

阿爾山区块链平台白皮书

V1.1



扫一扫，了解更多信息

邮箱:hr@arxanftech.com
网址:www.arxanftech.com

北京阿尔山金融科技有限公司

2017.06

目錄

版本	1.1
版权	1.2
前言	1.3
阿爾山区块链产品介绍	1.4
商业目标及产品优势	1.4.1
系统架构	1.4.2
区块链即服务	1.4.3
运维平台	1.4.4
行业解决方案	1.5
数字身份标识及KYC	1.5.1
数字资产管理及交易	1.5.2
供应链及供应链金融	1.5.3
物联网及物流	1.5.4
附：区块链简介	1.6
什么是区块链	1.6.1
区块链的技术特点	1.6.2
区块链的历史和发展历程	1.6.3
区块链的意义	1.6.4

文档

版本

版本	日期	说明
1.0	20161128	
1.1	20170605	

作者

北京阿尔山金融科技有限公司

版权声明

本文件是由北京阿尔山金融科技有限公司（“阿爾山金融科技”或“本公司”）准备和提供，仅用于学习交流，转载请标明出处。

图片来源

除了来源注解，所有图片均出自北京阿尔山金融科技有限公司

前言

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。联合国、国际货币基金组织，以及美国、英国、日本等国家对区块链的发展给予高度关注，积极探索推动区块链的应用。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

关于阿爾山金融科技

致力于以科技创新助力金融行业发展，为下一代金融基础设施建设贡献力量。以区块链技术为核心，结合云计算、大数据、人工智能等前沿信息技术在金融领域的应用为发展方向，推进金融监管、支付、数字资产交易、供应链金融等领域的系统建设，构建透明、信任、智能化、高效率的新金融。

北京阿尔山金融科技有限公司作为金融科技的初创企业，秉承科技引领发展的理念，实施“创新合伙人”战略，希望通过协同创新，与金融机构、科研院所和业务伙伴开展深度合作，为加快推进数字化时代金融基础设施建设做出贡献。北京阿尔山金融科技有限公司致力于自主研发金融科技产品，推动区块链、大数据、人工智能等新一代信息技术和金融服务深度融合，加快科技创新和成果转化。

阿爾山区块链产品介绍

- 商业目标及产品优势
- 系统架构
- 区块链即服务
- 运维平台

商业目标及产品优势

阿尔山区块链平台定位为下一代金融基础设施，打造企业级的区块链平台。帮助金融企业快速搭建基础设施，方便集成应用，安全、高效得落地。

产品优势

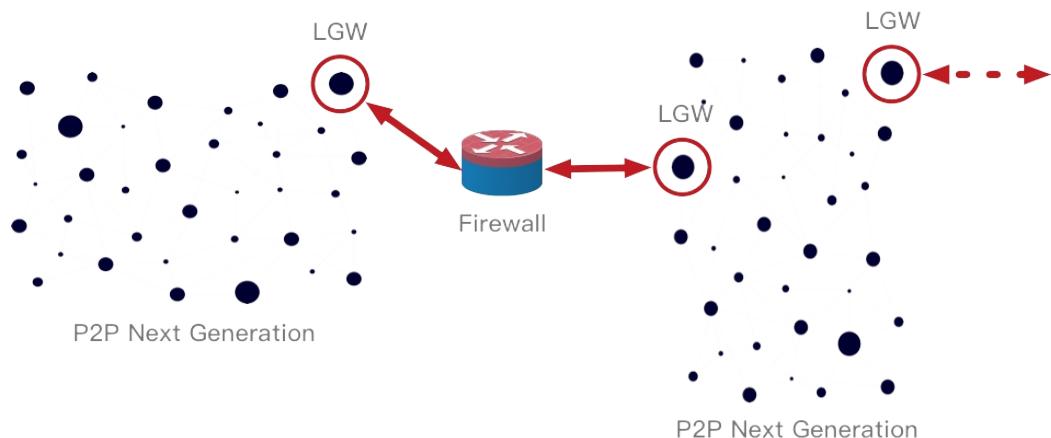
- 平台层面
 - 以“区块链即服务”（Blockchain as a Service）作为设计理念，适配多种云计算、容器、虚拟化技术，帮助企业级客户快速搭建基础设施
 - 预置多种基础业务模型及智能合约，定制化开发，实现快速应用对接
 - 数字身份认证
 - 数字资产管理
 - 数字钱包
 - 供应链金融
 - 物联网服务



