱包等媒介,可以直接和智能合约交互,一个钱包能完成任何应用或智能合约的支付请求,通过去中心化自治明文协议的交互,配合它们对应的各种数据库,协助记录任何一个区块链身份在区块链生态里的一切活动。让智能合约可以以去中心化自治的模式保护、证明和管理用户的零身份及其区块链资产,使得用户的身份及其区块链资产能够远离任何人为的操控与侵犯。

---

UDO 中用户信息和区块链地址是隔离的，从各节点的记录存储中，无法获取到相关联的用户信息。对交易保密程度较高的用户可以选择交易不相关性机制，同一个用户的每次交易都映射到区块链上不同的地址上，从而保证了在交易账本上无法获取一个用户的多笔交易的关联性。

## 数据隐私及安全

UDO 引入了 sideDB 机制，通过 Hash 处理和私有数据结构，在通道内部实现了更细粒度的隐私保护。Hash 后的交易内容仍然会发送到排序节点，并提交到公共的数据库和账本结构中。而授权组的 Peer 节点则在本地维护私有的状态数据库和区块链结构，保存交易的明文内容。这就保证了通道内其他节点无法看到授权组的交易内容。

UDO 用户可以选择明文数据上链，也可以对称加密的方式对上链数据进行加密。同时支持隐私分享模型，即将加密密钥通过另一把私密密钥加密，加密后的明文和加密后的密钥上链保存。私密密钥通过非对称密钥导出函数进行管理，提供服务化可编程接口，业务参与方根据各自不同的业务范围和分享范围获得不同的解密业务数据的密钥。

## 记录不可篡改

UDO 通过非对称加密的数字签名保证业务请求在传输过程中不能被篡改，通过共识机制保证各节点数据一致的存储。对于已经存储的数据记录通过节点内的自校验性和准实时多节点数据校验来保证已经存储的数据记录不能被修改。

---

## 节点的自校验性

UDO 每个记账节点都有自己的私钥，每个区块头中包含了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。当节点的私钥被盗取时，UDO 提供多节点间准实时的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。

## 网络安全保障

多个独立的区块链节点部署在 VPC 网络中，保证用户的区块链节点运行在安全的网络环境。

UDO 应用比其他散列函数更安全的 SHA-3Keccak，Keccak 使用随机排列结果的海绵结构，给定(若干)哈希值，在有限时间内能计算出哈希值并很难(基本不可能)逆推出原始消息，很难找到两段内容不同的消息，使得它们的哈希值一致(发生冲突)。

面向区块链的安全需求，基于传统的数字签名机制，UDO 使用了可以保障所有者的信息不可伪造和交易人信息不可否认的交互式数字签名协议 IIS(Interactive Incontestable Signature)，该签名技术生成签名的过程是一个交易者和所有者两个部分间的交互证明过程；签名的认证同时要求双方提供公钥，这意味着此签名获得了双方的认可；每个区块中的证明是唯一的，并且在该区块中的所有事务中共享，这在所有事务和该区块之间建立了强大的成员关系。

---

## 合规安全

完善的用户、密钥、权限管理及隔离处理，既保障数据、账户信息安全，又满足实时穿透的合规监管。

## 3.3 快速创建业务

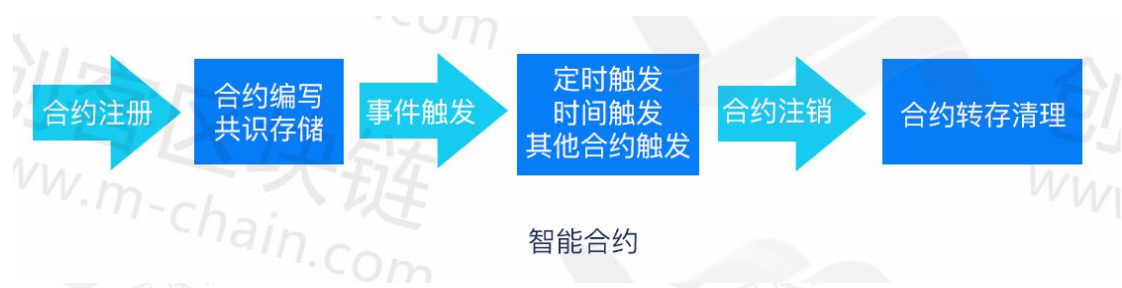
### 3.3.1 创建区块链网络

UDO 区块链服务提供了快速模式，企业和用户无需精通区块链底层技术细节，只需根据 UDO 官网提供的操作指南，填写必要的信息，即可完成创建链等操作，实现企业级商用区块链服务的部署和运行，快速获得完整的商用级区块链网络。这大大降低了区块链的使用门槛，有利于企业快速开展区块链业务创新。

### 3.3.2 创建智能合约

UDO 基于区块链底层技术，同时兼容支持以太坊（Solidity）和 EOS（WebAssembly）类型的智能合约，提供标准化可编程的合约开发和升级，通过智能合约构建出可执行商业逻辑的区块链应用，实现对应区块链应用的落地，助力快速部署智能合约，更加便捷地开发基于区块链的应用。

智能合约包括合约的注册、触发、注销三个部分：



**智能合约注册** 合约注册是将用户编写好的合约安全检查处理之后，共识存储到区块链的过程。链代码首先需上传安装在 Peer 节点上，然后在通道上进行实例化，实例化的过程需要参与方进行共识，智能合约实例化过程将被记录到区块链中，实例化后，链代码将在 Docker 容器中运行。UDO 合约部分包括标准合约以及业务定制的合约两种类型。标准合约是 UDO 内置合约，可以自动撮合成交、多方确认转账、到期自动清算；定制的智能合约包括通过合约模板修改配置和添加其他业务逻辑的形式，也可以支持更加复杂的用户自编程的合约，在独立的环境里运行。

**智能合约触发** 合约触发是在合约注册之后，通过外部条件来触发合约执行的过程，支持定时触发、事件触发、交易触发和其他合约触发的方式。定时触发是指满足合约中预设的时间之后，节点就触发时间共识之后，自动触发合约调用的过程。事件、交易和其他合约调用都是一次新的请求共识过程中触发合约执行。

**智能合约注销** 合约注销，是对已经执行过、过期作废或者业务需求变更不再需要的合约进行转存，清理，清理的过程需要多节点共识之后才能完成。



## 四、UDO 技术架构

分层划分功能，是解构复杂系统的有效手段。在各层内部，再按照“高内聚、低耦合”的原则，划分各个组件，从而形成相应的技术架构。根据这样的技术方法，UDO 把整体技术架构分为六大层次：



(UDO 六层架构)

**应用层**：区块浏览器、开发者平台、去中心化钱包、Dapps 等

**区块浏览器**：区块链浏览器是普通用户浏览区块链信息的主要窗口，UDO 区块

---

链浏览器可查询区块上的出块时间、出块高度等整条区块链基础信息；区块详情查询；区块上的交易记录查询（地址、资金动向）；区块上的合约执行情况查询。除了基本的区块数据、交易数据外，UDO 还将允许用户查看更多种类的聚合数据，通过图表洞察 UDO 社区的动向，从而能为 UDO 相关的产品设计、价值投资收集第一手的参考数据，同时地址和个人信息不挂钩，保证用户的个人隐私。

**开发者平台：**UDO 平台提供了一种使用开源框架快速便捷地创建和部署安全区块链网络的方法，允许用户构建和关联自己的区块链分布式应用程序 (DApps)，不用花费时间和精力设置区块链网络。同时开发者可以申请成为 UDO 链的节点，申请节点需通过平台管理员的审核，节点申请通过之后，开发者即可在其自有节点上发布智能合约。

**去中心化钱包：**UDO 平台内置支持去中心化钱包，如跨链钱包 MyBitt。MyBitt 基于区块链浏览器，为用户提供安全、高效的移动轻节点钱包服务；是全球唯一支持匿名链(XMC/XMR)的第三方数字资产管理钱包，支持 Bancor 协议并自动响应一切智能合约支付请求，支持领先的区块链协议和主流货币的主网及其代币交易，实现多链资产、多币种的跨链流通交易。

此外，开发者可以通过 UDO 区块链平台提供的 API 开发私有的去中心化钱包应用。

**Dapps (去中心化应用)：**UDO 将上线 DApps 开发平台功能，让开发者可以很



---

容易地将以太坊等其他公链的 Dapp 迁移到 UDO 主网，同时在 UDO 模块化功能的帮助之下，开发者可以非常容易、快速地开发 Dapps。

**接口层：**具有极强的可靠性和扩展性，通过 API 的接口为上层应用场景提供区块链基础服务的功能，打造高安全、高可靠、高性能的领先的企业级区块链基础平台。

**中间层：**合约部署、地址管理、权限管理、密钥管理、节点分配、节点配置、运行状态。

**合约部署：**UDO 支持以太坊和 EOS 智能合约系统，针对不同的应用场景进行技术抽象，搭建标准化、模块化的智能合约模版 (SSCU)，用于进一步组合、定制化面向不同行业、企业、应用场景的智能合约 (ASCM)。在此基础上构建区块链通用接口协议 (BGAP)，用于对接上层业务应用层。

