前沿跨链技术 Cosmos 简介

大家晚上好，我是万向区块链股份公司旗下万云平台的首席技术官奚海峰。感谢币乎社区的邀请，很高兴有这个机会跟社区的朋友们分享前沿跨链技术 Cosmos。

首先介绍一下 Cosmos 项目的背景，Cosmos 项目是由硅谷的 Tendermint 团队发起的一个公有链项目。Tendermint 团队以及他们的产品情况稍后会有介绍。Cosmos 项目的目标是建立区块链的互联网，通过跨链代币转移技术构造一个深度集成的代币经济生态系统。

Cosmos 项目在 2017 年四月份完成了 ICO，融资额为当时价值一千七百万美元的比特币和以太币。发放总量两亿枚 Atom 代币，分配是：ICO 的销售占 75%，天使投资人占 5%，ICF(Inter-chain Foundation)基金会 10%，团队保留 10%。ICO 的基准价为 10 美分，战略投资人和早期投资者分别有 25%和 15%的折扣。

Cosmos 主网原计划是 2017 年底上线，现在推迟到了今年 2 月底。主网上线以后代币才会上交易所交易，首先上哪些交易所，现在还不清楚。

很不幸的是已经有一个公链项目叫 Atomic Coin，它的代币符号也是 Atom,但它不是 Cosmos ,大家一定要清楚。如果你没有参与 ICO 的话 ,Cosmos 的 Atom 代币只能等到今年 2 月底主网上线上交易所以后才能参与购买。

Cosmos 是去年 4 月份比较热门的一个项目，当时 ICO 的时候一抢而空很快就结束了，国内知道的人不太多，因为他们这个团队一直都是作风比较低调。当时国内在杭州、深圳一些技术社区里面，了解区块链技术的一些团队参与了这个 ICO。关于 Cosmos 背景的一些详细资料,我给大家发一个链接，线上交流以后如有兴趣可以自己去看。

https://github.com/cosmos/cosmos/blob/master/PLAN.md

我们现在就来看一下跨链技术 Cosmos ,Tendermint 团队是最早研发 BFT 共识引擎的，也是最早提出的跨链概念的。大概在 2015 年左右就提出来了，所以这样看来 Tendermint 团队还是相当有超前意识的。团队做 Cosmos 这个项目最早的一个动机就是做为一个所谓去中心化的区块链技术 ,但是币币交易的时候需要依赖很多中心化交易所，中心化交易所的问题是很多的，那么去中心化的交易所是不是就没问题了呢？实际上也是有问题 ,现在看来就是基于以太坊的去中心化交易所，像以德 EehDelta 只能进行 ERC2 之间的币币交易，但实际上，如果大家看一下 coinbase 里面排名前三十的代币里面几乎没有几个是 ERC20 代币。去中心化交易所另外一个问题就是它要依赖于中心化的网关。所以说 Cosmos

团队他们当时想做这个项目的一个动机就是如何能够通过去中心化的区块链技术本身，把这个代币能转移到一个去中心化交易所上进行交易，我想这是他们最早的一个初衷。

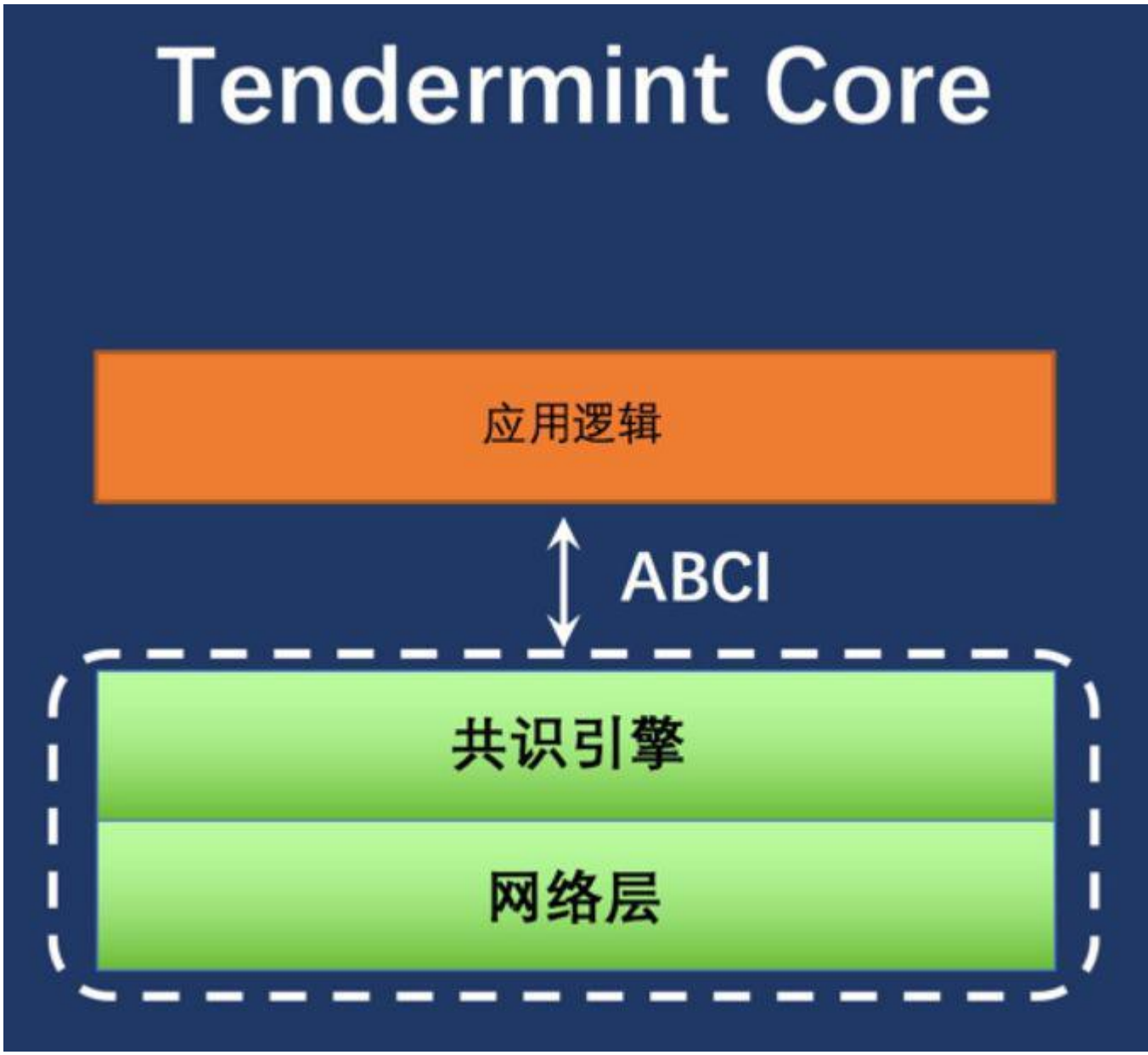
那么代币跨链的一些基础条件是什么呢？代币在跨区块链之间进行转移跟传统的互联网信息跨子网在互联网中转移的根本区别是什么？这个根本区别实际上就是后者涉及到价值转移。所以呢，这就全是关于钱的事，关于钱就很重要了，这个事情来不得半点错误，实际上这里就有两个很重要的条件，一个是发起跨链转移这个源头链，它发起这个跨链代币转移交易的真实有效性的证明就非常关键，而且更重要的是任何第三方都要能够独立地对这个交易的有效性加以验证。这就对区块链的特性提出了一些要求，最重要是两个：一个是共识算法要有实时最终性，所谓实时最终性就是一旦通过共识以后形成一个新的区块了，那这个块就是最终的，它不会将来再被推翻也就不会再分叉。那这就跟传统的基于 PoW 共识机制很不一样，第二,交易的提交确认要有高效的独立证明的方法，基本上就是基于 Merkel 证明。当然对于缺乏这些特性的区块链，比方基于 PoW 的比特币和以太坊，也可以通过一个叫 Peg Zone，就是一种锚定分区的桥接机制，可以接入 Cosmos 网络，后面我会对这个展开来讲一点儿。

