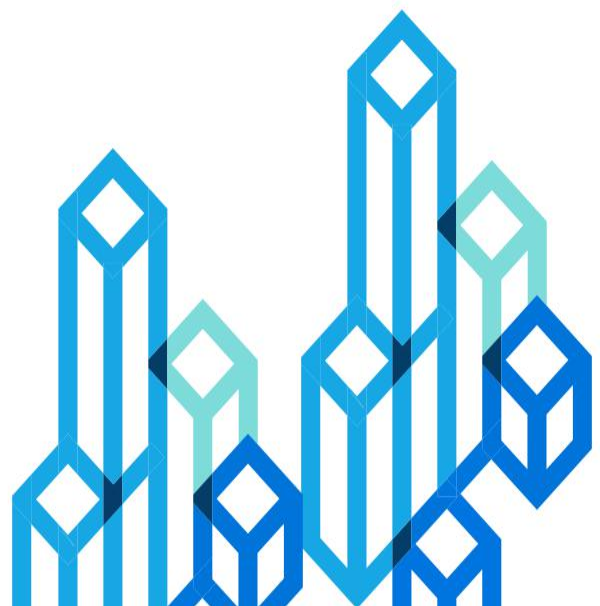
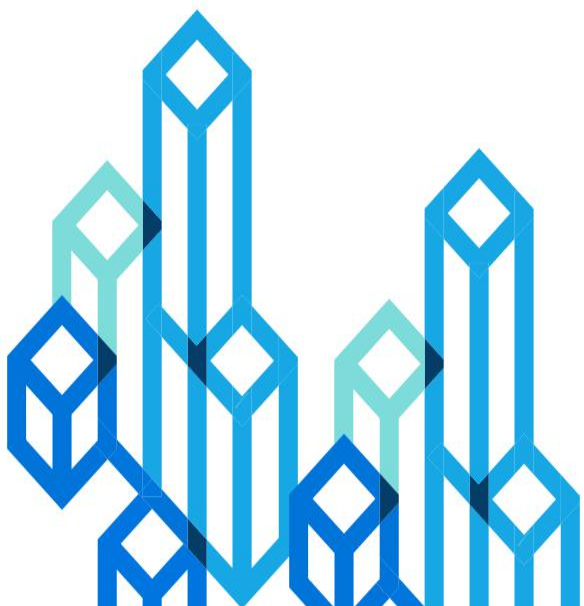


