分片专题研究报告

引言

分片是区块链扩容的热门方向之一。不仅以太坊基金会把分片作为官方钦定的扩容方向，有分片概念的一众公链在近期也受到投资界热捧。本文就分片技术的分类和实现方法进行讨论。

作者

节点研究中心 马旭颖 蔡晨曦 编辑 郎瀚威

哈希研究院 Alfred，LJ

鲸准研究院 王帆 陈泓伊

支持媒体

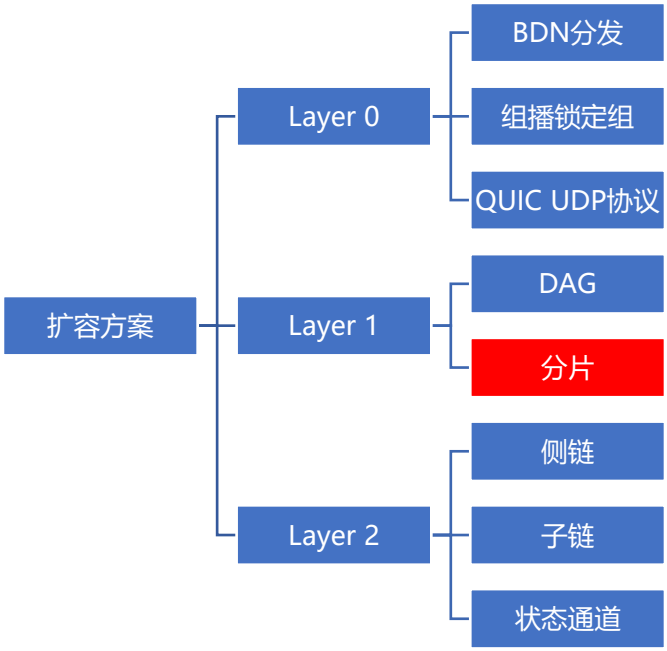
金色财经 BlockMasterMail 星球日报 陀螺财经 巴比特 嘻哈财经 金牛财经 耳朵财经 火星财经 荣格财经 零壹财经 币圈邦德 区块财经 链条 ChainHeadline

目录

一、分片是什么 3
1.1 分片解决区块链的扩容问题 3
1.2 分片的原理 3
二、区块链与分片技术 5
2.1 分片技术的层级 5
2.2 分片技术的进展 6
三、分片项目分析 7
3.1 分片项目一览 7
3.2 重点项目对比分析 8
四、分片项目的投资逻辑 9
4.1 技术上实现的可能性 9
4.2 与其它扩容技术的结合 9
4.3 服务质量是否能达到商业级别 9
4.4 项目的创新性和严谨性 9
五、分片技术的未来展望 10
5.1 技术优势 10
5.2 发展阻碍 10
六、附件 11
声明 11

1 分片是什么

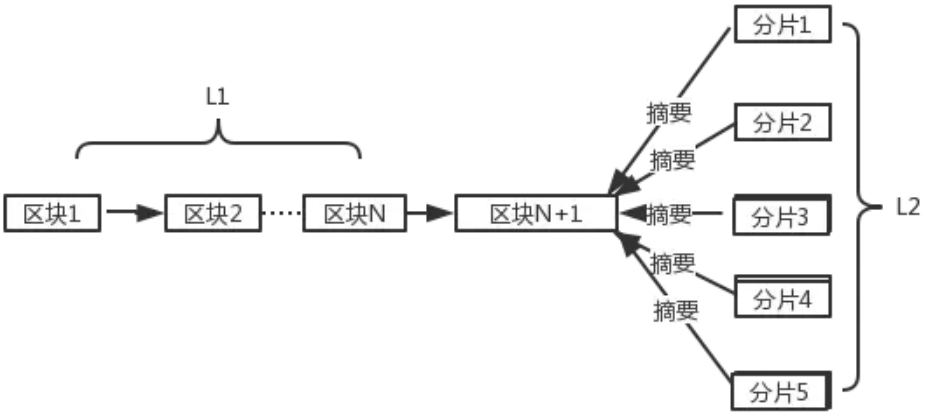
1.1 分片解决区块链的扩容问题



目前区块链的扩容方案主要分为三个不同的 Layer。分片和 DAG（有向无环图）同属对区块链本身架构进行改变的 Layer 1。分片目前被关注的热度很高，主打分片技术的公链被投资机构热捧，分片也和 Layer 2 的侧链、子链、状态通道等方向一起被列入以太坊官方的扩容方案。

