



# 区块链： 一种自带开源基因的技术

演讲者：秘猿科技首席架构师 宁志伟

China Open Source Conference 2017

2017中国开源年会  
CHINA OPEN SOURCE CONFERENCE 2017  
立足开源治理 · 胸怀全球社区



# 目录

CONTENTS

01

区块链

02

拜占庭容错

03

Ethereum

04

CITA



# PART01

区 块 链



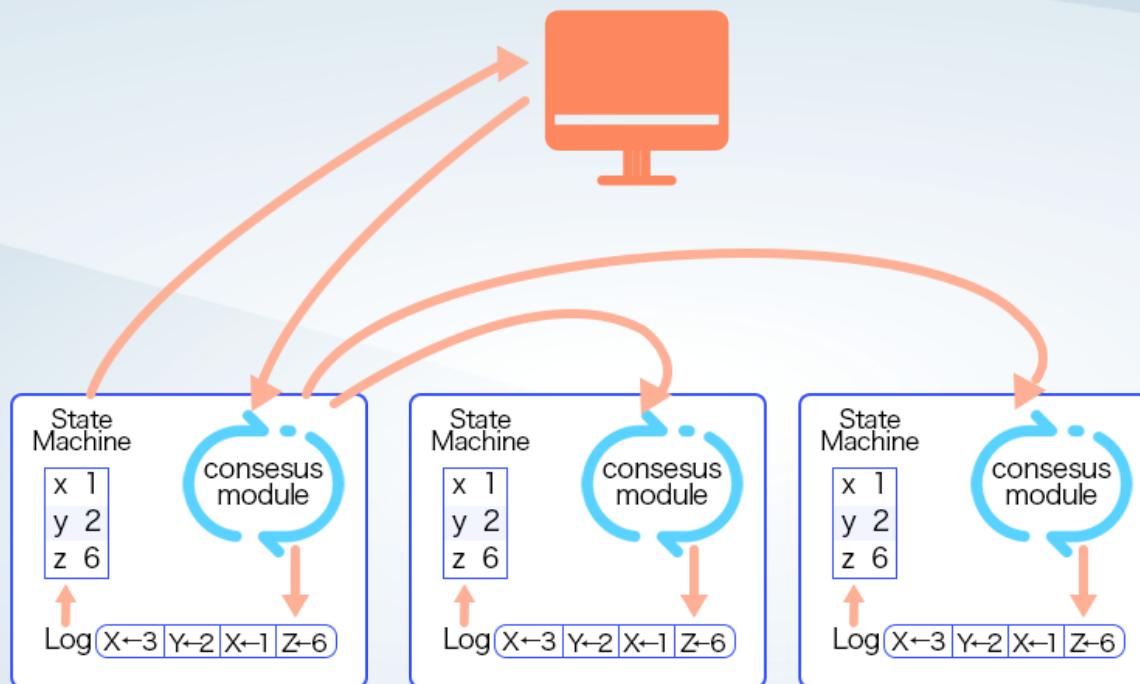
# 什么是区块链

众筹  
比特币  
博弈论  
挖矿  
先知  
账本  
莱特币  
智能合约  
去中心化  
以太坊  
莱特币  
莱特币  
加密货币  
经济激励  
区块链  
治  
交易所  
密码学