内置基础业务模型及智能合约

- 采用微服务技术框架，弹性伸缩，可扩展性强，快速适应客户需求
- 平台内置一体化、可视化的运维管理平台，并提供完备的监控、告警功能，便于企业维护
- 存储层面

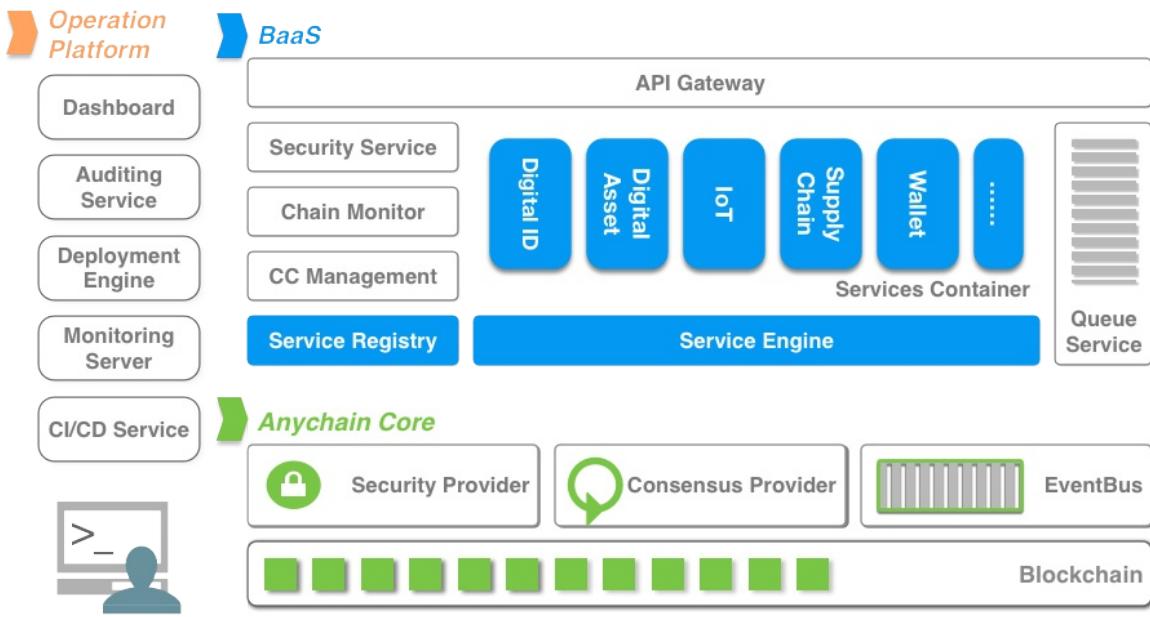
- 支持链上（On-Chain）和链下（Off-Chain）数据混合存储
- 支持分布式存储，并具备与企业现有存储系统对接的能力
- 内置IPFS 链下（Off-Chain）存储引擎
- 可适配多种对象存储服务
- 网络层面
 - 采用改进型点对点通讯协议（Peer-to-Peer Next Generation, P2P-NG）实现节点间的智能组网和通讯，并使得数据的传输效率大幅提升
 - 内置“账本网关”（Ledger-Gateway, LGW）组件，以适应金融机构/企业内部复杂网络



改进型点对点通讯协议和账本网关

- 安全层面
 - 内建CA服务，并可适配企业原有CA或第三方CA服务，节点授权接入，数据授权访问
 - 可插拔加密接口
 - 支持硬件加密(HSM)
 - 支持国产加密算法
- 性能层面
 - 采用多信道和多账本技术，大幅提高交易吞吐量
 - 根据不同业务适配不同共识策略，满足不同业务场景对交易吞吐量的差异化需求

系统架构



系统组件

- Anychain Core

- Blockchain

基于Hyperledger社区的Fabric v1.0框架及标准，在其基础之上，采用改进型点对点通讯协议（即Peer-to-Peer Next Generation, P2P-NG），提高了网络IO吞吐量。建立了高度自动化质量控制体系，打造稳定的，高质量的，适用于生产的企业级区块链发行版本。

- Security Provider

Security Provider是对社区的MSP (Membership Service Providers) 的增强版本，支持国密算法，支持HSM (Hardware security module)，和可信硬件终端。

- MultiChain

改进的多信道和多账本支持，以及多账本之间的相互访问，最终使得整个系统可以通过横向扩展来支持绝大部分应用场景对交易吞吐量的要求。

- Consensus Provider

在Hyperledger Fabric v1.0中，正如Fabric文档中提到的

“Consensus in v1 architecture is a broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.”

共识是对整个Fabric交易流程体系而言的，Endorser, Orderer, Committer等各组件协同完成共识。

阿爾山区区块链平台重写了共识架构，根据解决方案的不同，定制了若干种常用的共识策略，以适用于不同的场景和业务需要，如：PoW, PoET、PBFT、DPOS等。

- EventBus

EventBus（事件总线）是阿爾山区区块链平台的一个重要组成部分，它整合了Hyperledger Fabric事件功能，并跟业务场景相结合，为BAPP（Blockchain Application）提供了强大的事件驱动引擎。

- 区块链即服务（Blockchain as a Service, BaaS）

阿爾山区区块链平台为企业客户提供了区块链即服务来构造其私有链/联盟链。并同时面向企业和开发者，提供在云端搭建区块链的基础设施和快速开发环境，减轻企业运维负担。用户可以在集成管理平台一键构建区块链，并管理其智能合约。BaaS主要包括如下服务：

- 微服务网关
- 安全服务
- 区块链监控服务
- 智能合约管理服务
- 服务注册与发现
- 服务管理和支撑
- 队列服务

- 运维平台

阿爾山区区块链平台提供了对整个平台包括区块链、智能合约以及运行在平台上的应用服务的综合监控系统。并且提供多途径的告警和消息通知功能，告警策略可根据用户需要进行定制。同时集成了区块链节点管理，持续集成服务。具体功能如下：

- 区块链监控
- 监控服务

- 审计服务
- 部署引擎
- 节点管理
- 持续化集成及灰度发布服务

注：各组件的具体描述会在后续章节中说明。

区块链即服务 (Blockchain-as-a-Service)

BaaS是相对于私有链/联盟链而言的。公有链依赖巨大的点对点节点网络和机器设备来维护和强化去中心化基础设施，让比特币等区块链更加具有创新性。而私有链/联盟链需要企业投入大量手动开发工作和后端云计算支持，才可以搭建和维护其底层分布式基础设施。

阿爾山区块链平台为企业客户提供了区块链即服务来构造其私有链/联盟链。并同时面向企业和开发者，提供在云端搭建区块链的基础设施和快速开发环境，减轻企业运维负担。用户可以在集成管理平台一键构建区块链，并管理其智能合约。

Dashboard

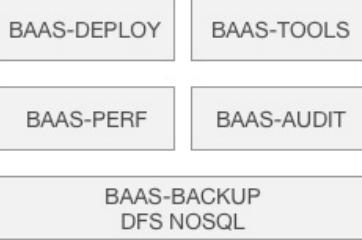


Proxy Auth

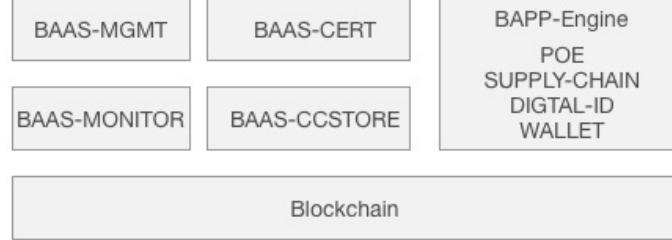
BAAS-PROXY

BAAS-AUTH

Operation Platfrom



BAAS Core



阿爾山区块链平台提供一套完整的区块链即服务解决方案，保证区块链平台在客户数据中心的快速搭建、测试和上线，方便区块链应用的快速落地。根据功能的不同，阿爾山区块链分为以下几个组件：

