侧链技术研究报告

2018 年 9 月 -> 10 月

TokenClub 研究院

目录

1. 行业综述

侧链协议是一种跨区块链的解决方案。通过这种解决方案，可以实现数字资产从一个区块链到另一个区块链的转移，之后又可以从第二个区块链返回到前一个区块链中。其中第一个区块链被称为主链，第二个区块链则被称为侧链。最初，主链通常指的是比特币区块链，而现在主链可以是任何区块链。侧链协议被设想为一种允许数字资产在主链与侧链之间进行转移的方式，这种技术为开发区块链技术的新型应用和实验打开了一扇大门。

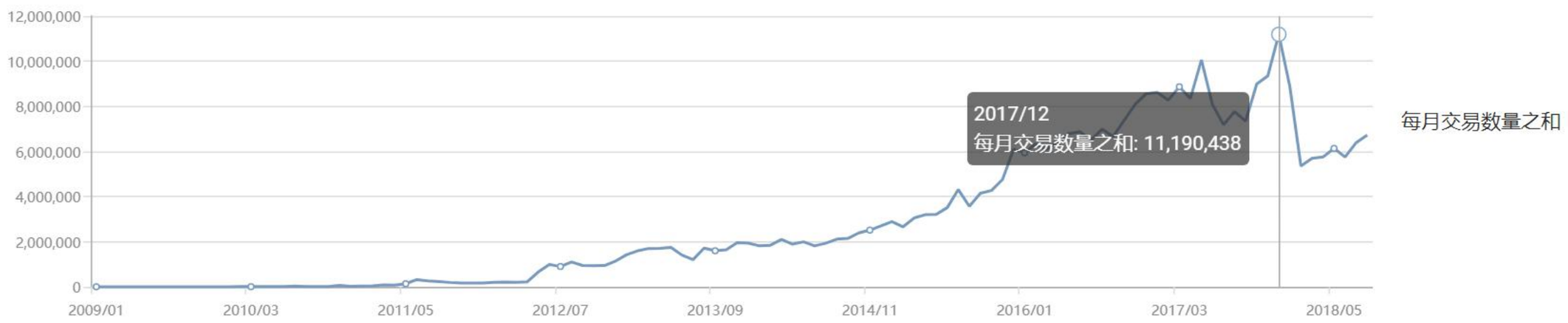
1.1 行业背景

比特币诞生至今已有十个年头，从最早期极客们相互转账的玩物，到现在演变成了千万用户的庞大生态。区块链技术也从最初的 1.0 向着 3.0 的概念演进，从最简单的点对点支付、到智能合约的部署应用，从数字资产的发行向着全行业包括存储、游戏、物联网、人工智能等领域广泛铺设。为满足行业的需求，越来越多的技术构想被应用到了区块链的场景中，侧链、跨链、DAG、分片等技术也发挥了他们重要的价值。

1.1.1 区块链发展的瓶颈

比特币发展至今，交易量呈一个线性增长的态势，从最初几乎无人使用到 2017 年 12 月份全网发生了一千万笔交易。伴随着交易量的激增，币价也达到了几百万倍的涨幅，这其中的关联性可以用梅特卡夫定律做一个很好的总结：**网络的价**

值等于网络节点数的平方，网络的价值与联网的用户数的平方成正比。



也就是说，对于像比特币这样的网络，其价值的增长不在于人们凭借信仰的加持，而在于用户人数（活跃地址数）与使用频率（交易数量）的增加。但是作为一条去中心化的网络，公链的性能也制约着比特币使用频率增长，为了保证去中心化程度主链目前只能承受每秒不到 7 笔的交易，倘若大量的交易在同一时间段内发生，主网就会陷入拥堵。

高度	播报方	大小(B)	块收益	时间
543,574	F2Pool	485,354	12.57188735 BTC	1 分钟前
543,573	SlushPool	572,766	12.61248207 BTC	8 分钟前
543,572	SlushPool	1,041,895	12.53058250 BTC	14 分钟前
543,571	AntPool	1,171,787	12.80940490 BTC	15 分钟前
543,570	unknown	1,175,908	12.79511998 BTC	45 分钟前
543,569	BTC.TOP	922,901	12.61559903 BTC	1 小时 02 分钟前
543,568	unknown	1,205,474	12.56723346 BTC	1 小时 08 分钟前
543,567	BTC.TOP	1,256,274	12.97159380 BTC	1 小时 11 分钟前
543,566	BTC.com	197,606	12.52469083 BTC	1 小时 52 分钟前
543,565	F2Pool	1,222,185	12.68062967 BTC	1 小时 52 分钟前

即便相较于牛市，目前比特币网络的拥堵状况有所减缓，但还是时不时会出现一些拥堵的状况。根据最近的 10 个区块信息来看，仍然有五个区块无法打包全部的交易信息，比特币的平均确认时间是 10 分钟，也就是说有部分交易需要等到下一个区块才能被打包。到了牛市顶峰，一笔交易需要几天后才能被打包，而若要快速网络确认，需要付出上千元的矿工费成本。如下图，在牛市的期间，比特币的矿工费随着交易量激增水涨船高：

除此之外，以太坊网络也面临着同样的问题，因为除了 ETH 的转账之外，区块链上还记录着成百上千的代币交易信息。在以太坊上运行着的大量 DAPP，譬如加密猫、Fomo3D，除了会弄堵以太坊网络，也会因为拥堵的网络制约着项目本身的发展。

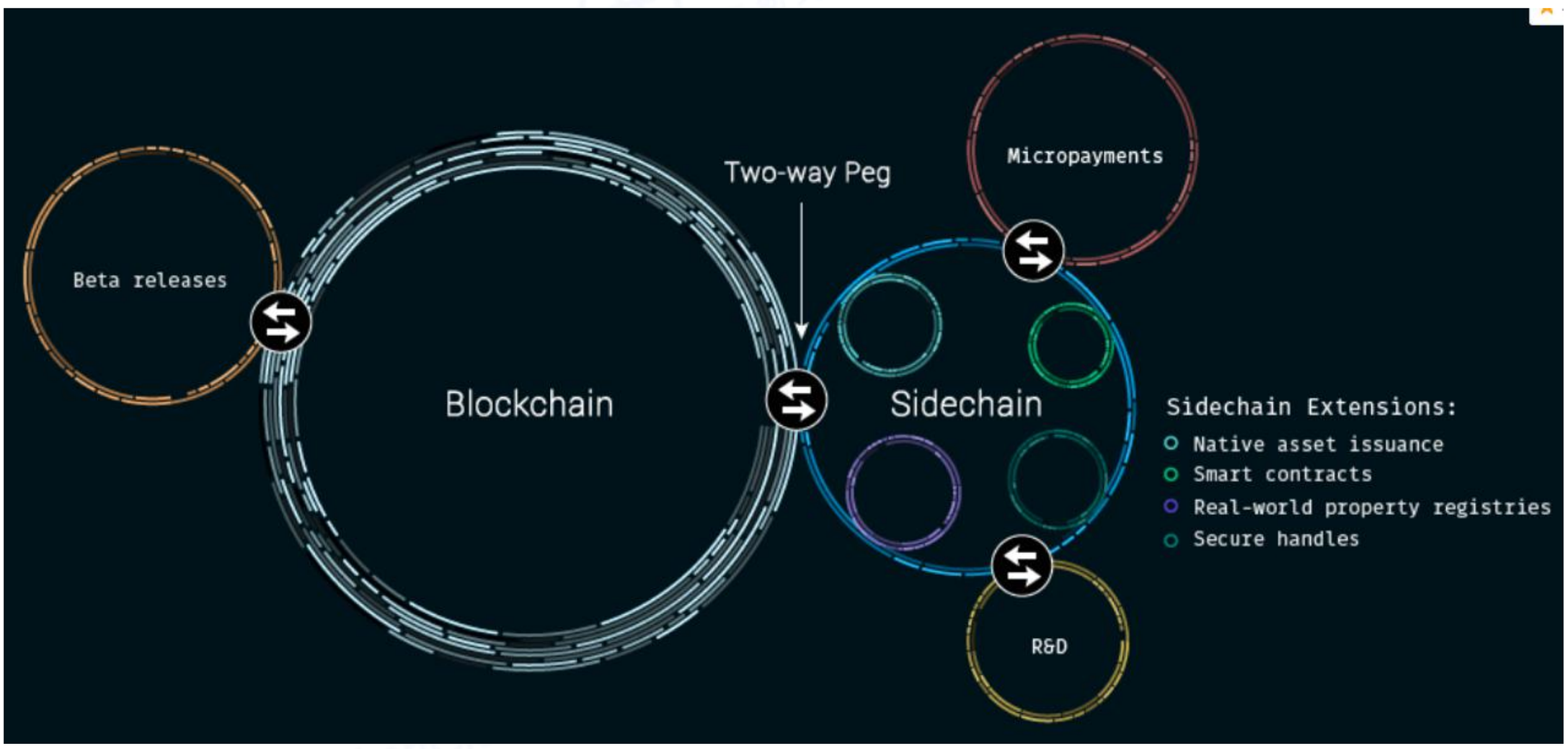
因此，社区的参与者提出在主链进行扩容之外，还提出了通过搭建第二层网络即侧链技术来解决主链的拥堵问题。

1.1.2 侧链概念的诞生

在 2012 年前后，比特币聊天室首次出现了关于侧链的对话，当时比特币核心的开发者们正在考虑如何安全地升级比特币的协议。其中的一个想法是进行单向锚

定技术“one-way peg”，即用户可以将比特币移动到一个单独的区块链来测试一个新客户端；然而，一旦这些资产被转移走，它们就不能在被转移回主链上去了。

在此后的一年的事件内，在比特币 IRC 的频道上，比特币核心开发者 Greg Maxwell 提出了一种“two-way peg(双向锚定)”的想法，即价值可以转移到另一个链上，然后再回到原先的比特币链上。在当时，一个双向锚定的技术又引起了另一个日益增加的担忧，即其他的币种，像是莱特币和域名币，正变得越来越流行。人们担心的是这些“山寨币”会稀释比特币的价值。比特币的核心开发者认为，把比特币作为一种储备货币，并将新功能转移到侧链上，这是有道理的。



为了将侧链的概念变成现实，在 2014 年，Back 与 Maxwell 和其他一些比特币核心开发者一起组建了 Blockstream。作为著名的区块链技术公司，Blockstream 的代表作就是用于解决比特币网络拥堵的第二层解决方案——闪电网络。

1.2 技术对比

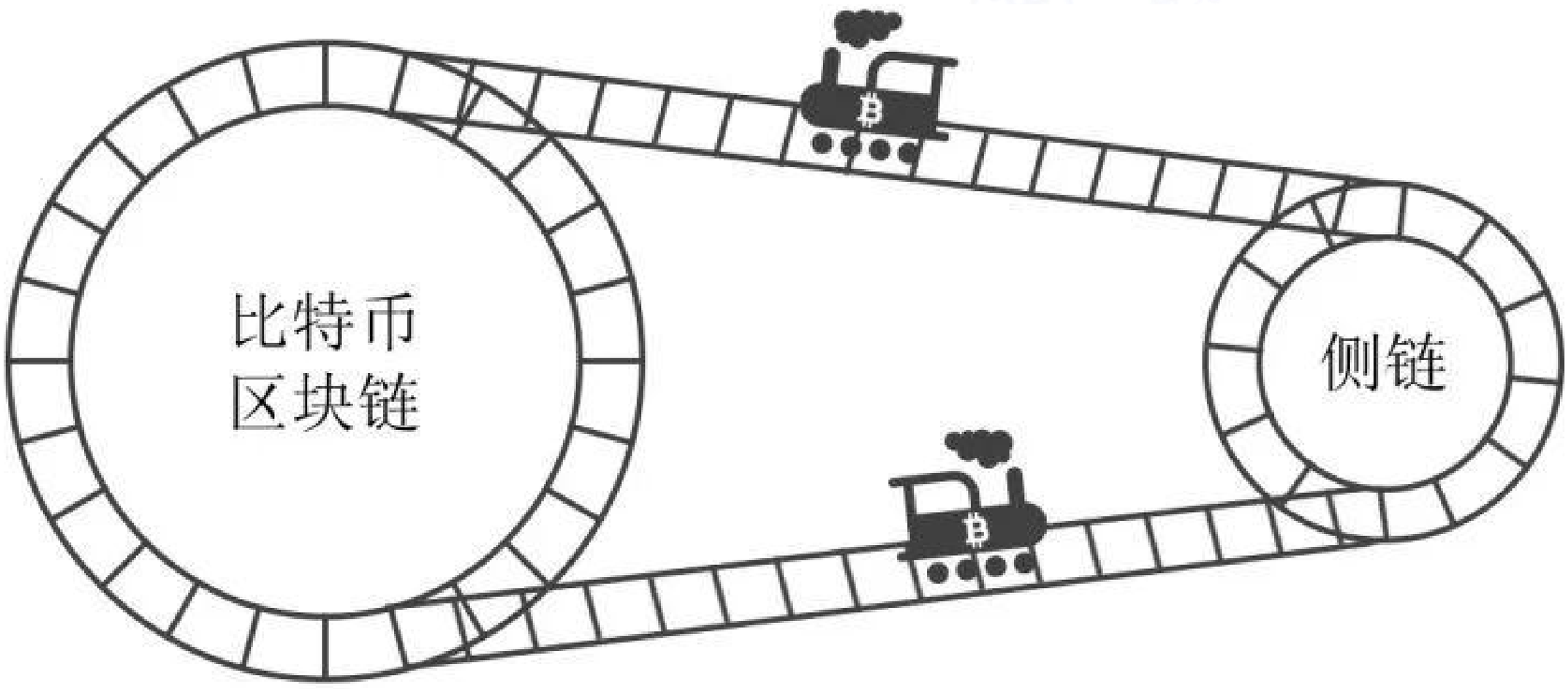
侧链技术只是优化区块链性能的一种解决方案，相比于其他技术有其一定的优势与不足。

1.2.1 主链与侧链

区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了若干网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块，对于普通用户来说它就像一个公有账本，记载所有的交易记录，对于开发者来说可以理解为一个分布式的数据库。区块链这个数据库的特点是去中心化、开放、自治、不可篡改，区块链与去中心化应用息息相关，非常适合为去中心化应用提供存储功能。

