八斗金链区块链白皮书

V1.0

广州八斗金链科技有限公司

前言

区块链技术的诞生给数字经济时代带来了革命性的变化，它改变的不仅仅是技术，它更主要的是改变了人类生产协作方式的变化，是人与人之间的利益分配机制的变化，是在法律层面、规则层面，重构人们之间生产关系的协作关系的变化，真正意义上为数字经济提供了全新的价值转移通道,构建真实可信，公正透明的信任经济社会。

由于区块链带来的社会价值无可限量，近年来各国政府机构,国际货币基金组织以及标准、开源组织和产业联盟等在纷纷投入区块链产业的拉通和应用，并且在工信部于 2016 年正式发布的《中国区块链技术和应用发展白皮书》，这充分展示了国家层面对区块链技术的重视程度。

八斗金链顺应时代的潮流，厚积薄发，经过长时间在区块链技术领域以及应用领域的不断研究与实践，总结得出，区块链应用的市场需求大且极具前景，但是区块链在底层技术以及基础设施的支持对区块链应用落地亟待改善。因此八斗金链致力打造一个区块链全流程的一站式服务平台——金链 BaaS 平台，为技术人员提供区块链的部署、开发和测试、调试部署和运维的低门槛、高效率的区块链使用方式；为不同业务应用场景提供快速落地区块链应用的途径。同时八斗金链在区块链数字资产、共享经济、供应链等行业应用场景上不断探索创新总结，结合大数据、人工智能、物联网等新技术，与社会多方合作共同促进区块链生态发展。

《八斗金链区块链白皮书》针对当前区块链各行业痛点进行分析，结合自身在区块链应用落地的实践经验，给出基于八斗金链 BaaS 平台促进区块链应用场景落地的解决方案，期待携手合作伙伴共建区块链技术生态，共同推动“区块链可信数字经济社会”。

目录

1 概述

1.1 什么是区块链

区块链(Blockchain)是一种由多方共同维护,使用密码学保证传输和访问安全,能够实现数据一致存储、难以篡改、防止抵赖的记账技术,也称为分布式账本技术(Distributed Ledger Technology)。典型的区块链以块-链结构存储数据。作为一种在不可信的竞争环境中低成本建立信任的新型计算范式和协作模式,区块链凭借其独有的信任建立机制,正在改变诸多行业的应用场景和运行规则,是未来发展数字经济、构建新型信任体系不可或缺的技术之一。

典型的区块链系统中,各参与方按照事先约定的规则共同存储信息并达成共识。为了防止共识信息被篡改,系统以区块(Block)为单位存储数据,区块之间按照时间顺序、结合密码学算法构成链式(Chain)数据结构,通过共识机制选出记录节点,由该节点决定最新区块的数据,其他节点共同参与最新区块数据的验证、存储和维护,数据一经确认,就难以删除和更改,只能进行授权查询操作。按照系统是否具有节点准入机制,区块链可分类为许可链和非许可链。许可链中节点的加入退出需要区块链系统的许可,根据拥有控制权限的主体是否集中可分为联盟链 1 和私有链 2 ;非许可链则是完全开放的,亦可称为公有链 3 ,节点可以随时自由加入和退出。

1.2 区块链的价值介绍

从上世纪末的“深蓝”大战，到最近的“阿发狗” 案例，我们能够感受到 AI 技术在快速发展，且其发展速度会超越人的意料之外。很自然地我们可以想象到下面的场景：未来人们周围将被智能设备所包裹。

面对如此多样而分散的智能设备，现实却存在像设备标识不统一、数据协议不统一、服务界面不统一等等不足，缺乏统一的基础共识机制导致诸如厂家间的博弈鸿沟使得“小白”用户无所适从、分散设备很难被有机整合形成群集智慧、产生海量数据却无法有效流动和应用等等问题，使得这些智能设备不能更好地服

务于大众。这些本质上因缺乏“共识”而导致的困境恰恰是比特币区块链技术可以充分发挥关键作用的场景。

区块链技术为世界带来最大的改变即将是：全面颠覆了过去的那一套中心化的信任机制。它用分布式计算的一致性算法和区块链的链式数据存储机制，让参与各方（也就是在数字世界中代表我们的计算机）基于算法形成了信任。从而创造一种全新的信任共识机制，不需要第三方参与。通过区块链技术建立一种网络结构，所有人都可以参与成为无数节点之一，进行认证、确权、交易、追溯和调整等一系列动作。它公开透明、没有权威可以篡改、伪造、取缔记录。

1.3 区块链应用方向介绍

根据实现方式和作用目的的不同,当前基于区块链技术的应用可

以划分为三类场景,一是价值转移类,数字资产在不同账户之间转移,如跨境支付;二是存证类,将信息记录到区块链上,但无资产转移,如电子合同;三是授权管理类,利用智能合约控制数据访问,如数据共享。此外,随着应用需求的不断升级,还存在多类型融合的场景。

类型	政府	金融	工业	医疗	法律	版权
价值转移		数字票据 跨境支付 应收账款 供应链金融	能源交易	医疗保险		
存证	电子发票 电子证照 精准扶贫	现钞冠字号 溯源 供应链金融	防伪溯源	电子病历 药品追溯	公证 电子存证 网络仲裁	版权确权

授权管理	政府数据共享	征信		健康数据共享		版权管理

1.4 主流的区块链技术介绍

1.4.1 区块链技术体系介绍

区块链本质上是一种健壮和安全的分布式状态机,典型的技术构成包括共识算法、P2P 通讯、密码学、数据库技术和虚拟机。这也构成了区块链必不可少的 4 项核心技术：

- 分布式存储

  区块链账本采用的是分布式存储记账方式，这是一种从分布在不同物理地址或不同组织内的多个网络节点构成的网络中进行数据分享与同步的去中心化数据存储技术。

- 密码学

  区块链中使用了哈希算法、加解密算法、数字证书与签名、零知识证明等现代密码学的多项技术。区块链采用哈希算法和非对称加密技术来保证账本的完整性和网络传输安全。

- 共识机制

共识机制用于解决分布式系统的一致性问题，其核心为在某个共识算法的保障下，在有限的时间里，使得制定操作在分布式网络中是一致的、被承认的、不可篡改的。在区块链中，特定的共识算法用于解决去中心化多方互信的问题。

主流的共识算法对比：

特性	**PoW**	**PoS**	**DPoS**	**PBFT**	**VRF**
节点管理	无许可	无许可	无许可	需许可	需许可
交易延时	高	低	低	低	低
吞吐量	低	高	高	高	高
安全边界	恶意算力不	恶意算力不	恶意算力不	恶意算力不	恶意算力不

	超过 1/2	超过 1/2	超过 1/2	超过 1/3	超过 1/3
代表应用	Bitcoin、Ethereum	Peercoin	Bitshare	Fabirc0.6	Algorand
扩展性	好	好	好	差	差

- 智能合约

区块链智能合约是一段写在区块链上的代码，一旦某个事件触发合约中的条款，代码即自动执行。目前较为成熟的智能合约支持图灵完备的语言，无须依赖第三方或中心化机构，极大地减少了人工参与，具备很高的效率和准确性。

智能合约根据图灵完备与否可以分为两类,即图灵完备和非图灵完备。影响实现图灵完备的常见原因包括:循环或递归受限、无法实现数组或更复杂的数据结构等。图灵完备的智能合约有较强适应性,可以对逻辑较复杂的业务操作进行编程,但有陷入死循环的可能。对比而言,图灵不完备的智能合约虽然不能进行复杂逻辑操作,但更加简单、高效和安全。

1.4.2 公有链

区块链平台根据去中心化程度、应用场景的不同,可划分为三类:公有链、联盟链、私有链。不同区块链平台在准入机制、共识算法等诸多方面均存在差异。

公有链常被形象化为“区块链世界的操作系统”,此类区块链平台允许节点自由加入网络,且所有节点均有权限查看账本信息。典型的、当前应用最为广泛的公有链平台为以太坊。以太坊提供了图灵完备的编程语言,允许开发者部署智能合约,可帮助处理复杂业务流程。然而,受限于交易处理速度、可扩展性等,以上公链平台难以进行大规模商业应用落地。自 2017 年以来,区块链逐步成为能够构建更高效社会活动的一种社会关系,成为能够减少摩擦提高效率的新范式。业界开始追求公链底层技术新的突破,探索更加普适、稳定的公链平台,并将基于该类平台的下一个时代定义为区块链 3.0。

1.4.3 联盟链

联盟链通常被用于政府机构、商业机构及公司之间,节点通过准入机制得到授权后方可加入,不同节点所拥有的信息查看权限不同。典型的区块链联盟项目如超级账本(Hyperleger)、R3。超级账本(Hyperledger)项目由 Linux 基金会发起,旨在构建跨行业开源区块链商业平台,推动各行业成员协同合作、共建开放平台、简化业务流程。其中,专注于提供企业级区块链解决方案的 IBM HyperLeger(也即 Fabric)区块链平台备受关注。R3 是由美国初创公司 R3CEV 发起的金融行业区块链联盟,目前已吸引多家国内外金融机构加盟。该项目旨在为银行业提供探索区块链技术的渠道,同时开发分布式账本平台 Corda。

1.4.4 主流联盟链技术介绍-Hyperledger Fabric

超级账本（Hyperledger）项目是首个面向企业应用场景的开源分布式账本平台。由 Linux 基金会牵头，包括 IBM 等 30 家初始企业成员共同成立的。

Hyperledger Fabric 定位是面向企业的分布式账本平台，引入权限管理，设计上支持可插拔、可扩展，是首个面向联盟链场景的开源项目。像其他区块链技术一样,它有一个账本,使用智能合约,是一个由参与者共同管理交易的系统。与其它区块链系统最大的不同点在于 HyperLedger Fabric 是基于联盟，具有许可机制的，但并不允许未知身份来参与 HyperLedger Fabric 网络（要求协议验证事务并确保网络的安全），HyperLedger Fabric 组织的成员可以通过一个 Membership Service Provider（成员服务提供者即 MSP）来注册。

Hyperledger Fabric 还提供创建通道(Channel) 的能力,每个参与者都保存着一个区块链账本的副本，所有参与者通过协作共同维护着账本。超级账本的总账子系统包括两部分：世界状态与交易日志。Fabric 的每个参与者都持有一份账本副本。世界状态部分描述了账本在某个时间点的状态。它是账本的数据库。交易日志部分则记录了导致当前世界状态的所有交易，是世界状态的历史记录。账本是世界状态与交易日志的结合。

Hyperledger Fabric 是一个由多节点组成的网络，分别是排序节点

(Orderer)、背书节点(Endorser Peer) 和记账节点 (Committer Peer)。不同类型的节点担当不同的角色，Hyperledger Fabric 中的交易信息统一由排序服务节点处理,保证每个节点上的交易顺序一致,天然避免了分叉问题。每个参与区块链网络的组织,可以控制多个节点,以解决组织间权利不对等的问题。

Fabric 引入只能合约实现对账本的访问与控制 ,智能合约也叫链码(Chaincode),可以用 Node.js、Java 和 Go 等语言进行开发。Fabric 上的链码分为系统链码和用户链码。系统链码用于实现系统层级的功能,包括系统的配置,用户链码的部署、升级,用户交易的签名和验证策略等。用户链码用于实现用户的应用功能,即具体的业务逻辑。智能合约运行在一个被背书 Peer 进程独立出来的安全的 Docker 容器中。智能合约通过应用程序提交的事务初始化和管理账本状态。

1.4.5 主流公有链技术介绍- Ethereum

Ethereum (以太坊) 是一个基于区块链技术的去中心化应用平台,它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。

以太坊普遍被认为是区块链 2.0 时代的代表性产品,创始人 Vitalik Buterin 于 2013 年底发布了以太坊白皮书,标志着该项目正式启动。2015 年 7 月,发布了 Frontier 阶段,以太坊主网正式上线。2016 年以太坊发布了第二个重大版本 Homestead。 2017 年 10 月,以太坊发布了第三个版本的 Byzantium 部分。至此,以太坊已经发展成为了区块链世界最重要的一个平台,大量的 DApp (分布式应用) 基于以太坊来开发。就像比特币一样,以太坊是去中心化的,由全网共同记账,账本公开透明且不可篡改。没有任何人或者组织能够控制以太坊区块链,任何新添加的数据都需要获得全网的一致认可。

