趣链科技
HYPERCHAIN

趣链科技公司与技术介绍

目录

第1章 公司介绍

1.1 基本情况

杭州趣链科技有限公司成立于 2016 年，创始人均毕业于浙江大学计算机学院，由中国工程院院士陈纯教授担任董事长。公司 170 余人的团队，90%以上为技术人员。其中 7 人具有博士学位，120 余人具有硕士学位。目前已经获得新湖中宝、国投高新、理想国际、兰石投资等超过 15 亿元人民币的 B 轮融资（约 2.26 亿美元）。

凭借自身领先的技术实力以及丰富的行业经验和资源，趣链科技在众多领域都取得了显著成绩。在金融领域，趣链科技与中国银联、上海证券交易所、中国银行间市场交易商协会、中国工商银行、中国农业银行、中国光大银行、兴业银行、浙商银行、北京银行、美国道富银行、葡萄牙商业银行、德邦证券等一大批国内外大型金融机构开展了区块链相关重要合作；在非金融领域，趣链科技也与谷歌、微软、华为等达成重要合作，是国际领先的区块链技术供应商。

1.2 公司目标

构建下一代可信任价值交换网络核心技术及其平台(联盟链)，并以此为依托，完成以金融业为核心的示范业务应用及通用行业解决方案。

1.3 获奖与荣誉

1. 入选杭州高新区（滨江）新一轮“5050 计划”；
2. 荣获 2017 全球区块链金融（杭州）峰会“区块链技术创新奖”和“区块链应用创新奖”；
3. 荣获首届中国区块链技术开发大赛一等奖；
4. 成为首批通过工信部中国电子技术标准化研究院区块链系统功能测试的区块链单位；
5. 成为首批通过工信部中国信息通信研究院“可信区块链平台”测评的区块链单位；

6. 荣获中关村创业大街“2017 创业先锋奖”；
7. 荣获创业黑马“2017 年度创业黑马企业级服务 TOP30”；
8. 荣获数据猿 2017 金融科技峰会“金猿奖-2017 金融科技优秀案例奖”；
9. 趣链科技成为中国支付清算协会金融科技专业委员会成员；
10. 荣获“2017 第一财经金融价值榜&年度区块链应用”大奖；
11. 荣获 2017 年度中国区块链行业优秀评选活动“先进个人”、“先进集体”、“优秀项目”三项大奖；
12. 成为中国银联电子商务电子支付国家工程实验室在《区块链成熟度评测报告》中优先推荐使用的区块链平台；
13. 成为唯一一家入选第 10 期微软加速器·北京的区块链技术公司。

第2章 管理团队

2.1 团队背景

团队核心人员均来自浙江大学超大规模系统实验室，具有深厚的技术功底和多年的项目开发经验。截至 2015 年，超大规模系统实验室及下属企业已完成开发的大规模信息系统 250 余项，累计开发经费超 12 亿元，技术方向包括金融信息系统、大数据与云计算。2015 年初，陈纯院士看到了区块链技术的先进性与广泛的技术前景，决定以超大规模系统实验室为依托成立区块链实验室，实验室由杨小虎、蔡亮教授领导，李伟博士、李启雷博士、邱炜伟博士、尹可挺博士、梁秀波博士等五名青年教师具体负责，并吸引了二十余位硕士、博士研究生加入。2016 年 4 月，随着研究的深入和合作的广泛开展，决定成立实体公司正式推动区块链技术的商业化进程，从而为业界做出更为直接和重要的贡献。

2.2 团队构成

陈纯：趣链科技董事长

中国工程院信息与电子工程学部院士，浙江大学计算机科学与技术学院教授，博士生导师，兼任浙江省计算机学会理事长。曾任浙江大学软件学院院长和浙江大学计算机软件研究所所长。

蔡亮：趣链科技副董事长

博士，副教授，浙江省重大科技专项专家。主要研究方向为区块链技术、云计算、网络安全技术，研究成果在国防、政府、金融得到了广泛应用。拥有国家发明专利两项，曾获得教育部科技进步奖一等奖、浙江省科技进步一等奖。

李伟：趣链科技 CEO

博士，毕业于浙江大学计算机科学与技术学院。研究方向为分布式系统及数据一致性。具有十余年金融信息技术工作经验。曾先后供职于微软亚洲研究院、道富银行浙江信息技术中心、Schooner 信息技术(硅谷创业公司)等公司。2015 年底投身于区块链基础平台即国产自主可控联盟链平台研发，2016 年创立趣链

科技，并主导了区块链技术的核心研发及在中国农业银行、中国银联、上海证券交易所、中国银行间市场交易商协会、浙商银行等大型金融机构的落地。同时，担任银行间市场区块链工作小组专家组成员，中国金融科技 50 人论坛特邀专家。

李启雷：趣链科技 CTO

博士，毕业于浙江大学计算机科学与技术学院，长期从事金融信息技术、分布式系统、大数据分析技术和移动互联网方向研发，对区块链共识算法和联盟链运行机制有深入研究。入选 2011 年宁波市领军和拔尖人才培养工程。作为核心研究员参与国家 863 计划和国家科技支撑计划，在国内外知名学术期刊和会议发表论文 9 篇，获得国家发明专利 1 项，软件著作权 1 项。

何鸿涛：趣链科技 COO

从事金融解决方案销售二十多年，熟悉交易所、银行、证券交易相关业务知识，曾在国内顶尖金融软件供应商及全球 TOP1 金融软件供应商担任营销总监，具有丰富的营销管理经验。

尹可挺：趣链科技 VP

博士，2010 年毕业于浙江大学后，担任浙江大学软件学院金融信息技术方向专业导师，从事金融信息工程及相关领域的研究生教学、科研及产业化工作，具有丰富的金融信息系统开发经验和扎实的金融信息化研究基础。2016 年作为联合创始人成立杭州趣链科技有限公司，专业从事国产自主可控区块链平台及应用研发，负责国内首个落地的采用区块链技术实现核心银行业务的应用项目的研发。在国内外知名学术期刊和会议发表论文 10 余篇，申请发明专利 6 项，获得软件著作权数项。研究领域为区块链、大数据等。

梁秀波：趣链科技 VP

博士，副研究员，主要研究方向为机器学习、区块链、移动互联网，曾赴法国进行为期一年的访问研究。主持或参与各级科研项目十余项、企事业单位委托项目二十余项。已发表 SCI/EI 论文十余篇，获得国家发明专利授权 3 项、受理

十余项。

邱炜伟：趣链科技 VP

博士，浙江大学计算机科学与技术学院博士后。主要研究方向包括软件可靠性工程、区块链、分布式系统可靠性优化与服务计算等。参与国家科技支撑计划、国家自然科学基金等国家级和省部级项目 5 项。在相关领域发表论文 5 篇，获得国家发明专利 1 项。