侧链是一种特殊的区块链。它使用一种叫做“SPV 楔入”的技术实现与其他区块链之间的资产转移，这使得用户能用已有的资产来使用新的加密货币系统。人们不必再担心比特币难于采纳创新和适应新需求，只要创造一个侧链，然后对接到比特币的区块链中即可，通过继承和复用比特币强大的区块链，还避免了新货币的流动性短缺和市场波动等问题。并且由于侧链是一个独立的、隔离的系统，侧链中出现的严重问题只会影响侧链本身，这极大地降低了创新的风险和成本。

通俗来说，主链可以理解为正式上线的、独立的区块链网络；而侧链则不然。它不会特指某个区块链，是遵守侧链协议的所有区块链的统称。



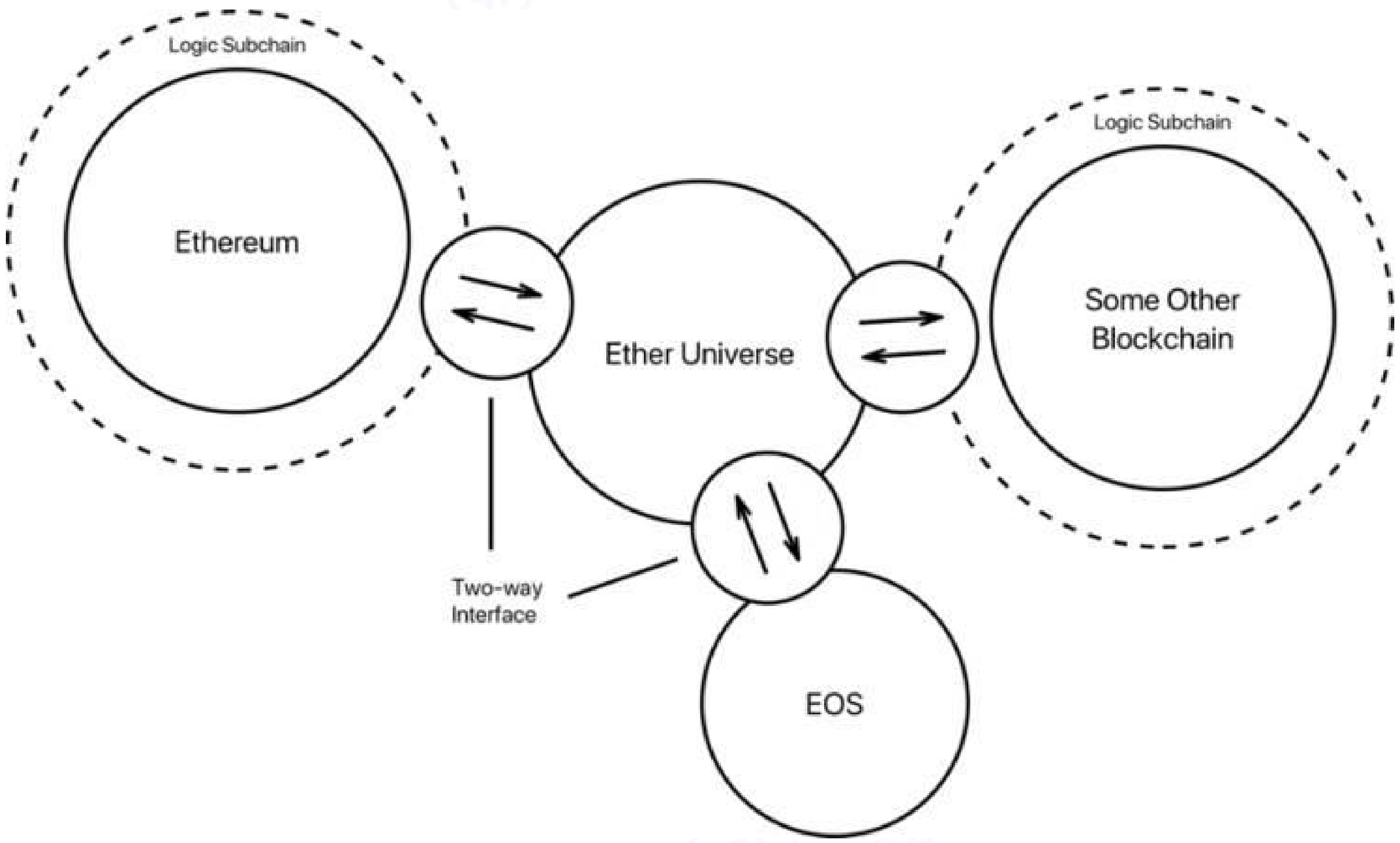
侧链旨在实现双向锚定，让某种加密货币在主链以及侧链之间互相“转移”。以比特币为例：通过侧链技术，比特币可从主链“转移”到其他区块链之上，并在“转移”后的区块链上使用，同时还能安全“返回”主链；整个过程比特币保持着相同的价值。所以说，侧链的概念是相对主链而言的；只要符合侧链协议，所有现存的区块链，如以太坊、莱特币、Zcash 等等都可成为侧链。

另一方面，由于侧链本是独立的区块链，有自己的节点网络，代码以及数据也是相对独立的；所以它在运行过程中不会增加主链的负担，避免数据过度膨胀的情况出现。不过侧链技术较为复杂，需要支持可被后期重组证明失败交易的脚本以及足够多的运行节点，来确保其安全性。

在主链上部署侧链技术，就意味着用户可以使用他们已有的资产访问新的加密货币系统，从而实现在主链上无法达到的操作目的。举个例子，使用 RootStock 技术将能让比特币通过智能合约技术进行更为复杂的交易操作，如微支付。与此同时，加密货币还可通过在主链以及侧链上的双向流通，来扩大其应用范围。

1.2.2 侧链与跨链

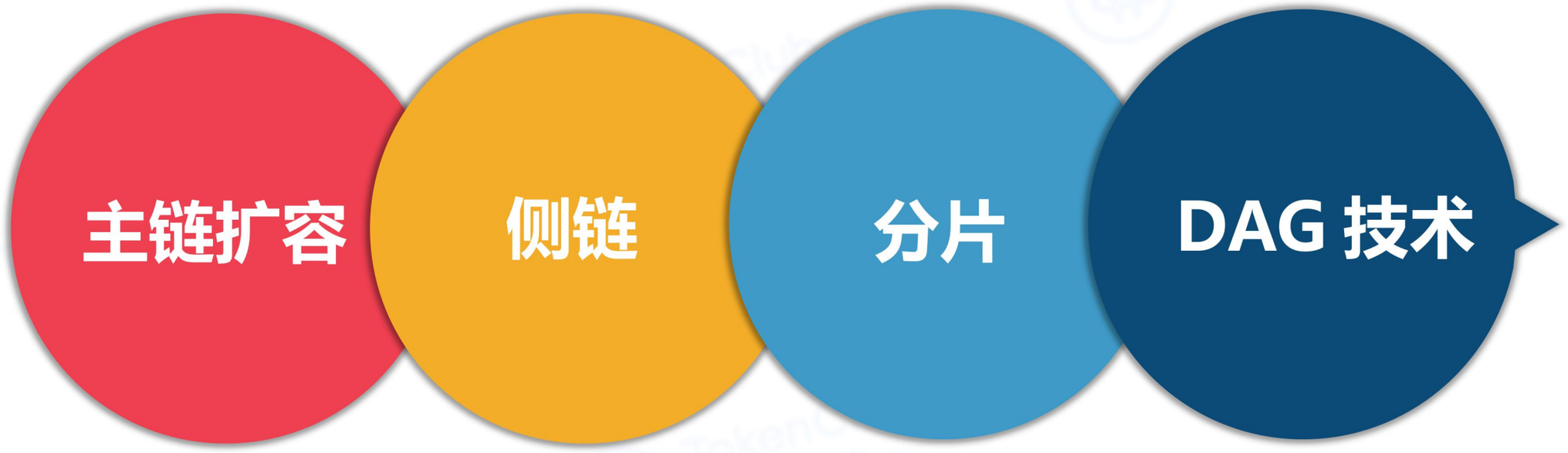
通常说侧链服务于主链，而跨链志在打通链与链之间价值和功能的连通。因此，侧链与跨链，在技术内容上大体相似，同一条链既可以做侧链也可以承担跨链的功能，比如阿希链，只在谈到他们所服务的对象时才需要做细致的区分。



相比于侧链，跨链的范围更为广泛，它可以使两条链上的不同数字资产通过信用机制可以相互转换，打通链与链之间的价值流通。跨链技术中，两条链之间不再是主从关系，而是相对等的关系，也因此跨链的应用场景比侧链更为丰富。

1.2.3 扩容技术对比

为了解决区块链网络延展性的问题，目前主要有以下几种技术方案：



1.2.3.1 主链扩容

主链扩容的方式是通过直接增加区块大小来实现的。为了解决比特币网络的拥堵问题，关于扩容的方式一直争议不下，以大矿工为代表的主链扩容派在 2017 年 8 月 1 日硬分叉出了 8M 区块大小的 BCH，结束了这场扩容的纷争。

下图是开发者制作的针对 BTC&BCH 实时交易的可视化网站，将区块大小比作搭载乘客的大巴车，BTC 只有一辆大巴，通过旁边的隔离见证可以缩减交易大小，而相应的 BCH 有 32 辆大巴，通常我们会看到 BTC 那边会发生交易拥堵，而扩大了区块容量的 BCH 则不会发生。

主链扩容的优势在于简单粗暴，技术含量较低施行周期短；另外还可以保证主链的健壮，让更多的用户去使用主链，增加主链手续费从而保证矿工的收入，有利于维护网络安全。主链扩容的问题在于对节点服务器的性能要求过高，增加小矿工搭建节点的成本，不利于交易信息的同步，最终导致节点减少，去中心化程度降低。**代表项目：BCH**

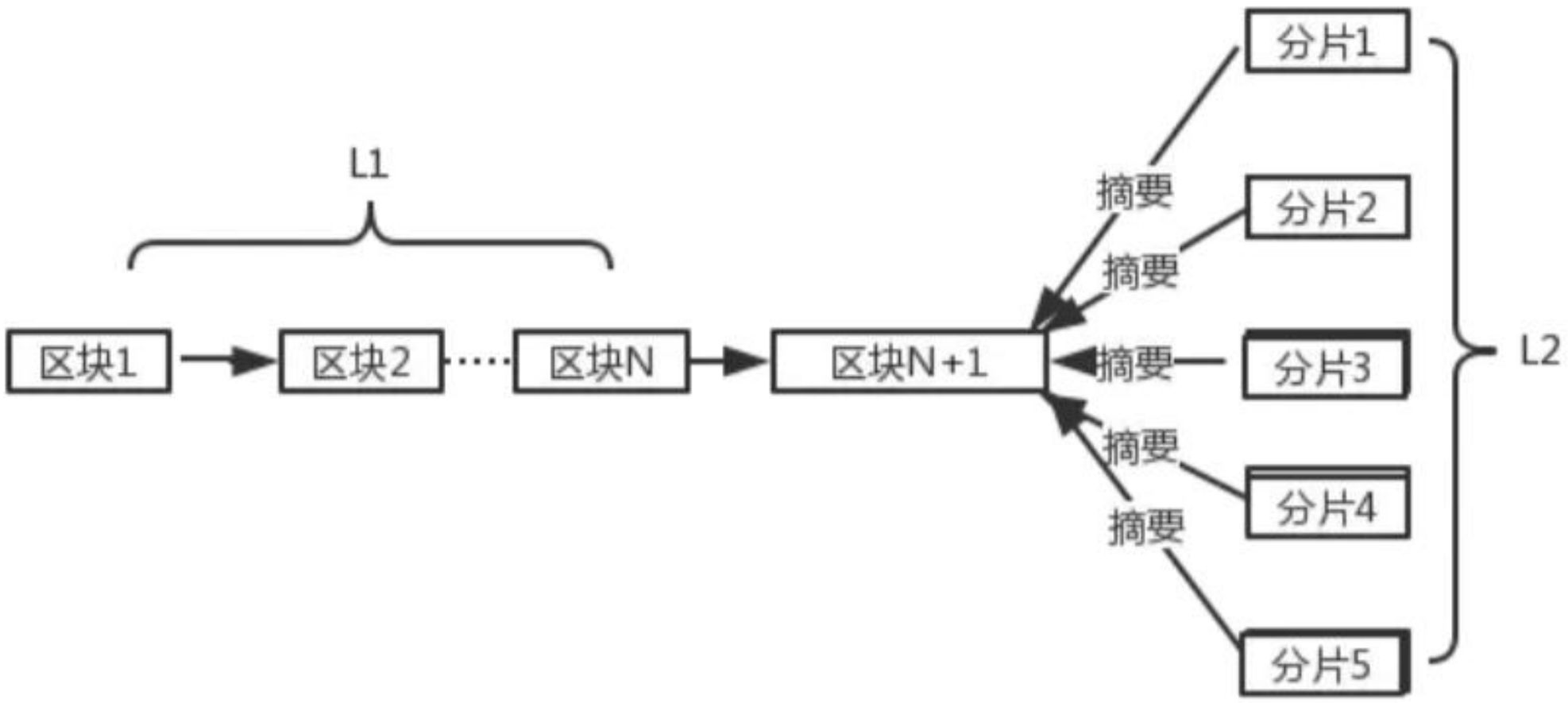
1.2.3.2 侧链扩容

侧链扩容是通过双向锚定的方式搭建了第二层网络，将比特币从主链“转移”到另一条链上去使用。

侧链扩容的优势在于搭建第二层网络，不需要修改主链的底层（闪电网络增加了隔离见证，是个例外），因此保证了主链的去中心化。其缺陷在于，技术进展周期比较长，目前比特币两条知名的侧链闪电网络与 RSK 都处于测试阶段，对主链拥堵的解决效果尚未可知。另外，侧链扩容是建立在牺牲矿工手续费基础之上的，未来比特币区块奖励减少容易影响网络安全。**代表项目：闪电网络、RSK、RDN**

