区块链3.0：侧链与跨链

OK Blockchain Capital

2018.7

战略合作媒体

火星财经

搜狐科技 it.sohu.com

联合发布媒体

(排名不分先后)

金色财经

节点财经 JIEDIAN.IO

猎云财经

巴比特 服务于区块链创新者

深链财经

火球财经 ihuoqiu.com

核财经

火讯财经

布洛克科技

TuoniaoX.com 鸵鸟区块链

蜂巢财经 HONEYCOMB FINANCE

白话区块链 HELLOBTC.COM

链向财经 -区块链第三方信息服务平台-

雷鹿财经 LEILOOK.COM

彗星播报

a·coin 壹块硬币

Chainology 链科技

一号财经 YIHAO·NEWS

博链财经

链观天下 LIAN GUAN TIAN XIA

Jpm.cn 金评媒

UP Blockchain Review

看币 不凡

链头条 资讯

目 录 Contents

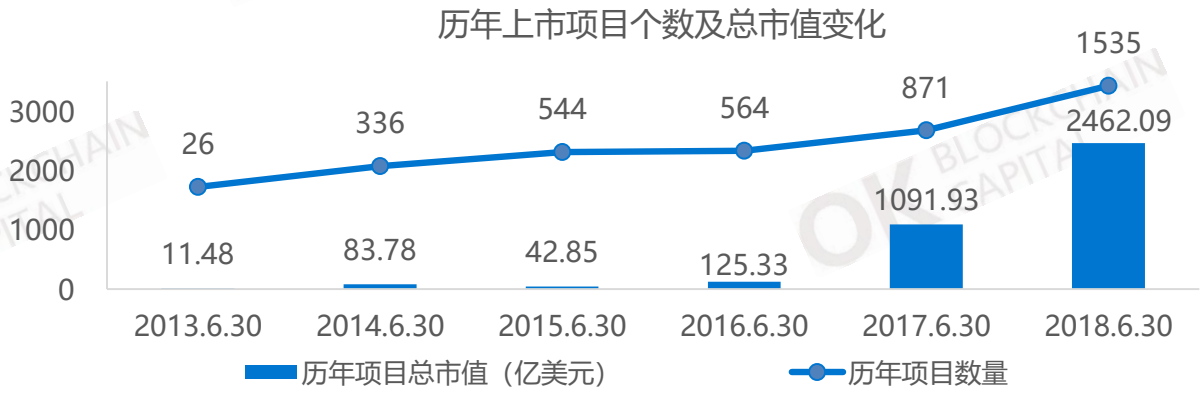
区块链行业10年发展

区块链的1.0、2.0、3.0

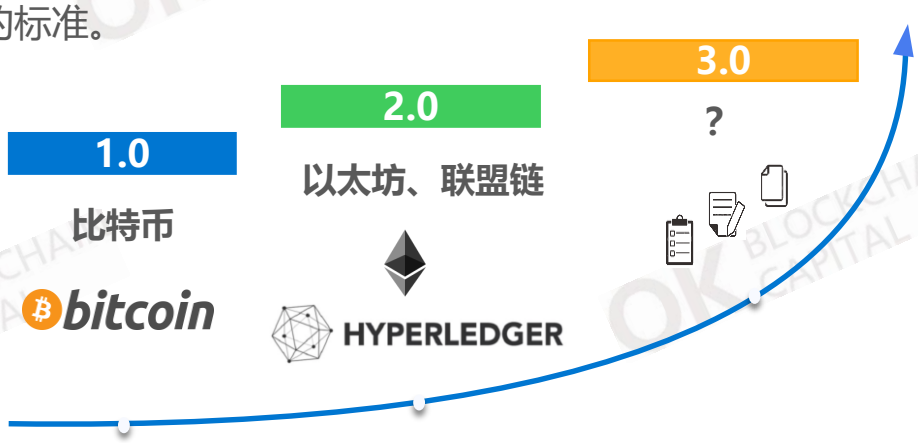
自2008年中本聪发表论文首次提出比特币的概念，区块链行业发展已将近10年，相较于底层互联网技术以及物联网、人工智能、云计算等其它技术，区块链的发展时间尚非常短暂。

过去10年间，以比特币为代表的1.0时期、以以太坊和联盟链为代表的2.0时期，区块链行业都取得了突破性的进展，尤其是从2017年上半年开始，基于以太坊创造的新型募资方式ICO的火爆表现，极大的刺激了区块链行业泡沫的产生，也让更多资金和创业者进入到这个行业，加速区块链产业革新发展。

2017年7月至2018年6月，新进入市场的区块链项目数量总和及市值规模已经达到往年历史总和的181.6%，近一年以来，区块链行业受到前所未有的关注。



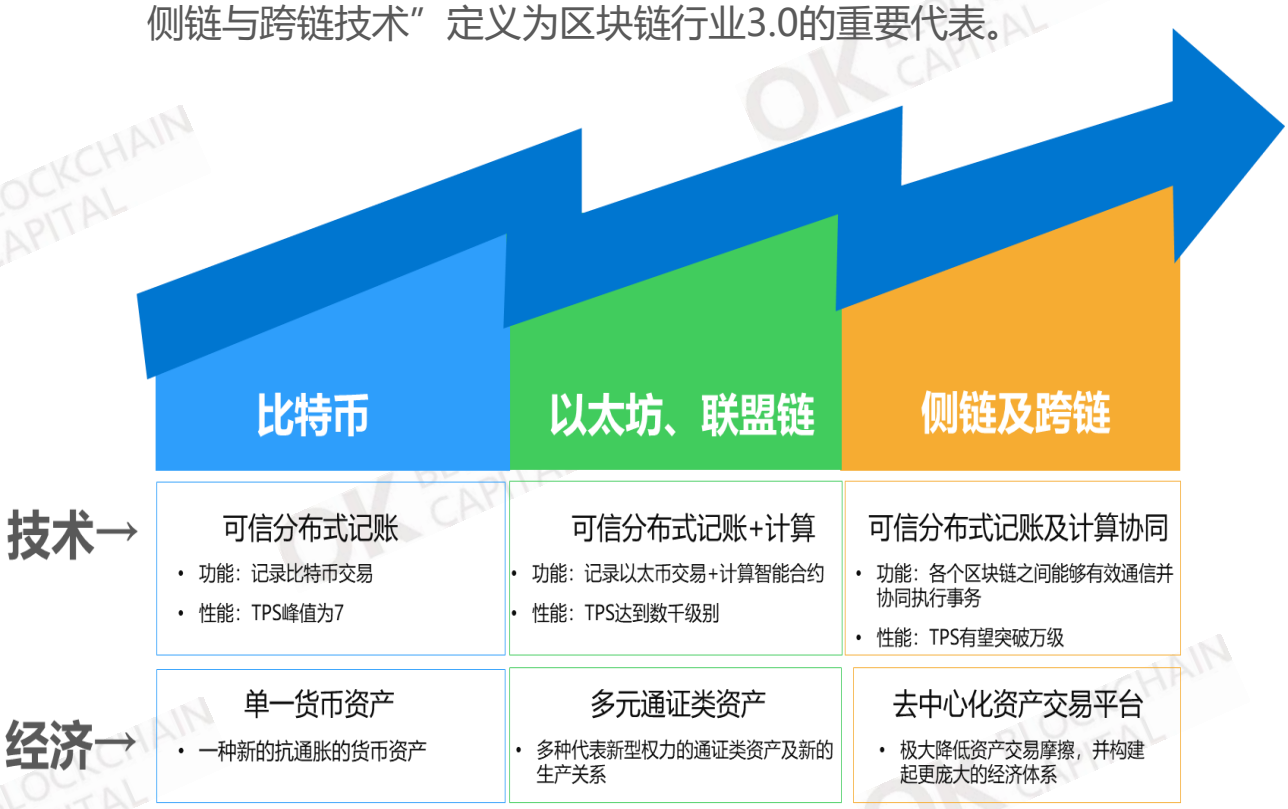
当区块链行业进入快速发展阶段，3.0 时代究竟将会实现哪些新的突破、存在怎样的机会，成为当前行业最关心的话题。关于区块链3.0概念的解读，目前已出现多种不同的版本，行业尚未达成统一的标准。



区块链行业10年发展

区块链的发展脉络：技术与经济

本报告，通过梳理区块链行业历史，研究分析其关键发展脉络，从驱动区块链行业两个核心维度“技术”与“经济”出发，将“侧链与跨链技术”定义为区块链行业3.0的重要代表。



区块链“技术”创新，主要围绕其系统功能上的拓展性，以及性能上的拓展性，1.0时期，比特币系统作为可信的分布式账本，仅能够实现比特币转账交易等功能，TPS为个位数；2.0时期，以太坊加入“智能合约”，支持图灵完备脚本运行，开始能够支持各式各样的业务逻辑和商业应用，极大的丰富了区块链系统的功能；联盟链及DPOS共识机制的公链，则实现了更高的交易性能。3.0 时期，侧链跨链技术能够在区块链功能和性能的拓展上都起到非常关键的作用。

区块链“经济”创新，主要围绕数字资产、资产的交易摩擦，以及基于新的资产分配方式的生产关系革新几个方向，从1.0发展至2.0时期，区块链世界创建出大量的数字资产，如何大幅降低各资产间的交易摩擦，构建起更大范围的价值网络和经济体系，这根本上依赖于跨链技术的发展。

区块链1.0

比特币，国际货币缺锚时代里一种抗通胀的自由竞争货币

站在历史角度，比特币被创造出来的时间点和08年全球金融危机的爆发非常接近。金融危机揭示了全球金融系统的脆弱性，而比特币为质疑这个体系的人们提供了新的选择。

Circle创始人Jeremy Allaire曾在博客上描述 2008年美国金融危机的那段时间，“仿佛天都快塌了，那是一个非常黑暗和不确定的时刻。我们所有人在那一刻都觉得我们的钱可能会消失，我们不知道钱是否还在银行里。整个世界对银行和政府都失去了信任。”

事实上，1914年第一次世界大战爆发后，各国为了筹集庞大的军费，纷纷发行不兑现的纸币，禁止黄金自由输出，金本位制随之告终。第二次世界大战后建立起来的以美元中心的金汇兑本位制布雷顿森林体系（即美元与黄金挂钩，美国承担以官价兑换黄金的义务）也在1976年随着美元危机的爆发而彻底终结。至此，全球货币体系已然失去黄金这一最后屏障，进入无锚滥发时期。

中本聪在比特币第一个创世区块中，写下了2009年1月3日当天泰晤士报的头版新闻标题，“英国的财政大臣达林被迫考虑第二次出手纾解银行危机”。这句话被中本聪的簇拥者解读为“他对传统银行这种中心化的金融机构的挑战”。

2013年4月，欧盟和德国打着反洗钱的幌子，通过对存款人增税的方式来应对塞浦路斯的债务危机。塞浦路斯的储户人人自危，开始将“去中心化”的比特币作为避险资产进行大量采购储藏，比特币价格短短几天从30多美元飙涨到265美元。这次比特币的大幅上涨，一定程度上说明比特币作为抗通胀的自由竞争货币的基础价值。

比特币背后所代表的经济理念，在诺贝尔经济学奖得主弗里德里希•哈耶克的著作《货币的非国家化》中有得到充分的印证。哈耶克提出的革命性建议正是，允许私人发行货币，并自由竞争，这个竞争过程将会发现最好的货币。

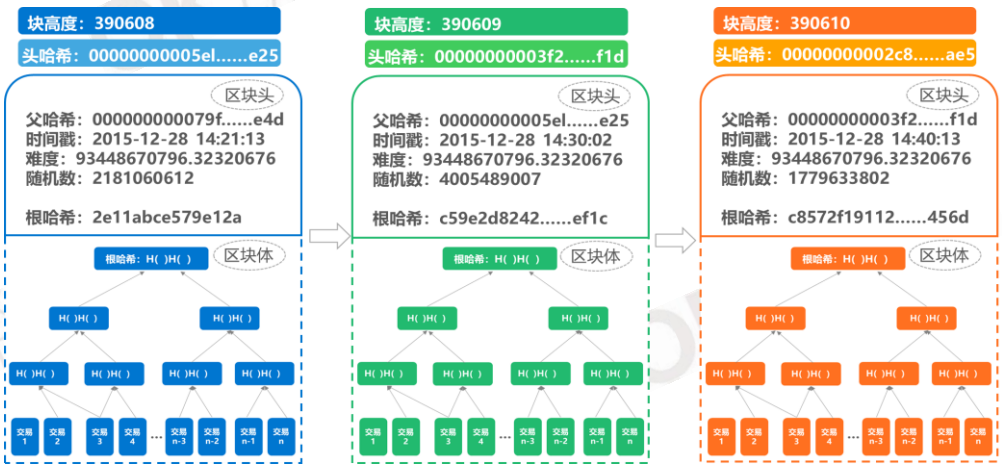
区块链1.0

比特币技术，基于分布式系统的融合技术解决方案

比特币区块链系统在原有分布式系统的的基础上发展而来，其要解决的核心问题与传统分布式系统相同，即如何在一个由众多不可信节点组成的、可能存在坏节点的网络中达成一致性正确，具体到比特币网络里，这个问题就是如何让众多分布式节点共同维护好一套账本，代替中心化机构履行记账职能。比特币区块链基于POW （Proof of Work） 共识算法，设计了一套非常巧妙的融合技术解决方案，其中的关键机制包括：

