YEECO

# 区块链扩容的探索之路

郭 斌

2019/06/20

# 共识

## Complex consensus

摇奖过程证明

摇奖机最新型号原则

开Party的小镇青年

# 区块链

Blockchain

工作量证明

最长链原则

身份

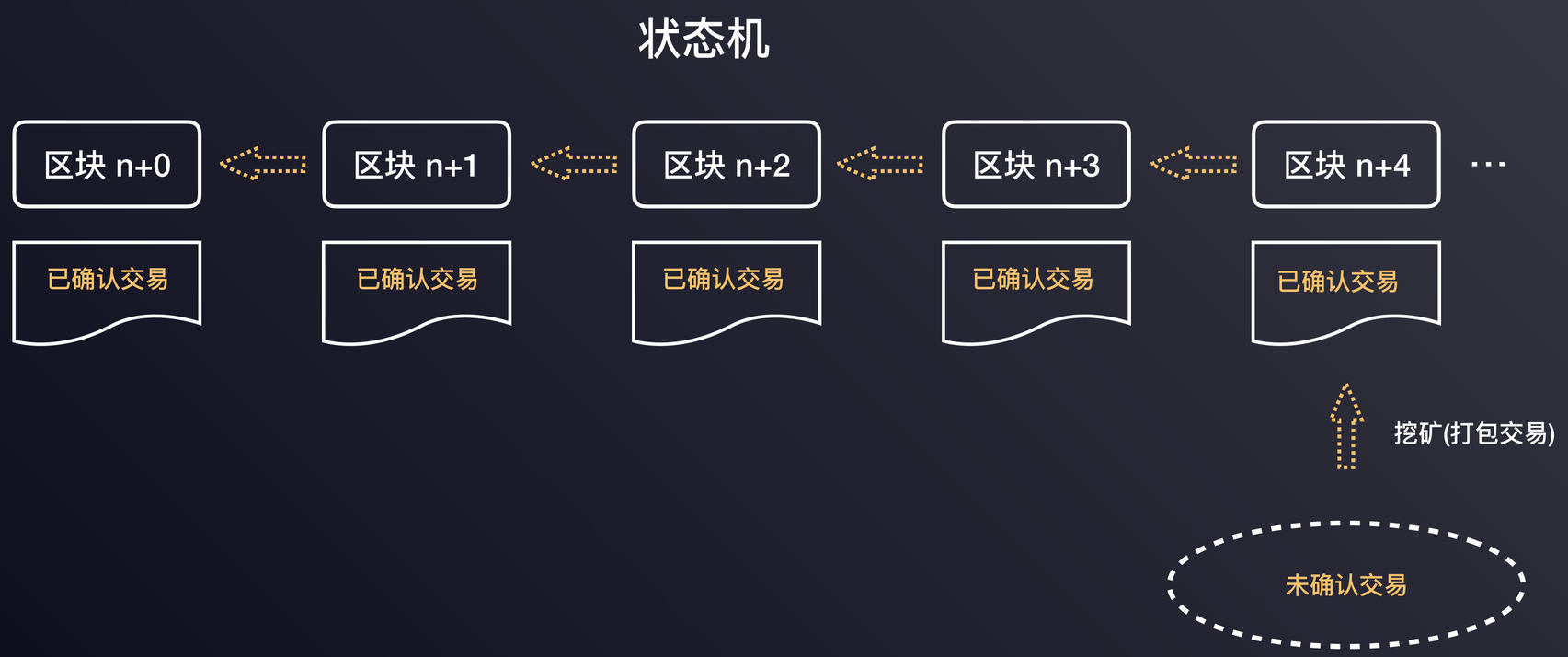
非对称加密

激励

出块奖励

交易表达

UTXO 锁定/解锁脚本




YEECO

# 挑战

Challenge

**多**

吞吐

**快**

延迟

**好**

去中心化
安全性
活跃性
公平性

**省**

成本

YEECO

# 挑战

Challenge