1.2.3.3 分片技术

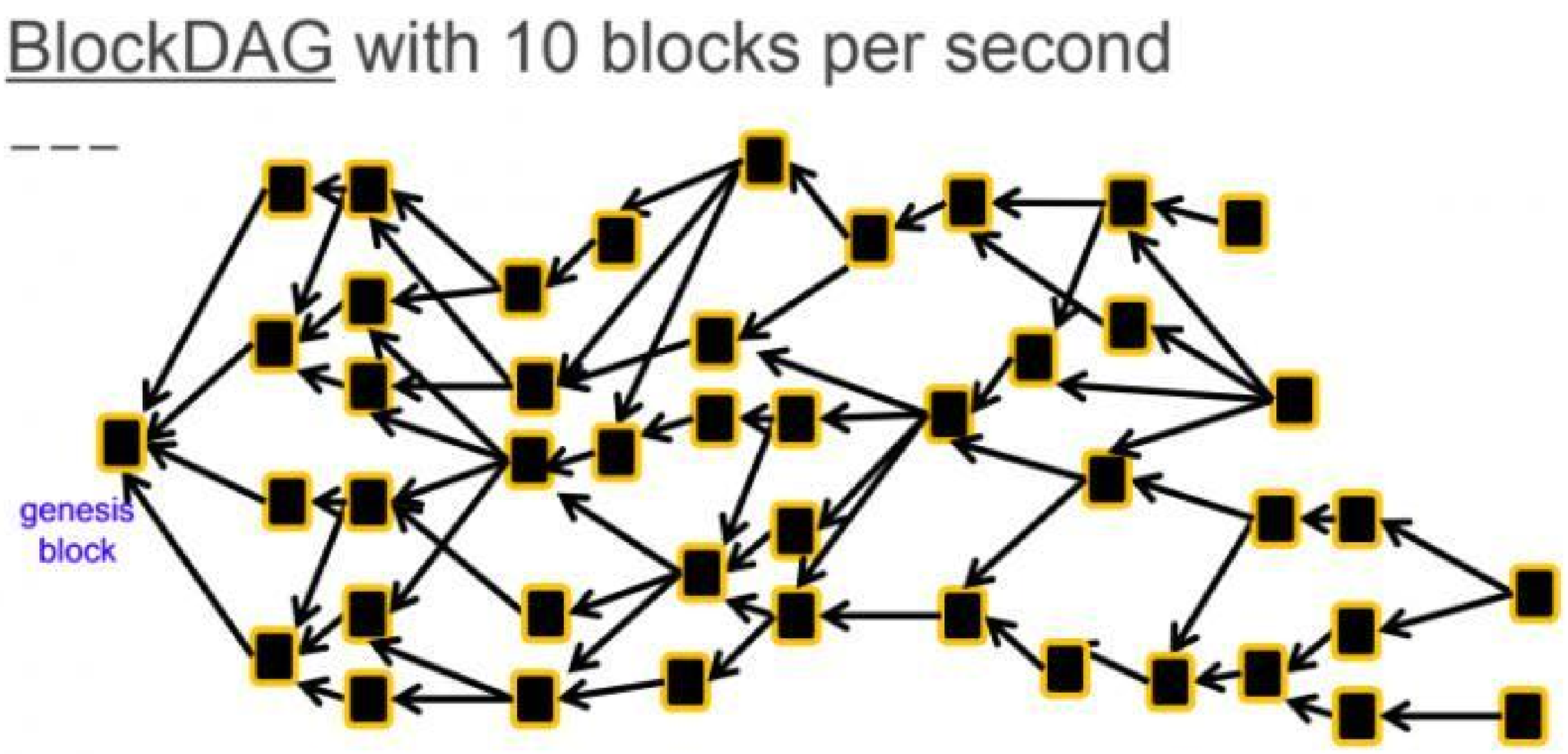
分片技术是一种基于数据库分片传统概念的扩容技术，它将数据库分割成多个碎片并将这些碎片放置在不同的服务器上。在公共区块链的情境中，网络上的交易将被分成不同的碎片，其由网络上的不同节点组成。因此，每个节点只需处理一小部分传入的交易，并且通过与网络上的其他节点并行处理就能完成大量的验证工作。将网络分割为碎片会使得更多的交易同时被处理和验证。因此，随着网络的增长，区块链处理越来越多的交易将成为可能。这种属性也称为水平扩容。



分片技术的缺陷在于过于复杂，目前仍处于探索中，正式施行需要一定的时间，另外过分的追求 TPS 也一定程度上影响到了网络的安全。**代表项目：ETH、ZIL**

1.2.3.4 DAG 技术

Directed Acyclic Graph，中文译为“有向无环图”，是计算机领域常用的一个数据结构。



DAG 技术摒弃了区块链的概念，它使交易进入全网中，并把交易确认的环境直接下放给交易本身，无需矿工打包成区块后同意交易顺序。因此，DAG 技术的交易速度比区块链要快很多，手续费低适合小额高频交易。但是 DAG 也存在一些问题，网络数据增加、影子链攻击、智能合约开发难度大以及网络安全性都难以协调。**代表项目：IOTA、NANO、GBYTE**

目前各种扩容技术都无法尽全尽美，或许将主链适度扩容并且通过侧链网络来缓解主链压力会是扩容的一个最佳方案。

2. 侧链概述

侧链本质上是一种跨区块链解决方案，通俗来说，就是将一条链上的资产通过技术手段“迁移”到另一条链上。以闪电网络为例，我们可以在比特币区块链上点对点的发送 BTC，也可以选择将 BTC 锁定映射到闪电网络中，在闪电网络中进行交易。这里交易的是闪电网络中的代币，可以把它简称 LNBTC，可以更快速、低成本的进行交易，关闭闪电网络通道后可以在主链上获取相应数量的 BTC。

侧链技术通常具有以下特点：

- 主链币通常通过双向锚定技术锚定侧链币，采用 1:1 的比例或者其他预定汇率。
- 侧链自己不能产出主币，只能接受主链的输入，并在自己链上生成对应的侧链币。
- 侧链需要足够的算力和共识保证侧链的安全。
- 侧链独立于主链存在，侧链上发生的任何事情都不会影响主链，从而可以保证主链安全性。

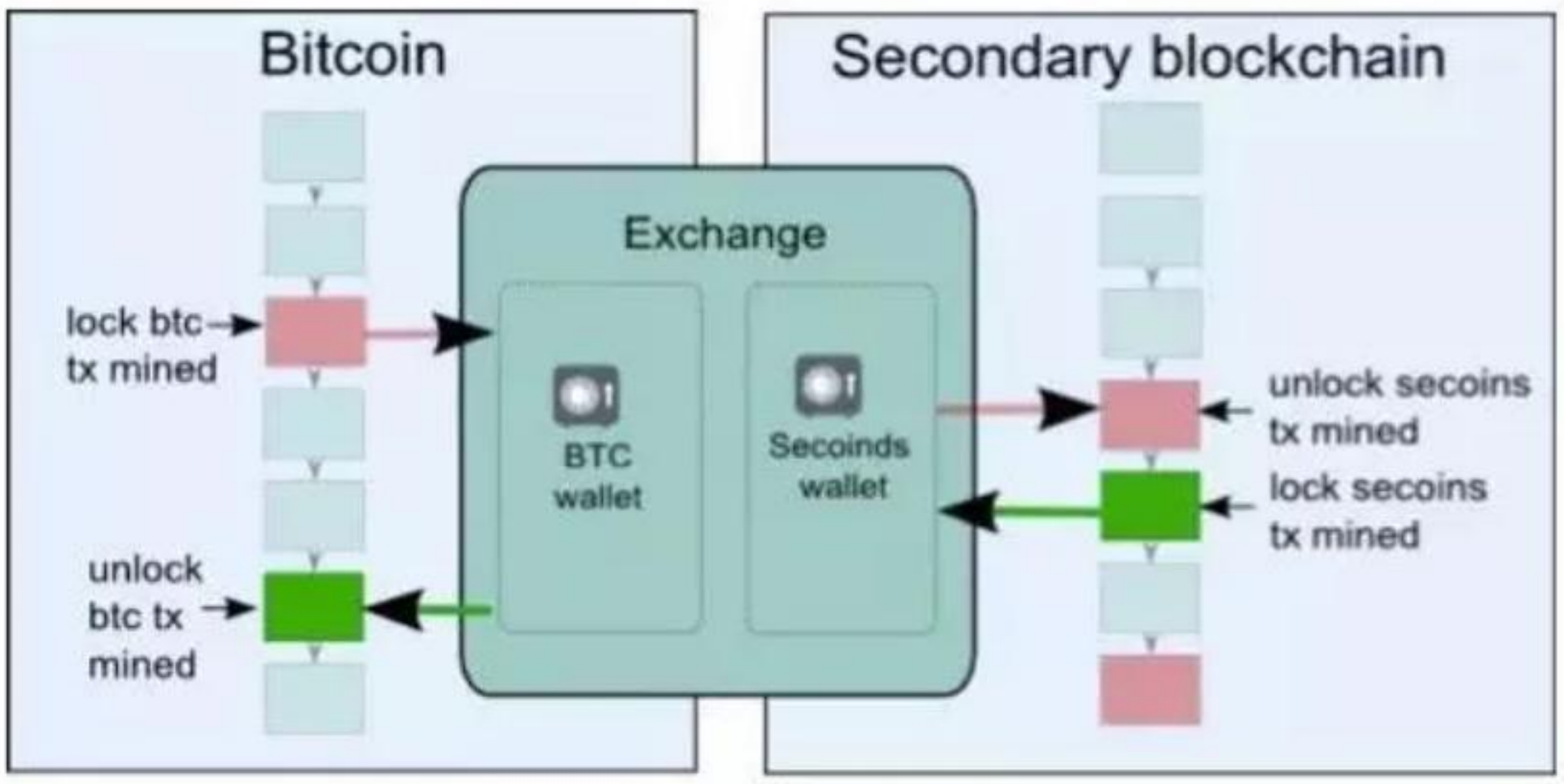
根据定义只要实现了侧链协议就可以认为是侧链，那么其实任何链都可以成为别的链的侧链。

2.1 侧链技术原理

实现侧链的技术有很多，目前大多是通过双向锚定的方式进行，当然也有单向锚定的方式去搭建侧链。二者的区别在于单向锚定往往是有去无回，将比特币移动到一个单独的区块链中，这部分资产将再也无法返回；而双向锚定技术可以使比特币移动到新的区块链中，也可以再次返回到比特币上。实现这些原理的技术主要有以下几点：

