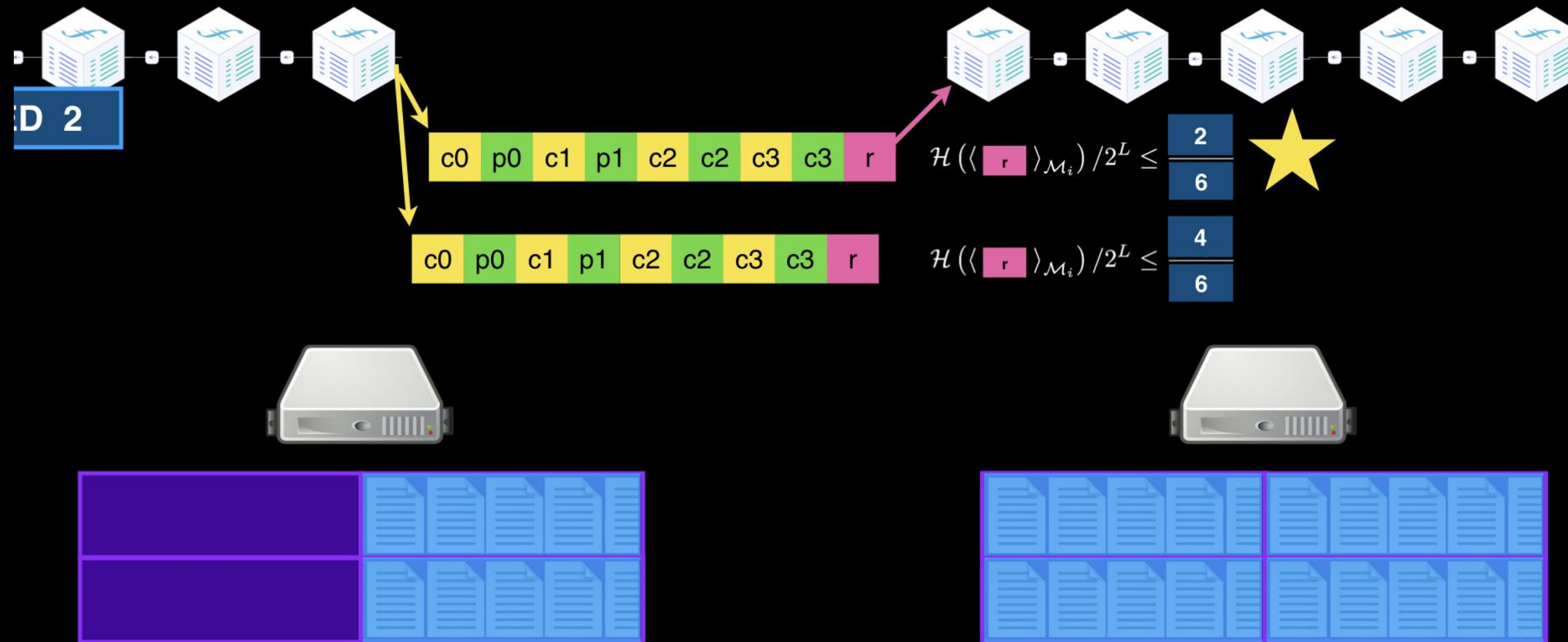


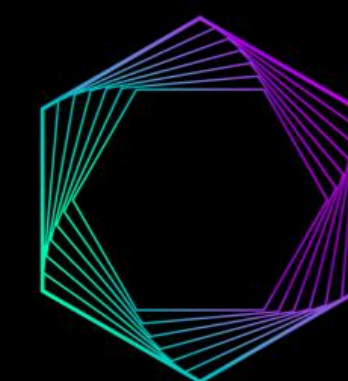
Useful Proof of Work
for Consensus

Now: How to mine / extend the chain



预期共识 - Filecoin对共识机制的探索

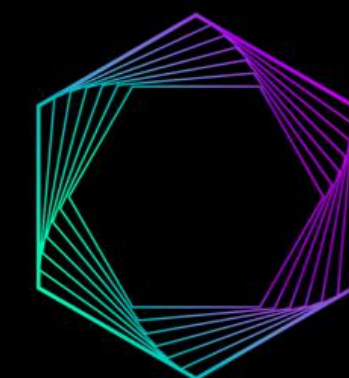
李 昕



ProtoSchool
Shanghai Chapter

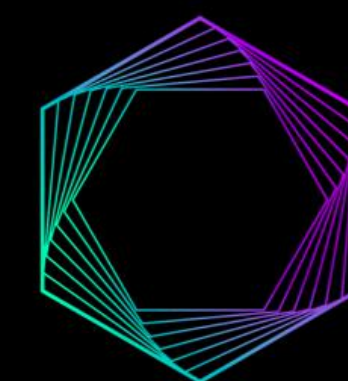
共识机制 - 领导人选举

1. 选举秘密进行 (Secret)
2. 选举是公平的 (Fair) , 基于一套规则, 在规则的基础上概率起作用
3. 最好没轮选举出一个领导人 (Single Leader)
4. 无法预测 (Unpredictable)
5. 十分容易验证 (Verifiable)
6. 能够承受攻击 (Anti-attack)
7. 消耗资源不大 (Efficient)



