bubi.cn 布比

商业级区块链技术服务及行业解决方案

布比区块链产品白皮书

V1.0

扫一扫，了解更多信息

邮箱:support@bubi.cn
网址:www.bubi.cn

2016.08

布比(北京)网络技术有限公司

布比区块链，让数字资产自由流动起来

目 录

布比区块链产品白皮书

摘要

本文主要介绍布比区块链的产品架构、技术特色与优势、行业应用案例等。区块链的核心价值在于构建可信任的多中心体系，有潜力成为构建价值互联网的基础设施。布比公司致力于打造企业级区块链产品并提供行业解决方案，已经开发了高性能、高可扩展的区块链基础服务平台，具备快速构建上层应用业务的能力，满足大规模用户数量的应用场景。瞄准企业级产品化运营能力，布比区块链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。在与产业合作伙伴共同深入探索区块链应用场景的基础上，布比区块链已应用于数字资产、贸易金融、股权债券、供应链溯源、联合征信、公示公证、物联网共享、数据安全等领域。以多中心化信任为核心，打造新一代价值流通网络，让数字资产都自由流动起来。

一. 价值自由流通的网络

今天的互联网，已经近乎完美地解决了信息传递问题，人们可以非常便捷、低成本地点对点传递信息。然而，目前的互联网技术还不能实现点对点的价值传递。不同于信息传递的可复制特征，价值传递需要保证权属的唯一性，所以当前价值的传递仍然需要依赖中心机构承担记账功能。简单地说，在信息传递之后，发送方和接收方能够同时拥有信息；但是，在价值传递之后，只能受让方拥有价值，转让方不能再拥有，目前这个转移过程的权属记录是通过中心机构记账实现。那么，如果网络本身能够提供可靠的记账功能，将使得价值传递不再完全依赖于中心机构，可以实现价值的点对点转移。

区块链这种分布式总账技术（DLT, Distributed Ledger Technology），能够让参与各方在技术层面建立信任（Trust），有潜力成为构建未来价值自由流通网络的基础设施，即形成价值互联网（Internet of Value）。尽管价值互联网广泛到来

的时间仍未可知，但从今天的发展状况来看，一些价值局域网已经在逐步形成。实际上，在某些特定领域，若干合作伙伴或产业链的参与方正在共同建立区块链信任网络，这种价值局域网已经在实施过程中，而不再只是概念。从价值局域网到价值互联网的一个可能的演进路径是：类比于互联网的发展历程，前期是一个个独立的、由各个行业按照自身需求形成的局部价值流通网络，后期在跨行业价值交换需求的驱动下，逐步形成大规模的、共有的价值自由流通网络。

区块链的核心价值在于构建可信任的多中心体系，将分散独立的各自单中心，提升为多方参与的统一多中心，从而提高信任传递效率，降低交易成本。

二. 我们的目标

目前，区块链产品可以大致分成两个层面：一是区块链底层技术；二是区块链上层应用。

布比区块链的产品定位是，提供商业级的区块链基础设施服务，主要包括：一是打造企业级区块链基础平台（“区块链底层技术”）；二是在其上构建具有高可扩展性的应用业务支撑系统（介于“区块链底层技术”与“区块链上层应用”之间）。

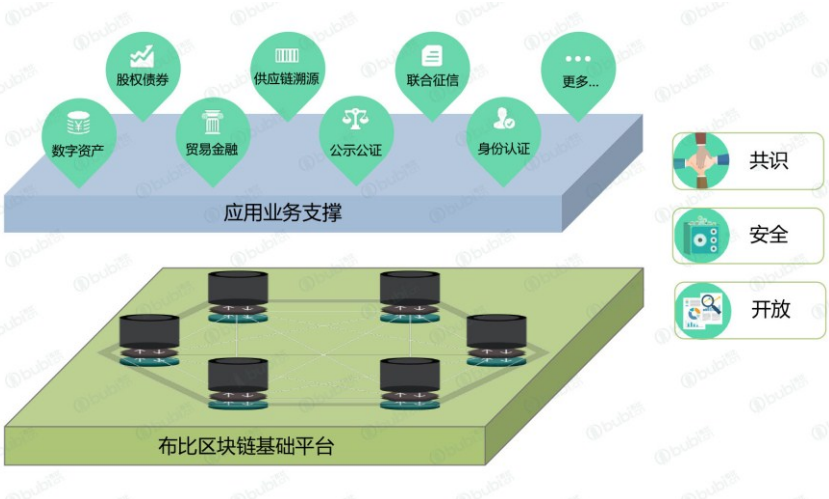

图 2-1 布比区块链的目标

布比致力于提高区块链的产品化程度，表现在如下几个方面：

（1）快速应用构建：多模式的账本结构及业务模型，方便快速构建应用；

（2）海量用户支撑：高效交易验证和同步，支撑千万甚至亿级用户规模；

（3）可视化运维管理：从网络、系统、业务层面提供可视化的运维管理；

（4）隐私权限策略：丰富的权限策略配置，依据应用需求进行隐私保护；

（5）内置智能合约：支持可编程的合约开发，并提供标准化的合约模板；

（6）区块链即服务：面向各行业领域，提供可配置企业级区块链云服务。

三. 商业探索的常见疑问

在过去一年多里，布比通过与十几个行业领域的三百余家企业机构进行深入交流和共同探索，体会到：区块链作为一项新兴的技术，还不能很好地直接适用于各种复杂的商业应用场景。以下是商业应用落地过程中几个常见的疑问：

1. 如何实现快速的应用对接

在很多的探讨和交流中，应用实现方虽然经常对区块链底层技术刨根问底，但真正落实到实际的对接使用中，大多数企业机构最关心的还是应用对接成本（包括时间和人力成本）和风险（安全性和可靠性风险）。

2. 能否支撑海量用户使用

很多大型企业机构目前已拥有上亿级用户量，他们在考虑是否更换一个新的技术时，一个重要考量就是能否平滑支撑海量用户的导入和使用：包括由此带来的性能、可扩展性、以及海量数据存取等问题。

3. 怎样保障私钥的存取安全

私钥的安全性是一个被高度关注的问题。在实际的商业应用里，用户不可能直接使用一串杂乱无序的字符串作为自己的用户名和密码，这就需要区块链平台与上层应用一起提供一套安全的私钥存取方案。

4. 区块链对上层应用是个黑盒

传统的企业机构运维人员习惯可视化的管理工具，他们可以直接看到整个系统的健康情况、登陆系统进行操作和管理。然而，区块链系统是由各个参与方共同建设与维护的，对于运维人员来说，与传统情况不同，整个体系是个黑盒。

