

区块链技术架构和应用解析

赵建强

2018-4-22

CONTENTS

01 *Part One*
区块链的概念和特征

02 *Part Two*
技术架构

03 *Part Three*
应用案例分析

CONTENTS

01 *Part One* 区块链的概念和特征



区块链的定义

- 区块链起源于中本聪在2008年发表的《比特币：一种点对点电子现金系统》
- 以区块结构存储数据，通过去中心化的方式集体维护的一个分布式账本，一种可靠的数据库技术方案。



多种技术整合



分布式数据库

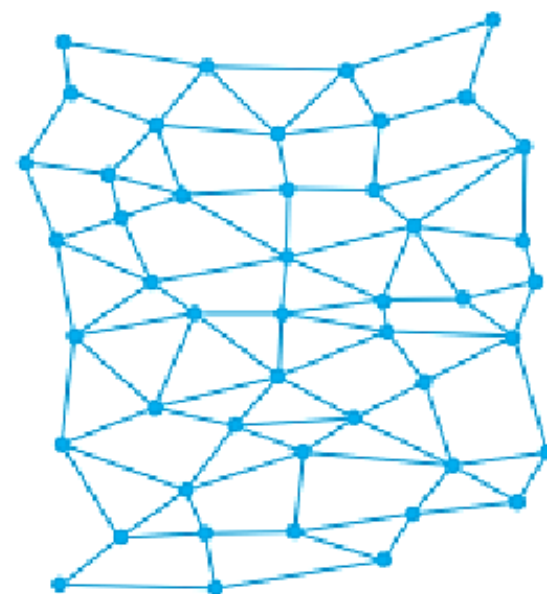
区块链的定义



中心式



分散式

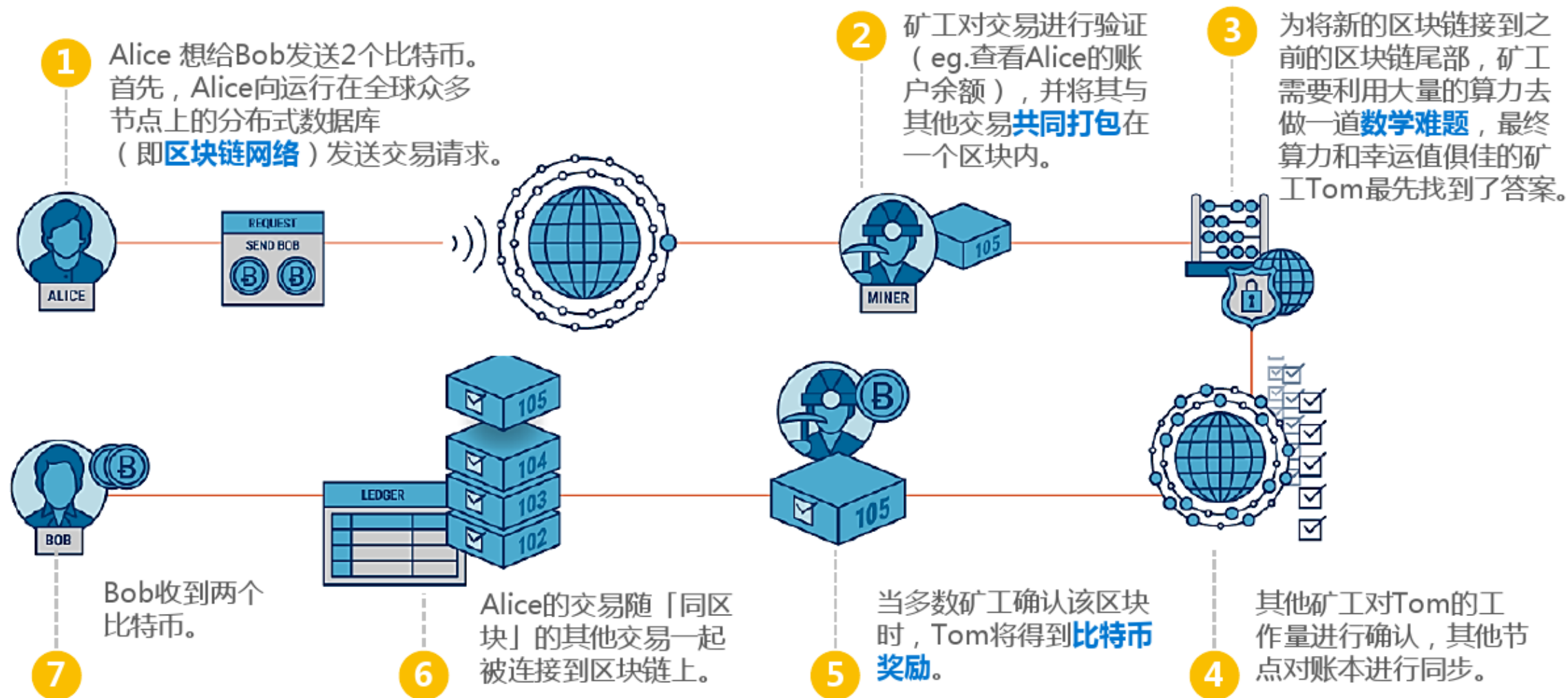


分布式

区块链的定义



区块链的定义



区块链的特征



开放、共识

任何人都可以参与区块链网络
每个节点都有账本
以共识机制通过竞争维护区块

去中心，去信任

完全分布式的端到端网络
无中心化的设备
无需互相信任

交易透明，匿名

交易规则公开透明
交易数据公开
参与节点匿名

不可篡改，可追溯

大部分节点同时确认新增
只允许新增
每个区块都包含前一区块的信息