与比特币不同的是,以太坊是可编程的区块链,它提供了一套图灵完备的脚本语言。以太坊平台对底层区块链技术进行了封装,让区块链应用开发者直接基于以太坊平台进行开发,只须专注于应用本身而无须实现区块链底层代码。以太坊上的程序被称为智能合约,它是代码和数据 (状态) 的集合。开发人员可以直接用以太坊原生支持的 Solidity 语言编写和区块链交互的智能合约,大大降低了区块

链应用的开发难度。

EVM (以太坊虚拟机):EVM 是以太坊的核心,它能执行遵守协议的任何复杂的代码。EVM 是图灵完备的,开发者可以在虚拟机上使用 Solidity 编程语言来创建应用。智能合约与链上数据的交互,也由 EVM 负责中间的交互过程。EVM 是以太坊智能合约的运行时环境.它不仅仅是个沙盒,而是完全隔离的。这意味着代码在 EVM 中运行时没有办法连接网络,文件系统或者其他进程,甚至一个智能合约没有办法访问另一个智能合约。为了解决支持图灵完备下的可终止性问题以及避免网络滥用,以太坊引入了 Gas 概念。EVM 中的每步操作和每个账本存储都会对应于一定的 Gas 消耗;当 Gas 消耗完后合约即会被终止。Gas 方式相当于即时付费的手续费模式,目前被大多数的公有区块链平台所采用。账号是以太坊的基本单元,每一个账号都有一个 20 个字节长度的地址。以太坊区块链跟踪每一个账号的状态,区块链上所有状态的转移都是账户之间的以太币和信息的转移。以太坊有 2 种账户类型,外部账号简称 EOA,是由私钥来控制的。合约帐户,由合约代码来控制,且只能由一个 EOA 账号来操作。

交易在以太坊中是指签名的数据包,这个数据包中存储了从外部账户发送的消息,交易包含以下内容:

- 消息的接收者;
- 一个可以识别发送者的签名;
- 发送方给接收方的以太币的数量;
- 一个可选的数据字段;
- 一个 GasLimit 值, 表示执行这个交易允许消耗的最大计算步骤;
- 一个 GasPrice 值, 表示发送方的每个计算步骤的费用。

目前以太坊采用了 ethash 共识算法,本质上这是 PoW 共识算法。依靠大量的哈希计算来找出一个符合规定难度的当前区块的哈希值,以此来证明记账节点的工作量。其优点是安全可靠,缺点是耗费了大量的能源。

1.4.6 主流公有链技术介绍-IPFS

IPFS 全称 InterPlanetary File System，中文名：星际文件系统，是一个旨在创建持久且分布式存储和共享文件的网络传输协议。它是一种内容可寻址的对等超媒体分发协议。在 IPFS 网络中的节点将构成一个分布式文件系统。它是一个开放源代码项目，自 2014 年开始由 Protocol Labs （协议实验室）在开源社区的帮助下发展。其最初由 Juan Benet 设计。

IPFS 是点对点的超媒体协议，可以让网络更快、更安全、更开放。它是一个面向全球的、点对点的分布式版本文件系统，试图将所有具有相同文件系统的计算设备连接在一起。

IPFS 的工作原理：

- 每个文件及其中的所有块都被赋予一个称为加密散列的唯一指纹。
- IPFS 通过网络删除重复具有相同哈希值的文件，通过计算是可以判断哪些文件是冗余重复的。并跟踪每个文件的版本历史记录。
- 每个网络节点只存储它感兴趣的内容，以及一些索引信息，有助于弄清楚谁在存储什么。
- 查找文件时，你通过文件的哈希值就可以在网络查找到储存改文件的节点，找到想要的文件。
- 使用称为 IPNS（去中心化命名系统），每个文件都可以被协作命名为易读的名字。通过搜索，就能很容易地找到想要查看的文件。
- 从 IPFS 的介绍可以看出， IPFS 设想的是让所有的网络终端节点不仅仅只充当 Browser 或 Client 的角色，其实人人都可以作为这个网络的运营者，人人都可以是服务器。

1.5 当前企业级区块链发展现状

1.5.1 存在问题分析

通过使用区块链技术能够有效达到企业效率提升和成本降低的目标,为经济社会发展和治理提供新的思路。依托区块链技术构建的经济生态,能够创造出丰富的产品和服务,人们基于一个可信体系,无地域限制地进行大规模协作。由此,一个全新的经济时代展现在公众面前。

区块链的行业应用正在加速推进,由数字货币等金融应用向非金融领域进行渗透扩散。企业应用是区块链的主战场,具有安全准入控制机制的联盟链和私有链将成为主趋势。区块链行业应用具有明显的效益的显著优势在于优化业务流程、降低运营成本、提升协同效率,这个优势已经在金融服务、物联网、公共服务、社会公益和供应链管理等社会领域逐步体现出来,但是区块链的技术发展却还没有到达成熟阶段,尤其在企业级应用方面,区块链的交易并发能力、数据存储能力、通用性、 功能完备性、易用性都还存在明显不足。

- 高并发交易能力

企业场景下的交易并发量通常要求在每秒处理数百至数千笔以上的交易,远高于目前包括公有链、联盟链在内的典型区块链的表现,而且还要求区块链的性能表现可以随着业务规模的增长而动态伸缩。因此,现实和目标之间存在数量级的差别,需要持续优化和提升区块链系统高并发交易性能。

- 数据存储能力

数据存储能力方面,目前开源的区块链技术，在数据存储方面的典型的实现是基于文件系统或者简单的 KV 数据库存储,没有使用分布式存储，随着时间推移,区块链系统对数据存储大小的需要也只能持续地增大，因此数据存储的扩展性比较低，目前不适用大部分的企业场景。

- 通用性方面

区块链需要适应多样化的业务需求,满足跨企业的业务链条上的数据共享,这意味着区块链对数据的记录方式要有足够的通用和标准,才能表示各种结构化和非

结构化的信息,并能够满足随着业务范围拓展所需的跨链要求。

目前市面上的区块链系统大多采用特定的共识算法,加密算法,账户模型,账本模型,存储类型,缺少可插拔能力,无法适应不同场景要求。

- 功能完备性

纵观现有区块链平台,模型抽象单一,难以适应业务系统快速开发的要求。另外,缺少对企业应用中常见的一些功能的支持,例如用户认证、多级授权等。再者,涉及到企业业务协作时,跨企业的事件通知机制显得尤为重要,但少有区块链平台支持。

- 易用性

区块链是由多种技术构成,导致学习成本高,实施难度大,人才稀缺。如何让用户快速理解区块链,低成本学习区块链,并将区块链技术快速应到自身的业务中去,目前来看有很大的挑战。区块链技术需要降低学习和使用门槛,支持快速实施部署,提供贴近业务的接口,推广使用。

1.5.2 解决之道

区块链技术作为一种组合型的基础设施解决方案, 需要在普适行业的区块链技术基础上, 根据企业的特殊业务需求、现有技术水平以及法律法规等方面的要求或条件, 从业务适当性、性能、安全、政策、技术可行性、运维与治理、成本等多个维度进行综合考虑。

- 区块链系统的性能

企业在多种业务场景比如电商交易往往具有海量交易、高频交易、及时确认等特征, 因此需要根据不同企业的御武场景当前业务规模, 分析区块链系统需要支撑的业务量、潜在业务增长规模、并发业务量、响应时间等技术性能指标需求，需要根据不同的企业需求，选择使用不同的区块链技术。

- 区块链系统的安全性

区块链可以从技术层面保证记录数据的可信, 防止数据被篡改、伪造等风险。此外在数据敏感性与安全性上, 需要评估上链数据的内容加密强度, 以及访问权

限控制等。不同的企业业务场景需要根据业务的具体安全要求，选择成熟、合适、安全的加密算法。

- 业务场景的适当性

企业的业务场景是多样化的，但是并非所有的业务场景都需要采用区块链技术，一般而言，涉及到多方参与、对等合作的场景时，传统的集中式系统架构往往难以满足需求，则可考虑采用区块链技术，从而增加多方互信、提升业务运行效率、降低业务运营成本与摩擦成本。

- 政策合规性

区块链是一套技术解决方案，在合理设计的前提下，可以对现有的业务起到良好的支撑或对现有中心化系统进行很好的补充。但金融机构在使用区块链开展业务的过程中，必须在国家现有的监管要求与法律框架内施行。

- 技术可行性

区块链技术已经在部分金融场景中落地，但目前还属于一项新兴技术，需要充分评估该技术与具体业务的契合度、及其与传统系统相比的优劣势后，最终选择合适的区块链平台进行论证与试运行。

- 运维与治理能力

由于基于区块链的业务与传统中心化系统在运营和管理上存在差异，而金融业务的持续治理要求极高，需要进行相应的规划与调整，评估新的治理结构的可行性、可持续性，评估版本迭代与系统正式上线的影响程度，实时监控区块链系统的运行，确保业务可控与金融环境稳定。

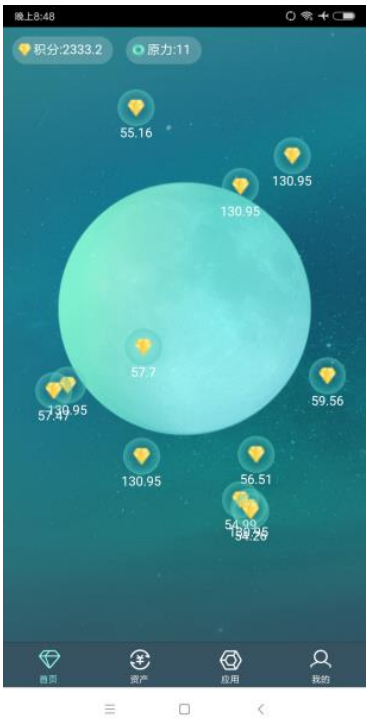
- 成本可控与经济可行

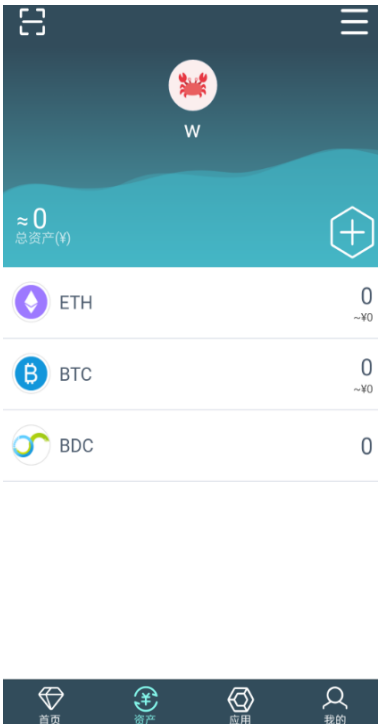
区块链应用通过技术特点来解决实际业务中的特定问题，有效解决痛点问题的应用可以为金融业务带来极大的收益，应用本身的价值也能得以显现；相反如果不能解决行业的重要问题，则需面临成本与收益的权衡取舍。

