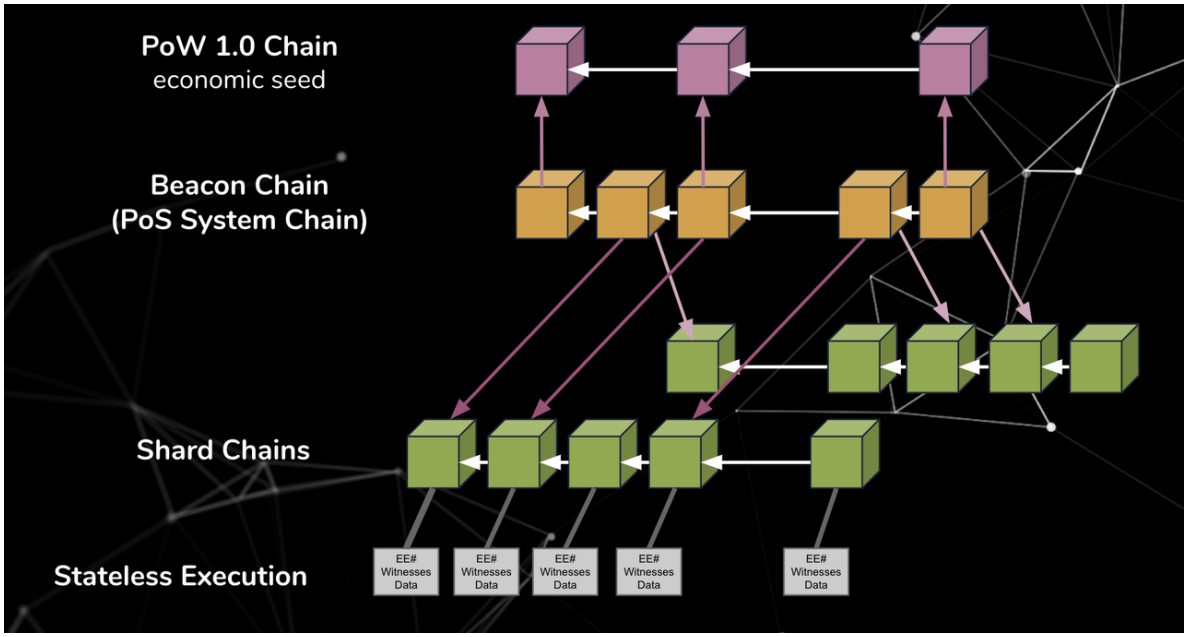
以太坊 2.0 的未来蓝图及挑战

以太坊爱好者 2019-11-11 21:15发布在 区块链 海盗号 37227

-Danny Ryan（来源: Crosslink 2019 Taiwan）-

十月底于台北矽谷会议中心举行的 **Crosslink 2019 Taiwan**，吸引了来自世界各地的区块链爱好者们齐聚一堂。第一天的议程，邀请到了**以太坊基金会（Etherium Foundation, EF）**的核心研究员 Danny Ryan，会中分享了**以太坊 2.0 （Ethereum 2.0）**目前的研究方向以及遇到的挑战，演讲的内容主要包含了以太坊 2.0 的架构，新的分片提案，**执行环境（Execution Environments, EE）**以及**双向桥接（Two-Way Bridge）**等议题。

一、以太坊2.0 的架构



-以太坊 2.0 架构（来源: Crosslink 2019 Taiwan）-

第零阶段（Phase 0）

在**以太坊 1.0 （Ethereum 1.0）**工作证明（Proof of Work, PoW）共识机制（Consensus）权益证明（ *Proof of Stake*, PoS）**

第零阶段会建立**信标链（Beacon Chain）**，信标链就是以太坊 2.0 系统层级的链，当从以太坊 1.0 移转到以太坊 2.0 时，信标链扮演着非常重要的角色，它是整个系统的基础。

一旦第零阶段完成，将会有两个使用中的以太坊链。以太坊 1.0 链（目前所使用的 PoW 主链）以及以太坊 2.0 链（新的信标链）。在这个阶段，使用者在 1.0 链把以太币锁到合约里以注册公钥，2.0 链会承认合约内注册的公钥。但是，他们无法将该以太币迁移回去以太坊 1.0 链上面，为了要执行信标链，你会需要一个信标链的客户端。目前，许多团队正在开发这些客户端。