区块链核心技术

01



共识机制

02



公钥机制

03



分布式存储

04



数字化合约

区块链分类



公有链

任何人都可以加入网络及写入和访问数据，任何人在任何地理位置都能参与共识，通过密码学技术和POW，POS等共识机制来。无官方组织及管理机构，无中心服务器，参与节点按照系统规则自由接入网络，不受控制，节点间基于共识机制开展工作



联盟链

由若干机构联合发起，介于共有链和私有链之间，兼具部分去中心化特征，授权公司和组织才能加入网络参与共识，写入和查询数据都可通过授权控制，可实名参与过程，可满足监管



私有链

建立在企业内部，系统的运作规则根据企业要求设定，修改甚至读取权限仅限少数节点，同时保留区块链的真实性和部分中心化特性。使用范围控制在一个公司范围内，改善可审计性，不完全解决信任问题

区块链的分类

	公有链	联盟链	私有链
参与者	任何人	预先设定和满足条件的成员	中心控制者决定参与成员
中心化程度	去中心化	多中心化	中心化
是否需要激励	需要	可选	不需要
特点	保护用户免受开发者影响 所有数据默认公开 交易速度低	低成本运行和维护 高交易速度及良好的扩展性 更好的隐私保护	交易速度非常快 给隐私更好的保护 交易成本大幅降低