第3章 合作伙伴与应用案例

3.1 合作伙伴

趣链科技的业务场景分为金融和非金融领域，金融业务场景包括数字票据、电子存证、供应链金融、股权登记、债券交易等；非金融业务场景包括物流、仓储、数据交易、医疗、能源、智慧政府等。趣链科技构造国产自主可控的区块链平台 Hyperchain，并基于此平台先后与中国工商银行、中国农业银行、中国银联、中国光大银行、上海证券交易所、中国银行间市场交易商协会、浙商银行、北京银行、兴业银行、美国道富银行、葡萄牙商业银行、德邦证券、中钞智能卡研究院、浙江大学、上海数据交易中心、浙江甲骨文超级码、华为、万云、广电运通、上海积成、国家交通运输物流公共服务平台、中国物流金融服务平台等开展了区块链相关重要合作。

3.2 应用案例

1. 2016 年 12 月（浙商银行）

浙商银行基于趣链科技提供的区块链底层平台，国内首个实现核心银行业务的移动数字汇票平台正式上线，标志着区块链技术在银行核心业务的真正落地应用。

2. 2017 年 3 月（上海数据交易中心）

上海数据交易中心有限公司基于趣链科技提供的区块链底层平台打造数据交易清算原型系统，解决了大交易量情况下的交易记账、清算的处理和分布式环境下的信息分发、同步和存储等问题，并支持交易业务多样化。

3. 2017 年 3 月（上海证券交易所）

上海证券交易所联合趣链科技共同研发高性能联盟区块链技术，并在去中心化主板证券竞价交易的场景中进行验证，是国内证券交易所首次与区块链技术公司开展合作，标志着区块链技术在国内证券金融市场的加速落地和应用。

4. 2017 年 4 月（中国银联、中国光大银行）

中国银联与中国光大银行联合使用趣链科技区块链平台构建的多中心可信 POS 电子签购单系统已经完成初步测试，成功建立起业界第一个跨物理空间、完

全基于真正的互联网环境的联盟链，也是两家不同金融机构首次共同运维一个异地多活的分布式账本。

5. 2017 年 8 月（中国农业银行）

基于趣链科技底层区块链平台，中国农业银行总行上线了基于区块链的涉农互联网电商融资系统，于 8 月 1 日成功完成首笔线上订单支付贷款。这是国内银行业首次将区块链技术应用于电商供应链金融领域，标志着中国农业银行在区块链技术应用领域走在了同业前列。

6. 2017 年 8 月（浙商银行）

基于趣链科技底层区块链技术平台，浙商银行推出了业内首个基于区块链技术的企业“应收款链平台”。在该平台上，应收账款可转化为电子支付结算和融资工具。这也是继移动数字汇票平台之后，双方基于区块链技术的第二次深度合作。

7. 2017 年 9 月（华为）

在 HUAWEI CONNECT 2017 期间，华为和趣链科技签署合作协议，双方将在区块链技术平台和行业应用层面深入合作，借助华为在公有云基础平台的研发积累、服务能力以及企业实践经验，助力趣链科技打造端到端的一体化区块链服务。

8. 2017 年 9 月（万云）

趣链科技开发者平台开放公测后，万云部署了 Hyperchain 联盟链节点并成功接入趣链科技开发者平台的联盟链，趣链科技也作为万云的首批联盟链平台成功入驻万云，与万云共同保障联盟链节点和数据的安全。

9. 2017 年 12 月（浙江甲骨文超级码）

趣链科技携手浙江甲骨文超级码科技股份将区块链技术应用于农业溯源防伪项目，并设计和构建了一套全流程全产业链的防伪溯源 SaaS 云系统＋区块链应用底层技术平台，目前已经正式上线并投入使用。

10. 2017 年 12 月（中国农业银行）

中国农业银行基于趣链科技自主研发的企业级高性能区块链底层平台 Hyperchain1.2 在同业中率先上线基于区块链的金融数字积分体系（简称“嗨豆”）。借助趣链科技的区块链底层技术，将嗨豆的生命周期与农行原有的理财、快 e 宝、无卡取现等 23 类金融交易实现交叉。“嗨豆乐园”统一接口设计，已完成与农行

掌上银行、微信 银行、晚点 WIFI 等多个渠道对接，形成了初步的全渠道营销体系。目前已具备与第三方积分系统进行通兑的条件，这一前提可以将不同机构的不同积分系统使用区块链进行打通，做到数据共享，不可篡改的同时加强了不同积分的之间的流通性和使用频率，可以很好的解决目前很多积分客户活跃度不高的业务痛点。

11. 2018 年 1 月（德邦证券）

趣链科技与德邦证券共同搭建基于区块链技术的 ABS 管理平台，并联合券商、证券交易所、评级机构、律师事务所等建立联盟链，进一步促进资产流通并提高业务处理效率，最终实现资产证券化业务全流程线上管理。

12. 2018 年 1 月（中国工商银行）

趣链科技成功中标中国工商银行区块链项目，为中国工商银行提供区块链相关技术培训，帮助中国工商银行完善区块链底层建设，并提供技术支持，最终实现区块链技术在中国工商银行产品中的应用。这是趣链科技继中国农业银行后，基于区块链技术合作的第二家国有大型银行，也是与趣链科技深度合作的第七家银行。

13. 2018 年 1 月（医伴金服）

趣链科技与医伴金服就区块链在医疗供应链金融领域的合作达成一致，共同签署了战略合作协议：双方将在应收账款可信交易与管理、交易的全程追溯、跨机构的互通互利以及区块链技术在医疗产业链上的运用研究等方面展开全方位合作。同时，利用趣链科技区块链底层技术打通医伴金服“金医卫”的平台架构并实现跨机构的互通，从而大大提升医疗产业链金融的风控有效性和及时性。

14. 2018 年 1 月（银联国际、中国银行）

趣链科技为中国银联提供基于区块链的银联跨境汇款产品于 2018 年 1 月 28 日正式上线运行，趣链科技提供了从底层区块链平台至上层业务系统完整的区块链解决方案，在中国银行及银联国际两地同时投产，此次投产的区块链是真正意义上物理隔离、运行在不同机构的联盟链，解决了传统人工查询过程繁琐、电子化程度低、人工回复限时差别大、汇款体验差、汇出/汇入机构信息不互通、监管需求复杂的痛点，此次上线产品是中国银联在跨境汇款业务上的应用区块链技术的一次新尝试，具有里程碑意义，趣链科技在此次研发过程中展现了强大的研发

能力以及运维实施能力。

15. 2018 年 2 月（葡萄牙商业银行）

趣链科技与葡萄牙商业银行基于区块链技术达成重要合作，趣链科技助力葡萄牙商业银行将区块链技术应用到其相关支付领域中。

16. 2018 年 3 月（谷歌）

趣链科技拿下谷歌全球首份区块链订单，与谷歌开展全面合作，主要分为三点：一是在谷歌的员工福利管理系统中嵌入趣链的区块链技术，用以提高结算、清算的效率和安全性；二是在谷歌 1100 亿美元金融资产和其委托的摩根斯坦利、高盛等投行之间嵌入趣链的区块链技术，同样用来提高结算、清算的效率和安全性；三是在谷歌的云平台上嵌入趣链的区块链技术。