**权限管理：**对 UDO 上数据的各种操作权限进行管理，包括对读身份（获取区块链上的交易、区块等数据等）、写身份（向区块链系统发起交易）、管理员身份（加入创建区块链、修改区块链的配置信息等）等权限进行限制。操作者通过签名组合满足了指定的规则，则证明拥有了对应的权限身份，允许执行相应的操作。

**密钥管理：**UDO 将 MTI/CO 协议与区块链多节点挖矿相结合，形成一种分布式环境下多节点会话密钥生成协议，简化密钥管理策略。

---

**节点配置:** 区块链节点设备接收到与之相互连接的网络设备的业务配置默认值或缺省值不一致时, 业务配置默认值或缺省值将被迫改变, 有些改变不符合用户真实的业务配置喜好需求。UDO 提供的区块链节点业务配置方法不仅能够在收到的配置数据不符合用户实际喜好需求的情况下最大限度地根据用客户喜好特征进行个性化定制业务配置, 而且还能够对用户喜好特征以及业务配置进行实时查询、修改和更新, 从而提高了区块链节点业务配置的灵活性和稳定性。

**服务层:** 在访问层之上构建高可用性、可扩展性的区块链应用基础平台产品, 用户可以通过标准智能合约接口, 根据不同应用场景构建不同的智能合约, 快速搭建上层区块链应用场景。

**智能合约引擎** UDO 支持多种类型智能合约, 并实时监控智能合约在运行时是否存在高危函数调用和容器逃逸行为, 预防恶意智能合约对区块链系统的威胁, 同时评估被开发者新开发的智能合约系统。

**共识算法** UDO 提供新的自适应共识机制 UPOS, UPOS 能在长期运行中缩短交易确认时间、减少通信资源的使用、提高系统的效率。

**运营管理** 为客户快速接入以及接入之后能够快速准确地识别系统的运行状态以及在运行中满足其他的运维需求, 如存储账本扩容、程序升级等。UDO 提供了完整、快捷、可视化的运营监控系统, 运营监控主要包括配置、监控、告警、发布和业务分析等功能。

**联盟成员管理** UDO 服务提供联盟链方式, 每个联盟成员为 UDO 独立用户, 独立管理自己的节点和账本, 联盟发起成员可以通过账号邀请的方式将其他用户加入到现有的区块链系统中, 根据业务需求逐步扩大联盟链成员。后期根据市场需

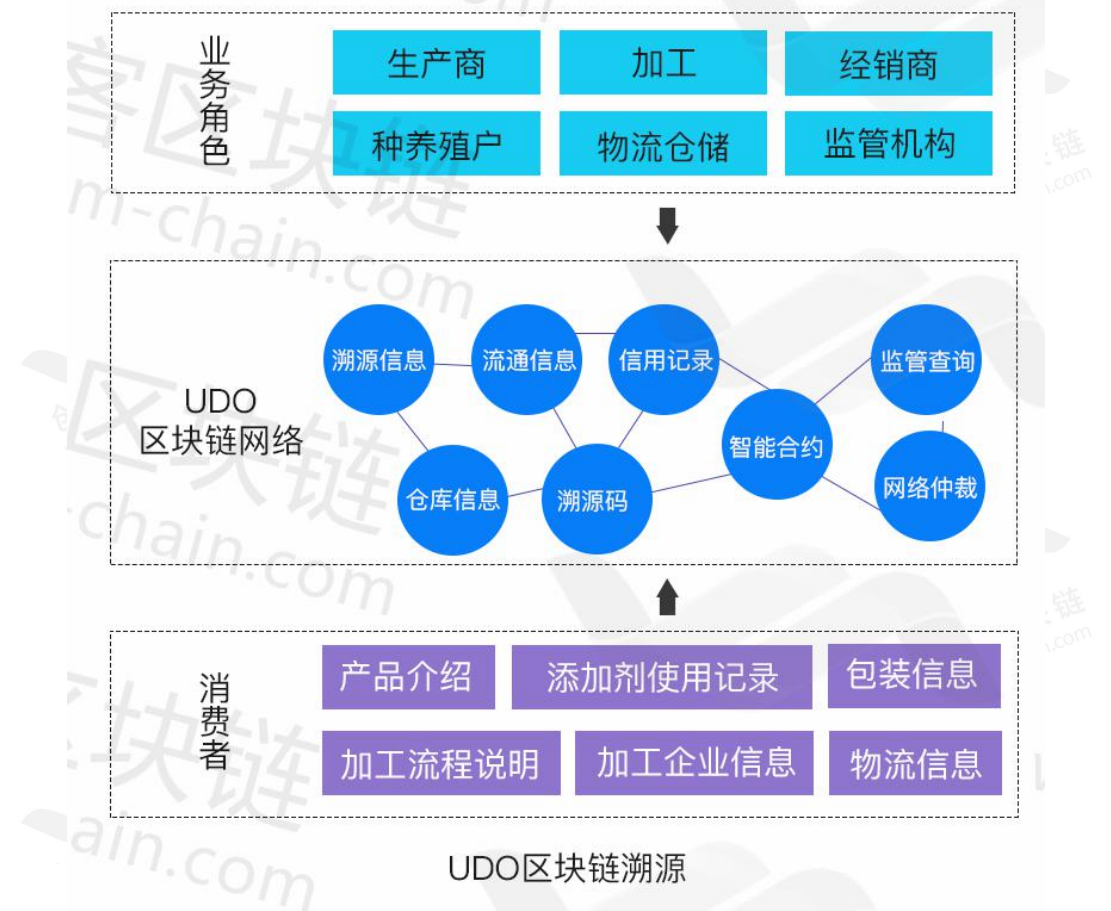
求将增加通过共识算法实现的节点成员自动加入机制, 实现更加动态的成员管理方式。

**访问层：**检索引擎、状态操作引擎、跨链访问引擎。

## 五、UDO 应用场景

### 5.1 商品溯源

在传统的商业零售场景中, 商品从出厂到消费者的链条存在中间环节信息不透明的情况, 当发生商品质量或安全问题时, 难以回溯和追责。同时供应链信息也存在被篡改或伪造的风险。



UDO 从底层重塑生产关系, 能够围绕核心企业搭建一条包括制造商、供应商、

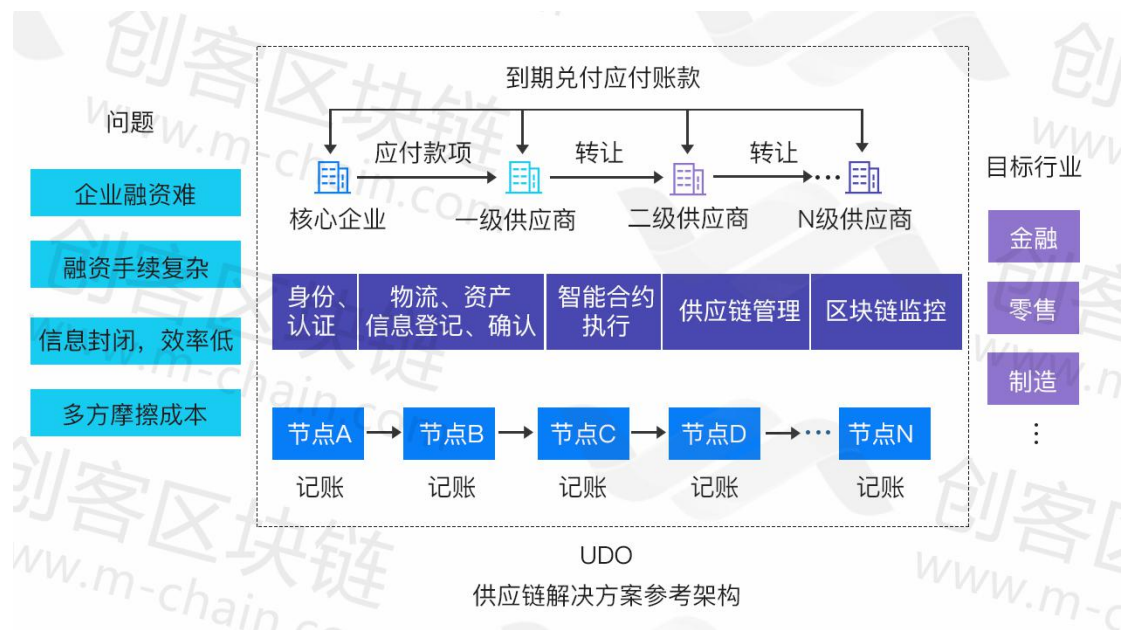
---

分销商、零售商、物流公司、消费者等在内的底层链，将资金流、信息流、物流都记录在链上不可篡改，实时记录并共享供应链各环节的最新进展。核心企业得以实现对供应链的掌握，及时地了解订单的生产、质量、运输等情况，提高供应链透明化和可视化；消费者可对商品实现溯源查询和验真伪。