区块链设计思想

解决信任

CONTENTS

02 *Part Two* 区块链的技术架构



区块链技术架构

应用层（记账和转账）

激励层（发行和分配机制）

共识层（PoW，智能合约）

网络层

（P2P网络，验证机制，传播机制）

数据层

（区块数据、数字签名、哈希函数、链式结构、非对称加密）

区块链技术架构

应用层

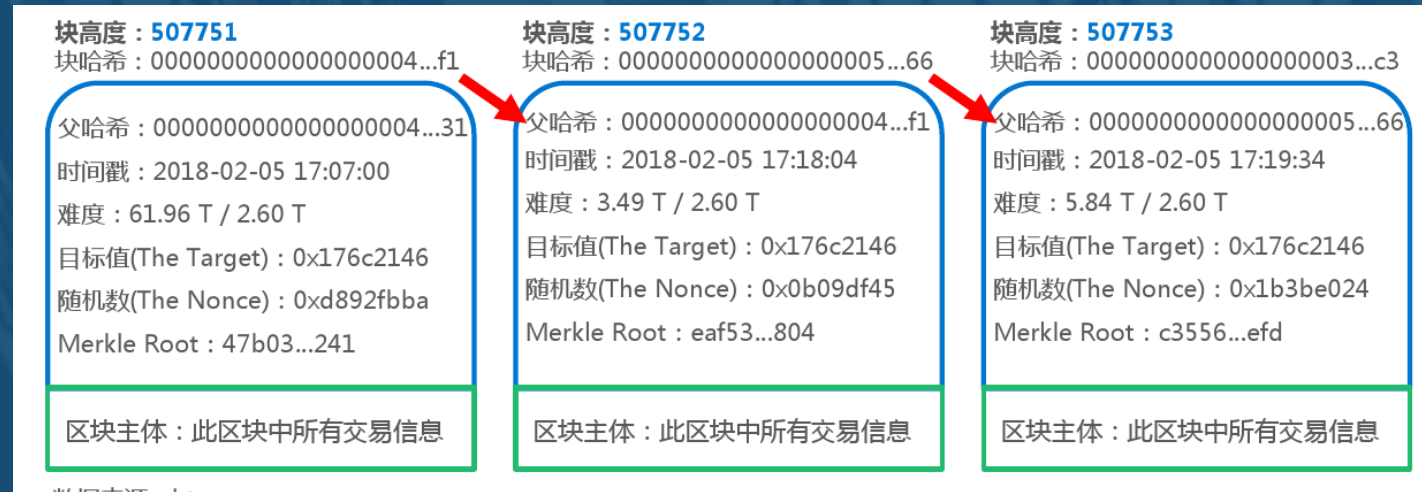
激励层

共识层

网络层

数据层

哈希算法：使得交易环环相扣



区块链技术架构

应用层

激励层

共识层

网络层

数据层

首页 / 块 - 0000000000000000027264033979f0905e40513e1c207f9779a41e749474207

摘要

高度	519,340	版本	0x20000000	块哈希	0000000000000000027264033979f0905e40513e1c207f9779a41e749474207
确认数	1	难度	7.19 T / 3.84 T	前一个块	00000000000000000031189ef2542d985552b4da05eb23cc88473ebdd223c02b
大小	4,030 Bytes	Bits	0x1749500d	后一个块	N/A
Stripped Size	3,774 Bytes	Nonce	0x2fa41b8d	Merkle Root	e1559af94d6f6d0f8525015f632e71a68f982a63635c2fcd193c742eb7cc546f
Weight	15,352	播报方	ViaBTC		
数量	14	时间	2018-04-22 09:38:52		

交易

排序: 块交易索引 交易hash 交易费 sigops 大小 weight 输入数量 输入金额 输出数量 输出金额 witness hash

f153e8a6c9156e66af2d01863f18e00837324b3c22269d2273f6f7dd6777542c

0.00042920 BTC2018-04-22 09:38:52

Coinbase

>

18cBEMRxxHqzWWC... (ViaBTC Bitco...[🔗](#))