1.6 八斗金链在区块链的实践

1.6.1 区块链会员价值星球平台

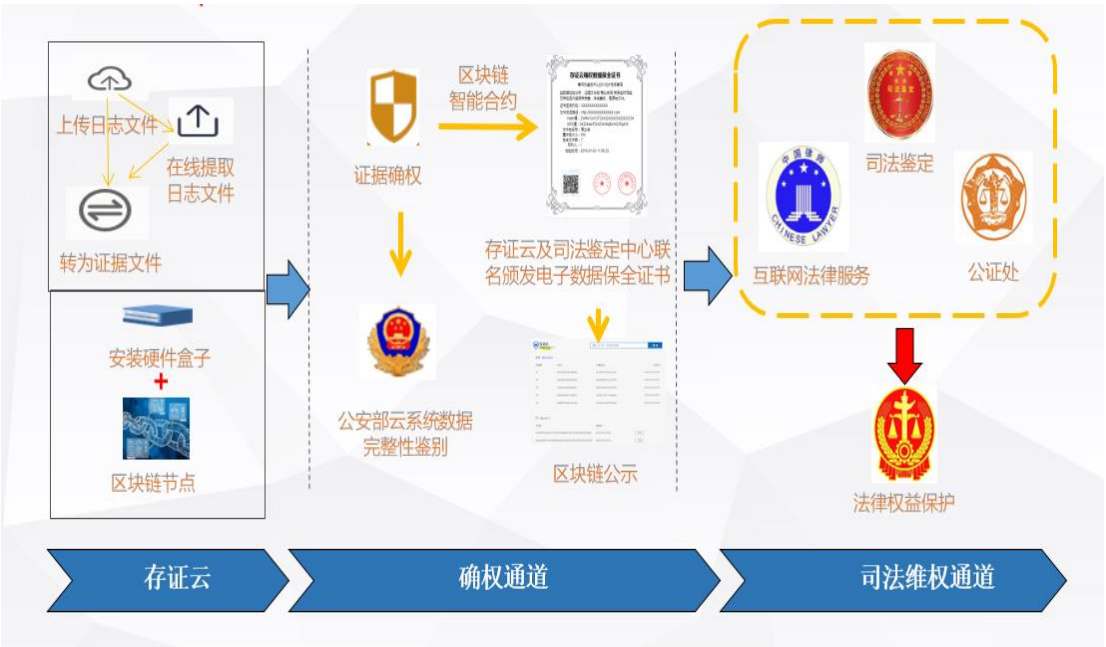
八斗金链搭建区块链会员价值星球平台，基于区块链技术打造的会员生态服务系统，主要由任务挖掘、好友互动、任务奖励、奖励应用、商城购物、钱包服务、数字货币交易等功能组成，为星球社区居民提供数字资产管理、增值和深耕等服务。





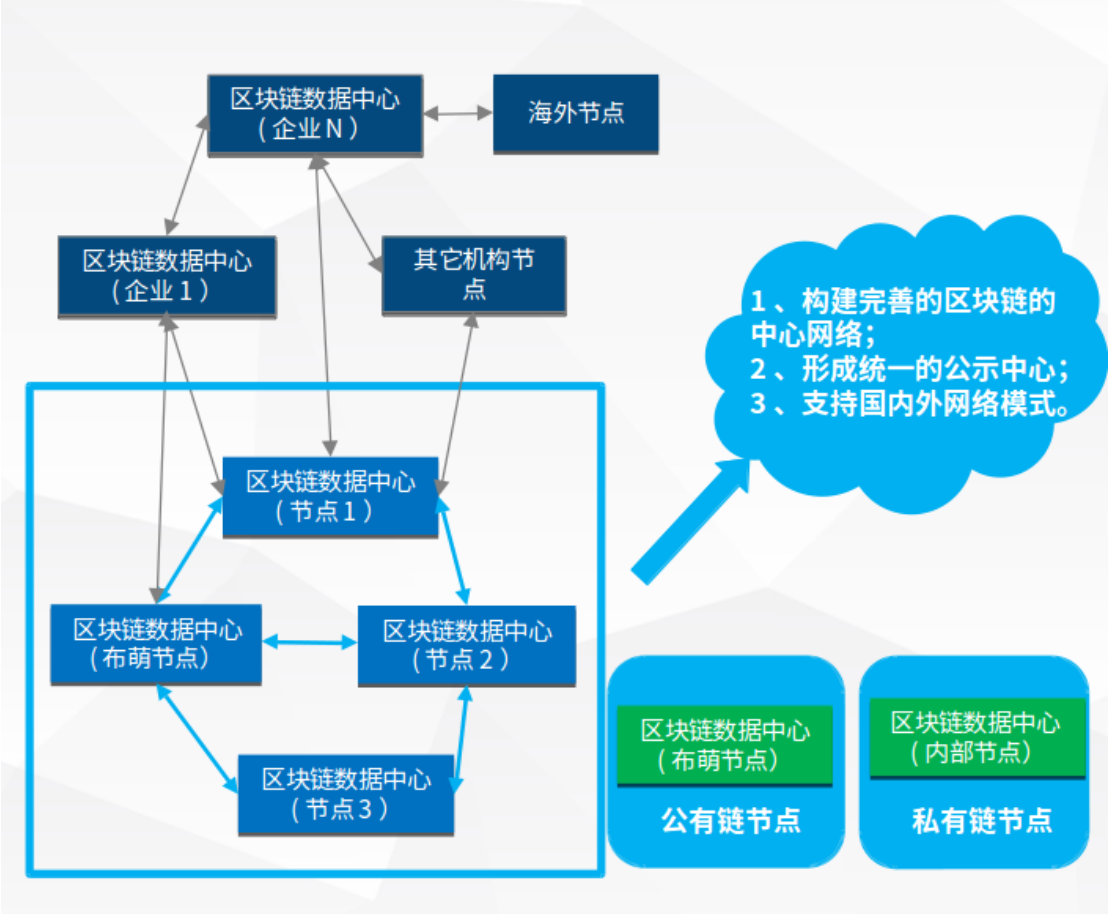
1.6.2 区块链电子证据平台

八斗金链搭建存证云平台，基于区块链技术实现可信的电子存证体系。存证云目前已建立超过 20 个区块链节点，正不断的邀请多方参与共同维护，目前国内云上节点阿里、腾讯（10 个）；海外节点-AWS（3 个）；合作伙伴企业节点（6 个）； 政府节点-电子口岸（2 个）；学校节点-桂大(2 个）。



1.6.3 区块链企业数据库

基于区块链建设的一个可信的企业数据中心，它将是一个既满足多方（企业、机构、政府等）对数据认证，数据不可篡改的准确有效的数据库，同时也兼顾高效存储、访问多方数据的信息化平台。区块链企业数据库是以块链式数据结构存储、分布式节点共识算法生成、密码学方式传输，使之具备不可篡改和不可伪造的特性，解决了数据被篡改的问题。结合区块链技术和大数据平台，建设一个既可信又高效的区块链数据中心。

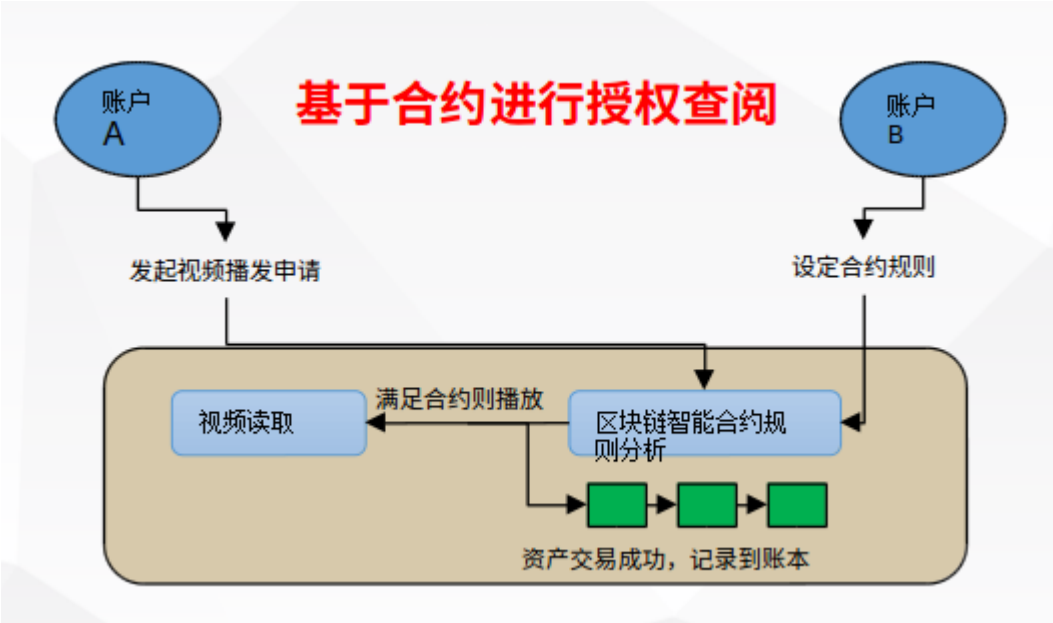


1.6.4 区块链视频数据中心

随着互联网、大数据等相关技术的发展，人们越来越重视数据的作用，开始探索将数据作为资产的可能性，但遗憾的是数据的可复制性与资产的唯一性是一对不可调和的矛盾，数据资源与物理资源最大的不同就在于其无可比拟的可复制性。

资产作为价值的载体，如果能被轻易复制，其价值自然会被稀释，为了避免这一点，当前的做法是由一个可信任的方式来掌握资产、确权资产，在有强信用背书的条件下保证经济活动正常运行。

八斗金链基于区块链技术搭建区块链视频数据中心，利用区块链去中心，不可篡改特性，实现视频资源的价值保障。


基于合约进行授权查阅
账户
A
账户
B
发起视频播发申请
设定合约规则
视频读取
满足合约则播放
区块链智能合约规则分析
资产交易成功，记录到账本

2 金链 BaaS 平台

2.1 BaaS 平台介绍

八斗金链基于区块链底层和应用开发技术，提供了企业级的区块链智能合约平台、应用开发平台、监控平台、证书管理和区块链浏览器等技术平台，基于区块链网络的搭建复杂、门槛极高，八斗金链提供区块链节点镜像，包含区块链网络和区块链企业级开发台，可以基于业务需求快速实现区块链应用的落地。建设具有高性能、良好扩展性、广泛场景通用性、安全合规、接口友好和易部署管理的区块链基础网络设施,打造开放共赢的区块链技术与服务生态。

- 从业务场景出发

企业落地区块链场景的需求多样化。八斗金链 BaaS 平台定位为企业级的区块链平台,需要适用广泛的企业场景,在设计上首先从定义企业场景的核心用例出发,设计八斗金链区块链的协议、数据结构和功能特性。

- 模块化设计

八斗金链区块链采用模块化设计,通过定义模块间清晰的接口实现模块之间的松耦合,以此获得整个系统的良好扩展性,系统可以根据不同用户和场景的需要,采用不同的可插拔的模块组件。

- 简洁与效率

八斗金链 BaaS 平台可靠和高效的运行来源于简洁的系统设计。八斗金链 BaaS 平台在协议设计、组件模型、系统实现、外部接口、部署管理各个方面都认真地遵循这一原则。

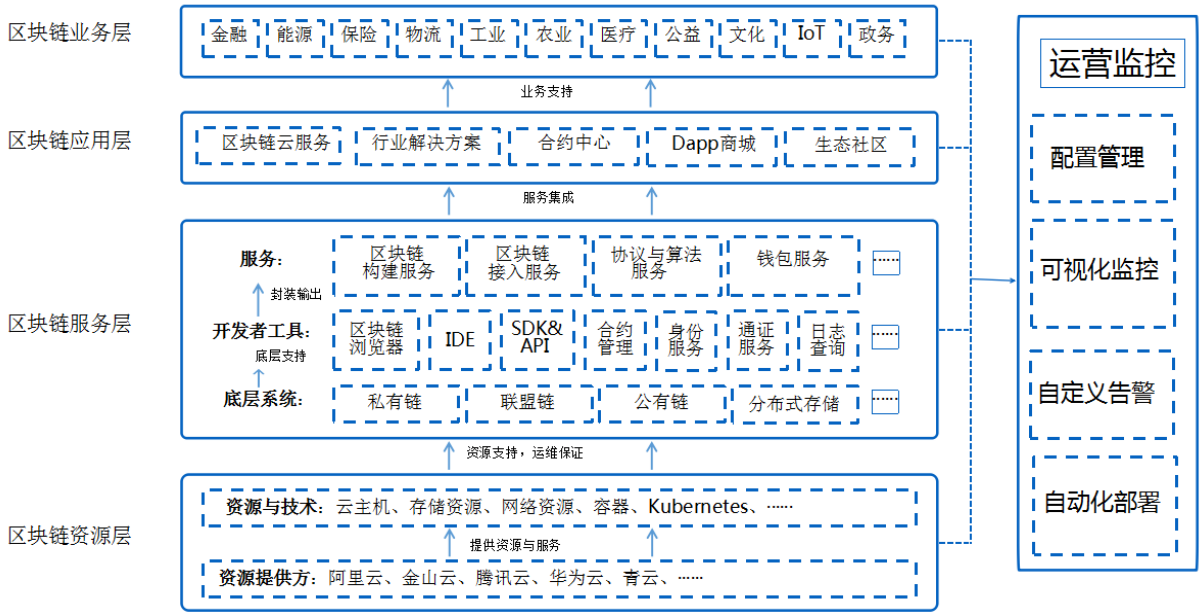
- 安全可审计

企业数据的保存需要满足“安全可审计”的要求,八斗金链 BaaS 平台在设计上将“安全可审计”作为十分关键的一条原则贯穿到每一个功能特性的设计和实现上,设计了可灵活定义的安全访问策略、基于密码学完整地标记数据变化的过