# 什么是区块链

- 拜占庭容错的复制状态机 BFT-SMR



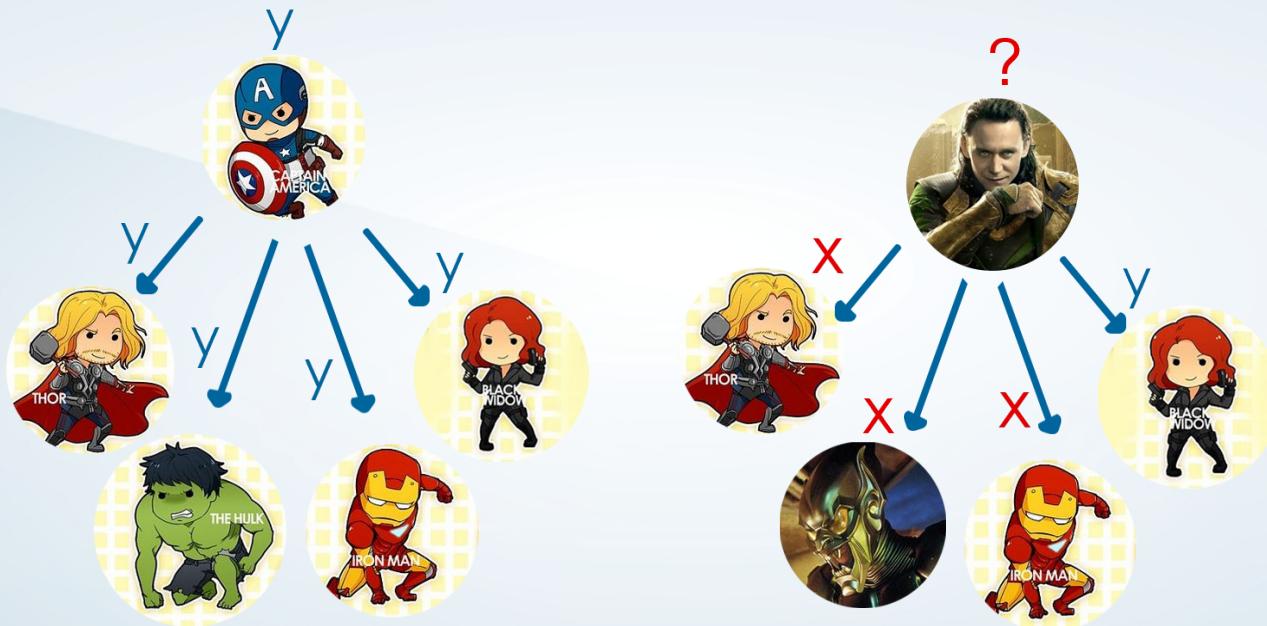


# PART02

拜占庭容错

# 拜占庭容错

- 拜占庭将军问题（分布式一致性）
- Paxos Raft
- PBFT POW POS





# 故障独立

- 硬件
  - 存储要采购多种品牌的硬盘
  - 双相供电
  - 多个网络出口
- 软件
  - NASA 火箭控制系统：三个团队分别独立实现



# PART03

E t h e r e u m

---



# Ethereum

- 以太坊 (Ethereum) 是一个开源的有智能合约功能的公共区块链平台

The screenshot shows the GitHub profile for the Ethereum project. It features the Ethereum logo and a link to the website. Below the header, there are two navigation tabs: 'Repositories 125' (highlighted in orange) and 'People 34'. The main area is titled 'Pinned repositories' and contains three cards:

- go-ethereum**: Official Go implementation of the Ethereum protocol. Metrics: Go, 8.6k stars, 2.7k forks.
- cpp-ethereum**: Ethereum C++ client. Metrics: C++, 1.8k stars, 1.2k forks.
- EIPs**: The Ethereum Improvement Proposal. Metrics: 1.2k stars, 293 forks.



# 以太坊客户端

- 以太坊黄皮书
- 多种语言实现  
(python/Go/C++/Rust/Java/Haskell/Javascript/Ruby)
- 被攻击/出 bug 切换客户端