SegWit commitment output

12.50042920

12.50042920

区块链技术架构

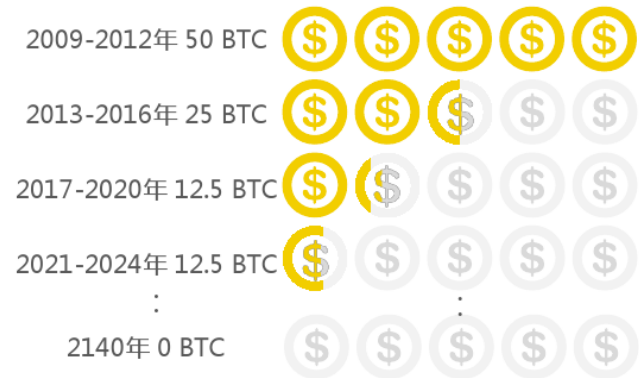
应用层

激励层

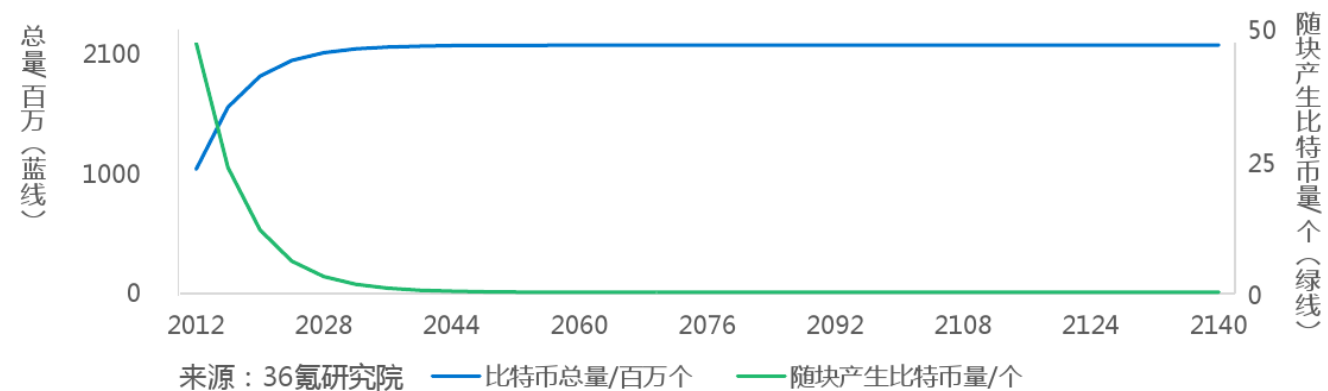
共识层

网络层

数据层



比特币总量增速放缓



区块链技术架构

应用层

激励层

共识层

网络层

数据层

共识机制：获取记账权的凭证

POW：工作量证明

POS：权益证明

BFT：拜占庭容错协议

区块链技术架构

应用层

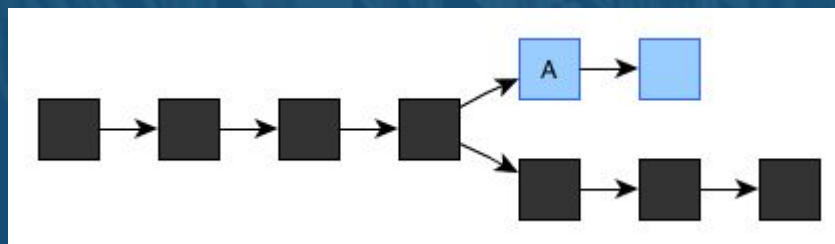
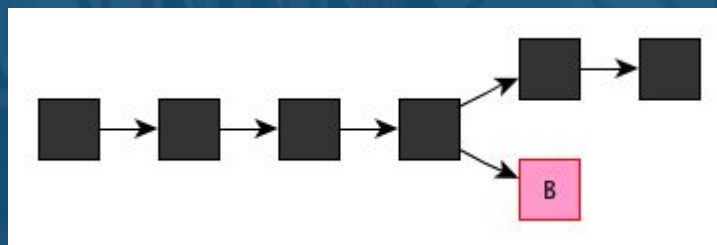
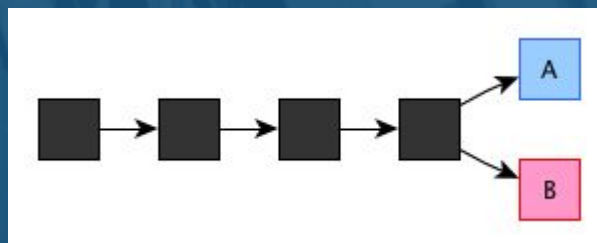
激励层

共识层

网络层

数据层

比特币“双花”问题



区块链技术架构

应用层

激励层

共识层

网络层

数据层

交易模型

- ✓ 交易输出：锁定比特币数量，锁定脚本（接受者的公钥哈希）
- ✓ 交易输入：解锁脚本（发送者的签名和公钥）
- ✓ 签名：对发送者和接收者的公钥韩系以及整个交易签名