核心服务层

阿爾山区区块链平台保证区块链网络的授权接入、服务管理和状态监控。区块链节点经过区块链认证服务(BAAS-CERT)的证书体系授权后加入区块链网络，通过区块链管理服务 (BAAS-MGMT) 对区块链网络执行管理，区块链网络的运行状态信息通过区块链监控服务 (BAAS-MONITOR) 搜集。

为保证区块链应用的快速落地，阿爾山区区块链平台根据总结与客户对接应用的实际案例，形成了面向行业的内置的区块链应用元模板，包括数字资产、数字身份认证、供应链金融元模板等。客户应用落地场景可以直接基于内置区块链应用元模板开发，或者基于区块链应用原型模板的定制开发。通过区块链应用引擎 (BAPP-ENGINE) 保证了区块链应用与客户业务应用对接的统一标准。

区块链服务平台提供的内置区块链应用原模板包括**基础应用服务**和**业务应用服务**。



阿爾山区区块链平台打造了以数字身份认证为基础服务的应用服务平台，对区块链的参与者、资产和设备装置等提供统一的标识服务。包括：

- 用户
- 政府机构
- 组织机构
- 企业机构
- 数字资产
- 权益资产
- 设备
- 装置
- ...等

在基础应用服务之上阿爾山区块链平台同时为上层的业务应用提供了部分通用的基础服务，包括：

- 客户信息服务（KYC）
- 数字资产服务
- 存在性证明服务（PoE）
- 数字钱包服务
- ...等

利用这些通用的基础业务服务，企业可以实现快速应用对接，降低开发成本。

控制管理端

为方便区块链平台的管理，阿爾山区块链平台提供了运维管理终端（对接区块链运维平台）、区块链监控终端（对接区块链管理服务）和区块链应用集成终端（方便业务对接应用的链上数据统计和区块链应用状态监控）。

代理认证服务

为保证区块链服务平台的安全性和可扩展性，阿爾山区块链平台提供了区块链网关服务（BAAS-PROXY），用于实现对接协议的转化及保证多个区块链服务平台的扩展对接，并通过区块链授权服务（BAAS-AUTH）对接入区块链网关服务的请求进行认证。

运维平台

运维平台用于保证区块链平台及新区块链网络的快速、可靠、稳定部署，并提供必要的区块链服务工具用于查询和分析平台状态信息。提供区块链平台性能管理平台，对区块链平台做持续压力的并发测试及状态分析并提升性能。

运维平台

区块链监控



The screenshot shows the Arxan Blockchain Monitoring Platform. On the left, a dark sidebar menu includes '陕西' (Shaanxi), '菜单' (Menu), '总览' (Overview), '云平台' (Cloud Platform), '主机' (Host), '存储' (Storage), '微服务' (Microservices), '区块链' (Blockchain), '区块总览' (Blockchain Overview), '区块详情' (Blockchain Details), '网络拓扑图' (Network Topology Diagram), '列表' (List), 'HOST', and 'ChainCode'. The main area displays real-time metrics: 0, 0, 2, 6, 8, 5, and a large value of 26688. Below these are sections for '最近区块' (Recent Blocks) and 'TPS' (Transactions Per Second) and '节点' (Nodes).

区块编号	时间	交易数	前一个区块的哈希	哈希
2701	10秒以前	10	fskNhUqv7Oggsox3Y8Usru9GxZbKq4A91BwJJTr+IV8=	XD+HCRJWnYXl7sa0zb+8PSQfuQB0RHR8ztngwYtqlX4=
2700	10秒以前	10	73DQ28chR1wrcuw0o1BVud4BgewqcNC9BlVZbjekU=	8vTdSlhuQatNrTT3qb9ulNXKuASh+ejc80Ej500p+w=
2699	10秒以前	10	G5hdhTGxhGDEPh873T4BJNqzJwGHINsbRVBneu9HAH4=	dr6R+XjnNq37wd11SNRSE/Aa3qJBdC46jl6pcXqdm3g=
2698	10秒以前	10	IAJLIB24JUkJb1C+1k1grC54rYaBvX3iuYkc22H4cKg=	OUpbxKH8F+BdGAm5lcI6+k0WQhTjmKEqbhoz6lieUK=
2697	10秒以前	10	QV92Y48Tmhlpixl715tjn/y4lo6Hm4NAnTeXsSLnMtE=	eFsWktzuMZrP5kQwP56n6q6v0CYODXJLDLMS2ac8kTl=

TPS
131.9

节点
14

阿爾山区块链平台提供了对整个平台包括区块链、智能合约以及运行在平台上的应用服务的综合监控系统。并且提供多途径的告警和消息通知功能，告警策略可根据用户需要进行定制。