以太坊状态管理提议

又快又好是可能的吗？

姚翔

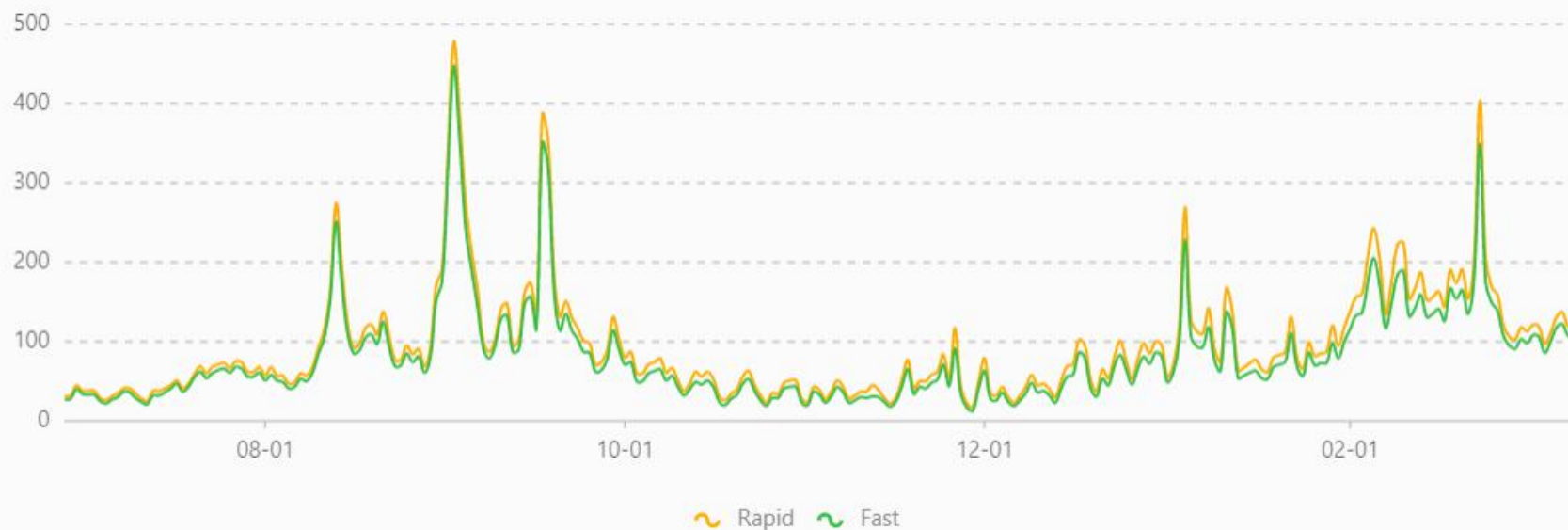


1. 状态管理：扩展以太坊
2. 四种解决方案详解
3. 社区驱动的技术研究

为什么以太坊这么拥堵？

Historical Gas Price

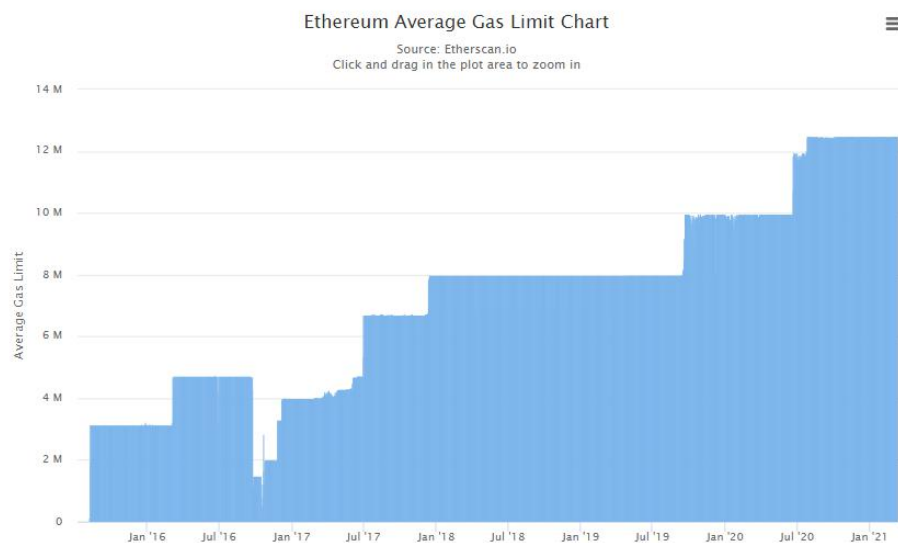
☒ Filter 1 day ▼



* Rapid/Fast: the arithmetic average value of the median/lowest gas prices of all the blocks mined within a given interval