区块链应用架构体系设计

服务平台

网关

服务

节点网络

SDK

工具

组件模型

共识网络

账本

持久化引擎

合约引擎

区块链协议

账本状态

历史证明

账本操作集

合约指令集

区块链应用架构体系设计



区块链协议

定义区块链数据格式标准：包括账本状态、历史证明、账本操作集、合约指令集等方面的数据标准



组件模型

区块链逻辑组件的框架模型，对区块链协议的实现框架，包括共识网络，账本，持久化引擎，合约引擎等



服务平台

上层协议和组件模型的实现，由网关，服务，节点网络，sdk和一套工具集等组成

区块链应用架构体系设计原则



面向业务

企业场景的特点是需求非常多样，性能要求高。从分析企业应用的典型用力出发，设计区块链协议和系统功能的特性确保系统能够最终适应广泛的企业业务需求



标准化

通过标准化的协议和数据结构，解决企业间数据交互问题，避免多链并存的技术演进过程中的数据孤岛
使区块链成为一种标准化的价值交换和信任传递协议



松耦合和模块化

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，满足不同用户和场景的需要，采用可插拔的模块组件。

区块链应用模型设计



定义身份

为参与者注册登记一个由公钥私钥对(证书)表示的身份账户



编写智能合约

把参与者之间达成的商业协议以智能合约代码的形式进行定义



签署智能合约

智能合约最后需要经过参与者以各自的身份账户做出签署，之后每一方参与者只需要根据己业务范围内的业务进程做出相应的操作，触发智能合约执行

区块链应用账本协议设计

- 账本协议是从数据的角度定义模型
 - ✓ 账本数据的标准格式
 - 账本状态
 - 历史证明
 - ✓ 读写账本数据的指令的标准格式
 - 账本操作集
 - 合约指令集

区块链应用组件模型设计



共识网络



账本



持久化存储



合约引擎

区块链应用组件模型设计

➤ 共识网络

- ✓ 典型算法有PoW, PoS, PBFT
- ✓ 共识过程
 - ✓ 交易扩散
 - ✓ 交易排序
 - ✓ 调用交易执行程序
 - ✓ 对交易结果进行共识
 - ✓ 提交共识结果

区块链应用组件模型设计

➤ 账本

- ✓ 账本状态与合约分离，使用基于身份的访问控制协议约束合约对状态的访问，这种将数据与逻辑分离的设计模式是典型的贫血模型，可为上层业务逻辑提供无状态的逻辑抽象。

➤ 持久化存储

- ✓ 利用成熟的NoSQL数据库实现持久化存储

➤ 合约引擎

- ✓ 前端包括合约高级语言规范及其工具链
- ✓ 后端提供轻量级合约中间代码执行环境

区块链应用服务层设计

➤ 区块链网关

- ✓ 私钥管理
- ✓ 隐私保护
- ✓ 协议转换

➤ 区块节点服务

- ✓ 账户管理
- ✓ 账户认证授权
- ✓ 账本数据访问框架
- ✓ 事件通知机制
- ✓ 智能合约管理

区块链应用服务层设计

➤ 区块链共识网络

- ✓ 由共识节点组成的网络，基于 P2P 网络和共识算法确保交易数据在节点之间保持一致

➤ 工具

- ✓ 配套的工具集合，包含 SDK、数据管理、安装部署工具、监控服务。

CONTENTS

03 *Part Three* 区块链应用解析



区块链适合解决那些问题？



业务开展需要跨主体合作



对方参与并需要低成本信任



业务存在长周期交易



区块链适合解决那些问题？

- 业务开展需要进行跨主体协作
 - ✓ 中心化的方式：协调、立项、成本分摊都是问题，数据隐私也是问题
 - ✓ SOA方式：技术复杂，方案缺少通用性，难以支持复杂的业务
 - ✓ 两种方式都难以防止数据被篡改
 - ✓ 利用区块链，共有数据，防篡改，分布式和数字化合约的特点，能够将一些业务层面协调解决问题，放在技术层面解决，更加高效，灵活和客观

区块链适合解决那些问题？

➤ 业务开展需要参与方之间建立低成本信任

✓ 数据可信

- ✓ 传统方式，数据由中心节点强势持有，数据可信由数据持有者的商业或社会信用来保证，只能建立主观的可信。
- ✓ 区块链结合密码学哈希和数字签名，以区块链的形式将数据变更历史结合，通过共识协议使得参与方共同拥有数据，多方持有相同数据副本，并数据被签名确认，数据变得可信

✓ 合约履行

- ✓ 契约更客观，更严格的执行方式，降低履约成本，确保高效履约。一般的契约是事后以人的主观意愿来执行，智能合约是在出发条件被满足后，由计算机程序来保证合约及时执行，具有客观性