包括：

- 主机监控
- 网络监控
- 区块链节点健康状况监控
- 区块、交易及共识监控
- 智能合约监控
- 业务服务监控

节点管理

阿爾山区块链平台可以通过Web管理平台，命令行，SDK等多种方式，对区块链节点的生命周期进行管理。

包括：

- 颁发节点证书
- 节点证书作废及renew
- 节点加入及删除申请

审计服务

所有在平台中的操作以及对区块链中数据的查询操作都被记录到平台的审计日志中，同时写入到区块链中，以备后续查询及审计时使用。

监控服务

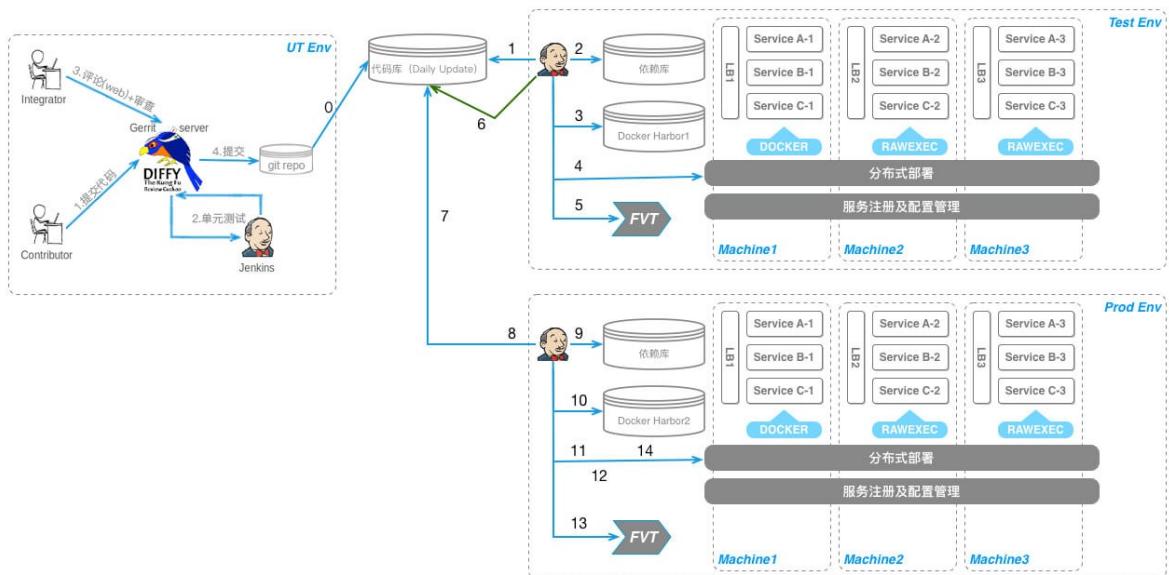
平台提供统一的、可扩展的监控框架，能够自动发现注册到平台中的系统及业务服务，并对其进行多项性能指标的实时监控。

部署引擎

强大的系统部署引擎，能够满足客户的定制化需求，方便快速的按模块化部署整个区块链平台。

持续化集成及灰度发布服务

阿爾山区块链平台内置了一整套完善的CI/CD系统，使得系统的升级更加安全和可靠。



行业解决方案

- 数字身份标识及KYC
- 数字资产管理及交易
- 供应链及供应链金融
- 物联网及物流

数字身份标识及KYC

目前我国对于泄露个人信息的处罚缺乏统一性和系统性，尚未形成一个统一的、关于个人信息保护方面的基本法，仅散见于民法、刑法等个别法律，且量刑偏轻。要彻底解决信息泄露问题，除了从源头上加强安全防护，不断修补网络漏洞，防止信息外泄，更关键的是要完善公民个人信息立法，抓紧制定《公民个人信息保护法》。

而在《公民个人信息保护法》尚未出台的背景下，两高出台相关《解释》，无疑有利于强化对于公民个人信息的司法保护。该《解释》亮点颇多：明确了“公民个人信息”的范围；明确了非法“提供公民个人信息”的认定标准；明确了“非法获取公民个人信息”的认定标准；明确了侵犯公民个人信息罪的定罪量刑标准。

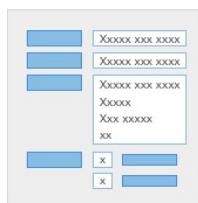
另外一方面，在国务院印发的《“十三五”国家信息化规划》中要求加强数据资源共享开发建设，打破信息壁垒和孤岛，构建统一高效、互联互通、安全可靠的数据资源共享体系。

如何在保护个人信息的情况下实现数据资源共享是本方案要解决的问题。

数字身份标识

阿爾山数据身份标识平台依托于区块链和语义网（Semantic Web）技术，主要解决以下四个方面的问题：

- 身份标识 对于个人和企业组织来说，首先要声明我是我，即：使用一个唯一的代码来标识自身。例如：我是某某，或我是某某公司，我的身份证号是什么，我公司的组织机构代码是什么。



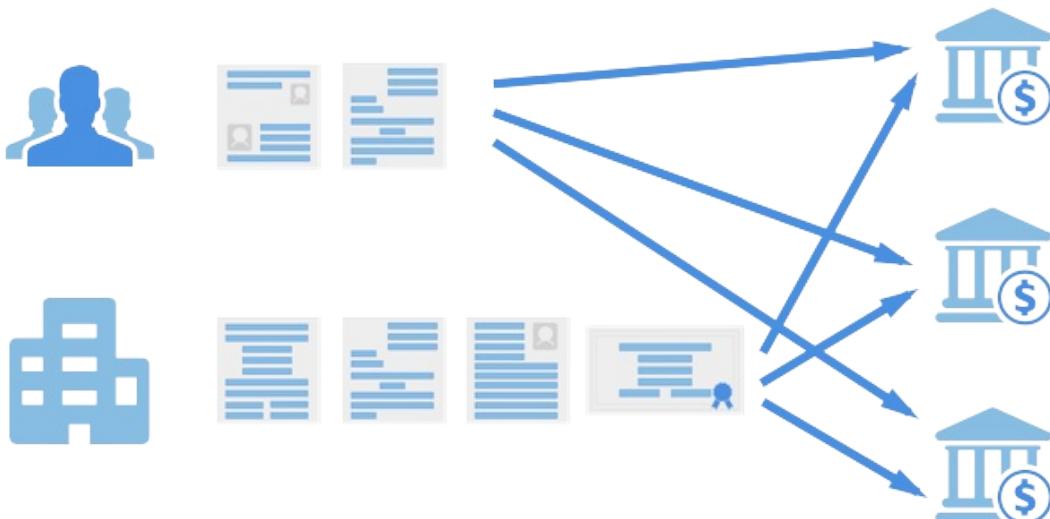
阿爾山身份标识平台基于数字加密技术为个人和企业组织提供唯一身份标识，并存储至区块链的分布式账本之中，同时使用语义网技术，附加各种身份证明信息。