17. 2018 年 3 月（北京银行）

基于趣链科技提供的区块链底层平台，北京银行首个区块链新建系统--贵宾权益管理系统成功投产，趣链科技提供区块链平台至上层智能合约业务系统的完整解决方案。本次区块链平台实现两地三中心六个节点部署方式，实现了 VP / NVP 的自动切换功能。相比较传统业务渠道或业务系统，基于区块链技术的新系统可以实现多个业务模块的灵活对接，业务拓展型更高，解决了传统业务模式交互复杂、系统对接成本高的问题。并且，区块链技术提供了更为可信、透明且不可篡改的存储机制，为客户提供更为优质的信任体验。此次贵宾权益管理系统上线是北京银行第一个成功的区块链技术实践，趣链科技在本次项目中提供了核心的区块链平台服务。

第4章 技术背景

4.1 区块链市场

2015 年，世界经济论坛将区块链列为六大趋势之一。当前利用区块链技术的创业公司热门业务领域为智能合约、证券清算\交易、资产管理、电子商务、物联网、社交通讯、文件存储、身份验证、预测市场、数据 API 等方面。区块链势头将起，各行业领头企业就纷纷发布区块链相关研究报告。高盛投资研究部门发布报告预测区块链技术可以简化证券的清算结算，每年为美国资本市场节省 20 亿美元，为全球资本市场节省 60 亿美元；而在支付领域，如果采用区块链技术，全球每年可以节约 5500 亿美金的支付成本；前摩根大通高管、“CDS 之母”Blythe Masters 认为区块链技术有机会为企业改善结算延迟以及提高系统的安全性，而区块链应用市场的规模最终将以万亿美元计。一系列的研究报道说明，区块链技术的整体市场前景非常广阔。

近几年资本市场助力区块链更快发展，越来越多的资金流入区块链相关初创企业。据 Algonomic.com 报告显示，2015 年，风投资本家在比特币和区块链投资近 10 亿美元，而在区块链领域投融资总额约为 4.74 亿美元，同比增长 43.51%。截止至 2016 年底，区块链领域累计投资超过 18 亿美金。相比较 2012 年累积的 200 万美金，区块链领域得到的投资增长 900 倍。其中获得投资金额最高公司分别是，国外 DAH A 轮融资金额 5200 万美金，国内矩阵金融融资 1.5 亿人民币。

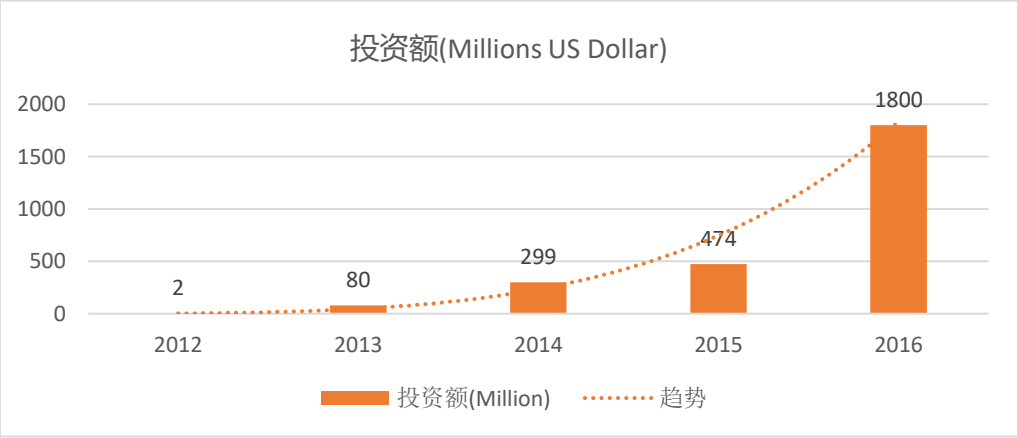


图 4-1 区块链领域 5 年投资金额比较

区块链技术当下炙手可热，2016 年起大量的区块链相关公司相继涌现。然

而大多数此类公司均聚焦于基于区块链的上层应用开发，且技术基本以开源的以太坊或 IBM Hyperledger Fabric 为主，较少聚焦于底层技术改进或技术创新。但是，随着区块链技术的普及，相关应用的不断涌向，目前开源技术已经不能完全适合大量应用的需求场景，众多企业级特性亟需开发与完善，比如数据加密、共识算法、合约安全、数据分区等等，均需要一个技术上更为领先且可靠的企业级平台作为技术支撑；同时，涉及到金融等关键的关系到国计民生的领域及政府的监管需要，也迫切需要有一个国产自主可控的企业级区块链平台，为上层应用提供有力的安全可靠的技术保障。

切实的市场需求为趣链科技的核心平台提供了广阔的市场前景，让趣链科技更加坚定地研发基于联盟链的国产自主可控区块链底层及其应用服务平台。趣链科技正在以此为目标快速前行。

4.2 区块链技术介绍

2016 年 1 月 20 日，人民银行在北京召集了一次数字货币研讨会，与会者包括人民银行、花旗银行、德勒公司的数字货币专家，就数字货币发行的总体框架、货币演进中的国家数字货币、国家发行的加密货币等议题展开研讨。在这次会议上，提出“早日推出央行发行的数字货币”的目标，并要求研究团队明确央行发行数字货币的战略目标。其实早在 2014 年央行成立了专门的研究团队，重点研究关于数字货币的技术、发行流通、法律问题、对现有经济体系的影响等。数字货币的底层建设就是区块链，**原央行行长周小川曾表示区块链技术具有保护个人隐私、无法篡改的特性，是未来数字货币的可选技术之一。**

4.2.1 定义

区块链技术本质上是利用非对称加密技术对交易进行数字签名，通过共识机制达成多节点一致，其中数据以链式区块形式组织存储的分布式账簿系统。这些数据块包含了多个交易的信息，相互串联而成，每个数据块包含了上一个数据块信息的哈希值，使得链成的数据难以被攻破和篡改。