- SHA256，是哈希运算中的一种，哈希运算通常满足“无论输入多长的复杂数据，输出的哈希值都是固定的长度”以及“从输出无法反推输入”两个基本特点，SHA256 则进一步实现“防碰撞”的安全特性，即很难找到两个不同的输入但输出结果相同。SHA256输出结果能够作为原输入数据的“指纹”，快速识别原输入数据是否被篡改。

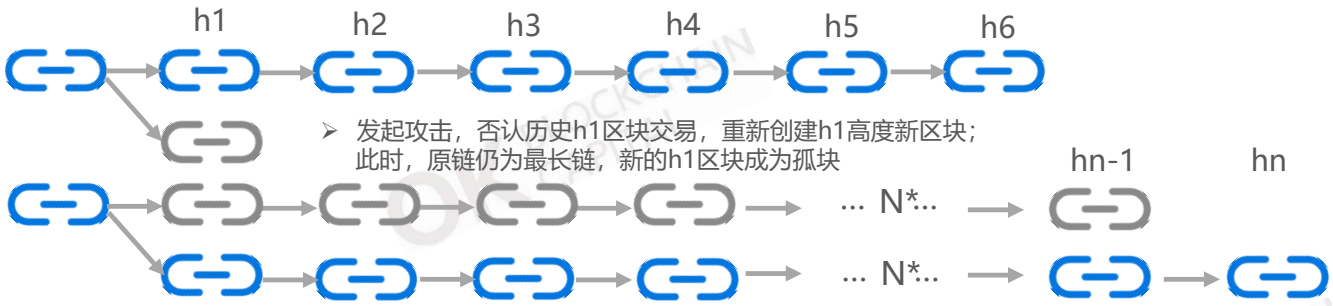
- 块链式数据结构，即将一段时间的交易数据打包存储在一个区块（数据块）中，区块按照时间戳有序排列。比特币区块分为区块头和区块体，具体的交易信息逐笔记录在区块体中，所有交易数据生成的Merkle根哈希值以及区块高度、父哈希等信息记录在区块头中。记账节点将之前哪个区块头的哈希值作为父哈希记录下来，即选择链接在这个区块的后面。在这样的区块链条中，如若对之前某个区块数据进行改动，其区块头哈希将无法与下一个区块的父哈希值匹配，这意味着如果要发动攻击、篡改一个历史区块，则必须重新从此区块开始往后创建新的链条。



区块链1.0

比特币区块链能够实现更充分可靠的共识和透明可信性

➢ POW共识算法和最长链原则，POW核心是指进行了最多计算工作最先完成计算任务的记账节点，能够有权创建新的区块并获得记账奖励（这些记账节点被形象的称呼为“矿工”），也就是一个区块的创建意味着一定算力的投入，最长链即算力投入最大、最具权威性，成为全网唯一有效的链。也就是说，想要成功发起一次攻击，则需要掌握全网一半以上的算力，来让新建的链条追赶上已有的链条成为最长链，也就是我们常说的51%算力攻击。



➢ 发起攻击，否认历史h1区块交易，重新创建h1高度新区块；此时，原链仍为最长链，新的h1区块成为孤块

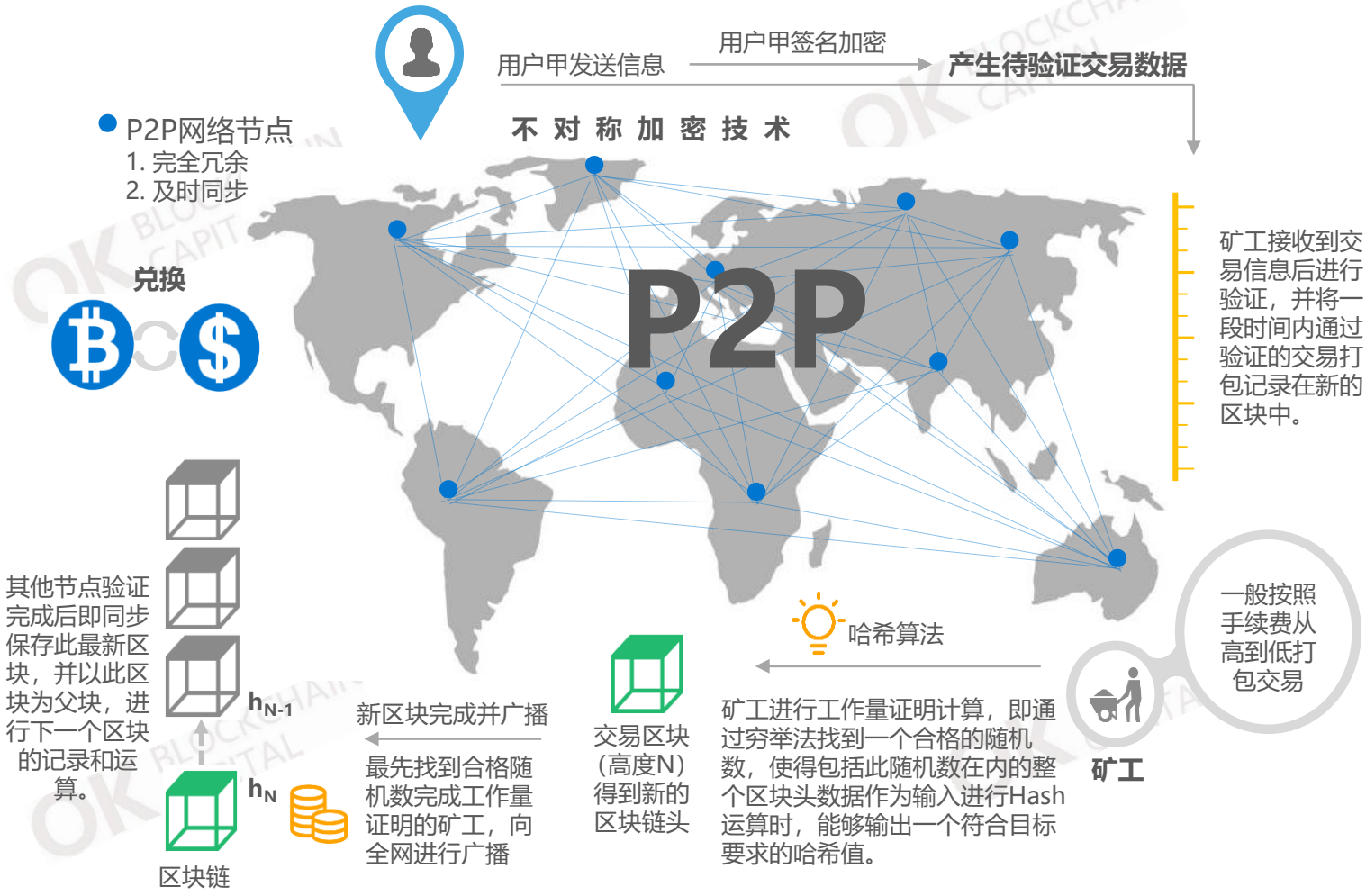
➢ 由于攻击方拥有51%算力，攻击链随时间推移不断缩小与原链差距；到达 hn 高度时，超越原链，成为最长链，完成攻击

传统分布式网络依靠拜占庭容错共识算法来实现一致性，网络容错率约为1/3，即作恶及失灵的坏节点必须控制在总节点数量的1/3以内，比特币网络将容错率提高到了50%，则能够支持分布式网络容纳更分散的、更多数量的节点，以实现更充分的共识。并且，比特币网络通过为矿工记账行为设置了算力成本并将比特币作为记账奖励，从而让矿工的收益与比特币网络的发展正相关，从经济合理的原则出发，拥有越多算力的矿工将更有动力去维护比特币网络安全来让自己获得的比特币奖励升值，而不是去发起攻击破坏它，这进一步提升了比特币网络的安全可靠性。

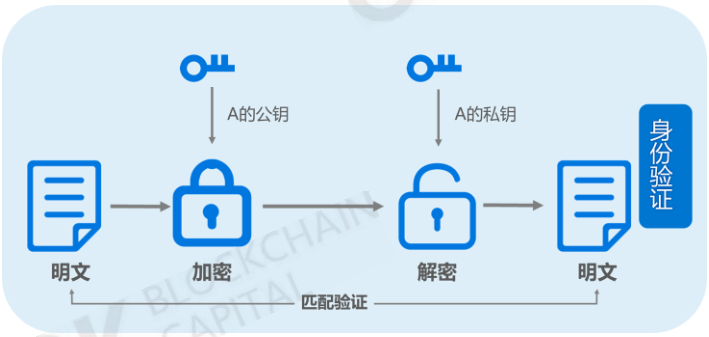
作为记录比特币交易账本，比特币区块链首先基于强大的共识机制，保障比特币交易能够被诚实的记录并且不可篡改。另外，由于是开源软件，比特币的所有工作原理向全球开发者公开展示，没有“阴暗的死角”，而且任何人都能够随时下载比特币客户端加入到比特币网络中，成为一个全节点，保存下来一份完整的比特币账本，这样使得比特币网络中的所有交易都能够透明可信。不可篡改、透明可信是区块链网络的核心特性。

区块链1.0

比特币区块链网络基本运行流程



➢ 其中，交易验证=身份验证（数字签名）+账户余额验证（UTXO）



m
输入：0
输出：25.0 ➡ Alice

n
输入：m【0】
输出：20.0 ➡ Bob，5.0 ➡ Alice　由Alice签名

w
输入：n【0】
输出：12.0 ➡ Carl，8.0 ➡ Bob　由Bob签名

z
输入：m【1】，w【0】
输出：17.0 ➡ David　由Alice、Carl共同签名

区块链1.0

比特币区块链系统的技术限制

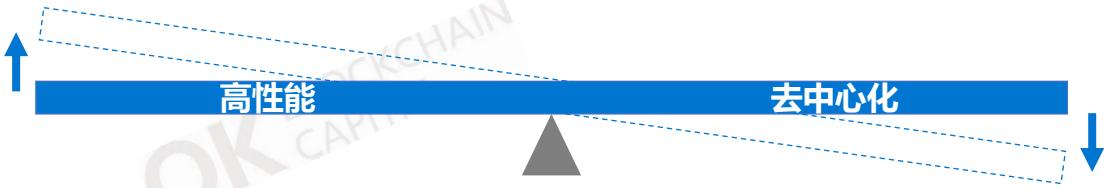
比特币客户端作为一套开源软件，由开源社区进行维护升级，在其过往数次版本的升级中，大都围绕“性能上的扩展”和“功能上的扩展”进行 。

➢ 性能上的限制

性能扩展也就是扩容问题，比特币每个区块1M大小，最多能容纳约4000笔交易，按照平均每10分钟新生成1个区块计算，比特币网络每秒能够处理的交易数量峰值为7笔，这距离中心化系统数十万TPS存在非常大的差距。

限制比特币交易性能的两个重要因素，分别是比特币的区块仅有1M，以及平均每10分钟才能算出一个合格随机数创建新的区块。比特币社区漫长的扩容之争，主要针对区块大小的设计方案展开。10分钟的延迟，主要是为了保障由全球各地的节点构建的分布式网络能够完成充分的通信，避免某个挖矿节点因为没有及时收到其他节点已经成功创建区块的消息，继续浪费算力并生成冲突的区块，所以很难通过大幅缩减出块时间来极大提升交易性能。

本质上，比特币网络为了实现充分的去中心化，要求在足够多且分散的节点中达成一致，控制出块速度、降低交易性能则是其必要的妥协。



➢ 功能上的限制

比特币系统使用了一套基于堆栈的非常简单的脚本语言，不支持for循环，无法访问全局数据，能执行的程序指令非常有限，而且还受到UTXO账户限制。比特币脚本指令目前能够实现的功能主要都与比特币的交易相关，多重签名已经算是其中复杂的功能。而且，比特币社区对于比特币系统的安全稳定性极其看重，对待技术升级非常保守，为了避免程序实现上会有bug，一些复杂的操作码都已经被禁用。

区块链2.0

以太坊“图灵完备”的智能合约极大的拓展了区块链系统的功能

以太坊的设计思想中很重要的一点就是要解决比特币区块链功能扩展性不足的问题，它的核心是以太坊虚拟机，其可以执行任意复杂算法的编码，也就是计算机术语中的“图灵完备”。

如果说比特币系统提供了一系列预先设定好的操作（仅限于比特币交易），那么以太坊则是允许开发者按照自己的意愿创建各种复杂的操作，具体是指开发各种智能合约，所以以太坊也被称为智能合约开发平台。

智能合约(Smart contract)本质上是一个由计算机自动执行的程序，程序的执行规则相当于一个合约，规定好触发条件和执行结果。智能合约是1990年代由尼克萨博提出的理念，它的设计目标是最小限度的依赖第三方中介，减少恶意和意外的状况，降低欺诈损失，减少仲裁执法成本和交易成本。由于缺少可信的执行环境，智能合约一直以来并没有被实际应用。以太坊首先看到了区块链和智能合约的相结合的可能性。