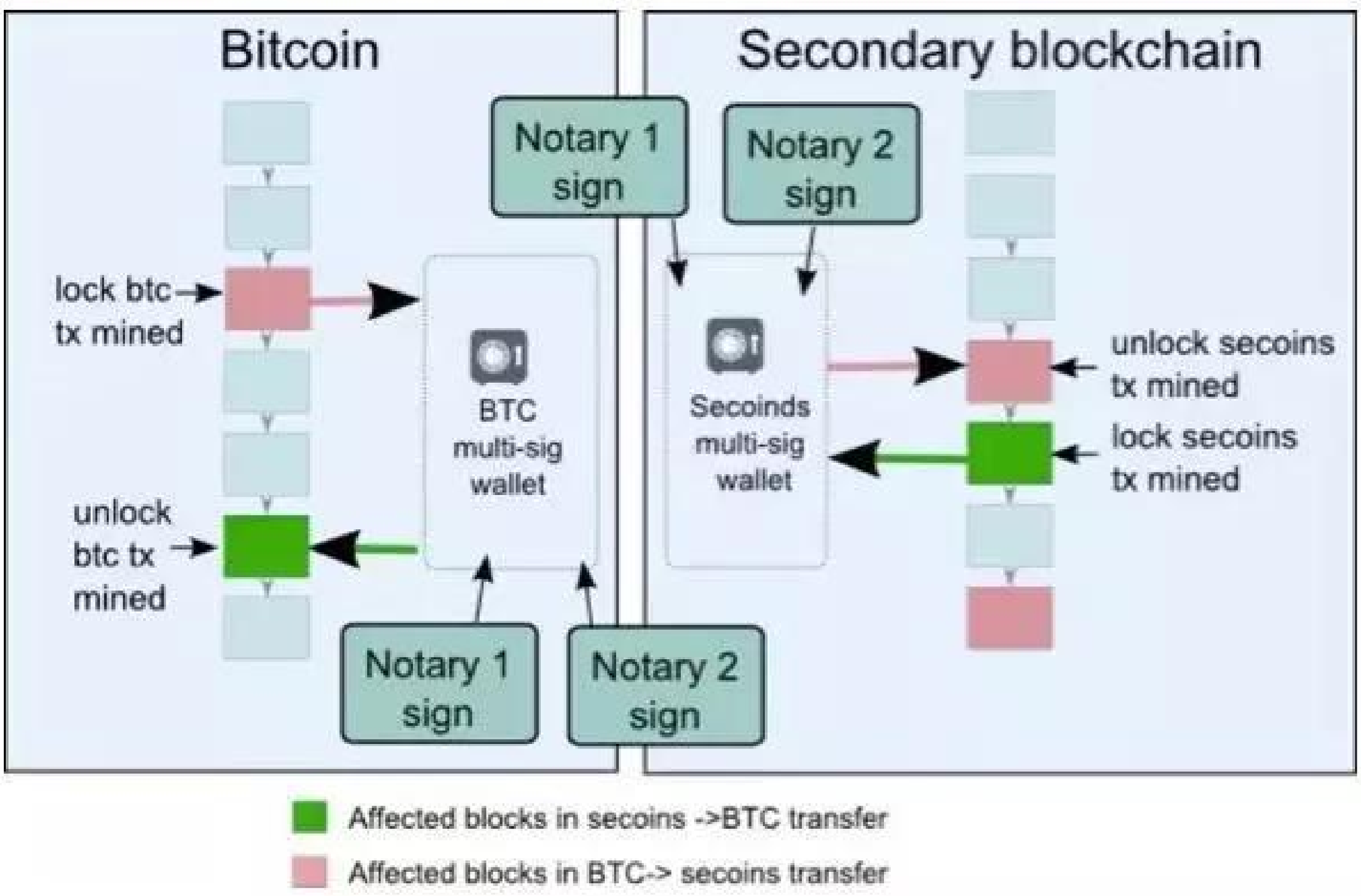
2.1.1 单一托管模式

最简单的实现主链与侧链双向锚定的方法就是通过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。这个解决方案的最大问题是过于中心化。单一托管模式的原理如下图所示：



2.1.2 联盟模式

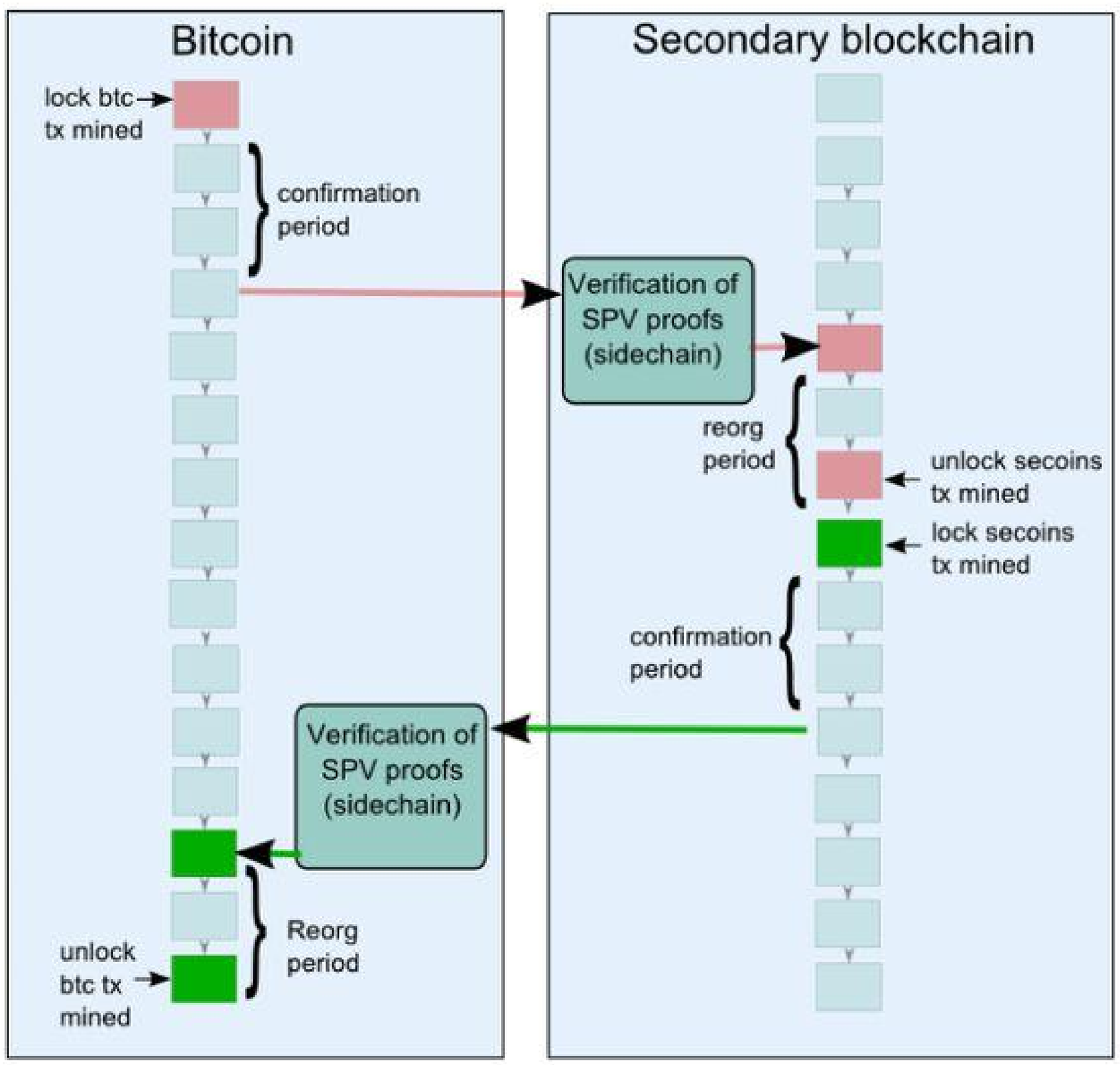
联盟模式是使用公证人联盟来取代单一的保管方，利用公证人联盟的多重签名对侧链的数字资产流动进行确认。在这种模式中，如果要想盗窃主链上冻结的数字资产就需要突破更多的机构，但是侧链安全仍然取决于公证人联盟的诚实度。联盟模式的原理如下图所示：



单一托管模式与联盟模式的最大优点是它们不需要对现有的比特币协议进行任何的改变。

2.1.3 SPV 模式

SPV（Simplified Payment Verification）模式是最初的侧链白皮书《Enabling Blockchain Innovations with Pegged Sidechains》中的去中心化双向锚定技术最初设想。SPV 是一种用于证明交易存在的方法，通过少量数据就可以验证某个特定区块中交易是否存在。



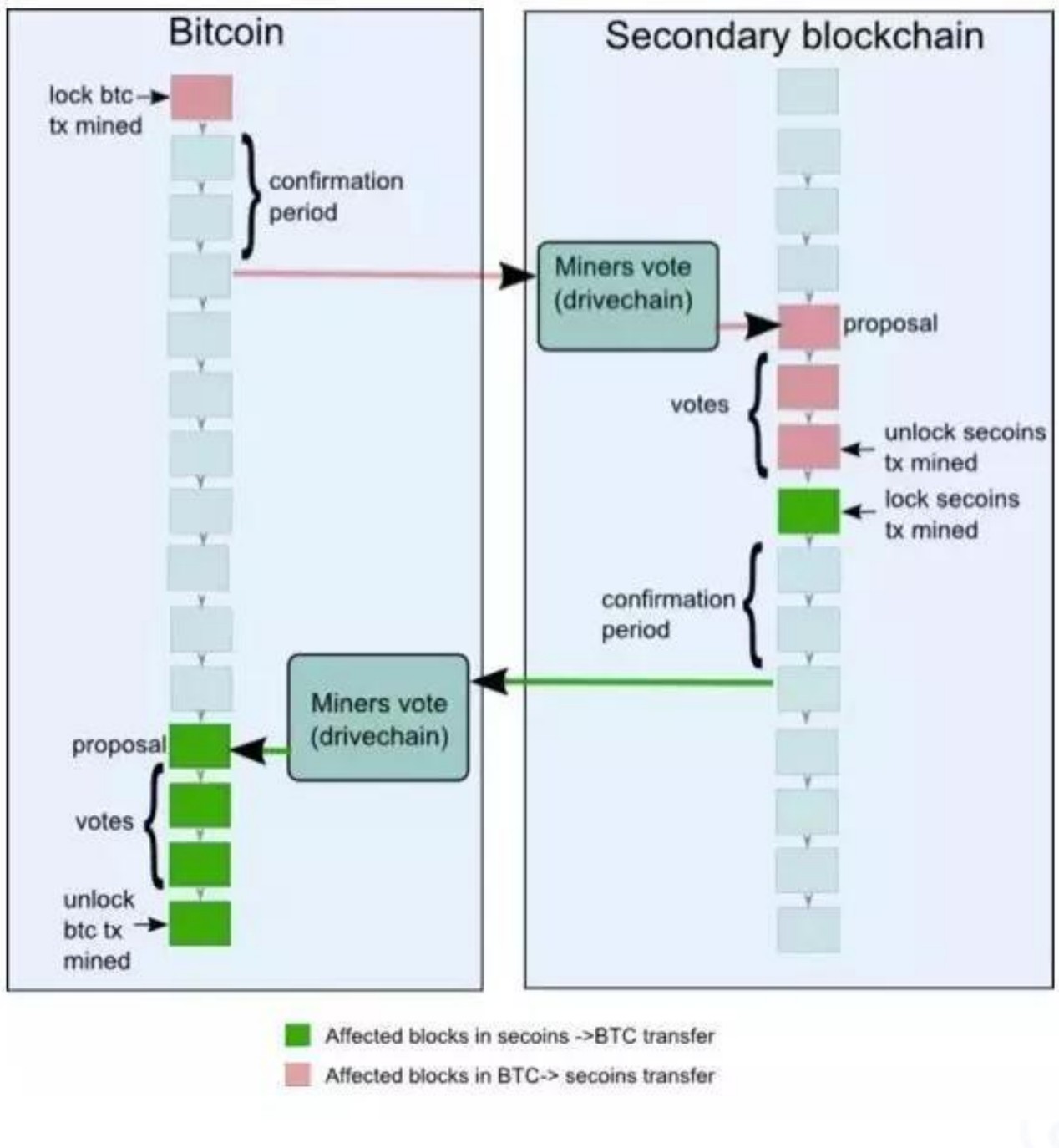
如上图所示，在 SPV 模式中，用户在主链上将数字资产发送到主链的一个特殊的地址，这样做会锁定主链的数字资产，该输出仍然会被锁定在可能的竞争期间内，

以确认相应的交易已经完成，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，然后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。

SPV 模式存在的问题是需要对主链进行软分叉。

2.1.4 驱动链模式

驱动链概念是由 Bitcoin Hivemind 创始人 Paul Sztorc 提出的。在驱动链中，矿工作为“算法代理监护人”，对侧链当前的状态进行检测。换句话说，矿工本质上就是资金托管方，驱动链将被锁定数字资产的监管权发放到数字资产矿工手上，并且允许矿工们投票何时解锁数字资产和将解锁的数字资产发送到何处。矿工观察侧链的状态，当他们收到来自侧链的要求时，他们会执行协调协议以确保他们对要求的真实性达成一致。诚实矿工在驱动链中的参与程度越高，整体系统安全性也就越大。如同 SPV 侧链一样，驱动链也需要对主链进行软分叉。驱动链模式的原理如下图所示：



2.1.5 燃烧证明

燃烧证明（Proof-of-Burn）机制主要应用于单向锚定的区块链中，即持有比特币的用户可以将比特币发送到一个专门的没有私钥的地址中，那么会在新的区块链中(侧链）生成相应数量的新币。由于地址没有私钥，发送完毕后资产将不会再返回，只能继续使用新币。

2.1.6 混合模式

上述所有的模式都是对称的，而混合模式则是将上述获得双向锚定的方法进行有效的结合的模式。由于主链与侧链在实现机制存在本质的不同,所以对称的双向锚

定模型可能是不够完善的。混合模式是在主链和侧链使用不同的解锁方法，例如在侧链上使用 SPV 模式，而在主链网络上则使用驱动链模式。同样，混合模式也需要对主链进行软分叉。

2.2 侧链应用场景

随着通证经济的繁荣，区块链性能的限制、功能的单一，以及项目的同质化等问题逐渐暴露出来。而区块链 3.0 时代，出现的侧链和跨链技术，为区块链产业克服以上缺陷带来了曙光。侧链延展了主链的性能，拓宽了代币的使用场景，既可以寄生于主链之上，也可以脱离主链独立存在。目前最大的两个应用场景在于解决主链拥堵，以及部署智能合约。