5. 能否满足隐私保护和权限控制

区块链宣称的数据共享与透明在很多商业领域都是非常敏感的词汇。区块链在建立多中心化技术信任的同时，如何满足商业隐私的保护和操作权限的控制是商业应用中最常见的疑问之一。

上述这些涉及性能、扩展性、安全和运维的诸多问题，是布比在进行区块链产品设计开发时的重要考量因素。

四. 产品的架构

为了解决区块链技术在应用落地过程中可能面临的各种阻碍，布比区块链平台采用两层结构：（1）底层 BubiChain 提供区块链基础服务；（2）上层 Bubi Application Adaptors 对内进行封装，对外进行建模适配，提供一系列符合应用场景的接口，降低应用对接的复杂度，如图 4-1 所示。

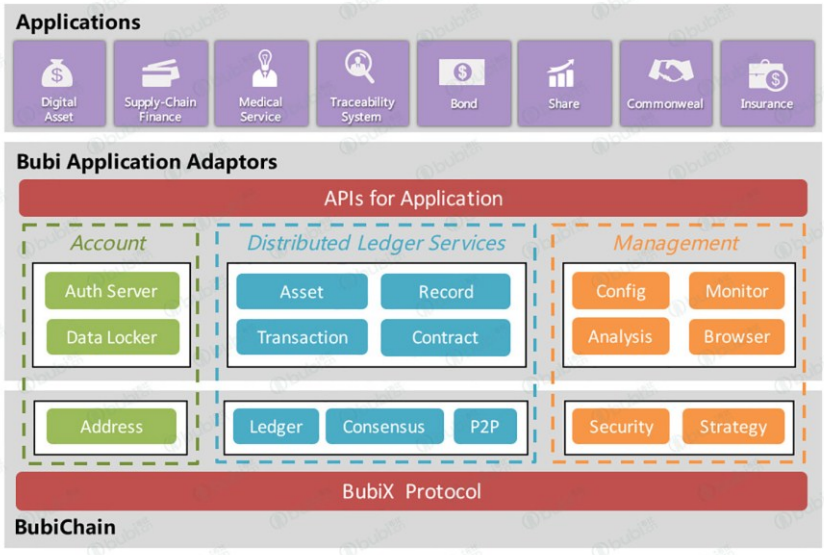

图 4-1 布比区块链平台架构图

布比产品体系架构分为三个组成部分：账户中心、分布式账本服务、策略与管理。其中，多数部分从零开始实现，有些部分采用某些标准的开源组件，还有一些部分是在成熟框架上进行优化和改进。

- ✧ **账户中心（Account）**：公私钥生成，公钥写入，私钥签名与管理；应用层用户信息与区块链地址的映射；支持实名认证及审计的监管需求。
- ✧ **分布式账本服务（Distributed Ledger Service）**：基于 P2P 协议的底层组网，各节点通过 P2P 协议进行消息分发；提供账本结构的定义和账本数据的存储；可插拔的共识模块，负责确保底层数据强一致性的同时抵抗来自“恶意”节点的攻击。针对应用的建模适配，包括对资产、记录、事务、合约等多种对象的建模和实现。
- ✧ **策略与管理（Management）**：提供完备的数据隐私安全及访问策略控制的解决方案。多种可视化管理工具，底层区块链的健康监控、系统参数配置、数据分析、区块链浏览器等。

4.1 账户中心

在区块链技术自有的公私钥体系下，账户中心负责：公私钥生成，公钥写入，私钥签名与管理；保存应用层用户信息与区块链地址映射关系；支持实名认证及审计的监管需求。为应用适配层提供两类接口：非托管型接口和托管型接口。

非托管型接口：适合有能力在应用端实现安全级别较高的私钥生成和使用的企业机构。例如，在金融领域，将私钥的生成与管理跟现有的 U 盾、电子签名等安全的客户端体系相结合。

托管型接口：适用于互联网化程度较高的应用场景。公私钥直接作为用户名和密码使用对普通用户来说识记成本高体验差，大多数用户习惯用手机号、邮箱、昵称等作为用户名。因此，在托管型接口里，通过安全的私钥生成与管理的体系，应用层用户信息与区块链地址映射，使上层应用和底层区块链平台都无法触碰到用户的私钥。

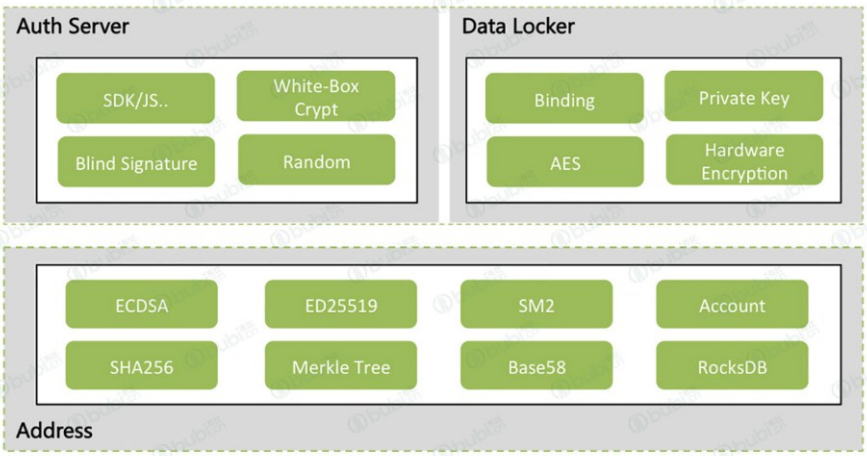

图 4-2 账户中心

托管型接口使用账户中心架构，由鉴权服务（Auth Server）、私钥保险箱（Data Locker）、区块链账户树（Address）三部分构成，如图 4-2 所示。

- **鉴权服务**

鉴权服务主要解决第三方应用与账户中心的安全问题。通过在交互过程中加入随机数和盲签名技术，增强密钥安全，降低暴力破解的可能性；同时利用白盒加密技术强化客户端的访问安全。

- **私钥保险箱**

私钥的写入和读取在保险箱体系里以密文的方式传输和存储。用户与密钥一一对应。密钥在客户端侧生成且客户端不用保存，每次需要使用私钥签名时，客户端能够通过盲签名流程得到加密过的私钥以及解密的密钥。