$$TPS = \frac{交易数}{时间}$$

**多**

吞吐

每个交易每个节点都要：

传输

验证

状态维护

存储

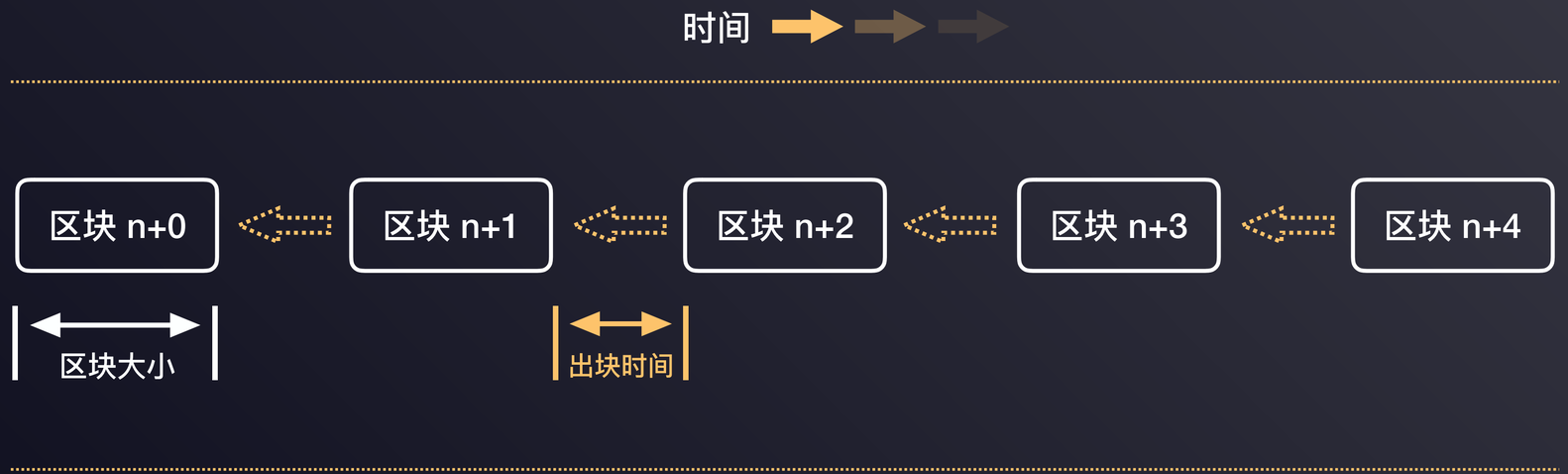
YEECO

# 扩容 - 起点

## Capacity scale

区块大小

出块时间



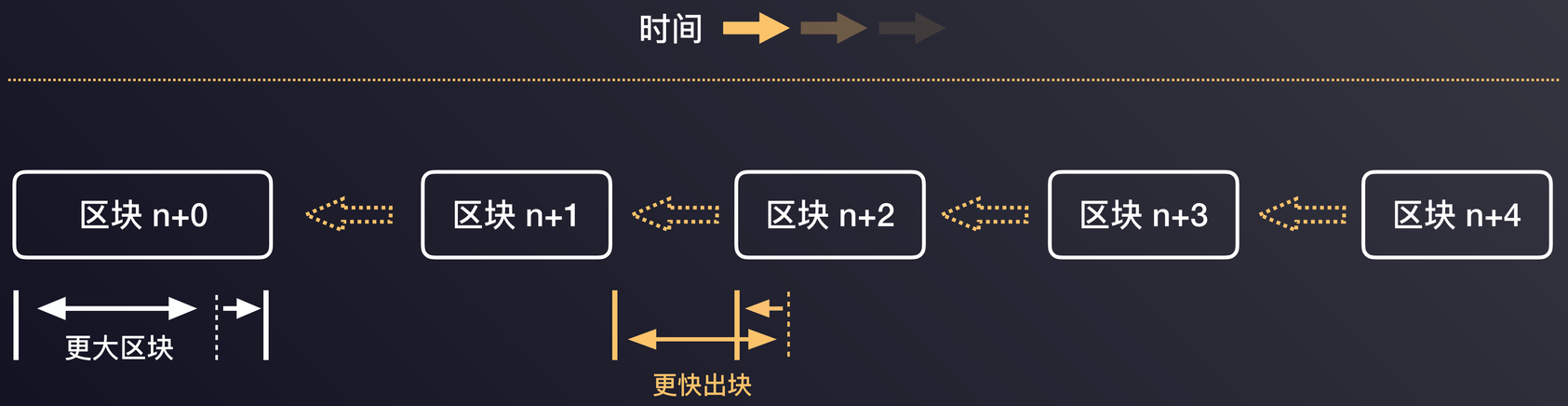
# 扩容 - 形态一

Form

缩小出块时间

增大区块

GHOST协议




YEECO

# 扩容 - 形态二

Form

一次出多个块

拜占庭容错

- 通过PoW选取
- 通过DPoS选取