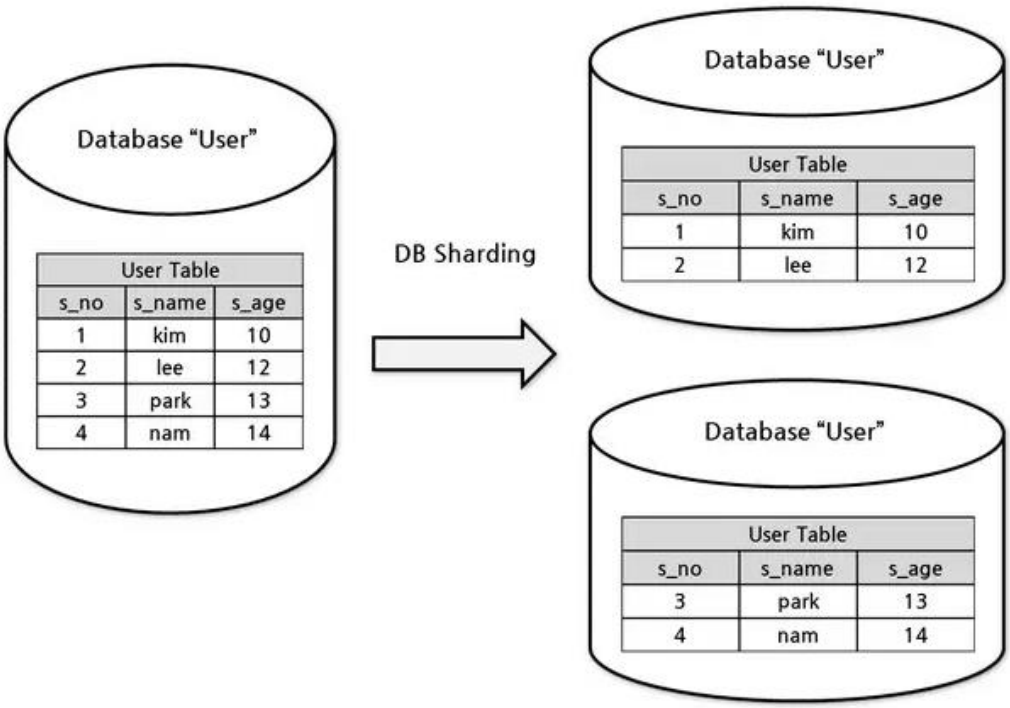
1.2 分片的原理

分片其实是一种传统数据库技术，它将大型数据库分成更小、更快、更容易管理的部分，这些部分叫做数据碎片。在公链中，它是通过使用多个网络设备来获得平行处理转账的功能，从而分散那些转账验证的工作量。这样会自动地把网络分成很多更小的部分，或者说进行“分片”处理，从而每一个小网络只需要运行一个更小范围的共识协议。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。所以，分片技术使用的是平行处理的方式，有越多的节点加入，网络中批准的速度也会加快。简单来说，分片的就是将一个大任务拆分为多个可以并行处理的小任务，从而提升性能。



图中，我们把以太坊的网络分为两部分，左边一部分 L1 为现有的以太坊主链，右边一部分 L2 为各个分片，他们各自是一个独立的账户空间。每个分片有专门的节点来维护，就相当于一个个独立的区块链，每个分片将自己的记录汇总发给主链。主链收集各个分片的摘要，然后生成主链区块（N+1）。但是主链收集的是摘要而不是具体的交易细节。

分片方案带来的主要好处是，网络节点进行的冗余计算量大大减少，每个节点只需对自己分片内的交易进行验证，不需要验证分片外的交易。如此可节约大量的时间与网络资源，进而完成更多的交易的处理。