- **区块链账户树**

布比区块链上存储完整的账户树，每个叶子节点记录一个账户的资产信息和身份信息（可选）；每个账户可以支撑多维资产的使用。支持多种加解密算法，依据不同场景选择使用。

4.2 分布式账本服务

布比区块链底层服务由 P2P 组网、分布式账本、共识服务三部分组成；同时，为方便应用层理解和对接，在分布式账本服务适配层抽象出应用组件。（如图 4-3 所示）

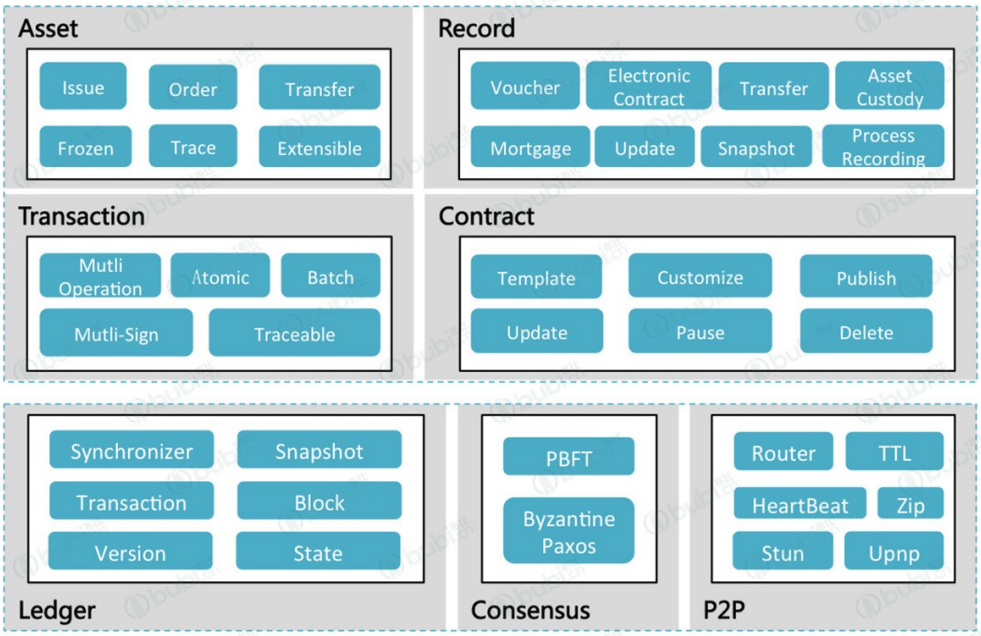

图 4-3 分布式账本服务

- **底层架构**

✓ **P2P 组网：**对等协议（Peer-to-Peer）实现基础组网和通信，每个节点维护一张邻居列表，实现动态自组织网络；并可与现有的安全防护设施配合使用，确保商用网络的安全性。

✓ **分布式账本：**解决数据格式、数据记录、数据存储问题，通俗的说就是“记什么账和如何记账”。因此分布式账本设计的好坏决定了区块链底层对外提供服务的能力。

✓ **共识服务：**是区块链的核心，也是区块链与传统分布式系统的最大区别之处。它保障底层数据的强一致性的同时，能抵抗“恶意”坏人的影响。布比的共识服务提供一组抽象的共识接口，用于连接共识算法和其它 BubiChain 模块。

它负责接受和处理 Transaction，并给出共识结果。共识服务采用开放式框架，可支撑不同种类的共识算法，目前布比已经开发 Byzantine Paxos、Byzantine Raft 商用共识算法，同时支持 PBFT 等共识算法，可以根据上层应用对性能、安全性、容错能力等需求选择不同的算法。

- **应用组件**

为方便应用层理解和对接，在分布式账本适配层抽象出：资产（Asset）、记录（Record）、事务（Transaction）、合约（Contract）等各类组件。

- ✓ **资产(Asset)**：支持目前已经数字化的资产，以及未来可以通过资产证券化、资产数字化的资产。
- ✓ **记录（Record）**：需要利用区块链增加信息记录的真实性和信任的场景，例如：金融领域的凭证、供应链的溯源信息等。
- ✓ **事务（Transaction）**：与区块链底层交互的原子级操作，一个上层应用可以对应一个事务，也可以由一组事务共同完成。
- ✓ **合约（Contract）**：提供两种合约——标准化合约、可编程合约。标准化合约，它主要针对场景相对简单、标准化程度较高，同时对执行效率有很高要求的业务需求。例如资产交换时的交易一致性保障、资产交易的挂单与撮合等。标准化合约可以通过配置生成直接挂在链上，无需编程，也不用通过虚拟执行，降低上层应用使用的成本，提升合约执行的效率。为了应对用户复杂的业务逻辑，布比也支持用户自编程，并且提供丰富的组件供用户针对特定的需求快速构建应用，如加密组件、权限管理组件等。同时布比对于通用的场景如资产、存证提供相应的模板，用户不需要从头编写代码，只需要更改模板的关键参数，加上自己业务的特性就可以建立成熟的合约应用。

4.3 策略与管理

布比区块链平台提供的安全与策略机制，既可以管理维护区块链系统本身的配置和安全，也可以管理区块链存储数据的访问策略和隐私安全。

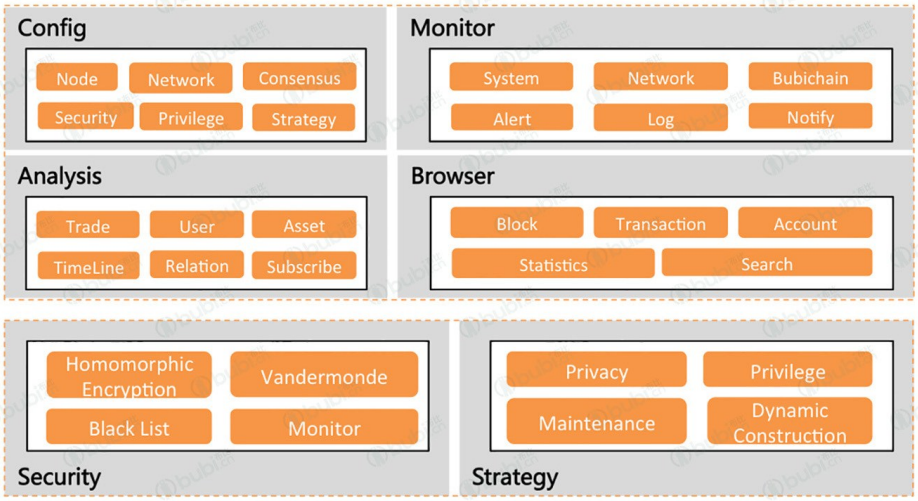

图 4-4 策略与管理

如图 4-4 所示，区块链底层提供安全（Security）与策略（Stratery）两个基础功能，应用适配层提供一系列可视化的管理工具，有配置管理（Config）、健康监控（Monitor）、数据分析（Analysis）、区块链浏览器（Browser）。