同时，UDO 可以实现多方共同记录溯源信息，保证溯源信息是经过各个业务参与方共同确认的，具备不可篡改性。区块链的时间戳功能和可溯源技术可以有效解决商品的溯源防伪问题，将供应链上的每个产品的信息，包括来源、生产数据、存储温度等以物联网的方式登记在 UDO 上，利用公共账本和不可修改的特性，提供验证服务，对产品进行有效溯源。UDO 上的全流程交易历史记录均可被审计，满足政策和监管的要求。此外，UDO 将结合适用于各种商品形态的防伪以及数字化技术，才能形成一套完善的溯源方案。

## 5.2 供应链金融

供应链金融从优化供应链整体运行效率的角度出发，成为中小企业融资的有效渠道。然而，无论是以物流企业为中心的“1+N”模式还是发展至今的供应链金融 3.0“N+N”模式始终面临诸多瓶颈，没有实质降低企业融资成本，随着大数据、人工智能、区块链等代表数字智能时代技术创新的出现，以数据为基础、在区块链去中心化的信用体系中，充分发挥人工智能的分析运算能力成为真正解决“融资难、融资贵”的有效途径。

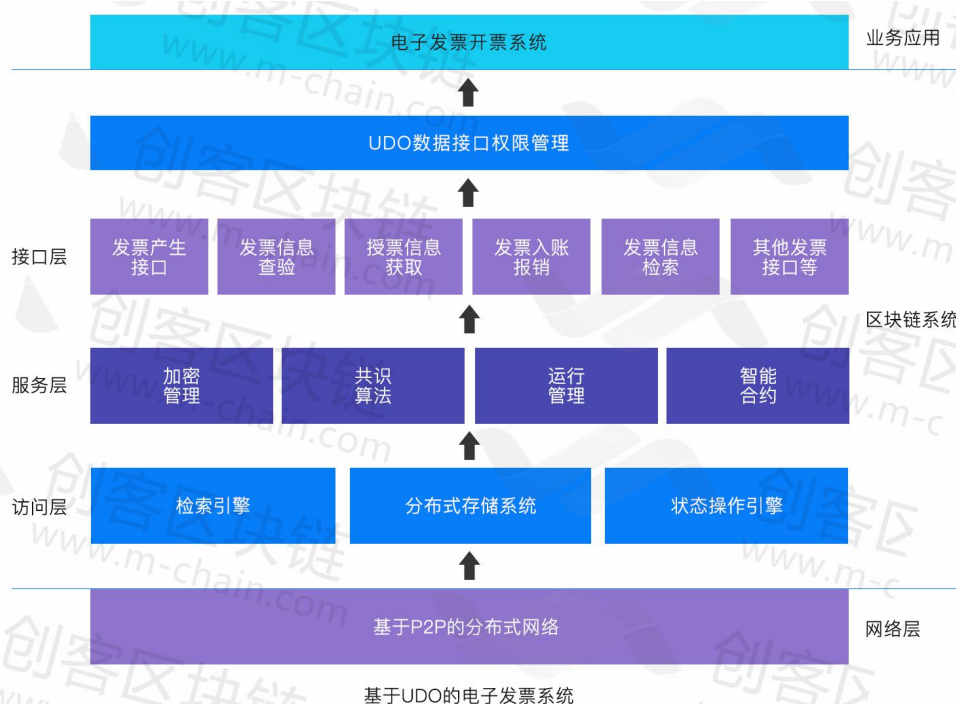


运用区块链技术，初步建立针对整个供应链内部的区块链体系，并充分发挥互联网金融资产交易的功能，将之与 UDO 体系相结合，完整记录供应链内部企业之间、供应链企业与外部企业的价值交换和债权、股权等金融资产的交易记录，在降低供应链金融本身风险的基础上，充分激活资金的流动性，提高资金的使用效率，激活供应链自身活力的同时，充分引入外部有效资源，补强供应链体系，提高供应链整体的运行效率。

### 5.3 电子发票系统

电子发票的大规模应用促进了经济和社会的发展，但也存在一些问题，如电子发票的重复报销等。区块链技术应用用于电子发票，可有效解决电子发票实际使用中的问题，从而实现电子发票数据的共享、确权、真实和信任的四大特性。





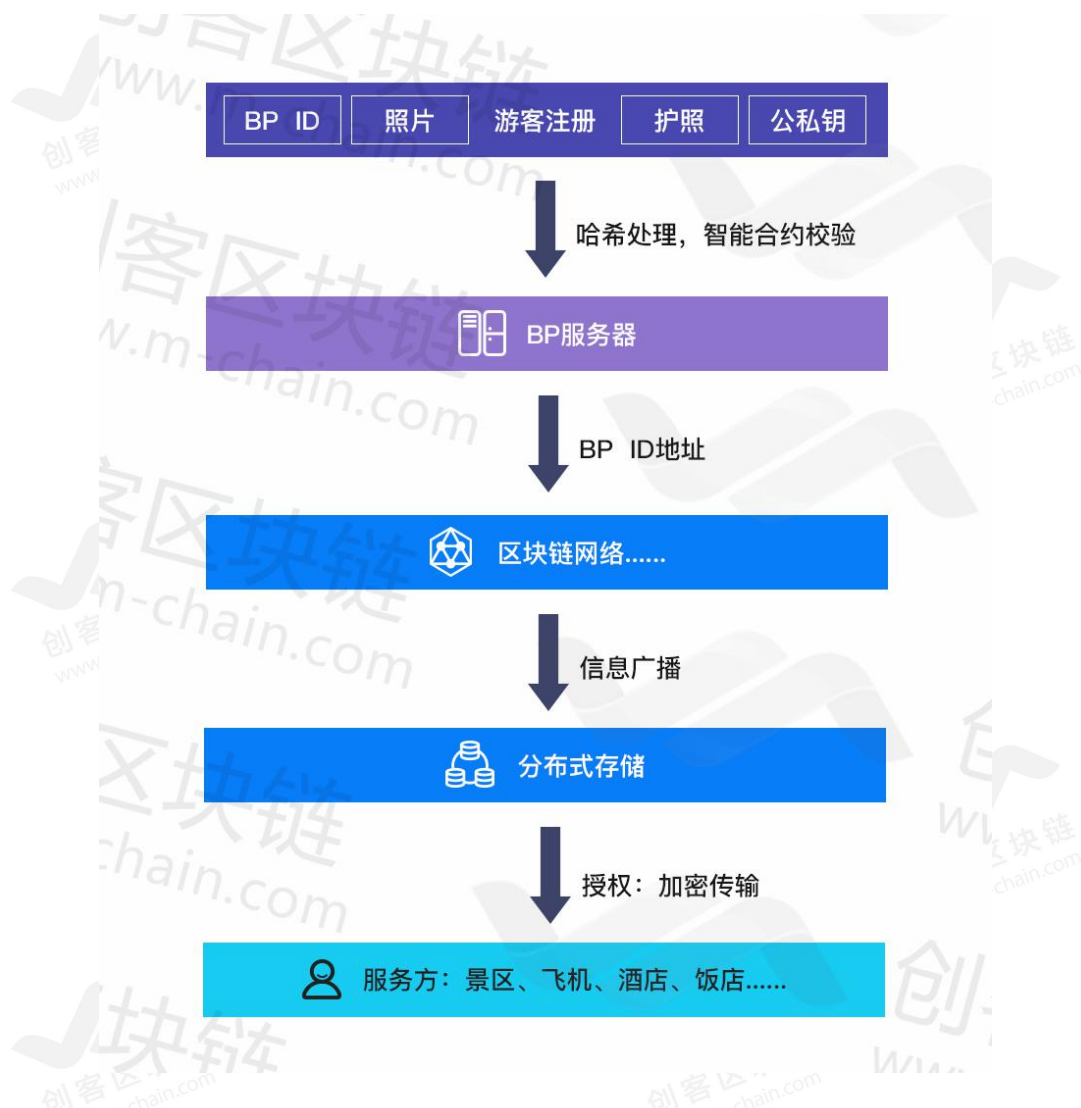
结合区块链技术，构建一个具有公有网络的联盟链模式的电子发票区块链，在这个区块链中，引入税务机关进行区块链制度上的监管机构，并由税务机关统一制定区块链的运行标准和合约条件，区块链上的各节点和加入者都必须按照事先制定的交易规则参与和运行。所构建的电子发票区块链中，第三方服务平台具有税务机关颁发的税务数字证书，并作为区块链发票的产生者，负责发票数据的真实性和有效性；区块链上的每个节点按照事先预定的相关发票业务的共识算法进行自行运转，维护区块链正常运行，并负责分布式记录发票账本。这样就可以在区块链中形成不可篡改、不可抵赖、可追溯、可查阅的分布式发票管理系统。

