以太坊历次协议升级回顾

Once Upon a Time in Shanghai

沙漏时间

2023-04-01

Content

以太坊是什么

社会语言与技术语言
以太坊客户端
以太坊改善提案

- 以太坊是社区运行的保障密码货币Ether及数以千计的去中心化应用的社区运行的技术。—— Ethereum.org
- 以太坊是一套共识协议，以黄皮书作为启动时的技术规范，通过叠加增量实现不断更新，增量的表现形式是以太坊改善提案（EIP）。

以太坊是什么

社会语言与技术语言

以太坊客户端

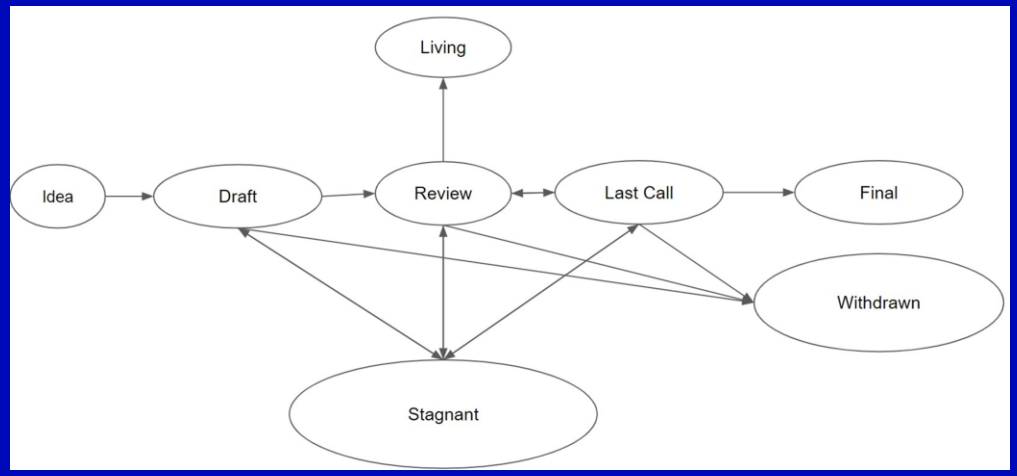
以太坊改善提案

- 如何加入以太坊网络?
  - 以太坊全节点
  - 以太坊客户端
  - 以太坊核心开发者

以太坊是什么

社会语言与技术语言
以太坊客户端
以太坊改善提案

- Ethereum Improvement Proposal
  - 描述了以太坊平台的标准，包括核心协议规范、客户端API、合约标准等。
  - 受 RFC-2119 启发，借鉴了BIP-0001和PEP-0001。
  - 谁能撰写 EIP?



谁定义以太坊

以太坊升级决策
以太坊升级做了什么
以 EIP 为中心的升级流程

- 谁来定义以太坊?
  - 以太坊基金会：注册在瑞士的非营利组织。不控制以太坊，也并非资助以太坊发展的唯一机构，是支持以太坊的机构、个人、公司的大生态系统中的一员。
  - 以太坊核心开发者会议：以太坊最高权力机关，用于决定EIP是否采纳，决定路线图变更等重大事项。
  - 谁是以太坊核心开发者?
  - 我能宣称自己是吗?

谁定义以太坊

以太坊升级决策

以太坊升级做了什么

以 EIP 为中心的升级流程

- 升级意味着什么？
  - 从某个区块开始，引入新的功能、参数调整或安全补丁
  - 所有全节点必须升级客户端，否则无法同步网络，即硬分叉
  - 潜在的安全风险