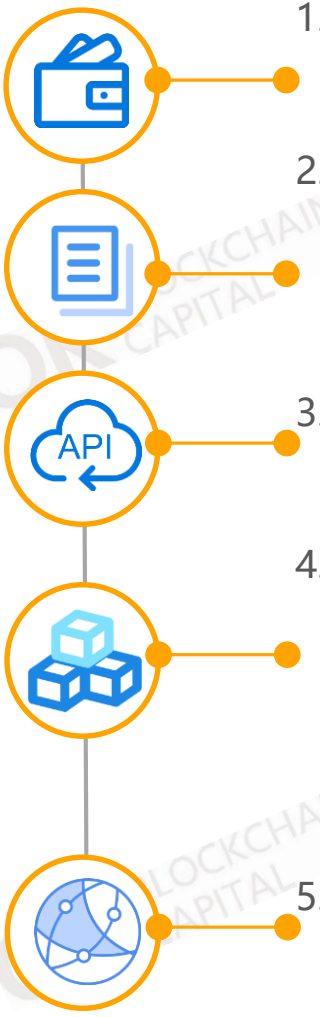
区块链　　智能合约　　以太坊

从技术角度来讲，以太坊是由众多计算机网络的节点共同运行一个开源的虚拟机(EVM)软件，由图灵完备的脚本语言编译成的智能合约程序可以在EVM中执行。对比比特币，我们可以理解为以太坊上智能合约的创建及执行的过程，如同比特币交易过程一样，被每个节点共同见证和记录。但相比于比特币矿工只需要进行简单的转账交易脚本的运算，以太坊的矿工则需要承担大量的智能合约的运算。

由于加入了图灵完备的智能合约功能，以太坊不仅能支持类似于比特币数字货币的交易功能，还可以支持一切能够以智能合约来表达的业务逻辑，比如登记、托管、抵押、投票等等，能够运用在各个行业中。并且，以太坊还创建了ERC20代币开发标准，帮助用户能够快捷的创建出一种新的Token，极大地拓展了区块链系统的应用范围。

区块链2.0

以太坊网络基本运行流程



1. 与比特币相同，用户通过下载以太坊客户端，生成一对公私钥，创建一个新的账户

2. 以太坊的账户分为交易账户和智能合约账户，开发者编写智能合约源码并编译成以太坊EVM虚拟机可执行的代码，通过以太坊客户端部署到以太坊网络上，就完成了一个智能合约的创建

3. 当我们要运行一个智能合约的时候，需要向该合约地址某个API发起一个消息

4. 以太坊网络中的矿工会通过以太坊虚拟机在他们的计算机上运行智能合约，技术上来讲，每一次智能合约的调用就是对智能合约程序进行一次新的运算，输出新的智能合约“状态”；与比特币网络相同，矿工们会互相竞争交易打包创建区块的权力，只是他们打包的“区块”数据，不仅包括交易转账信息，还有以太坊智能合约“状态”的更新

5. 最后，与比特币网络相同，当一个区块产出，矿工会把这个区块公布到网络中，其他的计算机会验证它们得到的结果相同，然后添加该区块到它们自己的区块链上。

并且，和比特币一样，以太坊用户需要向网络支付一定的交易费用，不同的是，以太坊智能合约交易费用，取决于运算智能合约所消耗的矿工的计算和内存资源，这里的资源以Gas作为单位

- 交易费用（单位以太币） = Gas数量（单位Gas） x Gas价格（单位以太币 / Gas）
- 智能合约越复杂（计算步骤的数量和类型，占用的内存等），完成运行就需要越多Gas。

区块链2.0

联盟链及公有链DPOS共识机制，牺牲了一定的“去中心化”来实现区块链系统的性能扩展

以太坊对比特币 POW 共识算法进行了一定调整，比如压缩了每个区块的大小、缩短了出块的时间，同时对没有及时同步到信息挖出孤块的节点进行补偿奖励。但本质上，仍然受到“去中心化”与“交易性能”平衡的限制，以太坊网络目前也仅能实现约15TPS。事实上，**区块链系统交易性能的大幅提升，率先在联盟链中得以实现。**

以太坊智能合约开发平台的创建让更多的商业机构意识到区块链技术的价值，开始进行区块链技术的探索。由于传统大部分企业级场景具有隐私性要求，比特币、以太坊等绝对公开透明的公有链无法满足其需求，联盟链应运而生。联盟链与公有链的本质区别在于，公有链可以允许任何人加入成为一个节点，联盟链则需要授权许可。由少量、经过授权许可的节点组成的联盟链，能够在一个有信任基础的小范围内快速达成共识，于是可以极大的提升交易性能。

超级账本作为迄今为止最出色的联盟链开发平台，它是Linux基金会于2015年发起的开源项目。其首个产品级解决方案 Hyperledger Fabric 能够实现上千级别的TPS。

由 BTS 项目首创、经过EOS 充分发展起来的DPOS 共识机制，则更进一步的提高了节点准入门槛，当选节点依次排队记账，省去了节点竞争的环节，理论上能够实现上万级别的TPS。

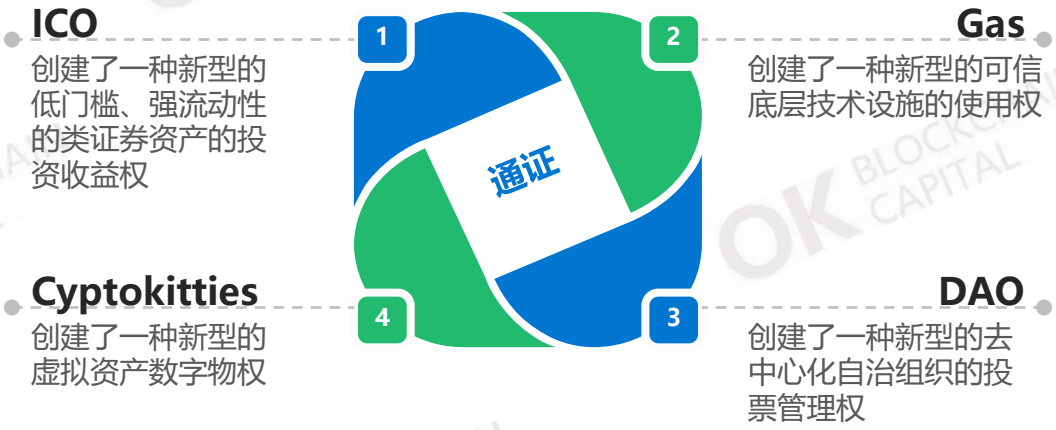
本质上，联盟链及公有链中DPOS共识机制，都是通过准入机制控制了记账节点的数量，牺牲了一定的去中心化来实现性能上的扩展。在少量节点参与共识的区块链网络中，决定网络性能的将不再是节点达成一致所需的等待时间，而是单个节点的GPU运算能力及网络带宽。

区块链2.0

通证经济创造出新的权益和新的生产关系

以太坊智能合约开发平台及其创建的 ERC20 标准的出现，让任何人都可以基于以太坊创建一个分布式的应用，以及发行自定义的token（通证）。以太坊通证与比特币相同的是，其发行规则透明可信，并且能够在区块链网络中实现“交易即结算”的高效流通；不同的是，比特币本身是一种新型的“数字货币资产”，通证则能够代表多种类型的资产及各种不同的权益。

其中，对于传统商业体系中，能够以积分、卡券等形式实现的使用权证明，Token化的价值主要在于增强此类权益的变现能力，从而对用户形成更有效的激励；对传统金融资产、实物资产进行映射得到Token，其价值主要在于提高资产的信用和流动性，尤其是推动资产证券化；更重要的是，基于通证创造了诸多新的权益：



人类的商业文明发展和经济形态革新，本质上正是新的权益不断被发掘、建立并符号化的过程，通证经济则加速了这个过程的实现。

另外，通证经济的核心理念在于创建一种通证持有者与通证所在的商业体系共赢的关系，一切为体系建设作出贡献的行为都能够被度量价值并得到通证奖励，包括提供算力及存储等资源进行网络维护、软件的开发升级以及创造智力成果或优质内容吸引新的用户、提供监督审计服务等等，能够在生产资料的供给、劳动协作、成果分配等各方面形成更加公平高效的机制，构建起更加先进的生产关系。

区块链2.0

复杂多样的商业应用涌现

资管、支付、票据、借贷、贸易、保险、风控、众筹

数字病例、隐私保护、健康管理

人工智能模型共享数据、算力众包

匿名社交隐私性保障

数据存储数据共享

智能交通、环境保护、平安家居、智能消防、食品溯源

云存储、云计算

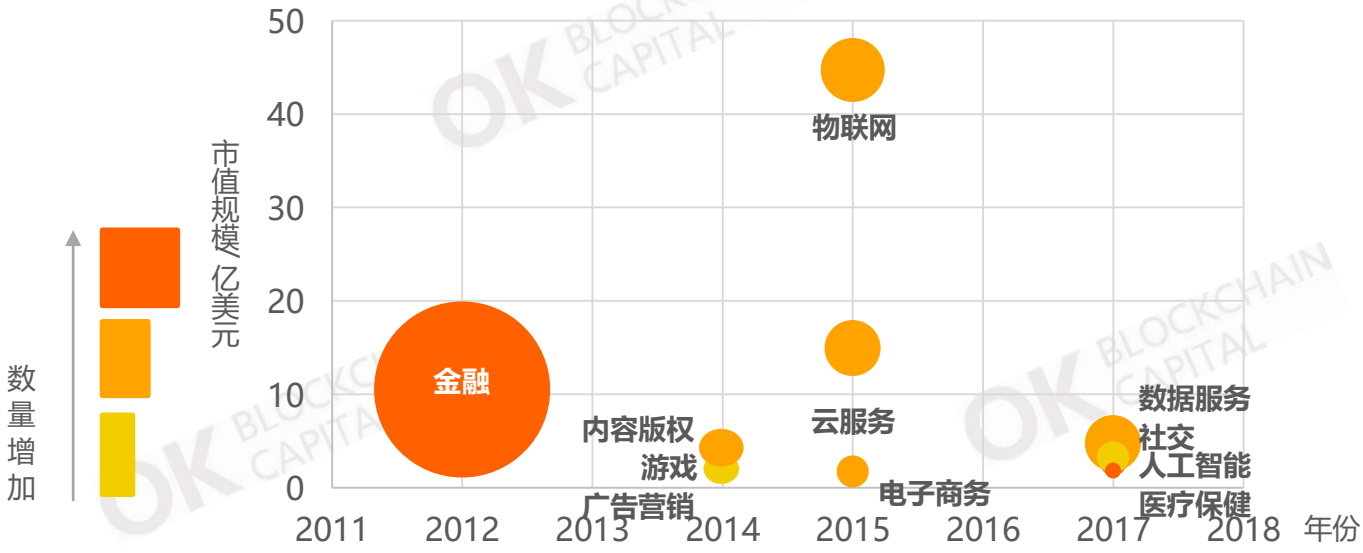
版权登记
内容分发
创作激励
Ip众筹

养成游戏、Moba游戏、动作类游戏、冒险类游戏

去中心化电商跨境电子合同

流量反欺诈
注意力经济

➢ 随着以太坊智能合约开发平台的发展及各种高性能公链的出现，继金融领域后，越来越多垂直行业应用及公链涌现出来。据2018年6月底数据，全球市值Top200各垂直领域种，物联网及云服务市值规模最大，但仍然仅有数十亿美元。



区块链3.0

区块链技术和经济的发展，对侧链跨链解决方案提出明显诉求

➢ 区块链技术：性能上的扩展性

区块链系统从基于POW的比特币、以太坊网络，发展到基于PBFT及DPOS共识算法的联盟链及公链网络，虽然实现了TPS从个位数向万级别的巨大提升，但却以牺牲了一定的“去中心化性”为代价，并不符合区块链系统的核心理念。

闪电网络等“侧链”方案以及建立多个子链分片共识的类“跨链”方案的提出，为区块链系统性能上的扩展带来新的思路，有望在更好的保持去中心化理念的基础上，大幅度提升区块链交易性能。

➢ 区块链技术：功能上的扩展

伴随着智能合约开发平台逐渐丰富并完善，大量纷繁复杂的垂直公链及商业应用涌现，形成众多独立的基础设施及业务体系，比如去中心化存储、去中心化身份认证、去中心化云计算、去中心化资管、去中心化电商等等，但当前的区块链都是一个个封闭独立的业务体系。

参照互联网各业务体系的合作，比如整合各种企业级服务的阿里钉钉办公平台；或者，通过微信开放接口以微信账号一键登录多个第三方应用；再比如最简单的从一个网页或者APP界面跳转至另一个网页或APP界面，等等，这些功能在当前的区块链商业体系中都无法实现，这极大的限制了区块链业务体系发展的可能性。跨链方案若能够实现，试想，一个去中心化资管区块链能够调用一个去中心化身份认证区块链的智能合约，来采集借贷人征信数据，这些将极大扩展区块链能够支持的业务场景。