程、提供记录级的数据证明。

2.2 BaaS 平台总体架构

平台以发挥区块链的共识价值和 Token 价值这 2 大价值为核心，提供一站式区块链技术服务。金链区块链平台架构如下：



- 区块链资源层：提供区块链部署资源，支持混合云部署，包括阿里云，金山云等；在部署技术方面，支持使用 Docker 容器部署等部署方式。
- 区块链服务层：基于区块链资源层构建区块链，支持部署联盟链 Hyperledger Fabric1.0.x 到 4，部署私有化以太坊节点以及分布式存储 IPFS；基于底层系统构建开发者工具，提供对区块链进行应用服务开发的工具，包括区块链浏览器，合约管理，身份服务，通证服务等；使用开发者工具开发区块链相关的服务，包括区块链部署工厂提供底层区块链快速接入 BaaS 平台渠道，区块链构建服务提供企业根据应用场景快速构建区块链应用并提供应用接口，区块链接入服务帮助企业将已有应用接入区块链服务，钱包服务等。
- 区块链应用层：集成区块链服务，提供区块链云服务，合约中心，

生态社区等应用。

2.3 产品整体功能结构介绍

2.3.1 BaaS 核心模块介绍

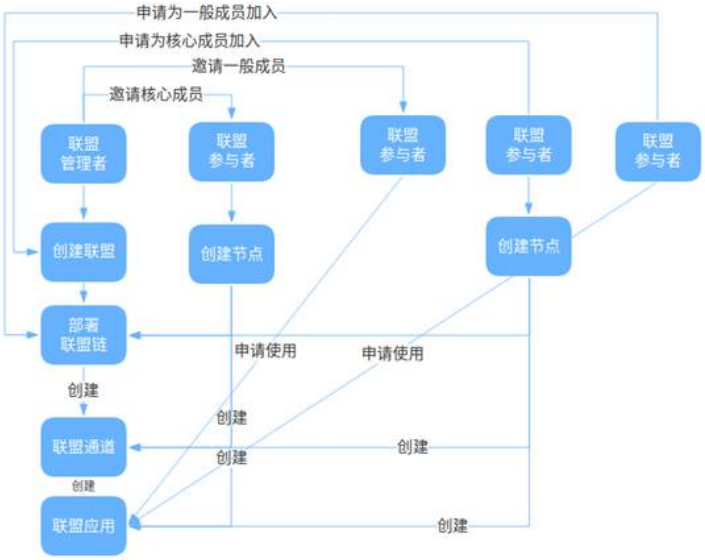
2.3.1.1 开发者中心

八斗金链 BaaS 平台提供开发者中心以最终使用需求为导向进行设计，向技术人员（部署、开发、运维）和运营人员（产品、运营）人员提供各类开具和服务，降低开发门槛，提升用户体验。同时开发者中心根据不同企业需求，为企业通过私有链区块链应用搭建方式以及联盟链区块链应用搭建方式，企业可根据实际的业务场景选择适合的方式落地区块链应用，具体流程如下:

- 私有链使用流程

序号	步骤	说明
1	部署区块链网络	部署区块链运行环境
2	创建fabric合约	创建合约链码，可使用模板合约或上传合约文件
3	选择配置部署合约	选择合约和已有区块链配置进行部署
4	访问业务网络	部署完成的业务网络，可以调试该网络下的接口
5	区块链网络管理	区块链网络的管理与监控，如查看交易、区块链状态等

- 联盟链使用流程

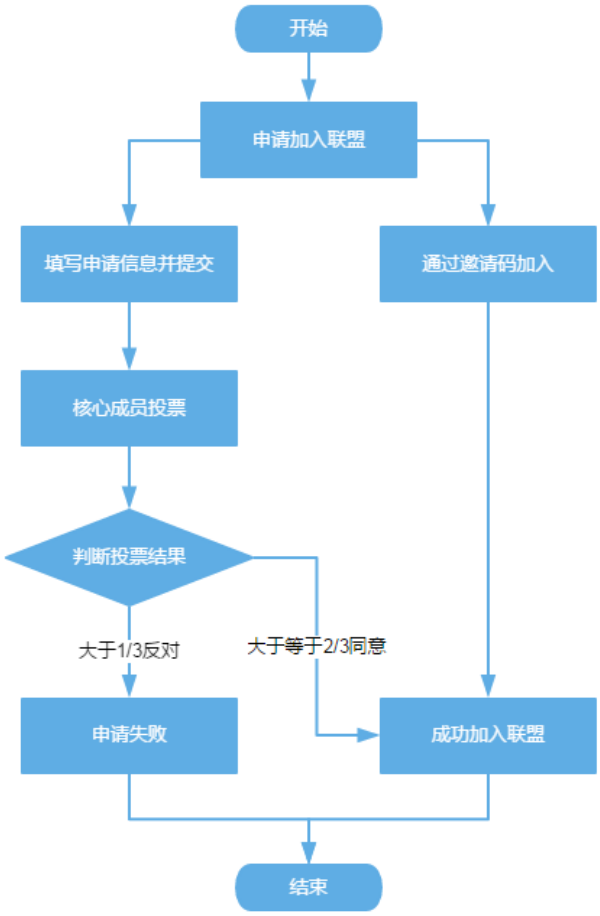


序号	步骤	说明
1	联盟管理者创建联盟	联盟管理者作为发起者创建联盟
2	部署联盟链	联盟管理者初始化部署联盟链，供后续参与者加入
3	邀请参与者加入联盟	联盟管理者可以要求其他用户作为核心成员或一般成员加入联盟
4	核心成员创建联盟节点	加入联盟的核心成员需创建节点加入联盟链中
5	联盟管理者、核心成员创建联盟通道、应用	联盟管理者、核心成员创建联盟内的通道、应用等，供联盟内用户使用
6	联盟一般成员申请联盟应用	联盟内一般成员可申请联盟内的应用，通过则可使用

2.3.1.2 联盟平台

金链 BaaS 联盟平台提供一个企业级分布式账本和智能合约平台，其共识过程受联盟节点控制。新增的节点需通过联盟的准入，拥有更高的性能及隐私性，公共区块数据对所有节点可见，私有区块数据仅对参与方可见，支持动态加入组织和通道，维护了联盟的集体权益，也保护了隐私信息。

加入联盟流程：



2.3.1.3 智能合约编辑器

智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议’也就是说智能合约是一套能够自动执行某些手动才能完成任务的协议。

八斗金链 BaaS 平台通过智能合约编辑器提供智能合约服务。我们提供了合约仓库功能，合约仓库可以用来管理我们的智能合约，您可以在该板块管理您拥有的智能合约，目前我们支持 fabric-composer、fabric-go、ethereum 三种类型的合约管理。

智能合约发布步骤：

1）智能合约编辑

用户通过智能合约编辑功能，根据具体需求对合约进行编辑。

2）智能合约初始化

初始化将 chaincode 的源代码打包成一种指定的格式，称为 ChaincodeDeploymentSpec（chaincode 部署规范或 CDS），并将其安装到运行该 chaincode 的 peer 节点上。

3）智能合约实例化

实例化事务调用生命周期系统 chaincode(LSCC)来创建和初始化一个 channel 上的 chaincode。这是一个 chaincode-channel 绑定过程：chaincode 可以绑定到任意数量的 channel，并分别在每个 channel 上独立操作。换句话说，不管 chaincode 安装和实例化了多少个其他 channel，状态都被隔离到一个事务提交的 channel 上。

4）智能合约交易查询

节点可以调用智能合约的 invoke 方法进行对账本状态的更新查询。

5）智能合约更新

任何时候，智能合约都可以通过更改其版本来进行升级，这是 SignedCDS 的一部分。其他部分，例如所有者和实例化策略是可选的。但是，智能合约的名称必须是相同的，否则，它将被视为完全不同的智能合约。

2.3.1.4 区块链配置中心

金链 BaaS 平台提供区块链配置中心，提供区块链一键部署功能，通过界面化配置的方式，简化配置流程，降低使用门槛，帮助企业快速搭建区块链，目前已支持 HyperLedger Fabric ， IPFS ， 以太坊以及恒星链一键部署并提供相关的区块链资源信息与区块信息监控，能够快速准确地识别区块链的运行状态以及在运行中满足其他的运维需求。

区块链一键部署流程：

- 生成区块链配置: 根据区块链组成与身份链节点配置生成区块链的部署配置。
- 初始化配置文件与脚本: 根据部署配置初始化区块链部署相关的配置文件与执行脚本。
- 打包并发送文件到远程身份链节点: 把部署区块链的相关文件打包发送到对应配置的身份链节点。
- 远程执行脚本: 连接远程身份链节点，执行部署区块链脚本。

2.3.1.5 区块链公示平台

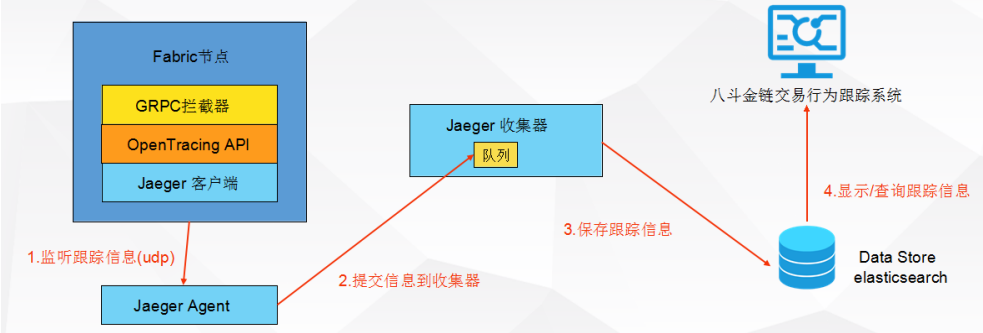
区块链公示平台用于公示八斗区块链 Baas 平台上所有区块链应用的交易情况,通过公示平台兑现区块链数据的可信度，八斗区块链公示平台提供平台让公众知悉区块链应用的交易信息，便于监督与保障公信力。

2.3.1.6 区块链交易行为跟踪系统

区块链是一个通过节点共识来维护信任的系统，当交易在发生共识的时候，常见的 Fabric 等其他区块链在应用交易行为在节点间的服务链路是缺乏可视化的监控,以致于在交易发生故障的时候难以定位问题给企业应用运维提高的维护的难度。

因此金链 BaaS 平台提供八斗金链交易行为跟踪系统实现了对区块链交易流程的跟踪监控，监控交易从背书节点进行交易背书，排序节点传输区块到广播区块的耗时与节点间的服务调用情况。

八斗金链交易行为跟踪系统实现：



2.3.1.7 镜像仓库

金链 BaaS 平台提供镜像仓库，镜像仓库里面包含八斗金链改造的区块链镜像，包括 Fabric，ETH 以及 IPFS 的节点镜像，用户通过下载八斗的区块链镜像能享有八斗金链基于企业定制化的区块链扩展功能，同时镜像仓库提供了金链 BaaS 平台各个子系统的镜像，企业可以向八斗金链申请合作，将 Baas 平台私有化部署到企业内网使用。

2.3.1.8 区块链监控平台

区块链监控平台是八斗金链与其他区块链 Baas 平台相比较的其中一个突出的平台，对于区块链来说在实际的业务场景对于节点的监控是必不可少的，节点的监控包括区块链的区块交易监控以及节点服务器本身资源的监控。通过监控预警的能够保持区块链以及区块链应用的健壮性以及可维护性。