- 通过VRF选取


YEECO

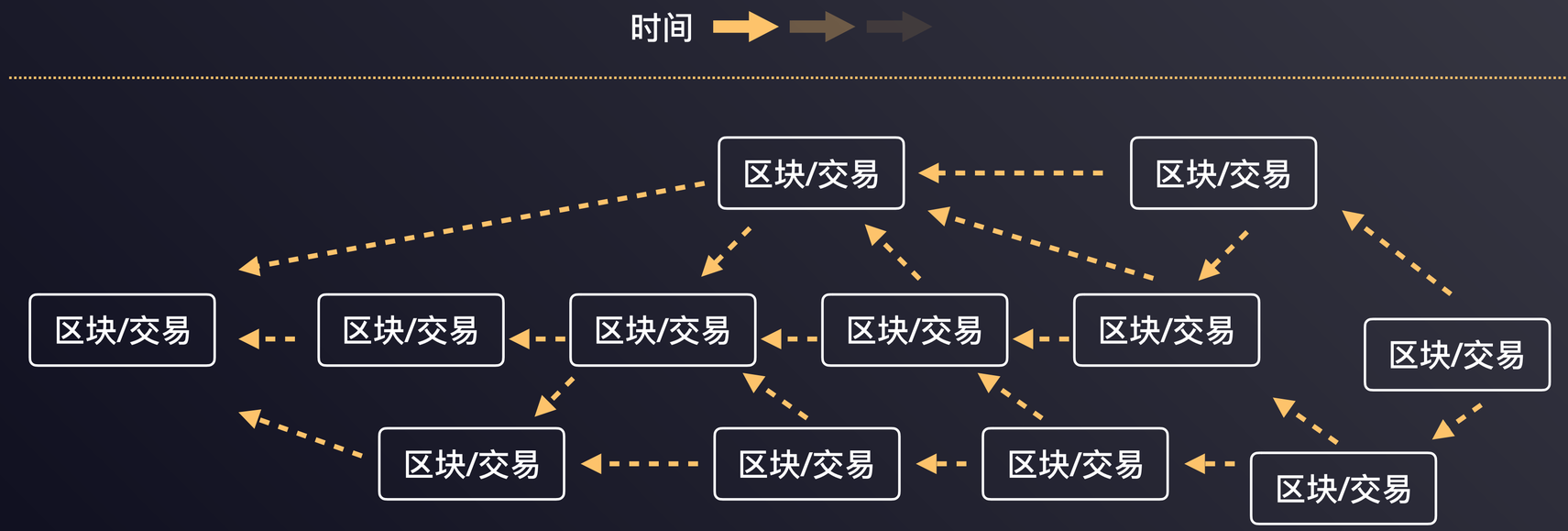
# 扩容 - 形态三

Form

DAG

定序

交易重复




YEECO

# 挑战

Challenge

$$TPS = \frac{交易数}{时间}$$

**多**

吞吐

每个交易每个节点都要：

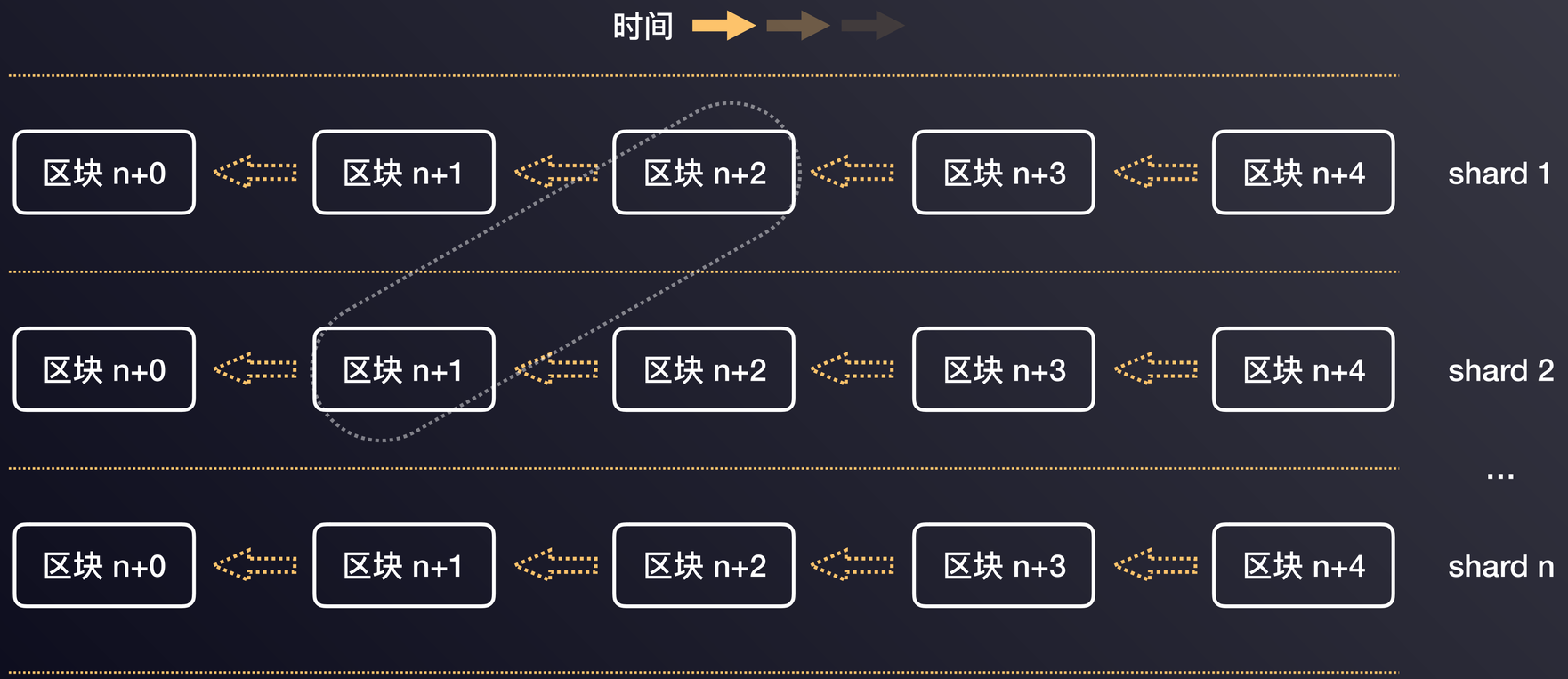
| | |
|---|---|
| 传输 | 带宽 |
| 验证 | CPU |
| 状态维护 | 内存 |
| 存储 | 磁盘 |

# 扩容 - 形态四

Form

安全性

跨分片交易




YEECO