第一阶段（Phase 1）

第一阶段会加入**分片链（Shard Chains）**

这个阶段分片链会与信标链**交联（Crosslinks）**，每个分片的当前状态— “**结合数据根（Combined Data Root）**”，会定期记录在 “信标链” 区块中，作为交联。信标链区块完成后，相应的**分片区块（Shard Block）**将被视为已完成，其他分片知道它们可以依靠这些区块进行跨分片交易。

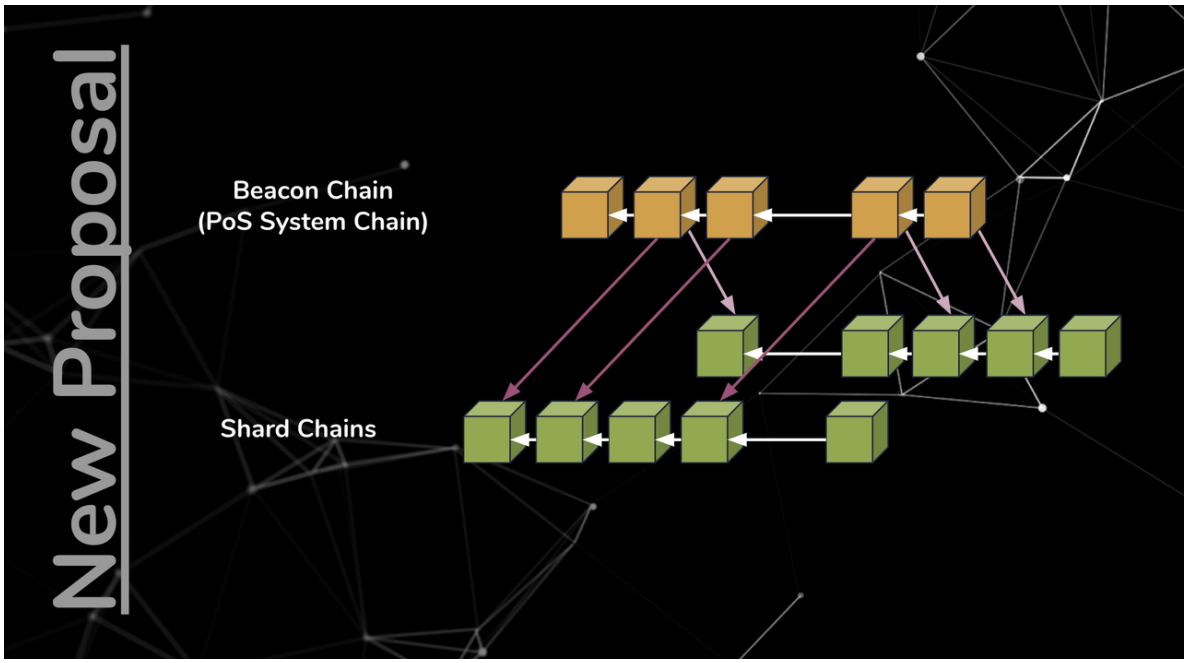
交联是**委员会（Committee）**的一组**签名（Signatures）**，证明了分片链中的某个区块，可以包含在信标链中。交联是信标链 “理解” 分片链更新状态的主要方式。交联还用作异步跨分片通信的基础结构。

信标链在每个**时段（Slot）**中的每个分片，随机选择**分片验证者（Shard Validators）**，分片验证者只是用来在每个区块的内容上达成一致，他们通过交联证明分片的内容和状态，分片中包含什么内容都没有关系，只要所有委员会都达成共识，并定期更新分片上的信标链即可。

第二阶段（Phase 2）

第二阶段会将所有功能开始结合在一起，在第二阶段，会完成分片化，分片链从简单的数据容器过渡到结构化链状态，并将重新引入智能合约。每个分片将管理基于 **eWASM（Ethereum flavored WebAssembly）**

