走近区块链

- 区块链是什么?
- 通过建造简易比特币系统来看区块链
- 区块链技术的应用与未来

区块链是什么?

- 去中心化
- 开放性
- 自治性
- 信息不可篡改
- 匿名性
- 分布式存储系统
- 非对称加密，共识算法等技术的集合

通过建造简易比特币系统来看区块链

系统功能要点

- 任何人都可以把交易信息记账（可用性）
- 交易信息要真实准确（安全）
- 不能出现入不敷出的情况（业务纠纷）

张三

宋七

记账

记账

公共账本

张三 ——> pay ￥30 ——> 李四

王五 ——> pay ￥20 ——> 张三

李四 ——> pay ￥20 ——> 王五

王五 ——> pay ￥2亿 ——> 李四

记账

李四

记账

记账

王五

1，如何防止恶意记账?
2，我们又如何能够相信账本上的交易记录?
3，如何防止有人欠钱不还?

- 交易可验证即可解决恶意记账问题。（电子签名）
- 保证欠款交易不出现的最对入不敷出最好的处理方案

Private key

宋七

记账 signature

Private key

张三

记账 signature

余额记录

张三： xxx

王五： xxx

李四： xxx

公共账本

张三 —> pay ￥30 —> 李四 signature（张三）

王五 —> pay ￥20 —> 张三 signature（王五）

李四 —> pay ￥20 —> 王五 signature（李四）

王五 —> pay ￥2亿 —> 李四 signature（王五）

记账 signature

Private key

李四

Private key

王五

记账 signature

加入电子签名后

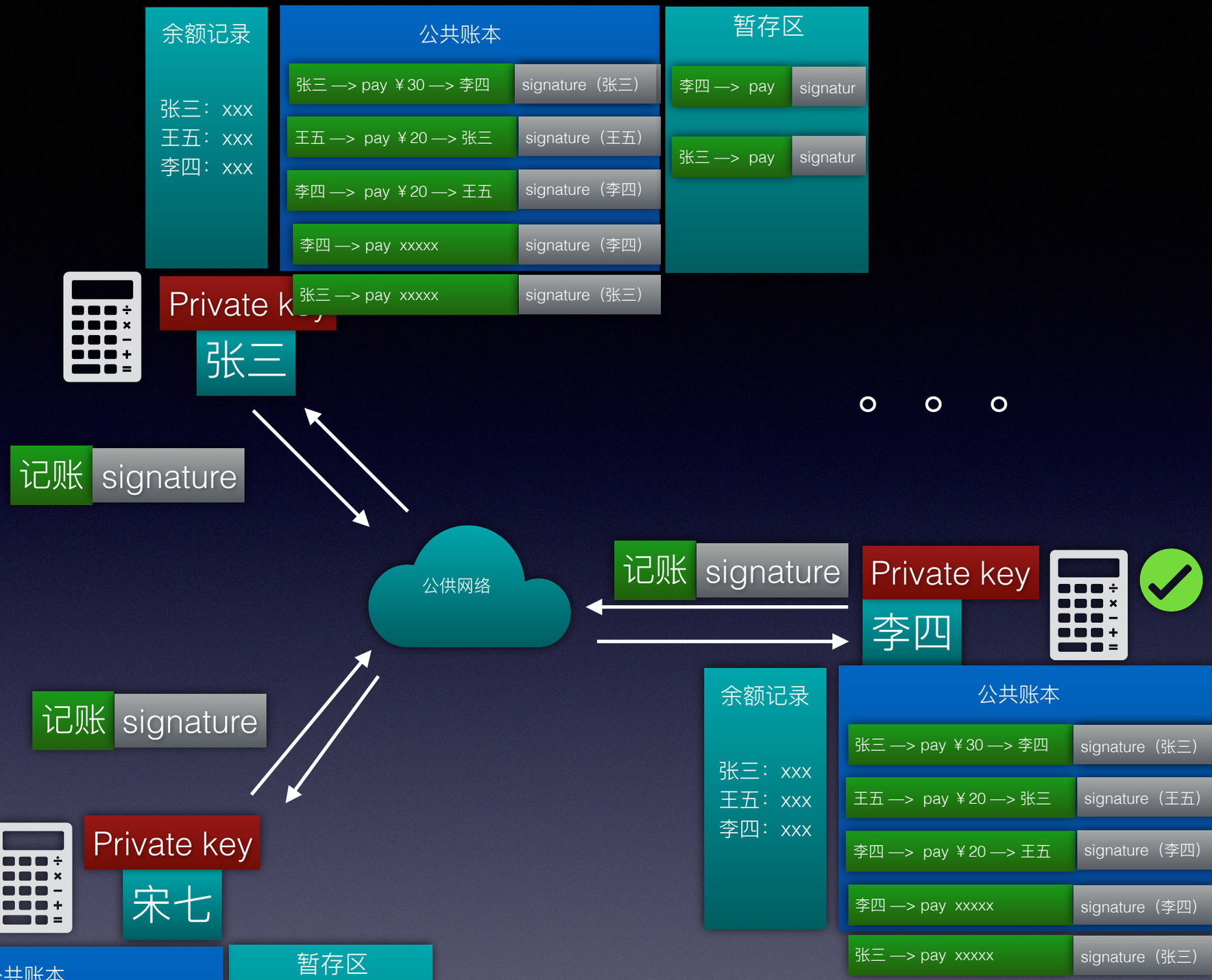
如何去中心化?