区块链监控平台提供监控区块链网络节点状态功能，通过区块链监控平台能实时监控用户部署的区块链情况，包括区块链的区块高度，历史交易 TX 数量，用户数量，最新区块产生时间以及每天交易数量。

2.3.1.9 区块链浏览器

区块链浏览器提供查询区块链上区块交易信息的功能，通过区块链浏览器可以查看与验证通过区块链应用的产生的区块详情与交易详情，区块链浏览器区块链交易 hash，八斗身份链账户地址，区块高度，合约地址查询具体的区块链数据信息，提供区块链信息查询入口，帮助企业确认区块链交易。

2.3.1.10 金链钱包

对大部分企业场景来说，账户是每一款产品都具备的基础配置，账户体系也是一项核心的产品价值体现。在区块链于企业的应用场景来说，无论是公有链还是联盟链安全可靠的账户体系与区块链智能合约交易是必需的，而类似 IBM 的 Baas 平台是对区块链账户体系在智能合约交易上的支持是缺乏的;而金链 BaaS 平台提供金链钱包产品对接区块链账户体系，金链钱包除了提供 BTC，ETH，ERC20 系等主流的数字货币交易功能之外，金链钱包可直接对接金链 BaaS 的账户体系，使用金链 BaaS 的账户管理金链钱包，同时通过金链 BaaS 平台发布的区块链应用，以共享应用的方式让应用通过金链钱包实现价值流转。

3 产品应用流程介绍

3.1 关键技术点介绍

3.1.1 身份链构建

八斗金链基于区块链技术构建企业身份链，提供企业构建区块链应用的去中心化账户体系，企业使用身份链对账户进行角色管理与身份认证，通过身份链实现企业区块链应用数据的安全可靠性。

八斗金链构建身份链如下：

八斗金链身份链特性：

- 身份链基本信息可配置，包括身份链账户地址前缀，身份链账户角色权限定义等。
- 为了保证身份链账户的安全性，企业可选择身份认证中心支持的身份链加密算法作为账户的公私钥生成算法。
- 使用金链 BaaS 平台快速搭建身份链，提供监控管理身份链以及智能合约调用身份链功能。
- 提供冷钱包支持，通过创建或者导入的方式创建钱包管理个人账户信息。
- 支持与企业用户关联的方式，通过企业用户授权登录钱包同步账户信息。
- 通过邮件方式备份账户私钥。

3.1.2 账本数据库扩展（MongoDB）

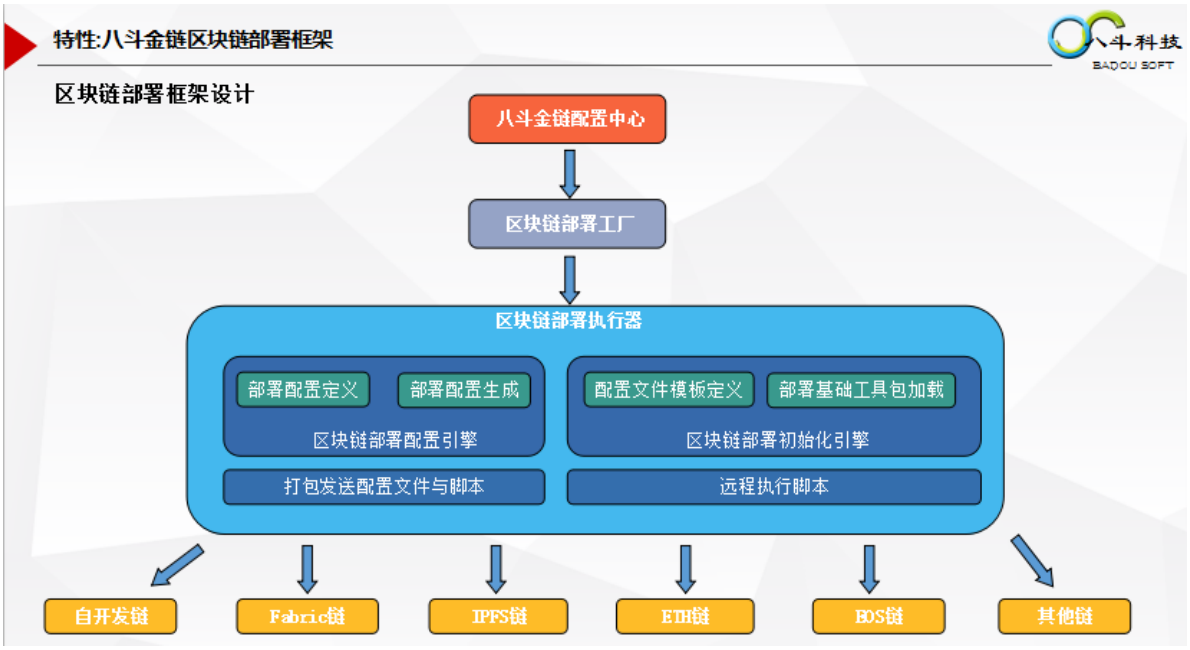
八斗金链 BaaS 平台支持 HyperLedger Fabric 联盟链的部署，原生 Fabric 的账本数据库是 CouchDB 与 LevelDB,考虑到数据库的可扩展性以及运维人员技术人员对数据库的熟悉度，八斗金链对 Fabric 进行改造，增加 MongoDB 作为联盟链 Fabric 状态数据库的可选项，企业可根据具体需求选择不同的数据库类型作为区块链账本数据库。

3.1.3 区块链安全隐私

八斗金链区块链服务在区块链安全和隐私方面在 Hyperldger Fabric 的基础上支持国密算法和企业用户签名策略多样性：支持 SM2/SM3/SM4；为每个企业提供完整的 CA 证书管理体系，确保用户通过 PKI 证书体系保障交易身份认证、数据传输安全和交易内容隐私保护等需求。

3.1.4 区块链部署工厂

八斗金链提供一套完备的区块链部署框架，通过区块链部署框架，能够实现在线配置多套区块链部署数据模型，配置文件，脚本，以插件的形式引入金链 BaaS 平台。通过区块链部署工厂能支持多类型的区块链部署。目前已支持 ETH，Fabric1.0.x - Fabric1.4,IPFS，恒星链等部署。



3.1.5 合约调用外部接口

对传统的企业应用来说，分布式系统通常接口的方式实现跨系统数据访问，降低系统的耦合度，提供系统灵活性，同时对于区块链应用来说在数据访问的需求上是相似的，无论是跨链数据访问还是对外部数据接口的访问是必要的，而根据分析，无论是 Eth 还是 Fabric 的智能合约都没有提供外部数据访问接口。

因此八斗金链开发 bdchttp 模块，支持使用 http/https 请求外部数据，在智能合约里面调用 bchttp 请求 HTTP 功能模块，通过八斗金链 BaaS 的消息队列服务，将 Http Response 返回到智能合约，实现智能合约调用外部接口，目前外部请求模块已支持 HyperLedger Fabric 智能合约，未来将在更多类型的区块链智能合约添加外部接口请求的支持。

3.1.6 区块链网络时区配置

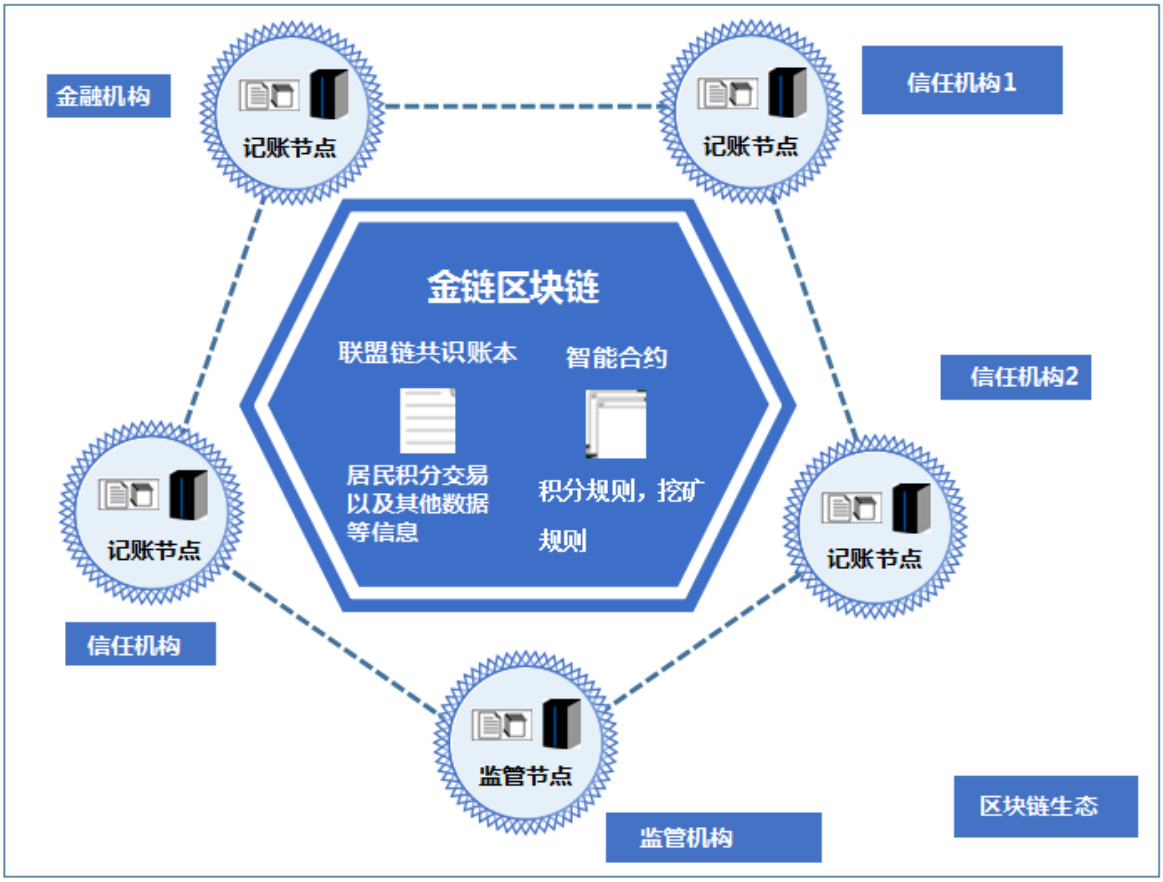
目前开源的区块链技术内部交易的时间戳是使用世界标准时间，也就是 0 时区，对于国内的区块链交易来说必要时在区块链应用层需要添加时区转换，相对比较不友好，八斗金链基于 HyperLedger Fabric 对时区的支持实现了改造，通过外部配置方式以及 SDK 方式，配置节点的时区以及客户端发起交易的时间戳使用时区，企业可以根据实际需求，配置相应的时区即可。

4 企业 BaaS 平台应用详细介绍

4.1 基于 BaaS 快速构建联盟链

构建企业区块链生态，以联盟链作为基石，在多方机构的参与下联合物联网、云计算、人工智能等技术构建智能可信生态圈。

- 采用金链区块链 Baas 平台搭建联盟链网络，引入各方共建账本
- 采用金链区块链 Baas 平台的智能合约服务，实现智慧生物岛积分生态以及居民数据采集上链。
- 采用 token 激励评级积分机制，鼓励各业务参与方诚信交易，按时履约。