理解上面讲的这些特性，就部分的解释了为什么是 Tendermint 团队最早提出做跨链。因为 Tendermint 团队是世界上最早的基于 PoS 做共识引擎的。他这个

PoS 引擎具有以下一些特点，第一，它是拜占庭容错的，就是所谓的 BFT，通过一个分布式的共识算法基于弱同步的假设的两轮投票机制,可以最多容忍三分之一的拜占庭节点。第二个特点，就是即时最终性。就是共识形成的最新区块就是最终区块，这种最终性不像 PoW 是基于概率性的。第三个就是它的这个共识效率非常高，秒级出快。TPS 可达到上千。

另外无论是公有链还是私有链都可以使用 Tendermint 共识引擎。比如咱们国内比较有名的杭州秘猿科技他们做的联盟链产品 CITA。底层就使用 Tendermint 作为共识引擎。最后一点 Tendermint 是其他一些重要 PoS 系统的参考基础，包括以太坊现在准备切的 Casper 这个机制也是大量的参考的 Tendermint 设计。

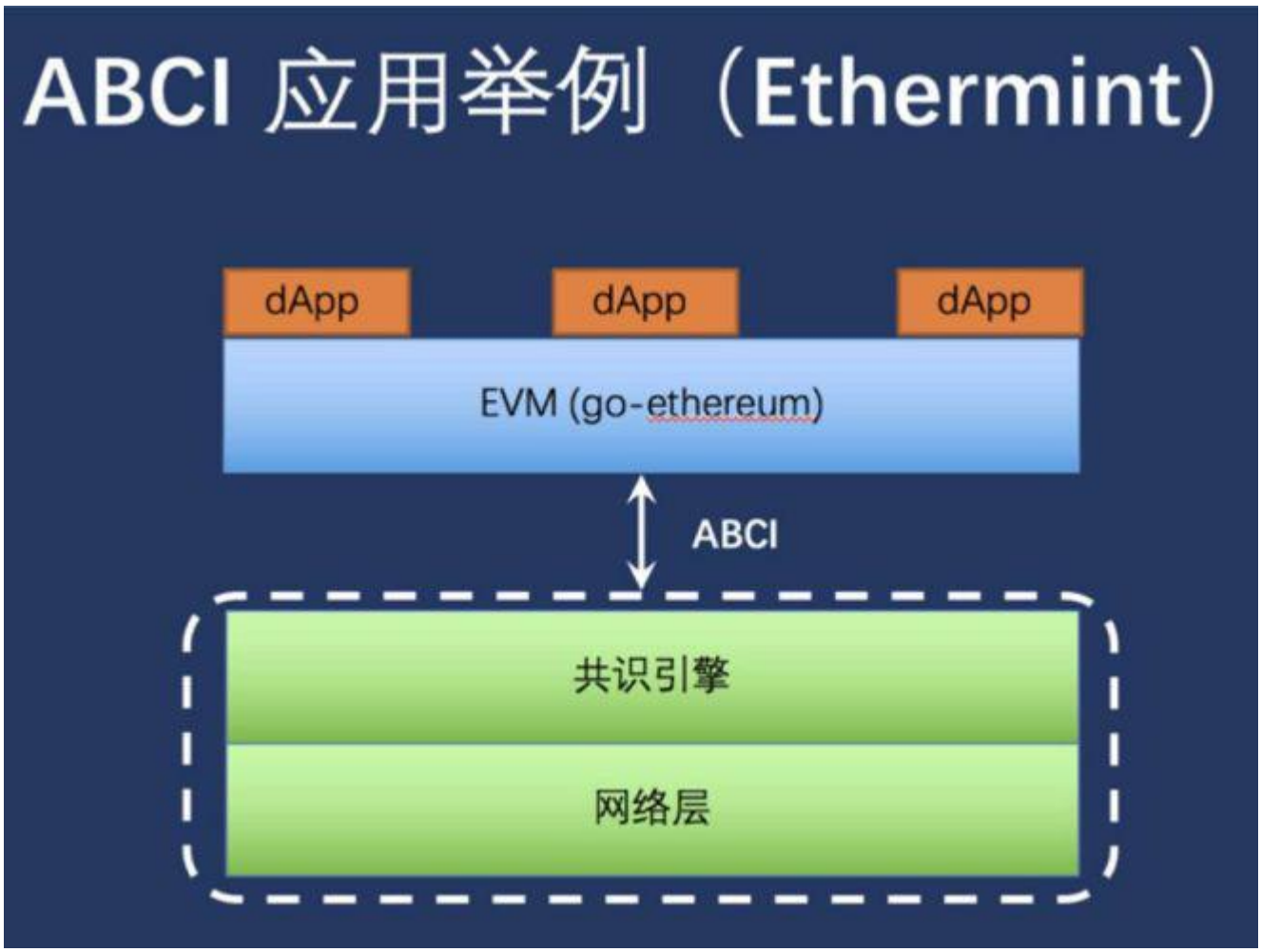
Tendermint架构设计上还有一个很重要的特点就是它把共识引擎和底下的P2P网络层,打包在一起组成了这个软件叫 Tendermint Core，这就是 Tendermint 这个产品的核心的功能。Tendermint 把这些底层最常用的和共识有关的功能提炼出来做成一个很精炼的一个产品 ,剩下的应用层的逻辑就是由应用开发者来实现。也就是说区块链的开发分成了两部分：一部分是底层常用共识引擎和网络层（这个由 Tendermint 团队来实现）。另外一个是区块链所要完成的应用逻辑，由区块链开发团队来实现。



