



# 纸贵区块链白皮书

## Ziggurat Blockchain White Paper

2018 年 9 月 20 日

v1.0

[www.zhigui.com](http://www.zhigui.com)

# 前言

区块链技术还处于早期的框架演进和协议探索阶段。纸贵白皮书公开阐述了对区块链发展路线的理解，以及一系列已有的技术积累，希望能为推动技术进步做出贡献。

同时，纸贵白皮书以若干商业场景为例，探讨文化、金融、制造业等诸多领域如何有效运用区块链技术，提升商业价值。

白皮书将不定期更新，欢迎读者留下宝贵意见！

## 编写委员会

顾问：何平、马治国、齐勇、陈红、裴庆祺、史佩昌、丁滟

研究与撰写：陈昌、唐凌、郝奕鸥、宣松涛、王昊、张一博、易晓春、杨文韬、陈楷、樊家合、  
颜振强、王强、史磊、马怀博、李治国、王智慧、李育林、王虎、杨识澜

设计与排版：张阿群、杨扬、吴振亮

## 第一章 综述

1.1 区块链技术 .....	06
1.2 当前阶段的问题 .....	07
1.3 纸贵的实践 .....	08

## 第二章 纸贵区块链通用技术架构

2.1 设计思路 .....	10
2.2 设计原则 .....	11
2.3 底层链架构 .....	12
2.3.1 共识引擎	
2.3.2 链上系统	
2.3.3 链外交互	
2.4 应用架构 .....	17
2.4.1 区块链适配器	
2.4.2 服务中间件	
2.4.3 区块链应用	

## 第三章 Zig-Ledger：纸贵许可链产品

3.1 简介 .....	21
3.2 基本模块 .....	21
3.2.1 基本概念	
3.2.2 底层系统架构	
3.2.3 节点功能描述	
3.2.4 交易流程描述	
3.3 扩展模块 .....	26
3.3.1 扩展实现原则	
3.3.2 高并发转账	
3.3.3 去中心化身份	
3.3.4 可调节的共识	
3.3.5 预言机和跨链	
3.4 运维 .....	35
3.5 SDK 与应用开发 .....	38
3.5.1 设计目标与原则	
3.5.2 结构设计	
3.5.3 应用场景	

## 第四章 Zig-BaaS：纸贵区块链云服务平台

4.1 简介 .....	43
4.2 Zig-BaaS 架构 .....	45
4.3 服务能力 .....	48
4.3.1 区块链应用开发全过程支持	
4.3.2 企业级区块链解决方案	
4.3.3 开放的区块链服务生态	
4.4 先进技术的融合与创新 .....	53

## 第五章 行业实践

5.1 简介 .....	56
5.2 版权 .....	57
5.3 溯源 .....	60
5.4 积分 .....	62
5.5 供应链金融 .....	64
5.6 对外合作 .....	67

01

# 第一章 综述

---

## 1.1 区块链技术

互联网（Internet）是人类进入信息社会的里程碑。历经半世纪从封闭到开放，从标准到规模的演化，今天的互联网像公路、电力一样已经成为人们生活的必需品，也成为商业活动的重要载体。尽管信息传递效率已经很高，但信任问题始终未得到解决。以商业活动为例，企业不得不浪费大量人力物力在对账、校验、合同约束、背景调查、权益证明等环节。这些大都源自信息的信任性缺失。同时，互联网也缺乏对数据来源进行保护。

区块链技术有潜力解决这些缺陷。互联网底层结构可以“尽力而为”地传递信息，区块链在此之上进一步打造能够传递“可信”信息的基础服务设施。一方面，记录在区块链上的信息将持久存在、不可篡改；另一方面，区块链网络可实现基于“代码规则”的安全协作。这些技术特征为商业活动提供了可信、可追溯的高效环境。

未来，以区块链及其衍生的分布式记账技术为核心，互联网将进一步演化为前所未有的大规模分布式协作商业网络。

## 1.2 当前阶段的问题

### 仍处于发展期的技术

互联网基于 TCP/IP 的体系结构经过长久的实践检验，得以沿用至今。区块链致力于构建“可信协同网络”，对信息传递的安全性更加敏感，需要特有的体系结构支撑。

当前，以比特币、以太坊、超级账本等为代表的区块链平台在不同场景下进行了大量应用探索。单一网络内的价值可信传递、资产可编程能力已得到验证，但大规模商用仍然受限于可扩展性和性能等核心技术问题。此外，目前尚未出现满足异构区块链网络互联互通的方案规范，区块链领域的“TCP/IP”尚未确立。

区块链融合密码学及安全技术，可以更好地满足对于数据隐私保护的诉求。这一方面也刚刚起步。例如，如何通过同态加密、可信计算等技术，实现链外信息真实、安全上链，并提供第三方验证凭据，确保智能合约被正确有效的信息触发执行；如何通过分布式身份标识构建去中心化的身份验证，在取得第三方授信的同时保护个人隐私；如何在链上数据交易的过程中，通过多方安全计算，使得各参与方在保护各自机密的前提下完成合作；如何引入基于硬件的安全模块，提升区块链系统整体安全性，防止隐私数据外流……以上问题都引起了业界的广泛关注，并进行了有益尝试，但进一步实用化仍需要学界和产业界的持续投入。

### 应用落地的现实问题

并非所有的商业模式都可以受益于去中心化，这是显而易见的。另一方面，为了构建“可信协同网络”，单单引入分布式记账能力可能并不完备。

例如，在一些金融属性场景中，需要综合运用区块链、分布式存储、声明和验证等技术。分布式账本负责记录重要的交易、信任源头的密码学证据等，而与此同时，外部数据、实体的可验证声明内容可放在分布式存储中，敏感数据则由本地存储。

再如，为了增强实体世界上链信息的真实性，往往需要权威的机构来提供可信数据上链服务。为了进一步避免过度中心化问题，一些有益的尝试包括通过 IoT 技术增强实体数字化程度，或引入分布式、交叉背书等机制来优化数据上链模型。

简而言之，区块链在技术层面需要和网络、数据库、信息安全等传统成熟技术有机配合，在业务层面要深入具体行业进行增强和适应，才能最大化其效益。

## 1.3 纸贵的实践

**面向上述问题，纸贵科技持续在底层技术、行业应用两个方面进行区块链实践。**

### 底层技术实践

纸贵提出以通用性、模块化、可插拔、安全性为设计原则的通用技术架构。在通用技术架构基础上，纸贵持续投入研发和产出血链产品。**通用技术架构描述可参阅白皮书第二章。**

Zig-Ledger 是遵循纸贵区块链设计原则和通用技术架构的一款许可链产品。底层包括密码学、账本、账户、交易、共识等多个许可链核心模块，通过 SDK 和 API 的接口为上层应用场景提供基础服务功能；中间层为平台服务层，在底层之上构建高可用、可扩展的区块链应用基础平台。应用服务层则向最终用户提供区块链应用产品。**Zig-Ledger 详细内容可参阅白皮书第三章。**

纸贵区块链云服务平台 Zig-BaaS，帮助开发者快速构建区块链基础设施，并提供区块链应用开发、部署、测试和监控的整套解决方案。Zig-BaaS 坚持自主研发和技术创新，希望通过探索新技术与区块链的融合，尝试为区块链赋能，拓展区块链的应用场景，提升区块链业务落地能力。纸贵将会在共识算法、密码学算法、分布式身份、分布式存储、预言机、跨链互操作协议等方面展开研究，并通过 Zig-BaaS 平台将研究成果输出给广大用户，共同建设区块链行业基础设施。**Zig-BaaS 详细内容可参阅白皮书第四章。**

### 行业应用实践

纸贵科技为全行业提供定制化的企业级区块链解决方案，支持文娱、供应链金融、物联网、数据安全等多个行业场景应用。

在评估应用场景时，纸贵科技结合我国宏观经济背景、政策导向、商业体系面临的主要痛点和问题，主动寻找增量占比大、提升效率明显、业务成熟度高，且具一定突破性的业务场景切入，用区块链赋能实体经济。**纸贵行业实践相关内容可参阅白皮书第五章。**

02

## 第二章 纸贵区块链通用技术架构

本章阐述纸贵区块链及其应用体系的通用技术架构

## 2.1 设计思路

目前，区块链应用构建者往往面临选择的难题，需要进行大量的取舍和开发工作，以实现自己预想中的产品形态。区块链底层的开发成本较为高昂，开发者通常需要基于合适的底层链进行二次开发，并对自己的应用进行适配性修改以适应该底层链的特点。同时，由于安全、效率、公平这三点存在矛盾而无法同时达到最优，能够适配所有场景的完美区块链底层并不存在。

例如，选定 PoW 作为共识算法的公链项目，在保证大量节点参与共识且达到 50% 容错的情况下，不得不牺牲吞吐量和交易确认速度，难以满足实时的应用需求，并耗费大量电能；选定有向无环图（DAG）作为共识基础的项目，虽然保证去中心化并获得吞吐量优势，但没有解决高能耗和交易确认慢的问题；选定 Hyperledger Fabric 作为底层链的项目，可以满足高吞吐量、快速确认、低能耗的需求，但引入了对中心化节点的依赖。

一个需要指出的问题是，不同平台上的开发往往不具有可复用性，在某个平台上付出的努力，通常无法直接迁移到另外的平台上，使得相比于业务功能的具体实现，初期的选择变得尤为重要。上述问题又被称为平台“锁定”风险，区块链的应用开发者不得不在开始阶段就选择某种具体的区块链底层技术，并且在之后受到它一定程度上的限制。

纸贵区块链致力于提供适用于多种业务需求的区块链底层服务，以期在保证底层开发维持其理想的技术栈的同时，方便区块链的上层应用开发。纸贵区块链底层平台以通用性、模块化、可插拔、安全性为设计原则，使得区块链底层的搭建尽可能轻量级。在底层的组织上，各共识模块、功能模块可定制且可插拔，为适配具体场景提供便利。

## 2.2 设计原则

### 功能解耦原则

各个模块之间，特别是不同功能层之间的服务应当尽可能地实现功能解耦。例如，底层模块的任务是构建安全、满足一致性要求的去中心化系统，它不应为用户如何使用自己的私钥而烦恼；区块链应用应当更多地处理具体的业务逻辑，而将接口适配、账户管理、区块链信息查询等功能交给其他的专门模块处理，从而有效地避免架构过于复杂、错误耦合、调试困难等问题。

### 兼容性原则

区块链的基本模块在设计上应当遵循兼容性原则，使得不同的应用开发者能够快速而方便地进行集成。例如，数据的传输内容应当使用通用标准，便于使用者理解；账户系统应当满足绝大部分场景的需求即可，而不应当添加诸如个人信息、角色信息等内容。

### 可插拔原则

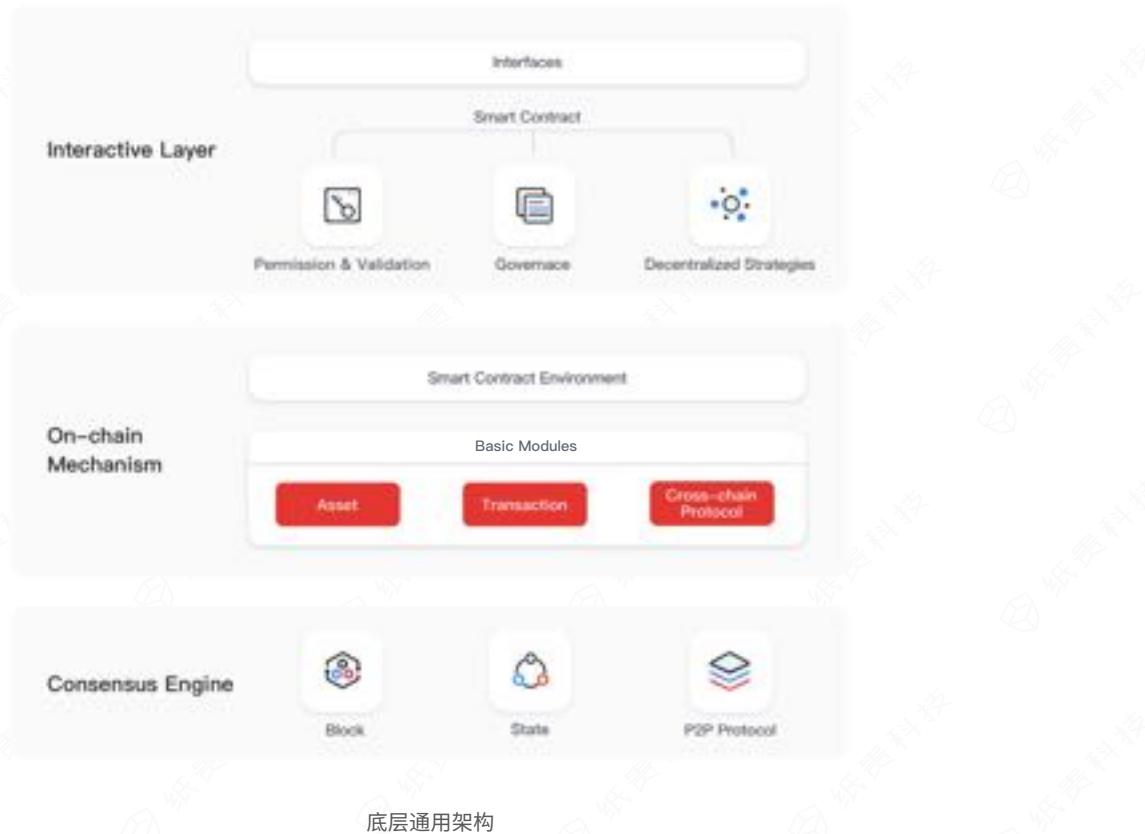
当兼容性原则无法满足，必须通过不同的模块来提供相同种类的功能时，应当考虑可插拔原则。例如，不同的共识引擎之间应当能够进行切换，使用者可以根据自身的需要对具体的功能模块进行组合，以达到特定的功能或性能要求。