2 区块链与分片技术

2.1 分片技术的层级

目前主流的分片技术分为网络分片、交易分片和状态分片等三个层级，其技术难度也随之依次递增。主要的核心在于分片内节点需要达到一致，并且防止被恶意攻击者控制，而分片之间需要信息传递机制，保证交易及智能合约的状态在不同分片间达到一致。

1．网络分片

利用随机性，网络可以用 VRF 方法随机抽取节点形成分片，用以防止恶意节点占据某个分片。分片内节点之间的共识可以通过 pBFT 等共识机制来实现。

2．交易分片

1）账本分片：在一个基于 UTXO 的系统内，系统可以根据发送者的地址分配一个分片。这确保了两笔双花交易将在相同的分片中得到验证，因此系统可以很容易地检测到双花交易，而不需要进行任何跨片的通信。

2）跨账本分片：在一个非 UTXO 的系统里，为了防止双花问题，在验证过程中，分片间将不得不进行相互通信。事实上，由于双花交易可能会在任何分片中出现，因此特定分片所接收到的交易将不得不与其它的所有分片进行通信。这种相互之间的高昂通信成本可能会破坏交易分片的最初目的。

3．状态分片

这一技术的关键是将整个存储区分开，让不同的碎片存储不同的部分；每个节点只负责托管自己的分片数据，而不是存储完整的区块链状态。状态分片一经提出，就伴随着挑战。

在一个状态分片的区块链中，一个特定的分片只会保留一部分状态。假设其中一个账户创建了一笔交易，它将支付另一个账户一笔钱。这笔交易将由第一个分片进行处理，一旦该笔交易被验证，关于第一个账户的新余额的信息就必须与它所在的分片进行共享。如果两个帐户由不同的分片进行处理，那么这可能需要进行频繁的跨片通信和状态交换。确保跨片通信不会超过状态

分片的性能收益仍然是一个值得公开的研究问题。

状态分片的第二个挑战是数据的可用性。比如由于某种原因，一些特定的分片遭到了攻击而导致其脱机。由于分片并没有复制系统的全部状态，所以网络不能再验证那些依赖于脱机分片的交易。因此，在这样的情况下区块链基本上是无法使用的。解决此问题的方法是维护存档或进行节点备份，这样就能帮助系统进行故障修复以及恢复那些不可用的数据。但是，这样就使得节点将不得不存储系统的整个状态，因此这还可能会引发一些中心化的风险。

任何分片机制需要确保分片在抵御攻击和失败时是具有弹性的；网络必须接受新的节点并以随机的方式将这些分配给不同的分片。然而，在状态分片的情况下，重新分配节点是非常棘手的。在一次重新调整网络的过程中，在同步完成前可能会出现导致使整个系统失效的问题。为了防止系统的中断，我们必须对网络进行逐步调整，以确保每个分片在所有节点被清空前仍有足够多的旧节点。类似地，一旦一个新节点加入了一个分片中，系统就必须确保该节点有足够的时间与分片状态进行同步。

2.2 分片技术的进展

层级	交易分片	交易分片	状态分片	状态分片	状态分片
分片技术	Ethereum Casper	Zilliqa	Omniledger	Chainspace	Rchain
描述	将交易分割成发送+接受两布，并且在不同的共识周期中完成，发送币后通过收据来进行确认	交易处理进行基于账户地址哈希值的分片，然后传送给分片leader进行全网共识	跨链UTXO首先将相关账号锁定，然后视返回信息，客户端可解锁并执行或中止，类似原理可以延申到跨链智能合约	智能合约执行时在客户端先模拟trace，标注出可能与其他交易冲突的地方，然后再分发到相关的分片中处理，再用S-BAC去共识	通过namespace对分片进行分级管理，用rho语言在执行期传递name
缺点	发送交易与接受交易不在一个周期，接受交易的分片可能遭受攻击导致币丢失	智能合约非图灵完备	需要客户端在交易过程中保持在线，解锁交易的签名较大	客户端需要较多计算量，分片间通信成本较高	rho语言入门门槛高，难学

