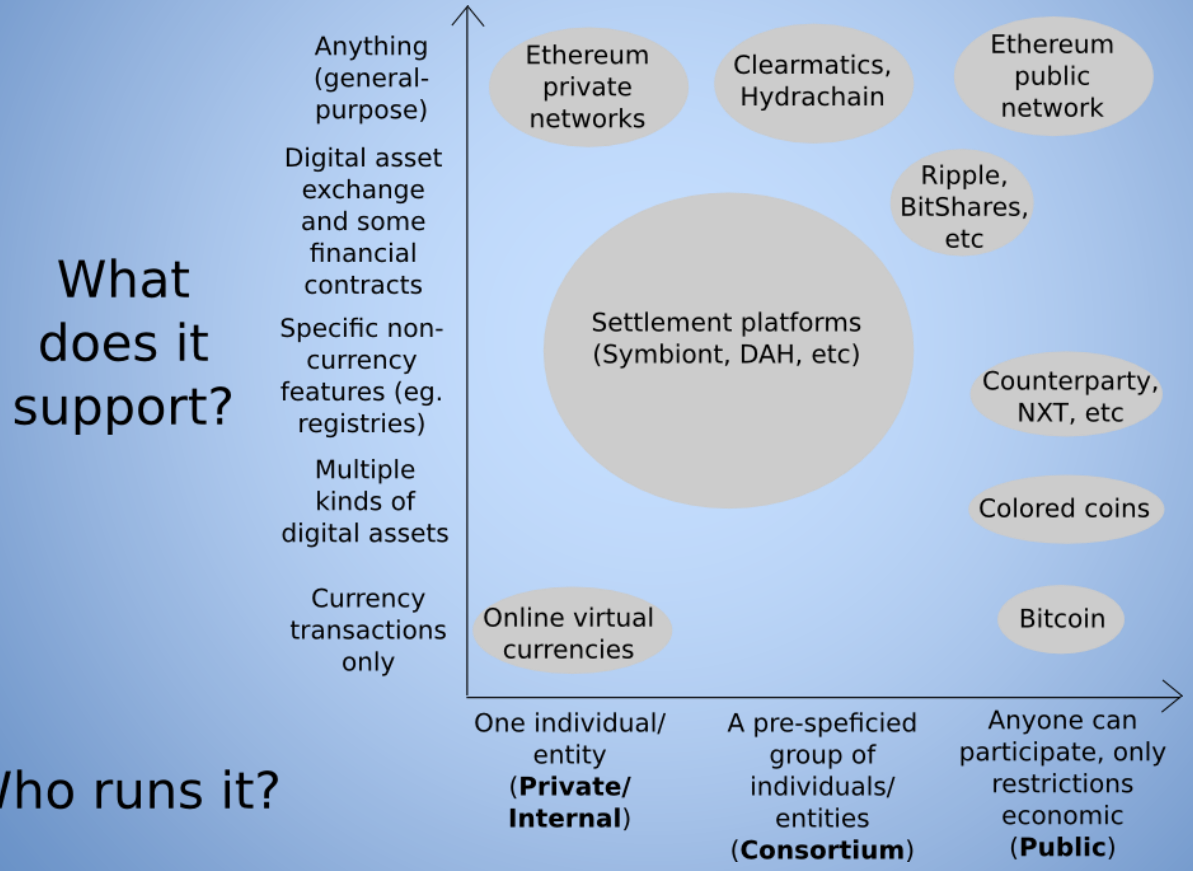
WANXIANG
BLOCKCHAIN LABS

私有链/联盟链的介绍

（以太坊创始人Vitalik Buterin在万向区块链实验室内部的分享）

有多种区块链

WANXIANG BLOCKCHAIN LABS



这种区块链的优点是什么？

WANXIANG BLOCKCHAIN LABS

私有链（内部链）——单独的个人或实体: 对公司、政府内部的审计和测试有用

联盟链(预先设定的组织): 对产业或国家的特定清算、结算用途有用，容易进行控制权限设定，更高的可扩展性

公有链(任何人): 任何人都可以参与，容易部署应用程序，全球范围可以访问，不依赖于单个公司或者辖区。

私有（内部）链

WANXIANG BLOCKCHAIN LABS

一个人/公司控制的，不完全解决信任问题,但改善可审计性

不太明确内部链和其他技术的差别是什么

　　git是不是内部链？

可能有几个审计的应用

开发，测试和黑客马拉松的工具

联盟链

WANXIANG BLOCKCHAIN LABS

几个人/组织/公司/政府 控制的

“多中心化”，改善信任问题

可以联合有多公司的行业

解决结算问题，降低两地结算成本和时间，比现有的系统简单和效率更高

能够继承中心化的优点（比如，网络效应），但是减轻垄断问题

公有链

WANXIANG BLOCKCHAIN LABS

每个人可以参加

- 工作量证明（PoW）
- 股权证明（PoS），“虚拟挖矿”