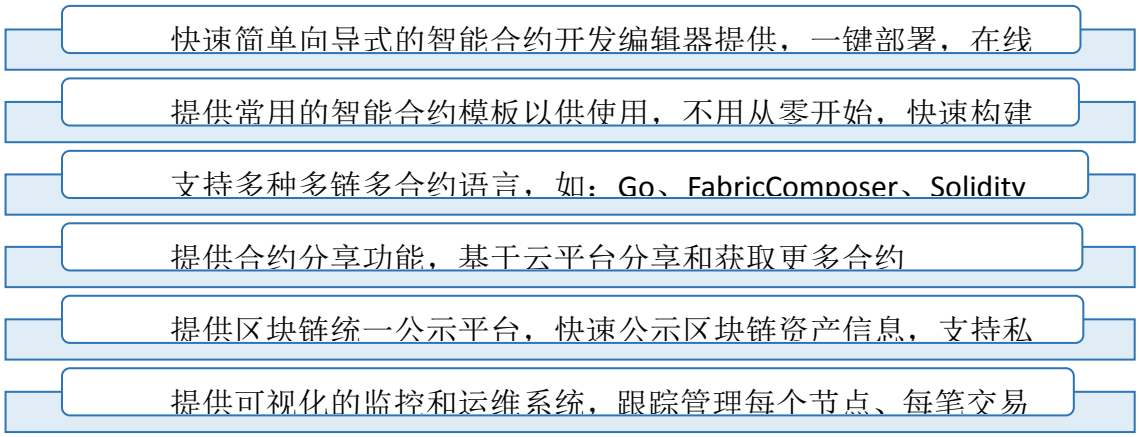


4.2 基于 BaaS 快速进行场景设计（智能合约开发）开发全过程支持

金链平台以发挥区块链的共识价值和 Token 价值这 2 大价值为核心，提供一站式区块链技术服务。

- 金链 Baas 平台相比于 IBM 等 Baas 平台的最大优势

1) 针对区块链的商业方向在币圈模式和生态模式的实现对区块链类型有不同



的需求，而市面上常见的 Baas 平台对现有类型的区块链支持比较单调，无法切合实际企业需求;

2) 对大部分企业场景来说，账户是每一款产品都具备的基础配置，账户体系也是一项核心的产品价值体现。在区块链于企业的应用场景来说，无论是公有链还是联盟链安全可靠的账户体系与区块链智能合约交易是必需的，而类似 IBM 的 Baas 平台是对区块链账户体系在智能合约交易上的支持是缺乏的;

3) 区块链是一个通过节点共识来维护信任的系统，当交易在发生共识的时候，常见的 Fabric 等其他区块链在应用交易行为在节点间的服务链路是缺乏可视化的监控，以致于在交易发生故障的时候难以定位问题给企业应用运维提高的维护的难度;

4) 对传统的企业应用来说，分布式系统通常接口的方式实现跨系统数据访问，降低系统的耦合度，提供系统灵活性，同时对于区块链应用来说在数据访问的需求上是相似的，无论是跨链数据访问还是对外部数据接口的访问是必要

的，而根据分析，无论是 Eth 还是 Fabric 的智能合约都没有提供外部数据访问接口。

- 金链 Baas 平台的特点

1) 开发和测试环境的敏捷性要求，完全自动化生成配置，部署时间从天级降低到分钟级；
2) 内置最佳实践，可快速实现区块链应用的开发和部署，没有返工；
3) 非技术人员也可以自行发行 token，降低门槛；

功能模块	企业级区块链 开发环境测试的场景	手工方式 消耗时间数量级	使用金链区块链 BaaS平台 消耗时间数量级
一键部署	从零开始，配置和部署一套全新的区块链网络，并配置好应用和Exploer	数小时或数天 （取决于对技术掌握的熟悉程度）	数分钟
智能合约在线编辑和合约库	从零开始，分析和设计应用的需求，编写合约，调试和部署上线	数天或更长 （取决于对技术掌握的熟悉程度）	数分钟
Token积分和会员生态	从零开始，分析和设计发行积分和会员生态的需求，编写合约，调试和部署上线	数天或更长 （取决于对技术掌握的熟悉程度）	数分钟

4.3 基于 BaaS 快速改造已有系统，让数据上链

八斗金链的企业级区块链解决方案是基于区块链技术，快速构建区块链中台，通过沉淀区块链业务服务能力进行输出(如:联盟管理、合约服务、身份服务等)，应用通过能力接口快速升级与交易改造，通过信用公示构建可信生态圈的平台。

5 行业应用解决方案

5.1 资产证券化

5.1.1 行业痛点

金融市场在这几年兴起了 Fintech(Financial Technology,金融科技) 的热潮。人工智能、区块链和大数据等前沿技术与资产证券化的融合成为人们讨论的热点话题。金融科技是金融和信息技术的融合型产业，它通过技术手段提高金融效率，降低金融服务门槛，以数据和技术为驱动。首先是数据维度，数据规模要大、维度要广；其次是技术维度，在数据的基础上，叠加机器学习、大数据、智能数据分析、人工智能、区块链等前沿技术运用。金融科技应用到资产证券化领域，可推动资产证券化发展，促进大量潜在优质资产实现证券化，并且可以建立以科技为核心属性的金融衍生服务体系。

资产证券化行业发展痛点

- 信息不透明不对称

原始信息分散导致难以保证供应链信息的一致性和透明性,而为了解决该问题往往需要耗费大量搜集和提取信息的成本。

- 发行管理困难

难以实时最终资金流向，底层资产监管缺乏透明性，无法通过底层穿透识别底层资产的真实性和风险性。

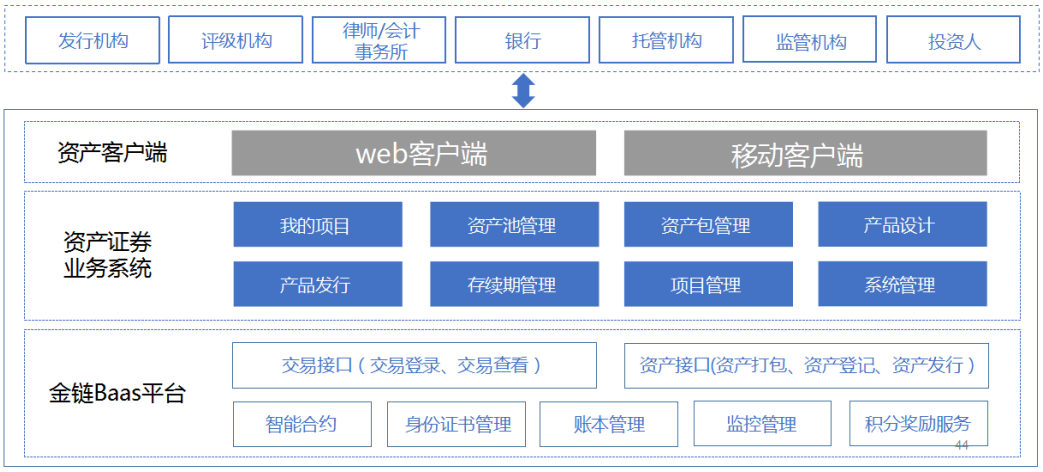
- 销售渠道单一

资产证券化由于市场体量较小，参与者相对集中，交易结果相对复杂，导致二级市场流动性差。

- 资产运行效率低

ABS 业务参与主体众多，存在复杂的一对多，多对多短息，资产运行效率低。

5.1.2 建设方案与原型展示



原型展示：

5.2 溯源行业

5.2.1 行业痛点

溯源是指对农产品、工业品等商品的生产、加工、运输、流通、零售等环节的追踪记录，通过产业链上下游的各方广泛参与来实现。在全球范围内，溯源服务应用的最为广泛的领域是食品和药品溯源，这在保障食品安全、疾病防护等方面具有重要意义。例如，在地方爆发流行性疾病时，通过食品追溯体系可以快速锁定传

染源或污染源,及时消除或控制疾病传播源。

虽然食品、医药行业溯源得到了国家政策的大力支持,但由于中国经济水平仍在发展期,消费者的食品安全意识缺乏,中国溯源行业发展仍不完善,仍处在由国家政策驱动、企业被动执行的早期发展阶段。

溯源行业通点：

- 溯源要追溯生产环节、流通环节，必然要增加做信任背书的主体，协作难度大
- 集中式的商品信息化系统安全性不足，数据容易被篡改，信息可信度低
- 供应链环节上存在各个信息系统，会有信息孤岛问题，各系统之间信息核对繁锁复杂
- 缺少相关的激励体系，对参与的消费者或联盟没有吸引力，产业链条不活跃

5.2.2 建设方案与原型展示

区块链溯源等技术可以将产品防伪,数据不可篡改及产品的每个环节可追溯形成大数据链的三大特性,从而消除供应链内产品流转过程中的假冒伪劣问题。

八斗金链解决方案：

- 基于区块链技术和芯片技术。将产品的生产、流通、交易和到消者者的各个环节的数据进行上链，进行全流程溯源。
- 数据服务。为运营商提供整合产品在流通过程中的各种数据，这些数据可通过挖掘，赋与在精细化运营分析、产业融资等方面为加入溯源联盟的企业提供数据共享服务 为个人消费者提供产品溯源信息查询服务
- 联盟服务。基于区块链技术，通过联盟的方式连接产业链上下游企业，加强生态企业间信息流转，实现全产业链资源整合。实现产品信息全产业链追踪，平台数据加密不可篡改，降低了交易摩擦边界，保障平台信息安全
- 生态服务。提供会员和联盟生态服务，通过各种行为进行用户的奖励发放，进行用户活跃度与参与度的激发。消费者用户的积累促进品牌企业

的互动营销，进而带动更多品牌企业的加入。

5.3 融资租赁

5.3.1 行业痛点

国家推行全民创新创业，如何推进企业快速增长已成为国家的一个重要任务。资本运作是推进企业的发展的一个重要手段，从传统的企业贷款，企业风险融资，到企业上市融资已是当下企业发展的一种策略，随着金融政策的发展，贷款和存粹现金的融资方式其难度在逐步增加，越来越多的企业在发展上无法快速获得资本的支持；融资租赁作为较为先进的手段投放市场好，为众多企业提供了更多的便利手段与方式。但随着创业潮的高速发展，融资租赁行业也遇到了越来越多的问题，其中有：

- 大部分企业还不清楚融资租赁的方式，将其误理解为风险投资，因此很多企业并未采用融资租赁模式。
- 融资租赁平台多，模式多，企业难以选择合适自身的融资租赁模式。
- 许多企业在融资租赁模式下，无法按时还租，导致融资租赁平台压力大，无法很好识别企业进行投资。
- 企业的融资沉淀资金大，投资企业资金的流转存在一定的风险，而且成熟的模式分担资金压力，提高资金流动性。

5.3.2 建设方案与原型展示

- 建立融资租赁的社区平台，学习平台，联合各类企业培训机构、协会组织等，通过互联网的分享阅读，帮助企业快速学习、理解合适自己企业发展的融资租赁方式。同时通过社区运作推进行业标准的发展。
- 建立融资平台入口通道，采集各大互联网的融资数据，为企业提供便捷的融资租赁入口。
- 建立信用公示门户，构建一个多方的数据信用评估体系，其中包括

企业信用、出租人信用、资产所属，投资机构信用等。基于区块链技术联合更多合作伙伴，多方共同维护数据，通过黑名单榜，提升企业信用意识。

- 建立融资组织管理平台，汇聚多方合作，为承租人、出租人、投资者、金融机构提供一个在线的合租平台，同时结合区块链智能合约，提供更多元化的服务。

6 区块链性能测试情况介绍

6.1 Fabric 性能测试结果

经过对 Fabric 的吞吐量性能测试，我们得出结论是：在使用 2 台服务器部署具有 8 个 Fabric 参与节点，10 个排序节点的区块链，基于在区块链创建智能合约交易对象的操作，对 Fabric 的交易吞吐量的进行测试，以排序节点数量，参与节点数量，交易字节大小作为控制变量设计场景，测试最高并发量为 100 个用户，对测试的区块链网络进行 10 分钟内压测 100 个用户量并发区块链交易，产生事务数最高达到 7 万，Fabric 的吞吐量平均可以达到接近 100 个/秒。

6.1.1 软硬件环境

序号	设备名/IP	硬件配置	软件配置
1	节点服务器	CPU：八核 2.40GHz 内存：32.0GB 硬盘：500G	系统：Linux centos_7.2_64bit 软件： Docker ,fabric-peer,fabric-orderer,fabric-ca,fabric-kafka,fabric-zookeeper,fabric-couchdb
2	节点服务器	CPU：八核 2.70GHz	系统：Linux centos_7.2_64bit

		内存：32.0GB 硬盘：500G	软件： fabric-peer,fabric-orderer,fabric-ca,fabric-kafka,fabric-zookeeper,fabric-couchdb