### 安全性原则

区块链底层及应用在设计上应当遵循安全第一的原则，保证使用者的利益，使得系统在受到一定程度的恶意攻击时仍能保持健壮。在没有中心化管理系统的区块链底层及应用中，这一点尤为重要。

## 2.3 底层链架构

底层链是区块链系统的基石，为链上信息的分布式共识提供支撑。纸贵区块链产品的底层通用架构如下图所示：



**共识引擎** —— 共识引擎是底层链的运行基础。其中，区块与状态是分布式节点之间通过一致性协议达成的共识内容，是区块链运行机制的基本数据存储；P2P 网络协议是节点间自组织与通信的基础协议。这两个模块共同作用，奠定了区块链系统的运行基础。

**链上系统** —— 链上系统是底层链的功能核心。该部分包括一系列可插拔的、与共识机制紧密结合的底层基础逻辑。该部分包括用于分布式实体识别与认证的密码学基础算法、链上资产、交易、跨链协议等。跨链协议是链与链之间资产的交互与连接、信息的传递与流转遵循的交互方式。此外，智能合约运行环境（如 EVM、JVM、x86 VM，以及 Docker 等）为支持智能合约的正常有序执行提供了适宜的环境。

**链外交互** —— 链外交互是底层链的对外窗口，包括智能合约与交互接口。用户可以对合约进行安装、删除、初始化、冻结等操作，也可以通过接口与智能合约交互，从而实现所需的分布式业务逻辑，或者对合约请求、用户身份、其他合约的状态进行审核，对区块链进行治理等。

## 2.3.1 共识引擎

**共识引擎是区块链分布式系统的运行基础，其核心的功能为对区块链网络中的交易进行定序。**

### 区块与状态机

区块链网络是由多个节点构成的分布式系统。区块与节点的状态机共同构成了该系统的数据底层。其中，区块存储了系统中所有需要共识的操作（如交易）的历史记录，这些操作的记录极难被篡改；节点的状态机存储了节点运行时的最新状态，是区块链底层维护自身状态的存储空间，它使得智能合约能够被正确执行。

如果将区块比作区块链的“硬盘”，那么状态机就是区块链各运行节点的“内存”。区块中记录了每笔操作的记录，通过整个链条的顺序回放便得到了区块链的当前状态。这种分离的设计使得智能合约的运行成为可能，否则，区块链将需要重放所有区块中的交易以获取用户的当前余额，在存在大量交易的场景中难以实用。由于状态机分别存储在每个节点上，单一节点机的状态机是有可能被篡改的，但是被篡改了状态的节点无法与其他节点达成共识，从而被整个网络所孤立。

### 共识算法

各个节点对区块和状态达成一致需要由共识算法保证。共识算法的选择往往受制于具体的应用环境和应用目的。例如，当区块链系统用于公司内相对独立的业务部门之间的协作时，可以选择 CFT (Crash Fault Tolerance) 类共识算法，更利于业务效率提升，降低各业务部门达成互信和共识的成本；当区块链系统用于联盟成员之间的共识时，可以选择 PBFT (Practical Byzantine Fault Tolerance)、Tendermint 等可以防御一定的作恶节点，同时兼顾处理效率的共识算法；当区块链系统暴露于公网供所有人自由接入时，可能需要选择 PoW (Proof of Work)、PoS (Proof of Stake) 等能够容纳大量用户，容忍低于 50% 作恶节点，安全维护分布式账本的算法。这些算法各有利弊，互相难以替代，只有面向具体业务场景，才能设计出真正合适的算法。

针对该问题，纸贵区块链采用可插拔的共识引擎，对共识算法进行统一接口封装，将上层业务逻辑与底层共识单元相分离。对于不同的共识方式，按照相同的共识接口进行开发，可实现兼容纸贵区块链的上层模块，实现业务逻辑与共识引擎相互解耦，并针对不同场景的需要，替换不同类型的共识算法。

## 2.3.2 链上系统

**链上系统包含节点的核心处理机制，在去中心化的场景下实现部分和区块链共识紧密相关的业务功能，并且其中的一些机制可以提供给开发者进行上层应用的开发工作。这些机制与共识引擎共同作用，完成底层链的基础功能。**

### 密码学基础方法

区块链又被称为 "System of Proof"，密码学基础方法则是支撑证明的强有力工具。它为各种去中心化功能的实现提供了可能性，也是分布式策略赖以实现的最基础的算法库与工具包。算法包主要包括但不限于以下几种开源的、经过理论推导与实验验证的密码学库。

### 哈希算法

哈希算法通过单向散列函数确保信息完整性，防止信息被篡改。在实现区块之间的链式结构、签名前对待签信息进行散列、产生链上唯一 ID 等场景中均会用到哈希算法。

### 非对称加密与数字签名算法

非对称加密在区块链底层系统中主要提供数字签名与验签功能。签名验证工作存在于整个交易过程中，涉及到中间的每个节点，如提交与验证交易请求，提交与验证背书签名、提交与验证出块签名等。在用户自主生成和管理的匿名账户地址体系中进行的资产交易，也会涉及到非对称加密与数字签名。出于对用户账户私钥安全性的考虑，纸贵提出了符合 ISO 7816 标准 [1] 的安全硬件私钥保存方案，确保用户链上资产的安全性。

### 环签名算法

纸贵通过提供环签名算法模块，满足用户对于交易匿名性的需求。通常情况下，一般的加密签名可以追踪交易，得到发送人的公钥与地址。通过调用纸贵的环签名模块，可以实现对于任何交易，无法追踪其付款方是谁；对于向外发送的两笔交易，其他人无法证明其是否发给同一个收款人。

[1] <http://cardwerk.com/iso-7816-smart-card-standard/>

## 同态加密

用户在接受数据服务时，需要将数据以明文形式发送给数据服务提供方。在注重数据隐私的场景中，如何在保证用户数据机密性的前提下，使用户获得数据服务就十分重要。纸贵通过提供同态加密组建，可以确保用户数据在整个服务过程中的机密性。用户将数据以密文形式发送给数据服务提供方，数据服务对密文进行特定形式的代数运算，得到仍然是加密的结果；用户得到加密结果后，将其解密所得到的结果，与对明文进行同样运算所得结果一样。纸贵科技目前支持满足加法同态和满足乘法同态的加密算法，并将在未来进一步支持基于带扰动学习的多密钥全同态加密方案。

## 账户与交易

账户与交易是由密码学方法直接保证的数字资产模型，也是实现链上激励机制的基本元素。其保证了区块链能够成为自组织、自驱动的去中心化系统。对于任意账户资产体系而言，最核心的问题是安全，其次是性能。

安全性是账户体系最基本也是最重要的要求。首先，由于区块链账本具有一定的透明性，所有共识节点均需要对交易进行确认并达成共识，传统的密码账户体系无法支撑区块链上的分布式应用。在此场景下，依赖非对称加密等密码学算法的去中心化账户体系应运而生，区块链应用得以在公开的环境确保每个人的资金权属。其次，由于区块链上的账本允许任何人访问，恶意操作难以控制和回滚，必须从机制上保证没有人能够作恶。其中最典型的一个要点是，去中心化账户体系应当确保可以抵抗双重花费攻击（Double Spending Attack）。例如，比特币采用未花费交易输出（Unspent Transaction Output）机制来保证资金的流动中流出始终等于流入；以太坊采用 Nonce 保证交易不会重放。不管采用何种方案，确保账户的资产安全，抵抗任何可能出现的攻击，是区块链账户体系最基本的要求。

由于账户系统与支付关系密切，去中心化的账户体系也应当支持高并发交易。去中心化账户体系中的交易在两个地方存在瓶颈。其一，所有交易必须经过分布式共识，共识的过程需要消耗时间；其二，区块链账户的账户状态根据每个区块的确认进行修改，如果某笔交易是根据当前区块的账户状态构建，而在下一个区块到来后被广播至区块链网络，这期间很有可能已经发生了账户状态的改变，从而产生冲突。去中心化账户体系应当能够正确并有效地处理这两个问题，支持高并发交易，从而能够获取更广泛的应用空间。

## 智能合约运行环境

智能合约具有特殊的分布式特性，其可进行的操作与可利用的资源应保证无法对宿主机造成任何损害。为了保证智能合约能够在资源受限的条件下正确执行，智能合约虚拟机是不可或缺的基础运行环境。它通过提供受限的指令集与特殊的资源调度策略，保证了智能合约的执行不会对底层链造成损害性的后果。

常见的智能合约运行环境包括以太坊的以太坊虚拟机（Ethereum Virtual Machine）、Fabric 的 Docker 等，也有部分依赖于特定硬件或实现了特殊算法的虚拟机，可根据应用的需要定制化使用。

## 2.3.3 链外交互

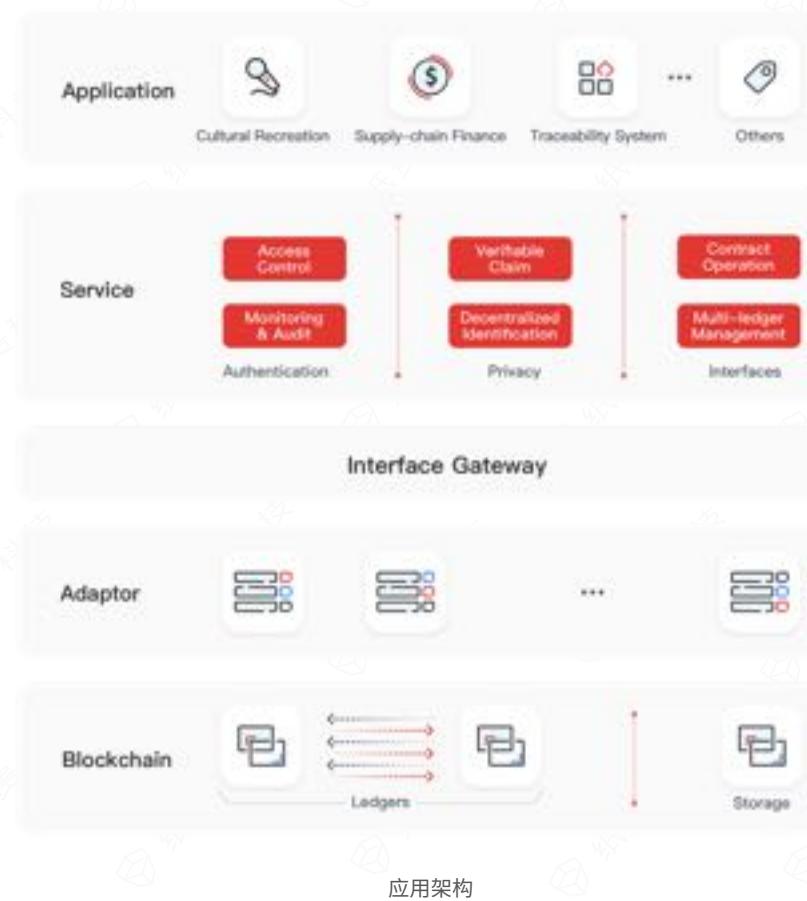
**链外交互层是区块链与外界进行沟通的窗口，由智能合约及其对外接口组成。**

智能合约是区块链应用的开发者与链上机制进行沟通，实现去中心化业务逻辑的重要载体，也是区块链生态得以繁荣的根本所在。通过智能合约，工程师们可以在区块链的去中心化环境中构建可信的应用程序，实现具有分布式共识特性的业务逻辑。他们写的每一行代码，以及程序的每一次输入输出，都将被底层区块链忠实记录与存证。这些智能合约根据功能的不同可以被分为三类：第一类是链外交互的过程中存在的权限认证、正确性检查等保护机制。通过这些机制可以构建具有权限管理的许可链，在不少受限的场景下具有广泛的应用；第二类是链上治理合约。这些合约将提供链上审计、合约管理等功能，并且所有操作均将作链上记录；第三类则是业务合约，这些合约与链外系统一起，构成各式各样的去中心化应用程序。所有智能合约必须遵守接口开发规范，按照对外交互的协议要求实现调用接口从而对外提供服务。

智能合约的开发者们仿佛戴着镣铐在跳舞。一方面，为了实现去中心化的应用，他们必须遵循链上机制提出的种种限制，使用有限的操作方法与受限的计算资源对链上的信息进行处理；他们被禁止使用随机数等会影响共识达成的机制；他们必须保证自己的代码毫无差错。另一方面，合约工程师们要针对外部系统提出的种种要求，以全面的、系统的观点设计合约功能与应用结构，最终适配并交付对外交互层，供外部应用使用。智能合约工程师必须做到逻辑严密，代码严谨，既熟悉计算机的基本原理与算法的灵活应用，又通晓分布式系统的运行逻辑与应用系统的架构设计，这对应用开发者提出了很高的技术要求。

## 2.4 应用架构

对于一个完整的区块链应用而言，纸贵区块链的应用架构如下图所示：



其中，区块链底层与存储模块相配合，能够满足大多数业务场景的需求；区块链适配器是将不同底层的接口适配并统一在同一协议框架下的转换器，通过向下兼容不同底层、向上提供统一接口的方式，大大节省上层业务服务的集成开发成本；接口网关是统一交互入口，进行请求转发、负载均衡的辅助模块，也是隔离恶意攻击、记录问题操作的防火墙；区块链服务是通过对区块链底层接口的再次抽象与封装，对外提供的简化操作形式，并按需为上层应用实现用户管理、身份识别与验证的基础设施；通过对区块链服务的定制化调度与包装，最终集成为区块链应用供用户使用。

## 2.4.1 区块链适配器

**区块链适配器使得上层应用的大部分功能可以不关心底层链的具体协议，而专心进行应用逻辑的开发。**

区块链适配器是使得底层与应用解耦的关键模块。正如在对底层链的链外交互层进行阐述时指出的，底层的开发者更注重底层的处理性能、接口效率等指标，他们不希望被应用束缚；而应用开发者则更注重业务逻辑的实现，他们不希望被具体的平台“锁定”。为了满足双方的需求，区块链适配器的存在必不可少。