直观的扩容方案（过去6年的主要/唯一方案）

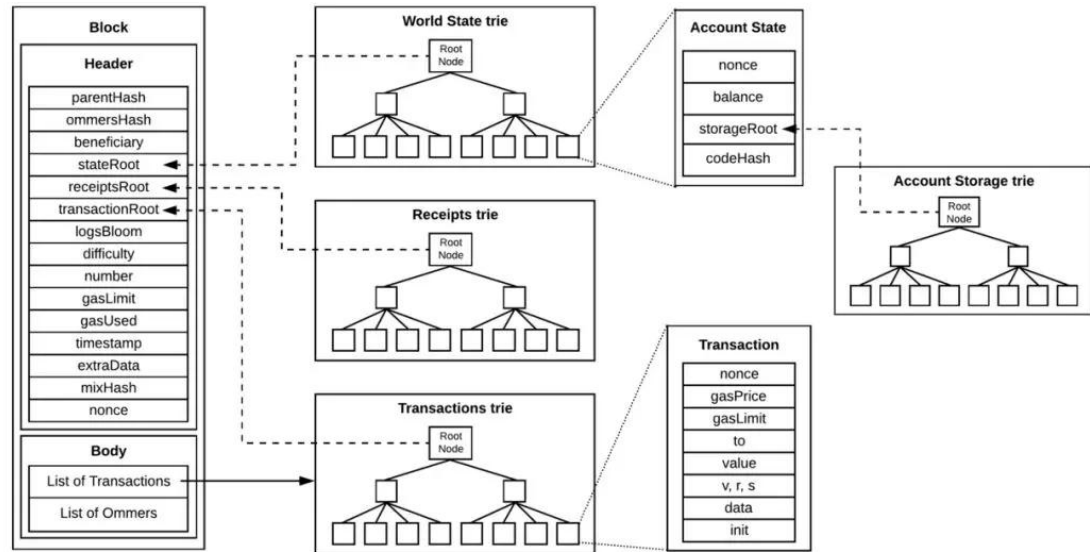
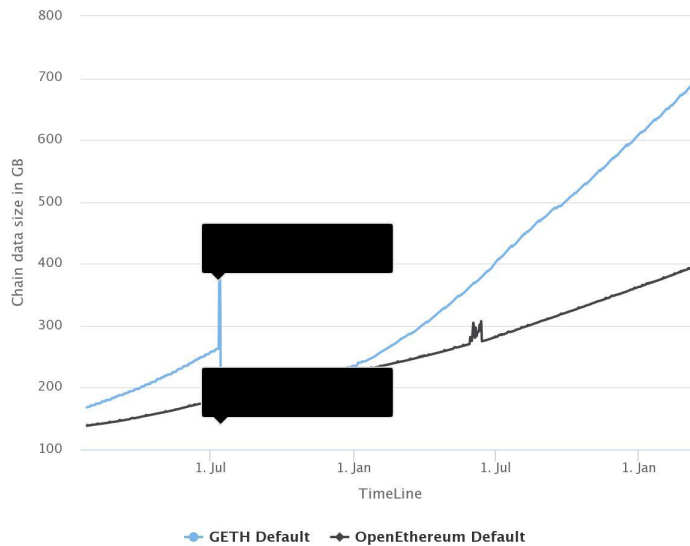
- 提高单位时间内的计算资源
 - 提高区块大小 12.5m
 - 降低区块间隔 13s
- 某公链
 - 大小：30m gaslimit
 - 间隔：3s
- Why not?
 - 带宽
 - 时延
 - 状态



以太坊有多大？

Ethereum Full Node Sync (Default) Chart

Source: Etherscan.io
Click and drag in the plot area to zoom in

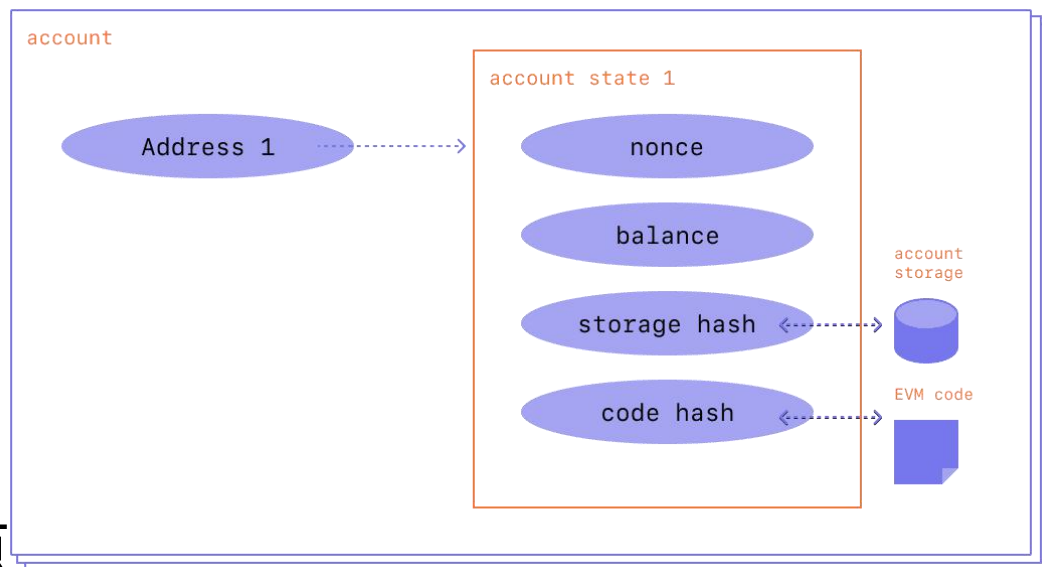


- 原则：个人笔记本电脑可以启动全节点，并独立转发、验证以太坊的所有事务。
 - 节点的硬件门槛不能太高（计算、存储、带宽）
 - 新节点能在较短时间内同步到最新高度