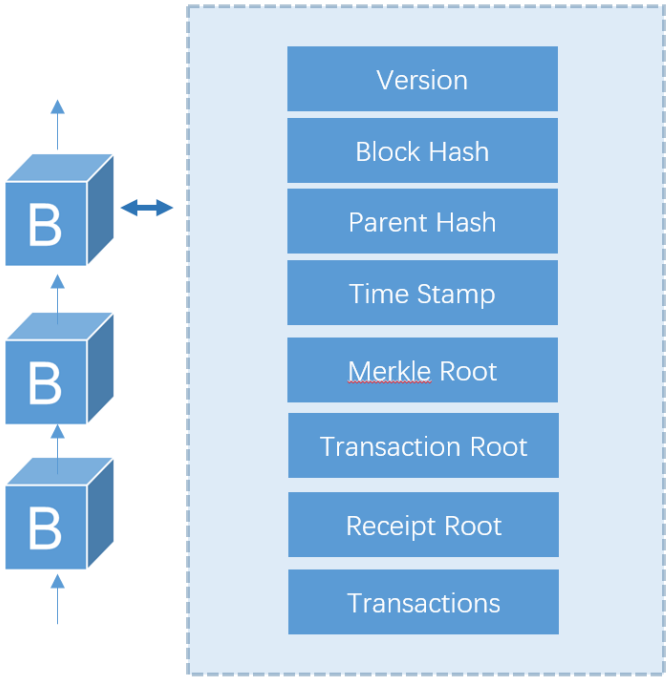


图 4-2 区块链结构概念图

4.2.2 特性

- 多中心。区块链中每个节点都存有一份完整的数据，多个机构之间数据实时同步，实时对账，多参与方之间在区块链网络中互相监督。
- 完整。数据完整储存在全球各个节点上面，其中一个节点如果被毁坏，不会影响整个网络的数据安全。
- 可信任。区块链上的每笔交易几乎无法修改，信息分布在几千几万个节点上，无法摧毁，也无凭空伪造出一笔交易。
- 公开。较低的数据公开成本，同时也支持分级加密。且所有交易与资产的生命周期都记录在区块链上，用户可以持续追溯。
- 自动。智能合约完全自动运行且不需要监督。大幅度改进商业模式，提升日常运营效率，降低营运成本。
- 安全。改变区块链上的数据所需要的代价非常高，一般意味着要控制 51% 以上的算力，成本昂贵，几乎不可能做到。

4.2.3 分类

区块链根据网络扩展性、节点的可参与性及其功能价值，可以分为公有链、私有链和联盟链三种模式。

- 公有链。任何人都可以作为节点参与区块链网络。货币提供交易验证激励，容易进行应用程序大规模部署，全球范围可以访问，不依赖于单个公司或辖区，匿名性强，任何参与者都可以在中写入、读取、参与交易验证（例：比特币）。
- 私有链。针对单独的个体或实体。交易验证成员范围，系统内不需虚拟货币提供奖励（例：总行可以联合其各城市分行，完成内部数据传输备份，转账等业务）。
- 联盟链。节点为事先设定，并通过共识机制确认，新增的节点需要通过联盟的准入。一般不需要数字货币提供交易验证激励。联盟链容易进行节点权限设定，拥有更高应用可扩展性。联盟链可大幅降低异地结算成本和时间，比现有系统更简单，效率更高，同时继承去中心化优点减轻垄断压力（例：商业银行加入 R3）。

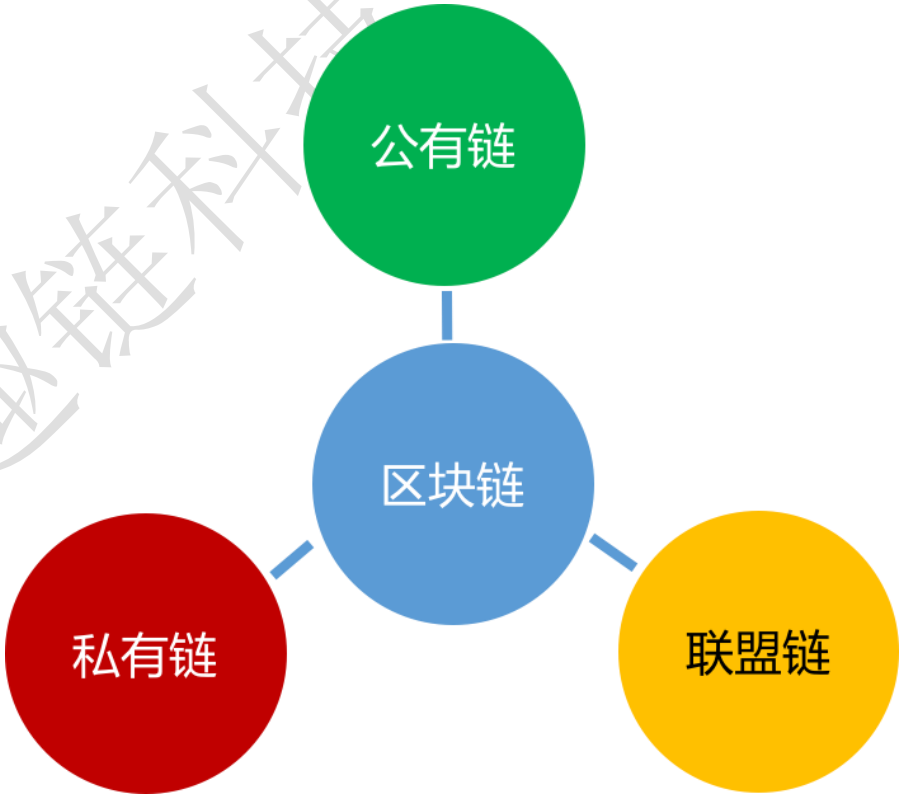


图 4-3 区块链分类

区块链解决了现存最根本的问题就是不平等和不对称，在《区块链革命：比特币背后的技术如何改变货币和商业世界》一书中，作者 Don Tapscott 表示，互联网允许人们进行欺诈，收集我们的数据，侵犯我们的隐私，如果下一代互联网，不仅能够用于信息的通信，还能直接用于价值和金钱的直接通信呢？如果我们能够建立的商业，能够实现 P2P 式的交易，而无需强大的中介机构呢？区块链将成为这一变革的核心。区块链不仅仅是记录金融交易，它几乎可以记录任何有价值的东西。

4.3 区块链生态

4.3.1 价值传输

区块链构造了可靠的价值传输网络，通过分布式账本和智能合约，实现数字资产和其流通逻辑的底层支撑。传统的中心化业务模式，价值传输必须要通过一个可信第三方，由第三方完成各方之间传输价值的对账、清算、结算，过程繁琐复杂，消耗资源和时间。通过区块链技术，参与各方各为中心，通过区块链底层技术及智能合约制定，方便快捷完成实时对账、清算和结算的动作。