2.2.1 解决主链拥堵

比特币通过侧链来解决主链拥堵的思路在于，大额转账走主链，因为大额转账通常不在意手续费与网络拥堵的劣势；小额转账通过第二层网络，不需要太多的算力来保驾护航，因此可以实现低手续费、秒级到账。

2.2.2 部署智能合约

比特币的能力是有限的，同时智能合约可能是资源密集型的。所以即使比特币一直支持基本的智能合约功能，但这两者从来都不是天作之合。受制于比特币的网络性能、区块大小，智能合约一直无法有效的在比特币网络中部署，可以通过第二层网络——侧链技术，来实现基于比特币的智能合约。

3. 侧链优劣分析

3.1 侧链能解决什么问题

首先，在主链安全性保障的前提下，侧链可以在小范围共识，优化确认时间。我们可以把 tps 放在第一位，达到秒级确认。

其次，多种侧链“并行”运行时，主链安全性和业务负载并不显著增加。因为主链上的数据只是侧链数据转入其中存储的状态，它不会面临数据膨胀的问题。

第三，侧链数据可以加密，在小范围传输，记录交易路径，且不泄露隐私。在这样一个策略下，我们既可以在专有领域内传递数据，又可以同主链交互。

第四，侧链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。

最后，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，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，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。

3.2 侧链暴露的问题

侧链解决了主链的一部分性能问题，一定程度上弥补了主链不可能三角的缺陷，但也并非十全十美。侧链本身也是一条区块链，同样受不可能三角的制约，在部署和使用的过程中也会引发一系列的问题，甚至会影响到主链的安全。

3.2.1 算力攻击潜在风险

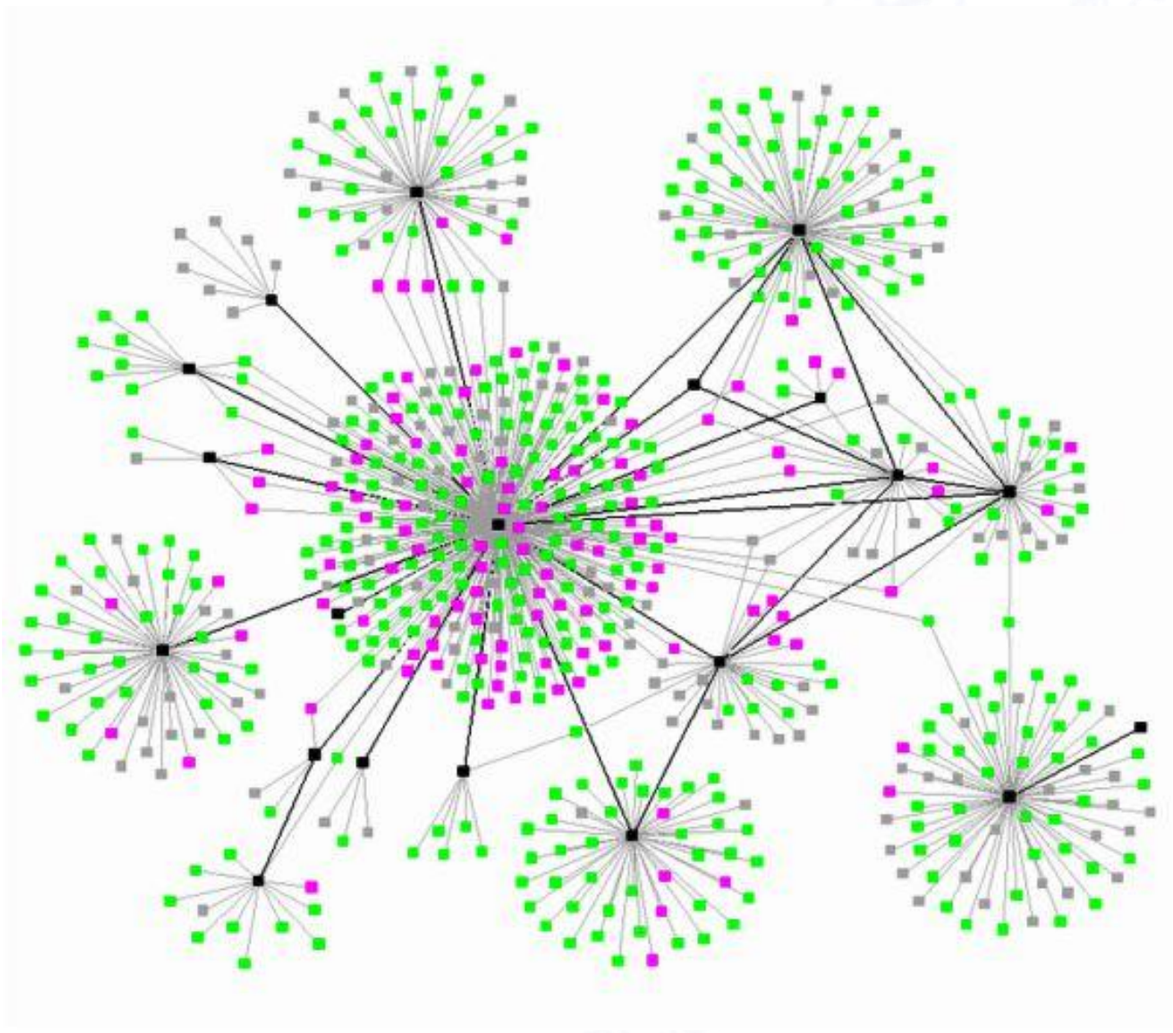
在侧链方案中攻击者只需要破坏最薄弱的侧链，就可以破坏整个网络。一旦在某个侧链完成 51%攻击，他们就可以创建一个（假的）最长侧链，用伪造的侧链币在原比特币块链中换成比特币。问题的本质在于，侧链们不共享同一个公共块历史。这意味着，从一个侧链到另一个侧链转移币的过程中，大部分侧链方案仅仅依赖所谓的“SPV 证明”，它只检查所涉及的币是否来自已知的最长链，而并不追溯币的历史来源至创世区块。这种 SPV 证明运行在轻钱包内部，安全标准远低于比特币网络。而在侧链方案中，一个 51%攻击者不仅可以双花一笔交易，甚至可以凭空制造侧链币。

3.2.2 联合挖矿的中心化

解决侧链攻击问题的一个办法是联合挖矿，以确保所有侧链同时以相同哈希率开采。联合挖矿的情形下，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，但实际上联合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。

3.2.3 中心化倾向

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。



按照闪电网络的设计，随着演化很有可能会出现有少数几个巨型节点占据的网络。其他侧链或也都面临着类似的问题，为了提升区块链的延展性，或多或少都有一些中心化的倾向。

3.2.4 影响主链安全

比特币是一种点对点的电子现金系统，为了激励矿工去维护网络的安全，中本聪设计出了区块奖励的概念，同时为了保证总量有限又通过每四年减半的制度维持，当未来区块奖励不足以维持矿工收益，大量的链上交易又被闪电网络夺走或许会影响到比特币网络的安全。

4. 具体侧链项目分析

目前基于侧链技术的项目有很多，部分具有投资价值，比如 RDN、LSK、XAS、LOOM 等，还有纯粹锚定比特币的项目闪电网络 Lighting-network、根链 RSK，也有通过燃烧证明发行的基于 BCH 的智能合约网络虫洞协议 WHC。

4.1 闪电网络

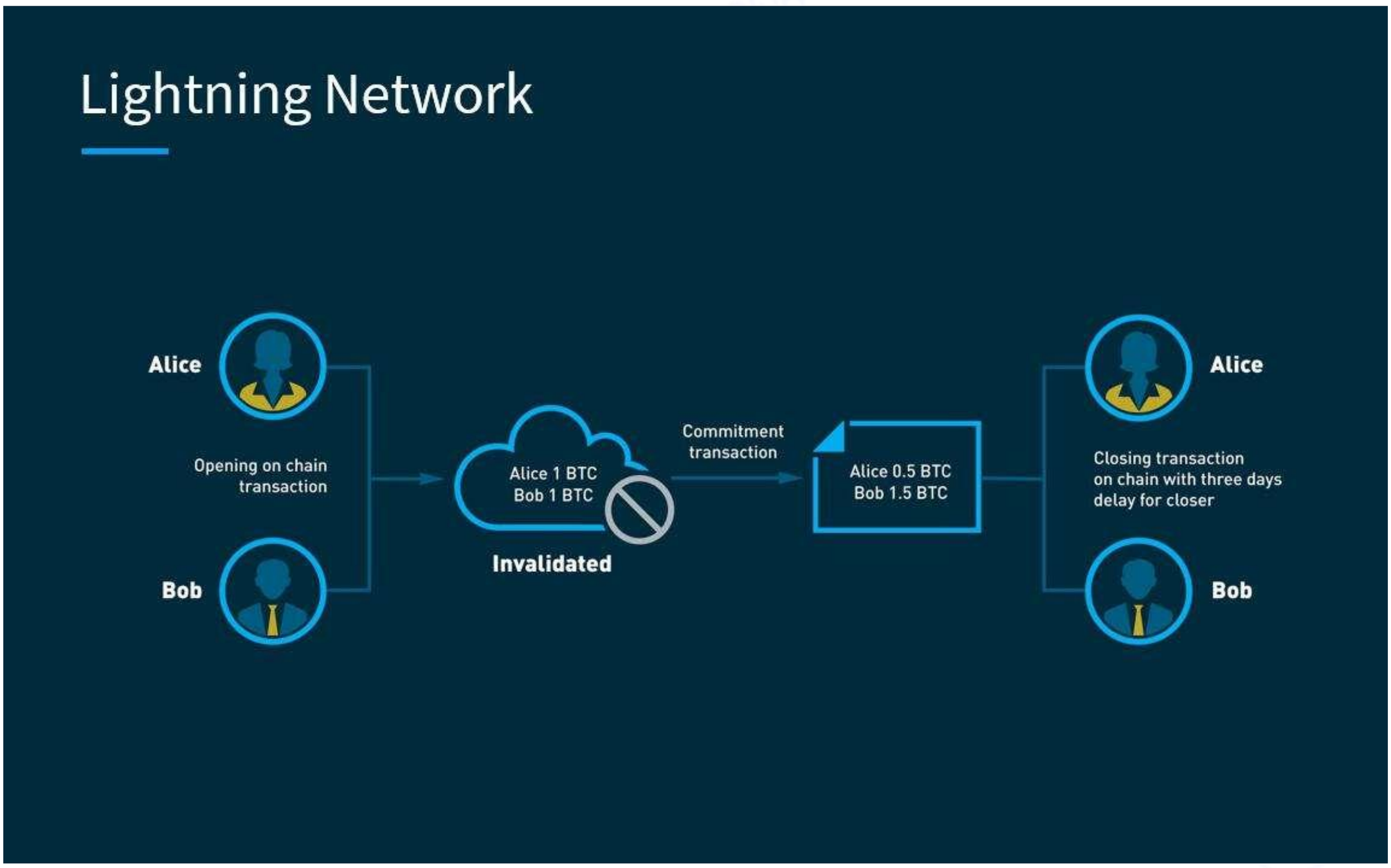
比特币拥堵问题由来已久，关于链上链下的扩容方案社区对此也一直处于争议当中。BCH 分叉后通过大区块进行扩容，而 BTC 则选择激活隔离见证，走闪电网络 off-chain 扩容的方式。

4.1.1 闪电网络是什么

闪电网络 Lighting Network，是一个链下服务方案，它不发送任何货币，而是在第二层级中进行账本的变更并随后在第一层级中完成结算，从而避免数千次的、实际的链上资金交易。

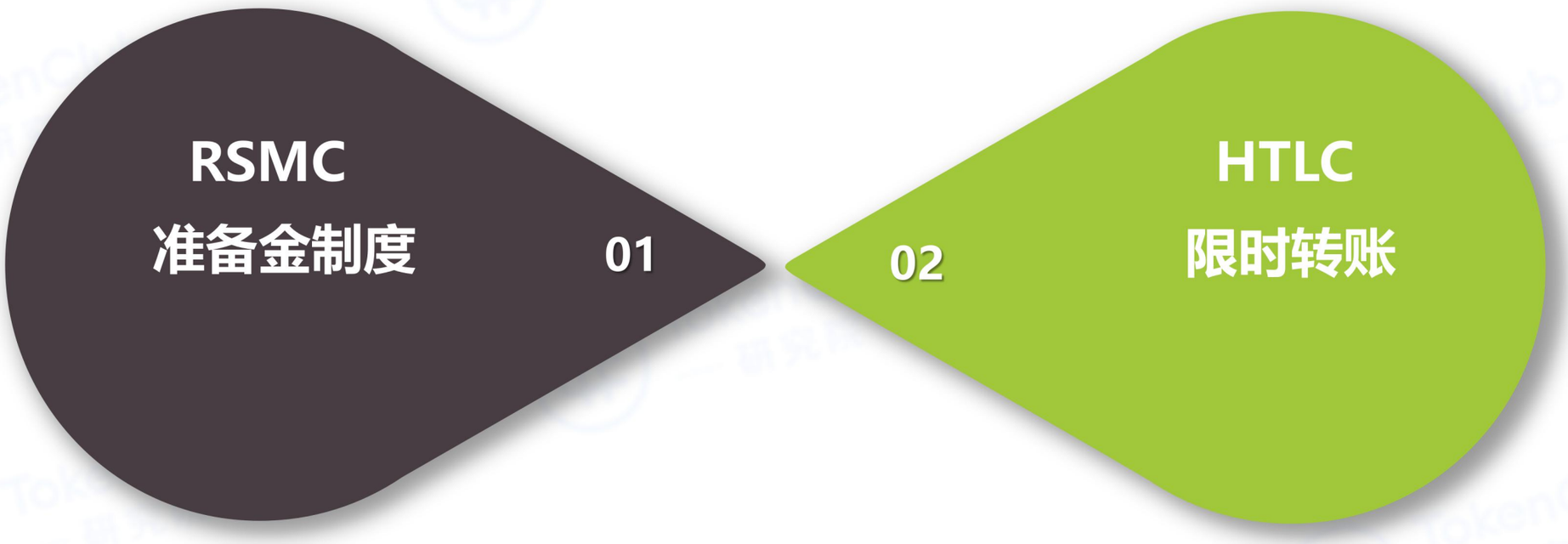
根据闪电网络浏览器中的数据显示，目前闪电网络已搭建 3639 个节点，形成通道 12289 条，网络容量达 114.83 个 BTC。

