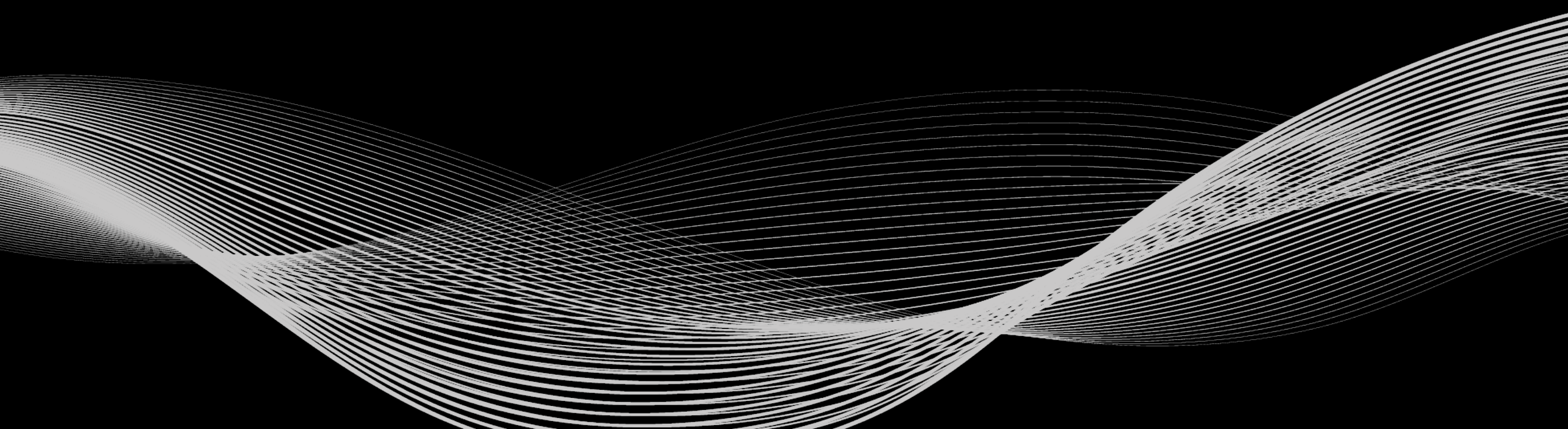
Substrate 快速入门与实战

讲师：Bryan



一块链习

第八节课

下一步

下一步：安全性

- 去中学化的项目需要更加严格的安全性要求和需要更高的代码质量

- Substrate帮我们解决了很多问题，但是我们还是要保证我们的代码是安全的

下一步：安全性

- 架构安全，协议安全
- 代码安全
- 攻击抗性
  - DoS 拒绝服务攻击
  - 暴力破解攻击

安全性：架构安全和协议安全

- 有安全漏洞的架构或者协议则意味着这个项目是从根本上不安全的
- 例子：
  - EOS的架构就是中心化的架构
  - 任何只基于短信验证的协议都是不安全的

安全性：代码安全

- 代码审查
- 代码规范
  - Parity style guide: https://wiki.parity.io/Substrate-Style-Guide
  - Any panickers have a proof or removed
    - 避免 unwrap
    - 使用 expect(“proof; qed”) 来证明

安全性：攻击抗性

- 好的区块链项目必须要由很好的攻击抗性
- 没有不透风的墙，也没有无漏洞的软件
- 攻击成本 > 攻击收益 = 相对安全
- 攻击成本 < 攻击收益 = 绝对不安全

一块链习

代币经济学

代币经济学

- Polkadot: http://research.web3.foundation/en/latest/polkadot/Token%20Economics/
- DOT
  - 质押
  - 治理
  - 交易费
  - 平行链插槽的租用

代币经济学：交易费

- 维持网络安全性和稳定性
- 控制最低攻击成本
- 链上资源消耗要和基本交易费成正比

代币经济学：交易费

- 交易模块实现：https://github.com/cennznet/cennznet/tree/master/prml/fees
- 交易费模块的初步设计讨论：
  - https://github.com/paritytech/substrate/issues/1515
  - https://github.com/paritytech/substrate/issues/1993
  - https://github.com/paritytech/substrate/issues/2910
- 如何测量合理的交易费用：https://github.com/paritytech/substrate/issues/2431
- 通过交易费控制区块大小：https://github.com/paritytech/substrate/issues/2430
- 合约模块的接口复杂度分析：https://github.com/paritytech/substrate/blob/master/srml/contracts/COMPLEXITY.md

安全性：攻击抗性

- hashing 哈希函数的选择
  - blake2
    - 安全
  - xx / twox
    - 高效

下一步：治理

- 一个完美的，绝对安全的网络是不可能存在的
- 治理机制来保证未来的发展
- 平行链可以拥有自己的自治机制，或者利用波卡主链的议会
- 测试时可以用 Sudo 模块
- https://wiki.polkadot.network/docs/en/learn-governance