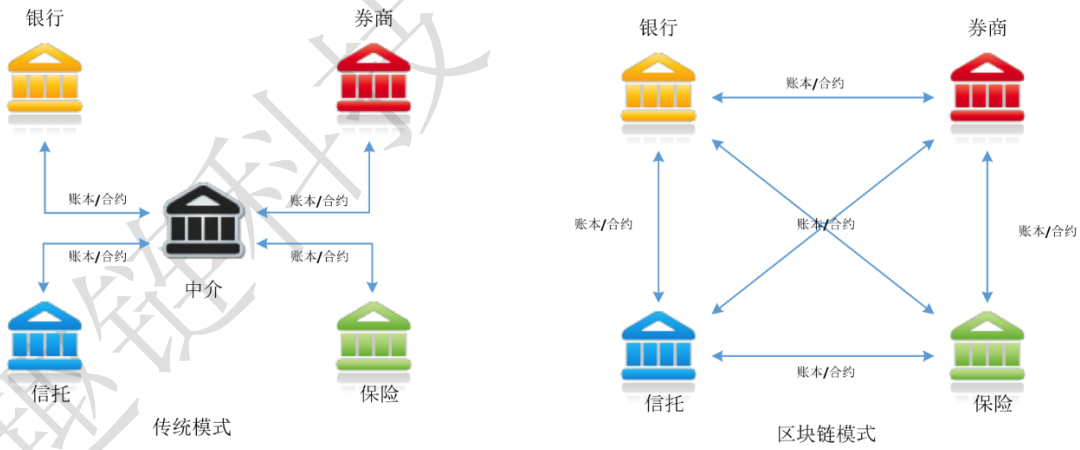


图 4-4 区块链生态-价值传输

4.3.2 业务协作

区块链改变了传统的业务协作模式，从传统的依靠基于业务流的低效协同升级为不依靠任何中介节点但是由平台保证基本业务流程的低成本、高效率、高可信协作系统。同时大幅度降低单点业务复杂度，任何机构只需要关心自身业务逻辑即可。

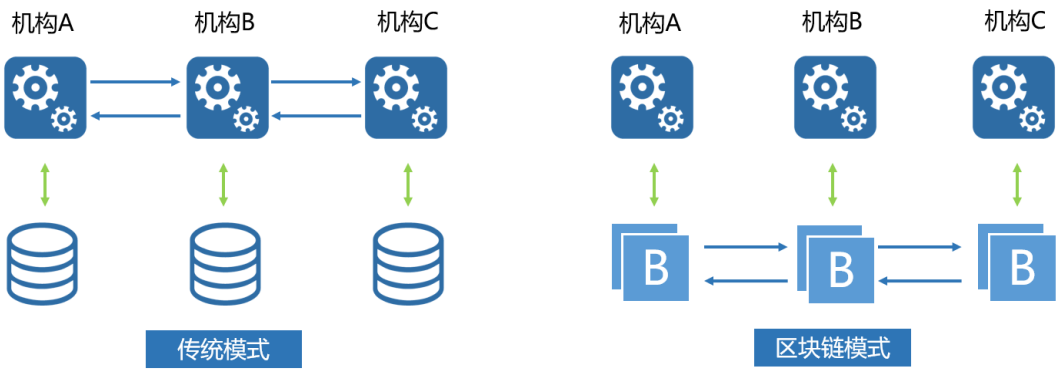


图 4-5 区块链生态-业务协作

4.3.3 现存问题

区块链技术无论在金融界还是在技术界，均显示出了巨大的技术与应用前景，其可以重新建立人与人之间的信任网络，大幅度提高信息传递的可靠性与智能化，从而从根本上产生对现有互联网的变革力量。

正如前文所言，目前的区块链公司主要是使用开源平台，诸如以太坊、Hyperledger，在此基础上进行应用和服务的搭建。但是这**两种当下最为常见的平台，并不能适应于当前所有业务场景的需求。**

1. 传统比特币/以太坊的 POW 工作量证明，适应于公链，但对资源消耗严重，且存在 51%攻击问题，系统分叉问题与记账性能低下问题等等。所以，业已基本形成共识，主流企业级应用是无法基于比特币/以太坊进行构建的。
2. Hyperledger 采用了适合金融应用的 PBFT 共识，客观上更适合金融业的需要。但目前的研发仍不完备，缺少隐私保护与分级权限机制，智能合约引擎使用简单的 Docker 容器存在安全隐患，需要升级与优化，而且作为国外开源项目并不支持国内金融业需要的国密算法。

所以目前的已有技术均处于初级阶段，不适合金融系统的核心需求，开发一套自主可控的区块链底层平台，完全具有技术的可行性。

同时，区块链作为金融等核心系统的底层支撑技术，关系到国家的金融安全与各个行业的底层技术安全。所以，开发一套自主可控的区块链底层平台，完全具有战略上的必要性。

所以，为了适应企业和产业联盟应用场景的需求，趣链公司的 Hyperchain 区块链平台孕育而生。

第5章 产品介绍

5.1 总体目标

趣链公司将以 Hyperchain 联盟链服务平台为技术支撑，以区块链行业应用为导向，将 Hyperchain 服务平台和区块链行业应用两条线并行发展。

Hyperchain 服务平台面向企业、政府机构和产业联盟的区块链技术需求，提供企业级的区块链网络解决方案。区块链行业应用着眼于区块链技术的实际落地，以业务场景合作为主要模式，在关键行业推出标杆型应用，对行业痛点针对性的提供基于区块链的解决方案。同时以实际需求推动 Hyperchain 联盟链服务平台的技术发展。

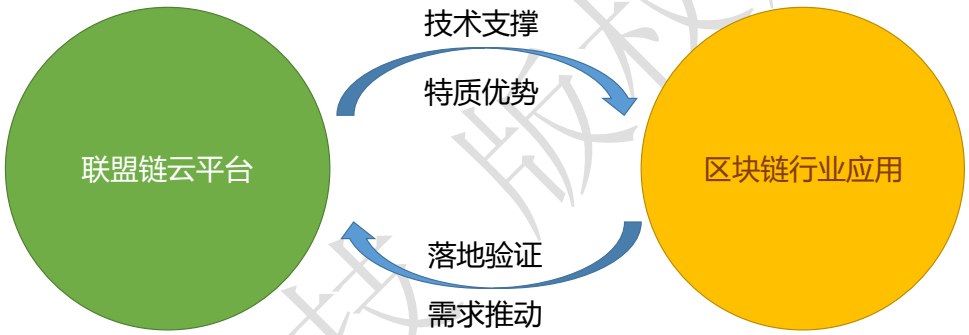


图 5-1 总体目标

5.2 技术路线

5.2.1 技术概述

趣链科技研发的国产自主可控区块链底层平台 Hyperchain 面向企业、政府机构和产业联盟的区块链技术需求，提供企业级的区块链网络解决方案。满足企业级应用在性能、权限、安全、隐私、可靠性、可扩展性与运维等多方面的商用需求。Hyperchain 支持企业基于现有云平台快速部署、扩展和配置管理区块链网络，对区块链网络的运行状态进行实时可视化监控，是符合 ChinaLedger 技术规范和国家战略安全规划的区块链核心系统平台。Hyperchain 平台具有高吞吐量和低系统延迟的特征，其交易吞吐量高于 10000 笔 / 秒，系统延迟低于 300 毫秒。

在中国银联电子商务电子支付国家工程实验室首度权威发布的《区块链成熟

度评测报告》中，趣链科技 Hyperchain 在各方面均优于 Fabric 和商业区块链 B。中国银联更在报告中建议各类企业优先选择趣链科技，足见趣链科技处于行业领先水平。