6.1.2 测试场景

对 Fabric 的交易吞吐量的进行测试，分别从排序节点数量，参与节点数量，交易字节大小进行控制变量测试，以下是测试场景设计内容：

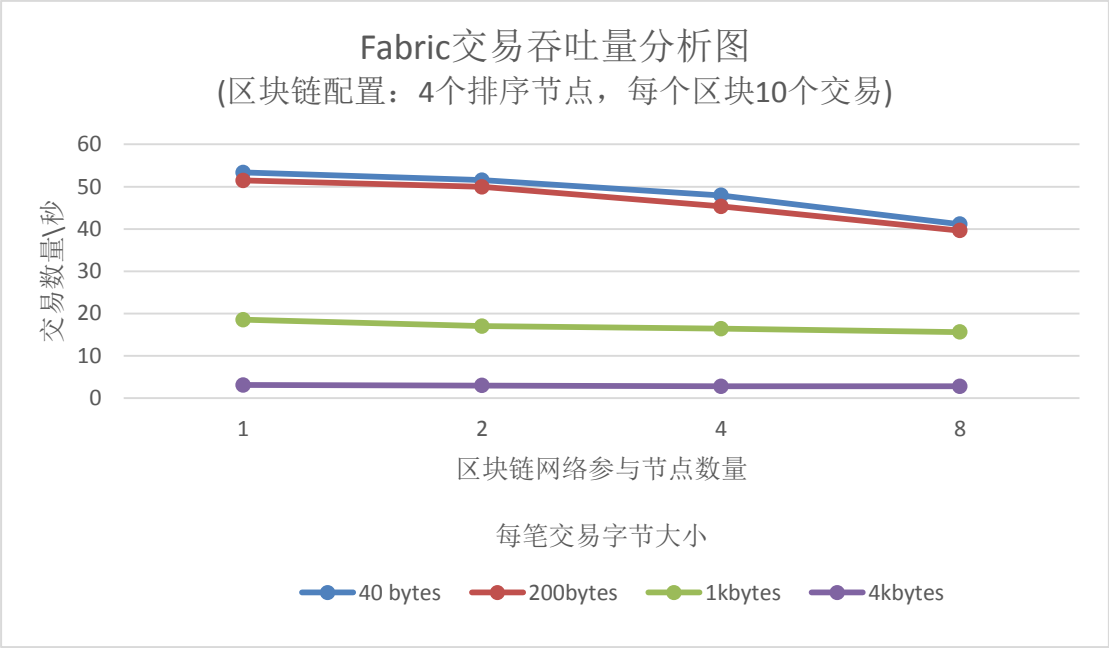
排序节点数量/个	参与节点数量/个	交易字节大小/bytes
4	1	40
		200
		1000
		4000
	2	40
		200
		1000
		4000
	4	40
		200
		1000
		4000
	8	40
		200
		1000
		4000
7	1	40
		200

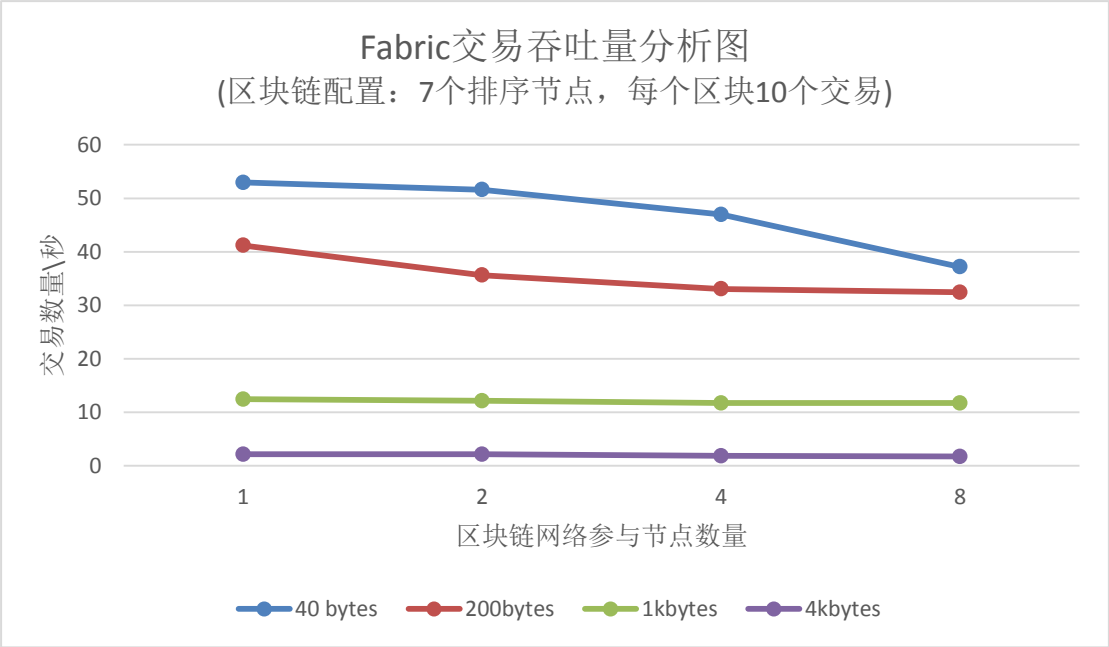
		1000
		4000
	2	40
		200
		1000
		4000
	4	40
		200
		1000
		4000
	8	40
		200
		1000
		4000
10	1	40
		200
		1000
		4000
	2	40
		200
		1000
		4000
	4	40
		200
		1000
		4000
	8	40

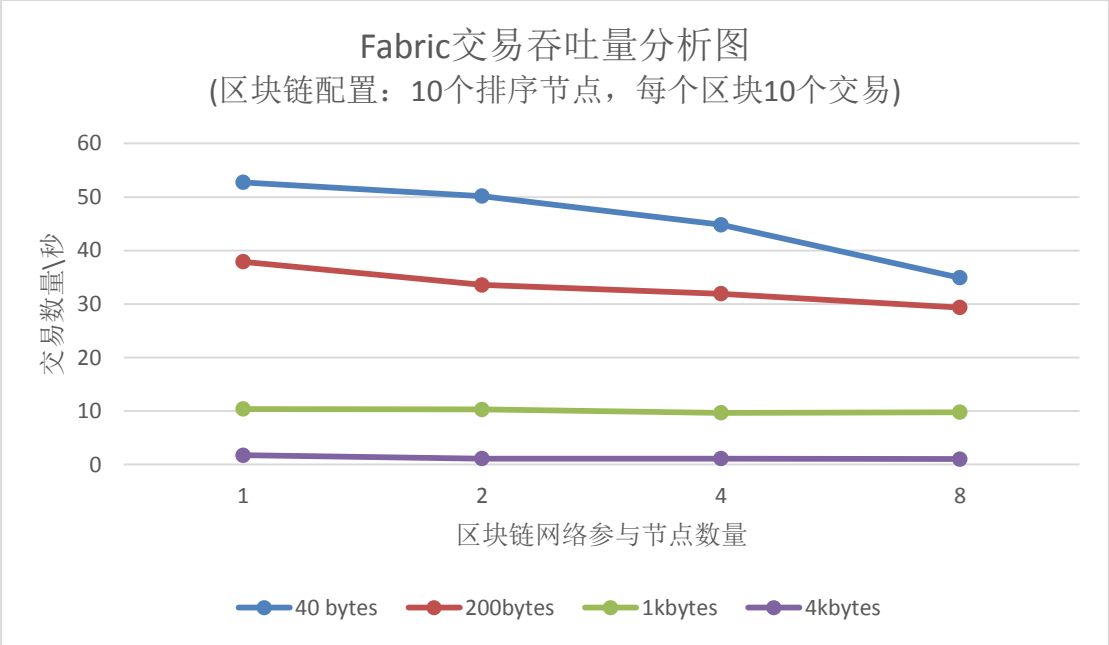
		200
		1000
		4000

6.1.3 测试结果

根据测试场景使用 Load Runner 性能测试工具进行测试。







从测试结果图表分析说明：

- 基于我们的服务器配置当 Fabric 区块链网络内的参与节点达到 16 个的时候，吞吐量曲线趋于平缓，由于大部分的资源都被消耗在网络内部的节点共识。
- Fabric 排序节点的性能受每个区块交易数量以及交易字节大小影响，当交易的字节不超过 200bytes 的时候随着区块交易数量越大，性能越好。
- Fabric 网络的交易字节越小，性能越好，当交易提案超过 200 字节，吞吐量曲线趋于平缓，并不会受到排序节点以及参与节点数量影响，是由于服务器的资源消耗在交易读写。

6.1.4 测试结论

使用 Hyperledger Fabric 作为区块链应用的底层链需要结合应用的实际情况进行配置，以下是配置建议：

- Fabric 的区块链参与节点要根据应用需求，以节点标识联盟组织，建议不超过 20 个参与节点。
- 应用在 Fabric 上面产生的交易大小取决于智能合约的复杂度预计写入的信息数据量，当交易字节小于 200 个字节的时候，且交易量频繁，可以

选择增大排序节点的区块交易批次数。

- Fabric 的排序节点集群是用于应对多节点多通道交易并发量比较大的情况，企业可以根据参与节点的数量以及合约的数量设置排序节点数量。

7 未来展望

八斗金链将一直以挖掘、提升区块链技术价值为导向，以提高效率、降低成本、打造高效的信任社会目标为己任以促进区块链科技应用落地为目标，深度服务区块链技术应用的开发者与用户为发展方向全面构建诚信公正、合规高效、与时俱进的新型产业体系。未来八斗金链区块链技术将着重几个方向努力：

- 优化区块链性能

目前区块链的交易速度与传统的中心化系统的交易速度还无法相提并论,为许多的区块链应用落地增加了难度，导致区块链应用市场发展速度缓慢，但不少的区块链开发者正在提升交易速度的道路上坚持前行,且已经取得了的进步，八斗金链也不甘落后，在区块链性能提升的道路将继续努力，推动区块链应用落地。

- 推动区块链标准落实

区块链技术还处于成长阶段,从国内外的标准推动来看,区块链标准推进速度较慢,这极大影响了区块链的产业节奏;同时安全一直是区块链技术的核心,但涉及到算法,系统等的标准问题仍然存在。中国也已着手建立区块链国家标准,从顶层设计推动区块链标准体系建设。八斗金链也将积极与国家政府合作加速区块链标准的制定。

- 安全与隐私

八斗金链高度重视区块链安全和隐私，同时安全机制是区块链中最为核心与关键的组成部分,而密码原语与密码方案是安全机制的支撑技术。区块链系统通过多种密码学原理进行数据加密及隐私保护。金链 BaaS 平台自身具备的技术和特性保证数据隐私、信息流转和网络传输的安全可控。八斗金链未来将安全散列、对称加密、非对称椭圆曲线、抗量子等加密算法,以及零知识证明算法、安全多

方计算等技术组合,保障数据隐私的安全,防止数据泄漏。

- 拥抱开源

八斗金链在自身发展金链 BaaS 平台以及区块链技术的同时，将积极参与国内外的区块链开源社区，与国内外同行进行区块链的技术交流，共同攻克区块链难题，并且未来将开源八斗金链区块链技术,聚拢产业力量,提高国内企业在国际区块链技术竞争中的影响力,实现共赢。

- 加快构建区块链生态步伐

金链 BaaS 平台在区块链的支持方面将继续努力,除了目前已经支持 HyperLedger Fabric，IPFS，以太坊以及恒星链的部署应用，将推出区块链部署工厂引入更多地区块链支持，给企业区块链应用落地提供更多的可选项，加快构建区块链生态。

8 附录

8.1 EOS 介绍

EOS 可以理解为 Enterprise Operation System，即为商用分布式应用设计的一款区块链操作系统。EOS 是 EOS 软件引入的一种新的区块链架构，旨在实现分布式应用的性能扩展。注意，它并不是像比特币和以太坊那样是货币，而是基于 EOS 软件项目之上发布的代币，被称为区块链 3.0。

- EOS 的主要特点如下：

1) EOS 有点类似于微软的 windows 平台，通过创建一个对开发者友好的区块链底层平台，支持多个应用同时运行，为开发 dAPP 提供底层的模板。

2) EOS 通过并行链和 DPOS 的方式解决了延迟和数据吞吐量的难题，EOS 是每秒可以上千级别的处理量，而比特币每秒 7 笔左右，以太坊是每秒 30-40 笔。