区块链适配器可以将不同链的链外交互接口统一到相同的协议下，使得应用开发者可以在相同的框架中构建应用。在区块链适配器的帮助下，开发者可以在不转变思维的情况下，上手在一个新的平台上进行开发；他们只需付出少量的学习成本去阅读某个具体链的扩展方法，就可以方便地集成该链的特殊功能。

## 2.4.2 服务中间件

**服务中间件是以“扩展包”形式存在的基础功能模块，它完成了某个细粒度服务的具体实现。**

例如，当某个应用开发者想要完成某个去中心化资产管理的功能时，他仅需引入区块链交互中间件，并对应用侧提供交易查询、账户查询、交易发起等接口，即可专心开发客户端的具体功能。

当某个应用开发者想要完成分布式数据管理的功能时，他需要引入存储管理中间件与区块链交互中间件，并对应用侧提供数据管理、数据摘要上链等功能，即可支持实现去中心化数据上链与存储的功能。

上述的服务中间件在初期将会以插件、独立项目的形式为开发者提供，后期将会以应用商城的形式存在。服务中间件可以大大加速区块链应用的开发，也是开发体系得以繁荣的根本所在。

## 2.4.3 区块链应用

区块链应用指的是某个基于区块链开发的应用实例，它是直接面对用户提供功能的服务，为方便人们使用区块链提供支持。常见的区块链应用包括区块链浏览器、区块链存证服务、区块链资产管理工具等等。这些应用在区块链诞生以来，为区块链的使用和普及发挥了巨大的作用，一些应用甚至成为了区块链项目的标配。

在与服务中间件的关系上，两者之间并没有严格的界限。当应用开发者认为时机成熟时，他便可以将自己的应用或其中的一部分包装成服务中间件，供其他应用开发者使用；开发者亦可以对不同的服务中间件进行封装，以实现特定的区块链应用。

纸贵科技在对区块链的探索过程中，亦积累了一系列的区块链应用，并将持续以行业应用或服务中间件的形式服务用户或回馈社区。

03

第三章  
**Zig-Ledger:** 纸贵许可链产品

---

## 3.1 简介

**Zig-Ledger 是遵循纸贵区块链设计原则和通用技术架构的一款许可链（permissioned blockchain）产品，及配套工具集。**

Zig-Ledger 底层许可链在 Hyperledger Fabric 1.x 版本基础之上进行了一系列自主改造。

包括但不限于：

- 提升并发转账能力的 Transfer Set 底层拓展。
- 同时支持基于数字证书的身份标识和自主生成的账户 - 地址体系。分布式身份标识与可验证声明模块。
- 原生链上资产标识（包括数值通证、权限通证、数字版权等）和交易手续费功能。
- 新的拜占庭容错共识（包括 Tendermint、RFBC），作为对基于 Kafka 排序共识的补充。
- 跨链协议，提供多 Zig-Ledger 链之间、Zig-Ledger 链与公有链之间的互操作性。
- 预言机服务，提供可信的外部数据接入能力。

其中，部分扩展功能模块已贡献至开源社区。

## 3.2 基本模块

### 3.2.1 基本概念

### 3.2.2 底层系统架构

### 3.2.3 节点功能描述

### 3.2.4 交易流程描述

## 3.2.1 基本概念

**账本 (Ledger)**：包括区块链结构和多个数据库结构（如状态数据库）。其中，区块链结构中的每个区块记录一段时间内发生的所有交易和状态结果，是对当前账本状态的一次共识；区块链结构由区块按照发生顺序串联而成，记录整个账本状态变更的历史；状态数据库记录变更的最终结果。

**账户 (Account)**：账户由地址唯一标识。终端用户可自行生成唯一私钥，单向推导出公钥与地址。每个账户可拥有多种通证，记录在账本中。终端用户构造的交易需要指定发起账户，并用账户所属私钥签名。

**交易 (Transaction)**：一次对账本的操作，导致账本状态的一次改变，通常由某个账户发起。交易类型包括调用智能合约、转移通证、修改区块链配置等。

**通证 (Token)**：通证是区块链上体现参与方权限与权益的凭证。通过查询参与方持有的权限通证的类型，可以确定其是否有权利访问特定的数据或获取特定的服务；参与方通过提供数据或服务获得权益通证，并通过消耗一定数量的权益通证，获取其他数据或服务。

**智能合约 (Smart Contract)**：由开发者编写的无状态的、事件驱动的代码，通常用于描述核心的应用逻辑。智能合约对外暴露若干接口，对应用发出的交易做出响应，执行代码逻辑，与账本进行交互。支持拥有权限的角色进行智能合约的升级。

**共识 (Consensus)**：共识过程表示多个节点对于一批交易的发生顺序、合法性、对账本状态的更新结果达成一致观点的过程。

### 3.2.2 底层系统架构



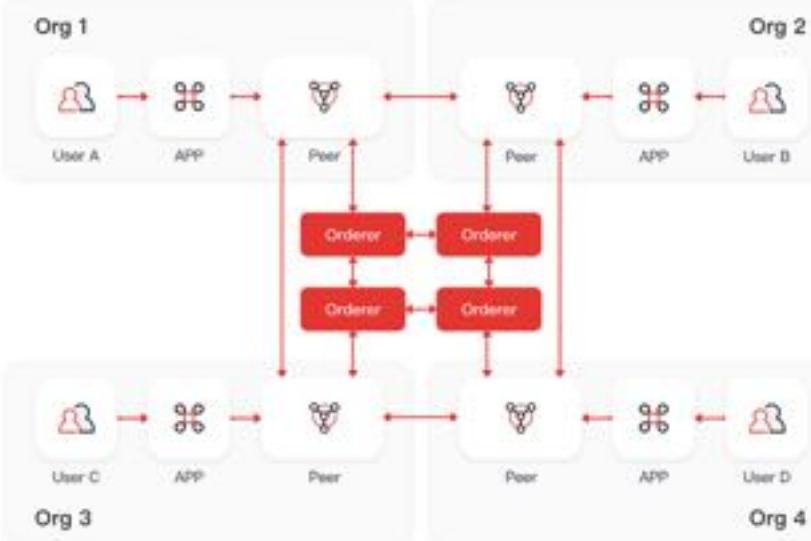
**P2P 网络:** 由多节点组成 P2P 网络，通过 gRPC 通道交互，通过 Gossip 协议进行数据同步。

**逻辑处理与链上资源:** 网络层之上为系统核心模块。账本、账户、通证、交易模块依赖区块链结构、数据库、共识机制等技术；智能合约依赖容器、状态机等技术；权限管理利用了 PKI、数字证书、加解密算法等安全技术。

**输出方式:** 最上层面向分布式系统和应用开发提供 API，并设计实现访问和管理区块链资源的 SDK。综合链上和链下资源，可构建出丰富多彩的应用程序。

### 3.2.3 节点功能描述

节点是在区块链网络中担任一定职能的服务或软件。节点功能可以是分工合作的。Zig-Ledger 区块链节点分为三种类型：客户端节点、Peer 节点、Orderer 节点。



网络拓扑示意图

**客户端节点 /App：**负责接收或构造用户交易。负责向特定的一个或多个 Peer 节点发送交易提案并收集背书，收集足够背书后向 Orderer 节点广播交易。

**Peer 节点：**Peer 节点为记账节点，负责验证 Orderer 节点生成的新区块中的所有交易，并维护区块链结构和状态数据库。部分节点会执行交易并对结果进行签名背书，称为背书节点。每个智能合约在实例化时会设置背书策略，调用该合约的交易只有满足策略条件的节点背书组合才是有效的。

**Orderer 节点：**Orderer 节点接收包含背书签名的交易，对未打包的交易进行排序生成区块，广播给 Peer 节点。排序服务提供的是原子广播，保证同一个链上的节点接收到相同的消息，并且有相同的逻辑顺序。Zig-Ledger 设计实现了拜占庭容错的分布式排序服务。

### 3.2.4 交易流程描述

Zig-Ledger 中的交易指一次对账本的操作，导致账本状态的一次改变，通常由某个账户发起。交易从发起到最终落盘账本，需要经历完整的“执行 - 排序 - 验证”过程。



客户端节点 /APP 发送的交易提案包含 Channel ID、智能合约和参数、发起实体的数字签名等信息。

Peer 节点收到交易提案后，需要校验提案结构完整性、发起方签名合法性、是否满足通道访问控制规则等，模拟执行交易并对结果签名，构造包含读写集和转移集的提案回复。

客户端节点 /APP 收到提案回复，并比对多个背书者的回复结果。若为查询类交易，则交易流程结束；若需要更新账本，则收集足够背书后，构造完整交易结构，发送给 Orderer 集群。

Orderer 集群按照特定的规则排序一段时间内的交易，生成新区块，并发送给 Peer 节点。  
Peer 节点需要进行交易的检查，并确定合法交易对状态的更新值。具体的检查包括交易结构完整性、签名、ID 等；还需对交易的读写集做 MVCC 验证，对转移集的转出方做余额检查。  
最后，根据所有合法交易更新账本状态。

## 3.3 扩展模块

### 3.3.1 扩展实现原则

### 3.3.2 高并发转账

### 3.3.3 去中心化身份

### 3.3.4 可调节的共识

### 3.3.5 预言机和跨链

### 3.3.1 扩展实现原则

Hyperledger Fabric 项目遵从功能模块化和组件插件化的设计哲学，在架构层面允许各个功能模块的可扩展性和互操作性。按照这一科学，合理，精良的架构特点和设计宗旨，Fabric 实现了一个商业级区块链的基础要件和基本功能。鉴于 Fabric 目前功能实现的不完善性和局限性以及商业场景潜在的复杂需求，在具体的商业实践中，对 Fabric 现有的功能进行增强和补充在所难免。

Zig-Ledger 在对 Fabric 某些方面进行功能扩展和优化的过程中，需要秉持和坚守若干的原则，这不仅是为了保证新增功能的质量，而且也是在设计哲学的风格上与整个 Fabric 保持一致，维持 Fabric 设计和构架风格的统一性和延续性的需要。这些具体的原则包括非侵入式扩展原则，渐进式增强原则以及测试驱动原则。这些原则的具体含义和实现方式分别叙述如下：

#### 非侵入式扩展原则

非侵入原则是指 Zig-Ledger 以 Fabric 原有代码为内核，自开发功能与之松耦合，新增功能代码不过度依赖 Fabric 的原有代码，也不过分的侵入到 Fabric 的原有代码。这个原则带来的直接收益是提供新增功能在不同版本的复用性，可以方便的在 Fabric 不同的版本中进行迁移，实现低代价的兼容 Fabric 的周期性升级。Go 语言丰富的语言特性和 Fabric 内置的多种机制为实现非侵入式功能扩展提供了多种方式。在 Go 语言中，是以 package 来进行源代码的组织和管理的，在一个 package 里面增加新的 Go 文件，不会破坏原有代码的结构和功能，并且新的 Go 文件对原有的 package 中的对象元素具有访问性和扩展权；并且 Go 语言支持内嵌的方式对接口和结构体类型进行灵活扩展，在实现继承关系上，没有采用显式的、强约束协议模式，为 Go 语言实现非侵入式编程提供了巨大的空间。Go 语言从 1.8 版本之后，开始支持动态库的加载，这也为 Go 语言实现非侵入式编程提供了强有力的支持。Fabric 要求 Go 语言是 1.9 版本以上，在其内部的实现中也使用了动态库加载的方式，来支持自定义系统链码的开发和加载。除了动态库的加载实现插件式编程以外，Fabric 采用了适当的设计模式来帮助扩展的灵活性，譬如 pre/post 模式，桥接模式，基类和辅助类模式，单态模式，工厂模式等等；而且在 Fabric 中，基于 stream 的 message 收发机制是整个 Fabric 体系中实现消息通讯和流程处理的主要方式；借助于这个消息机制，通过自定义的消息类型和数据格式，来实现自定义的功能扩展，也是非侵入式扩展的体现方式之一。

非侵入性原则的实现方式同样体现在自开发功能和模块风险可控这一要求上。实现这一要求的做法可分为两种，一种是通过配置文件的方式实现运行时的控制；另外一种是使用布尔常量控制标识，在编译阶段利用 ldflags 的可选项注入自开发功能的开关控制，这样可以轻松的实现自开发功能和 Fabric 原有功能的隔离。

## 渐进式增强原则

渐进式增强原则是对自开发功能的开发和发布流程提出的要求。为了解决功能迭代的速度和稳定之间的矛盾以及降低重构的成本，在设计和扩展新的功能时，按照核心接口不变，stable 的接口与 experimental 的接口都继承核心接口，experimental 的结构体实现逐渐过渡到 stable 的结构体实现的办法和路径，完成在主接口不变的情况下，逐渐完善具体的功能细节。在 Fabric 的源代码中，特别是链码的 shim, stub，以及 tx simulator 部分，大量的采用了 stable/experimental 相结合的方式进行代码的迭代和演进。在 Zig-Ledger 自有功能的开发和发布过程中，坚持和贯彻这一原则对于自有功能达到预期的目标和效果是大有裨益的。

## 测试驱动原则

在 Zig-Ledger 中，存在三种类型的测试，构成整个项目的测试框架与体系，来保证代码的测试覆盖率与质量，它们分别是单元测试，行为驱动测试和集成测试。单元测试是整个测试体系的基础；它不仅可以验证代码的微小修改，确保代码逻辑正确，工作符合预期，没有缺陷，而且能够更快的实施行为驱动测试和集成测试。通过单元测试，及早发现问题，简化集成，拥抱变化是 Zig-Ledger 扩展开发过程中一个必要环节和过程。Go 语言内置了单元测试框架，只需要编写以 test 的后缀的 Go 文件，通过 go test 命令行很容易执行单元测试代码，并且在 Go 语言的测试框架中包含了性能的 benchmark 测试结果。在功能性和性能两个方面，确保代码的质量。开发的功能经过单元测试之后，进行集成测试，保证新增的代码不破坏原有的代码功能。