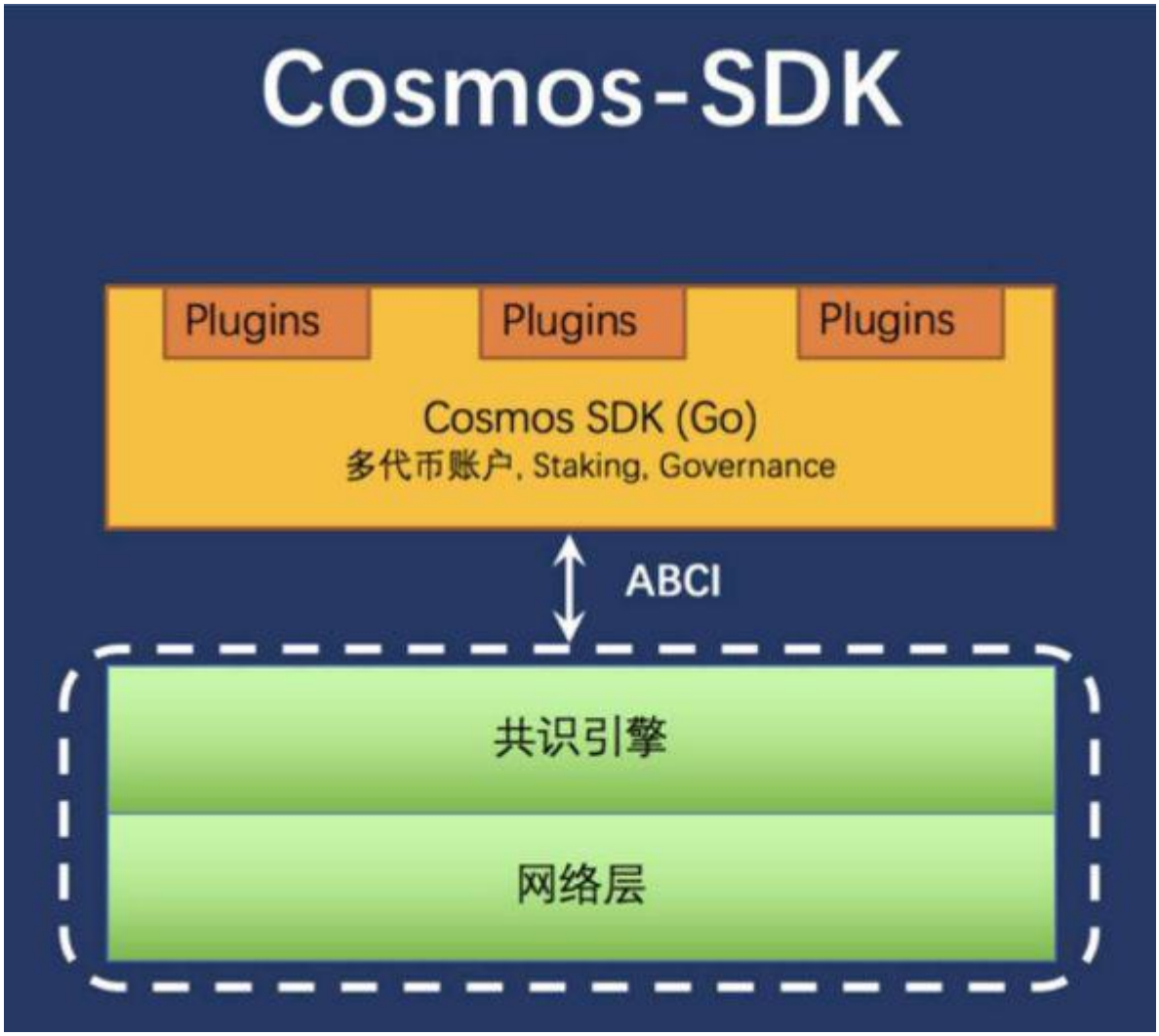
这样一个架构设计非常有意思。如果基于这种架构来设计的话，我们要实现比特币应该怎么做呢？Tendermint 在共识引擎和应用逻辑之间定义了一组回调的接口，即基于 socket 的 ABCI。那么我们看一下如果基于这个架构怎么实现比特币。那么底层的共识算法和网络层应该实现的是节点间通过这种点对点的 Gossip 协议，共享交易和区块。另外就是维护一个权威的、不可篡改的交易账本，也就是我们俗称的区块链。应用逻辑层负责维护这个 UTXO 数据库，验证交易的数字签名，确保它是有效交易。另外可以阻止一些其他的无效交易，比方