通过将资金发送到由多方掌管密钥的多重签名地址，闪电网络构建起一个支付渠道。收付双方之间的交易在链下完成，无论这个交易渠道关闭时的余额是多少，这些余额都会被如数发回用户的钱包。这就是双向支付渠道的工作原理。闪电网络是一个典型的双向支付渠道网络，通过这个网络，用户可以与自己的承包商进行定期支付或每月结算。



闪电网络的目的是实现安全地进行链下交易，其本质上是使用了哈希时间锁定智能合约来安全地进行 0 确认交易的一种机制，通过设置巧妙的‘智能合约’，完善链下通道，使得用户可以在闪电网络上进行 0 确认的交易。

闪电网络的核心的概念主要有两个：RSMC（Recoverable Sequence Maturity Contract）和 HTLC（Hashed Timelock Contract）。RSMC 保障了两个人之间的直接交易可以在链下完成，HTLC 保障了任意两个人之间的转账都可以通过一条“支付”通道来完成。这两个类型的交易组合构成了闪电网络。从而实现任意两个人都可以在链下完成交易。



RSMC 是指可撤销的顺序成熟度合同，类似于准备金制度。即双方发生交易的条件是双方需要在一个微支付通道（资金池）中预存一部分资金，之后每次交易，就对交易后的资金分配方案共同进行确认，同时签字作废旧的版本。当需要提现时，将最终交易结果写到区块链网络中，被最终确认。可以看到，只有在提现时候才需要通过区块链。

HTLC 则是指哈希的带时钟合约，可以理解为限时转账。即通过智能合约，双方约定转账方先冻结一笔钱，并提供一个哈希值，如果在一定时间内有人能提出一个字符串，使得它哈希后的值跟已知值匹配（实际上意味着转账方授权了接收方来提现），则这笔钱转给接收方。

闪电网络采用了更合理的支付网络架构，代表着效率的提高。与其向所有人广播交易，交易可以更直接地发送给收款人。只有当交易双方不诚实时，才需要进入繁琐的流程——链上共识操作。通过这种方式，可以实现相当于互联网上各方之间直接沟通所能达到的性能和效率，同时保留比特币区块链的一些安全特性。然而，如果各方想在出现问题时可以随时回归到区块链上并收回资金，那么建立这样一种支付系统是非常复杂的，并且还存在着一些重大风险和局限性。

4.1.2 闪电网络工作流程

闪电网络的正常使用包括通过向区块链网络提交正常的资金交易来开通支付通道，然后进行任何数量的闪电交易，更新通道内资金的临时分配而不广播到区块链，最后关闭支付通过广播最终版本的交易来分配通道内的资金。闪电网络是基于比特币区块链构建的智能合约系统，允许两方直接进行快速，廉价的支付。为了实现这些快速而廉价的交易，采取了以下步骤：

- 设置一个多重签名钱包，其中包含一定数量的比特币；
- 钱包地址然后保存到公共比特币区块链中，包括资产负债表（智能合约），证明该比特币存款的多少属于谁；
- 在此支付通道进行一次设置之后，这两方就可以进行无限次的交易，而无需触及存储在区块链中的信息；
- 对于每次交易，双方签署更新的资产负债表以便始终反映存储在多信用点钱包中的比特币的金额属于谁；
- 更新后的资产负债表不会上传到区块链，而是双方保留其副本；
- 每当发生争议或支付通道关闭时，双方都可以使用最新的互相签署的资产负债表来支付他们在多信用卡钱包中的份额。

闪电网络不需要对手方合作退出支付通道。双方都可以选择单方面关闭通道。因为所有各方都有多个多签名。在这个网络上有许多用户之间的通道，理论上可以通过这个网络向任何人发送付款。

4.1.3 闪电网络的优点

根据白皮书的描述，闪电网络主要包括以下优点及特点：

即时支付：闪电网络的支付速度可以达到毫秒级，从而快速完成支付，其通过区块链智能合约来保障安全，不再为每一次付款提交一次区块链交易，从而提高交易速度；。

无需可信第三方：在闪电网络交易中也是两个节点之间直接进行转账，没有第三方能够控制资金。

缓解主链压力：只有开启通道，关闭通道和争议性交易需要提交到区块链上进行，允许闪电网络内的所有其他交易保持未提交状态。这这使得闪电网络用户可以通过比特币进行频繁支付，而不会使必须处理区块链上每笔交易的完整节点承担过多的负担。

洋葱式路由：支付路由信息可以以嵌套的方式加密，以便中间节点只知道他们收到了可路由支付的人和下次发送给谁，防止中间节点知道发起者或目的地。

多重签名功能：每个参与方都可以要求通过多个密钥对他们的付款进行签名。

跨链功能：如果另一条区块链支持用于哈希锁的相同哈希函数，以及具备创建时间锁的能力，支付通道就可以跨多个区块链（包括侧链）进行路由。利用异构区块链共识规则，交叉链式原子互换可以立即发生在链外。只要链可以支持相同的加密散列函数，就可以跨区块链进行交易，而不需要信任第三方托管商。

可扩展性好：理论上闪电网络每秒可以处理数百万笔交易，无需托管即可完成支付。

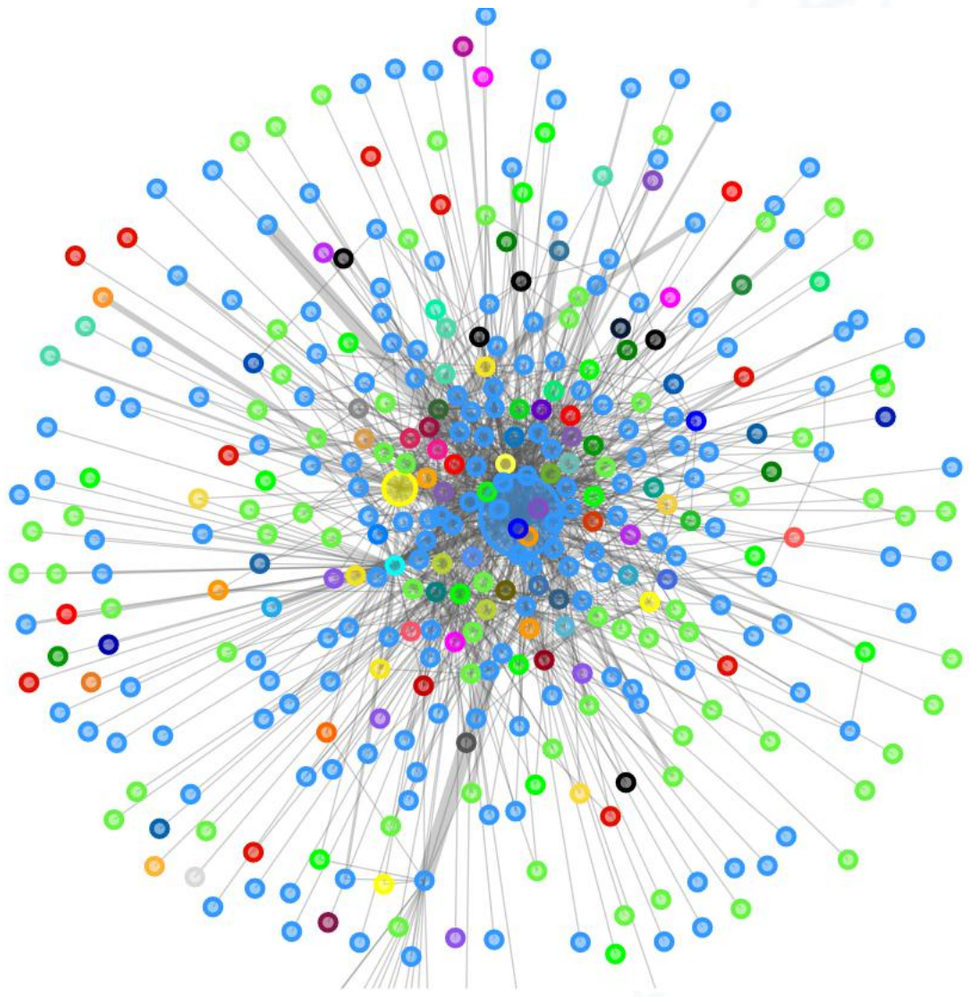
低手续费：闪电网络是通过链下交易，只需要极低的交易费用，使即时微支付成为可能。

4.1.4 闪电网络的问题

尽管闪电网络能够解决主链性能不足造成的一些问题，但它仍然有很多缺陷被人诟病，主要体现在以下几点：

技术复杂开发进程慢：闪电网络白皮书诞生于 2015 年，至今仍停留在测试网阶段，无法大规模使用，比特币的主链拥堵问题仍然无法缓解。

网络效应难以建立：对于一个网络来说，用户越多网络的价值也就越大，而闪电网络的复杂性提升了搭建闪电网络节点的门槛，用户难以形成规模效应。



节点的中心化倾向：按照闪电网络的设计，受成本与各种因素的影响，闪电网络的节点会演变成几个大节点连接的网络，目前排名第一的节点 **dead.cash** 占全网 15.5%的容量。虽然这些大型节点对网络无法控制，但从技术上讲，它们可以被视为中心转账机构，监管机构可以很方便的介入审查。

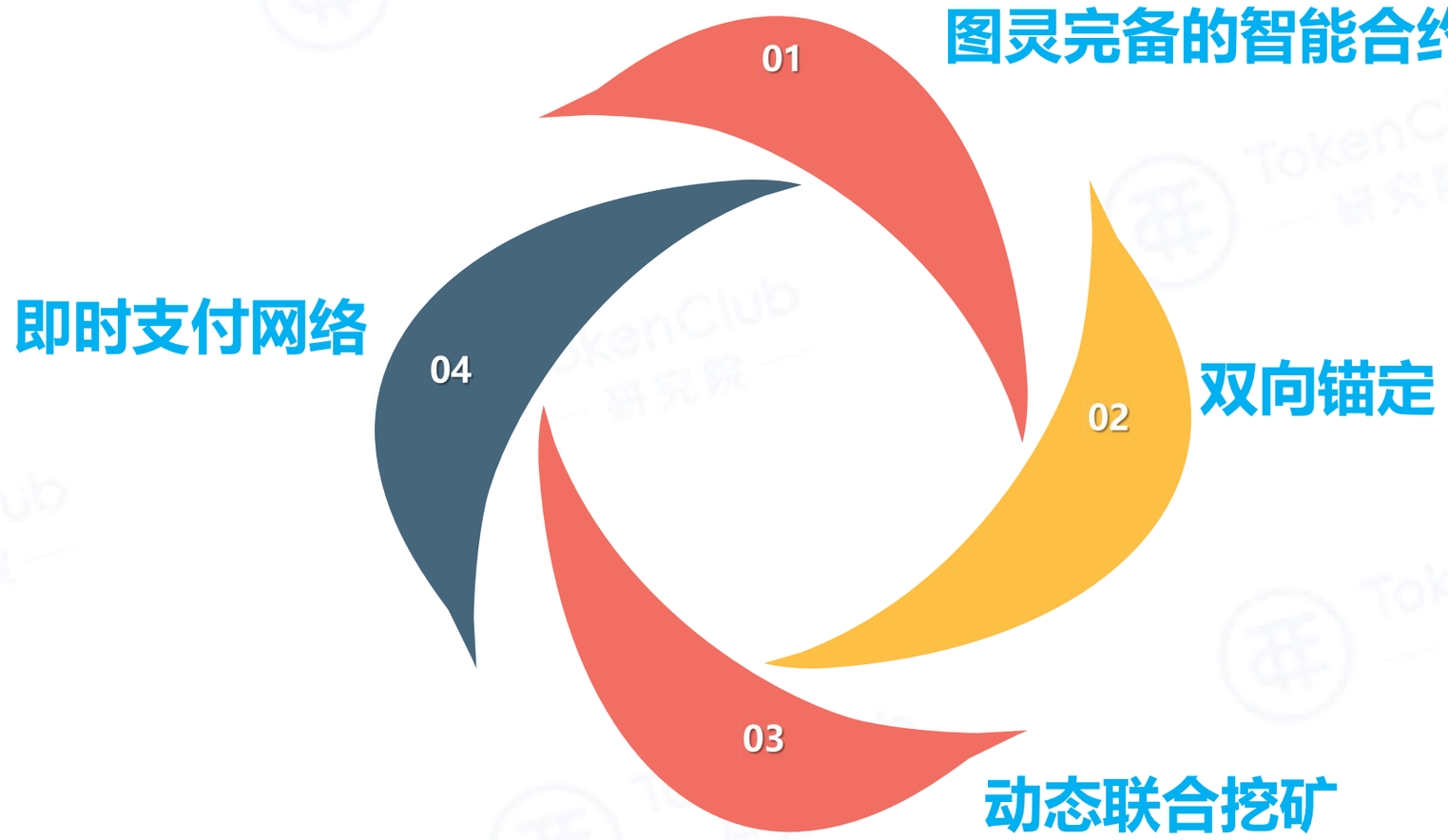
安全问题：闪电网络测试网上线后，曾发生了几起丢币的事件。此外，它也违背了中本聪点对点的电子现金系统的初衷，通过主链交易的结构是比特币地址-比特币地址，而通过闪电网络交易则是 BTC-LNBTC-LNBTC-BTC 这样一个过程。