二、新的分片提案



-新的分片提案（来源: Crosslink 2019 Taiwan）-

以太坊 2.0 原提案所运作的机制，是以每个**时期（Epoch）**为单位，来进行交联的动作，每个链上有 1024 个**片（Shards）**，当需要跨分链交易（Tx）时，由于是每个时期进行交联，会有较大的延迟时间；新提案更新为每个时段都进行交联的动作，并减少**片（Shards）**的数量为 32 个，来降低跨分片（Cross-Shard）交易时的延迟时间，每个时段都进行跨分片交易。

新提案的优点

对于以太坊 2.0 新提案的优点，首先新提案的片（Shards）数量由 1024 个降至 32 个，降低了运算的复杂度，因为跨分片时间，从一个 epoch 降到一个 slot，时间缩短的好处，是给 DApp 开发者及使用者更好的体验。在原本以太坊 2.0 的设计中，需要复杂的手续费市场模型与乐观（Optimistic） 解决方案，来实现跨分片交易手续费（Cross-Shard Transaction Fee）。但新提案改变了执行环境的设计，使得原本的复杂模型可以被大幅简化。

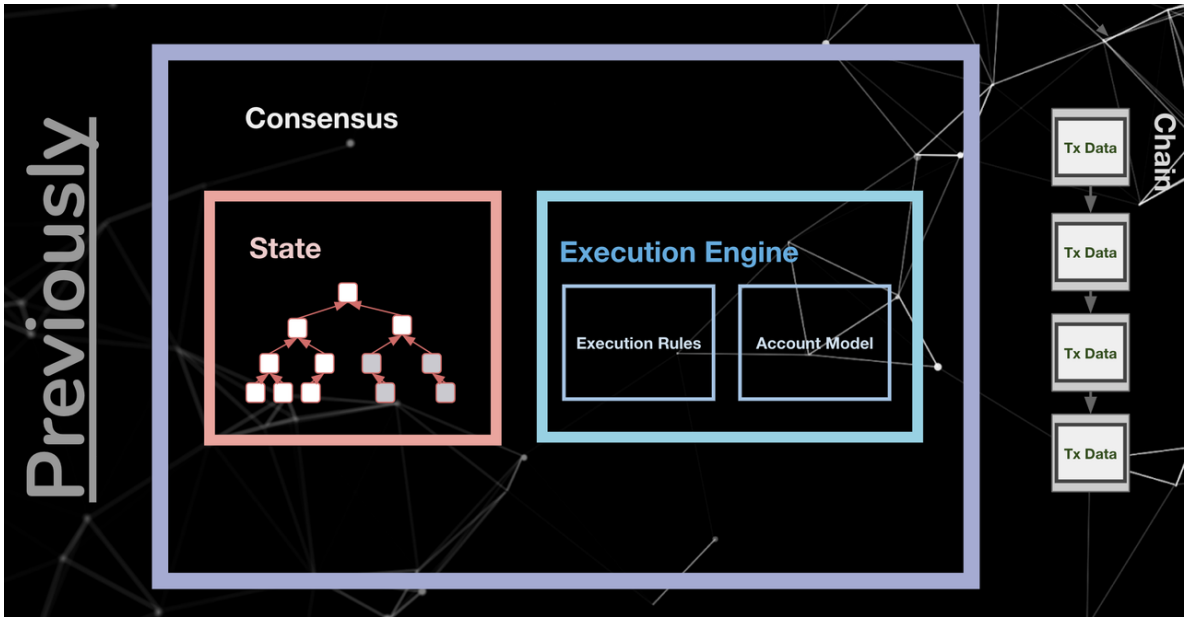
新提案的交易

新提案只需要比之前的提案更少的**片（Shards），****分片区块（Shard Block）**

目前的想法

希望能给开发者及使用者更好的体验，使用较大的分片区块（Shard Block），来改进数据可用性，以及要降低开发延迟和第零阶段发布所需花费的时间。

三、执行环境



-以太坊 1.0 简易架构图（来源: Crosslink 2019 Taiwan）-

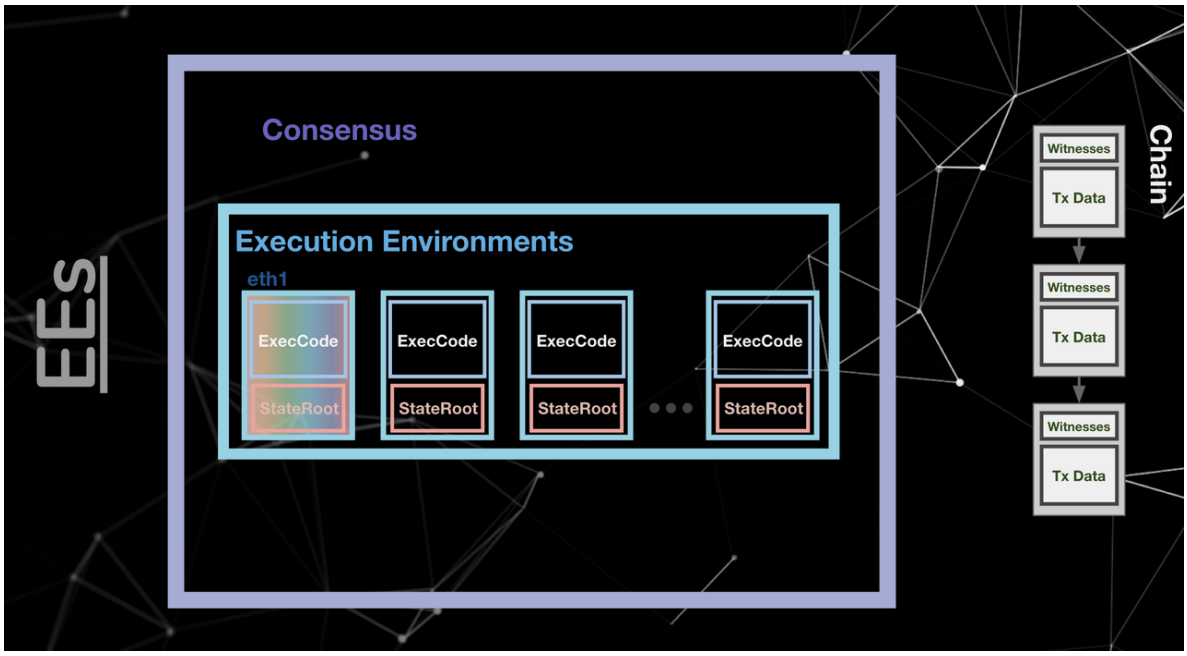