● 安全（Security）

底层安全服务负责解决系统组网、接口访问、共识算法、数据隐私等安全问题。目前，大多数行业应用都是联盟链和私有链。

✓ **系统组网安全：**组网方面可以用传统的一些安全措施进行加固：例如接入 IP 控制、专线、节点授权才能接入、节点信任列表等。

✓ **接口访问安全：**在接口层可以引入 CA 机制，只有授权的机构才能访问区块链平台的接口。

✓ **共识算法安全：**不同的共识算法都有一个安全边际，以 PBFT 为例，N/3 的安全问题是由配置决定的，安全性和容错能力在 2/3 阀值处于极大值。如果为了追求共识算法的安全，可以牺牲一部分容错能力，将投票通过阀值设置在 90%，甚至更高。同时还可以加入恶意节点发现与处理、黑白名单制等，加强共识算法的安全。

✓ **数据隐私安全：**区块链作为一个数据仓储的解决方案，它能提供的隐私保护

与传统的数据库没有太大区别：对称加密和非对称加密，常用的技术有同态加密和 RSA；隐私保护与区块链的数据共享信任之间的平衡是由业务场景来决定的。

- **策略（Stratery）**

策略服务除了提供上述的安全策略外，还包括节点部署策略、数据访问权限策略、多签名（Multisign）联合控制策略、合规性策略、性能策略等。

- **配置管理（Config）**

配置管理服务主要提供可视化的配置操作，针对上述的安全、策略、权限、区块链节点、分布式账本结构、共识算法、系统参数等进行灵活设置；配置本身也可以作为一种区块链的事务，由节点共同投票确定生效。

- **健康监控（Monitor）**

布比的区块链健康监控平台提供三个维度的监控：物理层（CPU、内存、磁盘等）、网络层（时延、断线）和业务层（区块生成、交易验证）；并且提供完善的告警、日志、消息通知机制体系，便于商用系统的运维。

- **数据分析（Analysis）**

分布式账本内存储的大部分是原数据，还有少量标准化的关联关系。为了满足上层应用各种复杂的数据分析需求，数据分析服务除了提供标准的数据查询接口，还支持批量导出和订阅式两种定制化的接口服务。

- **区块链浏览器（Browser）**

在不涉及隐私的情况下，区块链浏览器可以实时看到整个区块链底层存储的数据信息，包括区块信息（Block）、账户信息（Account）、交易信息（Transaction）、合约信息（Contract）等。

五. 技术特色与优势

通过大量业务模型、应用模型的数据测试分析，布比区块链在性能方面可达到：秒级交易验证、海量数据存储，高吞吐量、节点数据快速同步；在扩展性方面可达到：满足多业务区块结构、权限控制策略；同时，提供安全的私钥存取服务，以及隐私保护方案。

5.1 性能方面

- **快速交易验证**

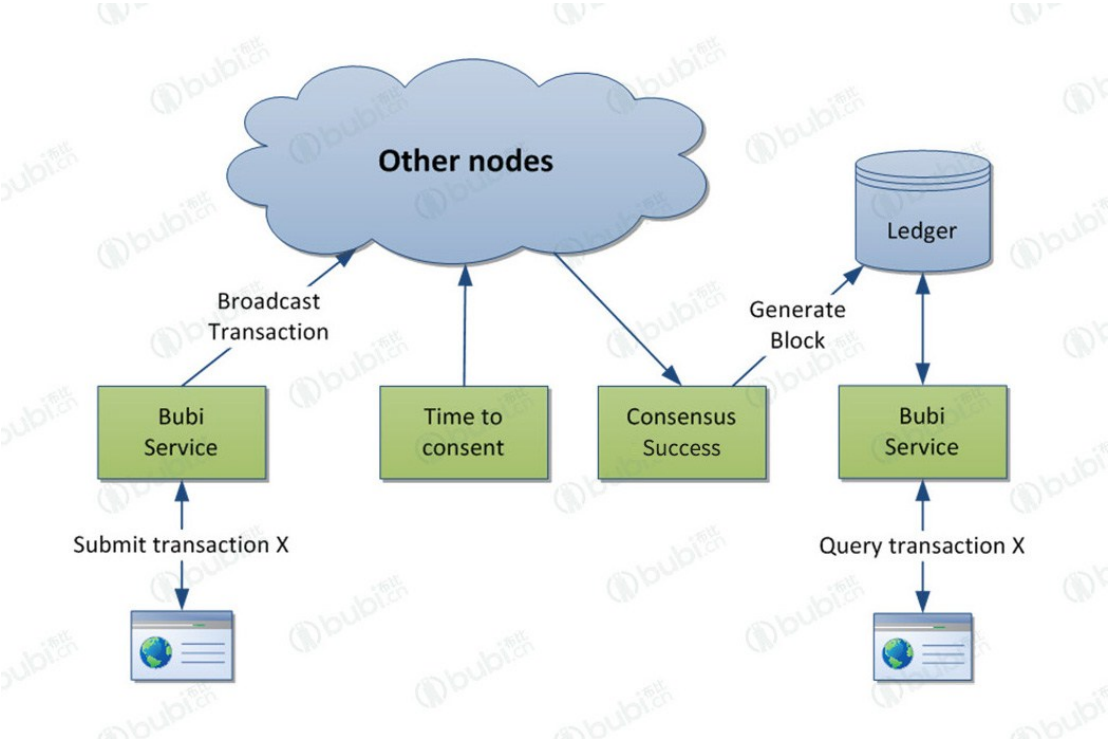

图 5-1 快速交易验证

通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，布比区块链可以实现秒级的快速交易验证。满足绝大部分区块链应用场景的用户体验。

- **海量数据存储**

区块链复式记账的模式，在系统长时间运行下，历史数据不断累积；布比区

块链借鉴传统金融系统中冷热数据分离存储、分表存储的机制，实现海量数据的有效存储。旧的交易数据，非活跃的资产数据等信息可以使用大数据存储平台进行存储（如 Hadoop，满足 PB 级别的数据存储）。