谁定义以太坊

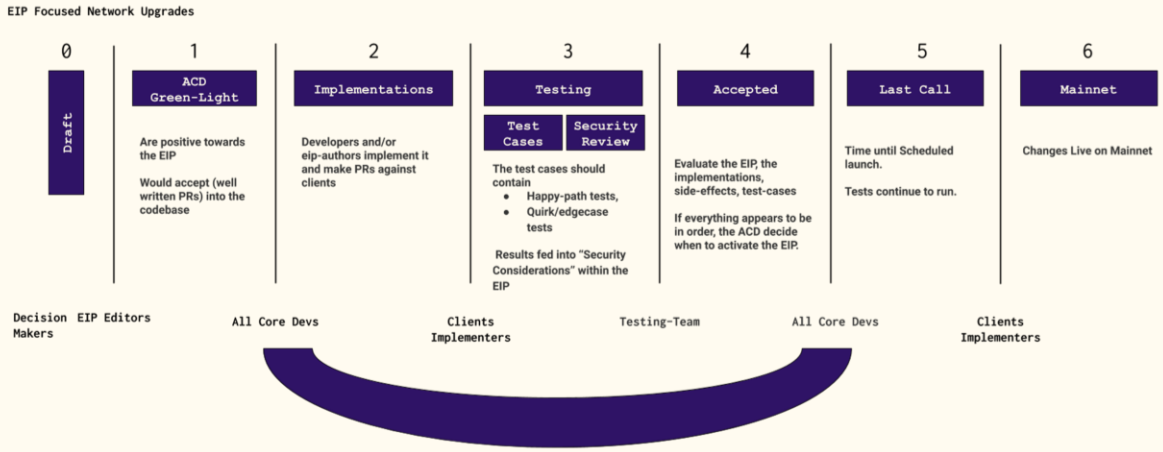
以太坊升级决策
以太坊升级做了什么
以 EIP 为中心的升级流程

Martin Holst Swende 2019-08-08 Source

- Before Berlin
  1. 选择升级时间
  2. 决定升级包含的EIP
  3. 花费大量时间做决定
  4. 可能推迟升级，增加或移除EIP

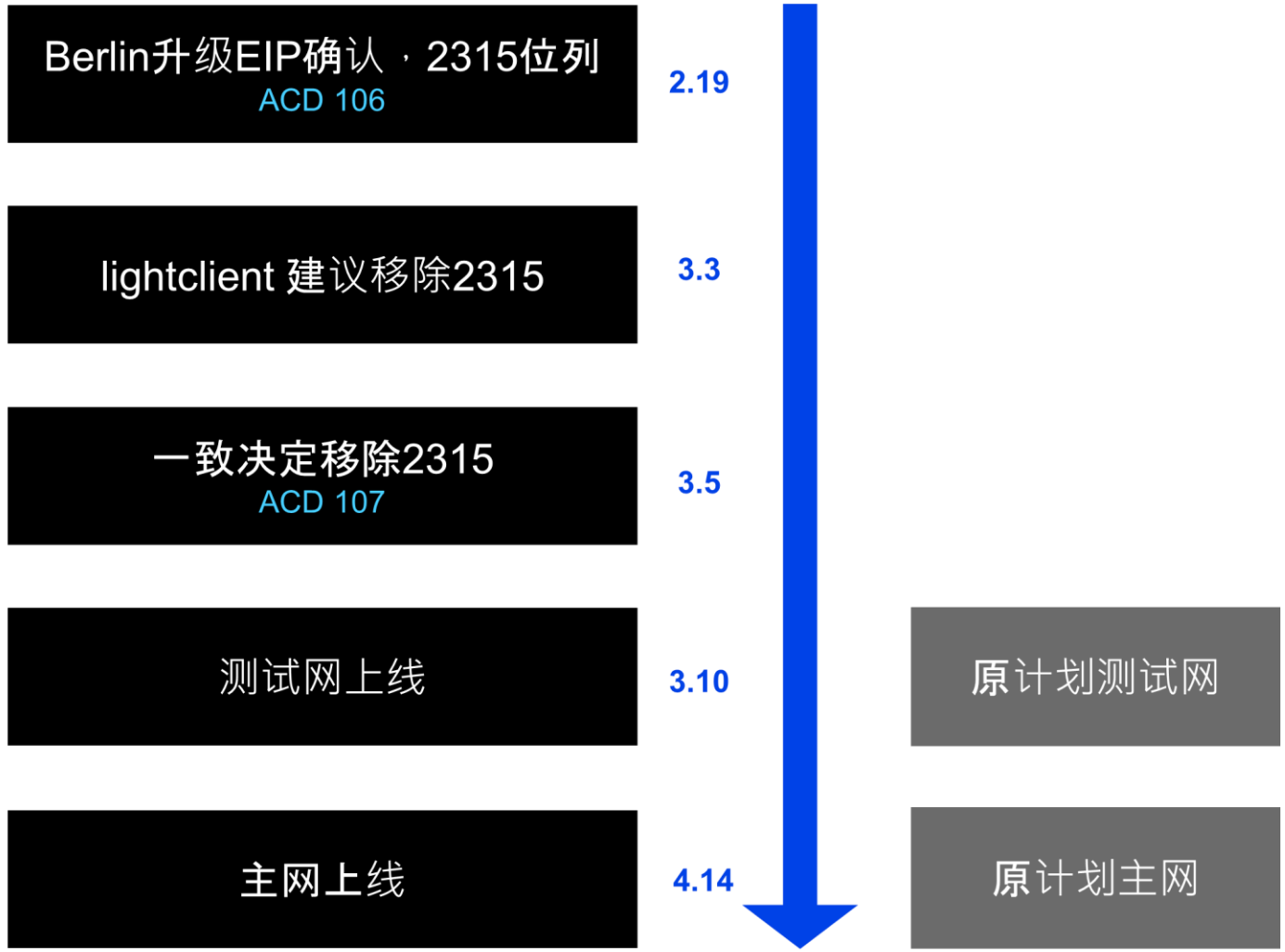
- 大量时间用于讨论什么包含哪些 EIP
- 缺少完整的测试
- 缺少跨客户端测试
- 总体进度被个体影响

- Since Berlin
  1. ACD 初步接受（祝福）一个 EIP
  2. 客户端团队的实现
  3. 测试用例
  4. ACD 最终接受（可同时多个 EIP）



