侧链跨链研究报告

引言

在不断推进区块链技术快速发展的同时，我们面临的一个关键瓶颈，是如何提高交易的吞吐量和交易的速度问题，随后各种解决方案应运而生。本文介绍了侧链和跨链的定义以及发展历史，同时分析了侧链的痛点以及区块链技术和痛点的相关性。根据目前已上市的币种/产品信息来对应用的技术方案以及侧链技术的投资逻辑进行分析，最后对侧链/跨链的未来进行了展望

（本报告由鲸准研究院 X Node Capital 联合发布）

作者：

鲸准研究院 谭莹、王帆、陈泓伊

Node Capital 研究中心 刘聪海，马旭颖，林婕茵，郎瀚威

支持机构：

巴比特，火星财经，金色财经，金牛财经

目录

一、 侧链

1.1 侧链的概念

早在比特币诞生初期，人们就意识到比特币在转账速度、容量以及智能合约等方面的不足，如果说能建立比特币账本的一个副本，就像以前许多法定货币由黄金担保一样，在需要的时候资产可以在两个区块链之间相互转换，就可以加速比特币或者其他数字资产的流动性。在继续基于公共区块链的比特币信用证明的同时，侧链也能支持完成一些更为复杂的应用操作。

比特币与比特币侧链都使用比特币作为系统货币。其实质是通过“双向锚定”机制实现主链货币价值向侧链体系的转移，从而在侧链上使用这部分从主链转移过来的主链货币的价值，至于以这部分主链货币价值背书而产生、发行的侧链货币的名称，则可以按需自由命名。

侧链协议可以帮助比特币在其他区块链上流通，其应用范围和应用前景会更加广泛。有创意的人们会研发出各种各样的应用以侧链协议与比特币主链对接，使得比特币这种基准自由货币的地位越牢固。

1.2 侧链的历史

侧链协议产生的原动力其实来源于其他区块链的创新威胁。首先，以太坊（Ethereum）、比特股（Bitshares）等更快、更智能的区块链对比特币产生相当大的威胁，智能合约和各种去中心化应用在以上两个区块链上兴起，受到人们欢迎；而基于比特币的应用则因为开发难度大，项目不多。其次，基于比特币区块链也有合约币（Counterparty）、万事达币（Mastercoin）和彩色币（ColoredCoin）等附生链，但是比特币核心开发组并不欢迎，觉得它们降低了比特币区块链的安全性。他们

曾经一度把 OP_RETURN 的数据区减少到 40 字节，逼迫合约币开发团队改用其他方式在比特币交易中附带数据。第三方面，2014 年 7 月份以太坊众筹时，获得了价值 1.4 亿人民币的比特币，还有 20%的以太币，开发团队获得了巨大的回报。但是比特币核心开发组并没有因为他们辛勤工作获得可观回报，因而他们成立了 BlockStream，拟实现商业化价值。基于以上三个原因，研发团队提出侧链协议、把比特币转出比特币区块链、另行开发二代区块链，这样的选择既能保证比特币区块链的安全，又能应对二代币的冲击，还能针对不同应用场景实现商业化，因而成了 BlockStream 的必然选择。

1.3 双向挂钩技术

双向挂钩（2WP）是侧链实现的核心原理。它允许将比特币从比特币区块链转移到辅助区块链，反之亦然。“转移”实际上是一种错觉：比特币其实并没有转移，但在比特币区块链上被暂时锁定，而同时在辅助区块链上有相同数量的等价令牌被解锁。当等量的令牌在辅助区块链上被再次锁定时，原先的比特币就会被解锁。这实质上就是双向挂钩所要实现的功能。这一功能的问题是，理论上只有当辅助区块链最终结算时才能被实现。因此，任何双向挂钩系统必须作出妥协并且依靠于假设双向挂钩相关参与者是诚实的。最重要的假设是，主要的区块链是无需审查的，而且大多数比特币矿工都是诚实的。另一个需要的假设可能是，大多数监管锁定比特币的第三方也是诚实的。如果这些假设不成立，则比特币及等效辅助区块链的令牌可以被同时解锁，那么恶意的双花就变得可行了。任何双向挂钩系统都必须选择一种措施，使得被假设要诚实的各方都能在经济和法律方面受鼓励去依章办事。这包括分析这些关键方对区块链网络进行攻击的成本及后果。双向挂钩实施的安全性取决于激励机制，以便参与双向挂钩系统的关键方能够真正执行双向挂钩所应实现功能。