5.2.2 技术架构

趣链科技 Hyperchain 联盟链平台由三个部分构成：包括企业级管控平台、联盟链核心模块和底层系统支撑技术系，体系结构如下图所示：

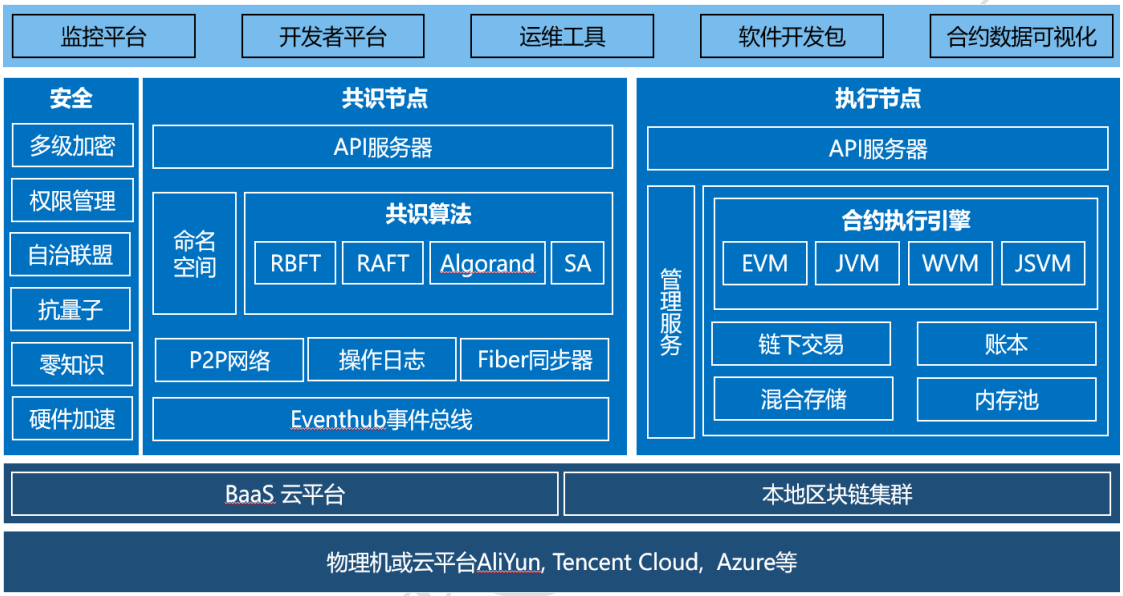


图 5 -2 技术架构

5.3 核心特性

5.3.1 验证节点授权机制

Hyperchain 通过 CA 认证授权实现联盟链准入机制。当一个新成员被准许加入联盟时，他将自己的公钥以及必要的身份标识信息发送给证书签证机构 CA。然后，CA 根据这些信息，为其颁发证书，作为加入联盟的许可认证，证书实际是由 CA 签发的对用户的公钥的认证。新成员发送消息时，需要附带自己的身份信息，其他节点收到该成员的消息时，对其身份进行认证，如果认证失败，则无法参与记账。所以，只有通过 CA 授权的成员，才会被联盟中的其他节点承认。

为解决 Internet 的安全问题，Hyperchain 采用 PKI 体系结构采用证书管理公钥，通过第三方的可信机构 CA，把节点的公钥和节点的其他标识信息捆绑在一起，在网络中验证节点的身份，将节点分为验证节点（参与共识记账）、非验证

节点（参与部分区域记账）监管节点（参与全网记账）。

PKI 体系结构把公钥密码和对称密码结合起来，实现密钥的自动管理，保证网上数据的机密性、完整性、有效性。

5.3.2 基于密码学的多级加密机制

5.3.2.1 多级加密安全机制

Hyperchain 采用了可插拔的加密机制，首先实现了椭圆曲线数字签名算法（ECDSA）对交易进行签名，防止消息被恶意篡改；其次通过 ECDH 密钥协商技术对传输层数据加密，保证交换双方可以在不共享任何秘密的情况下协商出一个密钥，然后根据该密钥对称加密进行安全的网络数据传输通信；最后通过 Hyper－key 对数据进行加密存储，保证了原始数据本身的加密。

多级加密实现了以下几种安全机制：

1)数据安全：实现安全哈希算法，为消息生成体积小、不可逆的数字指纹。

2)身份安全：实现数字签名算法对交易进行签名，防止交易数据被篡改。

3)通信安全：实现密钥协商技术对传输层数据加密，保证通信双方可以不共享任何秘密进行加密通信。

4)机构安全：实现基于 CA 的权限控制与准入机制。

5)交易安全：命名空间隔离，保证交易信息可以只存在于交易相关方。

6)信息安全：通过 Hyper-key 对数据本身加密存储于区块链中。

5.3.2.2 国密支持

在国密标准下，平台利用 SM3 密码杂凑算法对消息进行消息摘要，利用 SM2 椭圆曲线公钥密码算法对消息进行签名，平台根据 SM4 对称加密算法对广播消息进行加密传输，使平台具备了基于国密的安全机制。

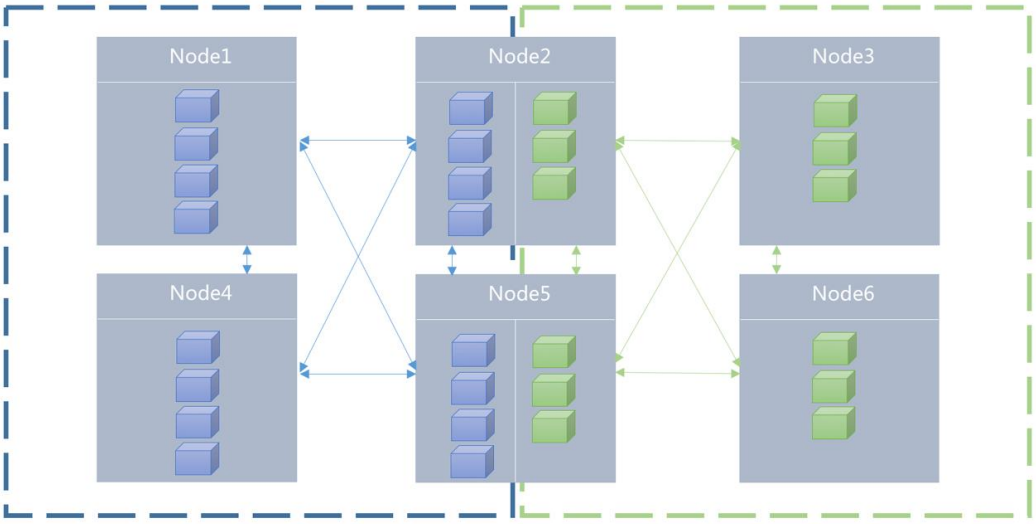
5.3.2.3 隐私保护

在隐私保护方面，Hyperchain 区块链平台提供 Namespace，同态加密，合约访问控制三种机制。

1. Namespace

传统区块链网络中各个节点维护同一份全量账本，所有节点对系统内部任何交易和数据拥有访问权限。这种交易数据的存储方式不能做到敏感信息的细粒度控制。Hyperchain 设计基于 Namespace 的分区共识机制通过区块链账本的分区维