### 3.3.2 高并发转账

在高并发的条件下，底层区块链服务能力容易存在响应时间长、交易速度慢、吞吐量低等高并发问题，这些高并发问题导致的交易效率低下实实在在的影响着区块链技术的商业应用和发展。为了应对高并发问题，在 Hyperledger Fabric 项目中，采用了支持多版本并发控制 (MVCC) 机制的 NoSQL 数据库作为分布式账本状态数据的持久化存储技术。

MVCC 这种事务控制和处理模型，从原理上有效的解决了高并发问题带来的挑战。具体来说，MVCC 与先前基于表和行的锁定机制为主要手段的事务模式不同，它是一种无锁的读写互不阻塞的并发控制机制，允许每个数据都有多个版本。在写入新版本的时候，可能会存在数据版本冲突问题，解决数据版本冲突问题的方式是在事务提交的时候检查一下事务开始后，有没有新提交改变数据版本，如果没有就提交，如果有就放弃提交。这种行为模式也被称为乐观锁，相对宽松的乐观锁，允许多个操作同时进行，在没有数据冲突以及数据冲突较少的情况下，很容易获得较好的并发性能和处理效率。

**Fabric 状态数据库的技术选型，从事务策略上很务实地保证了底层链网络处理交易的效率，但是这种方式在具体实践上，特别是转账交易这个具体业务上，存在明显的美中不足：**

- ① MVCC 对同一个区块结构下的多个交易的检查和限制过于严苛，无法支持在同一个区块内的两种常见的多笔转账交易：同一个账户向多个不同的账户进行转出操作和同一账户接收来自多个不同账户的转入操作；
- ② 不符合 MVCC 检验规则的交易会被视为无效的交易，浪费交易机会和交易费用，增加用户交易成本；与此同时，无效交易会写入区块文件，消耗不必要的存储空间。

Zig-Ledger 在 Fabric 原来读写集（ReadWrite Set）和 MVCC 检查的基础上，衍生和创造出了转移集（Transfer Set）的概念来提高高并发下单位区块转账交易的效率和成功率。转移集这个概念从数据模型来说，是一个和读写集平行等级的结构体存在。在保证高并发条件下数据一致性的基础上，在区块交易事务提交阶段，放宽 MVCC 的严格版本的检查，将符合条件的交易聚合处理，计算合并之后放入读写集的批处理事务中一同提交到状态数据库中。

**在具体实现上，整个转移集的大致流程和内涵包括如下几个方面：**

- ① 在背书阶段，接收客户端发送的转账交易请求，在对交易数据进行验证检查和验证之后，在背书节点模拟交易操作和执行，将交易结果放入到转移集中；
- ② 转移集和读写集作为模拟交易结果的构成部分，在客户端和共识节点中流转；
- ③ 在新的区块写入阶段，对读写集和转移集进行事务提交前的验证和检查，对转移集进行校验和处理之后，将所有的写操作移植到读写集的构建的批处理事务中。

Fabric 社区在最新的完善计划中，提出了 "Enhanced Concurrency Control" 的提案，这也说明社区已经意识到了这个问题的存在。Fabric 社区的提案是对转移集解决方案很好的印证，可以说转移集是对现有读写集有意义的补充和扩展，也是应对高并发条件下，高性能、高频率交易要求的有效答案。

### 3.3.3 去中心化身份

Zig-Ledger 同时支持基于数字证书的身份标识和自主管理的账户 - 地址体系。

基于数字证书的身份标识由中心化的 PKI 体系管理，适用于网络管理员、节点、应用提供方等角色的权限管理。每个身份由 X.509 数字证书表示，其权限可由记录在数字证书中的 properties（组织、角色、属性等）决定。成员管理服务提供者（MSP）组件将证书颁发、身份验证等机制进行了抽象，是实现权限管理的基础。

同时，Zig-Ledger 实现了用户自主生成和管理的账户 - 地址体系。该体系可作为大量终端用户与区块链资源的交互载体。终端用户可通过离线工具用特定算法（如椭圆曲线 secp256k1）生成私钥和公钥，并由公钥单向推导出账户地址。该账户具有匿名、自主管理、去中心化等特点，是终端用户管理链上资产标识和发起交易的载体。

在此基础上，Zig-Ledger 实现了通过分布式身份标识与可验证声明，实现去中心化的身份管理与验证。分布式身份标识（Decentralized Identity, DID）是一种新型的可验证的数字身份形式，具有分布式、自主可控、跨链复用等特点。我们遵循 W3C 提出的 DID 设计参考 [2]，将 DID 与 Zig-Ledger 相结合，使区块链上的任何实体可自主创建和管理他们自己的身份标识。并且一个实体可对应多个 DID，以满足实体所希望的身份、人物角色和应用场景的分离。这里的实体，可以指现实世界中任意客观存在，并可相互区别的事物，例如个人、组织或具体事物。

可验证声明（Verifiable Credential）提供了一种规范来描述实体所具有的某些属性。它能表示物理世界中的凭证所能表达的相同信息。DID 持有者，可以通过可验证声明，向其他实体证明自己的某些属性是可信的。同时，结合数字签名和零知识证明等密码学技术，可以使声明更加安全可信，并进一步保障用户隐私不被侵犯。



[2] <https://w3c-ccg.github.io/did-spec/>

DID 是一种去中心化的可验证的数字标识符。它独立于任何中心化的权威机构，可自主完成注册、解析、更新或者撤销操作，无需中心化的登记和授权。DID 具体解析为 DID Document，DID Document 中主要包含两方面内容，一是加密材料（如公钥、匿名身份识别协议等）、二是属性（包括用于身份验证的信息以及服务端点）。身份验证信息与加密材料可结合提供一套机制，作为 DID 主体进行身份验证。而服务端点则支持与 DID 主体的可信交互。



可验证声明是由签发者为其他实体签发且可被任意实体签名和验证的，用来描述实体所具有的某些属性的声明。此外，可验证声明同时支持中心化的信任体系和去中心化的信任网络。在中心化的信任体系中，指定一个或多个实体作为信任锚，信任锚作为被公认为绝对信任的实体，可指定其他实体作为其信任的实体，被指定的实体又可指定其它实体作为其信任的实体，由此形成以信任锚为中心的信任传递关系。而在去中心化的信任网络中，无需选定信任锚作为中心，实体间通过自发、对等的相互认证来产生信任关系，从而实现信任的传递。此外，实体被越多的实体或可信度越高的实体认证，其可信度就越高。

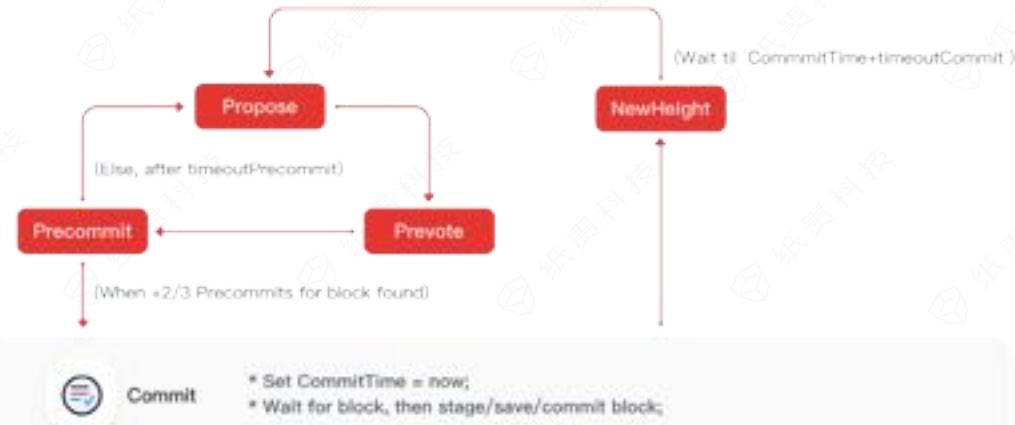
在现实世界中，认证机构会给一般实体签发可被公众信任的声明，例如车管所给司机颁发的驾照，学校给学生颁发学生证等。而当这些线下的声明被放到网络上进行验证和使用时，可能存在时间延迟、信息被篡改或者隐私信息泄露等问题。因此，通过将标准化的可验证声明放到区块链上，可使其更加便捷、更容易验证、且更加自主可控。进一步加入零知识证明来拓展分布式身份标识的功能，可实现匿名签发可验证声明，或通过验证身份的同时不暴露个人信息，保护用户的隐私信息。

### 3.3.4 可调节的共识

借助 Fabric 排序服务的可插拔性设计，Zig-Ledger 引入 Tendermint 和 RFBC 共识引擎以支持拜占庭容错的共识机制。同时整个共识流程会包含多个阶段，包括验证交易的合法性和交易的打包排序；Zig-Ledger 通过配置实现了在不同的阶段调节算法的松紧程度的功能，可根据不同的部署环境灵活适配。

#### Tendermint 共识算法

Tendermint 是一个基于状态机复制的共识算法，对于每一个块的提交都会经过一轮或者多轮的投票。每一轮都有一个根据算法确定性选出的 proposer。



Tendermint 共识阶段示意图

- Propose 阶段，本轮的 proposer 会通过 gossip 协议发送 proposal 给其他节点，接收到 proposal 的节点同样也会通过 gossip 协议转发 proposal 给其他节点。
- Prevote 阶段，所有的节点会独立生成自己的 prevote，包括然后通过 gossip 协议发送给其他节点。
- Precommit 阶段，同样所有的节点会独立生成自己的 precommit，当接收到超过 2/3 的接受本轮 proposal 的 prevote 时，将通过 gossip 协议将 precommit 发送给其他节点，否则不会发送 precommit。当在指定时间内收到超过 2/3 的 precommit 后，进入 Commit 阶段，否则会重新回到 Propose 阶段，进入下一轮的投票。
- Commit 阶段，需要同时满足两个条件，第一是节点需要已经接收到当前待提交的 block；第二是收到至少 2/3 的 precommit，就可以提交 block 到账本中。

## Zig-Ledger 排序服务

Zig-Ledger 排序服务支持多种共识插件，可以根据区块链所在网络环境进行选择和切换。

- Solo，单节点排序服务，用于开发和测试网络环境。
- Kafka，CFT 排序服务，用于可信网络环境，无作恶节点。
- Tendermint，BFT 排序服务，用于强同步网络环境，可容忍  $1/3$  作恶节点。
- RFBC，BFT 排序服务，用于弱同步网络环境，可容忍  $1/3$  作恶节点。

Zig-Ledger 排序服务分为三个阶段。第一阶段会由接收到客户端交易请求的共识节点进行验证，由于 Zig-Ledger 将区块链状态和排序服务进行分离，所以排序服务只做基本的签名验证和消息元数据验证。第二阶段，Zig-Ledger 会对同一个通道中的交易进行全局排序。第三阶段的验证可以选择执行，在非拜占庭环境下，如果没有发生配置变更，不需要执行第三阶段的验证；而在拜占庭环境下，需要在参与共识的多个节点上再独立执行一次验证。

## 3.3.5 预言机和跨链

### 可信链外数据接入

作为真实世界信息进入区块链的通道，预言机为区块链提供了可信的外部数据接入服务。通过预言机服务，可以实现链下信息触发链上动作，打破区块链与现实世界的信息壁垒。预言机服务可以帮助用户的链上平台对接可靠第三方信息平台的 Web API，满足其业务需求。

Zig-Ledger 预言机模块通过引入验证机构约束上链服务提供方，在密码学方法的辅助下，以不影响正常网络通信为前提，确保上链服务被约束为能且只能发送可信数据源提供的数据上链，且该约束过程可被验证。同时，上链服务运行在 SGX (Software Guard Extension) 创建的可信执行环境 (Trusted Execution Environment, TEE) 中，确保服务不受到恶意软件的攻击。每次提供上链服务的同时，也会生成证明文件，任何第三方都可以通过该文件，验证整个服务提供过程和结果的有效性。

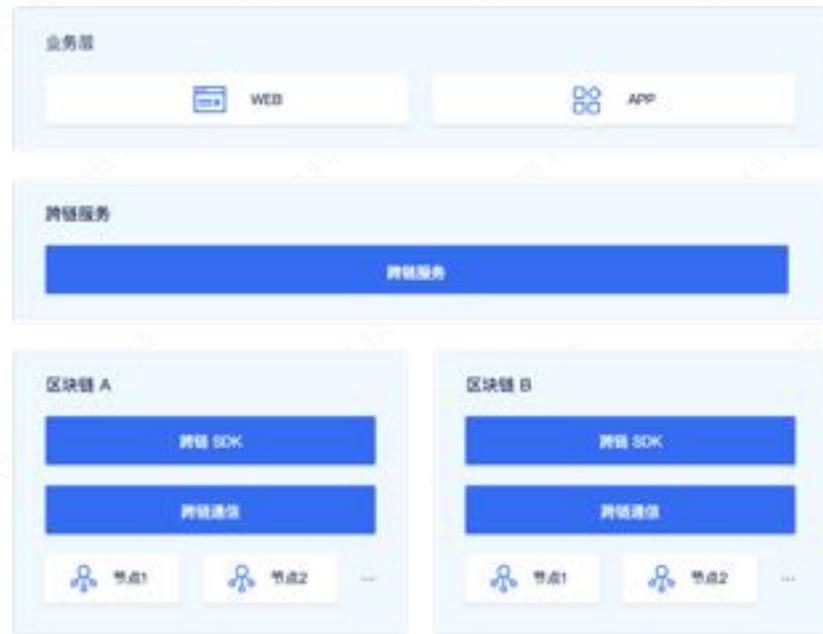


预言机方案架构示例

如图，链上智能合约通过调用预言机合约，获得可信的链外信息。预言机合约获得的上链信息及审计信息，由审计服务和上链服务两个模块共同提供。两个模块共同与可信数据源进行交互，一方负责数据获取，一方负责监督获取过程。