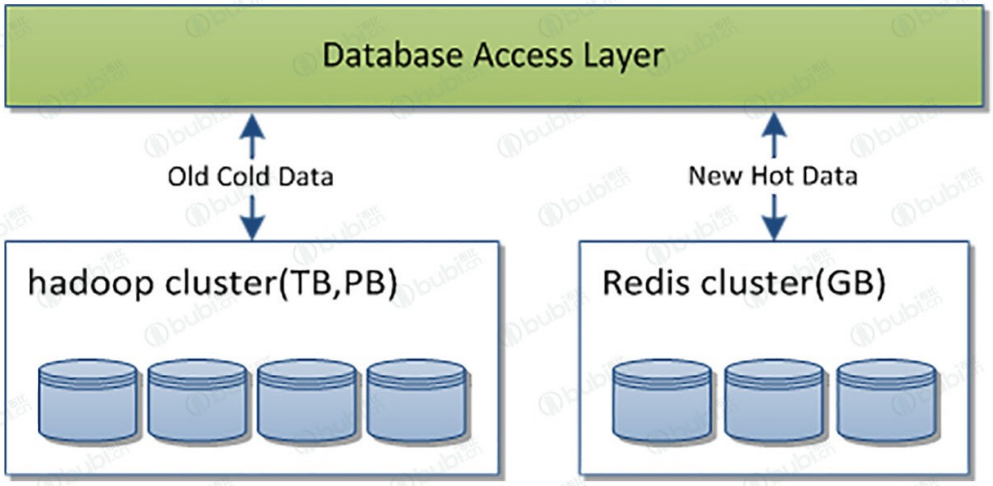

图 5-2 海量数据存储

- **高吞吐量**

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，布比区块链的处理性能已经能满足万级 TPS 的需求。如果再引入 Off-Chain 等机制，还能进一步大幅提高交易吞吐量。

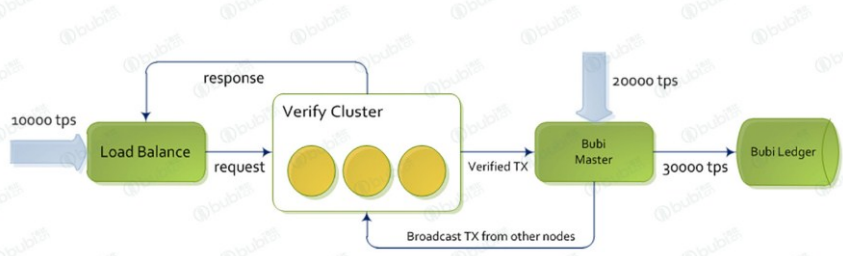

图 5-3 高吞吐量

- **节点数据快速同步**

布比区块链支持镜像(Snapshot)机制，可以定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚；同时，缩短新加节点加入运转的周期，仅需同步最新镜像及少量近期交易集合，即可融入网络并参与共识验证。

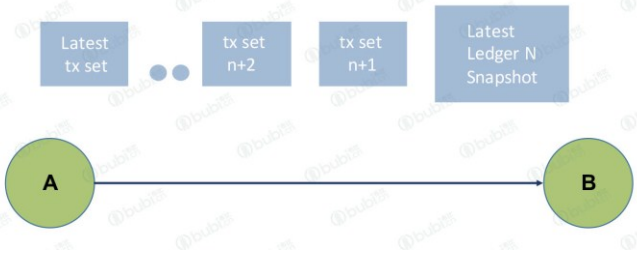

图 5-4 节点数据快速同

5.2 扩展性方面

- **满足多业务的块链结构**

布比区块链的块链结构，能够满足不同业务领域的需求，提高系统的可扩展能力和维护效率。即可用于标记资产和资产转移，也可提供不可篡改的多维事件记录，还可以用于溯源以跟踪物品的流通过程。

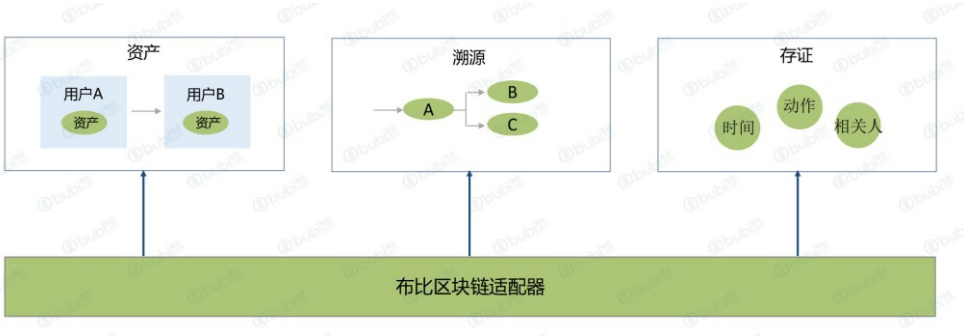

图 5-5 多业务块链结构

- **权限控制策略**

提供数据信息写入与读取两类权限控制策略。数据信息写入权限，同一账户

下设置多个使用用户，并针对不同的操作设置相应的权限，满足多方签名控制的使用场景。数据信息读取权限，用户可以授予和撤回单用户或用户组对数据的操作权限，用户组可以由用户灵活配置。数据包括用户账户信息，交易信息等，粒度可以细化到交易或账户的各属性字段。

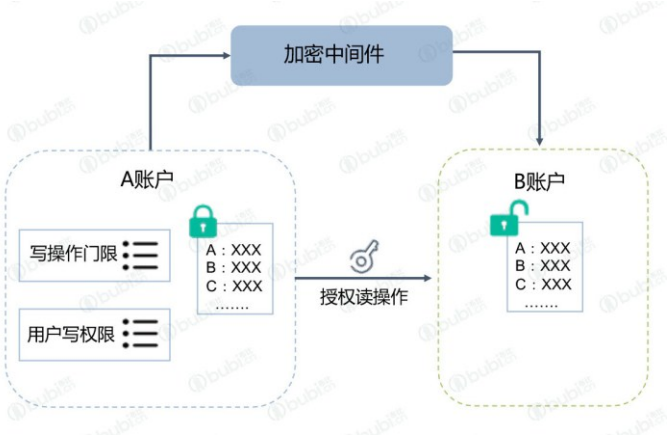

图 5-6 权限控制

5.3 安全方面

- **安全私钥存取**

为了方便用户使用区块链产品服务，除了传统的客户端生成和保存的机制，布比还提供网络托管存取和私钥硬件存取（U-key）两种方案。网络托管存取，即把用户名和密码通过特定算法映射成私钥并在服务端进行存储。服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；硬件私钥是为了满足金融行业及物联网行业的使用需求。