护，交易的分区共识实现了敏感交易数据的存储和执行空间的隔离。Namespace 机制允许部分区块链节点创建属于它们的 Namespace，这些 Namespace 成员之间的数据交易以及存储对其他 Namespace 中节点不可见。Namespace 中允许授权节点的动态加入和退出，单个 Hyperchain 节点支持授权加入任意数量的 Namespace。



2. 同态加密

Hyperchain 通过同态加密的加密思想实现区块中交易金额和账户余额的加密。同态加密是基于数学难题的计算复杂性理论的密码学技术，它的概念可以简单的解释为：对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。同态加密算法的这个特性，可以使验证节点在不知道账户的余额和交易的金额的情况下，进行交易合法性验证，并将通过验证的交易记录到区块链上。经过同态加密的交易验证时间约为 10 微秒。可以满足 Hyperchain 每秒上万笔交易的需求。

Hyperchain 采用 Paillier 同态加密算法。Paillier 同态加密算法的数学难题和 RSA 是类似的，并且因为新增的随机数 r 破解难度高于 RSA。

3. 合约访问控制

合约编码者可以在合约中定制合约函数的访问权限。目前 Hyperchain 能够支持运行用 Solidity 编写的智能合约，Solidity 中提供了一种权限修饰符的语法，该修饰符在函数被调用时进行合约部署者与合约调用者的地址比对，倘若合约的调用者地址与合约部署者的地址匹配，则进行正常的函数调用，反之此次调用直接返回。通过这种方式，合约编码者可以在合约中为一些高权限的函数设置权限控制，使得该函数只能被固定地址的调用者调用，从而实现访问权限控制。

5.3.3 基于 RBFT 的共识机制

在公有链中被证明有效的 POW 共识机制在联盟链中面临诸多挑战，其交易确认时间长、吞吐量性能低下、严重依赖算力竞争的记账确认机制存在安全隐患。另外，在联盟链的应用场景中存在大量高价值标的交易，这些交易的机制与节点验证激励机制无关，因此 POW 的算法无法为联盟链的可靠运作提供安全保障。

Hyperchain 共识模块算法基于 Allen Clement 等人在 2009 年提出的 Aardvark 算法进行改进，实现了高性能鲁棒共识算法 RBFT。在保证 BFT 系统强一致性的前提下，提升了系统的整体交易吞吐能力以及系统稳定性，可以稳定达到 3000-10000 的 TPS(不同复杂度的业务逻辑)，并可以将交易执行时间控制在 300ms 左右，为区块链的商业应用提供高性能的解决方案。RBFT 两个核心特性在于增删节点与动态恢复：

1)动态成员管理与权限控制（DMPC）：Hyperchain 共识模块实现了在区块链网络中动态增删节点机制，使得整个网络在不宕机的前提下准入或删除节点。同时，通过 CA 证书的方式区分不同节点，达到节点之间的权限控制功能。

2)动态数据失效恢复机制（ARCM）：共识模块在原有机制上，新增了 Recovery 机制。节点重启时，Recovery 机制能自动检测节点并自主更新，同时也是动态增删的基础。当一个节点发生 ViewChange 而无响应时，Recovery 机制进行自我恢复。Recovery 机制的存在大大地增强了共识模块的可用性。

5.3.4 智能合约执行引擎 HyperVM

Hyperchain 的智能合约执行引擎 HyperVM 采用模块化可拔插的设计方式目前提供了支持 Solidity 语言的执行引擎 HyperEVM 和支持 Java 语言的执行引擎 HyperJVM。

HyperEVM 是为了最大程度利用开源社区在智能合约技术和经验方面的积累，提高智能合约的重用性而深度重构 EVM 的虚拟机。HyperEVM 的智能合约实现完全兼容 Ethereum 的智能合约规范，使用 Solidity 作为智能合约的开发语言。 HyperEVM 在保持 Solidity 开发语言的兼容性基础上，对智能合约虚拟机进行性能优化，保持了以太坊虚拟机的沙盒安全模型，在执行性能方面由逼近二进制原生代码的效率。

HyperJVM 通过微服务的架构设计以及多重安全检查机制为原生 Java 智能

合约执行提供了一个高性能安全的执行沙盒。

5.3.5 数据管理

5.3.5.1 数据可视化

目前区块链平台提供接口完成交易的发送和查询，而交易的相关数据都是通过 16 进制编码的字符串，对于运维、管理人员来说，无法对具体合约或链上数据进行分析和管理。

面对以上现状，Hyperchain 提供账本可视化工具 Hyperchain-workbench，可以完美地满足以上问题的需求，对区块链底层平台的交易数据，进行解析，可视化展示。Hyperchain-workbench 支持区块数据浏览、智能合约指定方法过滤浏览以及整个智能合约业务数据的浏览。管理员可以实时查询当前区块链上具体合约的调用情况，以及从合约部署到当前时间，智能合约整理数据的查询浏览，这样方便管理员直观地看到具体交易的调用情况，便于管理员对合约的整体分析。

5.3.5.2 合约管理

Hyperchain 提供合约编译、部署、调用、查看、升级的接口。当业务规则变换后，Hyperchain 支持在不影响具体业务数据的条件下，进行动态的合约升级和数据迁移，所有操作对上层应用是透明的。

5.3.5.3 数据归档

随着区块链运行时间的增长，区块链的存储容量将呈线性增长，且这种数据的增长的速度甚至会超过存储介质容量增长的速度，因此，区块链数据存储将成为限制区块链技术发展的重要因素。面对这一棘手的亟待解决问题，Hyperchain 提出了区块链数据归档的方法，使得整个区块链系统能在不停机情况下，进行动态的数据归档。

5.3.6 区块链管控平台

Hyperchain 为企业用户提供了功能强大的 Web 管理控制平台，支持对底层云计算平台的运维，灵活确定区块链部署的规模和节点运行状态。

Hyperchain 在底层系统之上实现了一套功能完备的 API 接口以助力基于 Hyperchain 的上层应用的开发，Web 管理控制平台便是通过 Hyperchain 的 API 接口与 Hyperchain 进行交互，进而实现对区块链节点的实时监控报警、区块链日

志的实时分析、区块信息的实时监控、历史浏览，以及智能合约的部署、调用和管理功能。

5.3.7 智能合约在线编辑器

Hyperchain-complier 为用户提供在线的智能合约编程校验服务，支持关键字高亮、语法检查、合约规则选择与检查等。Hyperchain-complier 提供多选项的合约规则检查方案，开发者可以根据智能合约部署的实际生产环境，选择响应的合约规则，对编写的智能合约代码进行检查。目前支持与 Hyperchain-workbench 配套的可视化合约规则、可迁移合约规则、可视化并且可迁移的合约规则以及无规则合约代码检查，保证开发者编写的智能合约符合相应规范，减少后期维护成本。