## 跨链互操作

在区块链所面临的诸多问题中，链与链之间的互通性缺失很大程度限制了区块链的应用空间。跨链互操作协议的严谨描述、规范实现和普遍应用将成为实现“价值互联网”的关键。目前，Zig-Ledger 跨链互操作解决方案提供了同构（如多条 Zig-Ledger 或 Fabric 链之间）和异构（如 Zig-Ledger 和以太坊）区块链之间的信息交互和价值流转服务，满足区块链应用的业务扩展性需求。



跨链方案示例

跨链互操作解决方案包括区块链层、跨链服务层和跨链应用三个部分。通过在底层区块链中集成跨链通信协议和跨链 SDK，实现同构或异构区块链之间的跨链调用、信息交互、资产流通等功能。具体应用场景可包括：

**多链业务模型：**针对相互独立的子业务分别搭建不同的基础链，提升效率、保护隐私。各基础链可平等提供服务，也可采取分层结构。

**跨链信息互认：**不同区块链之间的信息互认，例如数字版权、公证公示、数字身份等信息的跨链访问和确认。充分利用已有资源，减少重复建设。

**原子互换：**通过哈希锁定的方式，保证分别位于两条链上的两个交易同时发生，适用于“一手交钱，一手交货”等场景。

**跨链资产流转和服务调用：**通过跨链交易的定义、可信传递和验证，实现资产标识跨链转移和计算资源跨链调用。

## 3.4 运维

### 运维概述

Zig-Ledger 采用现代化的微服务设计，天然的云原生架构，能够充分利用现有云计算平台的能力，为用户提供高安全性，高可用性，高性能的区块链服务。同时得益于 Zig-Ledger 灵活的设计，Zig-Ledger 也能方便的部署到各种传统的非云环境中。纸贵科技已经与国内知名的云服务厂商（阿里云、金山云、青云、华为云等）达成了战略合作协议，可以直接在公有云平台部署或者使用 Zig-Ledger。



## 基础设施层

基础设施层可以构建在任何的物理环境中，通过安全的网络方案和安全服务，以及底层的监控平台和日志平台，给上层区块链服务提供安全可靠的保证。

## 服务编排层

因为 Zig-Ledger 采用了现代化的微服务架构，通过服务编排层可灵活的定制和管理上层区块链服务组件。

## 区块链平台层

Zig-Ledger 的核心服务，提供了诸如智能合约引擎，共识算法，账本管理和身份证书管理等一系列区块链基础设施。

## 应用逻辑层

通过 API 接口将 Zig-Ledger 的能力暴露出来，使其能与外部系统或服务对接；通过浏览器服务，使用户能够直观的感受到 Zig-Ledger 的服务。

## 运维保障

区块链服务的运维面临很多的问题和挑战。如何应对各种网络攻击，如何简化区块链服务的部署和运维，如何保证区块链服务的安全性和稳定，纸贵科技在实践中研发出一套强大而灵活的运维系统和服务。

## 安全性

- 利用二层网络隔离、虚拟私有网络、IP 白名单等方式，给用户提供安全的可靠的网络部署方案。
- 监测和防范任何异常的访问登录行为，防御各种网络攻击。
- 安全的存储节点密钥和证书，对于用户敏感信息采用加密方式存储。同时对于用户私钥保存，可以为用户提供专用硬件方案。
- 节点之间通信均采用 TLS 加密传输方式，安全可靠。
- 联合合作伙伴对智能合约进行代码检查和形式化验证。

## 可用性

- Zig-Ledger 所有服务组件均可进行 HA 部署，保证区块链服务的高可用。
- Zig-Ledger 可以跨地域，跨平台进行部署，通过多数据中心，多私有网络来进行容灾备份。
- Zig-Ledger 可通过本地存储，共享存储，云存储等方式对数据进行持久化，同时利用快照和多副本的方式进行备份和恢复。

## 灵活性

- Zig-Ledger 可部署在多种环境中，同时也可部署在不同的平台上。
- 可自动生成各种配置文件和部署文件，同时兼容各种证书管理方式。

## 可运维性

- 完善的监控报警系统，通过采集系统级和应用级监控信息，触发条件会自动发出报警信息。
- 完备的监控图表，帮助运维人员实时掌控系统资源的变化，针对突发情况提前作出反应。
- 任何组件出现故障后，除了发出报警信息，Zig-Ledger 能够自动恢复故障的服务组件，极大的减少人工运维工作。
- 日志系统可以收集节点、智能合约在内的所有服务的运行日志，同时提供强大的检索功能，可根据关键字进行全文检索。同时支持日志报警功能，运维人员可提前设置日志关键字，当日志中出现相应关键字时，自动触发报警信息。
- Zig-Ledger 提供一系列的自动化脚本，不论是初次部署，还是后期运维，简化运维人员的工作。同时纸贵还在开发基于 web 的自动化运维系统，能够通过图形化界面来进行运维工作。

## 3.5 SDK 与应用开发

Zig-Ledger 底层采用通信数据序列化协议（Protocol Buffer）对数据进行封装，并在对外交互层提供 gRPC 接口供应用调用，以获得更高的网络传输性能。这些接口包括交易处理、安全验证、数据交互以及消息监听等。应用开发者需要具有较强的底层开发知识与经验，才能够妥善处理这些数据与协议。为了降低上述门槛，作为区块链适配器的 SDK 必不可少。

### 3.5.1 设计目标与原则

### 3.5.2 结构设计

### 3.5.3 应用场景

### 3.5.1 设计目标与原则

Zig-Ledger SDK 需要对区块链的交互接口进行一定合理、必要的抽象，为客户端提供基于自身语言的与链交互的基本功能，期望能够为应用开发者带来一定的便利，并达成以下三点目标：

- ① 支持区块链应用开发：为应用开发提供必要的交互接口。这些接口包括智能合约的部署和调用，区块链事件消息的监听，区块与交易相关信息的获取等。此外，SDK 应配合 Zig-Ledger 支持其高并发的特性。
- ② 智能合约开发：提供智能合约编写与测试的接口，帮助开发者快速进行智能合约的调试。
- ③ 开箱即用的服务：期望提供一套开箱即用的服务端解决方案，使得开发者可以快速将其接入传统应用服务。

为了达成以上三点目标，规范的设计原则必不可少，这些原则包括：

- ① 完善的文档：提供完善、清晰的文档，阐明其使用方法与数据模型设计，并提供相关使用示例。
- ② 易于使用：虽然了解区块链底层实现对于编写分布式应用有很大帮助，但应用开发者更应专注于实现业务逻辑。因此，SDK 应当尽量脱离对区块链底层架构的依赖，将应用开发者与底层实现相隔离，使得应用开发者在无需了解区块链底层的前提下能够快速安装和上手，设计和开发适用于业务需求的合约逻辑。
- ③ 高性能：SDK 在设计和实现时应当注重高性能，横向可扩展性以及低时延等特性。
- ④ 不存储隐私信息：SDK 应当只存储链交互所必需的信息，对于用户本身的隐私信息及数据应当在设计上避免进行网络层传输。例如，对于匿名账户 - 地址体系，其私钥应当完全在用户侧进行存储与使用，SDK 将只接受签名信息并进行相应处理。

## 3.5.2 结构设计

Zig-Ledger SDK 的构成主要分为三层：

第一层为直接封装数据并与底层链进行 gRPC 通信的部分。这一部分分为 chain-client 与 chain-ca-client 两个子模块，分别用于功能交互与权限交互。

第二层为对底层接口的再次封装。由于第一个层次的接口往往仅具有最基本的功能，为了实现接口服务，需要对所使用的资源如通信连接、内存等进行合理的管理，以适应长时间、高频率的接口调用处理。同时，在这一层增加了对高并发通证转移的支持，使得 SDK 能够配合底层链发挥出其最大性能。

第三层为服务化，是可选的服务端插件。这一层次中，第二层中的接口被再次封装，以通用的网络通信协议的形式对外提供服务，同时将交易的构造与签名部分放在客户端，维持匿名账户部分的隐私性。

## 3.5.3 应用场景

Zig-Ledger SDK 是应用与 Zig-Ledger 网络进行沟通的桥梁，一个典型的应用结构如下图所示：



其中，SDK 封装处理了与 CA 交互获取身份证书的功能，以及与 Zig-Ledger 交互实现去中心化应用的相关逻辑。SDK 能够但不限于应用在以下场景中。

## 基于 PKI 体系的身份注册与身份验证

为了与区块链进行交互，应用提供方、节点等主体必须持有合法的身份证书，该身份证书可以由内部或外部 CA 提供。

SDK 帮助应用程序封装了这部分交互接口，并能够完成基于 PKI 体系的身份注册、认证与权限相关功能。

## 匿名账户 - 地址体系管理

为配合面向用户的匿名账户 - 地址体系，Zig-Ledger SDK 实现了公私钥生成与地址转换工具，以及与区块链交互以实现转账功能的接口。为了遵循服务端不存储隐私数据的原则，SDK 还针对服务端部署的情形实现了交易构造与签名的客户端程序，保证匿名账户的安全性。

## 交易调用与查询

当 SDK 准备发起一笔交易时，它首先用自己所属应用的私钥对构造的交易内容进行签名，并异步发往特定的背书节点进行背书处理（背书节点由智能合约背书策略决定）。当获取到背书后，SDK 可以自行决定是否继续将交易与背书结果发往排序节点进行交易排序。由于该发送操作也是异步的，SDK 将监听账本事件来获得交易是否最终成功写入账本。

通过 SDK，用户可以快速进行交易的构造与执行，特别是能够方便地进行智能合约的调用与查询，并针对事件的成功与否设计不同的处理策略。

## 高并发转账

Zig-Ledger 从底层结构上支持对包含转账操作的交易的高并发处理。为了进行高并发转账，需要在同一账户不同的交易之间自动对交易计数器增加计数，以满足防重放攻击的要求。SDK 预置了对该机制的支持。同时，SDK 内部采用请求队列的方式对交易请求进行缓冲处理，防止资源浪费，更有利于实现高性能的应用模块。

04

第四章

Zig-BaaS：纸贵区块链云服务平台

---

## 4.1 简介

构建一套分布式的区块链环境绝非易事，既需要硬件基础设施的投入，也需要全方位的开发和运维管理。在这样的背景下，区块链即服务（BaaS, Blockchain as a Service）应运而生。BaaS 的概念在 2015 年底诞生，前期主要由微软 Azure 和 IBM Bluemix 提出并主导。起初，BaaS 是部署在云计算基础设施之上，对外提供区块链网络的生命周期管理和运行时服务管理等功能的一套工具，帮助开发者快速构建所需的区块链环境。随着区块链技术的不断火热，2017 年开始，国内外各大公司跑步入场，BaaS 的定义和功能范围得到了很大程度的延展，也吸引了越来越多开发者的关注。

Zig-BaaS（Ziggurat Blockchain as a Service）是纸贵科技发布的一款区块链云服务平台，旨在帮助开发者快速构建区块链基础设施，提供区块链应用开发、部署、测试和监控的整体解决方案。



Zig-BaaS 首页

Zig-BaaS 作为区块链云服务平台，支持各类主流的区块链和分布式网络开发环境，包括 Zig-Ledger、Hyperledger Fabric、Ethereum、IPFS，并将陆续支持 EOS、DID、跨链交互、形式化验证等更多的区块链技术与服务。基于区块链底层开发环境，Zig-BaaS 提供了简单易用的开发者工具与服务，包括区块浏览器、合约 IDE、SDK & API 等，开发者可以在可视化的操作界面下完成区块链的构建与操作，极大地降低了开发门槛，提高了开发效率。除此之外，Zig-BaaS 合约中心为用户提供众多优秀的示例智能合约，支持开发者免费下载、学习、部署和调试，帮助开发者快速上手合约开发。

Zig-BaaS 项目于 2017 年 8 月启动立项，2018 年 1 月上线内测版，并于 2018 年 7 月上线正式版本（<https://baas.zhigui.com>）。



Zig-BaaS 里程碑

Zig-BaaS 内测版本发布以来，支持了国内多个高校和地区的区块链活动和比赛，帮助开发者快速上手区块链开发，获得了开发者的一致好评。同时，Zig-BaaS 积极寻求合作伙伴，携手共建开放的区块链云服务平台。Zig-BaaS 的合作伙伴包括 Hyperledger、EEA、CertiK 等优秀的区块链技术社区与机构，也包括阿里云、金山云、华为云、京东云、青云等国内主流的云计算厂商。Zig-BaaS 将专注于技术研究和能力建设，与各行业合作伙伴携手合作，共同打造繁荣的区块链生态。

## 4.2 Zig-BaaS 架构

### 整体架构图

Zig-BaaS 架构如下图所示，自下而上包括资源层、服务层、应用层和业务层。



## 区块链资源层

区块链资源层，为上层区块链及服务提供稳定可靠的底层资源支撑，包括计算资源、存储资源和网络资源等。Zig-BaaS 的底层资源合作伙伴包括阿里云、金山云等国内主流的云计算服务商，共同为 Zig-BaaS 平台提供成熟可靠、安全稳定、灵活弹性的底层资源。

## 区块链服务层

区块链服务层主要包含了 Zig-BaaS 平台的各类区块链云服务产品，每个区块链云服务由区块链底层环境和可视化的开发工具封装生成，用户可以按需选购所需的云服务产品，在可视化的控制台页面内进行操作。

Zig-BaaS 提供多种类型的区块链云服务，包括但不限于：

- ① **区块链构建服务：**为用户构建一条专属的私有链或联盟链环境，例如 Zig-Ledger、Hyperledger Fabric 等；
- ② **区块链接入服务：**提供接入区块链网络的节点接入，帮助开发者访问该区块链网络，例如 Ethereum 等公有链环境；
- ③ **算法和协议服务：**区块链相关的算法与协议云服务，例如跨链协议、分布式身份标识、去中心化存储等；
- ④ **行业应用服务：**面向具体行业场景提供通用的应用服务能力，例如版权存证、数字积分、公示证书等。

