从0到1开发公有链

比原链
朗豫
langyu@bytom.io

什么是区块链

- 去中心化的协议，信息不可篡改
- 经济生态系统 ， 多角色参与的社区
- 互联网数据商业的新模式， 无法复制，有确定归属权
- 一种新思想， 不需要三方背书，所有运作的协议公开透明，参与者拥有各自的角色

公有链和非公有链

许可链

核心是“Control”

是内部系统，概括特征：

- 许可加入，需要审查
- 性能高，账本维护开销少
- 升级简单， 协同工作
- 追求特定场景的高TPS需求

非许可链

核心是“Permissionless”

是完全开放的系统，概括特征：

- 任何人随时参与随时离开
- 多方参与， 多方决策
- 升级更改艰难，强调不可篡改
- 可靠性大于效率

Kickoff 项目视角

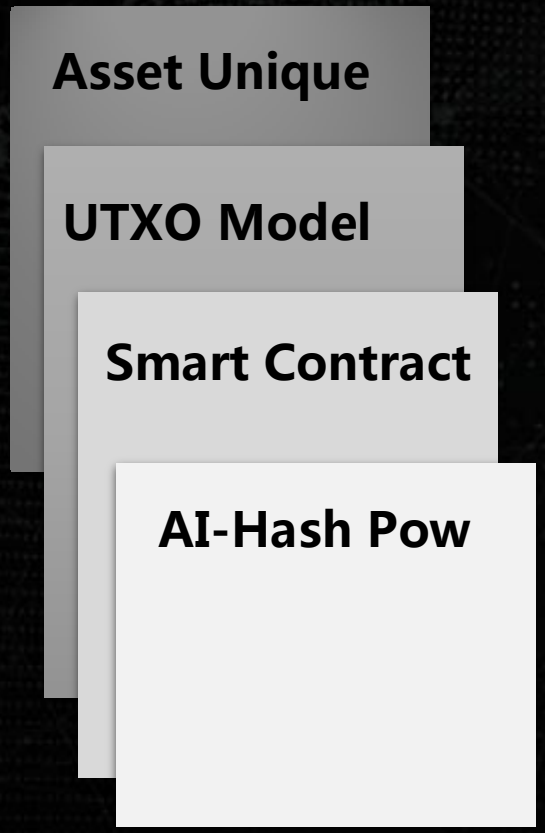
- 价值观要统一， 公有链开发应该是非赢利组织，是一个开源社区项目
- 社区项目， 多方参与并决策项目发展方向， 权力越分散社区的健壮性更强
- Bytom 持币人大会，开发者基金会， POW算力提供者三方决策

Kickoff 项目视角

- 需要撰写技术白皮书来阐述说明自己项目的必要性， 和能解决的问题
- 需要经济白皮书公开Token的激励方案，整体分配的策略
- 需要可行性说明书，描述整体技术架构，难点和所需要的资源
- 突出自己的项目亮点，竞争优势

Kickoff 项目视角

为什么需要比原链



数字资产所属权与唯一性，打通byte和atom的界限

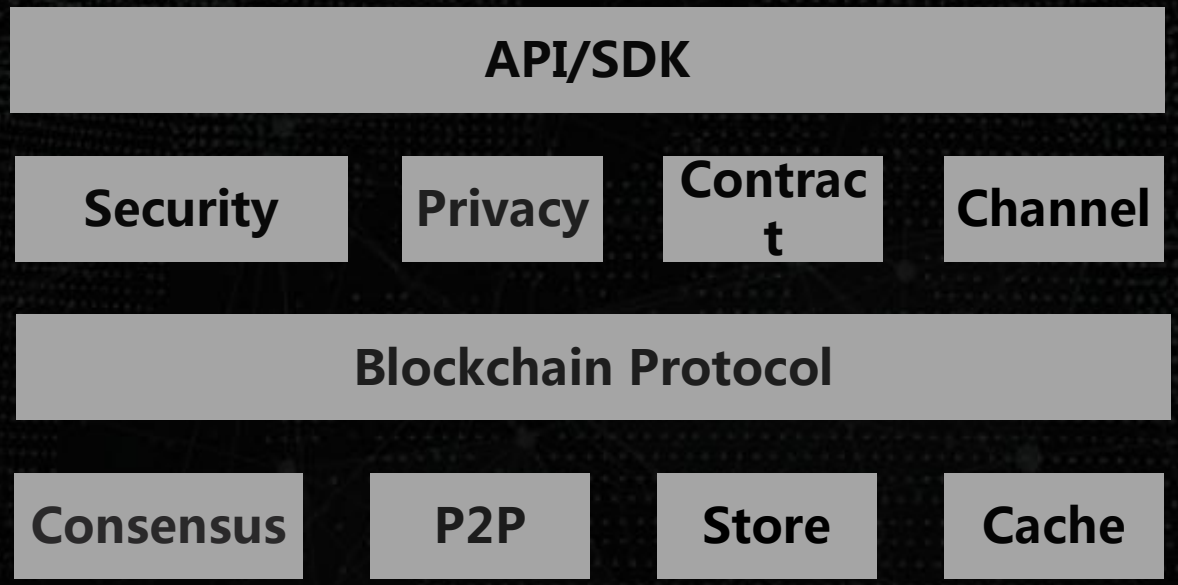
基于UTXO 模型，体现灵活性和可控性

设计独有的基于金融资产交易的合约系统

打通人工智能领域和区块链的交互渠道

Kickoff 开发模式

- 整体架构分离和清晰划分， 包括:



- 需要经济白皮书公开Token的激励方案，整体分配的策略
- 需要可行性说明书，描述整体技术架构，难点和所需要的资源

Kickoff 开发模式

开发模式的差别， 传统互联网模式并不适用

全网协议可升级

系统全平台兼容

协议可持续发展

维持账本记录连续和可靠

BYTOM 实现

“Tick-Tock”循环模式

Alert 紧急消息

系统发生影响范围大的BUG，需要通过全网广播通知时， 发布相应Msg信息

Alert在Bitcoin 0.14中被设计为Deprecate特征， 但始终未被移除，考虑了弹性(Resilient)

Kickoff 开发者视角

- 理解比特币，区块链的价值， 和传统系统的差别
- 理解开发公有链为什么需要Token系统， 与工具的区别
- 理解区块链“不可能三角形”理论， 安全，环保，去中心化不可能同时满足
- 理解基础经济学知识

Kickoff 开发者视角

- 理论知识， 分布式系统CAP定律， 拜占庭容错算法
- 基础密码学， ECDSA， 公钥加密体系 ， 哈希散列算法
- 跨平台编译器和虚拟机的设计
- P2P技术，DHT， NAT等网络技术

ONE MORE THING...

- Bytom 近况： Release Testnet Beta版， 代号SPARK（“晓”）， 欢迎大家体验
  https://github.com/Bytom/bytom **所有代码已经开源**
- 比原投资基金： 投资合适的区块链项目，项目合作资源整合， 扩大生态链
- 比原开发者：有计划加入行业的， 可以联系， 有竞争力的薪资和国际视野


THANKS