如何保证每一个人记录的账本的一致性?

如何保证交易的顺序不错乱?

如何防止交易造假?

如何保证每一个人记录的账本的一致性?



- 交易广播和记账分离
- 记账权竞争

如何保证交易的顺序不错乱?

余额记录

张三：xxx
王五：xxx
李四：xxx

公共账本

张三 —> pay ￥30 —> 李四 | signature（张三）

王五 —> pay ￥20 —> 张三 | signature（王五）

李四 —> pay ￥20 —> 王五 | signature（李四）

第1页

暂存区

李四 —> pay xxx —> xxx | signature（李四）

张三 —> pay xxx —> xxx | signature（张三）

记账权争夺

记账权争夺

前一页内容的hash：xxxxxx…

李四 —> pay xxxxx | signature（李四）

张三 —> pay xxxxx | signature（张三）

第2页

前一页内容的hash：xxxxxx…

李四 —> pay xxxxx | signature（李四）

张三 —> pay xxxxx | signature（张三）

第2页

记账权争夺

前一页内容的hash：xxxxxx…

宋七 —> pay xxxxx | signature（宋七）

王五—> pay xxxxx | signature（王五）

第3页

记账权争夺

o o o

记账权争规则夺设计

余额记录

张三：xxx
王五：xxx
李四：xxx

公共账本

张三 —> pay ￥30 —> 李四 | signature（张三）

王五 —> pay ￥20 —> 张三 | signature（王五）

李四 —> pay ￥20 —> 王五 | signature（李四）

第1页

暂存区

李四 —> pay xxx —> xxx | signature（李四）

张三 —> pay xxx —> xxx | signature（张三）

target：0000000000000000001d147cf61806e10ab7f7586e5ed901b7b057b216c5966

```
while(Hash256（前一区块的hash+Nonce值） >= target) {
    Nonce++;
}
printf(挖矿成功);
```

Hash256（前一区块的hash+Nonce值）

消耗大量的时间和算力

0000000000000000001d147cf61806e10ab7f7586e5ed901b7b057b216c5965

验证符合target的要求，得到记账权

王五

造假内容

李四

第一个月　第二个月　第三个月　第四个月

区块1 。。。

区块2 有造假内容

区块3 。。。

区块4 。。。

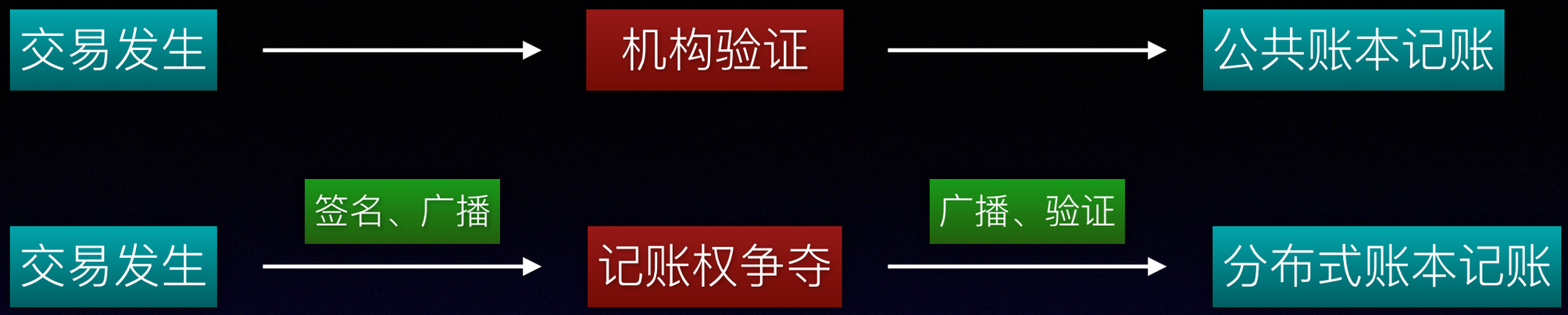
区块2 。。。

区块3 。。。

区块4 。。。

区块5 。。。

宋七　赵六　张三　。。。



1，如何防止恶意记账?
2，如何保证交易记录的真实性?
3，如何防止有人欠钱不还?
4，如何去中心化?
5，如何保证每一个人记录的账本的最终一致性?
6，如何抢到记账权?
7，如何保证区块的顺序?
8，如何避免分叉?
9，如何防止造假?

比特币常见问题

- 比特币哪里来的，以什么形式存在?
- 为什么要每10分钟出一个块?
- 为什么是每四年奖励减半?
- 怎么保证最多出2100万个?

区块链的核心是什么?

共识机制之工作量证明(PoW)

- 生成Merkle根哈希
- 把Merkle根哈希及其他相关字段组装成区块头，并作为工作量证明的输入
- 通过更换nonce值来找到目标输出。

工作量证明是完美的吗?