5.3.8 消息订阅

Hypechain 作为一个“共享状态”的区块链实现，其运转通过不断地进行状态变迁实现。每次状态变迁，系统内部都会产生一系列事件作为本次变迁完成的标志。为了让外部用户更好地监视区块链节点的状态变化，Hyperchain 提供了一组统一可定制的消息订阅接口，使得外部订阅者能够便捷地进行消息订阅。可供订阅的事件类型包括（1）新区块事件（2）虚拟机日志事件（3）系统异常事件等。

更重要的是，Hyperchain 将该消息订阅系统视为智能合约与外界通信的消息通道。合约编码者可以在合约中定义一系列的事件类型，当合约进行相应动作时，

可以主动向外界抛出预定义的虚拟机事件，事件中可以记录定制化的消息内容，从而实现了链上链下的消息互通。

5.3.9 可视化 SQL 查询

区块链平台为了维护合约数据的隐私性，所有部署在 Hyperchain 平台上的智能合约，其底层数据都采用复杂的编码方式进行编码，使得区块链节点即使拥有了全量的区块链数据，也无法获得合约数据的明文信息。

然而有部分机构需要分析或审计存储于区块链上的合约数据，因此 Hyperchain 提供了一种基于源码解析的合约数据解析方案。通过这种方式，在获取了合约源码、合约地址以及合约数据键集的前提下，机构可以利用 Hyperchain 提供的数据可视化服务进行该合约的数据解析，导出合约的明文数据以便于进行审计、分析等工作；而其他不拥有合约源码、合约地址、合约数据键集的机构，则无法解析出明文数据。

第6章 解决方案

6.1 供应链金融

针对供应链上小微企业融资难的困境，依托区块链上核心企业的信任传递，围绕核心企业及上下游多级供应链企业，并借助银行、保兑机构等服务商共同打造供应链金融产业生态闭环，从数字资产、产融平台、商业信用等多个方面打造全新供应链金融生态体系，促进多方企业互利共生，促进整个生态良性发展。

- 优势：

（1）基于全链条信息安全共享，实现供应链金融可视化，依托核心企业的信用传递，降低中小企业融资成本。

（2）为资金方提供全流程可追溯、穿透式资产确权和验真渠道，推动供应链金融健康稳定发展。

（3）通过区块链的价值连接，引导更多资金为实体经济服务，让科技赋能于产业，推动制造供应链向产业服务供应链转型。

- 应用案例：浙商银行应收款链平台

应收款链平台是浙商银行与趣链科技合作开发设计的企银业务合作平台，用于在线办理企业应收账款的签发、承兑、保兑、支付、转让、质押、兑付等业务。依托区块链分布式账簿的安全性和共享性，将企业应收账款设为在线支付结算和融资工具，帮助企业去杠杆，降成本。

6.2 数字存证

针对现有的各类电子凭证（如电子合同、电子发票等）可能存在造假以及难以自证其清的情况，通过区块链建立对于电子凭证的共识存储体系，基于数据多级加密和多维权限控制技术，安全保存电子凭证，实现高数字化、强可靠性的数字凭证分布式存储新生态。

- 优势：

（1）建立基于区块链的授信体系，多家机构的参与，为共识后的凭证信息提供了强大的信用背书。

（2）数字存证体系建立，记录凭证信息的同时建立凭证存储体系，全面记

录凭证流转信息。

（3）建立信用体系联盟，建立“数字存证+”的存证、合作、共赢新生态。

➢ 应用案例：银联光大可信电子凭证系统

可信数字凭证系统是中国银联、光大银行与趣链科技合作完成上线的国内首个落地的联盟链场景解决方案。依托区块链平台的安全性、强信任和信息共享机制，来管理企业消费者的电子签购单信息，实现信息登记上链、电子签购单查询等操作，提升客户信任感。同时，利用区块链平台的动态扩展便利的特点，支持对他行电子签购单的处理。联盟规模持续扩大中。

6.3 供应链溯源

通过与物联网等技术的密切结合，将商品在整个产业链的生产记录保存在区块链上。无论是生产商、经销商还是消费者，均可通过可信记录看到商品的全部流转信息，从而打通产业链，将信息触达 BC 两端，全面提升供应链的产品质量和管理效率。

➢ 优势：

（1）通过块链式数据存储结构，技术服务商、生产厂商可以自证其清，政府监管更加有迹可循，呈现给消费者的信息更加真实可靠。

（2）基于分布式协作优化业务流程，降低商品运营成本，提升供应链全量环节的协同效率。

（3）数据的公开透明，使整个供应链条形成一个完整且流畅的信息流，更有利于产业优化升级，进而提升供应链管理的整体效率。

➢ 应用案例：甲骨文超级码

趣链科技为浙江甲骨文超级码科技有限公司提供了基于区块链的防伪码溯源解决方案，建立甲骨文超级码防伪溯源系统。通过公证查询机构、政府监督机构的授信监管，将可溯源的甲骨文超级码存储至区块链中。配合物联网、分布式存储技术，服务于供应链、产业链全流程，提升链条全环节管理效率，达成供应链全面协同的新生态。

6.4 能源资产

通过物联网技术与区块链技术紧密结合，将能源资产数据录入到区块链上进

行可信存储与共享，实现能源资产数字化。通过建立多方联系的业务平台，为绿色资产全生命周期赋能，提高融资效率、投建效率、交易效率、管理效率。

- 优势：

通过物联网技术实现光伏面板等物理设备数据的可信采集，并存储于区块链平台形成数字化、标准化的可信绿色资产。

分布式信息化协作平台解决绿色资产投建过程的信息不对称矛盾，提升投建效率。

基于区块链的可信存储特质，绿色资产信息公开、透明、可信，为绿色资产融资、交易提供信用：保障。

- 应用案例：阳光智联绿色能源资产管理开放平台

趣链科技有限公司为杭州阳光智联区块链公司提供了基于区块链的能源资产方案，构建了绿色能源资产管理开放平台。通过物联网技术将绿色能源资产数据采集并在区块链上进行可信存储，配合线上信息平台打通绿色资产融资、投建、交易全生命周期管理，提升管理效率与资产流动性。

第7章 总结

趣链科技是一家以技术立命的底层区块链技术提供商。同时，由于区块链行业目前尚未形成完全成熟的底层技术方案，所以我们处在一个极其有利的历史阶段，完全可以从应用需求出发，创立自主可控的国产区块链平台，从而使中国的区块链底层技术与应用走在世界前端。公司已经在 2016 年 10 月正式发布面向企业的 Hyperchain 联盟链服务平台，至今已经迭代若干版本，为愈发层出不穷的区块链应用提供强有力的支撑；同时公司已经在 2016 年 12 月正式在浙商银行核心系统上线基于趣链 Hyperchain 平台的移动汇票系统，实现了区块链技术在银行核心系统的首个突破，公司将一直致力于与各个金融机构和其他价值传输相关机构与公司的合作，完成基于区块链的应用落地，不断的提高公司的价值，创造更大的社会效益与经济效益。