- 身份相关信息证明 身份相关信息证明是为身份标识提供相关的证明文件，如身份证件，营业执照等。



阿爾山身份标识平台将这些证明文件以及同身份标识相关的数据信息（metadata）（如个人相关的家庭、住址、学历、工作经历、病历等，以及企业相关的纳税记录、采购记录、销售记录等）加密存储至IPFS当中，并将其Hash值记录在区块链之中，以保证其不可篡改性。可以快速方便的为个人和企业组织提供身份证明和相关信息记录查询。另外阿爾山身份标识平台，还采用先进的生物特征识别技术、为个人提供更加可靠便捷的证明方式。

- 信息授权 为保护个人及企业信息不被泄露，阿爾山身份标识平台采用授权机制来控制对个人或企业组织的信息访问的授权。任何对于数据的访问均需要拥有者对其进行授权，并将访问记录存储至区块链的分布式账本之中。



- 基础服务 阿爾山数据身份标识平台作为其它应用平台的基础服务，为其它上层业务平台（如KYC，数字资产、供应链以及物联网等）提供统一有效的数字身份标识服务。

KYC客户信息共享平台

KYC客户信息共享平台是阿尔山金融科技在数据身份标识平台之上打造出来一个衍生应用平台，其主旨在于相应国务院印发的《“十三五”国家信息化规划》中要求的加强数据资源共享开发建设。解决在保护个人信息的前提下，如何有效共享数据。

功能如下：

- 客户信息上链 企业的存量客户信息批量导入KYC平台。
- 客户信息更新 企业系统增量客户信息通过API每天定时更新到KYC平台。企业客户通过手机更新个人信息到KYC平台。
- 客户信息查询 企业系统通过API通过KYC平台查询客户最新信息。客户通过手机APP查询个人信息
- 分润结算和查询 KYC平台根据内定分润机制使用区块链钱包自动结算分润，系统相关角色可查询分润详情和使用记录。
- 客户授权 任何的企业系统初次查询使用客户信息，需要用户通过APP进行授权，才可查询使用此客户经授权的部分信息。



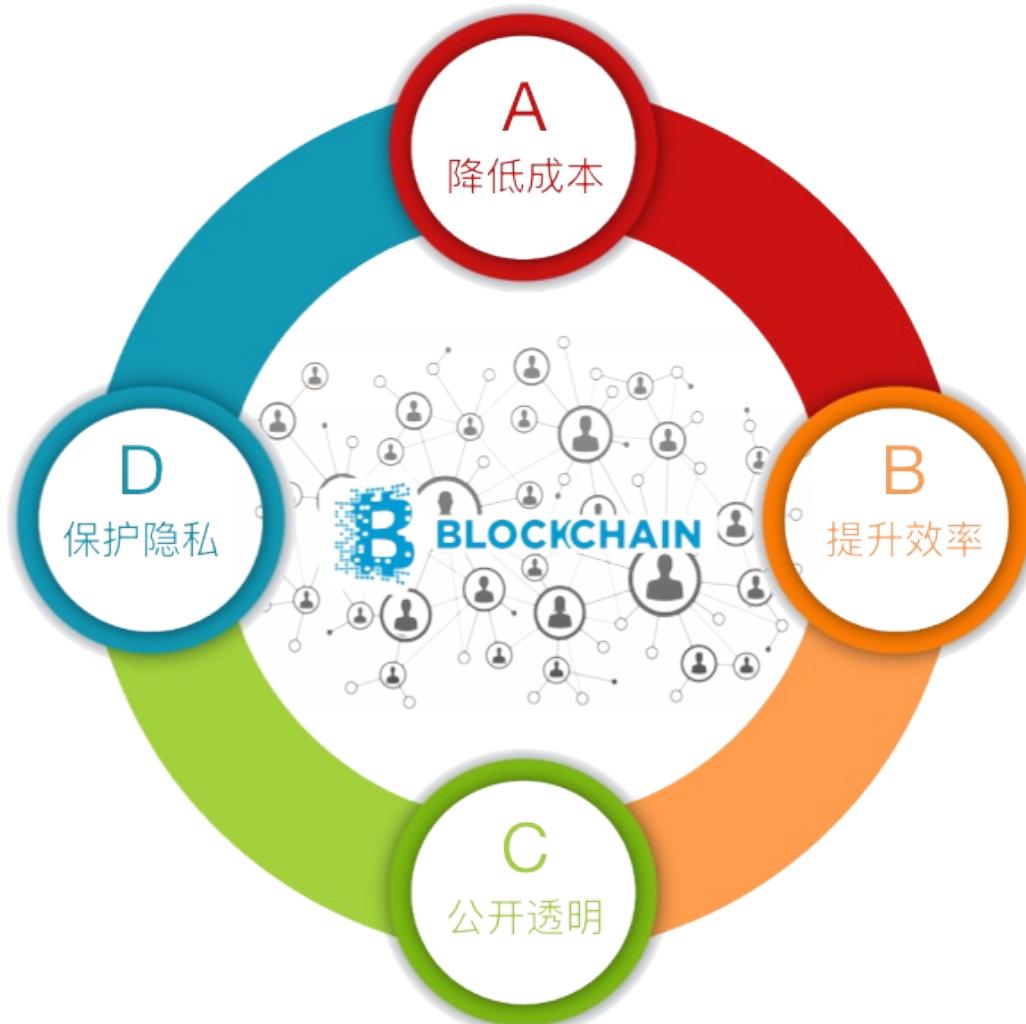
数字资产管理及交易

数字资产是指企业拥有或控制的，以电子数据的形式存在的，在日常活动中持有以备出售或处在生产过程中的非货币性资产。

数字空间的无限可扩展性、无限可复制性、多维可塑造性，可能意味着蕴藏在里面的待开发的海量财富，这些新财富的表现形式就是数字资产。除数字货币、数字股票、数字债券外，数字资产的范围比这要大得多，包括所有数字化了的资产，比如专利、版权、创意、信用等知识文化资产，视频、音乐、图画等艺术资产，还有在供应链各个环节的采购单、订单、发货单等等。

