

区块链的匿名性和开放性

- 蚂蚁链《区块链系统开发与应用》A认证系列课程



课程 目标

- 了解区块链技术的匿名性
- 了解区块链技术的开放性



课程 目录

01 区块链的技术特征

02 匿名性

03 开放性

04 总结

01 区块链的技术特征



区块链的技术特征

匿名性

开放性

可追溯

不可篡改

分布式共治

数据完整性

自治性

集体维护

不可抵赖内容

02 匿名性

什么是匿名性

匿名性存在的争议

匿名性的级别



02 匿名性

什么是匿名性

匿名性存在的争议

匿名性的级别



什么是匿名性

匿名性的定义

- 匿名性是指个人在去个性化的群体中隐藏自己个性的一种现象。
- 区块链的匿名性主要是指个人数字资产的匿名化，或者是个人在区块链上行为（交易）的匿名化。



匿名性存在的争议

匿名性与KYC

- 区块链因为匿名性在保护用户隐私的同时也为一些违法犯罪行为提供了“保护伞”。
- **KYC**——Know your customer（了解你的客户）是反洗钱且预防腐败的基础政策。



匿名性的级别划分

匿名性的级别划分为基础级、高级和极致级

- 基础级：如果知道转账记录背后的人，即可查询所有的转账记录及资产
- 高级：即使查询到地址背后的人，也无法知道所有的转账信息
- 极致级：只有持有私钥才可以查看对应地址的交易行为

基本级

——链上资产的匿名化

高级

——交易的匿名功能

极致级

——不可查看他人的交易信息

03 开放性

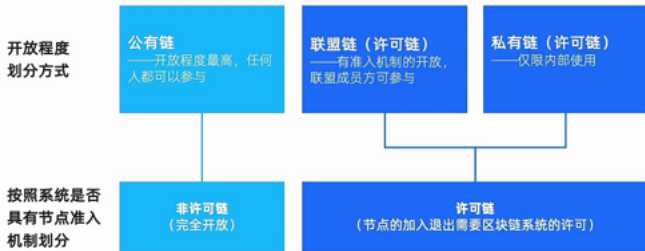
什么是开放性

区块链的开放程度

开放性与匿名性是否冲突



区块链的开放程度



开放性与匿名性是否冲突

开放的基础上匿名

- 匿名性要做到在系统开放的情形下还能做到个性隐藏；
- 区块链的匿名性是数据安全和身份安全的保障，身份匿名与身份认证是相辅相成的。

开放性
(参与程度)

&

匿名性
(个性隐藏)

04 总结



总结

匿名性

- 区块链的匿名性是通过密码学技术隐藏个人身份
- 区块链的匿名性包含基础级、高级、极致级三个级别

开放性

- 开发性体现为账目、组织结构、生态三个方面
- 开放性按开放程度可以分为公有链、联盟链、私有链，也可以划分为许可链和非许可链

谢谢



蚂蚁集团
ANT GROUP



蚂蚁链
ANTCHAIN