✓ 历史可证明

- ✓ 固化交易历史，并提供对交易历史的追溯查询，保证交易的不可篡改和不可抵赖。保留参与交易各方可信的历史记录

区块链适合解决那些问题？

- 业务过程存在长交易，长周期链条
 - ✓ 业务在多主体之间流转，难以确定间接主体的真实性和和有效性，
 - ✓ 由于多主体间业务隔离，难以延伸出多级业务
 - ✓ 区块链从技术上保证整个长交易，长周期链条的各参与主体身份真实，数据可信，实现信用多级传递，提升业务效率

支付（跨境支付）、保险、
证券、股权登记、众筹

金融

物联网

区块链物联、汽车租赁

区块链
应用生态圈

公共
服务领域

文化、教育、
产权、医疗

供应链

供应链金融、供应链溯源

公益慈善

区块链捐赠平台

区块链在金融行业应用

- 金融市场中交易双方的信息不对称导致无法建立有效的信用机制，产业链条中存在大量中心化的信用中介和信息中介，减缓了系统运转效率，增加了资金往来成本。
- 区块链技术公开、不可篡改的属性，为去中心化的信任机制提供了可能，具备改变金融基础架构的潜力。

支付（跨境）方面

通过区块链技术，实现资金转移，尤其在跨境支付业务上的潜在优势格外突出，在跨国收付款人之间建立直接交互，简化处理流程，实现实时结算，提高交易效率，降低业务成本，由此推动跨境微支付等商业模式的发展。

保险理赔方面

通过智能合约的应用，既无需投保人申请，也无需保险公司批准，只要触发理赔条件，实现保单自动理赔，支付理赔金额。区块链上数据真实、难以篡改的特点，可有效简化保单理赔处理流程，降低处理成本，降低索赔欺诈的概率。

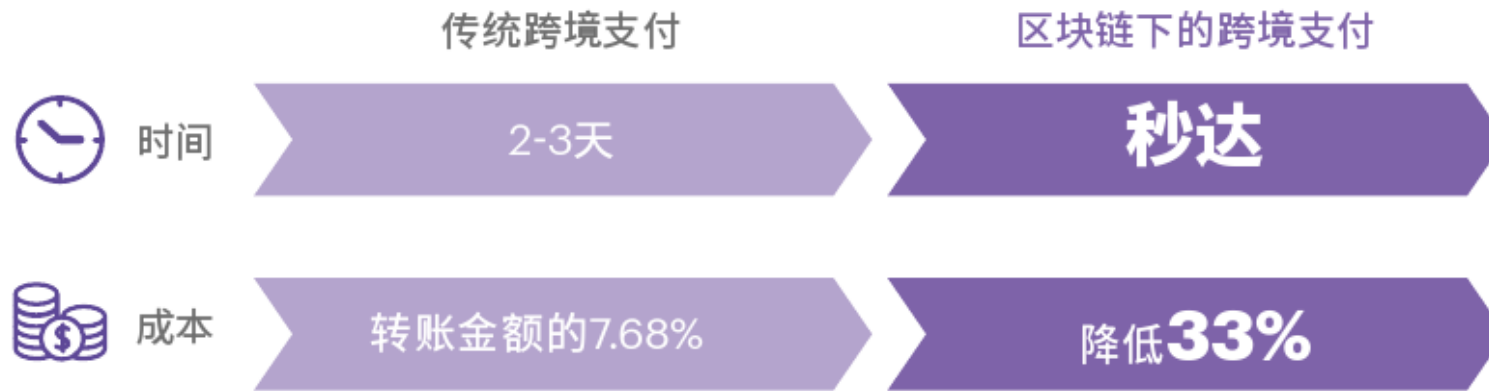
证券交易方面

将股权整合进区块链中，成为数字资产，可实现无需通过中介机构，直接发起交易。资产发行可根据需要，采取保密或公开方式进行。股票资产交易通过区块链代码表达相关各方一致达成的合约，实现合约的自动执行，保证相关合约只在交易对手间可见，而对无关第三方保密。

票据方面

基于区块链技术架构建立新型数字票据业务模式，借助分布式高容错性和非对称加密算法，可实现票据价值的去中心化传递，降低对传统业务模式中票据交易中心的依赖程度，降低系统中心化带来的运营和操作风险。。