Zig-BaaS 是开放的区块链云服务平台，不仅提供纸贵科技自主研发的区块链云服务，也提供第三方合作伙伴的云服务产品。Zig-BaaS 目前已提供了 Zig-Ledger 环境构建、Hyperledger Fabric 环境构建、Ethereum 网络接入、IPFS 网络接入、智能合约形式化验证等服务，为开发者提供了区块链网络按需部署、账本信息可视化呈现、智能合约一站式管理、应用服务快速对接的能力。Zig-BaaS 将持续与合作伙伴合作，不断推出更多区块链云服务产品。

## 区块链应用层

区块链应用层是 Zig-BaaS 面向用户提供的各个应用模块，包括区块链云服务、解决方案、合约中心、和生态社区等。

- ① **区块链云服务：**集成了多种类型的区块链云服务产品，是 Zig-BaaS 提供的核心服务；
- ② **解决方案：**面向多行业、多场景打造定制化的区块链技术解决方案，提供一站式的产品与服务，帮助企业客户落地区块链应用；
- ③ **合约中心：**提供众多优秀示例合约，支持开发者免费下载、学习、部署和调试，帮助开发者快速上手合约开发；
- ④ **生态社区：**将区块链相关的人、技术和企业等资源进行了融合，致力于在 Zig-BaaS 上打造繁荣的区块链生态。

Zig-BaaS 目前已经上线了区块链云服务、解决方案与合约中心模块，随着平台的不断建设与合作伙伴的加入，越来越多的应用和服务将会陆续上线。

## 区块链业务层

区块链业务层描述了可以使用 Zig-BaaS 云服务的多种行业场景，包括金融、能源、保险、物流、工业、农业、医疗、公益、文化等等。客户可以在 Zig-BaaS 所提供的基础服务之上，快速构建业务应用，满足自身业务需求，推动行业不断发展。

## 4.3 服务能力

### 4.3.1 区块链应用开发全过程支持

### 4.3.2 企业级区块链解决方案

### 4.3.3 开放的区块链服务生态

### 4.3.1 区块链应用开发全过程支持

一般来说，区块链业务应用的开发和上线，需要经历多个环节，包括业务逻辑设计、开发环境部署、智能合约开发、业务应用开发等。Zig-BaaS 作为区块链云服务平台，为开发者提供应用开发各个阶段的全过程支持。



Zig-BaaS 提供开发全流程支持

区块链应用开发的第一步，需要业务方对业务逻辑进行详细设计，并根据需求选择底层区块链环境。在这个阶段，Zig-BaaS 为开发者提供了多种类型的区块链环境，开发者可以灵活选择区块链的配置。

业务设计完成后，开发者需进行区块链开发环境的构建。Zig-BaaS 帮助开发者在云端一键部署区块链网络，并提供可视化的区块链浏览器，直观地呈现区块链的实时状态，展示区块链的节点、区块、交易和资产等信息。



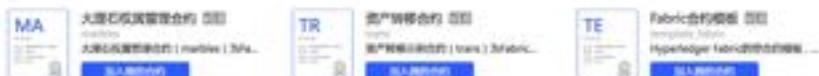
Zig-BaaS 中 Zig-Ledger 区块链控制台

接下来，开发者需进行智能合约的开发、调试和部署。Zig-BaaS 支持智能合约的上传、编辑、安装、部署、升级和可视化的调用调试，开发者可以在可视化的操作控制台中完成智能合约的开发与调试。同时，开发者也可以参考合约中心中的示例合约，基于现有的合约模板快速开发并实现所需的业务逻辑。

### Zig-Ledger



### Hyperledger Fabric



### Ethereum



Zig-BaaS 中 Zig-Ledger 区块链控制台

在业务应用的开发阶段，Zig-BaaS 面向上层应用提供了 SDK 或 Restful API 接口，支持区块链账本信息的查询，智能合约的调用以及账户与通证的管理等，便于业务应用的快速接入，极大地降低了开发门槛。

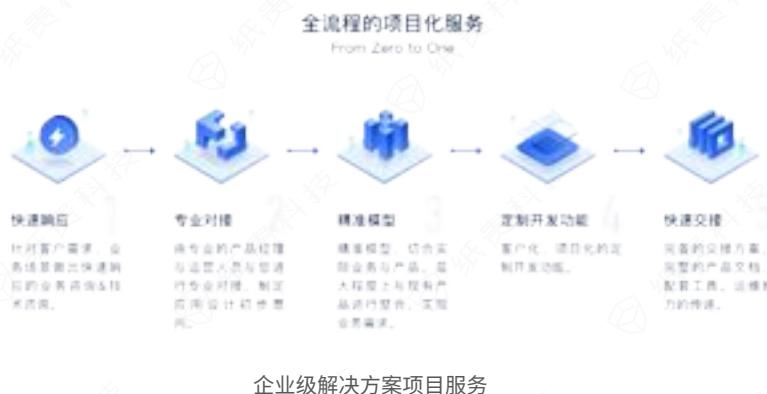
## 4.3.2 企业级区块链解决方案

基于 Zig-Ledger 区块链底层架构及配套的工具集，以及 Zig-BaaS 中众多的区块链云服务产品，纸贵科技面向企业客户提供企业级区块链解决方案。客户可以在多元、弹性的云平台上快速部署区块链环境，进行区块链应用开发、测试、部署和验证的全生命周期管理。

面向大规模生产级应用，纸贵科技企业级解决方案提供了全方位的技术保障，包括：

- ① 高性能：**从底层解耦复杂处理环节，消除计算处理瓶颈，实现商用级 TPS，满足企业长远发展。
- ② 高可用：**底层冗余链路设计，多链路高可用保障。
- ③ 高安全：**租户间网络深度隔离，保证数据不会越权获取，多副本备份，消除单点隐患。
- ④ 灵活的权限管理：**身份证书管理，支持多通道特性，提高数据安全性，为企业级应用提供底层权限管理能力。
- ⑤ 可扩展的系统架构：**遵循插件化设计风格，支持可插拔、可扩展的模块配置，包括共识、权限、加解密、手续费等。
- ⑥ 数据的隐私保护：**支持多样性的签名策略，支持国密算法，支持硬件加密与私钥保护，支持通过零知识证明、同态加密等密码学算法保护用户数据隐私。
- ⑦ 多链与跨链支持：**支持多链环境的部署与同构或异构区块链之间的跨链互操作能力，支持更加灵活的业务需求。
- ⑧ 灵活稳定的运维能力：**支持跨域、跨云的区块链网络部署，实时监控网络状态，自动化运维。

纸贵科技企业级区块链解决方案不仅包含 Zig-Ledger 等区块链底层及配套工具集，还包括上层的众多应用于服务，例如区块链通用浏览器和管理平台、面向行业的合约模板、可插拔的跨链或链外交互组件，以及全流程、定制化的项目管理与运营服务。



Zig-BaaS 提供的区块链云服务适用于丰富的业务场景，包括文化版权、供应链金融、医疗、零售、电商、游戏、物联网、公益慈善等，可帮助企业重塑其商业模式，提升客户可持续发展性以及在行业内的影响力，目前纸贵在版权、溯源、云计算、供应链金融、游戏等行业都有实际落地项目，将传统实业和颠覆性技术相结合，催化出新型生产关系，致力于打造一个真正的区块链生态体系。

### 4.3.3 开放的区块链服务生态

Zig-BaaS 作为开放的区块链云服务平台，积极拓展与合作伙伴的服务共建。Zig-BaaS 的合作伙伴包括 Hyperledger、EEA、CertiK、Codefine 等优秀的区块链技术社区与机构，也包括阿里云、金山云、华为云、京东云、青云等国内主流的云计算厂商。



企业级解决方案项目服务

区块链社区与机构与 Zig-BaaS 合作，在 Zig-BaaS 平台上共建区块链云服务产品，并实现区块链技术的能力升级。例如，作为以太坊企业联盟（EEA）的联盟成员，纸贵科技在 Zig-Ledger 中支持了以太坊账户体系，并研发了联盟链与以太坊之间的跨链技术，实现了区块链技术能力的扩展与升级。纸贵科技与 CertiK 公司合作，在 Zig-BaaS 中面向广大的企业客户，提供全球领先的形式化验证服务，保证智能合约和区块链系统的安全性。

云计算厂商与 Zig-BaaS 合作，将双方的优势资源连通、互补，共同为客户提供更加优质的企业级区块链服务。纸贵科技作为金山云的战略合作伙伴，为金山云区块链产品提供了源代码级别的技术支持，包括 BaaS 功能增强、易用性提升、共识优化、跨链交互等，为金山云的 "Project-X" 区块链全生态计划提供了坚实的支撑。

Zig-BaaS 将专注于技术研究和能力建设，与各行业合作伙伴携手合作，共同打造繁荣的区块链生态。

## 4.4 先进技术的融合与创新

Zig-BaaS 坚持自主研发和技术创新，希望通过探索新技术与区块链的融合，尝试为区块链赋能，拓展区块链的应用场景，提升区块链业务落地能力。纸贵将会在共识算法、密码学算法、分布式身份、去中心化存储、跨链互操作协议等方面展开研究，并通过 Zig-BaaS 平台将研究成果输出给广大用户，共同建设区块链行业基础设施。

### 共识算法

纸贵科技除了支持 Fabric 原生的 Kafka 排序外，还引入了多种拜占庭容错共识，如 Tendermint 和 RFBC。Tendermint 是一个使用 DPOS 共识，适用于强同步网络环境下，吞吐量较高的拜占庭容错算法。纸贵同时和国防科技大学联合研发了一种支持在弱同步网络环境下，节点记账权更加公平的高效拜占庭容错共识算法（Rapid Final Byzantine Consensus, RFBC）。为了满足在不同应用场景下对共识算法的需求，纸贵科技设计了可插拔的共识引擎模块，为了方便未来接入更多类型的共识算法。

### 密码学算法

密码学算法是区块链的底层核心技术之一，不同的应用场景，对密码学算法提出了不用的要求。Zig-BaaS 模块化的设计，可以很好的满足不同场景的需求。例如，在国内一些特殊行业，规定必须使用国密算法；在强调用户隐私保护、匿名性的场景中，需要使用零知识证明，甚至是同态加密等密码学技术；对系统性能要求高的场合，需要通过硬件加密设备提供密码套件服务。

### 分布式身份标识

分布式身份标识（Decentralized Identity, DID）是一种新型的可验证的数字身份形式，具有分布式、自主可控、跨链复用等特点。通过分布式身份标识与可验证声明，可以实现去中心化的身份管理。结合数字签名和零知识证明等密码学技术，可以进一步保障用户隐私不被侵犯。

### 跨链互操作

跨链互操作可以把不同生态下分散孤立的区块链平台，抑或是区块链与其他非链平台连接在一起，是区块链向外拓展和连接的桥梁。通过跨链技术，可以实现不同链之间、链上链下之间信息和价值的可信、有效流转。结合不同平台特点，实现复合型区块链应用。

## 链下预言机

作为真实世界信息进入区块链的通道，预言机为区块链提供了可信的外部数据接入服务。可以实现通过链下信息触发链上动作，打破了区块链与现实世界的信息壁垒。Zig-BaaS 提供的预言机服务，可以助力用户的链上平台轻松对接可靠第三方信息平台的 Web API，满足用户的业务需求。

## IFTTT

全称 "if this then that"，是一种跨平台交互操作技术，通过平台 A 的特定条件来决定是否触发平台 B 的特定动作。Zig-BaaS 通过提供 IFTTT 服务，为用户打通区块链与互联网、区块链与现实世界的连接。用户可以将自己在社交网络中的信息自动同步到链上，整个过程安全可控。也可以通过给某个设备的链上地址支付费用，自动获取其一段时间内的使用权。

## 数据安全共享

针对目前数据共享面临的数据安全、共享效率、隐私保护、过程可控等挑战，Zig-BaaS 提出了数据安全共享平台。利用数据安全分片、分布式加密存储、基于通证的访问控制、数据与服务解耦的安全计算、全过程链上监管等技术手段，实现了数据共享平台的安全、高效、保密和可控等特性。

## 形式化验证

纸贵科技携手合作伙伴，提供智能合约形式化验证服务，检验智能合约和区块链中潜在的安全问题。通过对智能合约全生命周期的验证框架进行潜在安全问题的检测，并针对区块链中常见的安全漏洞进行排查，向用户提供系统的验证报告和修改建议。

05

## 第五章 行业实践

---

## 5.1 概述

区块链技术的发展，离不开与行业的结合。通过业务落地也可以进一步推动技术进步，两者相辅相成，协同发展。目前我国“区块链+”行业应用主要集中在以下几个方向。

### 区块链+存证

从2013年1月1日起正式施行的新修订的《民事诉讼法》明确规定，电子数据也可作为证据。2018年9月6日，最高人民法院印发《最高人民法院关于互联网法院审理案件若干问题的规定》，《规定》共23条，规定了互联网法院的管辖范围、上诉机制和诉讼平台建设要求，明确了身份认证、立案、应诉、举证、庭审、送达、签名、归档等在线诉讼规则，对于实现“网上纠纷网上审理”，推动网络空间治理法治化，具有重要意义。在具体实施中，电子证据因为易修改，难以记录完整等特点导致公信力不高。利用区块链技术来建立和运营电子证据记录和保存系统，意味着电子证据一经存储，任何一方都无法篡改，并且电子证据会存储在每一个参与者处，帮助扫清电子数据成为有效的司法证据的障碍。作为“区块链+存证”的实际应用，我国首例区块链存证案，也于2018年6月28日，在杭州互联网法院一审宣判，法院支持了原告采用区块链作为存证方式，并认定了对应的侵权事实。

### 区块链+协作

典型的多方协作场景如：公益组织运营、跨平台活动开展与结算、大集团账目清算等。区块链技术应用在多方协作场景当中可以提升各方参与环节的透明性和公信力，提高各方的运转效率，降低各方参与成本。

具体，基础设施平台提供区块链技术支撑和运维平台，为多方协作中的数据传输、资源置换等基础功能提供底层支持。进一步地，可为各参与方对接信用和社交场景，引入激励、数据协作、信用等级等元素。最终，助力各方机构、监管、审计及其他企事业单位，构建起区块链协作生态体系。