资产数字化对于企业内部来说，更是能降低成本和增加效率的最优解决方案。将隐私文件用技术手段进行加密和保存，安全性也会远远大于在实体中保存，毕竟现实不像电影，能将高级密码技术简简单单破解的人并不存在。而且数字化的资产也便于企业进行管理，当大资管时代来临，资产管理需要面对的资产种类成千上万，涉及到大量的计算，仅靠人工将无法完成。

基于区块链的数字资产管理及交易平台的特性



- 降低成本 传统的资产交易是需要第三方参与才能够保证其交易的真实性和公证性，无形中增加了信任的成本和效率。而区块链的分布式账本，不可篡改，可追溯等特性，降低了人与人之间信任的成本，从而达到去中介。
- 提升效率 在现在，资产交易转让办理很多手续，各种不同的部门或交易中心，效率低下，成本高昂。而区块链技术加上智能合约就能改善这一问题，资产持有人可以像买卖T+0的股票一样去交易股权，而且还同样受到法律保护。
- 公开透明 应用区块链技术就能解决信息不透明和资产公示不完全等问题，只要是设置好公开的数字资产，每个人都能查看，完全公开透明化。如有需要，甚至连谁持有多少的资产都能显示，还能避免一些黑幕交易，便于监管。
- 保护隐私 人们的信息在某些不良的公司中被标价售卖，在日常生活中不时接到一些推销电话，诈骗电话。而在区块链中，交易只显示一个标识，能有效地保护自己的信息，减少信息被公开兜售的可能。

供应链和供应链金融

真正的竞争不是企业与企业之间的竞争，而是供应链与供应链之间的竞争。这句话高度概括了供应链的重要性。

在很多行业中，制造成本的降低几乎走到了极限，销售额的增加也难有大的突破，对供应链的优化成了现阶段企业发展的必经之路。

供应链管理信息化将帮助企业建立高效、一体化的供应链体系，就如同在企业与供应商、分销商和终端客户甚至在整个行业之间建立了一条畅通的高速公路一样。

行业痛点

供应链的参与方都有投融资的诉求来盘活自己的流动资产，但核心企业的二三级供应商获得融资通常都很困难：

- 基于应收账款的融资
- 基于预付款的融资
- 现货质押类的融资

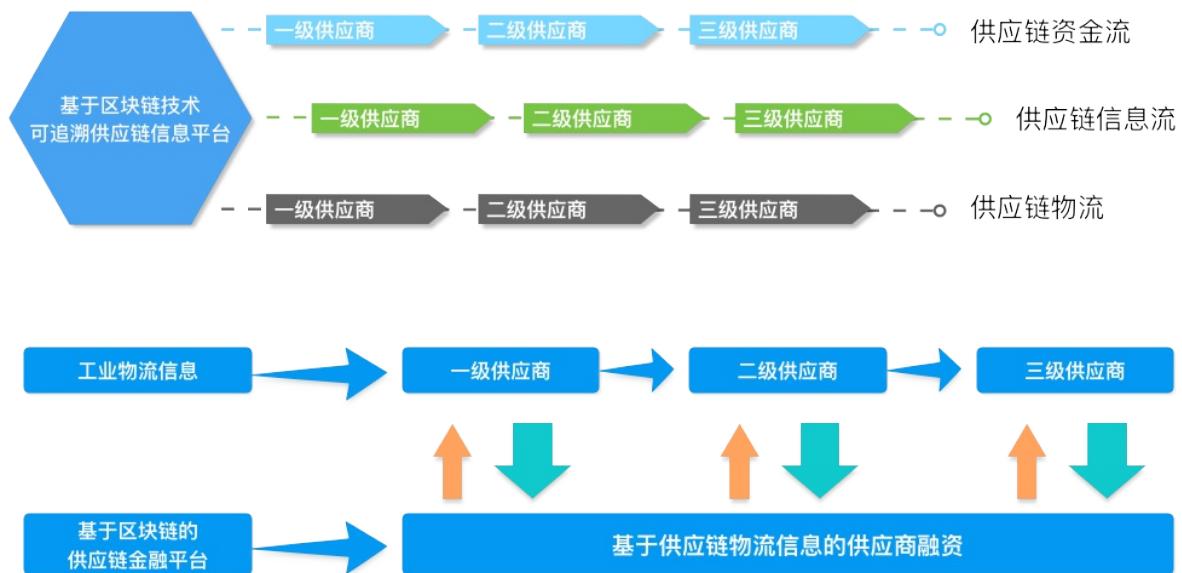
金融机构对企业信用了解不透彻，无法很容易的量化其信用等级，如何将核心企业的信用向其多级供应商进行传递，如何追溯订单等源头和链路是待解决的核心问题。

区块链和供应链金融的契合之处

区块链平台可以为供应链的参与者提供一个低成本可信基础设施，来注册、认证和追踪企业资产（如：商品、原材料、配件以及订单、发货单、收货单、发票、商票、银票等）。而所有的资产均可通过ID进行唯一标识，在区块链进行交易，而且这些交易是经过区块链加盖时间戳，并由交易方签名，加密存储在分布式账本当中。同时，部署在区块链上的智能合约可以自动完成支付、结算等功能。

阿爾山供应链金融平台

阿爾山供应链金融平台为企业提供一体化的供应链管理和金融平台，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，并保证其真实有效、不可篡改，除了凭证的共享，合同执行的过程也可以完整记录和跟踪，使得供应链中的核心企业的信用向下传递，降低金融机构的风控难度，提升企业融资的可行性，降低融资成本。