双向挂钩技术可通过以下四项技术实现：单一托管、联盟模式、SPV 模式、驱动链模式和混合式设计。

	概念	优点	缺点
单一托管模式	将数字资产发送到一个主链单一托管方（类似于交易所），当单一托管方收到相关信息后，就在侧链上激活相应数字资产	不需要对现有的比特币协议进行任何的改变	过于中心化
联盟模式	使用公证人联盟来取代单一的保管方，利用公证人联盟的多重签名对侧链的数字资产流动进行确认	不需要对现有的比特币协议进行任何的改变 要想盗窃主链上冻结的数字资产，需要突破更多的机构	侧链安全仍然取决于公证人联盟的诚实度
SPV模式	用户在主链上将数字资产发送到主链的一个特殊的地址，以锁定主链的数字资产，随后会创建一个SPV证明并发送到侧链上。此刻，一个对应的带有SPV证明的交易会出现在侧链上，同时验证主链上的数字资产已经被锁住，就可以在侧链上打开具有相同价值的另一种数字资产。 这种数字资产的使用和改变在稍后会被送回主链。当这种数字资产返回到主链上时，该过程会进行重复。它们被发送到侧链上锁定的输出中，在一定的等待时间后，就可以创建一个SPV证明，来将其发送回主区块链上，以解锁主链上的数字资产。	安全性增强,小额的交易通过走侧链的方式，可以更好的隐蔽拥有大量存储价值的主账户地址； 侧链可以分担主链上的交易负担，增快交易速度；智能合约可以更好的实现并保护交易过程，保证交易的稳定性；侧链的应用十分广泛，可扩展应用的范围，同时有效保护区块链的隐私保护	需要对主链进行软分叉
驱动链模式	矿工作为算法代理监护人，监管被锁定数字资产，投票决定何时解锁数字资产和将解锁的数字资产发送到何处	矿工在驱动链中的参与程度越高，系统安全性越大	需要对主链进行软分叉
混合模式	在主链和侧链使用不同的解锁方法	在主链和侧链上采用不用的模式解决，有效提高了处理效率	需要对主链进行软分叉

二、 跨链

2.1 跨链的概念

区块链是分布式总账的一种。一条区块链就是一个独立的账本，两条不同的链，就是两个不同的独立的账本，两个账本没有关联。本质上价值没有办法在账本间转移，但是对于具体的某个用户，用户在一条区块链上存储的价值，能够变成另一条链上的价值，这就是价值的流通。

跨链，顾名思义，就是通过一个技术，能让价值跨过链和链之间的障碍，进行直接的流通。跨链本质上和货币兑换是一样的。跨链并没有改变每个区块链上的价值总额，只是不同的持有人之间进行了一个兑换而已。 跨链技术的核心要素之一是：帮助一条链上的用户 Alice 找到另一条链上的愿意进行兑换的用户 Bob。从业务角度看，跨链技术就是一个交易所，让用户能够到交易所里进行跨链交易。

进行数字货币的交易所很早就出现了，最早交易所进行的是法币（国家发行的货币）与比特币之间的兑换。后来随着数字货币的种类越来越多，很多交易所也开始进行不同类型数字货币之间的兑换。交易所开展的不同类型数字货币之间的兑换，就是一种跨链价值转移的实现。严格来说，币币交易所就是一个跨链技术的实现。

鉴于已经发生过的多起交易所盗币、跑路的问题，单个人或者机构的信用都不足以支撑大额交易。因此，出现了无中心交易所技术——用区块链技术解决跨链时的信用难题。当交易所由多个主体共同运行，或者干脆是一个公有链，任何人都能参与到这个交易所的运行中，那么，跑路的风险就大大降低了。