### 区块链+金融

通过分布式多中心账本、数据时间戳不可篡改、交易记录可追踪可审计、支持跨平台认证与交互等区块链特性，提升各类金融场景中交易的透明性和公信力，提高各方的运转效率，降低成本。从而提高贸易的交易效率和安全性，去除纠纷、伪造品和不必要的风险。

纸贵科技结合自身特点，挖掘特定商业场景，在诸多领域探索如何有效运用区块链技术，为客户带来商业价值。并通过实践打磨自身技术，在深入钻研底层技术的同时，开发可以适配不同场景的产品。下面将以版权、溯源、积分、供应链金融等行业为例，介绍纸贵在自身聚焦的几类行业中的实践经验。介绍将会从行业自身痛点与区块链为行业带来的进步，如何组合产品模块、构建完整解决方案，梳理业务逻辑、发挥区块链优势等几个方面展开，希望能为读者带来启发。

## 5.2 版权

### 行业背景

2017 年，国内数字出版产业整体收入规模达到 7071.93 亿元，其中传统纸媒数字化收入占比增幅依然呈现下降态势，网络版权产业市场规模则达 6365 亿元，同比增长 27%，国民数字阅读率达 70%，数字化产品和服务在公共文化服务内容采购中的比例达 40%。而在 2017 年全年，盗版至少使 PC 端和移动端的付费阅读收入蒙受百亿元的损失，而盗版对网络文学行业带来的直接损失远高于此。网络文学盗版给整个行业带来的损失更是惨重。在版权保护方面，目前主要途径是登记著作权证书，由国家或地方版权局颁发，证明自己的作品原创权。著作权证书的登记价格为 800 元 / 每件左右，拿到证书需要等待 1-3 个月 [3]。

传统的版权登记方式，耗时往往很长，网络时代的数字作品具有产量高、传播快的特点，经过登记再发布早已经丧失了内容的时效性；且每次登记动辄费用上千，这就造成了大多数网络作者并不进行版权登记和保护，导致侵权频发。

在抄袭行为被发现后，往往要求原创作者拿出侵权证据，在作品未进行登记与保护的情况下，获取具有法律效力的证据更是难上加难。

在实际维权过程中，原创作者往往面临两难处境：内容分发平台的维权渠道手续复杂且效率不高，通过法律渠道进行诉讼的成本更高。导致大多数原创作者维权无门，只能选择沉默，任由权利被侵犯。

对互联网环境中的原创作者来说，能为其带来最大价值的是原创凭证和维权依据。针对作品的传播及交易需求，他们需要更加便捷、安全、可信、价格低廉的版权保护方式。从这个层面来讲，区块链的特性完美的满足了上述需求。

### 解决方案

区块链技术本身具有可定权、可溯源、不可篡改、分布式加密存储等特点，通过区块链版权保护平台，只需完成上传文件、确定作者、填写相关登记信息等简单几步操作，即可进行版权登记。在线生成的版权登记证书拥有区块链上唯一且可追溯的定权哈希和符合《电子签名法》的时间戳，一旦通过区块链技术完成了版权存证，即可联网查询版权登记信息，永久有效，无法篡改。

以“纸贵版权”区块链存证系统为例，在上传信息到拿到版权证书的同时，区块链版权存证服务将用户提交的申请人、作者、作品内容、存证时间等相关登记信息进行加密并上传至区块链网络中，完成区块链存证。“纸贵版权”引入公证处、版权局、知名高校作为版权存证联盟链的存证和监管节点，所有上链的版权存证信息都会经过多个节点的验证和监管，保证任何时刻均可出具具备国家承认的公证证明，具有最高司法效力。同时，通过在公证处部署联盟链存证节点服务器，存证主体即可视为公证处。在遭遇侵权行为时，区块链版权登记证书可作为证据证明版权归属，得到法院的采信。

[3] 《中国网络版权产业发展报告（2018）》

根据以上特点，纸贵科技有针对性的设计了区块链版权产品，通过加入可插拔的功能模块，使得产品架构能够很好的满足业务需求。其中的特色模块包括：

- ① 基于 PKI 体系的身份注册与身份验证**，将版权局、公证处、内容平台等生态参与方作为参与节点上链，保证各方在区块链上进行安全、可信的协作。
- ② 通过分布式存储技术**，将确权信息、侵权证据等信息安全、可靠的保存在分布式网络中，便于第三方进行查证。
- ③ 引入区块链浏览器模块**，提供链上信息查询服务，将用户授权的版权确权、侵权存证等数据公开，任何个人和机构均可查询，确保服务公平、公正、公开，促进行业健康成长。
- ④ 共识模块采用 Kafka 排序模块**，版权场景参与方均为具有一定公信力的机构，且针对确权、存证行为发生频率较高的特点，引入支持 CFT 的 Kafka 排序模块。在可信网络环境下，保证系统对于多点故障具有容错机制，同时尽可能提升系统吞吐能力。
- ⑤ 引入预言机模块**，确保侵权存证过程可信。在通过 URL 获取侵权凭证的过程中，引入验证机构约束取证行为，确保取证服务被约束为能且只能获取 URL 当前时刻对应网页内容，且该约束过程可被验证。
- ⑥ 将纸贵的区块链版权业务能力通过 SDK 与 API 接口进行整合并提供给第三方**，使得任何有版权服务需求的个人或组织，能够很快参与到纸贵的版权生态中来。



纸贵版权业务架构图

## 业务流程

区块链版权服务包含版权存证、版权检测追踪、侵权取证三个部分：

### ① 版权存证：

**1.1 选择文件、获取数据指纹：**选择需要存证的文件，通过哈希算法计算出该文件和关联信息的数据指纹。

**1.2 数据写入区块链：**在用户确认后，系统将得到的数据指纹写入区块链中，一经写入便无法篡改。

**1.3 获取存证结果：**根据用户需求生成存在证书供用户保留，也可根据用户需求，提供纸质书面报告。

**1.4 数字指纹验证：**根据客户需求，在用户需要对存证的指纹进行验证时，提供数字指纹比对查询。



版权存证流程图

### ② 版权检测追踪：

**2.1 作品哈希生成：**针对参与登记的版权作品，生成唯一的哈希值，并将其在联盟链上进行登记。

**2.2 全网检测：**提供重点网站自动化爬虫，将监测到的内容与作品进行匹配，相似度达到阈值自动进行侵权预取证操作。

**2.3 侵权匹配：**对已进行侵权预取证的内容进行持续追踪及进一步分析匹配。待确认侵权则直接进行侵权取证。

### ③ 侵权存证

**3.1 侵权取证:** 当发现侵权行为时, 快速调用版权服务中的侵权取证接口, 对侵权网站进行页面抓取取证, 并将取证结果保存在联盟链中; 系统对侵权 URL 地址进行域名解析, 通过预言机服务将 URL 对应的侵权内容进行存储, 并生成可供第三方检测的存证过程合理性证据, 将侵权行为固化为证据进行保存; 固化后的证据保存在区块链中, 数据永久存储且不可篡改, 符合法律对电子证据的要求。

**3.2 侵权追踪:** 对于已进行侵权存证操作的侵权内容, 版权服务提供持续性的侵权监控, 侵权追踪等服务, 确保侵权方对于侵权内容采取相应处理。



## 5.3 溯源

### 行业背景

溯源场景是目前区块链技术落地应用较多的一个场景, 目前已有多家企业开始从产品溯源这一细分领域切入市场。从区块链本身特征看, 弱中心化、开放性、自治性、信息不可篡改等特征, 和产品溯源拥有绝佳的契合度。

通过区块链技术的应用, 可以采集跟踪产品在生产、流通、销售、消费等环节的数据, 实现产品在原料进厂、生产加工、仓储物流、终端销售、市场消费的全链精细化管理, 可准确获得产品的流量、流向、流速信息。此外, 区块链技术还能提供出入库管理、库存管理、预警管理、物流监控、库存查询、渠道管控、窜货查询、消费者查询、统计报表、供应链执行管理、追溯召回、溯源管理、流向管理、移动营销、消费者管理、大数据应用、智能分析等服务。利用区块链的去中心化信息储存, 让众多节点共同维护数据的开放性和平等性; 添加到区块链的信息将永远被储存, 单个节点无法被篡改; 任何人都可以在公开的接口查询数据, 因此保证了信息的开放性和透明性; 上传到区块链的信息都具有时间戳的特性, 不可逆。

## 解决方案

纸贵区块链为溯源提供了产品、部署、定制化开发等服务，以及端到端团队保障、全流程的专业项目管理服务，通过灵活高效的 API & SDK，助力业务创新。可实现快速的业务集成和上线，保证业务系统运行稳定可靠。同时，针对溯源领域的特殊需求，纸贵也引入了特色功能模块，例如：

- ① **引入基于数字证书的身份标识体系**，将生产、物流、销售、消费等平台等各环节参与方作为节点上链，确保信息安全、可信及低成本的流转。
- ② **引入 DID (Decentralized Identity, 分布式身份标识) 和可验证声明技术**，为每一件商品注册唯一 DID，将产品信息写入 DID 描述文件中，各环节参与方通过 DID 为产品签发和校验可验证声明，实现产品全生命周期信息可信上链。
- ③ **引入二维码和 RFID 标签**，满足不同场景下对产品的标记需求；同时通过可信安全计算硬件，确保产品流通环节中由专人负责信息验证与可信上链，出现问题时可以精确定位到参与个人或设备。
- ④ **引入 Tendermint 共识机制**，通过引入支持拜占庭容错的共识算法，确保系统可以在任意网络环境下正常工作，在出现 1/3 以下节点作恶的极端环境下，仍可确保系统可靠运行。
- ⑤ **引入智能合约 IDE**，便于各参与方根据自身业务逻辑编写对应智能合约，实现链上信息的可信处理与流转。溯源系统架构图如下：



## 5.4 积分

### 行业背景

区块链具有分布式存储、不可篡改和价值传递等特性，非常适合与数字积分相结合。随着区块链行业的持续火热，越来越多的行业先行者开始尝试通过区块链技术优化自己的积分体系。除了传统的信用卡、航空、酒店等企业积分外，更多的行业用积分系统来优化自身业务，辅助用户运营。典型的行业包括互联网、电商、文化娱乐、内容媒体、甚至智能硬件，涌现出许多区块链积分应用。

基于区块链的积分具有更加多元化的产品形态，不仅仅打破了积分的概念和认知，甚至也超越了积分的功能。积分可以用于激励用户生产优质内容，可以用于鼓励生态参与者进行贡献等。通过区块链加密技术管理积分，让我们在数字生活中的行为产生价值回报。在社交、娱乐、购物、出行等方面，这些行为产生的价值得到重视，用户的数字行为得以资产化。基于区块链的积分有能力承载更多的功能与权益，并必将在未来发挥重要的作用。

传统模式中，用户间的积分交易需要通过第三方平台来完成。用户将数据上传到交易中心，由交易中心完成积分数流转和信息记录，用户对资产的查询和转移均由交易中心代为完成。对于中小企业而言，自建交易系统很容易存在安全漏洞，遭到恶意攻击。相比于实体商品，数据产品与仿制产品无差异性，在效用上也没有不同，很容易出现伪造现象。因此营造安全、可靠的积分交易媒介就显得尤为重要。

### 解决方案

纸贵科技推出的区块链积分业务主要包含以下三种服务：

- ① **区块链数字积分云服务：**面向广大具有内部积分需求的中小企业，提供基于公有云的通用积分云服务。通过低价的通用化云产品，迅速扩展客户规模，提升影响力。
- ② **单体区块链积分解决方案：**在原有单体积分解决方案上进行“区块链+”升级，扩充产品和服务组合包，向用户提供可选的区块链积分方案，满足大型企业内部区块链积分需求，为通用积分的兑换打下基础。
- ③ **区块链通用积分业务：**推出全新区块链通用积分业务，支持单体积分与通用积分的兑换，并享受通用积分的权益和服务。



针对积分系统对于数据隐私、安全性等问题的特殊需求，区块链积分方案选取了以下特色模块：

- ① 自主生成和管理的账户 - 地址体系：** 用户可通过离线工具生成私钥和公钥，并由公钥单向推导出账户地址，用户通过私钥操作该账户，作为与生态进行积分交互的载体，进行积分的管理和交易。同时，账户相关信息可以在链上持久化存储，有效防止信息丢失或恶意篡改，确保用户积分的安全。
- ② 基于数字证书的身份标识体系：** 支持对不同节点的分组和权限管理，可以实现第三方数据的可信授权访问，让数据查看权掌握在客户自己手中。
- ③ 数据加密技术：** 通过数据加密技术，客户可以将数据进行本地加密后再上传至区块链，加密数据仅自身可以解码，保证用户数据的隐私性。
- ④ 私有化部署：** 针对数据安全强需求的客户，可以实施私有化部署，实现数据的自我掌控，保证数据安全。
- ⑤ 跨链互操作：** 针对积分需要在不同平台、不同生态中进行流转的需求，纸贵积分区块链支持跨链互操作，使得信息、价值可以在不同平台、不同区块链上可信、安全流转。客户可以据此实现更灵活的业务及产品设计。

## 5.5 供应链金融

### 行业背景

供应链金融是基于真实的贸易，将核心企业与上下游企业联系在一起提供灵活运用的金融产品和服务的一种融资模式。在这个生态中由供应链上下游的全量业务数据驱动进行风险评估，而数据流的透明度与流畅性则是供应链金融发挥作用的重要基础。但在供应链金融业务实际运行过程中，小微企业会存在自有资金和融资渠道狭窄的境遇；核心企业的账期压力增大，且在供应商链条管理上的难度增加；金融机构由于信息不对称，在开拓小微客户上难以见成效，这些痛点一直制约着供应链金融市场的有效迭代和拓展。归根结底，获取真实性高、覆盖面广、有效的数据，是供应链金融风控的一把双刃剑。区块链技术具有价值传输和高效协同的特性，通过区块链的分布式账本等技术在供应链参与中的众多企业和金融机构间共建可信的信息网络生态，这个生态中每一个参与者都通过一个去中心化的记账系统共享各类信息。银行等金融机构根据链上的信息可以又快又好的进行授信决策，减少在数据收集、校验、评估等环节的时间，降低风险成本，进而提升决策的精确性并且提高效率。