# YeeCo

PoW
Full shard ...
Multi-mining
CRFG


YEECO

# YeeCo - PoW

非许可

安全性

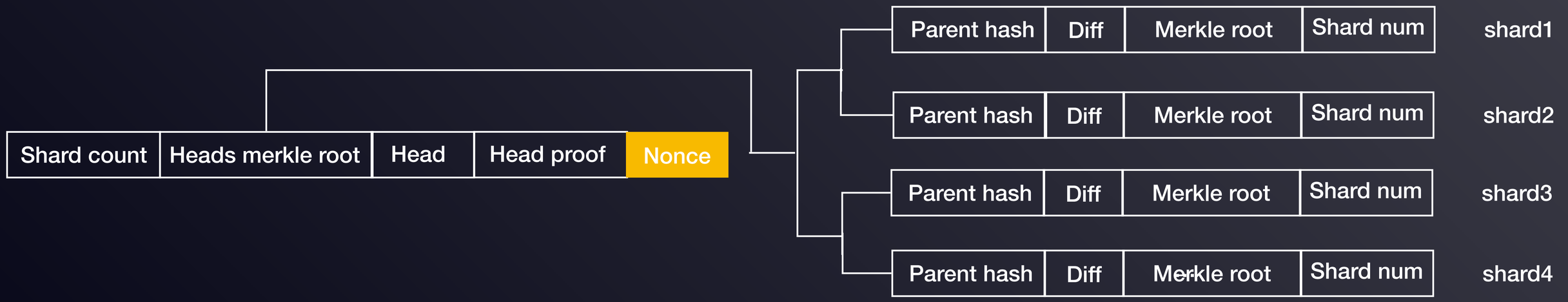
YEECO

# YeeCo - Full shard

| | |
|---|---|
| 传输 | 带宽 |
| 验证 | CPU |
| 状态维护 | 内存 |
| 存储 | 磁盘 |

YEECO

# YeeCo - Multi-mining




SingleHeadHash = hash(ParentHash + Diff + MerkleRoot + ShardNum)