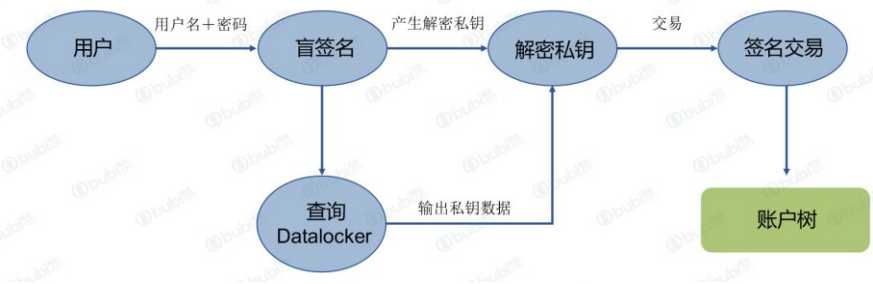

图 5-7 安全私钥存取

- **多重隐私保护方案**

提供多重隐私保护功能。首先，区块链底层提供同态加密方式，用户所有数据均加密存储，仅用户本身可见。其次，BubiAdaptors 提供加密中间件服务，用户可根据业务需要进行选择。最后，上层应用可以在录入时对数据进行加密处理，布比平台负责对用户生成的加密数据进行写入和读取。

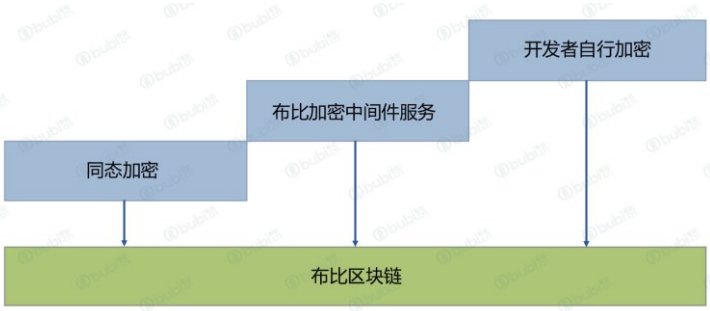

图 5-8 多重隐私保护方案

5.4 运维方面

- **全平台部署**

布比区块链的所有代码均可跨平台编译运行，平台相关代码均封装成基础库，业务逻辑独立于布比平台。除了 PC 及服务器的方式编译，同时支持交叉编译方式，如 ARM、MIPS 平台，方便在移动便携式系统部署，为区块链物联网化做预备支撑。同时，布比已与国内几家知名云平台达成战略合作，可以实现在云平台上快速部署。

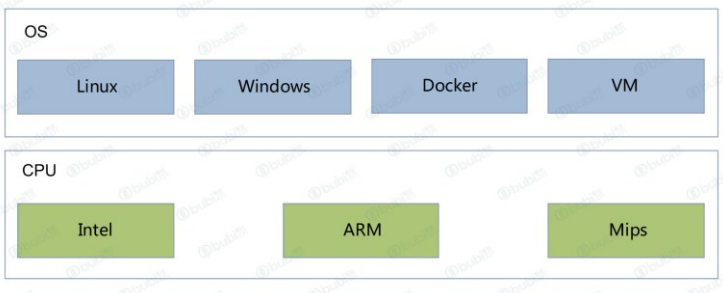

图 5-9 全平台部署

- **可视化运维**

提供运维管理所需的可视化工具。区块链节点上部署的系统监控服务（MonitorAgent）：支持业务（区块、交易、合约、共识等）、网络（组网、时延、吞吐量等）、系统层面（CPU、内存、磁盘等）的数据信息监控；同时提供完备的日志、告警与通知机制，便于商用系统的维护。

图 5-10 可视化运维

- **低成本接入方式**

BubiAdaptors 抽象出适用于多种业务场景的 API 接口，如：资产、溯源、存证等，供这些场景相关的业务直接使用。在新的业务场景下，布比可以基于现有的框架为用户快速定制接口，满足业务功能需求。同时提供已封装的支持多种主流开发语言（JAVA、C++、node-js、PHP）的 SDK 软件开发包。

图 5-11 低成本接入方式

目前区块链技术服务主要有两种：一种是搭建一套区块链底层，提供一套标准化的 API 并开放，然后由开发者自己对接应用；另外一种是配合上层应用解

决一些行业痛点，将分布式账本内嵌到已有的应用系统中。区块链是一项新兴技术，只有不断的满足业务需求，才能走向成熟，所以我们通过对底层分布式账本的封装，降低上层应用使用的门槛，在对接和使用的过程中，不断地优化和完善底层分布式账本和共识算法，使之更加贴近商用诉求。

六. 行业应用案例

以下是布比区块链已上线运行的几个行业应用案例，包括：数字资产的发行与流通，贸易金融/供应链金融，私有股权登记与转让，供应链溯源，公示公证，联合征信。

6.1 数字资产发行流通

相比于传统中心化系统，区块链应用于数字资产领域的优势在于：资产一旦在区块链上发行，后续流通环节可以不再依赖发行方系统，在流通中，资产由单中心控制变成社会化传播，任何有资源的渠道都可能成为资产流通的催化剂。因此，区块链能极大地提升数字资产流通效率，真正达到“多方发行、自由流通”。

传统的资产服务，需要相应的中间商，如资产所有者证明、真实性公证等均需要第三方的介入才可以完成，只有通过资产发行方、资产接收方、流通平台的三方介入，资产才可以完成整个流通过程。在目前的三方模式中，存在以下几个痛点：（1）资产进入流通后，仍必须依赖资产发行方系统才能完成使用、转移，这就将资产流通范围限制在发行方系统用户群内;（2）传统的资产流通渠道有限，几乎都依赖于大渠道，行业大渠道由于垄断地位大幅增加费用，从而导致流通成本显著提高，小渠道及个人难以在流通环节发挥作用。