具体而言，将供应链金融与区块链相结合，可以解决以下问题：

- ① **解决供应链上的中小企业融资难、成本高问题：** 区块链上发行的数字票据可以在公开透明和多方参与见证的情况下进行任意的拆分和转移。这种模式为大量原本融资困难的中小企业提供了机会，极大地提高票据的流转效率和灵活性，从而降低中小企业的资金成本。
- ② **解决供应链金融中汇票使用场景局限、转让困难的问题：** 银行等金融机构与核心企业之间通过构建联盟链生态，将供应链上的所有成员纳入其中，利用区块链多方签名、不可篡改的特点，使得债权转让得到多方共识，从而提高操作的简易性。
- ③ **解决供应链中金融节点和核心企业系统难以证实数据真实性、资金提供端风控成本高的问题：** 区块链具有可溯源、共识和去中心化，链上的数据携带时间戳的特征，这就屏蔽了存在侥幸的企业想要通过修改数据造假的可能性；打消银行对信息真实性的疑虑。由于每一个主体的信息都公开透明，这就能够在整个供应链条上形成一个完整且流畅的信息流，有助于参与各方及时发现运行过程中的问题，在针对性推出解决方案的同时，还有助于实现物流生态中商品的可追溯、可证伪和不可篡改。

### 解决方案

在实际的应用场景中，供应链金融系统对实时性、高并发、高吞吐、安全性等方面有很高的要求。纸贵科技提供的企业级解决方案，通过引入以下功能模块，很好的满足了以上诉求：

- ① **中心化的 PKI 体系：** 将相关企业、银行、保理机构、监管方等各参与方作为节点上链，通过链下确认与链上授权结合的方式，保证各方在区块链上进行安全、可信的协作。

- ② 高并发资产转移：**支持高并发处理从调用者账户转移指定类型资产至指定账户，满足原子转移、放重放攻击，并通过硬件安全设备实现对密钥的安全保存及转账操作的安全实施。
- ③ 国密算法支持：**国密算法是国家密码局认定的国产密码算法，采用国密算法实现密码学及安全服务，是国内金融、安全等领域对信息系统的基本要求，也是行业准入标准之一。
- ④ 修改底层数据库，引入关系型数据库 MySQL：**满足供应链金融系统需要在不同维度频繁查对企业信用、票据、资金等信息的诉求。
- ⑤ 引入零知识证明安全模块：**在保证有效传递参与企业信用的同时，保护各参与方商业隐私。

纸贵科技供应链金融业务将交易流、物流和资金流整合到一起，构建共识、不可篡改的信任基础设施，通过有效传递核心企业信用并保护商业隐私，促进产业转型与升级，推动供给侧改革，实现供应链环节中各主体全供应链共赢。纸贵科技推出的供应链金融业务主要包含以下服务：

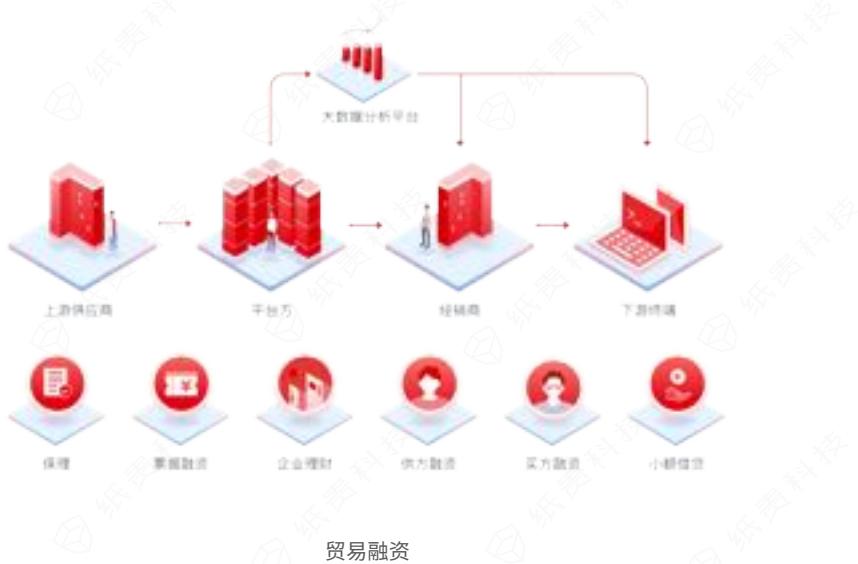
#### ① 应收账款融资：

链上各参与主体从源头上获取了真实有效的数据，资金需求方将企业各类信息上传到区块链平台，供货企业则履行筛选标的，票据摘牌的职责，应收账款信息与应付账款信息及时准确更新并同步给交易双方以及金融主体，将数字化信息及时与企业和提供动产质押融资的金融机构共享，资金供给方通过链上的数据进行信息刻画，降低信用评估流程和成本，提高融资效率，从而构建了全新可靠的供应链信用体系。



## ② 贸易融资：

记录联盟链上各参与主体资质、交易等信息，基于区块链的不可篡改性，主体之间交易流程清晰可见，以此为依托对各主体的交易、兑付情况进行建模分析，构建信用体系；通过对各参与主体减少线下采集审核信息所消耗的时间和人力，使各主体间公开透明地共享真实信息，真实勾勒企业的运营和资产情况，完成信用背书，动态评估融资服务，有效解决融资难的问题；通过提前回笼电商平台贷款，让库存快速变现，并基于此构建贸易良性循环融资生态。



## 5.6 对外合作

目前，区块链还在发展的初级阶段，还未形成成熟的技术框架与商业模式，同时也存在行业标准、法律法规的缺失。高校科研机构、区块链科技公司、行业龙头企业以及监管机构等各参与方，将在区块链发展的方方面面，起到中流砥柱的作用。各方之间的紧密联系、不断交流，是促进整个行业发展的坚实基础。纸贵科技努力推动、促进各方之间加强合作、互利共赢，共同携手推动区块链领域全面发展。因此，纸贵科技在对外合作领域进行了诸多实践。

### 加入 Hyperledger，打造跨行业区块链联盟，致力拓展不同行业的区块链应用

超级账本 (Hyperledger) 是 Linux 基金会于 2015 年发起的推进区块链技术的开源项目。成员除区块链技术开发公司外，还包含科技公司与其他产业的企业，目标是让成员相互合作开发来自多个不同行业的各种应用案例。截止 2018 年中，Hyperledger 的成员共有 200 余位，包括腾讯、百度、华为、万达、IBM、Intel、埃森哲、美国运通、戴姆勒、美国证券托管结算公司、摩根大通、三星等，范围覆盖北美、欧洲、亚洲及大洋洲等，影响力日益扩大。纸贵科技也在今年 1 月宣布成为超级账本的正式组织成员。

纸贵科技积极参与 Hyperledger 社区建设，将自身的技术能力回馈社区的同时，也为促进社区发展、扩大社区影响力做了很多积极有益的工作：参与 fabric、cello、fabric-sdk-py、fabric-sdk-node 等项目的开发工作；提交了 Fabric metrics、Fabric tendermint ordering service 的设计提案，实现了模块核心功能；参与了 Fabric enhanced concurrency control、Fabric fabtoken 等提案的设计与开发工作；组织或参与超级账本社区北京，深圳，武汉等地的 Meetup 十余场。

### 担任可信区块链联盟理事，集结国内领先精英，制定中国区块链可信标准

可信区块链推进计划由中国信息通信研究院牵头发起，主要目的是基于区块链技术，建立能够符合监管要求及各行各业需要的区块链体系。旨在推动区块链基础核心技术研究和行业应用落地，加快可信区块链标准的更新迭代，结合中国政策法规和业务逻辑，开发建立符合中国国家标准、业务逻辑和使用习惯的区块链技术标准，促进区块链行业良性健康发展，提升我国区块链国际影响力。目前，共有超过 158 家单位加入可信区块链联盟。2018 年 4 月，纸贵科技入选首批会员，成为正式理事单位。纸贵科技参与了可信区块链功能与性能评测，参与了联盟溯源、BaaS 等若干工作组的相关工作。

## 加入企业以太坊联盟，全面融入以太坊开发及社区生态系统

企业以太坊联盟 ( Enterprise Ethereum Alliance, EEA )，是基于以太坊建立的一个区块链联盟。作为全球最大的企业级开源区块链研究组织之一，EEA 致力于构建、推广和支持基于以太坊技术的最优应用、开放标准和开源参考架构。EEA 正努力将以太坊发展成为企业级技术，进行隐私性、机密性，可扩展性和安全性等方面的研究和开发。

纸贵科技与 EEA 联盟成员一起，共同促进以太坊区块链的完善，推动运用以太坊技术构建行业解决方案，为区块链产业的全面发展提供强有力的技术支持。目前，纸贵科技自主研发的区块链产品 Zig-Ledger，已经支持以太坊账户体系。同时，纸贵科技还研发了联盟链与以太坊之间的跨链技术，支持信息与价值在异构链之间的流转。纸贵科技的另一款重磅产品 Zig-BaaS 纸贵区块链云服务平台，同样支持以太坊开发环境接入，并提供以太坊智能合约的 IDE 以及形式化验证服务。未来还将在 Zig-Ledger 中引入以太坊虚拟机 ( Ethereum Virtual Machine, EVM )，全面支持以太坊生态中的各类应用。

## 联合顶尖学府，成立多家区块链实验室

实验室专注于区块链技术前沿研究、应用探索、知识传播、人才培养和项目孵化，主要工作包括：

- ① 进行区块链应用的研究，结合区块链技术的发展，聚焦于区块链在金融、健康、文化、能源等各大垂直领域的应用技术与商业模式创新等方面；
- ② 出版刊物、研究报告和专著，在重要学术期刊发表学术论文；
- ③ 为区块链专业人才的培养搭建研究平台，锻炼和培养具有国际视野的区块链领域专业人才；
- ④ 积极参与相关政策制定部门主导的区块链行业标准征询、研讨制定等；
- ⑤ 通过举办行业高峰论坛、会议、研讨会等形式促进政府、业界与学术界之间的交流合作。

目前已经成立的实验室包括：

**清华大学经管学院与纸贵科技——清华大学经济管理学院区块链金融研究中心：**中心主要承担了区块链应用研究，人才培养，促进政府、业界与学界交流等方面的工作。自中心成立以来，先后组织清华大学各院系教师 10 余位、本科生及研究生 30 余位，与纸贵研究院一起，在区块链技术发展，区块链技术在版权、供应链金融、新能源、溯源等领域展开了广泛而深入的研究。目前已发表 SCI 文章 1 篇、EI 文章 2 篇、高水平会议论文 2 篇（其中

一篇被评为 Best Student Paper），在投文章 3 篇。主办清华大学区块链应用与投资论坛、首届区块链产业发展论坛暨 2018 金融区块链创新应用高峰论坛、非标资产跨境交易项目与基于区块链技术的供应链金融和（跨境）贸易融资研讨会、区块链金融与投资研讨会等多次活动，促进政府部门、区块链企业与高校研究机构之间的交流与合作。发起、参与了区块链金融与投资联盟、北清金融科技创新联盟，围绕产学研融合发展、产业人才培养、科技深度孵化、贡献开源社区方面整合各方资源，为区块链产业提供新鲜血液，促进产业健康稳健发展。

**西安交通大学与纸贵科技——西安交大区块链与法律应用联合实验室：**发布《区块链深度专利分析报告》，系统梳理了区块链领域技术发展脉络，针对区块链技术本身相关的专利进行了检索梳理，并从发展趋势、区域分布、生命周期、技术构成、申请主体等多个维度进行了全面细致的分析总结。

**西安交通大学，Qtum 与纸贵科技——智能区块链技术研究实验室：**实验室自成立以来主要开展了区块链技术研究、课程培训两个方面的工作。研究了如何通过区块链技术记录电子商务交易中商家的声誉，相关论文已投 2018 INFOCOM；研究了基于区块链的“即停即付”的抢车位平台及其实现，相关论文已投 2018 NASAC。为计算机专业研究生约 100 人讲授《分布式系统原理》课程，详细介绍了包括数字签名、哈希散列函数、Merkle 树、时间戳、共识机制、容错与智能合约等区块链技术。

**西安电子科技大学与纸贵科技——西安电子科技大学区块链应用与评测研究中心：**针对政府、企业与个人之间的数据共享问题，设计了一个可信交互数据交易平台，用区块链技术来解决传感器数据的管理和安全问题；并运用智能合约实现交易的自动化，简化交易流程；同时对传感器数据进行合理的动态定价，提高数据交易的成交率。鼓励企业及个人更加积极地参与到城市中各项指标的监测中来，共同打造完善的城市大数据系统。

## 在其他开源社区的贡献

在其他区块链或相关技术的开源社区，也可以看到纸贵活跃的身影。

在 Tendermint 社区中，纸贵科技积极参与相关技术的开发与共享，在支持 secp256r1 算法、区块浏览器、以太坊虚拟机、归档功能开发等技术上，对社区有着积极有益的贡献；同时将 Tendermint 共识算法引入纸贵 Zig-Ledger 产品中，并将在实际应用中发现的问题积极反馈社区，与社区互相促进、共同发展。

在 IRISnet 社区中，参与 IRISHub 测试网络的公共评测，并提交 IRISHub 相关 issue；参与 Rainbow 在线数字资产管理服务的公开评测，提出几十项修改意见；参与 IRIScli 相关的开发工作，并编写了指令集实例及用户使用手册。

未来，纸贵科技也会进一步深化与开源社区、产业联盟以及高校科研机构合作，与各界有识之士一起，为推动区块链技术进步，区块链行业的健康、有序发展贡献力量。

v1.0



#### 联系我们

商务 & 市场合作: info@ziggurat.cn



纸贵科技订阅号



纸贵科技 VIP 客服