2.2 解构四种跨链技术

四种主流的跨链技术：

1、公证人机制（Notary schemes）

2、侧链/中继（Sidechains/relays）

3、哈希锁定（Hash-locking）

4、分布式私钥控制（Distributed private key control）

四种模式性能的对比：

	公证人模式（Notary Schemes）	侧链(Sidechains)/中继(Relays)	哈希锁定(Hash-locking)	分布式私钥控制(Distributed private key control)
互操作性	所有	所有（需要所有链上都有中继，否则只支持单向）	只有交叉依赖	所有
信任模型	多数公证人诚实	链不会失败或者受到“51%攻击”	链不会失败或者受到“51%攻击”	链不会失败或者受到“51%攻击”
使用跨链交换	支持	支持	支持	支持
使用跨链资产转移	支持（需要共同的长期公证人信任）	支持	不支持	支持
适用跨链Oracles	支持	支持	不直接支持	支持
适用跨链资产抵押	支持	支持	大多数支持但是有难度	支持
实现难度	中等	难	容易	中等
多种币智能合约	困难	困难	不支持	支持

四种模式的技术对比：

	公证人模式（Notary Schemes）	侧链(Sidechains)/中继(Relays)	哈希锁定(Hash-locking)	分布式私钥控制(Distributed private key control)
工作流程	在公证人模式中，使用受信任的一个或者一组团体向一条链声明另一链上发生了某事件，或者确定该声明是正确的。这些团体既可以自动地监听和响应事件，也可以在被请求的时候进行监听和响应事件。	假设区块链拥有区块Header和Body，Header中拥有Merkle等证明信息，可以将链A的区块链头，写入链B的块中，链B使用和链A一样的共识验证方法。等待链A的区块头序列之后，链B就可以通过Merkle分支的证明信息来证明链A的数据和操作。	A生成随机数S，并发送hash(S)给B;A在链LA上锁定币，并设定条件：如果在（当前时间+2X=TA）时间内链LA收到S，则转账给B，否则退回给A；B收到hash(S)，并看见A的锁定和时间设定后，在链LB上锁定币，并设定条件：如果在TA-X时间内链LB收到S，则转账给A，否则退回给B；A看见B的锁定后，在TA-X时间内发送S给链LB，得到链LB的币p；B收到S后，在TA时间内发送S到链LA，得到链LA的币。	利用一个基于协议的内置资产模板，根据跨链交易信息部署新的智能合约创建新的资产。当一种已注册资产由原有链转移到跨链上时,跨链节点会为用户在已有合约中发放相应等值代币,确保了原有链资产在跨链上仍然可以相互交易流通。
模式特点	假设A和B是不能进行互相信任的，那就引入A和B都能够共同信任的第三方充当公证人作为中介，那么A和B间接可以互相信任。相反它提供了一个顶层加密托管系统称之为“连接者”，在这个中介机构的帮助下，让资金在各账本间流动。	如果一个链B能拥有另外一个链A的所有功能，则称链B为链A的侧链，链A为链B的主链。其中主链A并不知道侧链B的存在，侧链B知道有主链A的存在。中继是链与链之间的通道，如果通道本身是区块链，那就是中继链。侧链和中继是目前应用相对多是两种模式。	哈希锁定起源于比特币闪电网络，闪电网络本身是一种小额的快速支付的手段，后来它的关键技术哈希时间锁合约被应用到跨链技术上来。	委托去中心化的网络掌管用户私钥，事实上用户同时还掌握了自身代理资产的那部分私钥，所以这笔资产从来没有离开用户的掌控，它并没有像中心化的交易所一样，完全用第三方来掌握这个资产。
优点	既可以提供灵活共识的主要竞争者，也无需进行昂贵的工作证明或关于利益机制的复杂证明。是链与链之间互操作最简单的方法	中继器/侧链模式均能支持跨链资产交换及转移，跨链合约和资产抵押	哈希锁定模式的设计是链与链之间尽可能少的了解彼此，并作为消除公证人信任的手段	用户并没有失去对这笔资产的控制权，拥有私钥才是拥有对这笔资产的控制权。
缺点	这种模式和区块链的去中心化的理念存在一些冲突，所以很多人不认为它是区块链，而更多是一种中心化的产物。	侧链从技术层面讲实现性很难	虽然哈希锁定实现了跨链资产的交换，大部分场景能够支持资产抵押，但是没有实现跨链资产的转移，更不能实现这种跨链合约，所以它的应用场景是相对比较受限的。	智能合约还需要多方面实现
典型项目	Corda，Interledger	侧链：BTC Relay 中继：Polkadot，COSMOS	Lighting network	WanChain，FUSION，EKT