➢ 区块链经济

基于跨链技术搭建去中心化交易所，能够进一步降低币币交易摩擦，提高流动性；成为中心化交易所的有效补充手段。

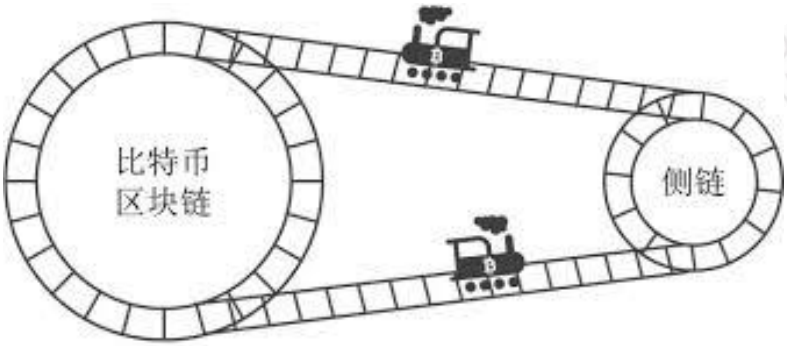
侧链技术

比特币扩容困境催生侧链技术

侧链的概念是相对于主链而言的。当主链的性能出现瓶颈，或者某些功能无法扩展的时候，把资产转移到侧链上，相关的交易只需要在侧链上执行，从而达到了分担主链的压力，扩展主链的性能和功能的目的。

早期侧链技术方案主要是针对比特币提出的。因为比特币的技术架构，天生就有扩展性的不足。比如交易延时长、吞吐量低、不支持图灵完备的智能合约，都是比特币内在的设计缺陷。这些设计缺陷必须通过重构比特币基础框架和算法才能解决。

但是比特币作为市值最大、流通性最高、认可度最广的数字货币，修改其基础架构可能会引起巨大的风险，比特币核心开发者在技术升级的态度上也比较保守，这决定了比特币很难通过技术升级提高自身的可扩展性。



侧链技术的基本想法是另外启动一条侧链，将比特币资产转移到侧链上。反之也可以将侧链上的资产再转回到比特币。比特币在主链和侧链上的资产双向转移，这个过程称之为资产的双向锚定(2WP)。

侧链上的资产有比特币的信用背书，在价值上等同于比特币。同时侧链的设计架构不受比特币网络的限制，开发者可以通过各种各样的区块链技术构建侧链，应用于各种应用场景。所以侧链技术间接的扩展了比特币的性能和功能。

跨链技术

跨链技术：侧链的延伸

相对于侧链，跨链是一个更为广泛的概念。跨链是泛指两个或者多个不同链上的资产和状态，通过一个可信机制，互相转移，互相传递，互相交换。侧链的概念是通过双向锚定实现了主链与侧链之间的价值转移，侧链的目的是为了扩展主链的功能和性能。从这个意义上讲，侧链是跨链技术的一个特例。在跨链的场景中，链与链之间的关系不仅仅是主-侧的关系，也可以是对等的，链上资产不仅仅可以双向锚定，也可以通过可变汇率互相兑换，甚至也可以是智能合约状态的交互。

跨链的出现是区块链技术演进的必然结果。区块链项目百花齐放，也带来了不同链业务体系和资产价值孤岛的问题，需要一种新的机制来打通和连接各个孤岛，跨链和侧链技术应运而生。

下面是两个跨链技术的典型应用场景：

应用场景一：水平扩容

分片是将一个区块链拆分成多个子链，每一个子链有独立的账本和共识机制。网络上的交易将被分配到子链中执行。因此，交易可以在多个子链上并行处理，随着子链的增多，区块链处理越来越多的交易将成为可能。这种技术也称为水平扩容。

水平扩容技术可以打破垂直扩容的限制，但是也引入了一个新的难题：如何处理子链间的交易？所以分片技术的实施必然需要跨链技术的支持。

应用场景二：去中心化交易所

去中心化交易所能够为用户提供更好的安全保障。当前的去中心化交易只能提供同一个公链内的资产交易服务。例如EtherDelta只能提供基于以太坊的ETH与ERC20代币互换。

跨链技术可以帮助去中心化交易所打破这个限制，支持任意两个公链上资产的交易。

侧链与跨链

侧链与跨链核心技术难点及解决方案

虽然应用的侧重点不同，侧链与跨链的技术天然是相通的，都需要解决链与链之间的通信协议、数据交互、资产转移等问题。一方面侧链的技术可以应用于跨链项目，反之侧链的项目也会借鉴跨链的成熟技术。

当前侧链与跨链解决方案的技术难点主要集中在以下4个方面：

1. 跨链交易验证问题

链与链之间如何建立一个信任机制，验证跨链之间的交易数据？
解决方案有：
a. 公证人机制，b. 区块头Oracle + SPV简易验证

2. 跨链事务管理问题

跨链交易包含多个子交易，这些子交易构成了一个事务。跨链的事务管理又分为两个子问题：
2.1 如何确定子交易是否被最终确认，永不回滚？
解决方案：
a. 等待足够多确认，b. 区块纠缠，c. DPoS/xBFT
2.2 如何保证交易的原子性？所有子交易要么都成功，要么都失败。
解决方案有：哈希时间锁

3. 锁定资产管理问题

资产跨链转移时，锁定资产如何管理？
解决方案有：
a. 单一托管人 b. 联盟托管人 c. 智能合约托管

4. 多链协议适配问题

N个链之间实现两两跨链协议，如何简化跨链协议的适配？
解决方案有：中继链

侧链与跨链

跨链交易验证问题——侧链与跨链关键技术

实现链与链之间的互联互通，首先要设计区块链系统之间的信任机制，使得一个区块链可以接收并且验证另一个区块链上的交易。比如比特币网络上的一笔交易被确认之后，交易内容发送到以太坊的智能合约里，以太坊必须正确验证此交易已经被写入比特币区块，然后才能执行后续智能合约的代码。

跨链交易验证的本质是一个Oracle问题。对于一个区块链系统来讲，跨链的消息来自于系统外部，自身无法直接验证其正确性，必须要额外设计一套Oracle机制来辅助验证跨链交易是否真实。

目前常见的跨链交易验证机制有：
a. 公证人验证机制，b. 区块头Oracle+SPV 模式。

	公证人机制	区块头Oracle+SPV
原理	通过外部公证人(联盟)验证跨链消息的可靠性，公证人验证通过后必须对跨链消息签名。	将公证人(联盟)提供的外部区块链系统的区块头数据保存在自己的网络中。根据SPV(Simple Payment Verification)机制能够验证交易。
优势	简单灵活，适用范围广。甚至也适用于银行账本与区块链系统之间的交易验证。	公证人并不直接验证交易，作弊的成本相对高。
劣势	1 公证人是中心化的信任机制； 2 每一笔跨链交易都需要公证人验证。	1 需要额外的存储空间记录其他链的区块头数据； 2 不适合银行账本与区块链之间的跨链交易。
案例	Ripple	BTC Relay

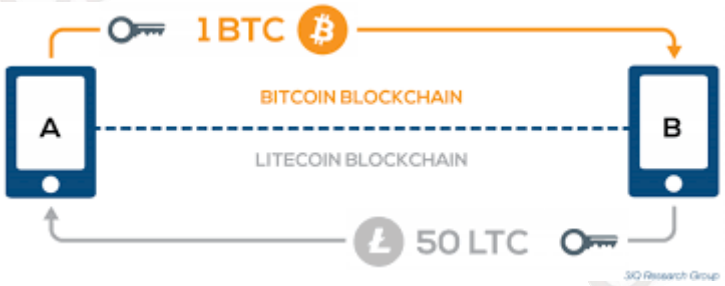
侧链与跨链

跨链事务管理——侧链与跨链关键技术

一个完整的跨链交易可以拆分成若干个子交易，每个子交易在各自所属的区块链系统中处理。这些子交易作为一个整体需要事务管理，保证事务的一致性、原子性。

举个例子，Alice有一个比特币，以1:50的兑换率交换Bob的50个莱特币。Alice和Bob之间互相转账的过程包含以下两笔交易：

1. 在比特币的网络中，Alice 获得Bob的账户地址，向Bob的地址转1个BTC。
2. 在莱特币的网络中，Bob获得Alice的账户地址，向Alice的地址转50个LTC。



这两笔转账交易分别发生在不同的区块链系统中，彼此是互相独立的原子操作。 同时它们又是同一个跨链交易的组成部分，构成了一个完整的事务，事务的管理需要保证两笔交易的一致性和原子性。

设计跨链的事务管理机制需要考虑两个子问题：

1 交易的最终确定性(Finality)：

一个交易被确认之后依然有可能回滚，如何保证交易的最终确定性。

2 去中心化的原子性:

如果一笔交易成功而且满足最终确定性，如何保证后续的子交易也一定能成功。如果其它子交易执行失败，如何撤回已经转出的资金?

侧链与跨链

跨链事务管理——侧链与跨链关键技术

交易的最终确定性(Finality)

在POW共识算法的区块链系统中，只要有足够大的算力，理论上每一笔交易都可以被撤销。只是被确认的区块越多，撤销的可能性越低。

在跨链交易中，必须要确定前一个交易已经被最终确认，才能处理后续的子交易，否则会有回滚的可能。常见的方案如下：

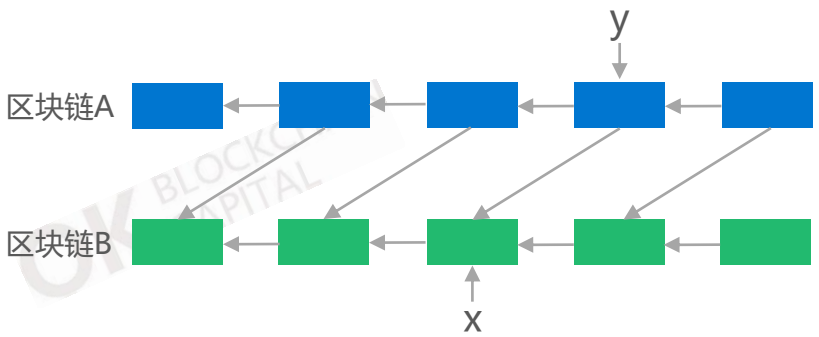
方案一：等待足够的确认数

最简单粗暴的办法就是等待足够多的确认，直到回滚交易的可能性达到预定的阈值之后，再执行其它的子交易。这种方案的劣势显而易见就是事务处理的时间会变长。

方案二：区块纠缠

另一个方式是区块纠缠，令两个链之间的区块有依赖关系，当一个链上的某个区块被撤销的时候，自动撤销其它链上的相关区块。

如下图所示：区块链A的每一个区块引用两个父块，一个在区块链A中，一个在区块链B中。这样A中的区块对于B中的区块有依赖关系。如果子交易x所在的区块被回滚，那么后面的子交易y也必须被回滚。



方案三：使用DPOS/xBFT等共识算法

相对于POW共识算法，DPOS或者xBFT等共识算法更容易达成最终确定性。比如EOS可以在3秒中达到100%的最终确定性。使用这类共识算法的区块链系统能更高效的实现侧链跨链交易。

侧链与跨链

跨链事务管理——侧链与跨链关键技术

交易的去中心化原子性: 哈希时间锁

传统的事务管理协议， 例如2PC、3PC，都依赖一个中心化的事务管理者协调各个子任务的执行状态，来保证原子性。但这需要第三方可信的中心，不符合去中心化的设计理念。

基于哈希时间锁(Hashed-Time Lock)的原子交换协议是一种去中心化的事务管理机制，可以保证多笔交易的原子性。

依然用Alice用比特币兑换Bob的莱特币的例子，具体应用流程如下：

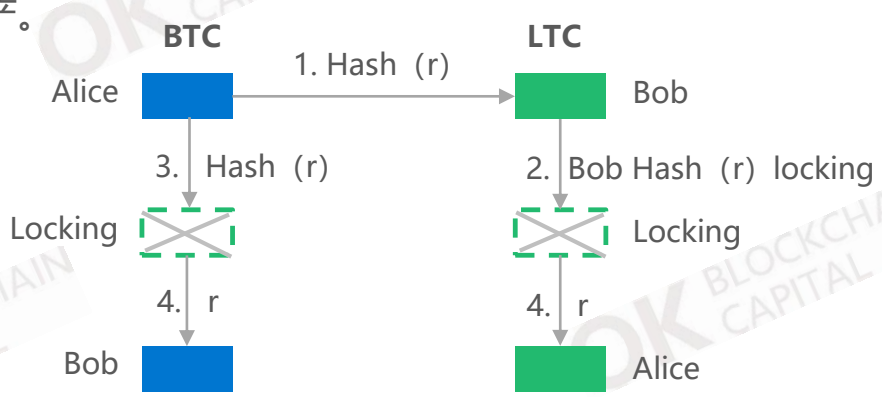
1. Alice创建了一个随机密码r，并且算出该密码的哈希值 hash(r)。Alice将这个哈希值hash(r)发给Bob。