## 5.4 旅游场景

### 1.UDO 旅游平台数字身份认证

区块链具有身份认证功能，其可追溯、透明性、不可篡改性保证了区块中所有人身份、信息的真实性。UDO 系统中的每一个人身份都真实可靠，游客在旅行途

中无需重复认证身份、机票订购、住宿等环节，管理机构也无需反复核实游客信息，为游客和管理人员节省了时间。



基于 UDO，游客得以在拥有数字身份的同时维护自身数据安全，并且只允许特定组织或个人访问、储存、分析或分享个人数据，如酒店、景区。与此同时，在进行游客身份的识别和验证时，UDO 中所有游客在遵守用户隐私规定的条件下，建立一个有利可图的可视化数据库。

## 2. 通证化改造，激活旅游生态

现阶段旅游服务商建立运营的积分平台相对独立，具有零散、消费乏力、使用限

制多、兑换繁琐、服务商之间积分难以流通，同时，积分无法转让、赠送，因而传统积分的作用并不突出；此外，用户在 OTA 平台点评、发起旅游话题缺乏奖励，参与游客少，不利于大数据的搜集和评估，对平台作出贡献的旅游达人并没享受到平台升值带来的效益。

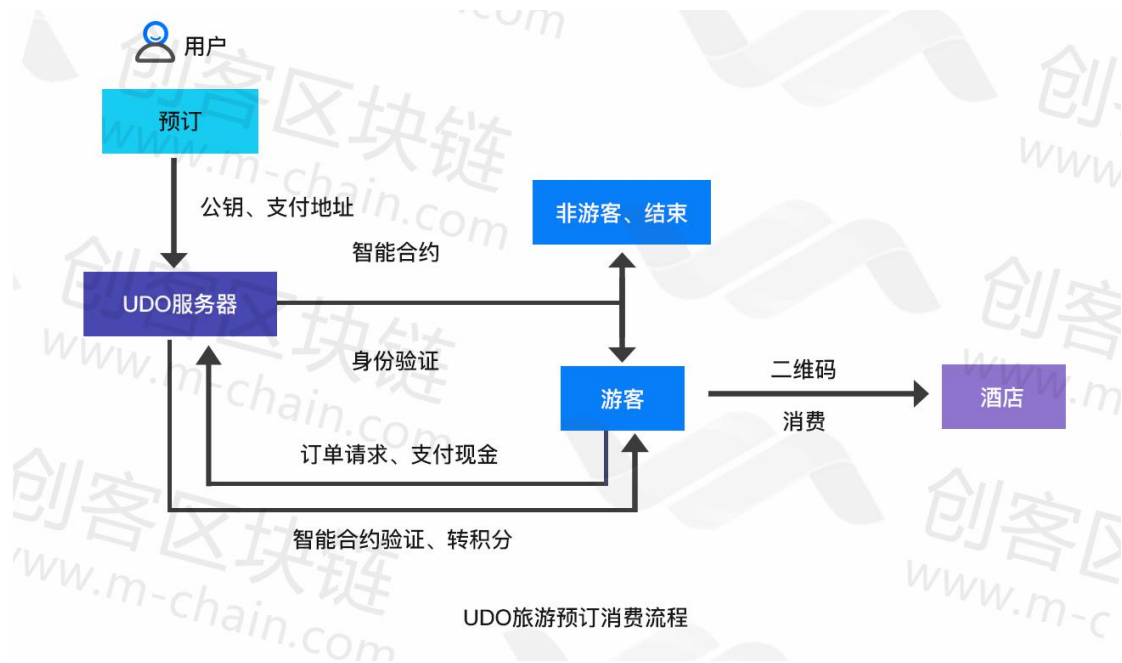


基于区块链技术，用积分链接 UDO 旅游平台各个消费环节，吸引更多旅游产业链商家入驻平台，让游客在平台实现跨行业的投资，拓展平台产业链，拓展积分价值，实现 UDO 旅游平台多元化发展。同时，通过积分产生消费激励、评价激励、推荐激励等形成平台、服务商、游客的利益捆绑，打造一个良性生态圈。

### 3.区块链在旅游预定领域的应用

OTA 为保证运营能力，建立庞大运营中心，产生高额运营成本，依托于 OTA 平台的服务商需支付较高佣金，高佣金又转嫁给游客，导致旅游价格居高不下，不利于旅游行业健康发展。

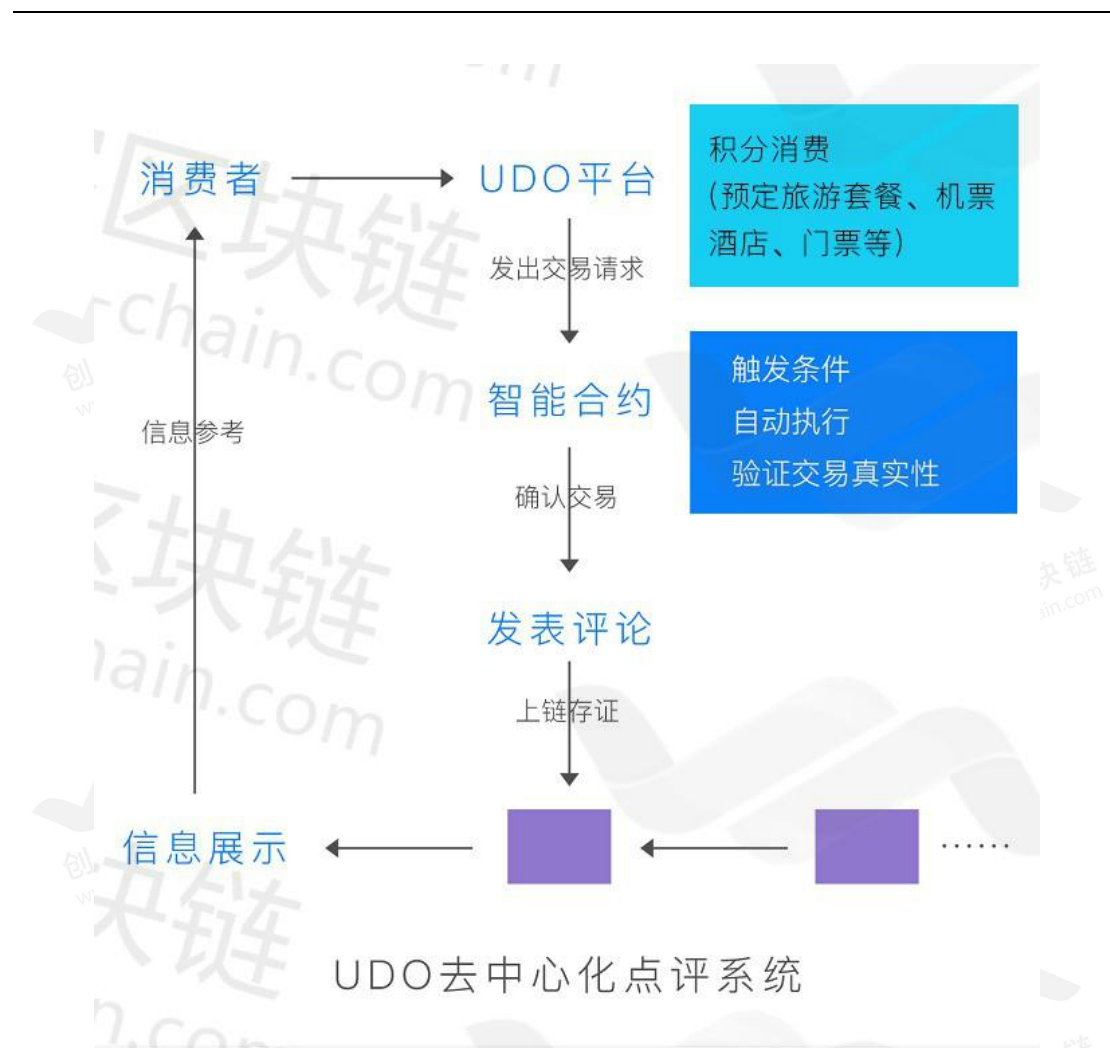




在 UDO 上，信息由分散在网络中的多个处理器同时保存和处理，可以让服务方和游客直接产生链接，同时，区块链智能合约可以实现交易流程自动化，加快交易速度，减少成本，增强用户管理。

#### 4.去中心化旅游点评系统

OTA 平台旅游评价（酒店、景区、餐饮、交通等）刷单严重，游客难辨信息真假，难以掌握旅游服务商、旅游产品的真实状况；评价错位对游客形成错误消费引导，致使旅游资源分配不均；