波卡与跨链

波卡与跨链

- 波卡生态中的部件
  - Relay Chain 中继链
  - Parachain 平行链 / Parathread 平行线程
  - Bridges 转街桥
  - 独立链

波卡与跨链

- 节点的类型
  - Full node 全节点
  - Light node 轻节点
  - Validator node 验证人节点
  - Collator 收集人
  - Fishermen 钓鱼人

波卡与跨链

- Validator node 验证人节点
  - 存在于独立链或中继链
  - 同时是全节点
  - 负责共识
    - Block authoring 出快 (Aura / Babe)
    - Block finalizing 确认区块 (Grandpa)

波卡与跨链

- Collector 收集人
  - 存在于平行链或者平行线程
    - 同时是平行链或者平行线程的全节点
    - 负责接收交易，打包出快
    - 新的区块发送给中继链的验证人确认
      - 平行线程确认区块需要由收集人使用DOT作为手续费竞拍
    - 由平行链自己决定如何奖励收集人

波卡与跨链

- Fishermen 钓鱼人
  - 存在于平行链或者平行线程
  - 同时是平行链或者平行线程的全节点
  - 负责监听并且验证新的区块
  - 防止收集人作恶
  - 质押DOT发起质疑
  - 质疑成功会得到被惩罚的收集人一部分质押资金作为奖励

波卡与跨链

- https://wiki.polkadot.network/docs/en/learn-parachains
- https://wiki.polkadot.network/docs/en/learn-parathreads
- https://wiki.polkadot.network/docs/en/maintain-index
- https://research.web3.foundation/en/latest/polkadot/ICMP/

Kusama 金丝雀网络

Kusama 金丝雀网络

- 不是测试网的测试网
- 所有POS网络的安全性都依赖于经济体系的完善
- 一个没有真正价值的测试网是无法测试经济体系的
- Kusama是一个希望拥有波卡 1% 价值的网络
- 是一个低成本，但是真实的试验场
- https://kusama.network

Substrate 目前的缺陷

Substrate 目前的缺陷

- 没有原生支持 Atomic Transaction 原子交易
- 不可分割
- 要么完全成功，要么完全失败，中间状态对外不可见

Substrate 目前的缺陷

- buy_kitty(owner, buyer, kitty_id)
- transfer_kitty(from: owner, to: buyer, kitty: kitty_id)
- transfer_money(from: buyer, to: owner, amount: amount)

Substrate 目前的缺陷

- buy_kitty(owner, buyer, kitty_id)
- ensure_owner(owner, kitty_id)
- transfer_money(from: buyer, to: owner, amount: amount)
- ensure_transfer_success
- transfer_kitty(from: owner, to: buyer, kitty: kitty_id)

Substrate 目前的缺陷

- 先验证合法性，然后执行交易
- 一旦数据被写入，就不能失败
- 原子交易和批量交易：https://github.com/paritytech/substrate/issues/1791
- 撤回机制：https://github.com/paritytech/substrate/issues/2980

Substrate 目前的缺陷

- 模块使用的自定义数据类型必须在前端重复定义
- 不够完善的Metadata元数据系统
- 包含了类型名称，但是没有类型的构成
- 没有命名空间，容易名称冲突
- 代码臃肿，一旦没有同步就会有隐性bug

Substrate 目前的缺陷

- 我对这个问题的解决方案：https://github.com/paritytech/substrate/pull/1328
- PolkadotJS 端的实现
  - https://github.com/polkadot-js/api/pull/678
  - https://github.com/polkadot-js/api/pull/712
- type-metadata
  - https://github.com/type-metadata/type-metadata

Substrate 目前的缺陷

- 数据迁移升级
  - 旧版本
    - struct Kitty([u8; 16])
  - 新版本
    - struct Kitty { dna: [u8; 16], birthday: BlockNumber }

Substrate 的未来

Substrate 的未来

- 平行链的支持：https://github.com/paritytech/cumulus
- 更多的可能性
- 与其他经济体系的交互
- 跨链财产的转移
- 与其他链上dApp的交互

Substrate 的未来

- 更友好的开发环境
- 更完善的Metadata机制
- 更完善的SRML模块
- Substrate DAO: https://github.com/polkaworld-org/SubstrateDAO
- 波卡标准提案：https://github.com/w3f/PSPs
- 一键发链：https://console.onfinality.io

Substrate 的未来

- 智能合约
  - srml-contracts：https://github.com/paritytech/substrate/tree/master/srml/contracts
  - ink!：https://github.com/paritytech/ink

Substrate 的未来

- 丰富的生态圈
  - Stablecoin 稳定币
  - DEX 去中心化交易所
  - DeFi 开放式金融
  - 智能合约平台
  - 应用链
  - 对接现有网络的转接桥

一块链习

THANK YOU!

Contact us:
info@yikuailianxi.com