# EEA 企业以太坊联盟

- 企业应用
  - 隐私性
  - 安全性
  - 扩展性
- 许可链





# PART04

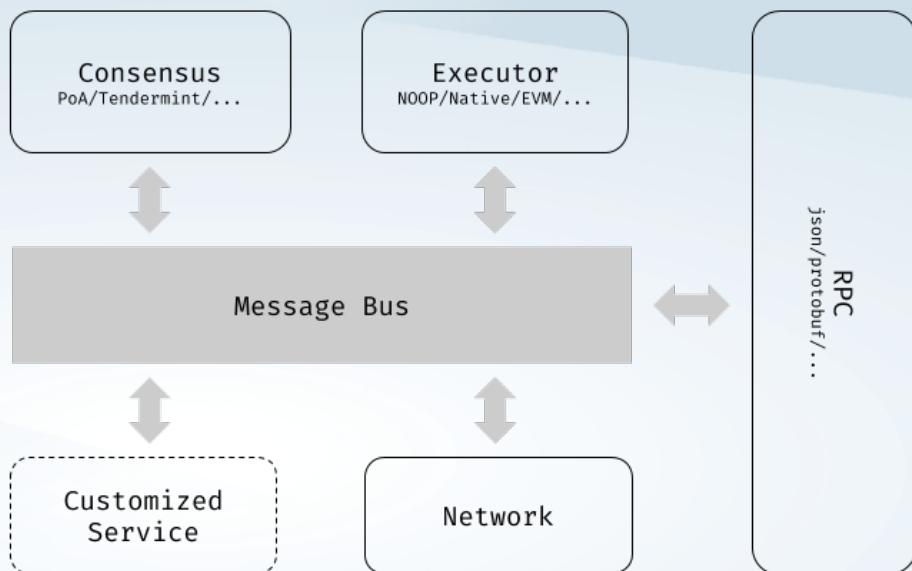
C | T A

---



# CITA

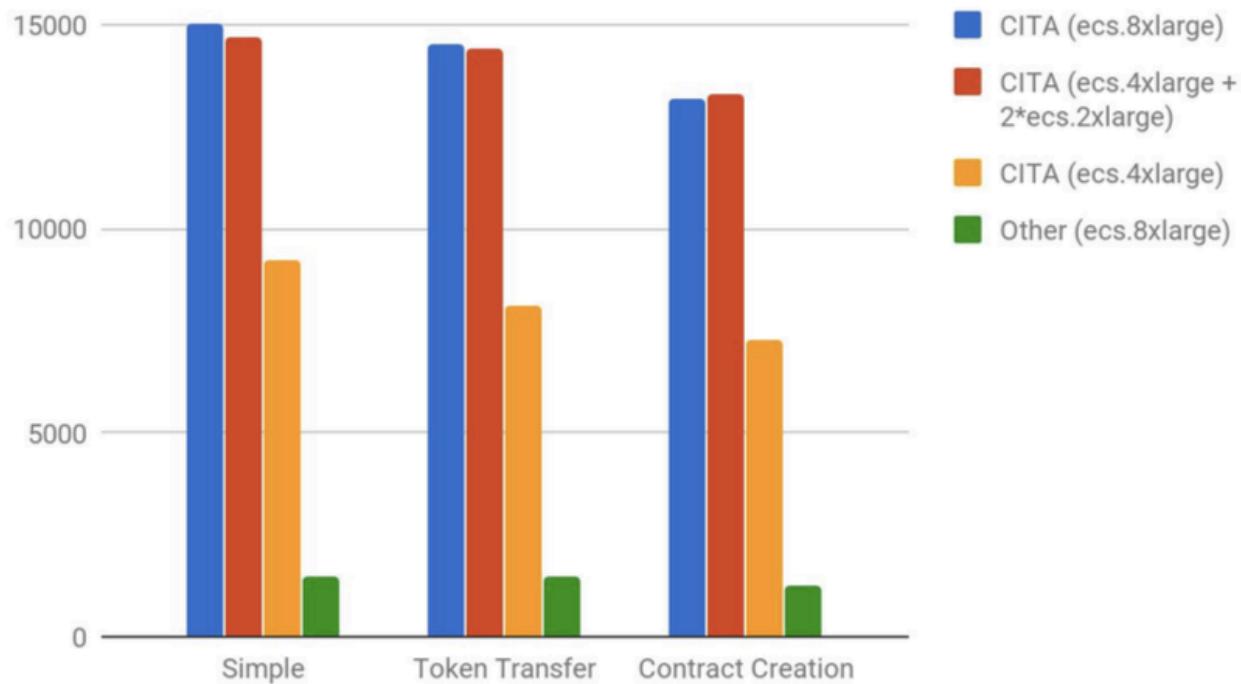
- 微服务架构
  - 逻辑节点
  - 异步交易执行
  - 原生合约
- Rust





# 性能

Throughput (in TPS, 10 logical nodes, 3s block finalization)





# CITA

- 成员管理
- 配额管理
- 隐私交易
  - 局部共识
  - 密码学/可信硬件
- 系统治理交易
  - 操作留痕
  - 状态可变





# 开源

- [github.com/cryptape/cita](https://github.com/cryptape/cita)
- [github.com/cryptape/cita-whitepaper](https://github.com/cryptape/cita-whitepaper)
- [http://cita.readthedocs.io/zh\\_CN/latest/](http://cita.readthedocs.io/zh_CN/latest/)
- DockerHub
- 动手训练营



# 合作单位



现在支付：





# 感谢您的聆听



演讲者：宁志伟  
[rink1969@cryptape.com](mailto:rink1969@cryptape.com)