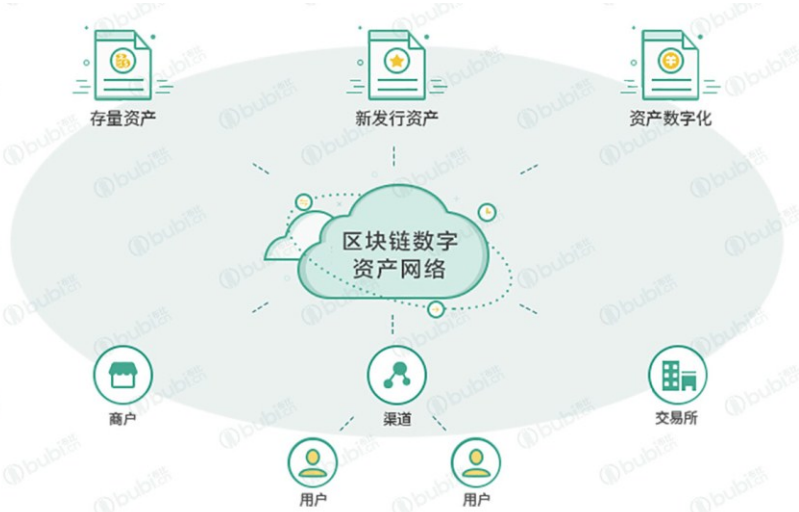

图 6-1 数字资产发行与流通

如图 6-1 所示，在数字资产发行与流通网络中，区块链用于资产登记、交易确认、记账对账和清算等。区块链数字资产网络，包括资产发行方、资产交易方、交易所、流通渠道在内的各个上下游机构，他们可以按照自身角色在链上自行开展业务。

- 任何可数字化的资产都可以在平台上实现登记、发行，各种主体（个人、机构）均可以在平台上登记、发行自己的数字资产。实现资产登记即公示，利于数字资产追踪查询，可以有效减少资产纠纷问题。
- 资产流通的核心是渠道，区块链技术使资产流通由原来的单中心控制变为社会化流通，任何有资源的渠道都可以成为资产流通的催化剂，促进流通、提高流通效率。
- 区块链“交易即结算”的基本特性使得实时清算成为可能，大幅提高交易后处理的效率，实现资产流通情况的实时查询功能。
- 数字资产可以是已经数字化的资产，可以成为资产证券化和资产数字化的入口，将现实资产映射成数字资产在链上发行与流通。

布比区块链正在被应用于商业积分、电子券、预付卡、游戏装备、保险卡单、资产证券化等。

6.2 贸易金融/供应链金融

贸易金融/供应链金融领域的业务链条中，天然就是多方参与协作。利用区块链，能将分散独立的各自单中心，提升为多方参与的统一多中心，打通贸易上下游各个环节，提高信任传递效率，降低交易成本，促进贸易金融的良性生态建设。

在贸易金融领域，信息散落在供应链各家自有系统中，流通和融资环节存在信息重复验证，效率低下；受各个供应链圈的信息流限制，中小企业和金融机构双向选择范围有限；缺乏统一可靠的中小企业征信系统，金融机构风控难度大，风控成本全部转嫁给融资企业。区块链可以促使供应链参与方共同创建和维护一份各环节都认可的统一凭证，并保障其真实有效、不可篡改；除了凭证的共享，项目/合同执行的过程也可以完整记录和跟踪，降低金融机构的风控难度，提升中小企业融资的可行性，降低融资成本；淡化供应链固有的圈子，扩大凭证授信范围，成为资产证券化、数字化的入口，增强流通性；链信息的记录和积累，也是企业自征信的过程，基于这些征信数据，可以展开各种金融服务。

图 6-2 区块链贸易金融

- 统一凭证，保障唯一真实性，极大降低核验成本；
- 过程可视，增强履约透明度，提高融资管理能力；
- 数据记录，促进征信的体系，减小风险控制成本。

布比区块链正在被应用于仓单质押融资、应收账款融资、票据托管贴现、消费金融理财、大宗商品交易等。

6.3 私有股权登记转让

应用区块链技术的加密股权、债券等证券化资产，有助于完善登记与流转服务，尤其是区块链构建的多中心体系，能够大幅地提升资产跨域流通效率，降低交易成本，使管理更安全、高效、可信、低成本、合规。

目前，股权登记需要人工处理，股东名册维护繁琐、历史交易维护与跟踪十分困难。传统股权交易，以双方信用为基础，需要建立双边授信后才可进行交易，信用风险由交易双方自行承担，而交易平台集中承担市场交易参与者的信用风险。

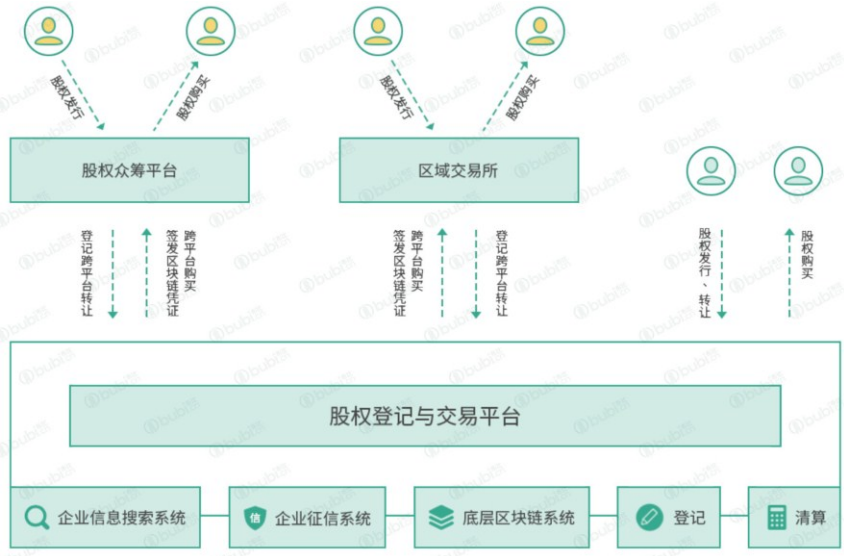

图 6-3 股权登记与转让

- 唯一真实的数字凭证，适于股权债券等证券化资产的登记；
- 跨域的多中心化信任，便于加密证券化资产的转让与交易；
- 增强的信息披露记录，易于符合监管满足合法合规性要求。

布比区块链正在被应用于众筹平台、区域股权交易中心、区域金融资产交易中心、私募管理平台等。

6.4 供应链溯源

区块链账本本身具有不可篡改性，链上各方共同参与账本信息维护，保证写入区块链的数据实时、有序、真实不可伪造。应用层支持多种实物扫码或编码录入方式进行商品溯源，杜绝物品身份的造假、恶意仿制放大流通量的情况。