说试图花费一些不存在的 UTXO，甚至是双花的这种尝试。另外就是允许客户端的查询 UTXO 数据库。

这是另一个 ABCI 应用例子，这个项目也是 Tendermint 团队做的：Ethermint。它实际上是以太坊和 Tendermint，两个词合在一起组成的。它实际上做的事情就是把以太坊 Go-Ethereum 代码底层的 PoW 共识算法去掉，然后通过 ABCI 协议回调接口跟 Tendermint 进行了一个集成。这样它就实现了一个基于 PoS 的一个高效的以太坊，已有的以太坊的智能合约和所有的以太坊的客户端工具，开发工具，智能合约调用工具全部都可以原封不动的拿到这边来使用。



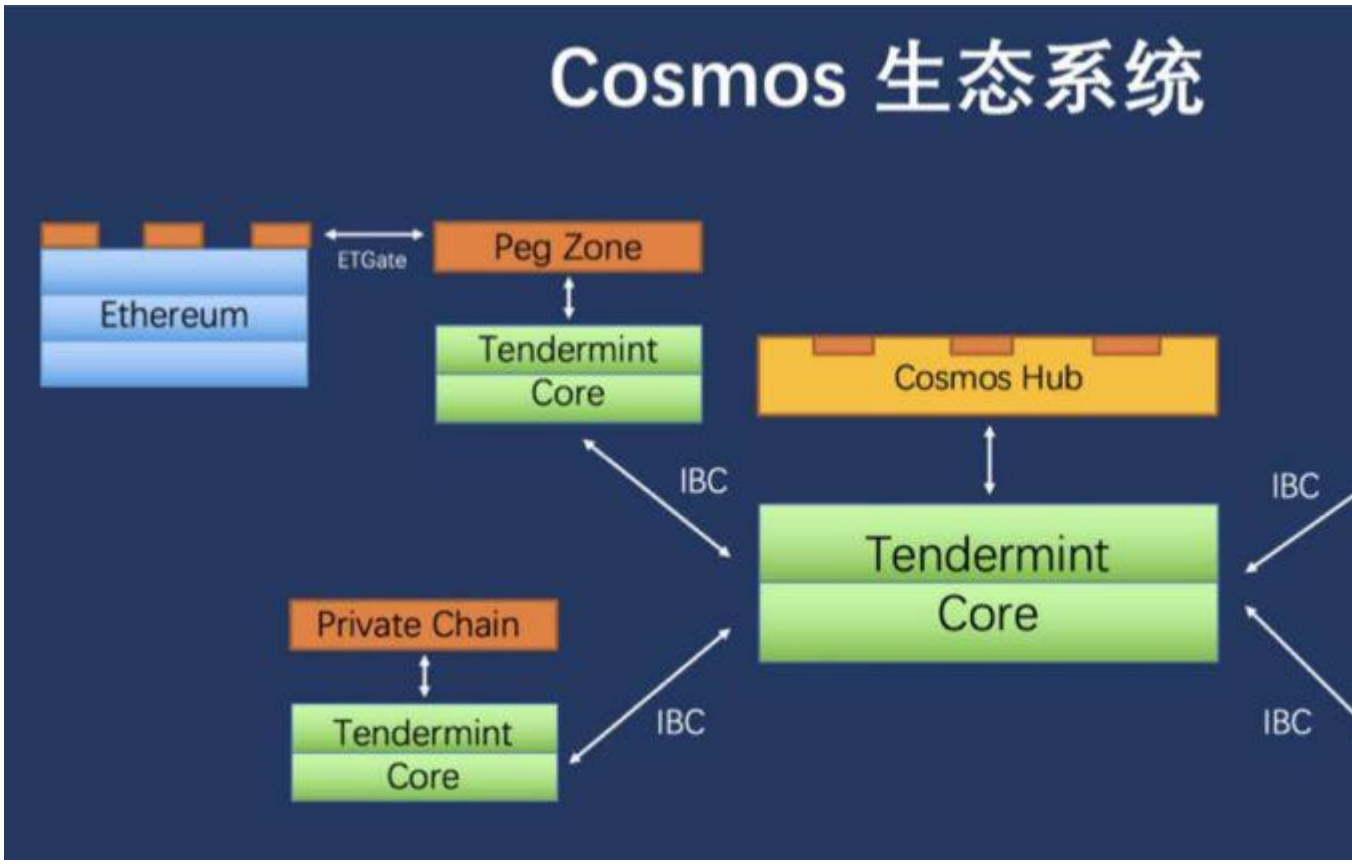
Cosmos SDK 是 Cosmos 团队在做的核心产品，大家能看到它实际上也是采用了相同的 ABCI 应用的架构。它是基于 Go 语言来实现一个简单的区块链。当我们希望实现一个基于 PoS 的一个区块链时需要实现的常见功能：像多代币账户体系、还有就是大家把自己的代币委托给见证人节点，负责共识和出块，还有链上的一些治理。这些常见的一些功能都已经在 SDK 里实现了。