2019/07/10: i3.2xlarge AWS EC2 instances (8 core, 61 GiB RAM, 1.9 TiB NVMe SSD)

Version	Sync time	Disk size	Disk reads	Disk writes
Geth v1.8.27	6d 15h 30m	341GiB	28.9TiB	21.8TiB
Geth v1.9.0	6d 8h 7m*	303GiB	40.2TiB*	32.6TiB*

- 状态是什么
- 什么行为会增加状态
 - 部署新合约
 - Token转移
 - 写入新数据.....
- 状态爆炸的后果
 - 普通人无法运行全节点
 - 以太坊的集中程度加剧



- 根本原因：
 - 这些操作只需事务的发送者一次性缴交按 gas 用量来计量的手续费，但会给整个网络造成永久的持续性成本，因为节点需要存储这些新数据（而未来加入的节点也需要在同步过程中下载这些数据）。
 - 这是系统设计中的一个显著的失衡，可能会让以太坊系统变得越来越难用，因为状态中充斥着不再有用处的“垃圾数据”。
- 解决方案：
 - 无状态客户端
 - 状态过期

- 1. 架构设计优化
- 2. 经济模型优化
- 3. 工程实现优化
- 4. 思想预期优化

解决方案 — 架构设计优化

思路：

设计新的全节点类型，让其无需保存全部状态也可以参与网络。



潜在方案：
无状态客户端



实现方式

每个区块增加“见证”数据，可验证状态转移的有效性。

- 彻底改造路线图.....
- 无状态客户端用途有限
- 在Eth2前不会实现
- 开发资源欠缺
- 需要研究和开发团队

Complete revamp of the “Stateless Ethereum” roadmap

Eth1.x Research



pipermerriam

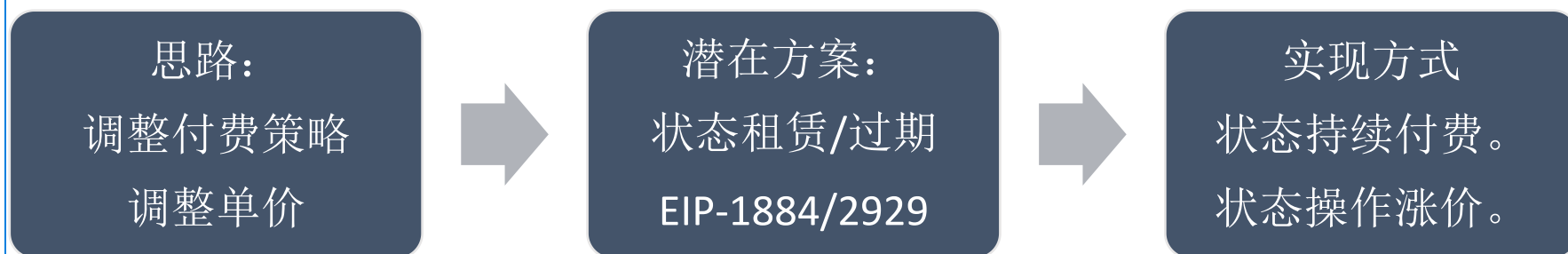
1 Jan 29

The “goal” of “Stateless Ethereum” is to modify the protocol such that we can have stateless clients which do not store the *state* and instead, use witnesses to execute and verify new blocks.

The current “Stateless Ethereum” roadmap can be loosely summarized as:

1. Use binary trie and code merklization to reduce witness sizes.
2. Modify the core protocol such that block witnesses are created and gossiped
3. Stateless clients use block witnesses for stateless block execution.

I am going to make a case that this roadmap is fundamentally flawed and that we’re unlikely to deliver on our goal of having clients that do stateless block execution.