2. Bob 锁定莱特币资产，解锁条件是：Alice 必须在**H小时**内出示哈希值为hash(r)的随机密码，否则超时后返还给Bob。

3. Alice 锁定比特币资产，解锁条件为: Bob 必须在**2H小时**内出示哈希值为hash(r)的随机密码，否则超时后返还给Alice。

4. Alice在**H小时**内出示有效随机密码r，成功将Bob的莱特币转移到自己的账户。伴随此交易成功执行，随机密码r被记录在了莱特币区块链上。

5.Bob得到随机密码r，至少有**H小时**的充裕时间可以解锁Alice的比特币资产。



侧链与跨链

锁定资产管理——侧链与跨链关键技术

双向锚定与锁定资产管理

双向锚定是主链与侧链上的资产按照1：1兑换比例双向转移的过程。比如BTC可以转移成RSK上的等量的SBTC，反之RSK上的SBTC也可以转成BTC。

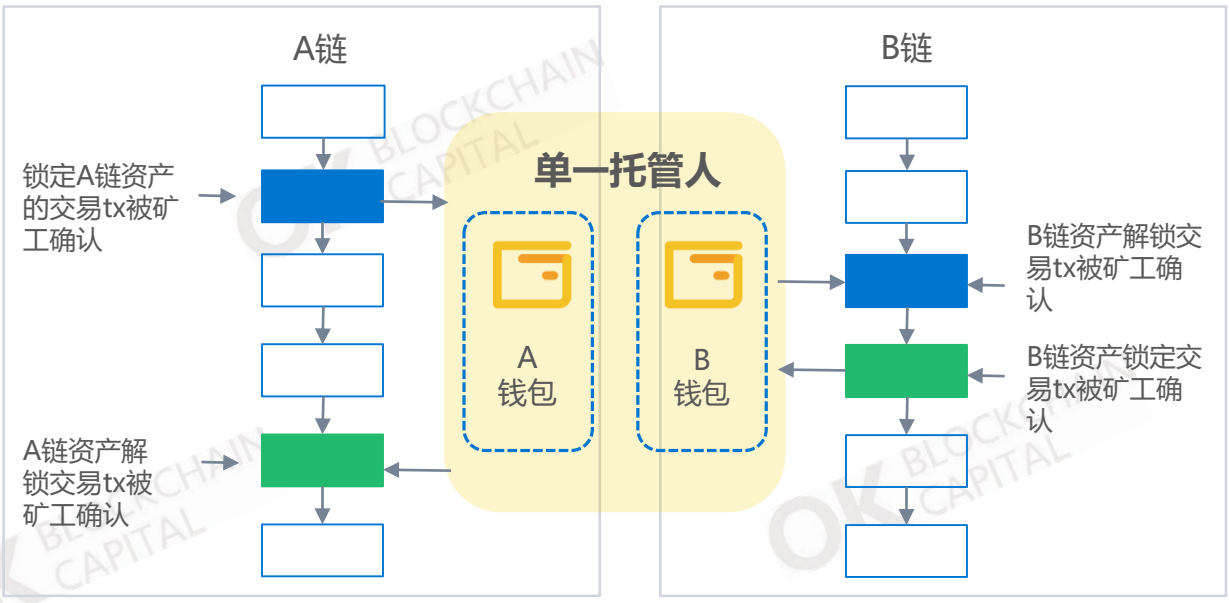
因为比特币上的BTC不能被销毁。所以实际上，当用户把BTC转换成SBTC的时候， BTC资产不是被销毁了，而是被转移到一个锁定地址上，同时在RSK上释放等量的SBTC。反之，当SBTC需要换回比特币时，把SBTC发送到RSK上的锁定地址，同时在比特币的锁定地址上释放等量的BTC。

在双向锚定的设计方案中的关键难题是，锁定账户由谁来管理，执行锁定和解锁等操作，如何保证锁定资产被安全的释放，不会造成双花。

锁定资产的管理有3种模式：

1. 单一托管人模式

由一个可信的单一托管人负责管理锁定的资产，执行并监管锁定资产的解锁操作。具体的流程可以由托管人手动执行，也可以通过软件协议来自动执行。



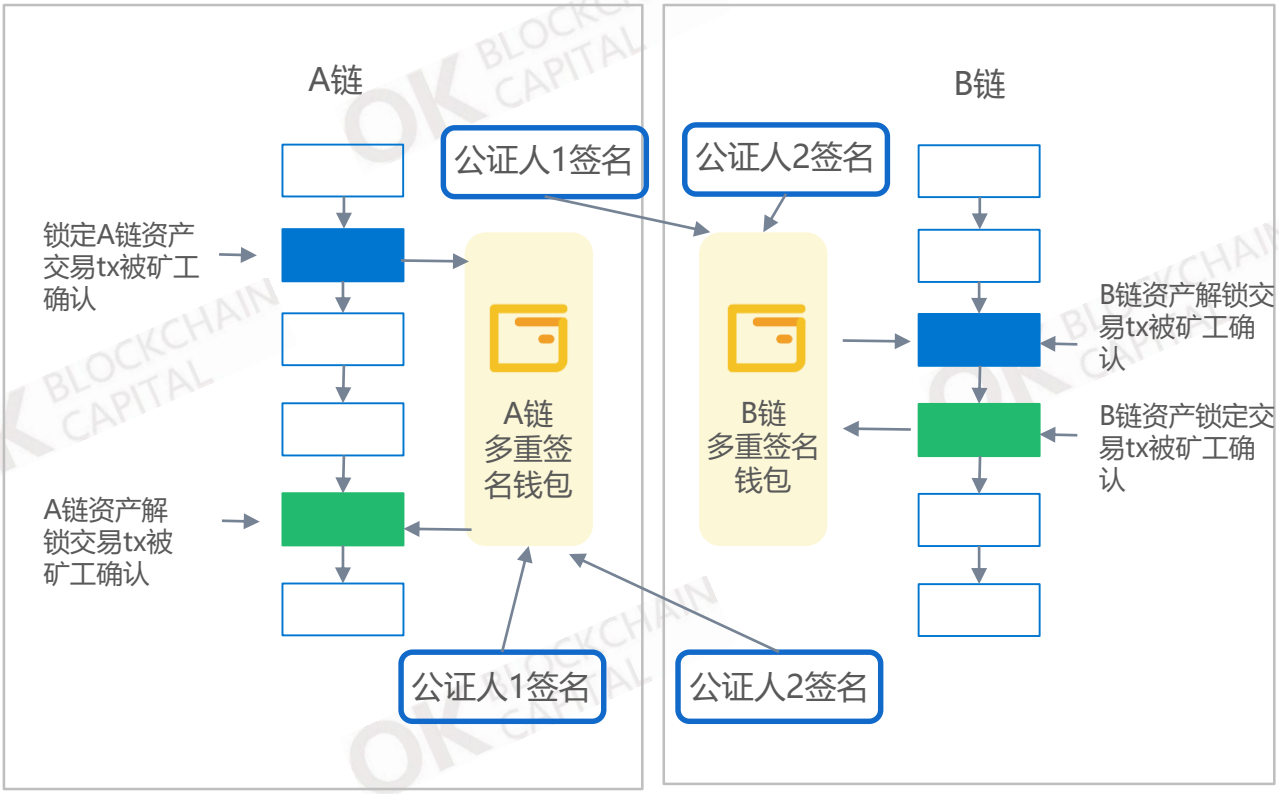
侧链与跨链

锁定资产管理——侧链与跨链关键技术

2. 联盟托管模式

单一托管机制虽然简单易行，但是过于依赖中心化的托管人。

更加去中心化的实现方式是联盟托管模式。类似于议会，总共有N个公证人，其中每一个位公证人都有一份投票权，当接收到跨链的解锁请求时，每一个公证人独立的验证交易并投票，当投票数达到M时，就能处置锁定的资产。这种验票、验证操作可以是手动执行，也可以是自动执行。



联盟公证人管理方式比单一管理更加合理，但是联盟中多个公证人依然可能互相串通，获得足够的控制权攻击锁定资产。为了保证资产安全，需要严格筛选公证人，尽量让他们分布在不同的司法管辖范围和商业机构、拥有良好的声誉。

侧链与跨链

锁定资产管理——侧链与跨链关键技术

3. 智能合约模式

为了实现更进一步的去中心化，锁定资产也可以通过智能合约来管理。这个方案的前提条件是该区块链系统能够支持智能合约，并且能够存储外部区块链的区块头来验证外部交易数据。

如下图，A链和B链分别有一个锁定地址，这两个锁定账户中的资产分别由锚定智能合约（Peg Contract）进行管理，而且这个智能合约存储了对方区块链的区块头，能够验证对方链上的交易。

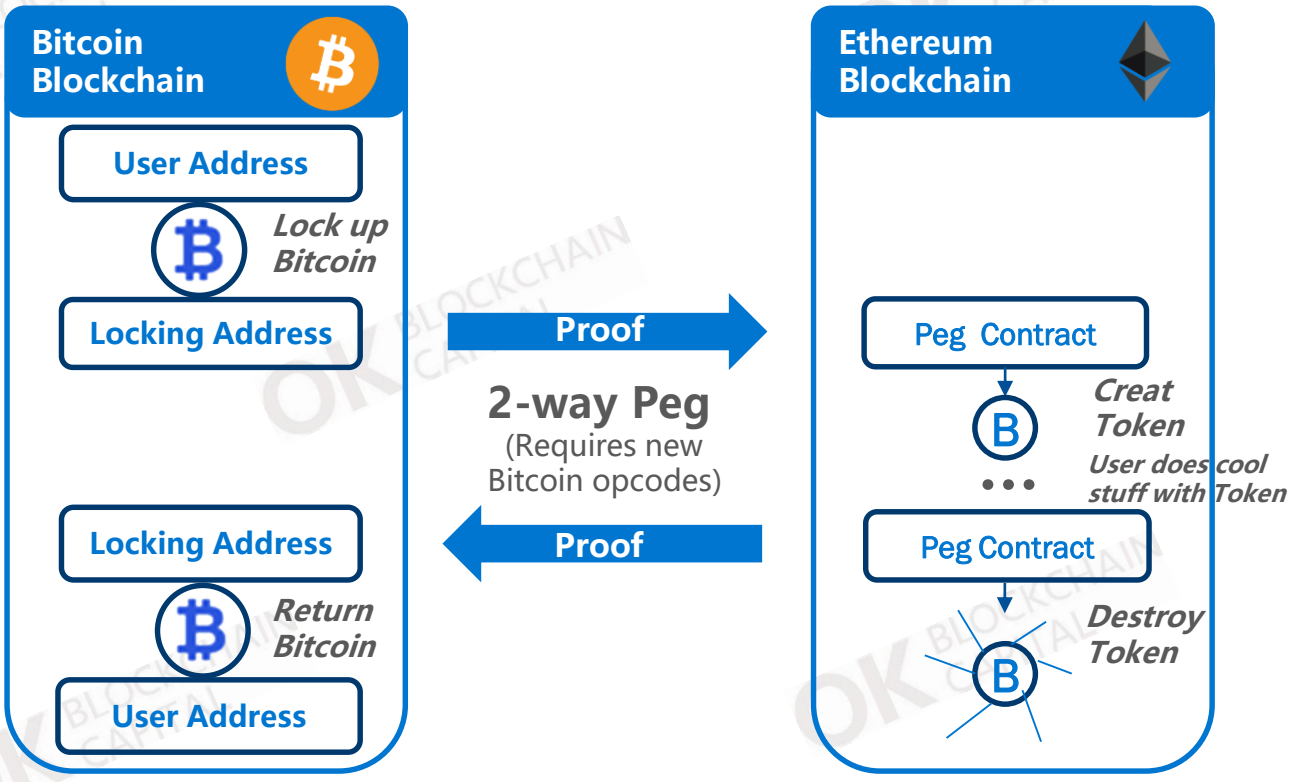
假设一个用户要把A链上的资产转移B链上，具体步骤如下：

1 用户在A链把资产转移到特定的锁定地址中，并且把自己在B链上的地址附加在交易中。

2 交易被矿工确认后，向B链的Peg Contract发送SPV验证。

3 B链的 Peg Contract 验证交易并且提取出用户在B链的地址。

4 如果交易验证成功而且满足最终确定性要求， B链的 Peg Contract 从锁定地址中转账对等的资产到用户的地址。

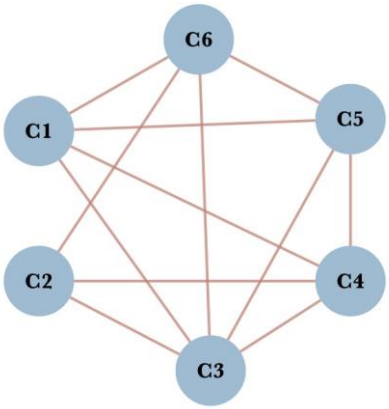


侧链与跨链

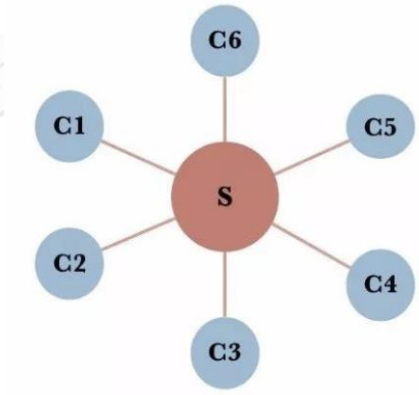
多链协议适配——侧链与跨链关键技术

以上讨论的问题都是1对1的侧链跨链问题。当更多的区块链系统需要跨链交互，就会出现多链协议适配问题。

如下图所示，一共有N个链，每两个区块链之间需要一个跨链协议，所以需要设计C(N, 2)个跨链协议，每一个跨链协议要适配两个区块链系统。当N变得很大的时候，协议适配的工作量会变得非常大。