这样呢，如果你用 Cosmos SDK 来实现你自己的区块链，只需要实现一个区块链的应用逻辑。基础功能已经在 SDK 中实现，如果你的应用还需要一些定制化的开发，可以用 Cosmos SDK 里的一个扩展机制。依据 Plugin 机制编写相关的 Plugin。所以 Cosmos SDK 是一个可以快速的开发区块链的一个架构体系。

有了上面这些知识呢，我们就来看一下 Cosmos 这个项目它想做的是件什么事情。这是一个非常抽象的系统架构。在中间的大圈是 Cosmos Hub，我们把它叫做 Cosmos 枢纽。边上的这些每一个小圈儿都代表其他的区块链。这些区块链都会通过互联链的通信协议跟 Cosmos Hub 进行连接。比方说像比特币，还有门罗币、以太坊，另外一些去中心化的交易所的一些链，理论上都是可以连到这个 Hub 上。

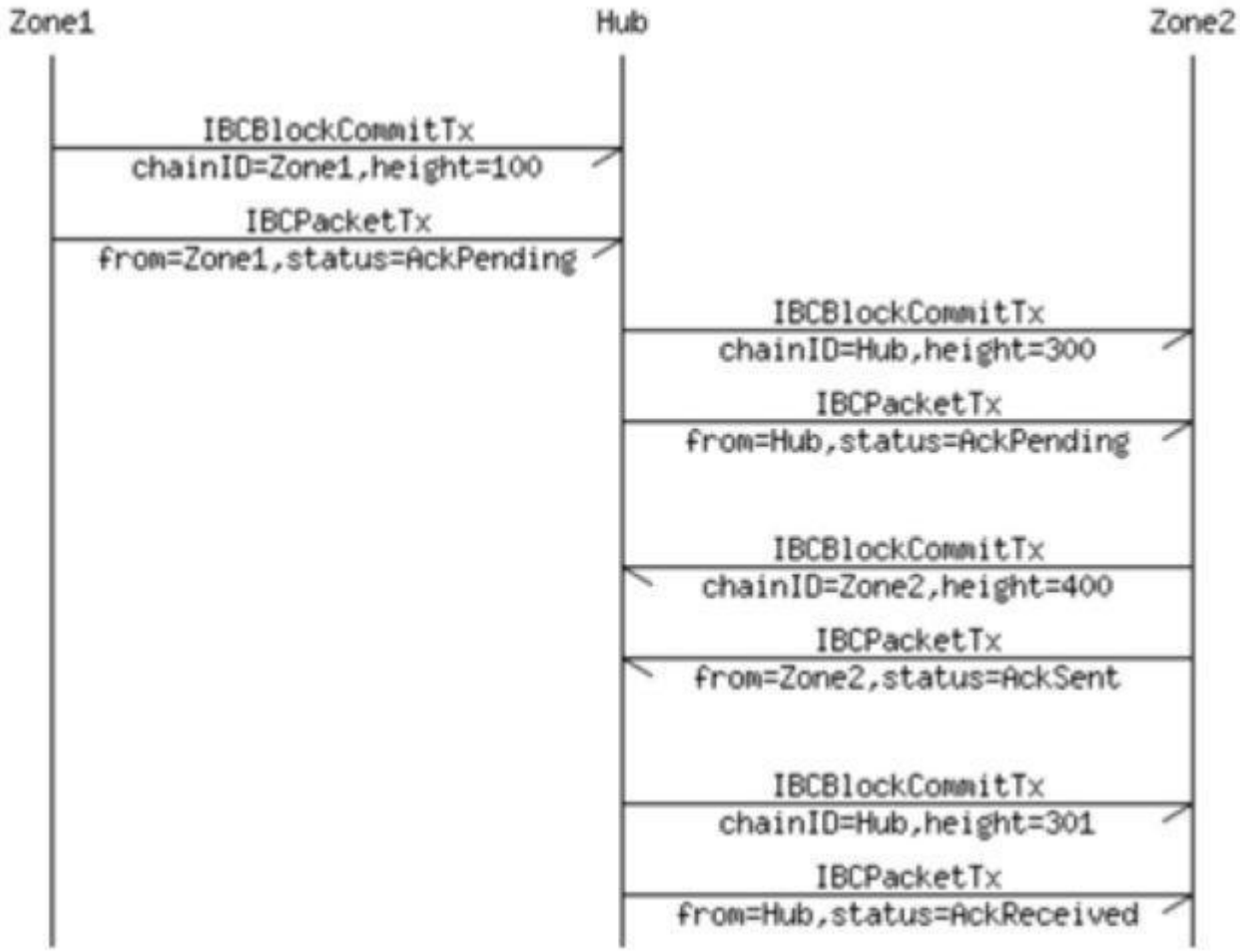
Cosmos 认为将来我们的世界不可能是有一两个区块链所主导的 ,会有比较多的区块链，每一个链都完成它自己特有的功能。我们会将来生活在一个多链多币的世界里。Cosmos 想做的事情就是实现代币转移这样一个基础的功能，以后再加一些扩展的功能，从而组成一个代币经济高度集成的这样一个统一的生态系统。



以上是架构的大概实现。我们如果再深入看一下是什么样子呢？在这幅图中大家能看出来，这些链都是基于 Cosmos SDK。中间实现的区块链叫 Cosmos Hub 就上面概念图里中的那个大圆 ,实际上这里面每一个链每一个地方代表的都是一个区块链，虽然它画的是这个区块链里的一个节点的一个架构。但你可以把它想象成就是几个链的一种组成结构中间的是 Cosmos Hub，边上可以有 Ethermint，还有基于 Tendermint 实现的私有链、许可链，也可以是另外的一