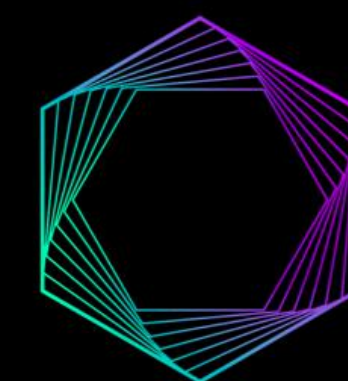
常见共识算法

| 共识算法 | POW | POS | DPOS | PBFT | PAXOS |
|-------|---------|--------|----------|---------|------------------------|
| 应用场景 | 公有链 | 公有链 | 公有链 | 联盟链 | 私有链 |
| 错误容忍度 | <50%节点数 | <50%权益 | <50%权益 | <33%节点数 | <50%节点数 (Acceptors) |
| 共识效率 | 低 | 中 | 中 | 高 | 高 |
| 典型应用 | 比特币 | 以太坊 | BTS, EOS | 超级账本 | 传统分布式产品 |



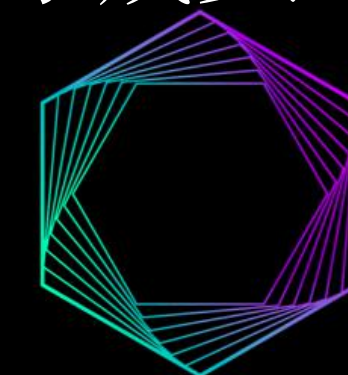
共识机制的目标 - SSLE

- 当前共识算法不能满足理想目标（各有哪些不足？）
- SSLE: Secret Single Leader Selection
 - 满足各方需求，但是，没有现成方案
- 提出方案，领取20万美元奖金