物联网及物流

物联网包含传感器、货物、车辆等移动的物体，基本上囊括了任何利用内嵌电子元件与外界通讯的设备。与区块链结合，有利于物联网设备和应用的整个生命周期的管理，是开展业务流程的助剂。可以试想一下这样的场景，联网物流货车可以利用私有链保证车辆的实时安全通讯、货品的实时监控，包括汽车起步、司机身份确认，使用传感器监控货品的温度、振动、位移等数据，利用智能合约交换燃料、保险和维修服务信息，提供实时位置信息，追踪车辆。

1. 在上述典型场景中，基于区块链的分布式账本可以为物联网提供信任、所有权记录、透明性、通信支持；
2. 区块链以安全的方式保存交易信息，利用去中心化服务器收集和存储数据的物联网架构可以把信息写入分布式账本，保证安全性和一致性；
3. 区块链上所有物联网交易添加时间戳，保证可追溯；
4. 区块链的真正创新在于智能合约，可以应用于区块链数据，在物联网通信中执行商业条款；
5. 物联网的最大缺陷之一是安全标准不到位，具备高端加密技术的区块链可以解决安全问题。

基于区块链的物联网及物流解决方案

阿爾山基于区块链的物联网及物流解决方案，是采用软硬件结合方式，从智能可信终端、电子标签、硬件传感器，到区块链软件平台，所定制的物联网及物流一体化解决方案，其中包括：

- 硬件设备
 - 智能可信终端
 - 电子标签及扫描设备
 - GPS, 硬件传感器
- 业务软件服务平台
 - 数字标识服务
 - 资产管理服务
 - 规划及追踪服务
 - 实时监控服务

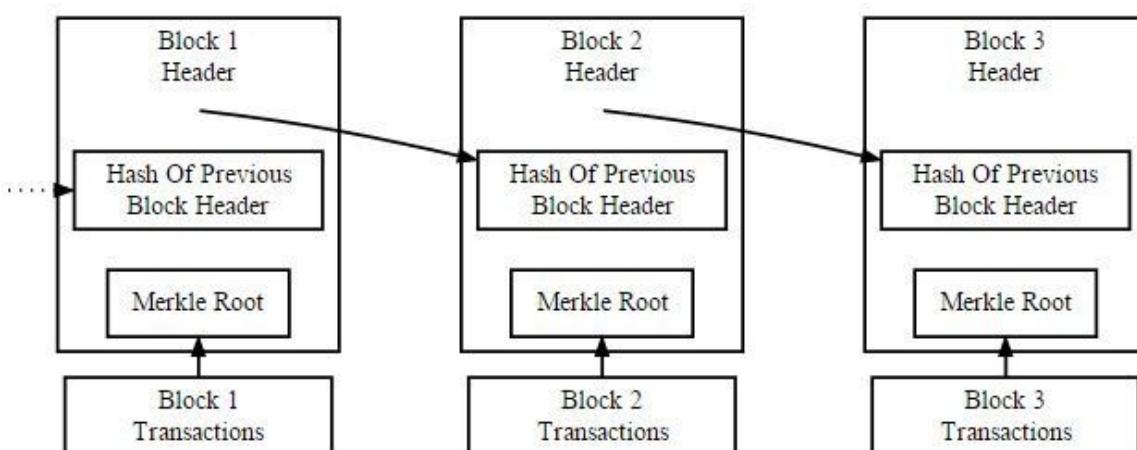
区块链简介

- 什么是区块链
- 区块链的技术特点
- 区块链的历史和发展历程
- 区块链的意义

什么是区块链

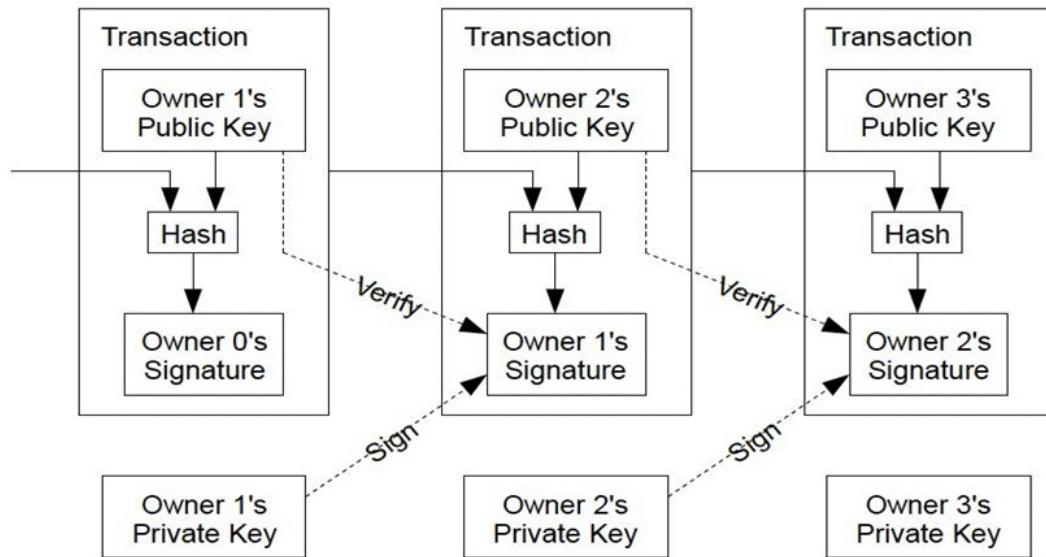
区块链是一个互联网协议和一种基础的数据结构。就如同HTTP是互联网应用层中最重要的应用协议一样，区块链也是应用层里一个点对点传输的协议。在协议基础上，区块链由“区块”和“链”共同定义了分布式账本。“区块”类似于证券交易中的成交记录，记录了特定时间段内所有发生的权益转移关系；这些“区块”间存在着严格且唯一的先后继承关系，组成了一条“区块”的“链”。区块链特有的机制保障了“区块”记录内容和先后继承关系的合理性和唯一性，这个过程并不依赖于特定的中心节点。