在之前设计的以太坊 2.0 和以太坊 1.0 中，状态在共识机制里，扮演着非常重要的角色，共识机制会随时去读写所有的状态，不管是执行的概念、交易的概念、帐户的概念、树状结构的概念、以及所有在数据结构中的概念，都深深地融入共识中。

上图是以太坊 1.0 的简易架构图，在图中我们可以看到共识机制及一条链，共识机制里包含了状态及一个执行引擎，状态里包含了状态树，在这里的执行引擎使用硬编码规则，里面包含了执行交易、帐户模型和帐户结构，我们可以看到图的右边有一条链，链上面有交易数据，在以太坊 1.0 中，我们会在交易数据上执行共识机制，去修改和更新状态。

执行环境是一个单独的虚拟机器，在以太坊 1.0 中，会有一个特定的**帐户模型（Account Model）**，以及事先定义好的**操作码（Opcodes）**，**矿工机制（Gas Mechanisms）**和**状态根（State Root ）**，以太坊虚拟机（Ethereum Virtual Machine, EVM）就是一种特定的执行环境。

如果遵循 **EIP（Ethereum Improvement Proposals）**的建议，开发者总是在要求新的操作码，或着是更改**矿工成本（Gas Cost）**来支援他们的应用，像是 Plasma 和 Zkrollup 这样的例子有很多，这样就会需要修改 EVM 1.0 的执行环境，才能支援到他们的应用程式（DApp）。

但是在以太坊 2.0 的第二阶段中，我们可以支持多个执行环境。也可以有多个状态根，不同的帐户模型等。举个例子，你可以定义一个脸书币执行环境（Libra EE），以便在以太坊 2.0 上运行Libra。或者，您可以定义一个比特币执行环境（BitCoin EE），这样就可以在以太坊 2.0 上运行比特币。