区块链在金融行业应用



区块链在公共服务领域应用

- 传统的公证依赖政府，而有限的数据维度、未建立的历史数据信息链常常导致政府、学校无法获得完整有效的信息。利用区块链可以建立不可篡改的数字化证明。在数字版权、知识产权、证书以及公益领域都可以建立全新的认证机制，改善公共服务领域的管理水平。

文化方面

利用区块链技术，将文化产业链条中的各环节加以整合、加速流通，有效缩短价值创造周期。通过区块链技术，对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。。

教育方面

利用区块链技术，解决现有的学生信用体系不完整、数据维度局限、缺乏验证手段等问题，简化流程和提高运营效率，并能及时规避信息不透明和容易被篡改的问题。在区块链中记录跨地域、跨院校的学生信息，追踪学生在校园时期的行为记录，构建良性的信用生态体系。

产权登记方面

房地产交易市场在交易期间和交易后流程中，存在缺乏透明度、手续繁琐、欺诈风险、公共记录出错等问题。区块链技术的应用可实现对土地所有权、房契、留置权等信息的记录和追踪，并确保相关文件的准确性和可核查性。此外，可借助区块链技术实现无纸化和实时交易。

医疗健康方面

医疗机构面临着无法跨平台安全共享数据的问题。在医疗服务商之间建立良好的数据协作，有助于进一步提高诊断准确率，改善治疗效果，降低医疗成本。基于区块链技术，医疗产业链中的参与方实现对网络访问权限的共享，同时也不会对数据的安全性和完整性造成威胁。

区块链技术在国内外布局

- 国外区块链企业四大军团都有其代表性企业或者组织。

类型	代表企业	优势/特点	案例/方案
初创公司或组织	R3 CEV	以搭建底层技术协议为主	公布源代码的Corda分布式账本
金融机构	高盛	以解决金融机构现有应用场景需求、降低交易成本为主要出发点	银行间清算、外汇交易等
大型科技公司	微软	将原有技术能力（如云服务）延伸至区块链领域	基于Azure云服务，发展莱切利（Bletchley）项目支持不同区块链联盟组建。
系统集成商/IT咨询公司	德勤	结合系统集成能力与区块链技术服务企业客户	基于以太坊的协议的Rubix项目，例如区块链智能身份项目。

区块链技术在国内外布局

- 国内的初创型公司、金融企业以及大型科技公司为主，也有相当的联盟成立。

类型	代表企业	优势/特点	案例/方案
初创公司或组织	万向区块链实验室	搭建开源的技术研究生态及投资孵化生态	基于以太坊的基础设施
Fintech	微众银行	搭建区块链底层服务	清算、票据
大型科技公司	腾讯	将原有技术能力（如云服务）延伸至区块链领域。	腾讯金融云+区块链解决方案。用于票据、资产登记及交易等场景。