3 分片项目分析

3.1 分片项目一览

名称	流通市值排名	流通市值（亿）	项目介绍
ETH	2	¥3,436.44	Ethereum（以太坊）是一个平台和一种编程语言，使开发人员能够建立和发布下一代分布式应用。 Ethereum可以用来编程，分散，担保和交易任何事物：投票，域名，金融交易所，众筹，公司管理， 合同和大部分的协议，知识产权，还有得益于硬件集成的智能资产。以太坊将使用混合型的安全协议，前期使用工作量证明机制（POW），用于分发以太币，然后会切换到权益证明机制（POS）。
Zil	30	¥57.60	zilliqa(zil)作为一个新的公有区块链，着重为高吞吐量的应用程序提供运行平台。它将分片技术从理论变为实践，运用创新的密码技术和共识协议，提供随着网络增容而不断提高的交易处理能力。在最新的实验中，测试网络达到每秒处理2,400个交易以上。这比目前的主流区块链平台快了200多倍。zilliqa区块链平台致力于支持高吞吐量和数据驱动的分布式应用程序，以满足诸如电子广告、支付、共享经济和产权管理等业务必要的扩容需求。
Elf	55	¥25.37	ælf是一个去中心化云计算区块链网络，具有高性能、资源隔离特性以及更完善的治理和发展结构。在ælf的网络中，节点根据类型进行划分，专业化记账节点（全节点）能够运行在服务器集群之上，提高整个区块链网络性能；“主链+多侧链”结构，有效实现资源隔离、“一链一场景”；设立代币持有人的委托票选制度，保障网络高效治理及良性发展。elf主要用于ælf的付费资源支付及治理决策，其中付费资源包括智能合约部署、升级及执行等操作(如交易手续费、跨链数据传输手续费等)，治理决策包括记账节点的选举、系统新特性的审批及产品重大更新的决策。
Moac	/	¥39.09	Moac独创的分层架构技术和子链技术大大增加了平台的扩展能力，可轻松上链区块猫等专属网络，可便捷上链试验新的区块链产品；突破异步合约调用、合约分片处理和全领域跨链等当前业界难题，对合约的处理速度远远优于当前譬如以太坊等智能合约平台。相对于以太坊每秒 7-14 次交易处理，墨客可以做到100倍的处理速度，在进一步优化后可以达到1000倍
QuarkChain	未上市	未上市	QuarkChain将自己形容为“高度可扩展，分散，安全，公开，无许可的区块链”。目标是通过提供增强的事务处理能力推动行业向前发展。QuarkChain提供高度可扩展的区块链，声称能够每秒处理100万笔在线交易。QuarkChain使用双层结构实现更好的可伸缩性。第一层提供弹性分片，这是一种数据库分区，可将超大型数据库分为更小，更快，易于管理的数据分片的组件。数据碎片是QuarkChain项目的关键部分。第二层被称为根区块链。这是确认第一层推送的事务的组件。QuarkChain的第二层可根据需要“重新划分”，而无需更改根层。
Emotiq	未上市	未上市	Emotiq是一款功能强大的分散式区块链，拥有PoS（Poof）共识和自然语言智能合约。Emotiq提供横向可扩展性和VISA和Mastercard级吞吐量，每秒处理数千次交易。Emotiq区块链旨在具有可扩展性，私密性和自然性：首先通过Omni- Ledger水平缩放或分片; 第二个与非交互式零知识证明，确保交易隐私; 与Ring - Emotiq的简单英文智能合同语言，启用非程序员创建易于理解的智能合约。
SMAC	未上市	未上市	SMAC通过实现区块链的分片，提高区块链系统的交易处理能力。相较于一条单独的区块链系统，SMAC系统可以通过连接多条子链的方式在交易处理能力上直线增长。交易的请求通过SMAC的分配进入不同子链，可以有效规避针对一条子链的集中请求。此外，可以在SMAC上部署同构子链的不同节点数的集群，对于同构链而言，多节点数量的集群会有相对较高的安全性，少节点集群的处理速度则更快。通过SMAC实现区块链的分片，可以根据业务需求灵活部署，为用户提供更高质量的区块链服务。