2.3 跨链技术的应用

1. **可转移的资产**：资产可以多链之间来回转移和使用。

2. **原子交易**：链间资产的同时交换。

3. **跨链数据预言机**：链 A 需要得知链 B 的数据的证明。

4. 跨链执行合约：例如根据链 A 的股权证明在链 B 上分发股息。

5. 跨链交易所：对于协议不直接支持跨链操作的区块链进行补充

三、 跨链/侧链的优势与问题

3.1 跨链与侧链的关系

早期的开源侧链项目比如 blockstream 的元素链，使用的比特币双向挂钩技术，它是跨链的雏形。到后来的 BTC-Relay（一种基于以太坊区块链的智能合约），是通过跨链将比特币和以太坊连接起来的技术。早期的项目主要关注资产的转移，而如今的跨链项目则更多关注链状态的转移，这就形成了各个跨链的技术今天的格局。一般的侧链服务于主链，而跨链志在链之间价值和功能的连通，可以说，侧链与跨链，在技术内容上大体相似，只在谈到他们所服务的对象时才需要做细致的区分。

3.2 跨链与侧链的优势

为了解决公有链的低吞吐量带来的高手续费、网络拥塞等诸多问题，很多团队都很有预见性的提出了相应的优化方案。从现有技术实现的角度来说，基本分为三种，分别是侧链，分片和 DAG。

三种技术对比：

	侧链	分片	DAG
技术定义	为了解决比特币拥堵的问题，提出的一种跨区块链的解决方案， 可以让比特币安全地在比特币主链与其他区块链相互转移	是一种传统数据库的技术，它将大型数据库分成更小、更快、更容易管理的部分	有向无环图，是计算机领域一个常用的数据结构，因为独特的拓扑结构所带来的一些特性，经常被用到处理动态规划，导航中寻求最短路径，数据压缩等场景中。
工作流程	侧链是以锚定比特币为基础的新型区块链，侧链是以融合的方式实现加密货币金融生态的目标，旨在使用户可以在具有不同规则设定的不同基于比特币的区块链上转移比特币	是将区块链网络划分成若干能够处理交易的较小组件式网络，以实现每秒处理数千笔交易的支付系统，应用到区块链当中会相当复杂。	DAG摒弃了区块的概念，交易直接进入全网中，速度相比于需要出块的区块链快很多；DAG把交易确认的环境直接下放给交易本身，无需由矿工打包成区块后同意交易顺序。所以DAG网络中没有矿工的角色，也因此不会出现类似比特币和以太坊因为矿工的激励机制带来的价格竞争，只需极低的手续费，适合小额高频交易。
典型项目	闪电网络，RootStock	以太坊，EOS（Region）	IOTA，dagcoin，Byteball

1.安全性增强

小额的交易通过走侧链的方式，可以更好的隐蔽拥有大量存储价值的主账户地址。

2.速度更快

现在比特币/以太坊转账速度已经达到瓶颈，17 年 12 月高峰时比特币主网曾经滞留 20 万笔未确认交易，突破了历史记录。大部分链上转账其实都是小额交易，把这部分交易走到侧链，既可以加快他们的转账速度，又可以减轻主网的压力。