- 状态租赁
 - EIP-1682 撤销
 - EIP-2026/2027/2029/2031 草案
- 调整价格
 - 提高存储状态数据的gas单价，分开冷热存储
 - EIP-1884 实施 造成部分合约不可使用
 - EIP-2929 实施 在London使用

- 好的动机 \neq 好的结果
- Gas Token
- EIP-3298:移除Gas Refund机制

在以太坊网络中，针对经济模型的攻击存在了近两年。该攻击手法最早由帝国理工的两位研究人员发现，并和以太坊开发者一起完善，通过EIP-1884/2929/2930的实施，减少了这一风险。该修复过程被隐藏在两次大的版本升级中，以避免黑客利用。

攻击的方法主要是利用随机访问存储数据，导致区块执行时间过长，大部分节点需要长达几十秒的时间来执行交易，因此无法同步区块链。

```
jumpdest    ; jump label, start of loop
gas          ; get a 'random' value on the stack
extcodesize ; trigger trie lookup
pop          ; ignore the extcodesize result
push1 0x00   ; jump label dest
jump         ; jump back to start
```

•10M gas exploit
using **EXTCODESIZE**

•Parity : ~50s

•Geth : ~38s

•Post-berlin, no
snapshots, 25M gas: ~3.1
s

•Post-berlin, with
snapshots, 25M gas: ~0.3
s

https://blog.ethereum.org/2021/05/18/eth_state_problems/

思路：

通过软件优化提高节点处理事务效率，提高gaslimit的安全阈值。



潜在方案：
Turbo Geth



实现方式

优化数据库结构，
利于全节点“验证”
而非“出块”

- Turbo Geth
 - 可以用来作为全节点，但还不能作为出块节点
 - 效率是Geth的7倍（实际测试结果）
 - 团队宣称：10倍
 - Vitalik：3倍

思路：

妥协：所有验证节点可以访问隐式状态来验证区块中的事务是有效的，且状态根哈希符合区块的执行结果



潜在方案：
reGenesis



实现方式
定期重启，清理状态数据

- reGenesis
 - 仍在研究中
 - 可能是较为务实的解决方案
 - 增加了社会共识的成本

方案对比

方案	思路	优点	缺点	进展
无状态客户端	更改交易验证模型	根本性解决问题	依赖密码学，工程难度大，无法向前兼容	调研中
经济模型优化	提高访问状态数据的成本	可行性高，工程改动小	持续性的治理成本 增加系统复杂性和不确定性	已应用
软件优化	提高软件性能	完整的兼容性	优化空间有限	开发中
reGenesis	定期重启区块链	工程难度小，效果立竿见影	增加社会共识成本	调研中

- Nervos
 - 用经济模型约束状态数据的大小
 - 当前流通量决定了状态数据的上限
 - 区块链维持稳定可控的增长速度
- Mina Protocol
 - 状态数据不再作为共识的一部分
 - 所有计算都在链外完成，区块链只验证提交的零知识证明
 - 区块链维持恒定大小