全球化

进入壁垒最低，很容易部署应用程序

联盟链的技术

WANXIANG BLOCKCHAIN LABS

需要选择几个控制区块链的节点

比如，每个公司有一个节点

拜占庭容错(BFT)的共识算法

PBFT

Paxos

联盟链：挖矿或PoS奖励利息的经济激励并不是必须的

联盟链的技术

WANXIANG BLOCKCHAIN LABS

取决于网络模型

同步：可以容忍50%的节点错误或攻击

异步：可以容忍33%的节点错误或攻击

一个区块是可以实现完全确认，不需要等到6个区块

也可以使用PoS的共识机制，给每个控制区块链的节点奖励一个“币”

如果这样，需要等到几个区块完全确认一个交易

联盟链的技术优点

WANXIANG BLOCKCHAIN LABS

在公有链，需要关注几个经济方面的因素：

如果运行一个节点的成本高，需要有经济激励去奖励确认区块的责任。

“矿池”

如果网络延迟低的节点有较大优势，可能导致网络中心化。

也需要一个普通的节点处理每个交易（导致网络整体性能受限）

私有链没有这个问题，因为可以控制谁参与共识的过程，保证每个节点有很好的计算机和网络连接

联盟链的技术优点

WANXIANG BLOCKCHAIN LABS

共识完成时间

公有链：一个区块（17 秒）* 12个区块 ~=3分钟

联盟链：一个区块（3 秒）* 1个区块 ~= 3秒

注：实际时间取决于节点的数量，节点之间的距离和互联网连接的质量

可扩展性

公有链：最高3-20次交易每秒

联盟链：最高1000-100000交易每秒

＊具体上下限取决于应用和服务器的计算能力

可扩展性

WANXIANG BLOCKCHAIN LABS

可扩展性主要受限于并行处理是否可行的问题。

如果可以实现并行处理，无限的可扩展性是可行的；但若并行处理的问题不能解决，那么一个处理器的吞吐量性能会对可扩展性有直接的限制。

关键问题是：每个应用程序里面，可以进行平行处理的部分有多少？

例子：数字货币

WANXIANG BLOCKCHAIN LABS

问题：账户A有100个币，发送两个交易

100个币给B

100个币给C

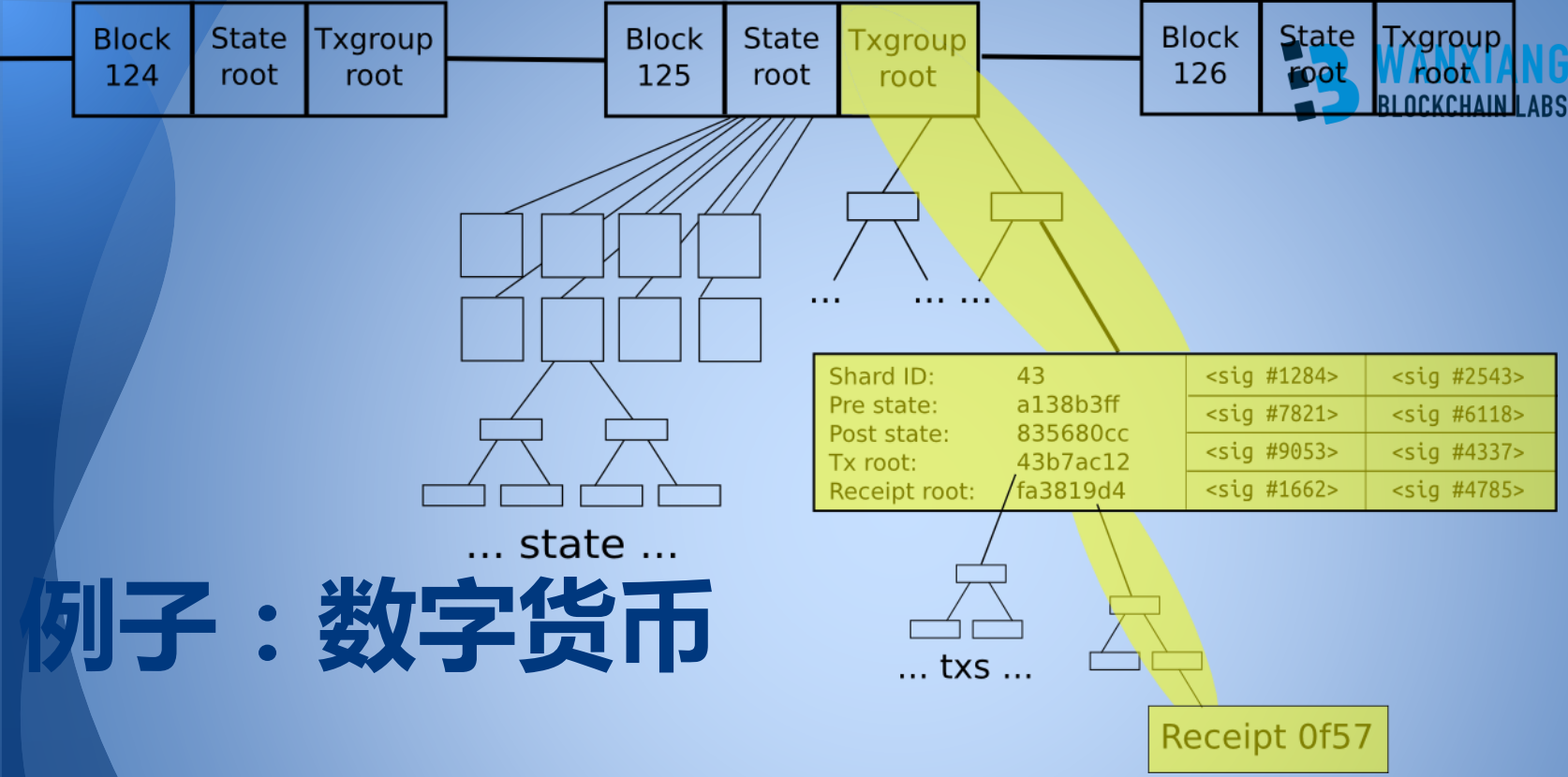