4.2 RootStock

根链 RootStock 是第一个和比特币双向锚定的开源的智能合同平台，矿工通过联合挖矿获得奖励。RSK 的目标是实现智能合约、即时支付以及更高的可扩展性，为比特币生态系统增加价值和实用性。

RSK 是比特币的侧链，当有比特币转入 RSK 区块链时，这些比特币将变成“根币”（SBTC）。根币相当于存活在 RSK 区块链上的比特币，并且它们可以随时转回比特币区块链，并且不需要添加额外的交易费（除了 RSK 的转账交易手续费外）。SBTC 是 RSK 这支侧链的代币，用于支付给矿工的转账手续费和合约处理手续费。根币并没有创造新的数字货币：所有的 SBTC 都是来自比特币区块链里的比特币转化过来的。（注：这里的 SBTC 不是指闪电比特币）

RSK 的核心部分包括以下几个方面：



图灵完备的虚拟机：根链的虚拟机是智能合约平台的核心。智能合约是由高比例的网络节点自动执行。智能合约可用于处理合约间的信息、创建资金交易和改变合约里的存储状态。虚拟机运算操作码兼容以太坊虚拟机，让以太坊的合约在根链上完美兼容。在第一个版本里，虚拟机是通过解释执行的。在下一个版本里，将计划通过动态重定向操作码以兼容使用 java 字节码的以太坊虚拟机，并且强化安全性和内存的限制，形成一个根链虚拟机新版本。这将给根链虚拟的执行性能接近本地代码。

双向锚定：RSK 是一个独立的区块链，其代币通过通过支付证明的方式自动锚定另一条区块链的代币。两个代币使用双向锚定实现自由兑换，并且是自动的，不会产生价格折损。在 RSK 平台，根币双向锚定比特币，在具体实践中，当比特币换成根币时，并没有比特币在两条区块链上转移，因为比特币区块链是无法验证另一条区块链的交易的。当交换发生时，交易的比特币是被锁定在比特币区块链

上，同时另一部分根币在根链区块链上被释放。当根币需要兑换回比特币时，就是反过来，根币被锁定，而等额的比特币在比特币区块链上被解锁。

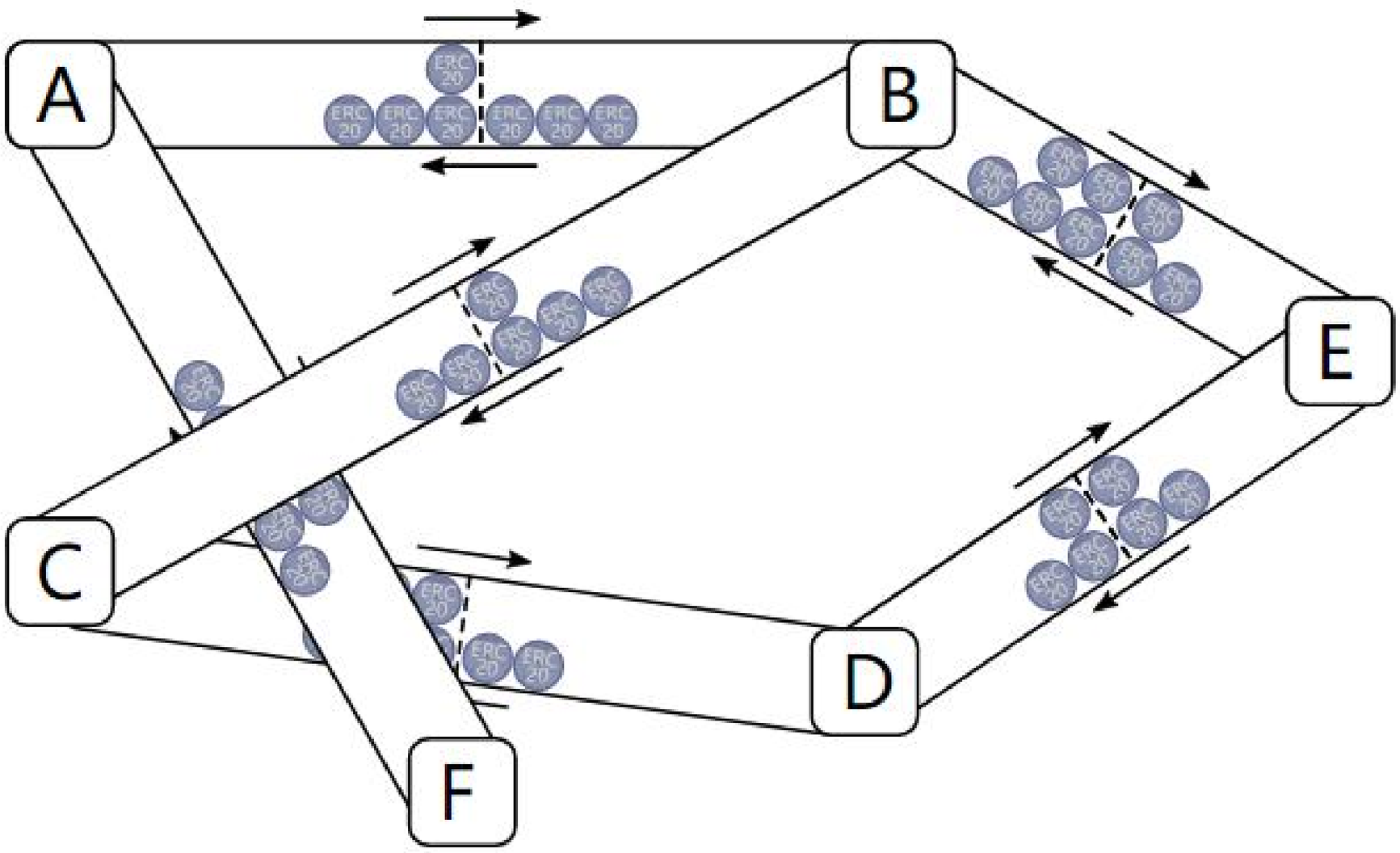
动态联合挖矿：RSK 采用与比特币联合挖矿的形式运作，目前已有包括 BTC.com 在内的多家矿池予以支持，联合挖矿不仅可以保障 RSK 区块链的安全，也可以提高矿工的收益。

快速支付和低延迟网络：RSK 可以实现每 10 秒出一个块，并且每秒最多交易次数达 300 至 1000 笔。这不仅可以缓解比特币主链上的压力，也可以让 RSK 被更友好的使用。

4.3 雷电网络

雷电网络 Raiden 是一种脱机缩放解决方案，用于在以太坊区块链中执行符合 ERC20 标准的令牌传输。它是基于以太坊的比特币闪电网络版本，可实现近即时，低费用，可扩展和隐私保护的付款。

Raiden 网络允许在参与者之间安全地转移令牌，而不需要全球共识。这是通过数字签名和哈希锁定传输实现的，称为余额证明，通过先前设置的链接存款完全抵押。付款渠道允许两个参与者之间几乎无限制的双向转移，只要其转账的净额不超过存入的令牌。这些传输可以立即执行，而不需要实际的块链本身的任何参与，除了最初的一次性链接创建和最终关闭通道。



Raiden 的真正实力在于其网络协议。由于开通和关闭两个对等方之间的支付渠道仍然需要进行链式交易，所以可能的所有对等体之间创建渠道将变得不可行。然而，事实证明，如果通过连接双方的渠道网络至少存在一条路线，则您不需要付款人和收款人之间的直接付款渠道。该网络及其相关联路由和互锁通道传输协议称为雷电网络。

雷电网络的原理与闪电网络大致类似，不过区别在于雷电网络通过 ICO 的方式进行募资，发行了 RDN 代币，代币的用途在于支付打开交易通道。上线后经过投资者广泛追捧，单价一度超过 50 元人民币，现在在 3 元左右，由于目前生态为广泛铺开，RDN 没有足够的应用场景去支撑它的代币价值，也被业内广泛诟病。

4.4 Loom Network

Loom Network 是以太坊应用程序特定的侧链网络，开发人员可以在其中大规模地运行分散的应用程序。Loom Network 旨在成为一个平台，社区可以在侧链上运行软件，在平台上拥有既得利益的公平透明的既得利益，同时能够根据需求调整安全限制。社区将能够在区块链上运行，用户可以启动自己的节点并保护网络。

根据官网介绍，LOOM 并没有发布白皮书，它通过发布项目来证明自己的价值。根据技术介绍，LOOM 采用 DPOS 的共识机制，允许高度可扩展的游戏和面向用户的 DApp 在其之上运行，同时仍然受到以太坊的安全支持。

LOOM 致力于社交、游戏类项目的开发，目前上线了 CryptoZombies，一个学习智能合约编程的交互学习网站。此外还包括 DelegateCall-Blockchain based Q-A，一个问答系统。以及 The Adventures of etherboy in blockchain world、Cryptozombies Rancher、Cryptozombies World 等游戏。

4.5 Wormhole

Wormhole 中文名称虫洞协议，它的特点在于代币 WHC 通过燃烧证明的机制发行，即将 BCH 发送到一个特定的没有私钥的地址中，最低发送数量为 1BCH，即可按照 1：100 的比例声称虫洞代币 WHC。目前虫洞地址上已经燃烧了 2300 个 BCH，发行了上百个代币。

虫洞燃烧地址

qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc

与一些主流侧链所使用的双向锚定机制不同，WHC 通过燃烧证明的方式发行，所发送的 BCH 将再也不可使用，造成人为的稀缺。此外，WHC 的安全将受到两层保护，第一层是 Bitcoin Cash 的交易安全，采用 POW 的挖矿算法作为去中心化的时间戳服务器；第二层保护是运行 Wormhole 协议的节点，不符合 Wormhole 协议的数据不会被 Wormhole 协议的节点解析，每个节点都有能力通过重新解析交易数据，计算出 Wormhole Cash 的最近的合法最终状态。

可以说，WHC 所起到的作用相当于基于 BCH 侧链的以太坊，通过在第二层网络上搭建智能合约平台，不会占用主链的太多资源，又可以为主链的生态带来更多的应用场景。

4.6 阿希链

阿希链 XAS 本身是一条公有链，作为一款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，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。

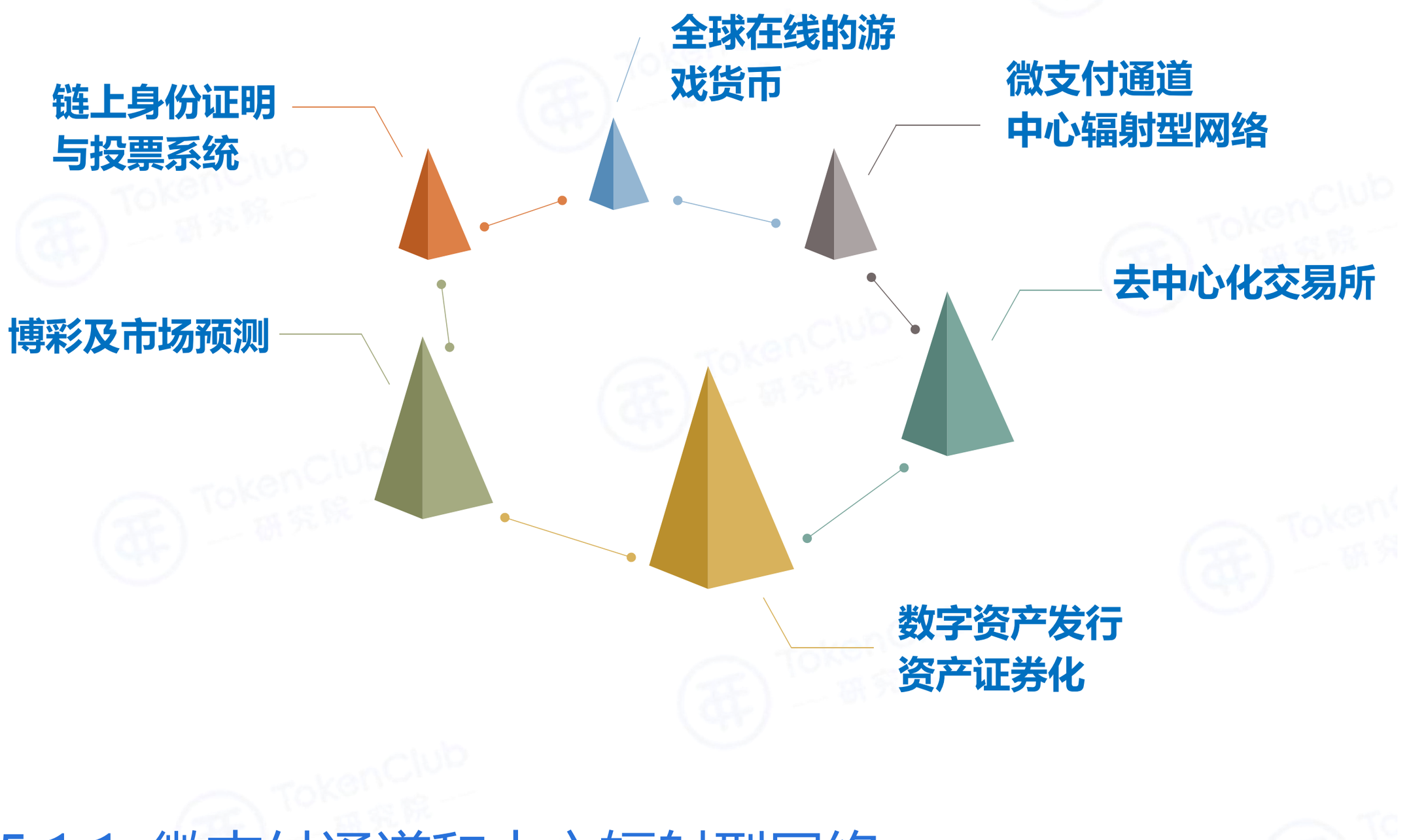
阿希链采用 DPoS+PBFT 的共识机制，其特点在于它可以通过侧链(跨链) 的方式来承载应用，解决了区块链的分片问题。相比于以太坊网络主链作为应用的载体，阿希链的侧链架构使得每一个 DAPP 都相当于一条侧链，这样侧链之间不会相互影响，不会出现像以太坊那种一个应用流量太大会造成其他应用拥堵的情况，应用的燃料也可以由开发团队自定义。