3) EOS 是没有手续费的，普通受众群体更广泛。EOS 上开发 dApp，需要用到的网络和计算资源是按照开发者拥有的 EOS 的比例分配的。当你拥有了 EOS 的话，就相当于拥有了计算机资源，随着 DAPP 的开发，你可以将手里的 EOS 租赁给别人使用，单从这一点来说 EOS 也具有广泛的价值。简单来说，就是你拥有了 EOS，就相当于拥有了一套房租给别人收房租，或者说拥有了一块地租给别人建房。

- EOS 架构：

1) 资源层 在资源层主要由超级节点的各种物理资源组成，根据 Block Producer 的竞选标准，在计算资源方面，每个区块生产者至少需要配备双核 Xeon 处理器，128Gb 的 RAM（可升级到 2Tb），512Gb 的 SSD；在存储资源方面，至少需要配备双核 Xeon 处理器，32Gb 的 RAM（可升级到 1Tb），Raided 500Gb 10k RPM（缓存驱动），10Tb 7.2 RPM；在网络资源方面，每个节点至少需要配备 1Gbps 的光纤接入。在运维资源方面，节点需要配备负载均衡、电源备份、设备冗余备份、抗 DDoS 设备、各种网络安全防护设备以及节点运维人员。

2) 协议层 在协议层每个超级节点通过特定的哈希算法和 Merkle 树数据结构，将一段时间内接收到的交易数据和代码封装到一个带有时间戳的数据区块中，并链接到当前的主区块链上，形成最新的区块。该协议过程涉及区块、链式结构、哈希算法、Merkle 树和时间戳等技术要素。数据区块一般包含区块头和区块体两部分，区块头主要有当前区块的版本号和序号、上一区块哈希值、Merkle 根、时间戳等，区块体主要记录当前时间段内节点打包的交易。链式结构是由各个区块包含上一区块的哈希摘要依次连接，形成从创世区块到当前区块的一条最长主链，从而记录区块链数据的完整历史。哈希函数是一种摘要生成函数，任意长度的字符串作为哈希函数的输入都可得

到一个独一无二的等长的字符串输出，通过哈希的输出几乎不能反推输入值，并且输入仅相差一个字节也会产生显著不同的输出值。Merkle 树是一种数据结构，其作用是快速归纳和校验数据的存在性和完整性。非对称加密是在加密和解密过程中使用两个不同的密钥，分别称为公钥和私钥，用其中一个密钥加密信息后，只有另一个对应的密钥才能解开，并且公钥可以向其他人公开、私钥则保密，其他人无法通过该公钥推算出相应的私钥。

3) 共识层 在共识层 EOS 主要采用 BFT-DPoS 共识算法来调度各超级节点的资源和区块生成顺序，采用宪法来协调社区内部的分歧，从而形成社区的高度自治管理。其具体过程为：EOS 的持有者通过投票系统对各个超级节点竞选者进行投票，选出 21 个节点为超级节点。然后这 21 个超级节点以自身的网络资源状况商议出一个出块权拥有顺序，在每个超级节点拥有出块权时，超级节点 A 产生第一个新区块后，A 将该区块进行签名并广播给其他超级节点，其他超级节点对该区块进行验证后对其进行签名并返回给 A 节点，当 A 节点收到来自 14 个不同节点签名的区块后，该区块就成为不可逆区块串联到之前的区块链中。EOS 社区的宪法主要是为了调节社区成员的分歧而设立的基本原则，由于目前许多区块链项目在发展过程中会出现内部分歧从而导致区块链系统不能有效的进化，因此必须在项目之初就设立项目的进化原则，从而使得 EOS 成为一条可以持续不停进化的链，以满足市场和技术发展的需要。当 EOS 发展需要分叉和升级合约时，就可以根据宪法的规则来修改和升级 EOS 代码。

4) 合约层 在合约层 EOS 通过开放 RPC（Remote Procedure Call 远程过程调用）接口来使虚拟机与 EOS 进行集成，并且脚本语言和虚拟机的实现将独立于 EOS 操作系统技术，任何开发语言或虚拟机只要有适当的、性能足够的沙箱都可以通过 RPC 与 EOS 集成在一起。并且 EOS 目前已经可以支持 Wren、WASM、EVM 三种虚拟机，因此以太坊上的应用可以通过简单的修改就能直接移植到 EOS 系统中。由于虚拟机与 EOS 的分离，使得开发人员可以选择自

己熟练的编程语言进行智能合约的开发，这使得 EOS 上的应用开发更加灵活，从而大大降低了区块链技术的使用门槛。

5) 工具层 在工具层 EOS 已经封装和模块化了诸多调用模型，目前 github 上已经开源了 11 种工具的 API（Application Programming Interface 应用程序编程接口）。开发人员可以直接调用这些 API 实现账户管理、数据库操作、逻辑计算、交易构建、进程控制、Token 生成等操作，这样的工具组件又极大的降低了开发人员的技术门槛，使得在 EOS 上开发自己的去中心化应用成为一项简单而愉快的工程。

6) 去中心化应用层 EOS 通过对合约层的优化和工具层的模块化，使得 EOS 成为真正意义上的区块链技术基础设施。在 EOS 系统中，我们不仅可以开发自己的公链，还可以锚定某条公链开发相应的去中心化应用。目前市面主流的 DAPP 类型都可以在 EOS 系统中复现出来，截止笔者完稿时，在 EOSindex（EOS 应用检索平台）上已经有 114 个 DAPP 开发出来了。 七、生态层 由于在 EOS 上可以开发自己的公链，因此开发者可以围绕一条公链开发相应的去中心化应用，如钱包、区块浏览器、区块搜索引擎、去中心化交易平台等，形成某种特性场景下的区块链生态系统，从而形成物流、金融、医疗、能源、社交、游戏等一体化的区块链解决方案。

8.2 恒星链介绍

恒星币（Stellar），一个由前瑞波币（Ripple）创始人 JedMcCaleb 发起的数字货币项目，用于搭建一个数字货币与法定货币之间传输的去中心化网关。此外通过免费发放的形式提供给用户，其供应上限为 1000 亿，其中 95%数量的恒星币用于免费发放。Stellar 是一个连接银行、支付系统以及广大民众的平台。集成的目的是实现快速、可靠且近乎无成本的资金转移。

- 恒星链的核心价值：

1) 恒星共识协议，（SCP：Stellar Consensus Protocol）是一种建立在联

邦拜占庭协议之上的成果，是一种新的共识方式。它提供了一种不用依赖于封闭系统就可以准确记录金融事物来达成共识的方式，是第一个可证明安全的共识机制，同时享有四个关键属性：分散控制、低延迟、灵活信任和渐近安全。

2) 恒星共识协议主要想解决的痛点是：当前的金融基础系统太过封闭，系统之间存在着的鸿沟，交易成本高，资本转移速度慢。Stellar 网络交易确认时间的中值为 5 秒，SCP 对算力的要求极低，理论上每秒交易吞吐量可达到 1000。

3) Stellar Lumens，恒星币（XLM），其意义在于可以在 Stellar 网络中起到反垃圾攻击的作用，每次交易都会消耗 XLM，这样就使得网络垃圾攻击变得非常的昂贵。另外就是 XLM 为 Stellar 网络内置去中心化交易平台增加了流动性，为货币交易对提供了交易桥梁。

8.3 Ripple 介绍

Ripple 是一种用以进行金融交易的互联网协议，它可以让独立系统像邮件系统那样互联起来，该协议可以用来即时免费地以任何币种向世界的任何角落转账。Ripple 网络作为 Ripple 的核心，是一个共享的公开数据库，数据库中记录着账号和结余的总账，任何人都可以阅读这些总账，也可以读取 Ripple 网络中的所有交易活动记录。 Ripple 网络可以在几秒中之内达到共识，这种达成共识的机制是一项技术突破，它可以在 Ripple 网络内进行迅速、安全而分布化的交易结算。

Ripple 进行金融交易有如下优势：

- 支付费用更低。因为 Ripple 不属于任何人，所以进行支付的成本就更低，通过 Ripple 接收款项的商家可以节省大量的费用。
- 支付更迅速。因为 Ripple 交易是自动进行的，所以可以在几秒内就完成支付，Ripple 让资金到账更迅速，加速了经济活动。
- 外汇兑换更简单。Ripple 协议让外汇兑换无需支付额外费用，这使得国际商贸活动更简单，利润更高。

- 金融服务可用性更高。只要有互联网连接就可以使用 Ripple。
- 金融服务互联性更强。Ripple 通过创造一种共享的货币协议来让独立的公司之间进行交易更加简单，减少了金融系统中的阻力，增强了系统的效率

Ripple 支持任何货币，可以进行通用货币兑换，是世界上首个分布式货币兑换机构。用户可以选择持有一种货币，但使用另一种货币支付。在 Ripple 中你可以持有美金，同时以日元、欧元、比特币、黄金以及其他任何货币向商家进行支付，每一种货币都可以作为一种自由交易的全球货币，Ripple 可以让每个人都收到其想要的货币。 Ripple 的分布式外汇交易可以让用户无需中间人，也无需其它兑换所就能完成交易。任何人都可以在全球的订单池中输入买单或卖单，而 Ripple 网络会找到最有效的途径来撮合交易，无需网络费用，也没有最低数额限制。Ripple 网络通过在大量争相赚取差价的做市商之间传递兑换单的方法来进行货币交换。

Ripple 的网关和传统的银行非常相似，不同的是，任何可以访问 Ripple 网络的商家都可以成为网关。“网关”是法定货币进出 Ripple 网络的关口。网关可以是银行、货币兑换商、交易市场或是任何金融机构。成为网关的商家为其客户创造了高级的金融功能，并能从中赚取收入。

8.4 Quorum 介绍

Quorum，是一个企业级分布式账本和智能合约平台，可看作企业版的以太坊（以太坊，是第二代公有区块链智能合约平台）。Quorum 通过一套区块链架构，提供私有智能合约执行方案，并满足企业级的性能要求。

Quorum，适用于任何需要高速和高吞吐量处理联盟许可间进行私有交易的应用程序。Quorum 解决了区块链技术在金融及其他行业应用的特殊挑战。

Quorum，是基于以太坊分布式账本协议开发而成，为金融服务行业提供以太坊许可链方案，以便支持交易与合约的隐私性。

Quorum 的主要特点及其基于以太坊公有链的扩展功能，具体如下：

- 交易与合约的隐私性
- 多种基于投票的共识机制
- 网络/节点的许可管理
- 更高性能

Quorum 的本质是使用密码学技术来防止交易方以外的人看到敏感数据。该解决方案，需要一个单独的共享区块链，和一个智能合约框架与以太坊原始代码的修改组合；其中智能合约框架对隐私数据进行了隔离。对 go-ethereum 代码库进行的修改，包括区块提案和验证过程的修改。区块验证过程，是通过执行交易合约代码来进行的，比如所有节点都对公开交易、和与交易方相关的私有交易进行验证；对于其他私有交易，节点将会忽略合约代码的执行过程。

Quorum 采用了基于 Raft 的共识机制（使用 etcd 的 Raft 实现），而不是以太坊默认的 PoW 方案。这对于不需要拜占庭容错并且需要更快出块时间（以毫秒而非秒为单位）和事务结束（不存在分支）的封闭式成员资格/联盟设置非常有效。此外，对比 QuorumChain，这种共识机制不会“不必要地”创建空白区块，并“按需”有效地创建区块。

当 geth 二进制文件传递--raft 参数时，节点将以“Raft 模式”运行。

Raft 和以太坊都有自己的“节点”概念：在 Raft 中，正常操作中的节点是“领导者”或“追随者”。 整个集群有一个单独的领导者，所有的日志条目都必须流过。 还有一个“候选人”的概念，但只有在领导人选举期间。

在基于 Raft 的共识机制里，我们在 Raft 和以太坊节点之间建立了一对一的对应关系：每一个以太坊节点也是一个 Raft 节点，并且按照惯例，Raft 集的领导者角色为仅有的能够产生新块的以太坊节点。铸币者有责任像以太坊矿工一样，将交易和块绑定起来，但不需要提供 PoW 工作量证明。