解决这个问题的办法是，添加一个特殊的区块链作为中继链，它的角色是作为枢纽和其它所有区块链系统交互，居中转发其它区块链之间的跨链交易。采用这种架构，只需要设计N对跨链协议即可，而且每一个新加的区块链只需要适配中继链的跨链协议接口，大大降低了协议适配的复杂度。



侧链与跨链

闪电网络——本质上是可拓展的链下即时支付解决方案

闪电网络(Lightning Network) 是在2016年1月发表的论文"*The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*"中首次提出的新型比特币支付解决方案，作者是Bitcoin Core开发组的重要成员Joseph Poon, 和 Thaddeus Dryja。闪电网络在2017年12月发布了1.0 RC版本，成功在比特币主网上进行了测试。

随着比特币的普及率越来越高，自身的可扩展问题也越来越严重，具体表现为：

- 吞吐量低：平均每秒3笔交易
- 时延高: 每10分钟出个块
- 最终确定性慢: 等6个确认才能是为最终确定
- 存储量大: 50+万个区块，约160GB数据，而且不断增长

这些问题的根本原因在于每一笔交易都要广播给所有节点，所有记账节点必须:

- 限期地存储交易
- 验证交易
- 传递交易
- 打包并计入账本

所以导致资源的严重浪费。

闪电网络的思路是在比特币之上建立一个结算层，大量的微支付交易可以在结算层处理，没必要在比特币网络上处理。这样就可以降低比特币网络的压力，节约了资源，变相的扩展了比特币的处理能力，同时还能有很好的隐私性。

闪电网络底层的关键技术有3个：

- 时间锁(Time Lock)与哈希锁(Hashed Lock)

- Recoverable Sequence Maturity Contract (RSMC)
  拓展了单向支付通道技术，实现了双向支付状态通道

- Hashed Timelock Contract(HTLC)
  当一个交易包含多个子交易，可以使用HTLC保证交易的原子性。

侧链与跨链

闪电网络——本质上是可拓展的链下即时支付解决方案

托管合约(Escrow Contract) 与解锁条件

一般来讲，被托管合约管理的资产会一直处于锁定状态，只有两种方式才能将其中的资产解锁：

1. 在规定时间内，合约被正确执行
2. 合约逾期未执行，资产被原所有者赎回

哈希锁技术被用于约定谁拥有资产执行权，而时间锁技术是用于约定赎回的时间期限。在托管合约中往往这两种技术搭配使用。

时间锁(Time Lock)

比特币里面有两种方式定义时间锁：

- ❑ Transaction里的nTimeLock字段
  - 这个字段用于限制一笔交易在某个时间段内不能被打包，矿工只能把它放入 memory pool 中，直到指定的时间之后才能将此交易写入区块
- ❑ Transaction Output 解锁脚本中的操作码 OP_CHECKLOCKTIMEVERIFY
  - 这个操作码用于限制一个UTXO在某个时间段内不能被花费，在此期间所有花费此UTXO的交易自能临时保存在memory pool 中。

从上面的定义可以看出，他们的差异是作用的对象不同，一个是作用在交易上，另一个是作用在UTXO上。

哈希锁(Hashed Lock)

资产的执行权用一个大的随机数r来代表，先提前计算好它的哈希值 hash(r), 然后在托管合约中规定：申请解锁资产的人必须出示一个能匹配哈希值 hash(r) 的随机数才能有执行合约权力。在比特币中，操作符 OP_HASH256 用于匹配随机数和哈希值。因为这个解锁条件是通过哈希值来定义的，所以被称为哈希锁。

侧链与跨链

闪电网络——本质上是可拓展的链下即时支付解决方案

Revocable Sequence Maturity Contract (RSMC)

RSMC技术的作用在于：实现了双向支付通道，通过可撤销的资产分配合约表达双方的支付协议，而且此协议可以一直由双方本地保存，不需要上链也能保证可信性。大量的支付请求可以在链下处理，直到最终双方决定清算的时候才需要在链上执行。

如下图所示，假设Alice和Bob同意建立一个双向支付状态通道，共同出资建立一笔资金并存入一个托管账户。以后一段时间内，根据双方的交易情况，通过协商分配这笔资金，直到最终才清算这笔托管资产。原理如下：

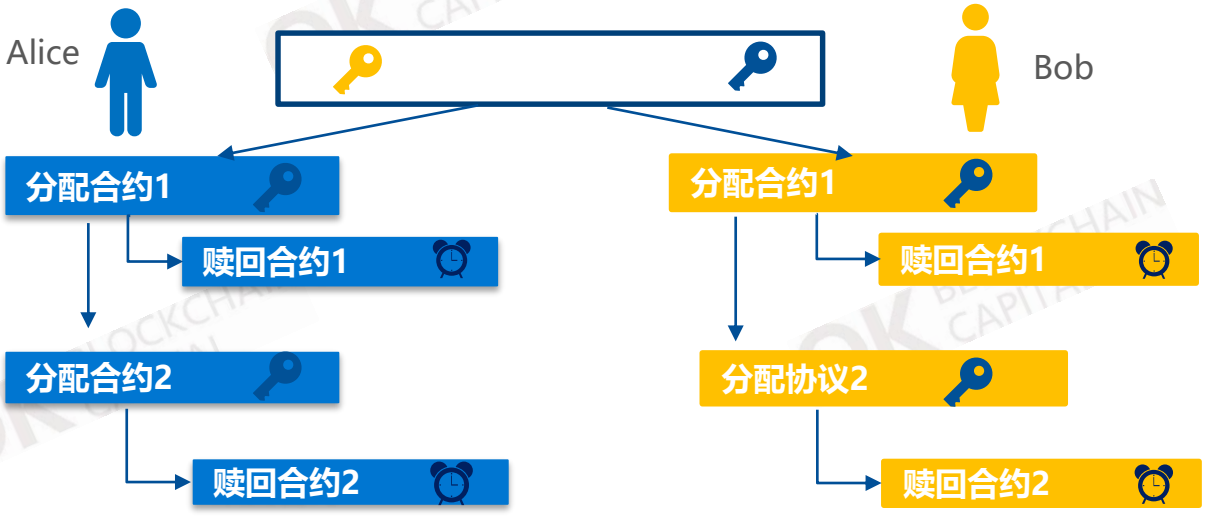
1 双方抵押的资产存入一个多重签名的托管账户，必须同时有Alice和Bob双方的签名才能花费其中的资产。

2 双方就如何分配资产达成分配合约。

每一次分配合约都由Alice和Bob各执一份，每一份都有对方的签名。比如Alice手中的分配合约有Bob的签名，如果Alice想按照这份合约清算托管资产，随时可以添加自己的签名就能处置托管账户。

3 新分配合约生效，旧的分配合约失效

每一次达成新的分配合约，旧的分配合约就会失效。失效的关键在于分配合约中隐含的赎回合约带有时间锁，在规定的时间内，清算发起人的赎回合约处于冻结状态。例如Alice按照分配合约1处置了托管账户中的资产，那么Bob通过监控监管账户及时发现Alice违背了分配合约2的约定，那么Bob可以在Alice的赎回合约1生效之前抢先处置资产。通过这样一个违约惩罚机制防止作废旧合约。



侧链与跨链

闪电网络——本质上是可拓展的链下即时支付解决方案

Hashed Timelock Contract(HTLC)

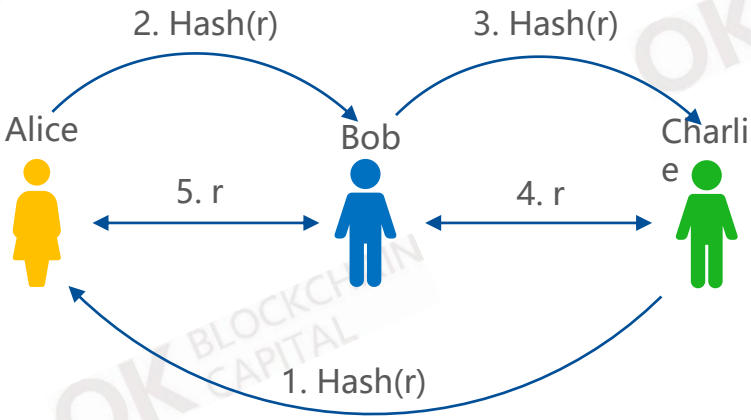
由多个支付通道首尾相连可以组成的一个支付通路，两端的双方即使没有直接相连的支付通道，也可以完成交支付交易。HTLC 技术就是协调多个支付通道最终对交易达成一致的协议。

假如Alice 要支付1 BTC给Charlie，但是他们没有直连的支付通道。但是Alice和Bob有一个状态通道。同时Bob和Charlie也有一个状态通道。

1 Alice 通知Charlie要向他发起支付，Charlie 生成一个随机密钥r，然后把其哈希值hash(r) 发给Alice

2 Alice 首先和Bob建立合约，如果Bob在2H小时内，出示一个匹配hash(r) 的随机密钥，那么Alice向Bob支付1BTC，否则逾期之后合约作废。

3 Bob得到hash(r)后，也和Charlie建立合约：如果Charlie在H小时内出示匹配hash(r)的随机密钥，那么Bob向Charlie支付1BTC，否则逾期之后合约作废



4 Charlie在H小时内向Bob出示随机密钥r，获得1BTC

5 Bob获得随机密钥r后，在2H小时向Alice出示随机密钥r，从Alice那里获得1BTC。最终完成支付交易。

小结：巧妙的运用哈希时间锁技术，闪电网络建立了链下支付通道的结算方式，然后再聚合支付通道形成一个网络。只要双方能够在这个网络中找到一条联通的路径，就可以通过一系列链下协议完成微支付交易。大大扩展了比特币的性能。

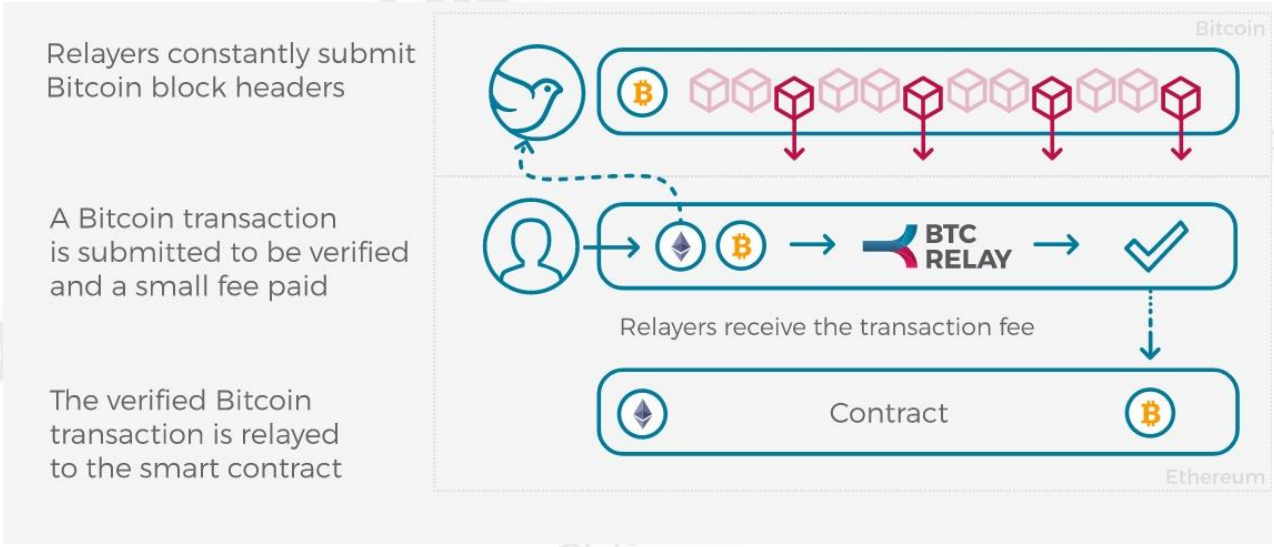
侧链案例

BTC Relay——比特币至以太坊的单向跨链通信

由ConsenSys团队推出的BTC Relay被认为是第一个侧链项目。BTC Relay是以太坊的一个智能合约，其核心功能是能够验证比特币上的交易。

Relayer：比特币Oracle

前面已经提到，跨链的交易验证本质上是一个跨链Oracle问题。BTC Relay为了能够验证比特币的交易，由Relayer 扮演Oracle的角色不断的向智能合约提交比特币的区块头数据。因为区块头里包含该区块里所有交易的Merkle Root，BTC Relay可以依据SPV(Simple Payment Verification) 机制验证比特币交易。



BTC Relayer 的功能依赖于 Relayer 能够提交正确的比特币区块头数据。所以设计了一个激励机制，奖励那些及时提交正确区块头数据的Relayer。鼓励社区更多的人成为 Relayer，一方面能够保证和比特币网络及时同步，一方面通过彼此竞争保证区块头数据的正确性。

侧链案例

BTC Relay——比特币至以太坊的单向跨链通信

跨链交易验证流程

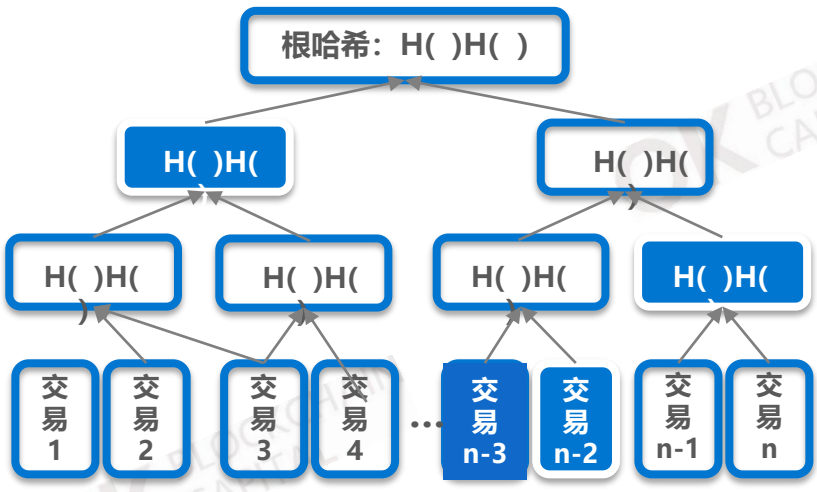
BTC Relayer的智能合约有了比特币的区块头数据之后，相当于成为了比特币的SPV轻客户端，可以验证所有来自比特币的交易。

验证的结果是判断这笔交易是否被写入某个比特币区块，以及得到了多少的确认数。交易验证的流程

1 用户首先为待验证交易构造SPV证明。证明包括：

a. 交易数据本身，以及所属的区块高度

b. 根据待验证支付交易对应的Merkle tree 认证路径。获取重新计算Merkle Root所需的哈希值.