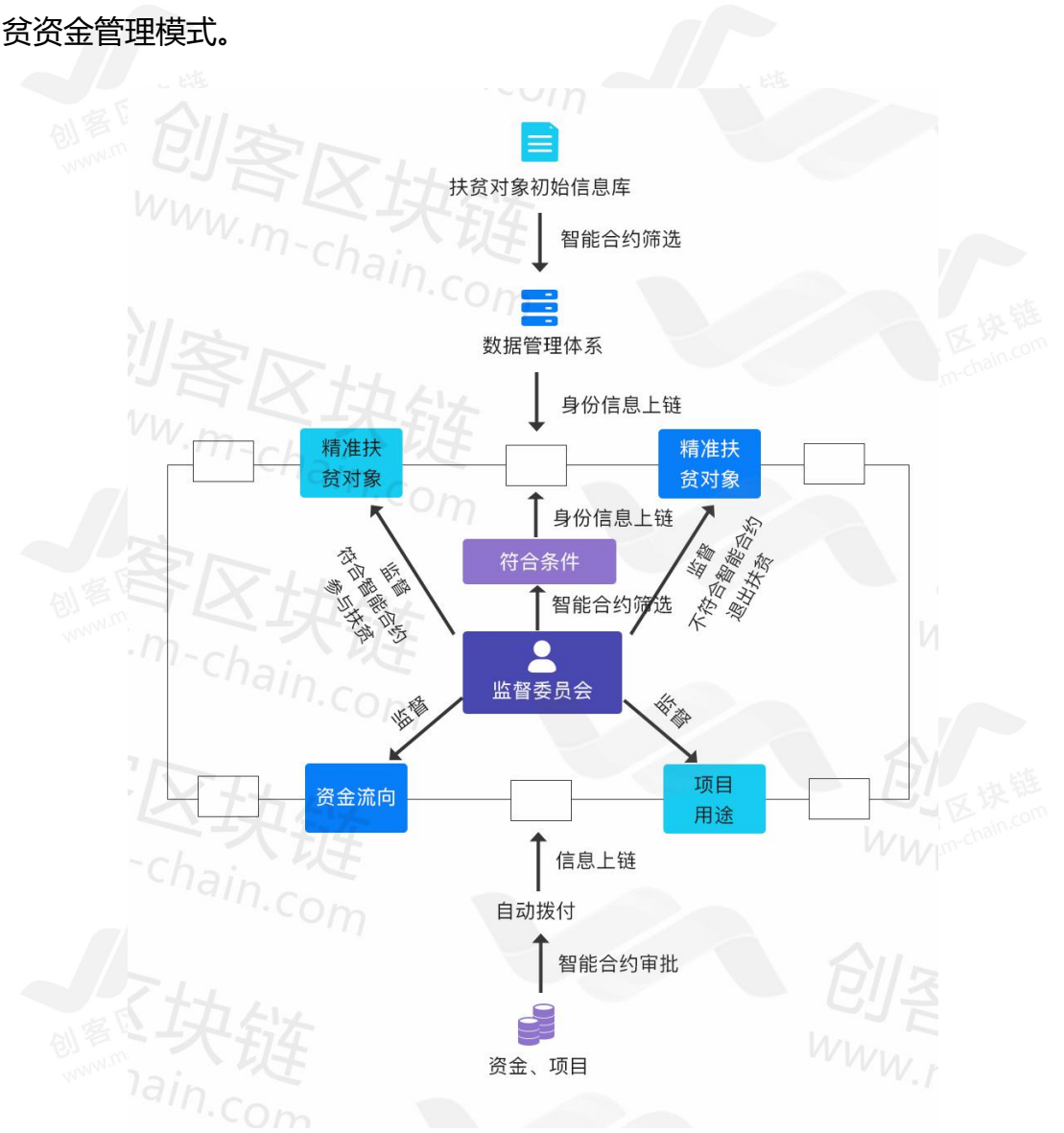


开发一个基于 UDO 的旅游点评系统，合作接入 OTA 平台，用户的点评信息上传到链上保证其存证溯源性，有效遏制 OTA 平台刷单，提高平台的服务质量和游客粘合度。每一笔交易都通过智能合约校验，并真实可追踪，可以有效避免黑色交易，增加政府财政收入和税收；用户更准确、清晰的了解旅游项目，合理规划自己的旅游线路，提升消费体验。

## 5.5 精准扶贫

巨额的扶贫资金需要通过省市县乡各级政府拨付，在这个过程中，如何精准确定贫困人口，如何解决帮扶过程中资金短缺、挪用、不透明的问题，是各级政府面

临的重要课题。将区块链作为扶贫资金管理的基础技术，通过共同建设脱贫攻坚区块链管理平台，将金融服务、科技创新与精准扶贫三者有机结合，变革传统扶贫资金管理模式。



(UDO 精准帮扶示意图)

1.精准扶贫身份体系上链和有效的退出机制

作为精准扶贫的前提条件，对扶贫对象的精确识别尤为关键。运用大数据指纹识别或人脸识别手段，记录拟扶贫对象的初始信息并录入数据库，运用区块链智能合约的扶贫标准筛选出精确的扶贫对象，建立扶贫对象数据管理体系，体系上链，不可篡改。

---

利用区块链可追溯性，监督委员精准记录帮扶行动和效果，根据区块链智能合约退出机制，确保帮扶对象精准退出。

## 2.精准投放扶贫资金

将过去层层拨付的方式变为项目驱动，在链上管理系统中，行政审批链和金融链跨链为各级政府提供数字化扶贫支持，地方政府在智能合约上确定扶贫项目和标准、资金用途和金额，一旦项目达到资金拨付的条件，只需审批完成，资金就会在智能合约的驱动下自动拨付，无需人为干预，大大提高了资金拨付的精准度和使用效率。

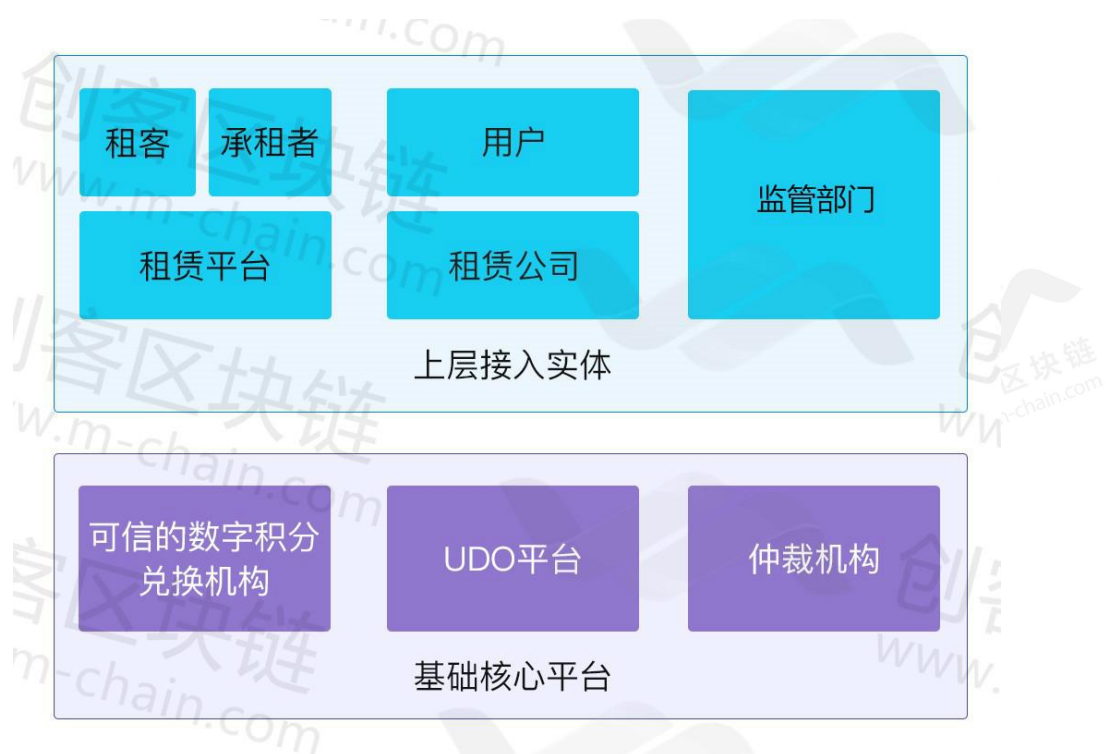
## 3.扶贫资金全流程管理

资金的发起、审批、拨付以及监督委员身份信息上链，实现整个流程的透明化；通过智能合约监控金融扶贫中各个项目的实施进程，形成全程跟踪式管理；分布式加密账本保障了各个节点共同监控下的信息安全，所有数据的变动系统内同步进行，不可篡改。