条去中心化交易所公链。对于基于 PoW 的这些链，可以通过一个 Peg Zone 把它们桥接在一起。

大家都注意到了就是在不同的这个链之间连接的地方注释了 IBC，即跨链通讯这样一个协议，这个协议是非常关键的，因为代币的跨链转移就是通过它来实现的。那么下来，我就给大家简单的介绍一下这个 IPC 协议是怎么回事。

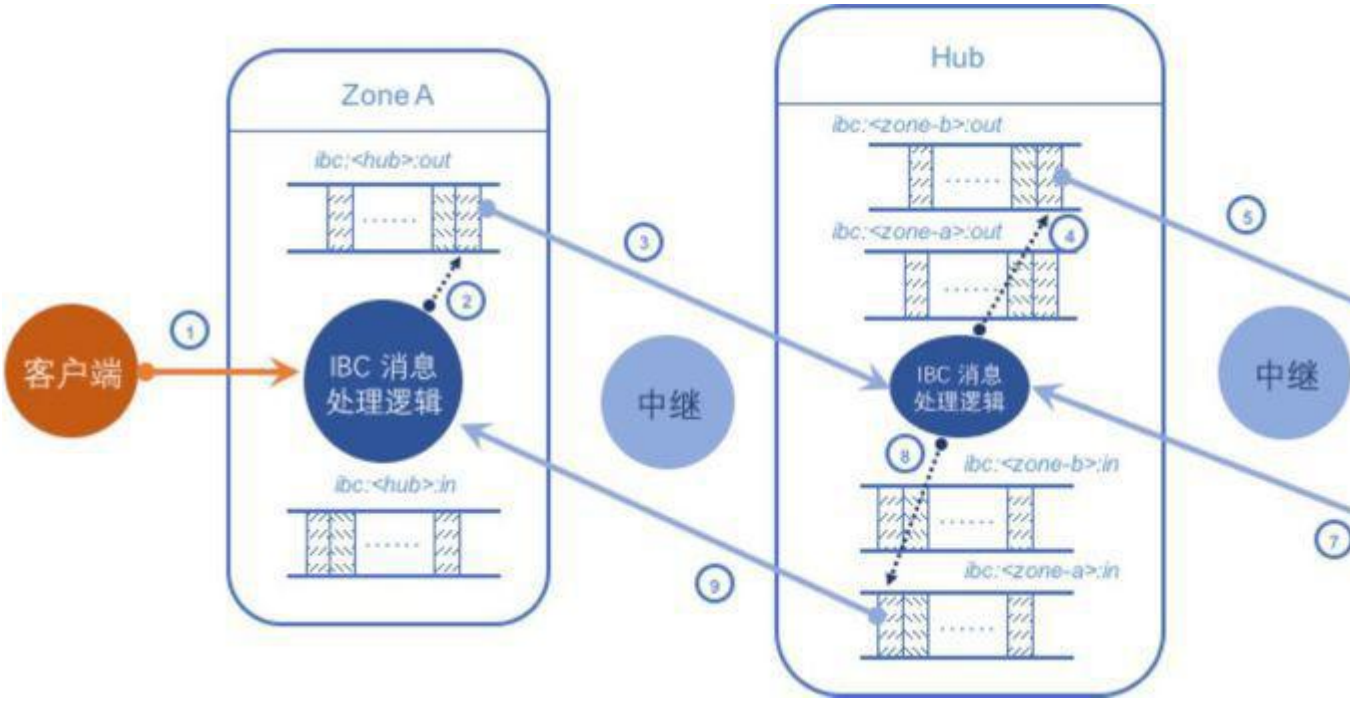


IBC 协议定义了最主要的两个交易类型的数据包。一个就是 IBCBlockCommitTx。它做的事情实际上就是把发起的这条链的当前最新的区块的头部信息传到目标区块链。这样的目标区块链就获得了当前最新的这个链里面 Merkle Root。另外一个包的类型就是 IBCPacketTx。这个就是传递了跨链转代币的交易信息，这个交易信息实际上是在消息体里面实际包含的 payload 信息。这个消息在原链上的一个 Merkle Proof 。

以左边为例，如果把 Zone1 当前最新的一个区块的头传递给 Hub，那么 Hub 就知道它最新的区块的 Merkle Root。当它接着收到一个 IBCPacket 的时候，他就可以利用 Packet 中的 Merkle Root 来验证它所包含的 Merkle Proof 是不是正确的。当然隐含的条件就是这个 Hub 是知道 Zone1 当前有效验证者的，也就是说 Hub 知道 Zone1 所有验证人的节点的公钥。它就可以判断头里面的这个信息是有效的，因为它每一个区块头里面都是由超过三分之二以上的验证人的私钥签名的。

大家看这个图实际上是一个逻辑时序图。那么大家可能就想知道了这个消息是怎么从 Zone1 传到 Hub，以及从 Hub 传到 Zone2，是谁发起的这个消息传递呢，这里实际上就涉及到了一个叫 Relay 的概念，实际上就是在不同的两个区块链之间，它有一个就是独立第三方独立的叫摆渡程序，这个程序负责从原链生成这个

Merkle Proof 然后组装成 Packet，然后把它摆渡到目标链上。具体的这个架构图的我现在给大家贴一下。



这个图稍微复杂一点，我给大家稍微从左到右解释一下，客户端如果想发起一个从 Zone A 到 Zone B 一个代币转移。那它实际上第一步就要构造一个这样的交易，这个交易发到 Zone A 这条区块链以后，Zone A 就对它这个消息进行逻辑处理，主要比方说包括检查发起的客户在 Zone A 里面这种代币有没有足够的数量。如果说是有效的，就到第二步，生成一个对应的把这个交易放到面向这个 Zone 的消息队列里面。这个消息队列在这里面显示的是一个先进先出的队列，但实际上它在这个队列里实现是一个 Merkle Tree 。