3.智能合约

侧链还可以在锁定主网价值的同时，开发智能合约的功能。如果比特币自身就拥有智能合约，那么现在以太坊等众多公链的存在价值将大大降低，大多数的预言机相关应用都可以回归比特币，促进数字货币在比较统一的框架体系下的发展。

4.扩展应用范围

侧链是以融合的方式实现加密货币金融生态的目标，而不是像其它加密货币一样排斥现有的系统。利用侧链，我们可以轻松的建立各种智能化的金融合约，股票、期货、衍生品等等。你可以有成千上万个锚定到比特币上的侧链。其特性和目的各不相同，所有这些侧链依赖于一种主区块链保障的弹性和稀缺性。在这基础上，侧链技术进一步扩展了区块链技术的应用范围和创新空间，使传统区块链可以支持多种资产类型，以及小微支付、智能合约、安全处理机制、财产注册等，并可以增强区块链的隐私保护。

3.3 侧链/跨链目前的问题

侧链攻击问题

在侧链方案中攻击者只需要破坏最薄弱的侧链，就可以破坏整个网络。一旦他们在某个侧链完成 51%攻击，他们就可以创建一个（假的）最长侧链，用伪造的侧链币

在原比特币块链中换成比特币。问题的本质在于，侧链们不共享同一个公共块历史。这意味着，从一个侧链到另一个侧链转移币的过程中，大部分侧链方案仅仅依赖所谓的“SPV 证明”（译者注：简化交易验证，一种轻量钱包使用的验证机制），它只检查所涉及的币是否来自已知的最长链（而并不追溯币的历史来源至创世区块。这种 SPV 证明运行在轻钱包内部，安全标准远低于比特币网络。而在侧链方案中，一个 51%攻击者不仅可以双花一笔交易，甚至可以凭空制造侧链币。）

合并挖矿带来中心化挖矿

解决侧链攻击问题的一个办法是合并挖矿，以确保所有侧链同时以相同哈希率开采。合并挖矿的情形下，所有侧链使用相同的哈希算法，这样可以在同一时刻为两个侧链生成工作量证明。矿工只需要一次哈希运算就有相同概率完成两个工作量证明。这看上去好像巧妙地化解侧链的缺陷，遗憾的是它没有那么简单。合并挖矿要求矿工运行所有侧链的完整节点，这就会造成中心化挖矿的趋势，这是我们不愿意看到的。此外，如果任意侧链受到 51%攻击，风险依旧存在。

侧链的中心化问题

从用户的角度来看，转账速度、操作顺畅、高可用性是关注的重点。考虑到公有链在区块大小、转账速度、手续费方面的局限性，侧链可以在其上打开一个快速流动的通道。但由此引发的关于中心化/去中心化的社区争论也长期难有定论。