2 用户把SVP证明发送给BTC Relay的智能合约

3 BTC Relay根据SPV证明重新计算Merkle Root，将计算结果与本地区块头中的Merkle Root相比较。

4 如果结果一致说明交易真实有效，并且根据区块头所处的位置，计算该交易已经得到的确认数。

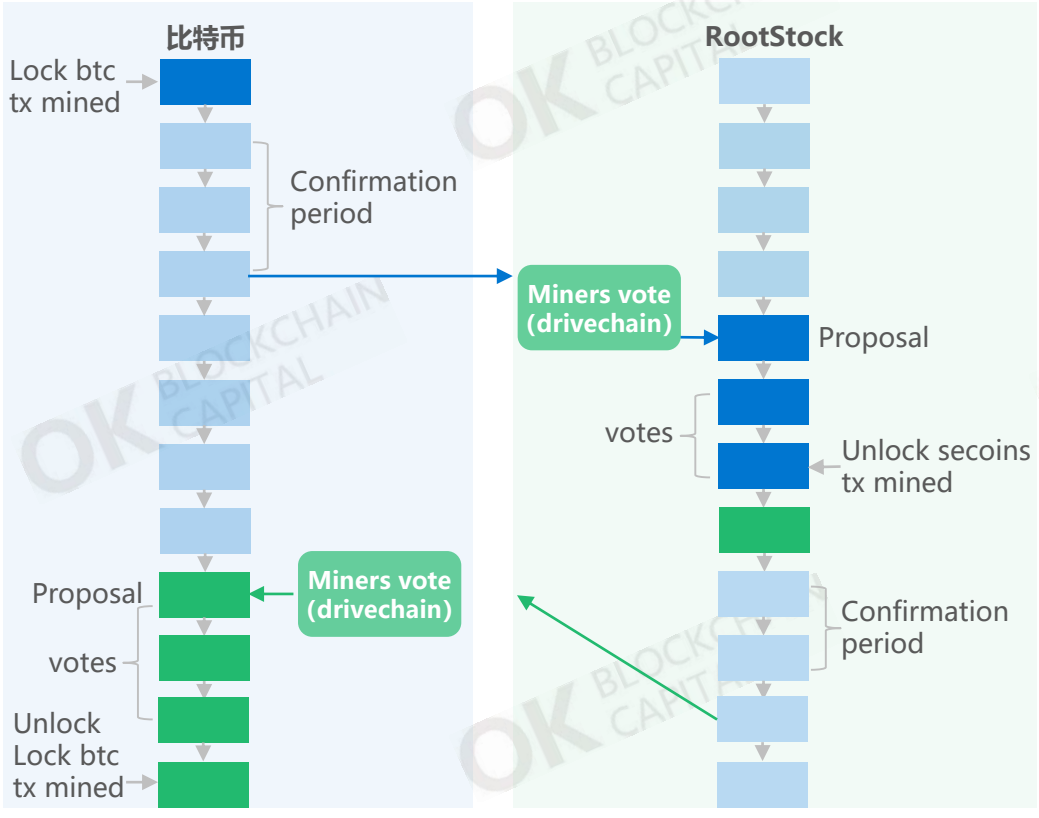
侧链案例

RootStock——双向锚定的比特币侧链

根链（RootStock）诞生于2015年，是建立在比特币上的智能合约平台，通过创建一条支持智能合约的侧链，并且通过双向锚定技术把BTC与侧链上的SBTC等比兑换，在保证安全性的同时扩展了比特币的功能。

根链的核心特点包括：

1. 图灵完备的虚拟机（智能合约）
2. BTC与根链上的SBTC双向锚定(2-Way Peg)
3. 动态联合挖矿/联邦的共识协议
4. 高吞吐量(300TPS)，低延迟(平均出块时间10秒)，低交易费



非对称双向锚定

比特币网络与根链有巨大差异，根链本身作为侧链支持图灵完备的智能合约，也可以验证比特币的交易。但是主链比特币没有对等的功能。

所以根链的双向锚定技术是不对称的。从BTC转成SBTC的转账机制，与SBTC转成BTC的转账机制是不一样的。

下表对比了BTC/SBTC 双向资产转移时所采用的跨链技术。

	BTC 转 SBTC	SBTC 转 BTC
跨链交易验证	区块头Oracle + SPV	公证人机制
交易最终确定性和原子性	等待多个交易确认	等待多个交易确认
锁定资产管理	通过侧链智能合约自动解锁SBTC	矿工+公证人投票解锁BTC

侧链案例

LISK——基于JavaScript的可扩展公链

LISK成立于2016年，是一种基于JavaScript的高度可扩展公链。Lisk平台可以使数百万开发者能够创建自己定制的区块链，特别是围绕着客户应用程序，包括游戏，社交网络和物联网。

LISK的关键特点包括：

1. 对于Javascript开发者社区友好
2. 使用Dpos共识算法，共有101个出块节点
3. 可以部署任意多条侧链，侧链与主链上的资产双向锚定。

5,800,000 USD	筹资金额	18,439,086 USD
100M LISK +Forging	总量	72M ETH+Mining
8M LISK	基金会留存	12M ETH
85M LISK ICO	分配	60M ETH ICO
1 year: 15.7M 2 year: 12.6M 3 year: 9.4M	出矿奖励	1 year Casper release:13M
DPoS	共识机制	PoW
10秒	出块时间	15秒
JavaScript	编程语言	Solidity

从侧链与跨链的技术角度来看，LISK的创新性在于：

1 采用了Dpos共识算法，每一笔交易都能很快的达到最终确定性，降低了跨链交易的延时。

2 每一个Dapp可以部署在一个独立的侧链上，与其它Dapp隔离，避免一个Dapp拥堵整条链的情况，起到了水平扩容的效果。

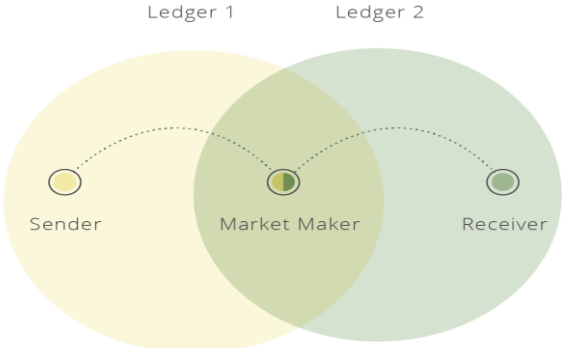
跨链案例

Ripple – Interledger (跨银行的全球清算系统)

Ripple 的目标是通过共识账本技术构建一个的全球支付网络，让世界各地的银行可以无需中央对手方或代理银行就可直接交易，从而使得让世界上的不同货币（包括法定货币和虚拟货币）自由、近乎免费、零延时地进行汇兑。

Ripple 的最底层是一个共识账本，共识算法名为”Ripple Consensus Protocol”，属于一种联盟链的共识算法。Ripple 同时还定义了Interledger（ILP）跨账本交易协议。此协议可以让Ripple账本既可以连接其它区块链系统，也可以连接银行，移动支付，ACH，p2p支付等传统金融机构。所以Ripple不是一个孤立的账本体系，而是通过ILP协议和许多大型金融机构互联互通的账本体系。

在ILP协议中，通过公证人机制建立银行账户与Ripple账本的双向映射关系。在银行间汇兑过程中，利用这个双向锚定机制，把发起者，流动性提供者，接收者的资金托管账户(Escrow)都映射到Ripple账本上，让托管账户的行为透明化。同时采用Hashed Timelock Agreement 协议，保证关联转账交易的原子性。最终实现去信认，高效的银行汇兑。

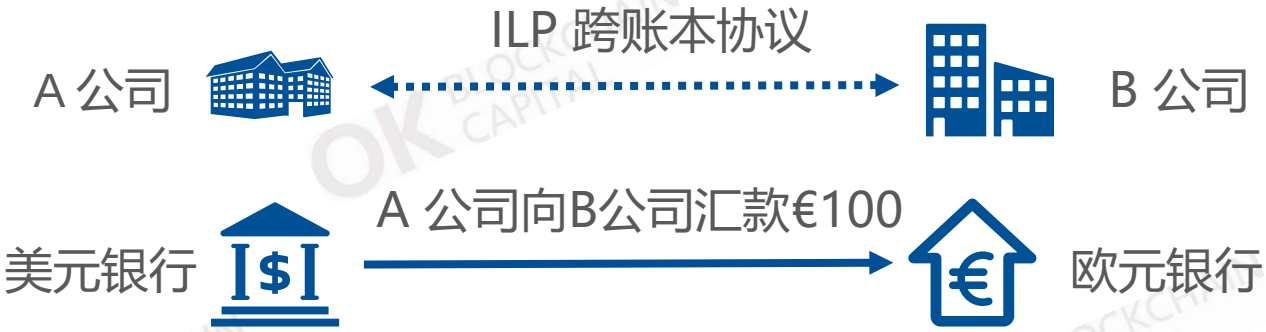


跨链案例

Ripple – Interledger (一个主要为金融机构设计的全球清算系统)

跨境汇款案例分析

假设在美国的A公司需要付给在欧元区的B公司100欧元。A公司在美国有美元账户，B公司在欧元区有欧元账户，流动性提供者同时在美元银行和欧元银行开设账户，并且在欧元账户持有头寸。这次美元银行和欧元银行之间的跨境汇款使用Ripple的 ILP 协议完成最终的清算。



整个汇款过程中涉及：

- 3个账本：美元银行账本、欧元银行账本、ILP Ledger账本。
- 4个参与者：付款方A公司、收款方B公司、流动性提供商C，Ripple资金托管者
- 账户：

1. A公司有美元账户，B公司有欧元账户，

2. 流动性提供商有美元账户和欧元账户。同时也在ILP Ledger 账本中有美元/欧元账户。银行账户与ILP Ledger账户双向映射。

3. Ripple资金托管者在美元银行和欧元银行分别开设独立托管账户（Ripple Segregated Account），这两个托管账户与 ILP Ledger 账本中的托管（Hold）账户双向映射，最后资金由Ripple网络负责清算。

跨链案例

Ripple – Interledger (一个主要为金融机构设计的全球清算系统)

汇款流程

1　汇款前准备：流动性提供商C 预存准备金

在交易发起之前，流动性提供商C在欧元银行中存入了1000欧元，并且全部转入到Segregated独立账户，用于这笔交易的流动性支出。并且将美元/欧元汇率报价提供给外汇交易市场。Ripple 将Segregated账户的存款同步到流动性提供商C在Ripple账本中的欧元账户。

此时各个账户的状态如下：

美元银行账本	
账户	余额
A公司	$125
流动性提供者C	/
Ripple Segregated Account	/

欧元银行账本	
账户	余额
B公司	€0
流动性提供者C	€0
Ripple Segregated Account	€1000

Ripple网络上的 ILP Ledger	
账户	余额
美元银行（Hold）	/
流动性提供者C	/

Ripple网络上的 ILP Ledger	
账户	余额
欧元银行（Hold）	/
流动性提供者C	€1000

2　付款方A公司询价

- A公司在外汇报价市场中选择汇率最低的流动性提供商C，确认汇率为EUR/USD=1.25，所以A公司要付款125美元。A获取B公司的欧元收款账户信息，然后将收款人的银行账户以及转账金额等信息打包广播到Ripple网络里面。

跨链案例

Ripple – Interledger (一个主要为金融机构设计的全球清算系统)

3　A公司支付美元：

美元银行将A公司账户的125美元转到Ripple Segregated账户，账户余额的变动映射到Ripple网络账本的托管账户中，美元银行(Hold)账户余额更新为125美元，发送转账证明给验证人（Validator），证明美元银行(Hold)账户的资金已经到账。