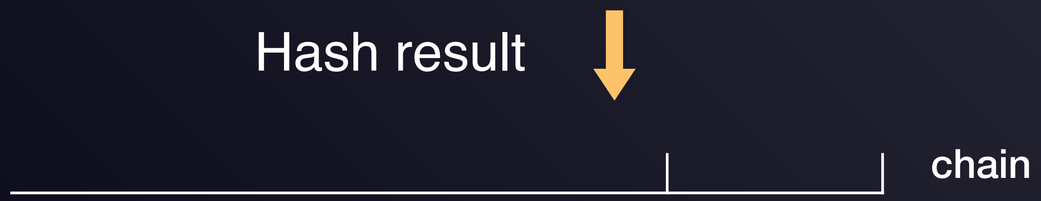
Hash = hash(ShardCount + HeadsMerkleRoot + Nonce) vs Target

MultiHead = ShardCount + HeadsMerkleRoot + Head + HeadProof + Nonce

YEECO

# YeeCo - Multi-mining

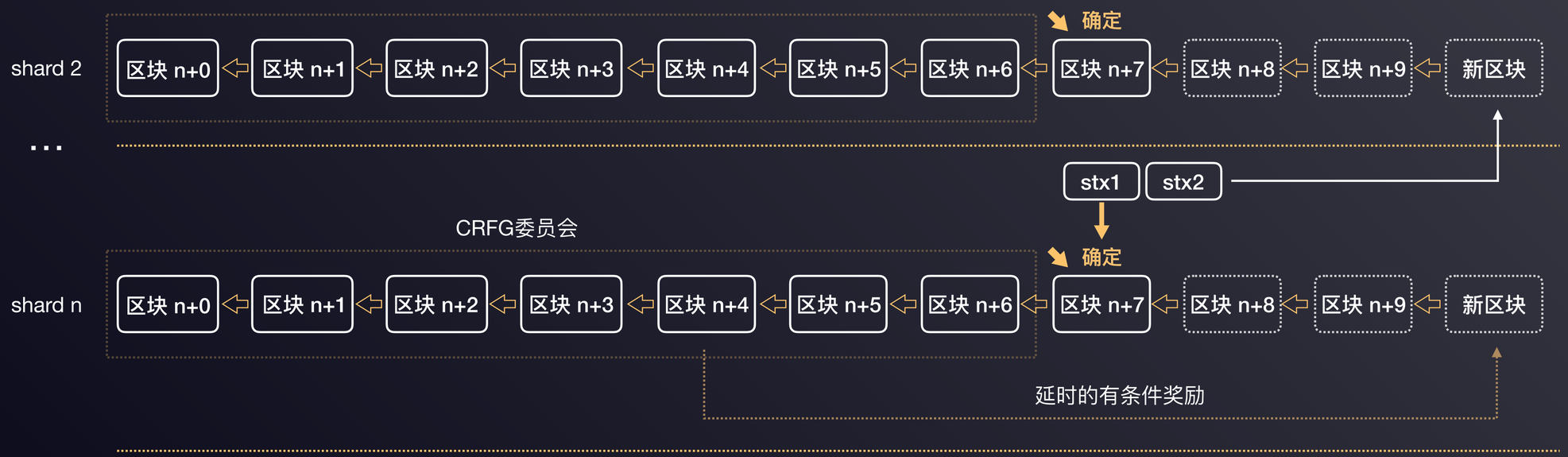
## Mining




## Multi-mining


YEECO

# YeeCo - CRFG




Conditional Reward Finality Gadget

1. 对已经具有概率确定性的块投票决定其确定性
2. 由近期出块节点构成投票委员会
3. 出块节点的奖励被延迟有条件发放

YEECO

# YeeCo 扩容

#01
## PoW
共识

#02
## Full shard
数据结构

#03
## Multi-mining
安全性

#04
## CRFG
跨分片原子性

YEECO

# 谢谢

THAKNS!

YEECO