跨链的稳定性有待提高

跨链的意义在于能够不经过中心化的交易所就能直接转换不同公链之间的价值，但其稳定性和转账速度仍然是用户现在使用的最大障碍。

四、 跨链/侧链项目具体分析

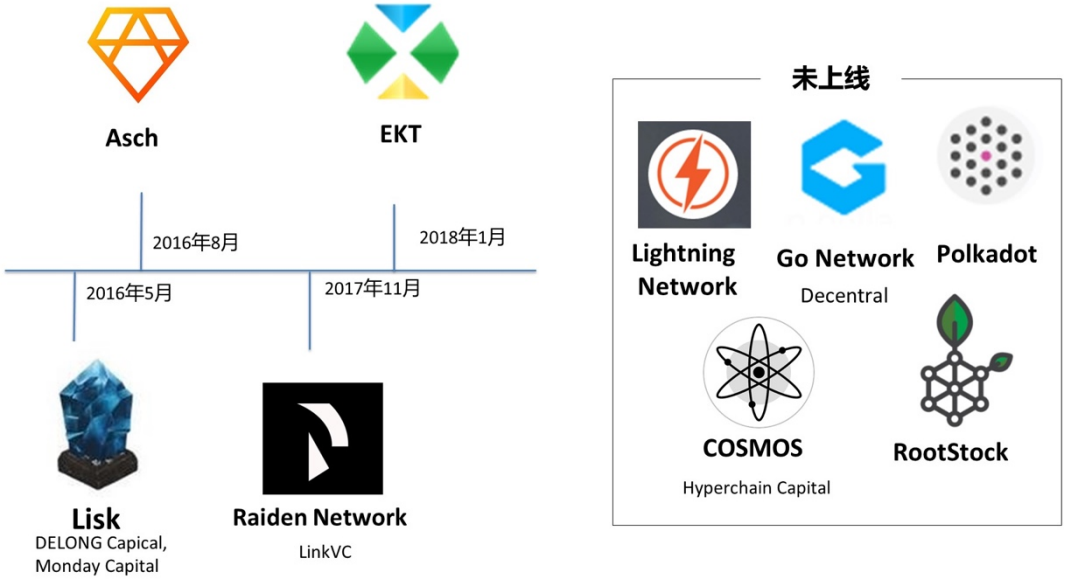
4.1 跨链/侧链项目一览

名称	交易量排名	流通市值（亿）	项目介绍
Lisk（侧链技术）	19	¥80.55	lisk是一个基于node.js与javascript，建立于区块链技术之上的区块链应用平台，开发者可以通过官方提供的sdk，使用javascript语言在lisk平台内开发自己的blockchain app，我们认为，未来必定是中心化应用与去中心化应用共存的时代，lisk提供这么一种简单，易行的方式，让开发者可以很快速的在区块链上建立自己的应用。
EKT（分布式私钥控制+侧链）	45	¥5.83	EKT设计了一套独特的多链架构。在这套多链架构中，除了EKT的主链外支持多条并行的主链，每条主链都会有一个主币。不同的主链可以采取不同的共识机制，不同主链的资产通过EKT的大钱包可以自由的在整个EKT生态中流通。
Asch（侧链技术）	129	¥4.90	Asch是一个去中心化的应用平台，其设计初衷是为了降低开发者的门槛，比如使用javascript作为应用编程语言，支持关系数据库来存储交易数据，使得开发一个dapp与传统的web应用非常相似，相信这对开发者和中小型企业有很大的吸引力，只有开发者的生产力提高了，整个平台的生态才能够更迅速的繁荣起来
RDN（侧链技术）	125	¥4.68	雷电网络（raiden network，代码rdn）是一个链外扩展解决方案，是一个运行在以太坊上基于erc20的代币。雷电网络目前正在运行中，支持即时转账、低成本、可扩展和保护隐私。雷电网络是以太坊区块链上的基础设施层。虽然基本的出发点很简单，但底层协议相当复杂，实现起来也不容易。尽管如此，技术仍可以被抽象出来，使开发人员可以用一个相当简单的api接口来构建基于raiden的可扩展的分散式应用程序
RSK（侧链技术）	未上市	未上市	RootStock是一个建立在比特币区块链上的智能合约分布式平台。它的目标是将复杂的智能合约实施为一个侧链，为核心比特币网络增加价值和功能。RootStock实现了以太坊虚拟机的一个改进版本，它将作为比特币的一个侧链，使用了一种可转换为比特币的代币作为智能合约的“燃料”
Lightning network（哈希锁定）	/	/	Lightning network闪电网络提供了一个可扩展的bitcoin微支付通道网络，它极大提升了比特币网络链外的交易处理能力。交易双方若在区块链上预先设有支付通道，就可以多次、高频、双向地实现快速确认的微支付；双方若无直接的点对点支付通道，只要网络中存在一条连通双方的、由多个支付通道构成的支付路径，闪电网络也可以利用这条支付路径实现资金在双方之间的可靠转移
Go network (哈希锁定）	未上市	未上市	GoNetwork是专门针对移动端以太坊平台上高度可扩容的，转账速度快，低成本，低延时的数字货币平台。
Polkadot（中继技术）	未上市	未上市	Polkadot是由原以太坊主要核心开发者推出的公有链。它旨在解决当今两大阻止区块链技术传播和接受的难题：即时拓展性和延伸性。Polkadot计划将私有链/联盟链融入到公有链的共识网络中，同时又能保有私有链/联盟链的原有的数据隐私和许可使用的特性。它可以将多个区块链互相连接。
COSMOS（中继技术）	未上市	未上市	Cosmos是tendermint团队推出的一个支持跨链交互的异构网络。Cosmos采用的Tendermint共识算法，是一个类似实用拜占庭容错共识引擎，具有高性能、一致性等特点，而且在其严格的分叉责任制保证下，能够防止怀有恶意的参与者做出不当操作。