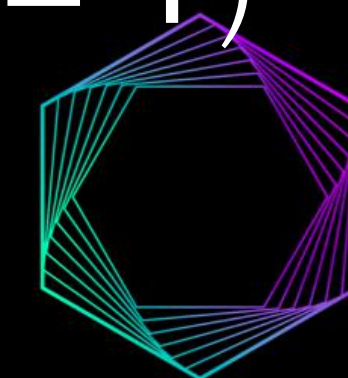
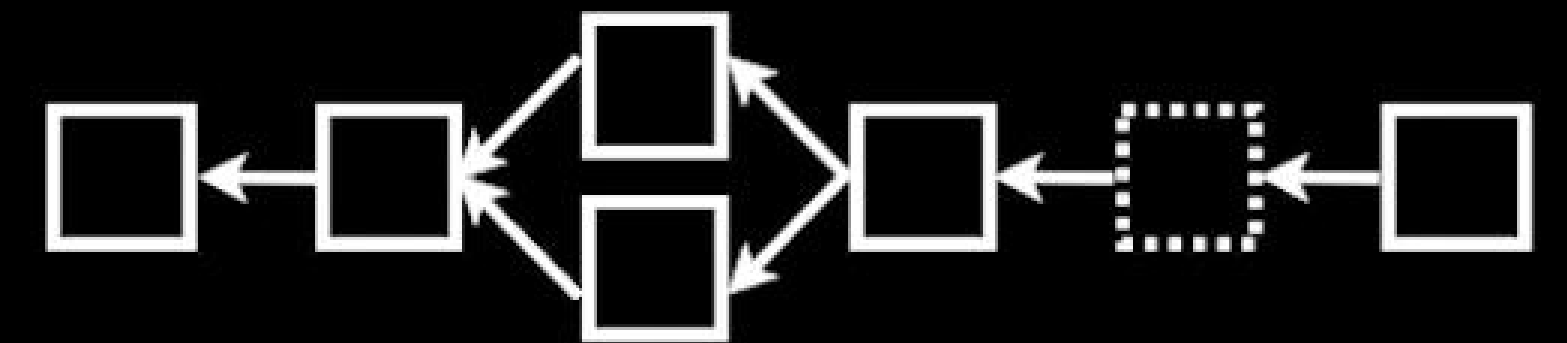
SSLE实现需要考虑的问题

- 链上效率：要实现链上尽量少的存储需求来满足共识；以及如何兼顾已有的和新进入的参与者
- 合理的通信复杂度：这是一个选举，如果通过大量的通信，比如安全多方计算的一些方式，完全可以实现这一目标，但是，通信过于繁复，使得成本和安全性都可能降低
- 计算的有效性：任何的参与者都应该能够通过相对简单的计算就可以实现这一选举机制
- 可扩展性：设计要求支持大量的参与者，比如数十万甚至百万
- 强健性：作为一个共识，最好能够在全网50%（或2/3）以上的诚实节点的支持下，整个网络能够有效运行。




预期共识 - SSLE前的折衷方案

- 几乎满足SSLE的所有特性，就差一点：
- 不能实现每一轮单个领导人选举
 - 每一轮可能没有人被选中，
 - 也可能有多人被选中
 - 平均起来说，每一轮一人 (Expected Number == 1)



Filecoin 的预期共识 - 有价值的共识



1. Storage-based Proof of Work

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@bitco.in
www.bitcoin.org

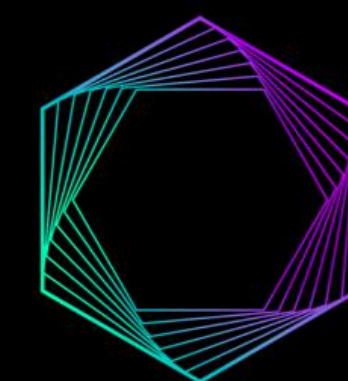
2. Byzantine-style Consensus

Algorand: Scaling Byzantine Agreements for Cryptocurrencies

Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nikolai Zeldovich
MIT CSAIL

3. Proof of stake style consensus

- 基于存储的工作量证明 (POW) 共识
- 拜占庭容错共识机制
- 权益证明 (POS) 共识机制



预期共识 - 基本术语

Ticket

票：预期共识的随机源；每一个区块产生会至少产生一个Ticket。

Election Proof

选举证明：由上一个ticket 计算而来，置于区块头，表明矿工拥有此轮的采矿权。

TipSet

同一高度的合法区块组成的集合，他们具有同一父Tipset，和同样数量的Tickets。

Round

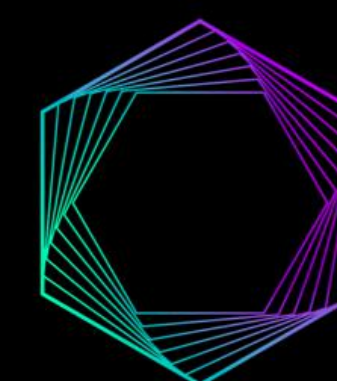
轮：一个选举周期称为一轮，也是新区块产生的周期，同时也是随机数Ticket产生的周期。轮由VDF函数控制