此时各个账户的状态如下：

美元银行账本	
账户	余额
A公司	$0
流动性提供者C	/
Ripple Segregated Account	$125

欧元银行账本	
账户	余额
B公司	€0
流动性提供者C	€0
Ripple Segregated Account	€1000

Ripple网络上的 ILP Ledger	
账户	余额
美元银行（Hold）	$125
流动性提供者C	/

Ripple网络上的 ILP Ledger	
账户	余额
欧元银行（Hold）	/
流动性提供者C	€1000

4　从流动性提供商C的欧元账户计提欧元

- 在ILP Ledger 中，从流动性提供商C的欧元账户转出100欧元到欧元(Hold)账户.并且发送转账证明给验证人（Validator），证明欧元银行(Hold)账户的资金已经到账。
- 此时各个账户的状态如下：

美元银行账本	
账户	余额
A公司	$0
流动性提供者C	/
Ripple Segregated Account	$125

欧元银行账本	
账户	余额
B公司	€0
流动性提供者C	€0
Ripple Segregated Account	€1000

Ripple网络上的 ILP Ledger	
账户	余额
美元银行（Hold）	$125
流动性提供者C	/

Ripple网络上的 ILP Ledger	
账户	余额
欧元银行（Hold）	€100
流动性提供者C	€900

跨链案例

Ripple – Interledger (一个主要为金融机构设计的全球清算系统)

5 资金清算：

- 验证人（Validator）收到两个转账证明，而且验证通过之后，开始触发Ripple网络在ILP Ledger上进行资金清算。通过Hashed Time Lock Agreement 原子交易协议，同时释放美元Hold账户与欧元Hold账户资金。由于双向锚定机制，把ILP Ledger上的转账分别同步到美元银行和欧元银行账本。
- 最终A公司的125美元支付给了流动性提供商C，流动性提供商C的100欧元支付给了B公司，流动性提供商C居中提供了汇兑服务，整个汇款过程完成。
- 最终各个账户的状态如下：

美元银行账本	
账户	余额
A公司	$0
流动性提供者C	$125
Ripple Segregated Account	/

欧元银行账本	
账户	余额
B公司	€100
流动性提供者C	€0
Ripple Segregated Account	€3900

Ripple网络上的 ILP Ledger	
账户	余额
美元银行（Hold）	$0
流动性提供者C	$125

Ripple网络上的 ILP Ledger	
账户	余额
欧元银行（Hold）	€0
流动性提供者C	€3900

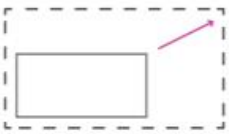
6 总结

- ILP Ledger协议使得两个不同的记账系统可以通过流动性提供者来自由地兑换货币。记账系统无需信任第三方流动性提供者。该协议采用公证人机制，将银行资金转账映射到 ILP Ledger账本，再利用区块链的公开性、透明性、可编程性实现跨银行的清算，极大提高了跨境转账的效率和安全性。

跨链案例

Polkadot——创新的平行链和多链桥接技术

Polkadot 的愿景是解决异构多链互联互通问题，支持众多高度差异化的共识系统在完全去中心化的网络中交互操作，允许去信任地相互访问各区块链。同时向后兼容一个或多个现有的网络，比如以太坊等。



Scalability

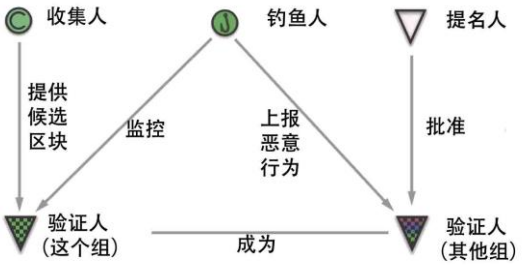
在异构多链架构里，Polkadot 的定位是一条中继链，作为跨链通信的枢纽链接其它链，其本身不关注区块链平台上应用的丰富性，只实现尽可能少的功能。它提供一套通用的跨链协议，其它兼容此协议的区块链系统都可以通过Polkadot互联互通。

Governance

为了支撑中继链的功能，Polkadot 的技术特点有：

- 激励和监督的机制——网络中的基本角色划分如下4种，其中验证人需要锁定押金才能获取记账权，用于惩罚将来的不当行为。
  - 验证人：参与记账共识，并且验证平行链上的数据
  - 提名人：为验证人提供押金和信用背书
  - 收集人：采集平行链上的数据并且提交给验证人
  - 钓鱼人：作为赏金猎人，监督其它参与者的恶意企图。

Isolability



Developability

- 共识算法：采用基于POS的共识算法， 系统内有144个验证人，出块时间为4s，达到最终确定性需要1个小时(900个块)。
- 智能合约：内置一些特定的系统合约，包括共识合约、验证人合约、平行链合约， 不支持公开部署合约。
- 平行链的注册： 简单的类数据库的结构，管理着平行链的静态信息和动态信息。
- 平行链的验证：建立了验证平行链数据的共识机制。
- 跨链交易路由：提供一个无需任何信任人的跨链消息路由机制。
- 手续费：使用通用的手续费标准，没有资源计数器(gas)

Applicability

跨链案例

Polkadot——创新的平行链和多链桥接技术

以Polkadot 与以太坊的双向跨链通信为例，来阐述跨链通信的机制设计。

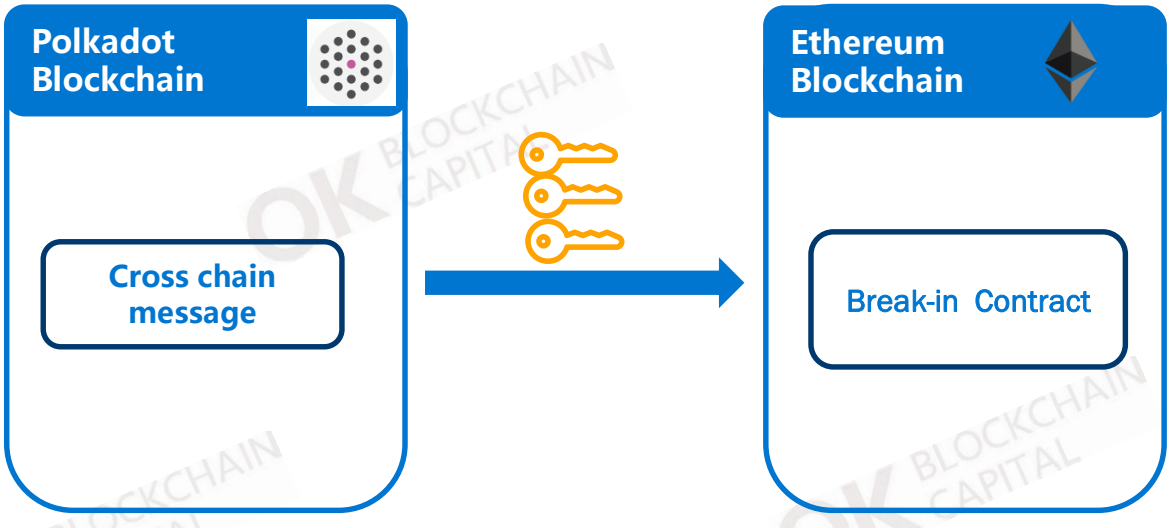
Polkadot到以太坊的跨链机制

以太坊作为消息的接收者，需要验证来自Polkadot转发的跨链消息。前文中提到，跨链验证通常有模式：1.公证人联盟模式，2.区块头Oracle+SPV模式。

由于Polkadot的出块频率比较高，采用第2种模式需要以太坊存储大量区块头数据，所以采用了第1种模式。让验证人先签名，然后再转发给以太坊，在那里通过合约来解释和执行。

- 在Polkadot端，由144个公证人组成联盟，依据拜占庭容错算法，每个跨链消息需要97个公证人签名。
- 在以太坊端：部署一个内向合约(break-in contract) 控制和维护144个签名，验证来自Polkadot的跨链消息。

一个跨链消息首先由Polkadot验证人在本地验证并签名，收齐97个签名之后由验证人发送到以太坊的内向合约。内向合约验证所有签名，如果验证通过之后1小时没有被撤回就被最终确认(Polkadot共识机制的最终确定性需要1个小时)。



跨链案例

Polkadot——创新的平行链和多链桥接技术

以太坊到Polkadot的跨链机制

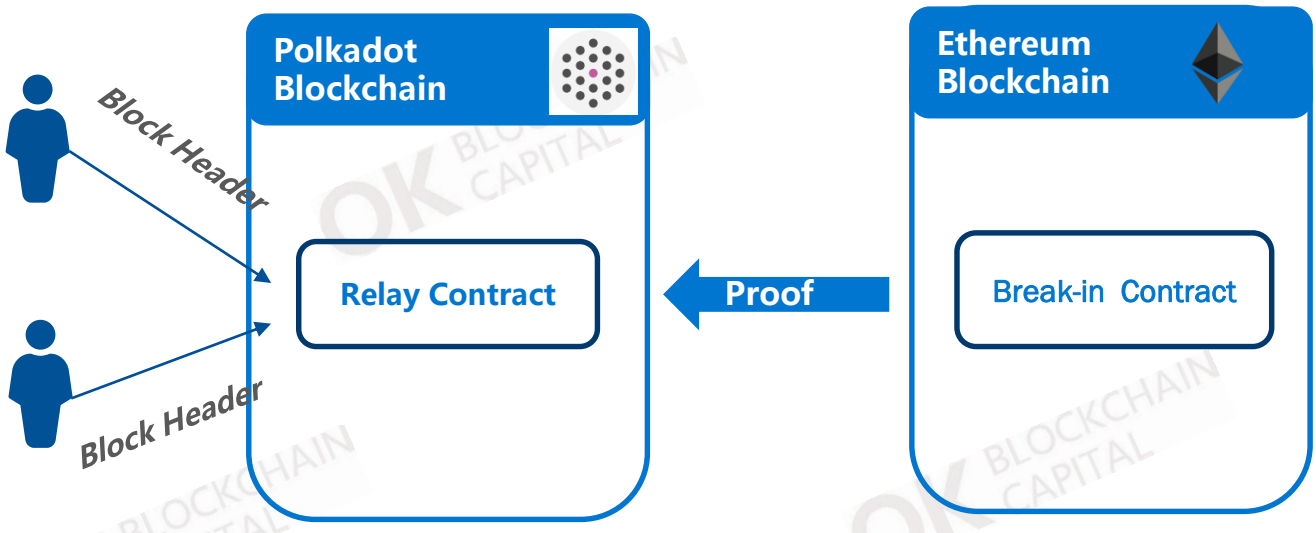
Polkadot采用区块头Oracle+SPV模式接收并且验证来自以太坊的跨链消息。

- Polkadot端：提供一个接受以太坊新区块头的接口，以token鼓励第三方参与者提交以太坊的新区块头。同时要求参与者必须提交押金，当钓鱼人发现参与者作弊时，扣除押金作为惩罚。以此奖惩机制建立去中心化的区块头Oracle。另外部署一个Relay Contract，根据已知的区块头验证来自以太坊的SPV证明。

- 以太坊端：部署外向合约(break-out contract)。其功能是把待转发的消息输出到以太坊日志，日志可以通过SPV的方式验证。

跨链通信流程如下：

1. 待转发的消息通过外向合约输出到以太坊日志
2. 生成日志的SPV证明，并且发送至Polkadot 的Relay Contract
3. 如果Relay Contract 验证通过，并且此日志已经积累了120个确认就被最终确认。



总结

侧链跨链技术

以比特币、以太坊为代表的公链项目已经向我们展示了区块链的巨大发展前景。但是由于区块链本身技术特点，单链解决方案受到去中心化，安全性，可扩展性的不可能三角的约束，在可扩展性上一直缺少革命性的突破。侧链跨链方案带来新的解决思路：

资产双向锚定、单一资产跨链使用，扩展应用场景

通过双向锚定技术，可以把一条链上的资产转移到其它链上。借助于新的区块链系统，可以大大扩展原有资产的技术特性和应用场景。不但可以分担主链上的交易，节约主链的存储，计算，网络等资源，避免了主链上的交易拥堵，还不会损害原有代币的价值。

同构跨链，水平扩容方案

侧链跨链技术也为水平扩容解决方案提供了可能。利用分片技术，一个主链分成若干个同构的子链。每一条子链的功能性能都是类似的。用户的资产选择其中任何一些子链管理。通过跨链技术这些资产可以在子链之间转移和交互。系统的交易可以在多个子链上并行处理，达到了水平扩容的效果。

另外，Dapp 也可以部署在自己专属的子链上，和其它子链上的Dapp隔离。在提高性能的同时，也提高了安全性：不受其它子链上的Dapp的影响。

异构跨链，构建多链资产的去中心化交易

去中心化交易所是异构跨链技术的主要应用领域。长期以来，去中心化交易一直受跨链技术的制约，当前的去中心化交易只能提供同一个公链上的资产交易服务。未来，跨链技术可以帮助去中心化交易所打破这个限制，支持任意两个公链上资产的交易。

侧链跨链技术的兴起，为突破单链可扩展性的限制带来了希望。但是，目前侧链跨链还有不少开放式的问题没有得到彻底解决，随着更多区块链开发者在这个领域的探索和实验投入，侧链跨链技术有望在近2年中实现巨大的突破。

OK BLOCKCHAIN CAPITAL