常见的共识算法

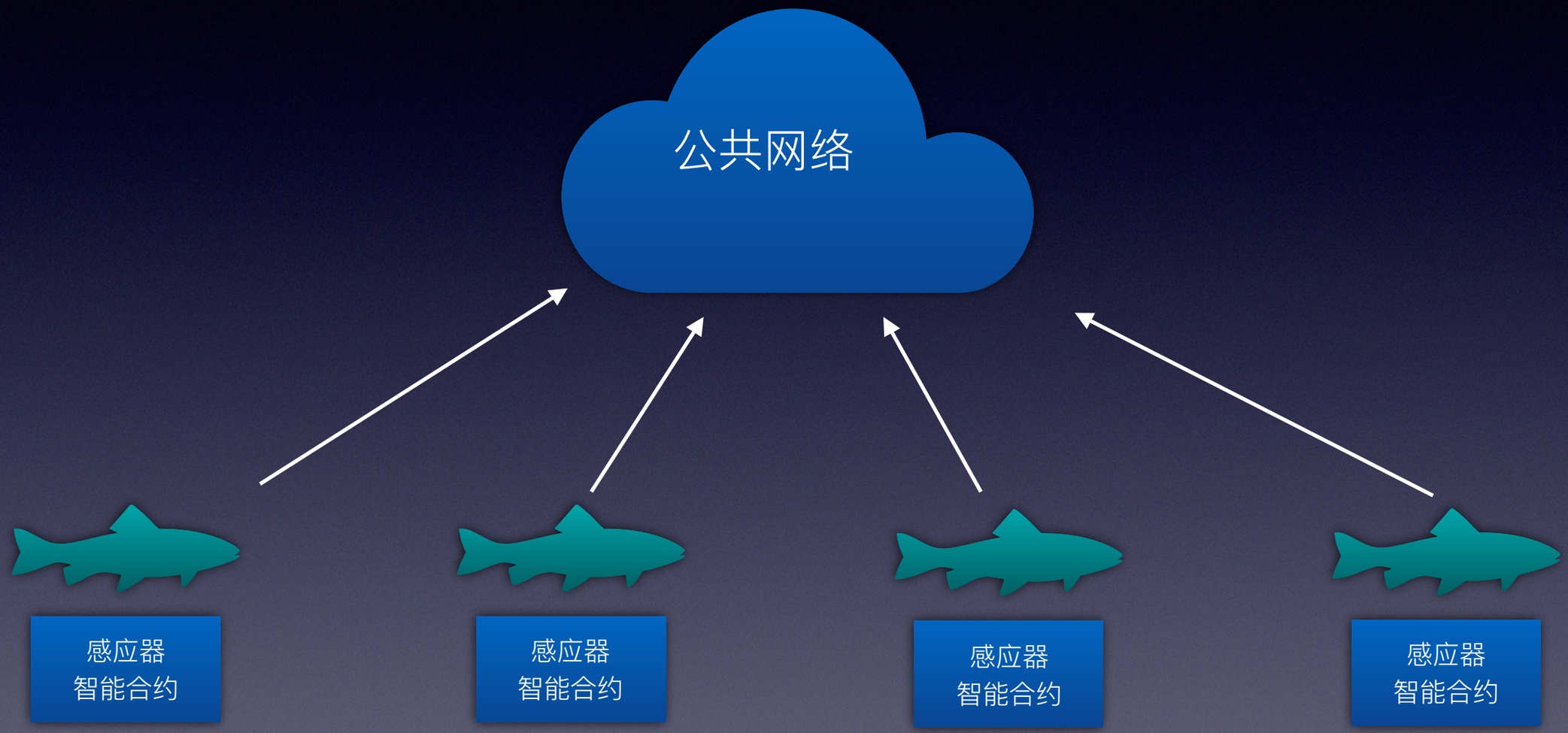
- 股权证明 Proof of Stake(PoS)
- 委任权益证明 Delegated Proof of Stake(DPoS)
- Ripple共识算法
- 拜占庭容错技术（Byzantine Fault Tolerance，BFT）
- PBFT：Practical Byzantine Fault Tolerance，实用拜占庭容错算法
- PAXOS
- ZAB
- Raft

区块链在现实生活中到底能干嘛?

区块链分类

- 公链
- 联盟链
- 私链

沃尔玛生鲜溯源



打捞　运输　分销　售卖

- 保险（保单的追踪）
- 医疗档案
- 个人信息
- 信用记录
- 京东跑步鸡
- 发票
- 知识产权

- https://baijiahao.baidu.com/s?id=1635921853363022467&wfr=spider&for=pc（开发、测试工具）
- https://ethereum.org/ （以太坊）
- https://btc.com/000000000000000001d147cf61806e10ab7f7586e5ed901b7b057b216c5965 （比特币浏览器）
- https://www.cnblogs.com/X-knight/p/9157814.html （常见共识算法）

谢谢欣赏

请扫码填写问卷及签到

欢迎报名参与分享哦~

报名方式：

发送主题至：

chenjing02@youxin.com