Height

高度：从创世区块（高度为0）开始的 Tipset 高度

Epoch

代：一个新区块产生的真正周期，因为有些轮可能不会产生区块，因此一代可能包含多轮

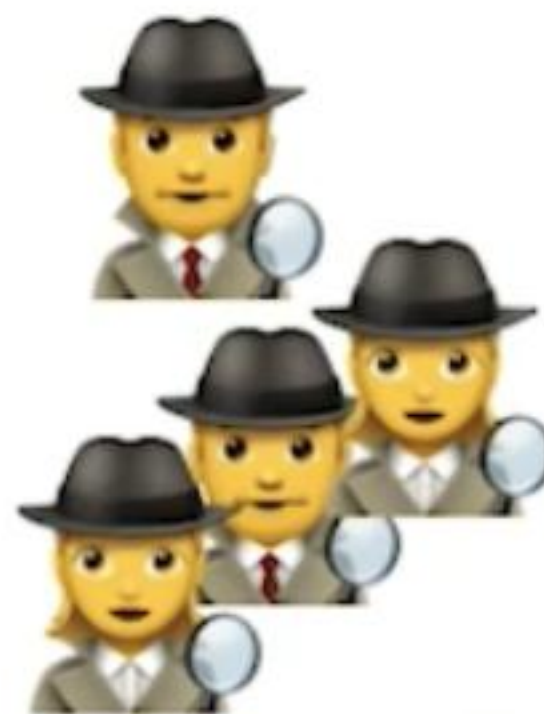




Live



Fair



Verifiable



Convergent



Honest



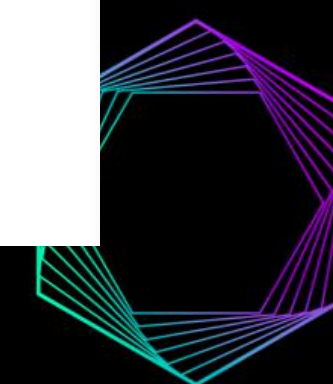
Rational



Adversarial

目标

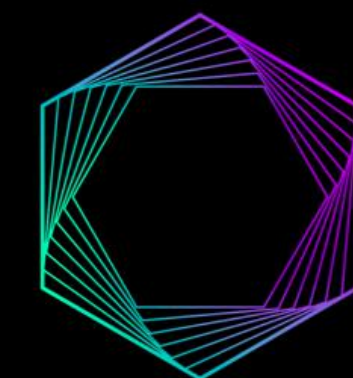
现实



ProtoSchool
Shanghai Chapter

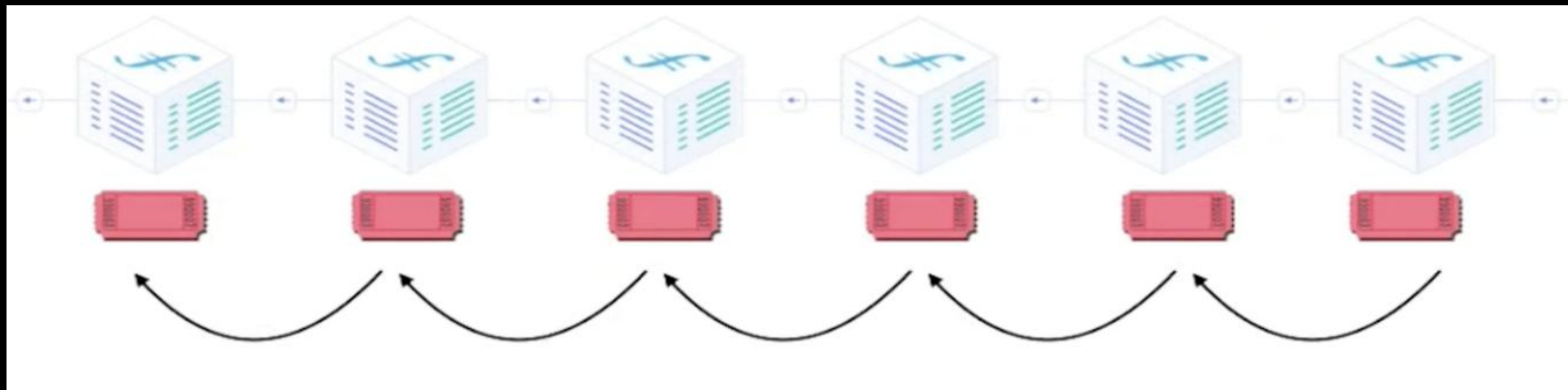
Tickets - 实现EC的随机数列

- 秘密，公平，可验证，每一轮一个，简单
- Tickets可以看成是单独的一条链，与Filecoin自身链的数据没有任何关系
- 目的：1) 实现Delay (VDF)，2) 作为随机源
- 矿工可以通过简单计算知道自己是否被选中，并可向网络证明



Tickets - 实现EC的随机数列

- 秘密，公平，可验证，每一轮一个，简单
- Tickets看成是单独的一条链，与Filecoin自身链的数据没有任何关系
- 目的：1) 实现Delay (VDF)，2) 作为随机源