-以太坊 2.0 简易架构图（来源: Crosslink 2019 Taiwan）-

在以太坊 2.0 简易架构图中我们可以看到状态根，它可能是 32 Bytes 的 Blob，上面有 WASM 的**执行码（Execution Code）**，可以在使用者层级中去做细部设定。图片右边有一个链，链上有一般的交易数据以及见证（Witnesses），见证实际上显示在数据库的区块中，你需要针对该状态而不是数据库执行该笔交易，而且还需要证明数据对于当前状态根是有效的。举个例子，如果我们要在帐户 A 和帐户 B 之间传递数值，假设从帐户 A 移动 5 以太币到帐户 B，我们不能直接说帐户和**余额（Balance）**是确实可用的，在过程中，我们需要加入**见证数据（Witness Data）**，来证明两个帐户当前的状态，当执行码正在执行交易数据时，状态根可以修改和更新状态树。

执行环境并不是共识机制预先定义好的，他可以在使用者层级上去做新增，我们也可以把以太坊 1.0 复制一份到以太坊 2.0 的执行环境中，将现有的状态根放入 EVM 直译器，用**默克尔见证验证器（Merkle Witness Verifier）**来当作他的执行码。

在原先的提案中，状态和共识息息相关，且执行帐户和共识中包含了状态树结构；而在新的提案中，执行环境为**无状态模型（Stateless Model），**高度抽象化的，并且它的可扩展性，相较原先的提案高出非常多。

执行环境的优点

执行环境有许多优点，相较于旧系统，它也许可以更快地将产品推向市场，因为我们不必等到核心共识推出之后，才研究并发展这个概念，在 Layer 1 会有更少的阻碍，它可以在各种应用上，使用具高扩展性及数据可用性的执行引擎，所以未来会长期使用这个核心基础层。

执行环境的设计完成，让以太坊 1.0 到以太坊 2.0 的迁移，有了更清楚的方向，使用执行环境比较不会有技术随时间迁移而过时的问题产生。

执行环境交易

对于执行环境交易，开发者及使用者可能会觉得太抽象，对什么是执行环境感到困惑，像是这一层加了什么？应该在这一层做什么？谁应该写执行环境？而且相关的开发规范会趋向更严格的形式。