## 5.6 租房领域

由于市场的自发性，现阶段，房屋租赁市场发展相对滞后，大部分房屋租赁市场缺乏规范管理，市场供需不匹配，浪费大量人力物力。区块链技术核心特点是解决信用问题。从这个角度出发，在租房领域可以从以下几个方面利用区块链技术：第一是让房屋产品变得可信，第二是让房主和租客双方变得可信，第三是让整个

租用流程变得可信、高效。



## 1.租房信息上链，虚拟现实(VR)场景链上发布，让房屋产品变得可信

租赁平台通过区块链技术将房屋的基础信息全部记录上链，从土地规划开始，到施工建造、合规销售直至物业交付，发挥区块链的去中心化、安全透明、不可篡改等特点，有效减少租客在租房子时遇到虚假房源情况，减少纠纷和交易成本。

基于区块链技术的 UDO 租赁平台可以提供虚拟现实场景模拟服务，由系统或者其他外包第三方先进行现场房屋查验，制作虚拟现实场景，而后发布于 UDO 上供租赁者体验和欣赏，由 UDO 系统担保模拟场景的真实性。通过这种方式可以提高房屋租赁效率与签约成功率，减少时间成本的损耗。

## 2.资信评级建立租用双方的信任关系

---

区块链技术通过其建立一套完整的底层信任协议,可以有效联系租赁双方当事人,将中介排除于租赁交易体系之外。同时,区块链可以将租赁双方真实的不可篡改的资信情况上传到 UDO 底层协议,资信考察涵盖双方注册信息、历史交易情况、价格情况、平台奖惩情况等,信息公开透明,双方利用其系统分析功能,了解交易对方的资信状况,在掌握尽可能完全的信息的前提下,做出最优的决策。

### 3.智能合约技术提高交易效率

传统的房屋租赁流程繁琐,一般是筛选、看房,满意后,房主和租户签订合同,并且互相出示相关的证件及说明。这些行为大多是为了降低双方的风险。区块链时代,可实现智能检索和链上交易。

当租赁双方有不同的个性化需求时,可以在发布或者接收信息的同时设置信息筛选过滤器。UDO 智能合约通过设定的程序对房屋的区域、价位、质量和租客身份标签自动进行信息匹配筛选,出租人可以设置偏向的人群特征,承租人可以选

择偏好的房屋类型和合适的合租室友,提高选房效率。

双方确定交易后,基于链上的信任,可直接在链上进行交易,相关的合同协议均可以通过智能合约完成,从最开始的合同签署以及租金的缴纳,后期的续约等都可以基于智能合约自动完成,双方无需进行反复沟通。

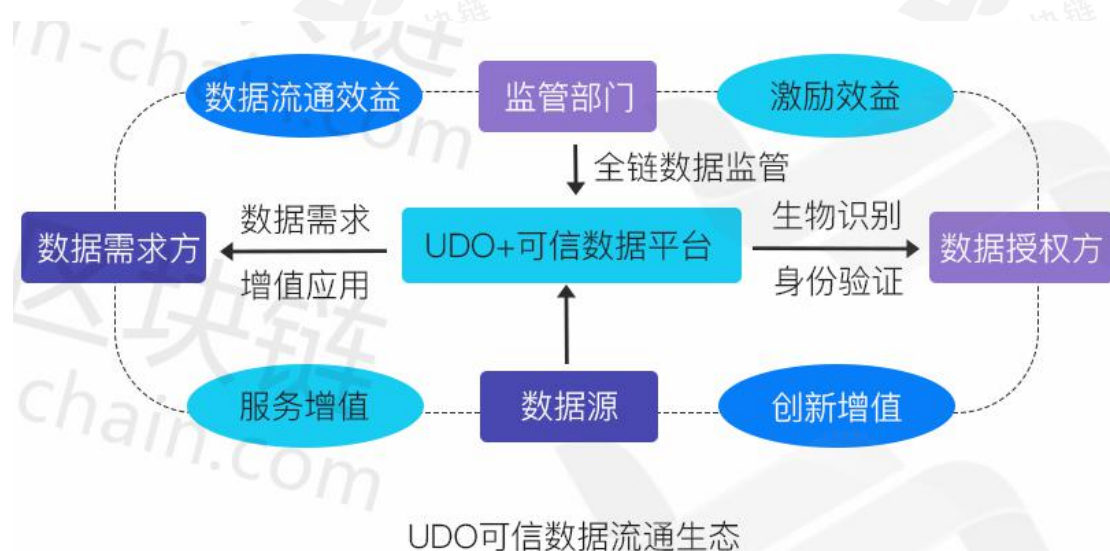
## 5.7 区块链可信数据共享方案



共享经济的繁荣发展产生了大量的数据，电子数据存在一些问题，比如系统故障导致数据丢失，数据容易被轻易篡改和伪造，电子数据易修改、易复制。

通过区块链技术可将数据所有权人的业务参与信息即时同步到数据需求方、数据源方、共享服务平台，在业务授权的前提下实现数据的流通，并将授权信息和数据调用过程记录在 UDO 区块链上，形成不可篡改、随时可追溯的具有公信力的可信凭证。

区块链的数据传输可插拔地结合了数字摘要、对称加密、非对称加密技术，能够保证数据在数据需求方、数据平台方、数据源之间的加密传输，防止数据泄密，确保只有数据接收者能解读数据内容，且能方便验证数据发送者身份，除此之外任何人都无法从截获的数据内容中解读出任何有意义的信息。



### 基于 UDO 的可信数据流通生态：

UDO 在技术上保证数据流通中产生的授权信息、过程信息等的不可篡改、不可删除，在所有相关节点形成同步记录。尤其是将部分节点交由数据源、数据需求

---

方、监管方控制，形成联盟区块链后，解决利益相关多方信任的问题。

UDO 只对数据流通的过程进行记录，无需留存任何具体数据。平台方发挥资源整合的作用，同时也可以结合大数据分析等技术，作为数据服务方接入区块链，满足共享服务需求方对数据的处理和汇集的个性化需求。

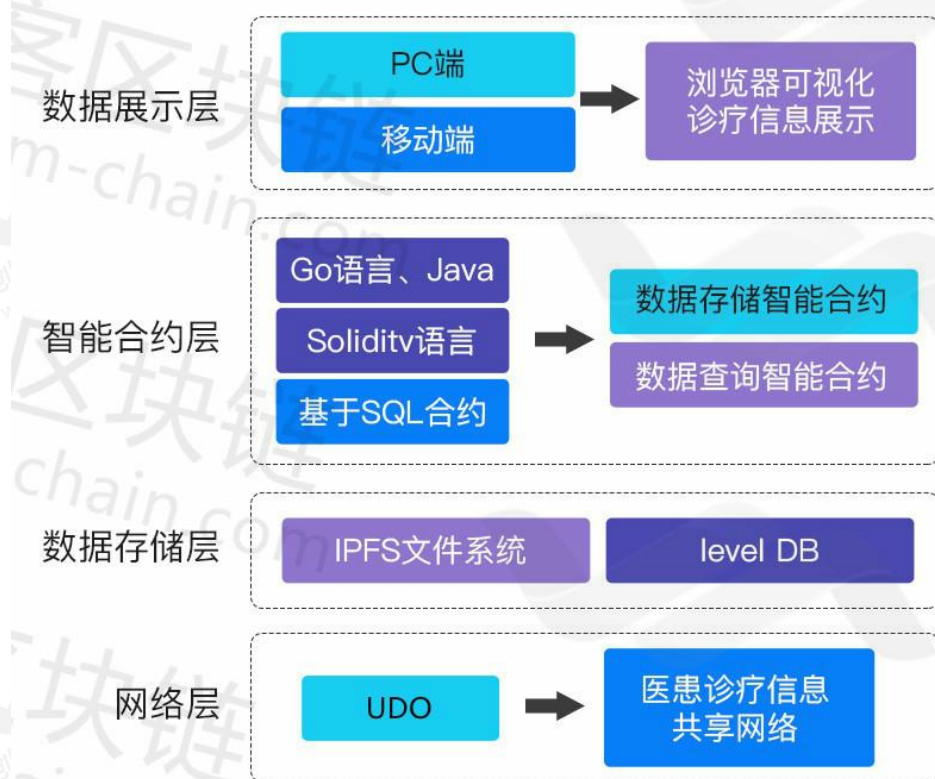
通过构建 UDO 的数据可信流通平台，连通共享服务的各个参与方，共享平台将能提供更多具有价值的 DataService，最终建成可信数据流通生态圈，极大提高共享经济的效率。

### 5.7.1 医疗信息共享

在医疗领域中，患者的个人诊疗信息（包括化验单、核磁共振图等）都是宝贵的数字资产，如果能够为各个机构的医生创建一个共享的个人诊疗信息数据源，提供及时、准确和广泛的病人健康数据，并且实现跨机构医生之间的诊疗信息共享，则可以帮助医生制定更加科学的诊疗计划、优化治疗方案。