4.2 重点项目对比分析

	Lisk	EKT	Asch	RDN	RSK	Lighting network
开发阶段	投入使用	还未落地	投入使用	投入使用	还未落地	还未落地
项目目标	致力于降低区块链应用开发门槛，开发者可以用JavaScript来开发区块链应用	致力于降低开发者开发DAPP的门槛，降低DAPP的延迟，为DAPP提供一个良好的运行环境的支持	旨在降低开发人员进入门槛，致力于打造一个易于使用、功能完备、即插即用的系统。	是打造类似以太坊一样的去中心，图灵完备智能合约平台	是专注金融包容性、公共管理透明度和物联网，优化跨行业的过程	建立无需信任对方以及第三方即可实现实时的、海量的交易的平台
共识机制	DPoS	DPoS	DPoS	DPoS	POW结合图灵	DPoS
项目特色	Lisk主链提供了稳定性和安全性，而侧链则被用来具有无限的灵活性。Lisk为开发者提供了一个完全控制的环境来创建他们自己的区块链网络，简单的入口让人们快速实现从创意到产品，不必从头开始创建区块链网络。开发者可以完全实现和定制他们的区块链应用程序。	把Token和Dapp分开，token链多链多共识，DAPP的共识机制可以实现大部分事件的秒级确认和执行，可以做到与传统互联网的延迟没有特别大的差异。	Asch提供了一套完整的开发者平台、主链及SDK。Asch引入了新的PBFT（实用拜占庭容错）机制，在对节点控制力上有提升	增强了Ethereum的可扩展性，Raiden网络承诺每秒吞吐量达到100万次，将是质的突破。	是首个由比特币网络担保的通用智能合约平台，它将一个图灵完备虚拟机合并到比特币中，并增加了网络的性能，如更快的事物处理能力和更好的扩展性	支付速度快，无需在拥堵的主链上等待自己的交易确认；使用闪电网络的交易是在链下执行的，只需要很少的交易费用；交易效率高，无需受区块容量和记账速度的限制。TPS可达百万甚至千万级。
工作流程	开发者可以基于自己的区块链网络和LSK代币，部署链接到Lisk网络上自己的侧链，在一个平台上完成从设计、开发、发布和货币化的所有步骤。	提供发行token和链的支持，用户可以根据自己的需求选择不同的共识机制。同时对于想要开发DAPP的用户，可以使用EKT提供的SDK开发，每个DAPP都是独立的一条链，不同DAPP之间互相隔离且共享用户。	Asch平台提供的服务包括一个公有链和一套应用SDK。这个公有链为主链，使用Asch应用SDK可以开发出拥有独立不可篡改账本的区块链应用，也叫做侧链应用	在以太坊上建有一个智能合约，双方需要在以太坊区块链上开设通道并各自锁定以太。这步动作可通过向雷电智能合约发送一条双方签名认可的报文来实现。报文中的关键信息包括：双方公钥、双方锁定资产数量、双方签名。	当BTC转换到RSK上时，锁定部分比特币在比特币区块链上，同时在RSK上释放等量的代币。当需从RSK换回比特币时，再次在RSK上锁定代币，同时在比特币区块链上释放等量的比特币，通过安全协议保证相同的比特币不会在两条区块链上同时释放	序列到期可撤销合约RSMC解决了链下交易的确认问题和哈希时间锁定合约HTLC解决了支付通道的问题
技术模式	Lisk是去中心化的网络，有自己的区块链，用于帮助开发者创建各种各样的自定义侧链	token链的多链架构提供了互相隔离但是共享用户的功能，不同链的资产可以自由的在整个生态中流通，是一个高TPS的方案。提供了与传统互联网类似的编程语言，可以帮助开发者开发复杂的DAPP。	应用SDK内置了跨链协议，通过该协议可以与主链进行资产互通，也就是说主链承担了资产路由的功能，通过资产路由，各个应用之间可以实现多种资产的流转。阿希的生态体系包含多条链，每个链可以承载多个代币或资产，每个代币或资产也可以转入多条链上	提供了一个可扩展的bitcoin微支付通道网络，它极大提升了比特币网络链外的交易处理能力	与BTC双向挂钩，当BTC转移到RSK中，BTC会被锁定在比特币区块链协议中，并且同样数量的RTC在RSK中解锁。	基于微支付通道（双向支付通道）演进而来，在比特币主链以外再架设一个通道，让用户的货币（数字货币）在这个通道上可以进行快速支付