阿希链采用侧链与跨链的方式作为扩展机制，交易中没有携带代码，不仅减少了交易数据的负载量，还使得合约逻辑更容易编写。此外，主链进程内提供若干 API，以管道接口开放给侧链应用，通过这些 API 开发者可以更轻松的创建丰富的应用。

5. 侧链的应用场景及未来展望

5.1 侧链技术的具体应用

侧链技术所支持的平台，提供了图灵完备的智能合约，可以在很多场景发挥其实际作用：



5.1.1 微支付通道和中心辐射型网络

微支付通道允许两人构建一个安全的支付规则，并且不需要手续费来完成小额支付，但是只有一次支付机会，然后支付通道就要关闭。中心辐射射型网络让用户可以无需相互信任直接使用支付通道来完成小额支付，也可能依靠一个最低信任

的第三方来完成支付。通过侧链可以构建中心辐射型支付网络，实现即时到账以及百万 TPS，简单直接并且是标准的电子钱包支付方式。

延伸一下，通过侧链网络可以迅速铺展零售支付系统，让比特币等加密货币成为全球的日用零售业务支付方式。

5.1.2 去中心化交易所

侧链技术使得价值在两条区块链之间进行流通，本身就是去中心化交易的行为。侧链技术作为一项底层协议，自动匹配出售和求购信息也是非常容易建立，这就使得任何人可以依托侧链技术构建一定去中心化的不需要第三方参与的数字加密资产交易所。

5.1.3 发行数字资产及资产证券化

像以太坊平台一样，具备了图灵完备的侧链平台也一样可以发行包括 ERC20、ERC721 等标准的数字资产。鉴于侧链平台对在平台上创造合约所需要的燃料费用要求很低，任何人包括学生到银行和公司都可以利用根链平台创建自己的加密资产。

侧链平台也可以基于原子资产来发布数字化证券，将原子资产证券化。包括商业房地产信托基金、股票、债券和其他资产（或未来价值）都可以利用侧链来完成数字证券化。这个功能将可以为缺乏现代金融系统的发展中国家里的小企业提供运营和成长资金解决方案。

5.1.4 全球在线的游戏货币

拥有众多游戏玩家的游戏是有其内存的经济体的，包括提供了特殊的货币。随着游戏的发展，游戏玩家获得的虚拟游戏币是有价值的，并且常常会在二级市场里出售。但通货膨胀、欺诈和网络偷盗都威胁着游戏里的经济安全。并且游戏公司保管用户的虚拟财产本身也要面临法律和安全风险。随着全球化的进展，已经虚拟游戏的发展，游戏玩家越来越对一个游戏里的游戏币不能被应用于其它游戏感到不适。

侧链平台可以解决这些问题，将比特币或其他加密货币整合进游戏，也可以使用侧链平台上创建一个数字资产。侧链支付系统非常快，游戏引擎也可以将侧链用做游戏支付系统，为玩家和玩家或公司和玩家之间的虚拟资产交易提供支付方案。支付过程仅仅需要点击一个链接或扫描一个二维码，支付系统就可以完成标准和电子钱包支付，也可以用于游戏公司的佣金支付。

5.1.5 博彩及市场预测

受制于主链的性能，一些搭建在主链平台上的博彩类应用往往难以提供叫好的用户体验。另一方面，像著名赌博网站中本聪骰子使用的是 0 确认的链上交易方式，对博彩网站也造成了巨大双花风险。侧链平台可以提供同样的用户体验，同时也能保证交易确认的安全性。使用智能合约，并结合加密协议可以构建各种无需信任的第三方参与的博彩预测类应用。

5.1.6 链上身份证明与投票系统

发展中国家主要问题之一是穷人缺乏信誉文档和身份信息。这种情况阻止了穷人拥有投票权，获得健康信息，获得刑事受害报告以及无法享受金融服务。侧链平台可以使用极低的成本建立数字身份，并且保证安全性。

有了安全可信的个人链上身份，可以凭借该身份证明参与各项选举，享受链上账户中的津贴发放等。

5.2 未来侧链发展趋势

不仅仅是侧链，即便是目前的区块链行业，各公链的发展尚不成熟，公链生态缺乏用户，公链之间像是茫茫大海中的一座座孤岛，缺乏价值的传递与流通。比如 EOS 的用户只会使用 EOS 链上的应用，而 ETH 的用户只会使用 ETH 链上的应用，这两大公链如此，更不用说其他公链了。在行业发展的早期，价值传递的闭塞，不利于整个生态的扩展速度。

此外，基础设施建设的瓶颈也限制了公链及侧链的发展，大部分项目的用户仍然处于将代币存放至交易所炒币的阶段，钱包用户的稀缺以及钱包体验差、开发成本高、回报率低的特点仍然存在，而且目前大部分钱包只支持公链的币种及生态，对侧链的支持甚少。这一切都说明目前区块链技术仍处于一个非常早期的阶段，而侧链则是早期的早期。

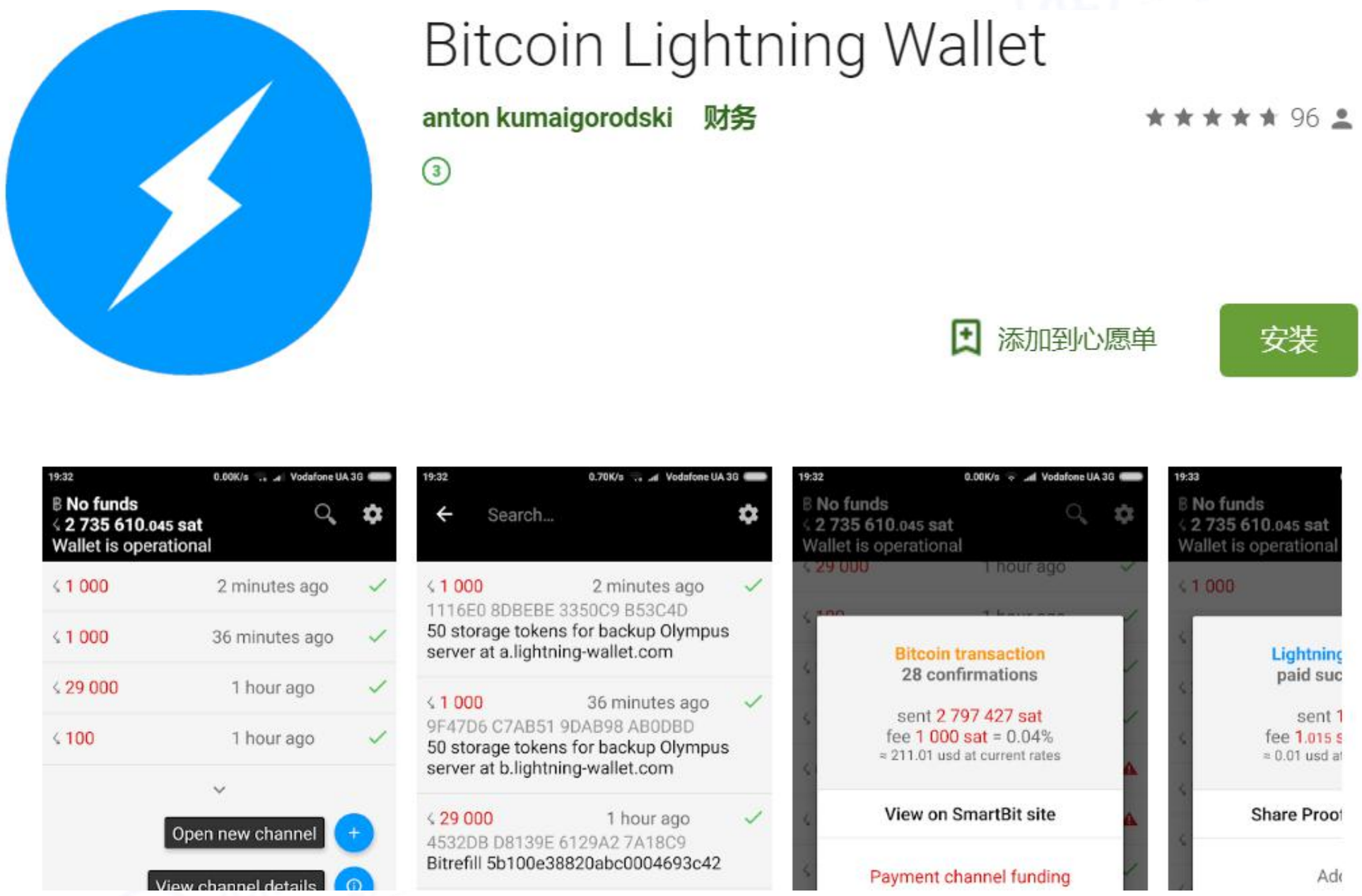
未来的侧链发展大致会呈现以下几个态势：

5.2.1 安全性加强

目前的侧链普遍安全性不足，闪电网络在测试阶段发生过丢币的现象。此外相比于主链，侧链的共识基础比较薄弱，更容易发生 51%算力攻击，这也是为什么很多侧链号称能解决主链延展性问题，而大部分用户开发者都选择在主链上开发的原因之一。

5.2.2 基础设施的广泛支持

目前区块链中主要基础设施之一就是钱包生态，只有通过钱包才能直接使用各种数字货币，但是目前绝大部分钱包都只支持单一币种的交易功能，很多公链的生态并未予以支持，更不用说能够将侧链的功能与生态整合到钱包中的供应商了。随着技术成熟用户增多，需求带动生产，很多大的钱包品牌会在发展的过程中将侧链技术及生态融合到钱包中。



首款登陆谷歌应用商店的闪电网络钱包

钱包之外，像区块链浏览器之类的设施也会增加对侧链的更多支持，比如 BTC.com 提供了增加了虫洞协议的区块链浏览器，并且能够显示闪电网络相关的交易。见下的图黄色闪电标识：

输入 (1)	0.00044764 BTC	输出 (1)	0.00043798 BTC
bc1qk8gsvdnq86shqksk...z9fa0qerd9mr4snf2af4	0.00044764	bc1qlz7cnvdyp92hzgvh...ud50j4tyh0mxwqrqpd8m	0.00043798

确认数 11,787

5.2.3 一条侧链服务于更多公链

从技术角度上来说，很多侧链是可以服务于多条公链的。比如闪电网络可以在比特币与莱特币的区块链上部署，去年 11 月份在比特币和莱特币发生了首笔基于闪电网络的原子互换交易。其他侧链比如 RSK、XAS、LSK 等都可以服务于多个公链。在未来，更多技术成熟的侧链会嫁接到更多的公链上，甚至于跨链的技术相融合。

5.2.4 公链侧链化

从定义上来说，只要符合侧链协议，所有的区块链都可以成为侧链，甚至现在的侧链本身也可以是一条独立的区块链。在未来，一条最为稳定的公链（比特币）作为整个区块链生态之锚，其他公链包括 ETH、EOS 都可以作为其侧链而存在，区块链的世界将进一步的融合。

6. 风险提示

本报告所采用的的数据均来自合规渠道，分析逻辑基于作者的职业理解，本报告清晰准确地反映了作者的研究观点，力求独立、客观和公正，结论不受任何第三方的授意或影响，特此声明。

本报告的信息来源于已公开的资料，TokenClub 研究院对该等信息的准确性、完整性或可靠性不做任何保证。在任何情况下，本报告中的信息或表述的意见均不构成对任何人的投资建议。

TokenClub
研究院

TokenClub 是国内领先的数字货币投资社区，致力于构建一个自治、信任、高效的数字资产投资服务生态。

“TokenClub 研究院”是 TokenClub 旗下研究区块链的专业机构，专注于区块链行业研究、项目评级。

扫码关注
TokenClub 研究院

扫码下载
TokenClub APP