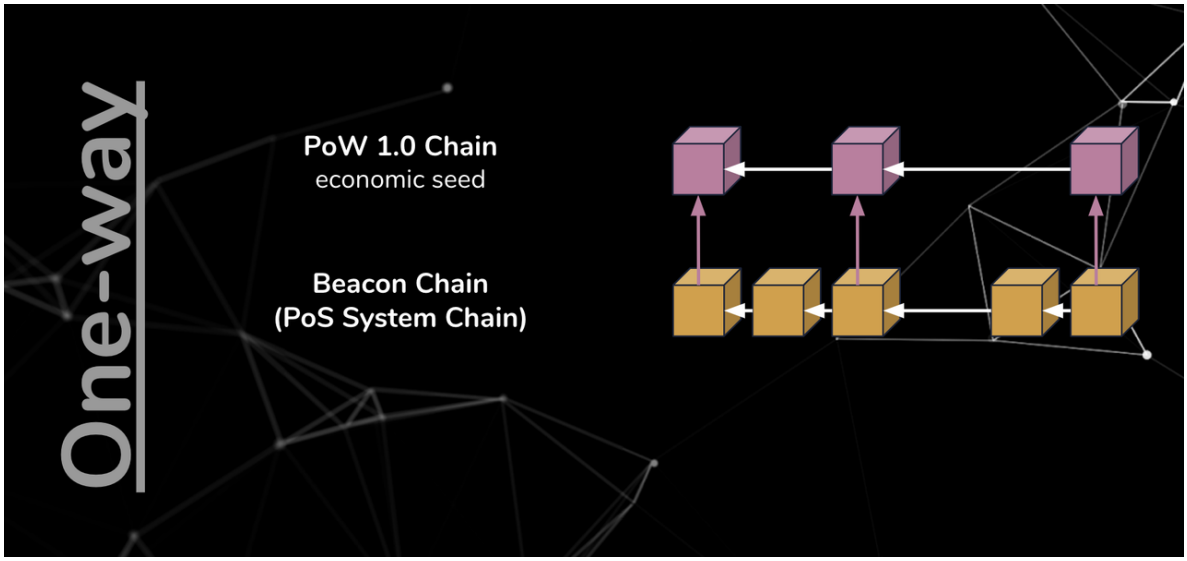
虚拟机可能会有潜在的碎片化问题，进而影响到交易速度。

目前的想法

目前所有的研究都是正向发展的，还有充裕的时间，尝试并更好地了解设计空间，未来会多花一些时间，在建立更好的执行环境通讯机制上面。整体来说，现阶段的进度，对于未来是重要的里程碑。

四、双向桥接

最后一个主题，主要讨论开发双向桥接是否是值得的？团队可能可以在什么时间点，来去做双向桥接？



-单向桥接示意图（来源: Crosslink 2019 Taiwan）-

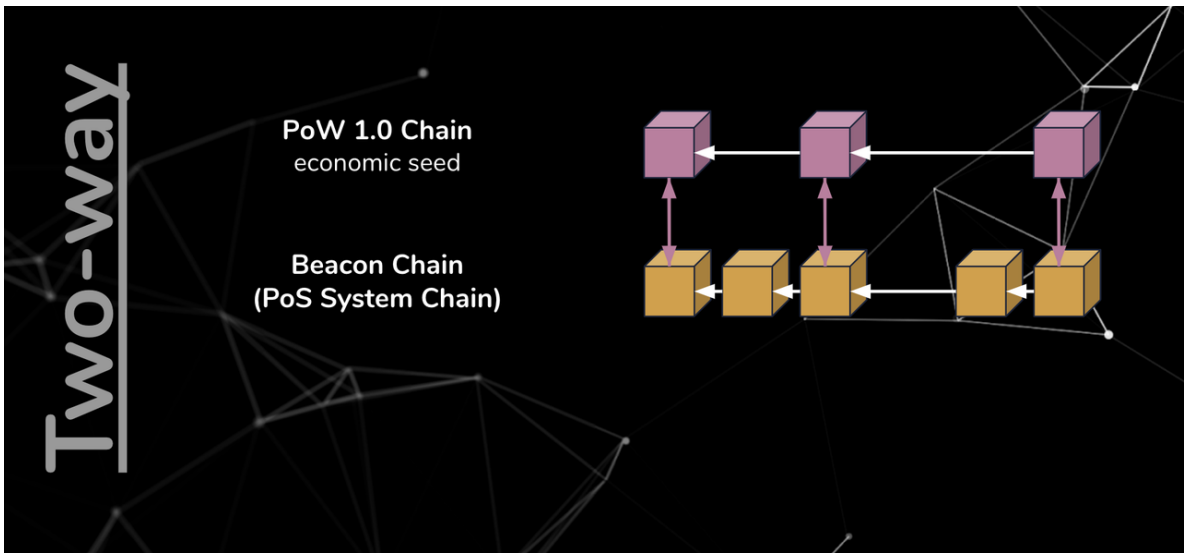
讲者先前提过的提案中，以太坊 2.0 最初有一个单向桥接，所以你可以从以太坊 1.0 转换到以太坊 2.0，但是最初的架构不允许回传，这主要是出于几个原因，这需要我们将以太坊 1.0 的发展与以太坊 1.0 和以太坊 2.0 的硬分叉紧密结合，并把两个系统置于互相影响的风险之中，因此团队认为以太坊 2.0 在发布且稳定之前，将两边紧密耦合是不明智的。