区块链技术在国内外布局

大型互联网公司布局区块链概览

电子商务



京东

阿里巴巴
Alibaba.com

+ 区块链 =

商品防伪溯源

人脸修图

meitu 美图

+ 区块链 =

智能通行证：身份识别认证

游戏

网易游戏
游戏热爱者

+ 区块链 =

网易招财猫：区块链云养猫

云计算

迅雷
XUNLEI

暴风影音
BAOFENG.COM

快播

+ 区块链 =

共享CDN

挖矿回报

社交

人人网
renren.com

+ 区块链 =

人人坊：社交平台支付



蚂蚁区块链



腾讯区块链



百度Trust

2015

2016

2017

如今

7月应用于支付宝爱心捐赠

10月联合法大大
区块链邮箱存证
3月普华永道合作
区块链跨境食品供应链

8月阿里健康在常州推出
区块链医联体的试点项目

11月承接雄安
区块链实施平台

已经应用到
供应链、金融、公益、医疗
等领域

5月微众银行加入金联盟，
并研发金联盟BaaS

9月上线与上海华瑞银行
共同开发的区块链贷款清算平台

4月发布《区块链方案白皮书》

9月通过《可信区块链检测标准》
与英特尔共同开发物联网安全服
务

10月加入加拿大区块链研究所

11月发布金融级BaaS开放平台

已应用到
金融、公益、法务、物流
等领域

2015年开始探索区块链金融

6月投资美国区块链
支付公司Circle

5月联合合作方发布
4.24亿区块链ABS项目
7月上线云计算BaaS平台

9月区块链场内公募ABS
在上海交易所发行

10月百度金融加入
“超级账本”开源项目

主要应用于
资产证券化、资产交易等金融业务
已支撑了超过500亿元资产。

区块链技术在国内外布局

- 受 R3、Hyperledger 等区块链联盟的影响，国内的金融机构不约而同将加入联盟作为探路区块链的第一步，区块链行业始于联盟成立。



区块链技术应用解析：共享经济

Airbnb爱彼迎
全球450万民宿任你挑

P2P房屋共享

快速解决信任问题？

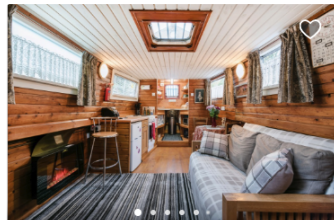
区块链技术应用解析：共享经济



为您推出爱彼迎Plus 品质和舒适性经过验证的精选房源



PLUS 已验证 · 上海
前往迪斯尼十分方便的极简北欧风情公寓
¥ 409起 每晚 · 免费取消
★★★★★ 96



PLUS 已验证 · 阿克苏布里奇
Cosy Dutch House Boat Close to London
¥ 726起 每晚
★★★★★ 134



新市区 · 整套公寓

北歐風公寓_3 Rooms_6 mins to Metro!

3间卧室 8张床 3个卫生间 最多住10人

将房源描述翻译为中文 (简体)



房东: Cherry 联系房东

- ★步行六分鐘到捷運/地鐵站
- ★門口有直達車到台北101 (20分鐘車程)與信義區夜店
- ★20分鐘到西門町商圈

[更多房源介绍](#)

评价

★★★★★ 171条评价

搜索评价

如实描述	★★★★★	位置便利指数	★★★★★
沟通交流	★★★★★	办理入住	★★★★★
干净指数	★★★★★	性价比	★★★★★

将评价翻译为中文 (简体)



Chen
2014年10月

不错的房间,房东本人很nice,提供了很多帮助,谢谢啦!



来自Cherry的回复:
謝謝Chen,下次要再來台灣玩啲:))
2014年10月



丽颖
2018年2月

房间很漂亮,三个卧室都有卫生间,比较方便,楼下有很多超市,还有家乐福



凯
2017年12月

很热情很贴心,房子很漂亮,

区块链技术应用解析：共享经济



房主和顾客交流
耗费大量时间



评价房主、顾客
和房屋存在困难



支付和担保速度慢

痛点何在？

区块链技术应用解析：共享经济



区块链技术应用解析：共享经济

—	改进前体验	区块链增强后体验
预定	• 人工输入政府签发的ID信息 • 顾客依赖图片和与房主短讯交流 • 房主依赖顾客既往评价记录和短讯交流	• 政府签发的ID安全储存并验证 • 顾客和房主依赖完全得到验证的评价
支付	• 人工输入信用卡信息 • 入住后24小时放款给房主	• 安全储存ID关联的支付证书 • 按“智能合约”条款放款
评价	• 顾客和房主互留评价 • 评价的作者难以追溯 • 负面评价可删除 • “水军”评价存可能	• 依靠电子签名写评价 • 评价验证需要既往交易记录 • 评价可追溯，不会消失

区块链技术应用解析：供应链



信息不透明，不流
畅，交易效率低



纠纷处置难
举证追责难

痛点何在？

区块链技术应用解析：供应链

➤ 解决思路

- ✓ 各方交易数据公开透明
 - ✓ 加快信息流，提升效率
- ✓ 交易数据不可篡改
 - ✓ 举证和追责
- ✓ 交易数据可追溯
 - ✓ 虚假交易、假冒伪劣

区块链技术应用解析：供应链

➤ 物流

- ✓ 利用数字签名机制，保证无法伪造签名，防止货物丢失、冒领
- ✓ 保护个人隐私，落实实名制度
- ✓ 简化物流流程

➤ 溯源防伪

- ✓ 数据完整性和不可篡改
- ✓ 商品交易全流程记录
- ✓ 贵重物品的防伪溯源

谢谢