此外，区块链建立在IP通信协议和分布式网络两个技术基础上，实际上是一个分布式数据库系统，全球与该系统相关的数据都记录在一本公开透明的总账上。该账本数据库采用共识算法进行存储与维护，通过非对称加密算法构成安全保障，篡改难度极高。区块链技术具有去中心化、分布式账单、可靠安全以及透明公开等特点，将在网络、数据与应用层面提升并改造现有金融体系最核心的生产系统，给金融机构带来巨大的潜力和价值。同时，基于区块链的登记、结算、清算系统与智能合约两个方面可望实现应用层面的创新。由此可见，区块链的技术特点非常适合金融基础设施体系建设，也因此引起了全球金融基础设施机构的极大关注。



区块生成逻辑

图片来源 > <https://images.google.com>



在区块中，交易记录生成逻辑

图片来源 > <https://images.google.com>

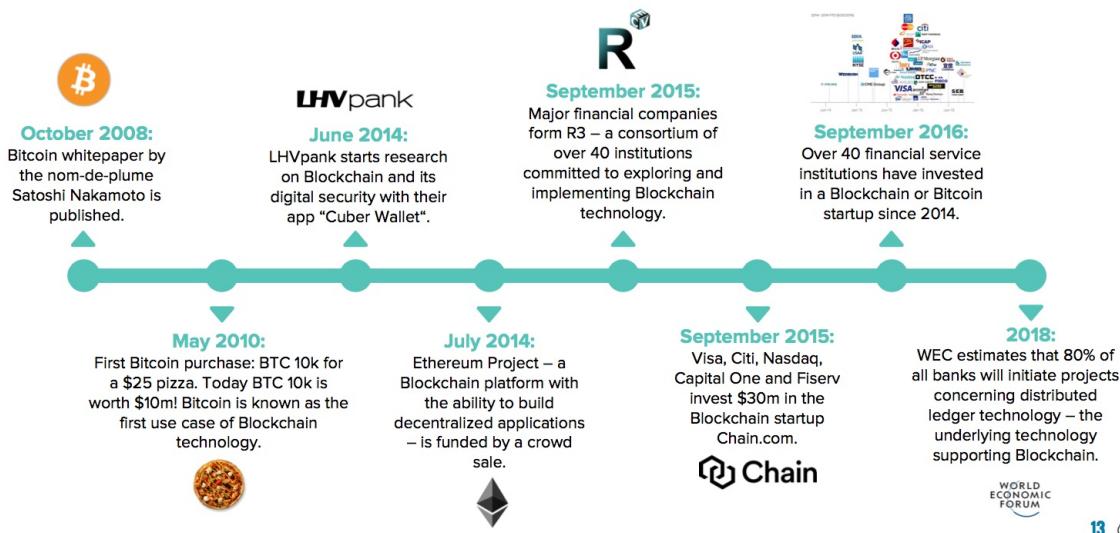
区块链的技术特点

只允许通过身份认证的用户加入网络，这样的区块链可以被叫做许可链，又可以依照其中节点的所有权而划分为联盟链(节点由一个企业联盟维护)或是私有链(节点由单个企业维护)。有以下特点：

- 去(多)中心化系统 (Decentralized), 通常没有中央机构或中心节点
- 通过共识机制 (Consensus), 来验证或确认交易
- 信任成本低 (Trustless), 由算法和加密证明来建立信任机制 (高度信任)
- 可编程 (Programmable), 具有智能合约 (Smart Contract) 功能
- 匿名性, 不可篡改性 (Immutable)

区块链融合了点对点 (peer- to- peer) 网络保证了无单点故障甚至多点故障，密码学签名 (cryptography) 使得每一个操作都可鉴权可审计，哈希 (hash) 数据结构使得所有的数据融为一体,无法单独修改其中的一点和共识算法规则 (consensus) 是所有节点能形成合力的关键。并且增加监管机构运行的节点,监督整个网络中的交易数据。

区块链的历史和发展历程



区块链的意义

- 降低信任风险。区块链技术具有开源、透明的特性，系统的参与者能够知晓系统的运行规则。在区块链技术下，由于每个数据节点都可以验证账本内容和账本构造历史的真实性和完整性，确保交易历史是可靠的、没有被篡改的，相当于提高了系统的可追溯性，降低了系统的信任风险。
- 交易过程扁平化，减低复杂度及成本。在区块链上，交易被确认的过程就是清算、结算和审计的过程，这相对于金融机构的传统运作模式来说能够节省大量的人力和物力。对优化金融机构业务流程、提高金融机构的竞争力具有相当重要的意义。
- 共同执行可信流程，是实现共享金融的有利工具。共享金融的本质是通过减少金融信息的不对称性，从而实现金融资源优化配置的目的，通过严格第三方认证和监督机制，保证交易双方权益的落实，促成交易达成。通过使用区块链技术，金融信息和金融价值能够得到更加严格的保护，能够实现更加高效、更低成本的流动，从而实现价值和信息的共享。
- 区块链技术具有灵活的架构。根据不同的应用场景和用户需求，区块链技术可以划分为公有链、私有链和联盟链几大类型，可根据机构的实际用途进行选择。
- 驱动新型商业模式的诞生。区块链技术的特点让它能够实现一些在中心化模式下难以实现的商业模式。比如在物联网产业，已经有机构提出要使用区块链技术管理上百亿个物联网设备的身份、支付和维护任务。利用区块链技术，物联网设备生产商能够大大延长产品的生命周期和降低物联网维护的成本。
- 区块链技术的开放性鼓励创新和协作。通过源代码的开放和协作，区块链技术能够促进不同开发人员、研究人员以及机构间的协作，相互取长补短，从而实现更高效、更安全的解决方案。现在区块链技术已经被视为下一代全球信用认证和价值互联网的基础协议之一，区块链技术对我国金融产业和金融体系的重要性同样不容忽视。