单向桥接的问题

月初在日本大阪举行的 Devcon 5 上，桥接的问题受到了广泛的讨论，原提案的**单向桥接（One-Way Bridge）**

另外也希望鼓励大家，在这些早期阶段进行验证，但是在早期阶段进行验证，肯定会有很高的风险，因为存在未知的锁定期，因此也希望找到方法减轻这种风险。

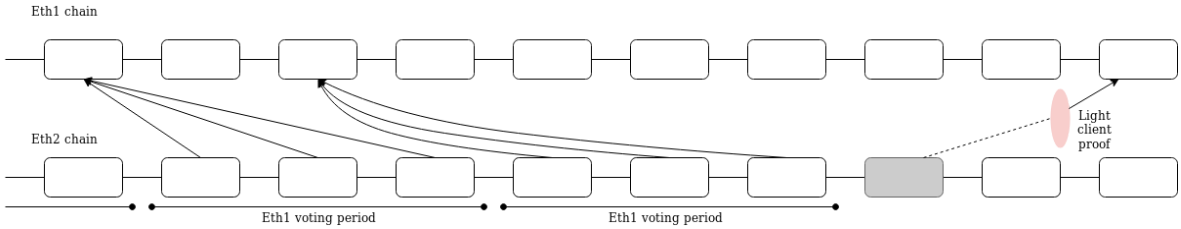
双向桥接



-双向桥接示意图（来源: Crosslink 2019 Taiwan）-

双向桥接目前可能的路线有两条，一种是在以太坊 1.0 上面，建立以太坊 2.0 的轻节点；另一种是在以太坊 1.0 上运作以太坊 2.0 的全节点。

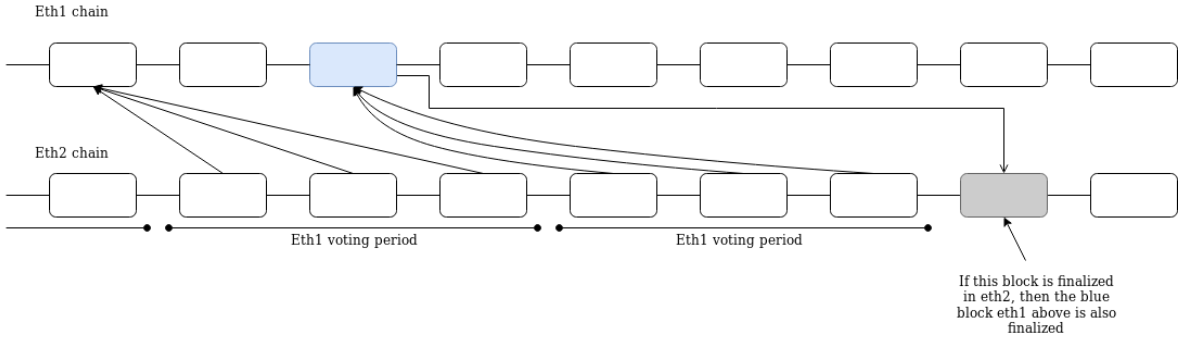
路线 A： 在以太坊 1.0 上，建立以太坊 2.0 轻节点



-路径 A 示意图（来源: Crosslink 2019 Taiwan）-

这个路线需要在实际的 EVM 中支援 **BLS-12–381**，会花费很多开发时间，而且它只提供**轻量客户端（Light-Client）**层级的安全性。当验证者在 2.0 链上产生提款交易的收据时，我们会拿到以太坊 2.0 的轻量客户端证明，一但收收据的区块在以太坊 2.0 上敲定了，你就可以在以太坊 1.0 的合约上提款。不过，这可能不是团队最终选择的路线。

路线 B：在以太坊 1.0 上，运行以太坊 2.0 的全节点



-路径 B 示意图（来源: Crosslink 2019 Taiwan）-

第二种路线，会在以太坊 1.0 的节点上，运行以太坊 2.0 的全节点，这个路线允许我们使用敲定性机制，因此，我们不仅可以使用这种机制，来促进以太坊 1.0 和以太坊 2.0 之间的转移，我们也可以利用验证者的安全性，来保护以太坊 1.0 链，我认为大家对此感到非常兴奋，这通常被称为 “敲定性小工具提案（Finality Gadget Proposal）”。

但是还是需要一种机制，去输出以太坊 2.0 状态根在以太坊 1.0 上，所以有一些以太坊 2.0 社群的讨论，在研究如何实作它，可能会包含矿工机制。

输出以太坊 2.0 状态根的另一个优势，是以太坊 1.0 有稳固的机制可以实现它，以及同时拥有以太坊 2.0 的高扩展性及数据可用性，可以做一些有趣的应用，像是 ZK Rollup 和 Optimistic Rollup。