4.3 项目的投资明细



五、 跨链侧链的投资逻辑

1．项目技术的创新性

跨链技术虽然被大众所熟知，但目前还没有社区普遍承认和使用的项目，因此不算是成熟的技术。在稳定性和安全性上还不能和传统的公链技术相媲美，尤其是跨链侧链从技术上讲较难实现，很多提出利用跨链侧链解决的项目和应用目前很少有落地，因此现有的区块链跨链项目的团队技术经验还有许多不足之处。

2．与同类项目进行对比有明显的优势点

虽然已经落地的项目不多，但我们可以看出，采用跨链侧链技术的项目大体都是相同的机制，那么使项目脱颖而出的关键是在于其性能和项目进展程度，能在短时间内开发出实际高可用性的跨链，将是以后跨链项目市场的主宰。

3．技术上实现的可能性

分析项目的关键主要是去看其技术实现的可行性。跨链技术的实现需要很多机制和合约的制约和保障，能够保证项目在跨链技术下稳定运行是成为一个值得投资项目的关键。

4．经济激励模型的设计

仔细考察期经济激励模型，是否足以支撑初期社区冷启动，并在后期形成正反馈生态。

5．社群运营能力

长期看来，团队是否有社区运营能力，并能否通过社区形成网络效应，进而提高项目性能。

6．服务质量是否能达到商业级别

存储的可靠性，可用性，最终都需要经过市场的检验。目前大部分跨链项目和应用离商业可用性还有很大距离，怎样解决区块链之间在一个统一的标准下通过跨链相互联系的问题，如何制定合理的智能合约。如果能在这些方面设计出比较好的解决方案，即能成为这个行业里具有强竞争力的项目。

六、 跨链侧链的未来展望

1. 交易速度加快，主链分担减轻

所有的交易记录都被锁定在主链上，而各种区块链应用的代码和数据都可以独立保存在侧链中，这样就可以分担主链上的交易，使交易在侧链上完成并发生转移，主链不容易产生交易拥堵，从而提升了交易速度。

2. 多条侧链并行处理，实现完全去中心化交易

主链可以通过智能合约链接多条侧链，可以实现数据去中心化并且并行处理，这样一来，不单单是速度提升的方面使项目性能提升，交易数据可以完全实现去中心化，也实现了区块链之间的搭建，区块之间不再是独立的个体，而是真正实现了数据在分块之后依然是可联系的。

3. 安全性得到保障

万一侧链出现代码漏洞，主链不会受到影响，而因为去中心化的机制，部分数据的丢失对整体并无影响，交易记录一旦发生就被锁定在链上，用户不用担心丢失或篡改等问题。

4. 扩展空间，增强隐私保护

跨链侧链技术的引入进一步扩展了区块链技术的应用范围和创新空间，使传统区块链可以支持多种资产类型，以及小微支付、智能合约、安全处理机制、财产注册等，并可以增强区块链的隐私保护。

总体而言，在这场区块链大浪潮下，侧链与跨链作为提高区块链性能的重要手段，一直受到核心开发者的重视。无论是作为技术研究还是投资的角度，跨链侧链的发展都是值得进一步的关注和研究。