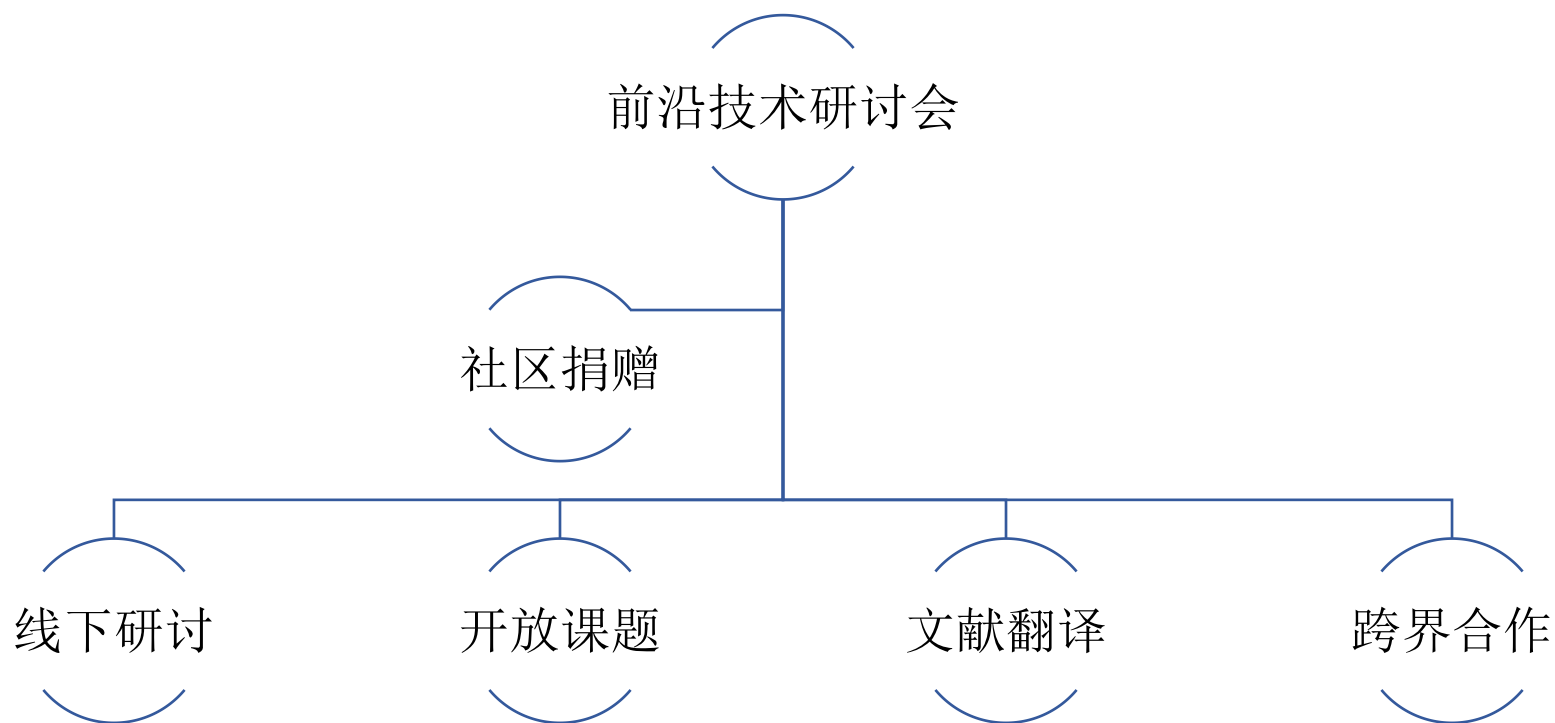
上海前沿技术讨论会（原语里弄）

原语里弄是聚焦前沿技术发展的非营利社区，致力于探索底层技术的发展路径，进行基础公共课题研究及应用。通过线下研讨、课题研究等形式，为行业提供公共技术讨论平台，推动行业内深度交流，并提高行业在社会中的影响力。

成立一年来，累计举办 **12** 次研讨活动，累计 **40** 场主题分享，涵盖密码学、DAO、Layer 2、互操作性等主题。在研课题 **6** 项。

参与协办以太坊全国行-已在**6**个城市进行。





聚焦有意义的区块链基础课题，旨在探索技术与应用及行业生态的相互作用，并提升公众对公共性问题的理解。

原语里弄将给予研究者研究资料、专家建议、写作技巧、研究经费、交流平台等基础支持。

课题研究

尼克·萨博对以太坊的“粉转黑”

2021

作为“智能合约”的提出者，萨博如何看待智能合约平台的发展？

难度炸弹

2021

难度炸弹的有点和潜在的风险是什么？爆发时背后又存在怎样的问题？

Layer2/跨Layer2的MEV

2021

探究针对Layer2的MEV提出的现有方案及MEV对Layer2的影响等。

ZCash考古

2021

考古ZCash的诞生与发展历程。

GasToken考古

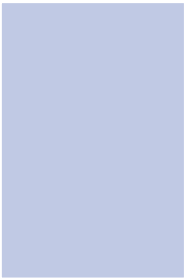
2021

考古GasToken的产生背景及影响。

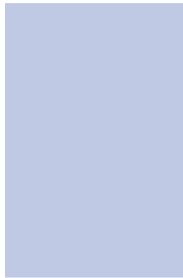
病毒与Memes研究

2021

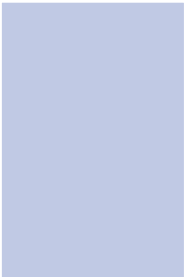
探究病毒与模因之间的发展与联系。



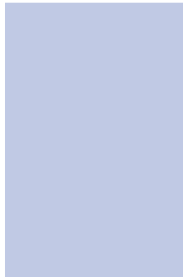
状态问题制约了以太坊的可扩展性



目前有四类方法解决或缓解状态问题



其它公链也在底层做出了不同的设计



社区推动的研究有助于公共基础设施的搭建

谢谢