3.2 重点项目对比分析

	ETH	Emotiq	QuarkChain	Moac	Elf	Zilliqa
共识机制	PoW,PoS	Omniledger	分层	分层	DPos,PoW	PoW,PBFT
技术模式	以太坊是一款能够在区块链上实现智能合约、开源的底层系统，它是是一个平台和一种编程语言，使开发人员能够建立和发布下一代分布式应用。 以太坊可以用来编程，分散，担保和交易任何事物。	Emotiq建立在Omniledger分片技术之上，采取门罗和零知识证明系统中的Bulletproof提供额外隐私保护；通过开发RingVM让非程序员来进行部署智能合约	QuarkChain采用双层区块链结构，的分片层用于交易记账，根链用于确认分片中的交易；基于博弈论框架设计了一个用于激励矿工工作并合理分配算力的机制；利用多个廉价节点组成集群实现一个超级节点；支持跨分片交易	通过分层化的结构来支持数字资产交易，数据访问和流程控制。创建允许用户使用高效的方式执行智能合约的框架，提供开发体系结构，采用底层基础设施来快速简便地产生子区块链	Elf包含一条主链和多条附加在主链上的侧链，可通过适配器和比特币、以太坊以及其他一些区块链系统对接。主链是Elf系统的基石，主链提供一个开发侧链的模板和基础设施，让侧链之间可以互相通信。	Zil将网络划分为若干个子网络独立的进行事务处理，以此来达到提高整个网络事务吞吐量的目的。
工作流程	将区块链网络中的每个区块变为一个子区块链，子区块链中可以容纳若干（目前为 100 个）打包了交易数据的 Collation（大概可以称为“校验块”，为了在分片的情景中将其与区块的概念区分开），这些 Collation 最终组成一个在主链上区块	利用Emotiq智能合约的自然语言，非程序员可以轻松创建智能合约，以满足广泛的协议和应用程序并以交互方式进行测试。通过子代币系统在Emotiq上发布属于自己的虚拟货币，并且可以通过客户端完成Emotiq代币与子代币之间的相互交换。可通过比特币网络或者以太坊网络进行跨链交易	通过允许集群中的多个诚实节点作为完整节点运行来解决这个问题。群集中的每个节点只验证一个子集。只要它们的子集的联合覆盖根链和分片，我们就可以证明它们能够完全验证整个区块链而不需要建立昂贵的超级节点。另外，如果其中一个节点在群集中崩溃，其余节点仍然能够完全验证任何块，因为它们中的任何两个形成另一个群集，从而实现这样的集群的高可用性	大多数交易将在顶层（POS层）处理，关键交易和控制流程在底层（POW层）中处理。顶层的所有交易都是以智能合约调用的形式进行，底层节点的智能合约服务器（SCS）节点都可以处理顶层的用户请求。特定的SCS节点处理特定的事务。	Elf在主链上使用DPoS机制来激励持币大户去维护一个稳定的系统，同时在侧链上使用PoW来产生代币。每个链上的共识机制都可以根据实际需求定制。在一条侧链被接纳后，它需要给主链支付一定的费用才能被索引。Elf采用动态收费策略来反映每条侧链对Elf生态系统的贡献度。	矿工们使用PoW在Zil区块链上建立身份，随即被分配到一个共识组，其中可以运行多轮PBFT（拜占庭）共识。执行一个PoW可将多个区块写入链中，从而提供更大的保证奖励
核心团队	“天才神童”以太坊创始人Vitalik Buterin2011年全年为比特币线上媒体《比特币周刊》工作，2011年后期作为联合创始人创建了《比特币杂志》（Bitcoin Magazine），曾击败Facebook创始人Mark Zuckerberg，获得2014年IT软件类世界技术奖。	Joel Reymont, 前AE的CTO。在Emotiq白皮书尚未发布前，很多私募就用Joel的名头开始收币。	创始人周奇是前Google软件工程师，也曾在Facebook工作。技术研究团队中多位人员为前谷歌高级软件工程师，还有乔治亚理工学院教授，西安交通大学教授等。团队人员都有着较高的学历与实力。工作经验丰富。但是创业经验较为缺乏，都为初次创业者	周沙：硅谷超过 20年工作经验硅谷风投精准资本创始人，《区块链世界》及《区块链与大数据》的第一作者；陈小虎：硅谷超过 18 年工作经验区块链技术公司的创始人。在区块链领域内首先提出异步智能合约及分流技术；杨歆乐：硅谷超过 18年工作经验区块链技术公司首席架构师，拥有多项区块链相关专利正在申请中	马昊伯，ELF创始人，好扑创始人兼CEO，区块链行业专家，数字资产领域早期从业者，曾任GemPay CTO、AllCoin CTO、现任中国电子协会区块链专家委员会委员，近10年间曾在信息安全、社交网络、智能家具设备和移动互联网等领域有创业探索及技术积淀。	ZIL的创始人Xinshu Dong是新加坡国立大学的计算机专业的博士，首席科学顾问是加州伯克利大学博士，首席策略师是康州大学麦迪逊分校的博士；负责市场有资深的咨询行业背景