第三步中，中继程序作为 Zone A 的客户端，它实际上一直在监控这个队列。当它看到有新的消息进来的时候呢，它就会生成一个 Merkle Proof。然后把这个作为 IBCPacketTx 的 Payload。第三步，把它发到这个 Hub 里面。Hub 对这个消息进行验证，因为 Hub 拥有 Zone A 的当前有有效的所有的 IBCBlockCommitTx 和所有 Validator 的公钥，即得到所有交易的 Merkle Proof。所以它就可以验证收到的这个 Merkle Proof 是不是有效的，如果是有效的，那就第四步：给 Zone B 的 Outgoing Queue 里放一个 Message。

第五步和第三步非常像，就是在 Hub 和 Zone B 之间也有另外一个中继程序，那这个中继程序一样的，它也在监控这个 Hub 里面的队列，当它发现有新的消息进来的时候，它就构造一个这个消息在 Hub 里面的 Merkle Proof。然后把这个消息传递到 Zone B 里面。那接下来呢就是处理的结果就会以收据的方式，按照这个 6789 这样一个过程。这是一个高度简化的一个流程，这里面实际上还有很多技术细节，我们今天不可能展开来讲。但是这个图基本上准确的反映了 IBC 的工作原理。

如果大家还记得我刚才讲的 Peg Zone 的话，如果我们现在想从以太坊把代币传到一个 Hub 里面或者从 Hub 把这个代币传回到以太坊，怎么办呢，那就是要通过一个叫所谓 Peg Zone 机制。我给大家讲一个叫 ETGate 的项目，这个项目是一个叫 Joon 韩国大学生在 Cosmos 黑客马拉松里一个得奖项目。这个暂时没有

以区块链的方式实现它，它只是写了一个网关程序，那这个网关程序做的事情，实际上就是在以太坊和一个 Tendermint 分区里面传递代币。

就是当你要从以太坊发送代币出来的时候以太坊里头会有一个智能合约，这是这个大学生写的一个智能合约，这个智能合约会收到转账请求。收到转账请求的时候，它就生成一个 Event，即以太坊里的一个事件。ETGate 作为以太坊的轻客户端在经过足够的块确认以后提取 Merkle Proof。包含这个 Merkle Proof 证明发到 Tendermint 里，Tendermint 收到了这个交易以后，证明 Merkle Proof 无误以后呢，就算转账成功了。这就是比较简单的过程。

反过来也是一样，Tendermint 分区如果要向以太坊转代币的时候，就会在 Tendermint 分区里发起一个定制的一个转账交易。ETGat 作为 Tendermint 分区的一个轻客户端，它将转账交易的证明发到以太坊智能合约。智能合约验证这个证明无误，算转账成功。当然这个也是有一个前提就是 ETGate 会在以太坊和 Tendermint 分区之间不断的发送两个分区最新的区块头。ETGate 只是一个网关程序，ETGate 如果说加以扩展，很容易实现一个 Peg Zone，但前提是你要对它增加 IBC 协议的支持，这个细节我就不展开了。

基于 Cosmos 这个技术的区块链互联网应该有什么样的特性呢？这个特性有很多，那么我今天就简单讲两个特性，一个是可扩展性，一个是自主性。

它这个扩展性分成垂直扩展性和水平扩展性，垂直扩展性主要是针对单节点，就是区块链里单节点的这个性能处理交易的能力，那么基于 PoS 共识机制大大的改善了垂直扩展性，所以吞吐量 TPS 得到了提升。通过 Hub 加 Zone 的方式通过多链获得水平扩展性。

针对垂直扩展性，Tendermint 团队对 Tendermint Core 做了一些测试。在跨五大洲的一百个验证节点网络上的可以取得每秒超过一百个交易。这个比传统 PoW 来说是大大的提高。

水平扩展性比较好理解，就是在以太坊里面，现在你作为一个全接点，上面几百个上千的 DApps 你都要参与维护它们的状态。但实际上，你也许最关心的时间就是其中的几个应用。这种情况下以太坊的性能，面临的很大的性能瓶颈。所以它现在的一个改善的方式一是迁网，迁到这个 PoS 共识算法。另外一个就是分片。在 Cosmos 中通过不同的分区实现分片，所谓 Zone 就是不同的区块链。按照不同的应用逻辑进行分片的方式。这个水平扩展的分片方式是非常自然合乎逻辑。

另外的就是自主性，自主性也比较好理解。比方说当你这个社区不能取得共识的时候，区块链治理很自然的结果就是分叉。比方说当时的以太坊分叉出来以太坊和以太坊经典。那在 Cosmos 架构上很自然的这两个区块链的就是两个不同的分区 ,这两个不同分区里面它们有自己不同的验证人节点。有不同的出块的速率。不同的性能的设置 ,就是这就很自然地反映了不同的区块链不同的分区就反映了不同的治理特点，因此，这也很自然就是许可链或者联盟链。也是可以在不失自主性的前提下和共有链交互。

自主性还有个好处体现在当一个区块链的社区达不成共识的情况下它不需要通过分叉，它只需要通过增加一个新的分区，在这个新的分区里把一些达不成共识的部分 ,相当于对于这个社区的这个区块链的治理的一些方式给设到这个新的分区里面。用户完全基于自愿的原则把自己的数字资产移到这个新的分区里面。你可以想象在 Cosmos 架构内完全可以跑比方说三个分区：EVM1.0、EVM2.0，还有 EVM3.0。那么大家就各自相安无事，体现一个区块链的自主性。