怎么处理这个交易，选择什么机制去判断交易是否成功？

“收据”的机制：

交易的过程分为两个步骤：

第一步：减少A的账户余额并在区块链上保存一个“收据”

第二步：确认（i）收据有效，（ii）若还没消耗收据，则增加B或C的金额


Block 124
State root
Txgroup root
Block 125
State root
Txgroup root
Block 126
State root
Txgroup root
WANXIANG BLOCKCHAIN LABS
... state ...
... ...
Shard ID: 43
Pre state: a138b3ff
Post state: 835680cc
Tx root: 43b7ac12
Receipt root: fa3819d4
<sig #1284>
<sig #2543>
<sig #7821>
<sig #6118>
<sig #9053>
<sig #4337>
<sig #1662>
<sig #4785>
... txs ...
Receipt 0f57

例子：数字货币

联盟链的访问权限控制

WANXIANG BLOCKCHAIN LABS

1、需要选择参与共识机制（确认交易）的节点

2、也需要选择，谁能读取区块链上的信息：

全球任何人能读；

限制谁能读；

只参与共识机制的节点能读。

3、也需要选择，发送交易的条件

在公有链，交易费的需求是唯一的限制，任何人可发送；

在联盟链，需要交易费？还是给特定用户无限发送交易的权利？还是同时用这两个模型？

私有链/联盟链的隐私保护问题

区块链（包括私有链）技术本身不是一个隐私保护的方案。

联盟链在交易的真实性问题上可以容忍33-50%的错误（因为有共识机制），但关于隐私保护的问题并没有任何容错的空间——毕竟任何节点都可以拥有整个区块链的信息。

如果你的应用需要隐私保护，需要将区块链和其他技术结合：

- 秘密共享
- 完全同态加密
- 环签名
- 零知识证明

怎么做自己的私有链/联盟链

WANXIANG BLOCKCHAIN LABS

选择谁参加

选择技术：

基于以太坊技术的联盟链（比如，hydrachain）；

比特股的技术；

专门为私有链设置的平台；

其他技术。