4 分片项目的投资逻辑

4.1 技术上实现的可能性

分片的技术难度非常之大，尤其是状态分片尚未在计算机科学理论中得到很好的解决，因此只有世界顶尖的技术团队才有希望进行突破。

4.2 与其它扩容技术的结合

分片可以与 DAG、状态通道等互补，各自发挥优势，实现系统整体扩容。

4.3 服务质量是否能达到商业级别

扩容性是否提高最终都需要经过市场的检验。目前大部分分片项目和应用离商业可用性还有很大距离，怎样解决分片项目之间不同区块之间的相互联系，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。

4.4 项目的创新性和严谨性

严谨性指的就是要有已发表的学术论文验证，在理论上能通过。如果没有严谨的论文来证明，系统最起码要有一千个节点以上的测试网络，代码也是公开的，这样才会比较有说服力。

5 分片技术的未来展望

5.1 技术优势

分片与以比特币、以太坊为代表的传统共识机制有本质的区别。对于分片技术来说，在实现了多方共识的同时解决了节点增加导致网络拥堵的问题。比如最近 zillqa 的一个测试实验显示，仅有 3600 个节点，6 个分片的状态下，就达到了两千笔一秒的交易性能，如果把以太坊的现有矿工移植到 Zilliqa 来，那么 Zilliqa 的性能可以达到以太坊的 1000 倍以上。看似只是从串联到并联的简单跳跃，却给了区块链技术发展提供了更大的优化空间。

5.2 发展阻碍

由于分片技术的优势，越来越多的从业者开始关注和支持分片技术。这一方面推动了分片技术的优化同时也带来了一定的问题。

一方面，分片技术着眼于解决性能问题，而部分参与者却过于执着 TPS 的竞争，却忽视了其安全性的保证。

另一方面由于分片技术的大火，致使很多人盲目的参与到分片技术的创业之中，但是很多人没有搞清楚分片的治与分的平衡关系，很简单的认为分片的逻辑就是分，这种不严谨不仅会阻碍技术的发展，同时也会伤害到市场对技术的信心，甚至会产生更加严重的后果。

分片技术还处于初级阶段，而市场的浮躁也为技术的发展和落地带来了一定阻碍，技术完善与市场教育依然任重而道远。

6 附件

参考阅读：

20160527 Rootstock 发布测试网络 比特币迎来了智能合约

20170528 阿希（ASCH)系统，升级版的以太坊

20170708 Vitalik 给 R3 提供的跨链技术报告

20180109 深度解析：区块链跨链技术

20180304 2018 最顶级项目“RSK” 即将上线，热度最高，回报率惊人！

20180308 一站式开发区块链 DAPP | Lisk

Vitalik Buterin 《Sharding doc》

Vitalik Buterin 《Chain Interoperaability》

声明