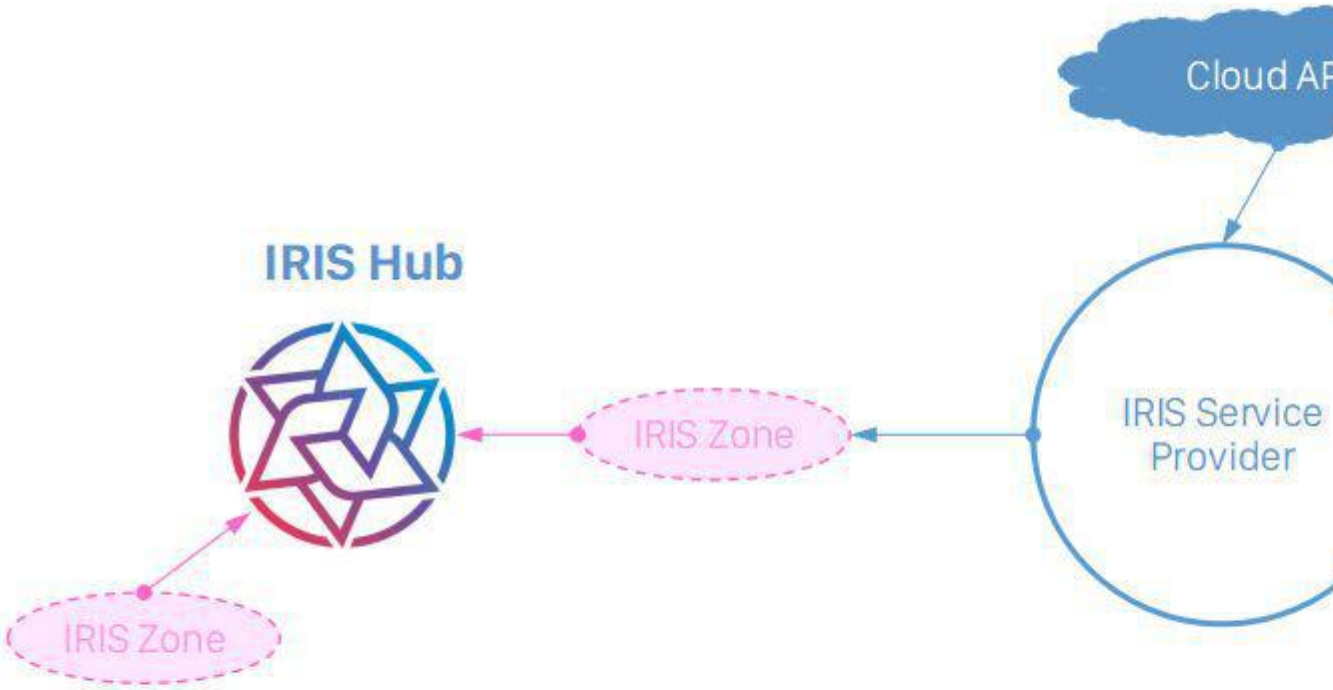
基于 Cosmos 技术以及它的技术特点，我们所说的 Cosmos 团队所设想的一个生态系统 ,大概涉及到哪些使用场景呢？第一个就是我已经提到过的就是去中心化交易所。它可以真正实现跨多种区块链交易的技术平台。比方说现在 Kyber 和 OmiseGo 都决定当 Cosmos Hub 上线后，它们都会接入 Cosmos。这样就

可以不仅仅进行 ERC20 代币之间的交易 ,也可以把一些非 ERC20 代币转移到交易所里进行交易。如果这个真的实现的话呢，应该说可以满足现阶段的刚需的。

Cosmos 团队的另外认为潜在的经济模型就是 :代币不一定只能用原生链。现在大家默认的好像形成一种认知就是一个区块链有一个自己的原生代币 ,那这个原生代币只能在这个链上使用。但实际上 Cosmos 认为未来世界代币和链是可以分离的。一个有价值的货币，比方说像数字代币比特币或者以太币。它完全可以通过跨链转移，转移到一些新的或者其他链去使用。它的使用价值在全网都是一致的。比方说你有一个链，是用于做分布式存储的它可以有自己的默认的原生代币 ,但是完全也可以把以太币或者是比特币转过去作为有价值的一个代币在它的这个区块链里面加以使用。

那最后一个应用就是许可链、联盟链和私有链也是可以通过 Cosmos 这个架构可以与其他的联盟链或者是其他的公有链进行交互。而且还可以想像一下就是现在各国都在推央行的这种数字货币，这个是不可避免的肯定将来会有的。联盟链和私有链一般都没有自己的代币，但实际上它们解决的现实世界中的很多问题。智能合约在运行的过程中都跟经济、金融有关系。如果基于 Cosmos 这样一个架构的话 ,央行的数字货币完全可以通过这样一个架构把它转移到相关的这个联盟链里作为一个稳定货币加以使用。

最后，Cosmos 只能用来做数字代币跨链吗？能不能做一些其他更有趣的事情呢？Cosmos 团队也说了就是现在这个 IBC 协议的只是用来转移代币的，但是它的 IBC 协议的 Payload 里面是定义的扩展机制，理论上它是可以传输其他类型的数据结构，可以做其他的事情。现在像万向的新链加速器投资的边界智能团队就在做这样的尝试。他们想通过基于 Cosmos 实现基于服务调用的跨链。



这就是他们团队做的一个 IRIS 项目。它可以把基于云的服务，基于传统企业系统的一些功能，还有其他公有链或者联盟链的一些功能，以服务的方式提供到 Cosmos 世界上，让大家可以跨链调用这个服务。

最后这个就是关于 Cosmos 的一些信息，谢谢大家。