双向桥接的优点

如果你在交易所中，列出以太坊 1.0 以太币和以太坊 2.0 以太币，它们的价格应该一样。如果不一样，你可以用较低的价格买一个以太币，把他发送到桥上，然后以较高的价格获得另一种以太币，并把它出售。这种套利会使它们的价格保持不变，这样会让用户，验证者和开发人员感到困惑，双向桥接可以防止两边的货币借由套利的形式，来互相转换。

双向桥接的交易

但是还是有一些权衡在这里，尽管对以太坊 2.0 的设计非常有信心，团队还是希望在影响到以太坊 1.0 的安全性和风险状况之前，先在生产环境中得到验证。

双向桥接是一种紧密耦合的共识机制，对于两边链的攻击及产生的问题，都会影响到另一边的链，协定的开发势必会非常烦琐，我们需要考虑到每个协定的安全性，如果我们越早开发协议，那么我们实际上的进度就越少，当每个障碍随着时间发展，它们就会相互阻碍，这让以太坊 1.0 在这一点上的开发速度比以太坊 2.0 慢得多，因为实际用户群存在很多担忧，并且需要大量的协调，才能在我们的生产网络上获得硬分叉。

所以，如果我们越早将这些东西连在一起，就可能会减慢以太坊 2.0 的开发和分叉周期，并且这增加了一些额外的开销，换句话说，验证我们可以链接客户端的开销是相对的。

目前的想法

我们应该会在加入验证者流动性之前启用桥梁，但是会等到第一阶段的产品稳定之后再开放；同样的，有很多相关的研究都在同时进行，这可能会影响到，何时完成这个操作。

名词解释：

1. **EIP（Ethereum Improvement Proposals）**：EIP 是以太坊平台的标准，其内容包含了核心协议的规范，客户端 API 以及合约标准。
2. **epoch**：在以太坊 2.0 中，epoch 指的是时长 6.4 分钟的时间单位，每个 epoch 包含 32 个 slots。
3. **Slot（时段）**：每个时段为 12 秒，不一定每个时段都能产生区块，而 epoch 中最后一个 slot 称为**边界时段（Boundary Slot）**，或称为**检查点**（C **heckpoint**）。
4. **Solidity**：Solidity 是一种合约导向的语言，主要用来开发智能合约。
5. **Consensus （共识机制）**：共识机制是区块链为了在各节点间达成共识，所开发的演算法。
6. **Validator 验证者**：验证区块的节点，由信标链在每个时段（Slot）为每个**片（Shards）**随机产生。
7. **Gas**：交易所需的费用，当 Gas 消耗完时，智能合约会终止并进行 Rollback。
8. **EVM（Ethereum Virtual Machine）**：EVM 中文为以太坊虚拟机，是一种轻量级的虚拟机环境，Eth 1.0 中智能合约的运行环境为 EVM。
9. **Dapp（Decentralized App）**：在以太坊中，基于智能合约的应用都称为去中心化的应用程序，即 Dapp（Decentralized App）。
10. **ether（以太币）**：以太坊的货币名称。
11. **Finality（敲定性）**：「敲定性」是 Casper 中的概念，是一种透过验证者投票，在链上产生不可回朔（Rollback）的检查点的机制。
12. **Libra**：脸书提出的加密货币，预计于 2020 年发行。
13. **Merkle Tree**： Merkle Tree 由计算机科学家 Ralph Merkle 所提出，中译为默克尔树，因为是由哈希函数形成的树。

参考: Ethereum Improvement Proposals

参考: Two-way bridges between eth1 and eth2

参考: Ethereum 2.0 （Serenity） Phases

参考: ethfans

参考: eth2 quick update

感谢 Danny Ryan、Chih Cheng Liang、Juin Chiu、Hsiao-Wei Wang、Yahsin Huang、和 Jerry Ho。

（完）

原文链接: https://medium.com/taipei-ethereum-meetup/eth2-0-roadmap-70e1c23f139f

作者: Frank Lee

本文首发于 Taipei Ethereum Meetup 的 Medium 站，EthFans 经授权转载，为符合大陆读者的习惯，进行了简繁转换并将部分术语改为习惯用法。