如图 6-4 所示，布比区块链对供应链特性的支撑，使每一个物品静态（固有特性）和动态（流转、信用等）信息能够在生产制造企业、仓储企业、物流企业、各级分销商、零售商、电商、消费者以及政府监管机构中共享、共识。区块链平台在链接商品供应链权属关系和上下游关系的同时，还可以有效链接了间接发生关系的上下游企业。

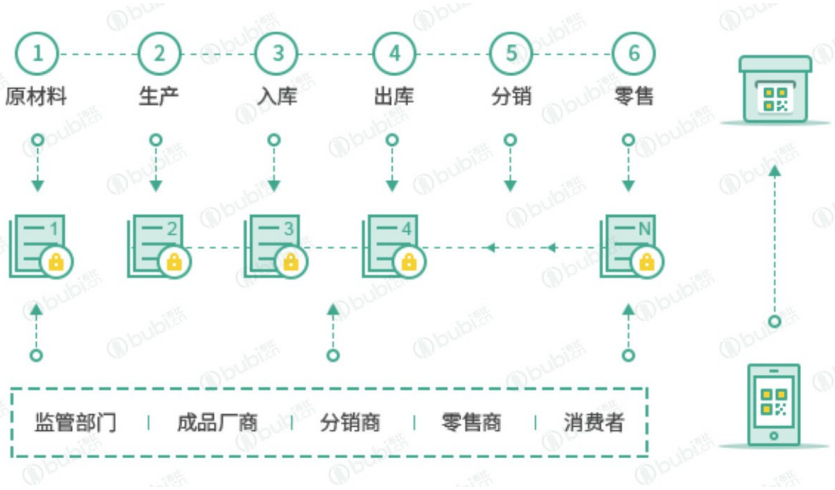

图 6-4 区块链供应链溯源

- 信息记录：每个物品的关键信息会以明文或加密方式记录到区块链中，公开不可篡改的区块链属性，防止数据伪造。
- 信息跟踪：商品码信息是平台中标识一个物品的唯一加密字串，也称为“一物一码”。通过使用智能手机、便携或大型射频、传感器装备等对物品的商品码进行自动识别，透明的共享的过程，连接商品权属及转移关系。
- 多方参与：基于区块链开放、共识、多中心网络信任特性，企业不仅能够可靠的掌握上下游企业情况、建立交易关系、跟踪交易状况，了解间接环节直至最终消费者的状况；同时提供监管方介入接口，有利于政府/市场监督。
- 最终实现：对品质型商品、作品的价值保护；对流通渠道和最终消费者的保

护；具有公信力的价值转移和再生。

布比区块链正在被应用于食品、药品、消费品、艺术品等。

6.5 公示公证

在信息公示中，公示主体的公信力是核心。因为数据完全受控于系统管理者，所以即使在数据时代，公信力的缺失问题并没有被有效解决。区块链的不可篡改、不可抵赖的特征，能够提高公示主体的公信力，打造新一代信息公示服务。

公示需求由来已久，在没有信息化技术之前，张榜公布、立碑刻字是曾经较为广泛采用的“公示”形式。公示的本质就是通过将信息公开化获得大众群体的确认及共识，这与区块链达成共识后不可篡改的本质具有异曲同工之处。区块链技术本身是提高公信力的有效途径：一是让更多的人知悉，从而提升抵赖难度；二是利用特殊介质，增强物理凭据的存在。

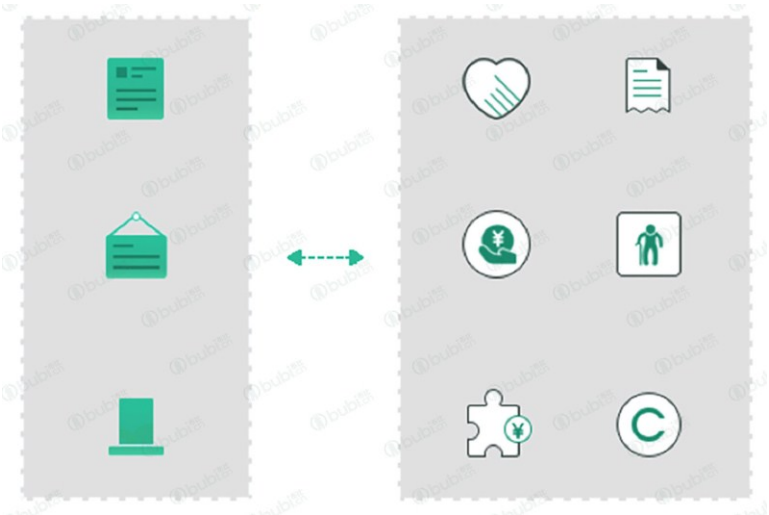

图 6-5 区块链公示公证

- 区块链是解决公信力的利器。区块链之所以能提高公信力，是因为它具有不可篡改、不可抵赖的特征。
- 公示中的“隐私保护”。由于数据本身并不能被篡改，所以在信息公示中，无论支持隐私保护和权限控制，或是支持完全公开和授权访问，都不会降低公示的公信力。

布比区块链正在被应用于慈善公益、养老扶贫、互助保险、网贷众筹、版权登记、政务公示等。

6.6 联合征信

目前，征信通常是单中心模式，即单机构通过自己的数据收集能力和信用做背书，进行风控和征信系统的开发和维护，为其它机构及个人客户提供有偿的征信服务。

单中心的征信模式有几个明显的弊端：首先，单中心维护数据信用的成本过高，包括系统建设的成本和数据审核的成本；其次，单中心提供的征信服务使用范围有限，只有密切合作并且充分信任的机构才会认可。

图 6-6 区块链联合征信

随着区块链技术在各个领域的点滴渗透，单中心维护的信用体系将被改善；由区块链构建多中心体系下的联合征信优势在于：

- 降低征信成本：联合征信的可充分保护各方数据隐私的基础上，实现成本分摊式的征信系统搭建，降低单中心系统构建和维护的成本，从而降低整个征信平台的使用成本。
- 扩大征信服务使用范围：征信数据的录入和累积，由上下游参与方共同验证和维护，这种方式产生的征信服务，将大幅提升使用范围。

- 数据自征信：随着参与方越来越多，联合征信的生态越来越完善；企业、C端用户的数据不断积累，其实也在完成各自自征信的过程。
- 数据共享，互利共赢：区块链在底层提供数据确权、不可抵赖的访问记录、低成本的对账清算等功能；同一行业实现互利互惠的数据共享。

布比区块链正在被应用于黑名单共享、信贷记录共享等。