区块链作为一种多方维护、全量备份、信息安全的分布式记账技术，为医疗数据共享带来一个很好的突破点。可以设计一种基于区块链技术，结合 IPFS（InterPlanetaryFileSystem）的个人诊疗信息共享模型，帮助实现患者个人诊疗信息的便利共享、快捷流转和海量诊疗信息的低成本、分布式可靠存储。





### 诊疗信息共享模型的建立:

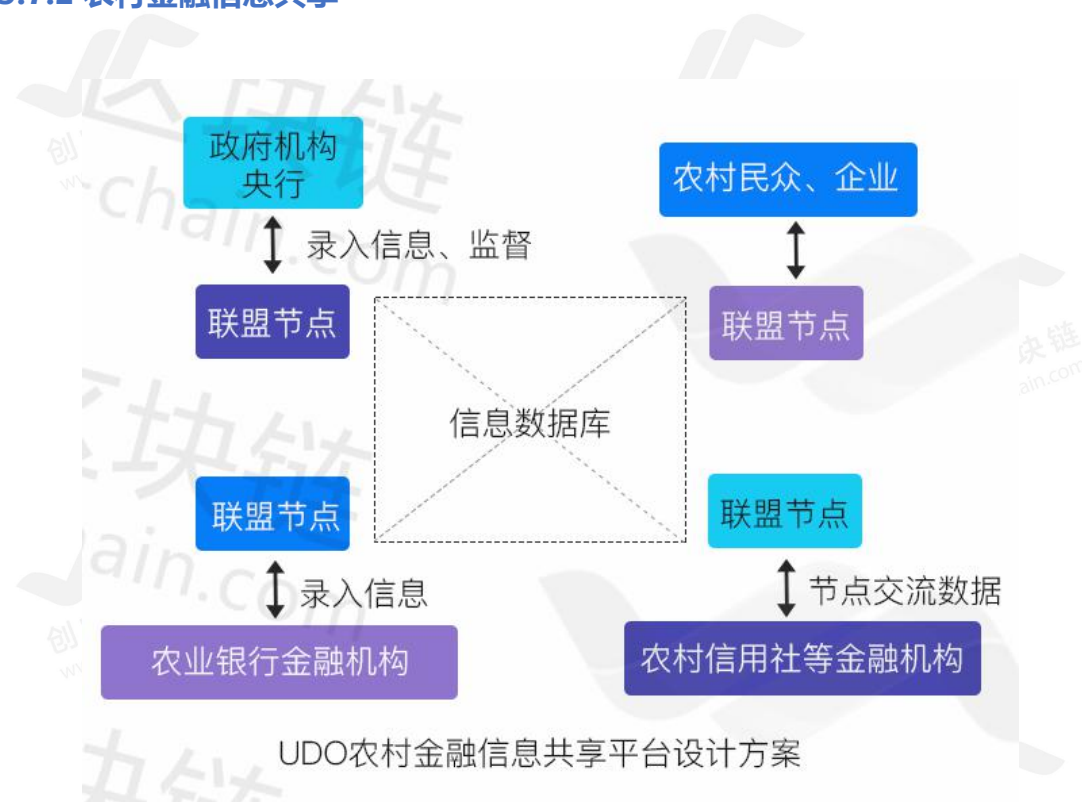
诊疗信息共享模型主要分为网络层、数据存储层、智能合约层和数据展示层。

医生节点录入患者诊疗信息，通过诊疗信息采集系统将诊疗信息存储至 IPFS 文件系统，IPFS 文件系统生成并返回唯一的哈希值标识患者诊疗信息，利用智能合约将该唯一哈希标识存储在区块链上，并且返回索引 ID 给患者，从而实现诊疗信息的分布式可靠存储。

当医生节点需要获取患者的诊疗信息时，向患者请求诊疗信息的唯一哈希标识在区块链上的索引 ID，获取到诊疗信息在区块链上的 ID 后，利用智能合约获取该索引 ID 所指向的诊疗信息唯一哈希标识，医生节点通过已获取的诊疗信息唯一哈希标识，基于内容寻址，在 IPFS 文件系统中查询患者的诊疗信息，从而实现

医患诊疗信息的便利共享。

### 5.7.2 农村金融信息共享



UDO 系统上的节点分为联盟节点与其他节点。其中，联盟节点主要为央行、农业银行、农村信用社等政府监管部门或金融机构。

央行可导入目前已有的征信系统信息数据。金融机构在获取农村民众或企业信息并进行一定的核实之后，将信息数据引入 UDO 区块链。每一个联盟节点之间都实现直接对接，共享、交流数据，通过 UDO 系统自动运行的共识机制与智能合约功能，仅在该节点与其他节点的数据保持一致时，即确保信息可靠、非重复的情况下，才能够导入 UDO 储存系统，形成数据库。导入的数据通过密码学算法实现加密且不能篡改。当金融机构需要提取数据时，输入所设定的索引（如身份信息等信息）即能进入数据库导出相应信息数据。

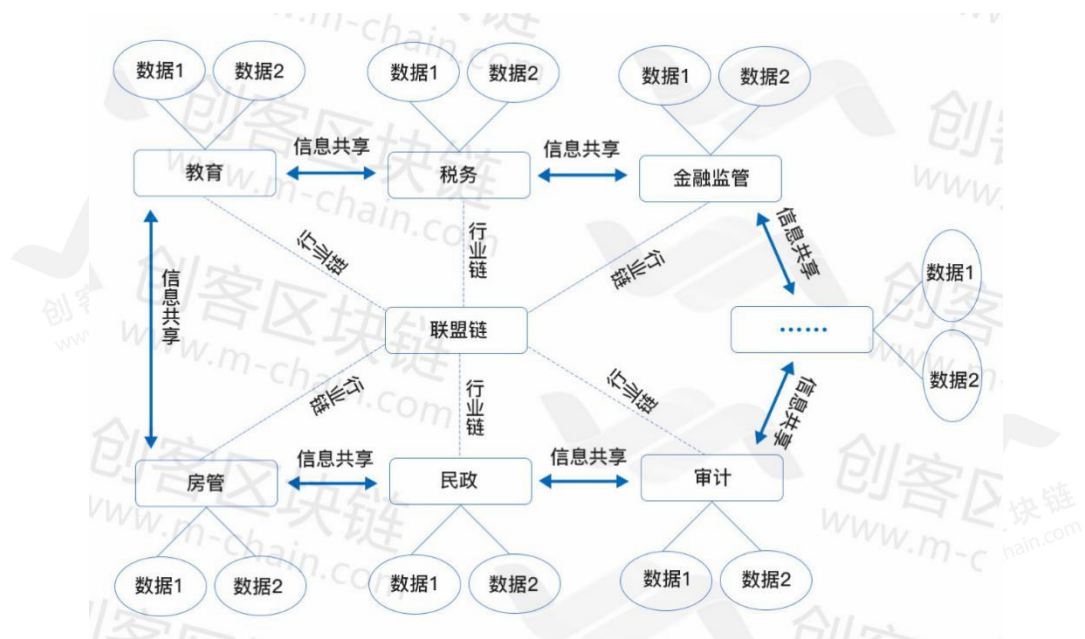
---

其他节点上主要为农村民众、企业等普通用户，在得到金融机构等授权之后能够读取个人在数据库中的金融信息数据。参与 UDO 系统的节点越多，数据库的可靠性以及安全性就越强，在 UDO 系统基础上，还可拓展设置权限、数据管理、信息反馈、信息更新等多种功能，从而建立一个较为完善的农村金融信息共享平台。

## 5.8 区块链在政务领域的应用

区块链技术的分布式、透明性、可追溯性和公开性与政务“互联网+”的理念相吻合，其在政务中的应用也将进一步推动政务“互联网+”的建设，并对政治、经济、社会发展过程中各类主体及制度、文化、态度、行为等都会产生重要影响。

区块链弃用原先的 C/S 架构模式，采用 P2P 对等节点模式，大幅降低了统一数据平台技术研发的难度，另一方面提高了专用数据的处理能力，对等节点中，每个节点都享有同样的存储信息，独立作业并互相监督。通过引入共识协议使得系统在面对新的业务、数据模型时，仅需通过软件部署共识协议即可实现，无需再次构建现有的数据存储结构及接口数据结构，提高了系统的可扩展性。



(政务大数据平台结构)

### 1.审计部门：降低成本、提高效率

区块链显著增加了造假的成本，为审计、审查工作提供了便利。传统审计工作会消耗大量资源在收集信息、分析数据、判断问题严重性以及形成客观公正的结论上，而时间滞后性和覆盖范围的局限性容易影响审计结果的准确性。区块链以时间戳的形式在特定时间点固化凭证，在确保信息真实、完整方面能节省大量的工作资源，并且智能合约能自动化执行部分审计流程，提高审计工作效率。