移除 EIP-2315

以太坊柏林升级前的紧急刹车



以太坊升级历史 - 故纸堆中

概览
主动与被动
代表事件
统计数据

- 自 2015 年 7 月30日上线起至『合并』，共进行了 14 次硬分叉，包含 39 个 EIP。
- 间隔最近的两次硬分叉是 26 天，间隔最远的两次则是 490 天。
- Berlin, London, Shanghai 升级的命名来自于举办 Devcon 的城市

以太坊升级历史 - 故纸堆中

概览
主动与被动
代表事件
统计数据

- 硬分叉分为「主动升级」和「被动升级」。主动升级指的是开发团队主动对以太坊协议的修正，而被动升级则是「不得不」采取的行动，以应对潜在的安全性风险。
- 被动升级至少包括 DAO Fork, Tangerine Whistle, Spurious Dragon, Muir Glacier, Arrow Glacier, Gray Glacier，它们或处置黑客盗窃，或应对 DDOS 攻击，或仅仅处置难度炸弹。
- 主动升级大致符合白皮书的规划，Frontier, Homestead, Metropolis，而 Berlin 和 London 则是以太坊路线图变更后的过渡性升级。此外，多次主动升级也包含了推迟难度炸弹的选项。

以太坊升级历史 - 故纸堆中

概览
主动与被动
代表事件
统计数据

- DAO 分叉

  DAO 分叉事件是以太坊发展过程中最为深远的一次事件。由于 the DAO 的智能合约被黑客攻击，约 360 万 ether 被黑客盗走，但有 28 天的冻结时间。

  在这期间，借助 Carbonvote，持币者表达意愿，以太坊基金会决定将这部分资金转移到新的智能合约，允许投资者提款。此次分叉产生了 Ethereum Classic，也引发了大量的社会争论。

以太坊升级历史 - 故纸堆中

概览
主动与被动
代表事件
统计数据

- 上海 DOS

  Devcon 2 期间，以太坊核心开发者们齐聚上海，以太坊网络遭遇网络流量攻击，造成了拒绝服务。由于 EXTCODESIZE 操作码所消耗的实际系统资源远高于攻击者所需支付的手续费，攻击者反复调用该操作码，全网大多数节点无法追上最新区块。

  开发者们协调矿池启用受影响较小的 Parity 客户端，降低区块 gas上限(从 5 M 降低至 1.5 M)。

  借助 Tangerine Whistle 和 Spurious Dragon 两次硬分叉调整了相关操作码的价格，并做了状态清理，才缓解了 DOS 攻击的影响。

以太坊升级历史 - 故纸堆中

概览
主动与被动
代表事件
统计数据

- 双堡奇兵

  为什么在 7280000 高度会有「君士坦丁堡」和「彼得堡」两个分叉。差别在于「彼得堡」移除了 EIP-1283，EIP-1283 会为部分合约引入重入攻击的风险。

  在硬分叉激活前 32 小时，以太坊基金会发文提醒节点升级或降级以推迟君士坦丁堡升级，随后发布新版本引入彼得堡硬分叉，客户端需要将「双堡」配置在同一块高或禁用君士坦丁堡硬分叉。

以太坊升级历史 - 故纸堆中

概览
主动与被动
代表事件
统计数据

- 拆弹危机

  为什么 Muir Glacier 和 Istanbul 两次硬分叉之间只有 26 天，这是因为核心开发者们错误计算了难度炸弹的爆炸时间，导致在 Istanbul 中未纳入推迟难度炸弹的提案。

  等到发现难度炸弹即将要对网络产生影响时，第 76 次核心开发者会议迅速接受了 EIP-2384，并纳入到 Muir Glacier 硬分叉中。

以太坊升级历史 - 故纸堆中

概览
主动与被动
代表事件
统计数据

- 共有 43 人，77 人次参与了这些 EIP 的撰写，其中参与 2 个以上(含） EIP 的作者有 11 个。Vitalik Buterin 参与撰写的最多，共 17 个，占 43.6 %。Martin Swende 和 Christian Reitwiessner 各参与 5 个，Alex Beregszaszi 和 James Hancock 各参与 3 个。
- 在新的硬分叉流程实施之后，EIP 作者的数量发生了显著变化，这或许说明新的流程提高了 EIP 的参与度。Berlin之前，28 个 EIP，43 人次，平均每个 EIP 有 1.54 个作者；Berlin之后，11 个 EIP，34 人次，平均每个 EIP 有 3.09 个作者，增长了一倍。

以太坊升级历史 - 吉光片羽

- 共有 6 个 EIP 在推迟难度炸弹，占 15.4 % 。超过 40% 的ACD涉及难度炸弹的讨论，50%的升级包含难度炸弹。
- 有 2 次硬分叉伴随着经济模型的调整，即降低新区块奖励。其中有 3 次仅为了推迟难度炸弹而实施的分叉，即名字中带有 Glacier 的硬分叉。
- 有关难度炸弹的历史，可见原语里弄的报告。

以太坊升级历史 - 吉光片羽

- 这些 EIP 的作者没有假名或匿名的。
- 以太坊 2.0(The Merge) 的路线图变更并非在 ACD 上得出的，因此没有通过 EIP 的形式表述。

原语里弄
PRIMITIVES LANE

Thanks

Tribute to the golden times of ethereum