### 2.法制部门：提升司法效率

9月7日，最高人民法院《关于互联网法院审理案件若干问题的规定》开始施行，提出了区块链技术在司法当中的应用，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。将“区块链+司法”作为底层技术，让电子数据变成电子证据，规范数字经济中的产权认定等问题，这将会极大地提

---

升司法效率，更是区块链技术应用落地的一个重要里程碑。

### **3.教育部门：学历信息、学术成果存证**

利用区块链技术，解决现有的学生信用体系不完整、数据维度局限、缺乏验证手段等问题，简化流程和提高运营效率，并能及时规避信息不透明和容易被篡改的问题。在区块链中记录跨地域、跨院校的学生信息，追踪学生在校园时期的行为记录，构建良性的信用生态体系。此外，通过区块链为学术成果提供不可篡改的数字化证明，可为学术纠纷提供举证依据，降低纠纷事件消耗的人力与时间成本。

### **4.房管部门：产权登记**

目前，房地产交易市场在交易期间和交易后的流程中，存在缺乏透明度、手续繁琐、欺诈风险、公共记录出错等问题。区块链技术的应用可实现对土地所有权、房契、留置权等信息的记录和追踪，并确保相关文件的准确性和可核查性。此外，可借助区块链技术实现无纸化和实时交易。杭州已有利用区块链进行房产登记的业务上线，从具体的操作上看，区块链技术在房屋产权保护上的应用，可以减少产权搜索时间，实现产权信息共享，避免房产交易过程中的欺诈行为，提高房地产行业的运行效率。

### **5.交通部门：智能理赔、自动维护**

通过区块链智能合约可将每辆接入车联网的汽车都变成可以自我维护调节的独立网络节点，这些节点可在事先规定或植入的规则基础上执行与其他节点交换信息、核实身份、路桥费支付以及无人驾驶汽车的自主维修保养等功能。

---

同时区块链的智能合约还能显著提升目前交通理赔的智能化水平并创新汽车保险市场。智能合约可以记录相关政策、驾驶记录和驾驶员报告，允许车辆在发生事故后依据事先嵌入的规则自动执行处理相关索赔流程并获得赔付，大大节省目前的赔付时间。

## **6.文化部门：知识产权保护**

传统的版权登记流程至少需要一个半月时间，与数字内容创作和流通短平快的特性不相匹配。利用区块链技术，将文化产业链条中的各环节加以整合，加速流通，能够有效缩短价值创造周期。通过区块链技术，对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品在区块链上被确权，后续交易都会进行实时记录，实现文娱产业全生命周期管理，也可作为司法取证中的技术性保障。

## **7.税务部门：纳税证明支持贷款**

一段时间内的税务信用等级、销售收入、利润、增值税、企业所得税等关键指标能够反映企业的信用状况和盈利能力，适用于作为银行评估中小微企业贷款能力的一个指标与凭证。为了确保企业纳税凭证的真实有效，税银贷款业务通常以纸质材料形式办理。将区块链技术应用用于在线税银贷业务，由贷款企业授权银行查询纳税数据后，银行根据内部风控模型给予企业授信额度，以此快速实现税、银、企三方数据对接。采用区块链技术，不仅能够实现电子纳税凭证的鉴真，而且智能合约可保证数据使用授权执行、控制操作权限，并存证全流程应对争议。



## 8.卫生部门：推动电子病历存证

我国早在多年前就主张推行电子病历，但由于患者隐私信息易泄露和电子病历易被篡改两大安全顾虑阻力重重。医患争议发生时，电子病历也难以被法庭采纳为关键证据。电子签名是将医疗责任落实到人的证据指向，而区块链存证提供了不可篡改的电子证据验真记录。也只有充分保障数据流通的可信和安全，才能实现电子病历的方便流转。

## 9.档案系统：方便查询、不可篡改

各单位都有档案室，都建有档案管理系统，能够方便查到公民的出生、籍贯、工作经历等综合信息。但违法更改个人人事档案的事件屡有发生，如修改个人出生日期、修改工作经历、修改民族、修改学历等问题。由于个人年龄等和个人的职业发展密切相关，目前的个人人事档案管理手段也存在漏洞，现有人事档案管理方式不能完全杜绝人事档案修改作假。应用区块链技术后，通过区块链记录每个公民的出生日期、任职履历等基础信息，形成无法篡改的个人电子档案，从技术上彻底解决传统档案管理中存在的问题和积弊。一旦档案信息经过验证并添加至区块链后，就会永久的存储起来，区块链的数据稳定性和可靠性极高，为公民人事档案的准确、完整提供了技术保障。

## 10.信访部门：政务信息公开落实

政府的主要职能在于经济管理、市场监管、社会管理和公共服务。而电子政务就是要将这四大职能电子化、网络化，利用信息技术对政府进行信息化改造。通过

---

电子政务，政府可以将社会公众关注的事项及时公开，接受社会公众的监督。由于区块链技术能够保证信息的透明性和不可更改性，有助于社会公众对政府信息公开信息的信任，对政府信息公开的落实有很大的作用。如在土地登记方面，使用区块链记录将能保证完整的土地流转信息，包括登记土地的位置、大小、权属、交易记录等。

### 11.民政部门：公益慈善项目监督

区块链上存储的数据，高可靠且不可篡改，天然适合用在社会公益场景。公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等，均可以存放于区块链上，在满足项目参与者隐私保护及其他相关法律法规要求的前提下，有条件地进行公开公示，方便公众和社会监督，助力社会公益的健康发展。例如 BitGive 建设的捐赠平台。BitGive 是一家非营利性电子货币慈善基金会，致力于将比特币及相关技术应用于慈善和人道主义工作中，促进慈善事业发展。2015 年，BitGive 公布慈善 2.0 计划，应用区块链技术建立公开透明的捐赠平台，平台上的捐款的使用和去向都会面向捐助方和社会公众完全开放。

### 12.食品药品监管部门：产品防伪溯源

区块链技术可以用于产品防伪。数据不可篡改与交易可追溯两大特性相结合，可根除供应链内产品流转过程中的假冒伪劣问题。基于区块链的酒类/奶粉防伪溯源体系有效结合传统二维码、分布式数据库与区块链技术，定制信息录入设备、手持扫码设备、编码机器等硬件，通过软硬件结合来实现方案。



### 13.财税部门：电子票据打假验真

在票据方面，基于区块链技术架构建立新型数字票据业务模式，借助分布式高容错性和非对称加密算法，可实现票据价值的去中心化传递，降低对传统业务模式中票据交易中心的依赖程度，降低系统中心化带来的运营和操作风险。通过区块链的可编程性，有效控制中介市场中的资产错配，借助数据透明特性促进市场交易价格反映资金需求的真实性，控制市场风险。区块链技术不可篡改的时间戳和全网公开的特性，能有效防范“一票多卖”“打款背书不同步”等问题。

### 14.金融监管部门：风险防控事前监管

在各类互联网金融创新的繁荣下，也逐渐隐藏着各类由于风险防控手段不足所构成的信用风险以及事后监管所面临的证据缺失等问题。

政府金融监管部门通过引入基于区块链的点对点数据授权共享机制，能够为广大互联网金融从业企业提供更为完整的可信数据分析产品，从更为完整的数据维度对线上信贷客户进行风险评测与风险定价，从而有效防控系统性风险的产生并维持社会稳定。另一方面，针对于穿透式监管在互联网金融领域的创新实施，通过将区块链存证系统接口前置接入各互联网金融业务平台，将业务操作流程记录经过哈希后实时向政务区块链进行锚定同步，能够有效地实现在保护业务隐私的前提下对互联网金融业务进行事前监管。一旦出现违规经营，链上完整、不可篡改的数据记录将作为监管审计调查的有效证据链条。

---

## 参考引用文献

1. Ethereum whitepaper: <https://whitepaperdatabase.com/ethereum-eth-whitepaper/>
2. Smart contracts [https://en.wikipedia.org/wiki/Smart\\_contract](https://en.wikipedia.org/wiki/Smart_contract)
3. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake  
<https://pdfs.semanticscholar.org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf>
4. Bitcoin whitepaper: <http://bitcoin.org/bitcoin.pdf>
5. Bancor Protocol :  
[https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor\\_protocol\\_whitepaper\\_en.pdf](https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf)
6. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies  
<https://ieeexplore.ieee.org/abstract/document/7423672>
7. EOS whitepaper : <https://whitepaperdatabase.com/eos-whitepaper/>
8. Blueprint for a New Economy
9. In Search of an Understandable Consensus Algorithm  
<https://www.usenix.org/system/files/conference/atc14/atc14-paper-ongaro.pdf>
10. Tendermint: Consensus without Mining  
[https://cdn.relayto.com/media/files/LPgoWO18TCeMlggJVakt\\_tendermint.pdf](https://cdn.relayto.com/media/files/LPgoWO18TCeMlggJVakt_tendermint.pdf)