- 矿工可以通过简单计算知道自己是否被选中，并可向网络证明



Tickets 的运算

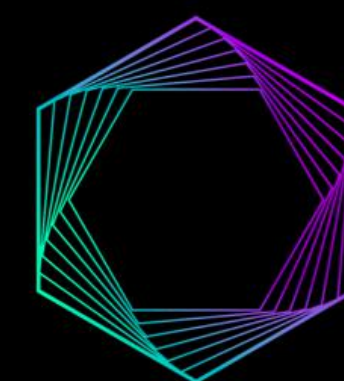


$\text{old_ticket} := \text{sort}(\text{parentTickets})[0]$
 $\text{new_ticket} := \text{Sig}(\text{VDF}(\text{H}(\text{old_ticket})))$

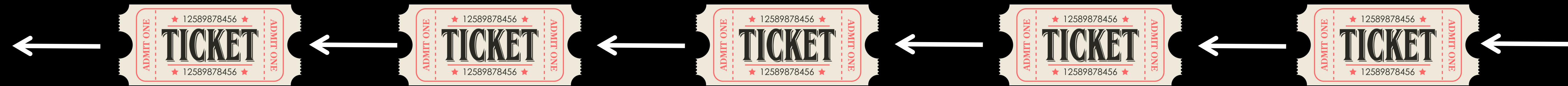
每一轮的 ticket 就是一个签名

new_ticket 的值依赖于:

- 1) 前一轮的Ticket值;
- 2) 爆块矿工的签名 (私钥)



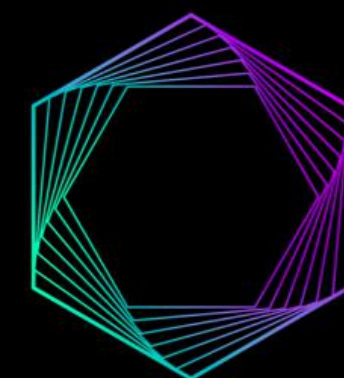
Tickets 的运算



`old_ticket := sort(parentTickets)[0]`
`new_ticket := Sig(VDF(H(old_ticket)))`

问题： 当一个Tipset有多个区块怎么办？

- 每个区块都有效
- 当有效 Ticket 只有一个，哪一个？ 最小的那一个

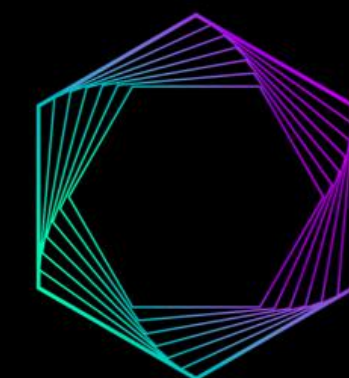


CreateTicket in 0.2.2

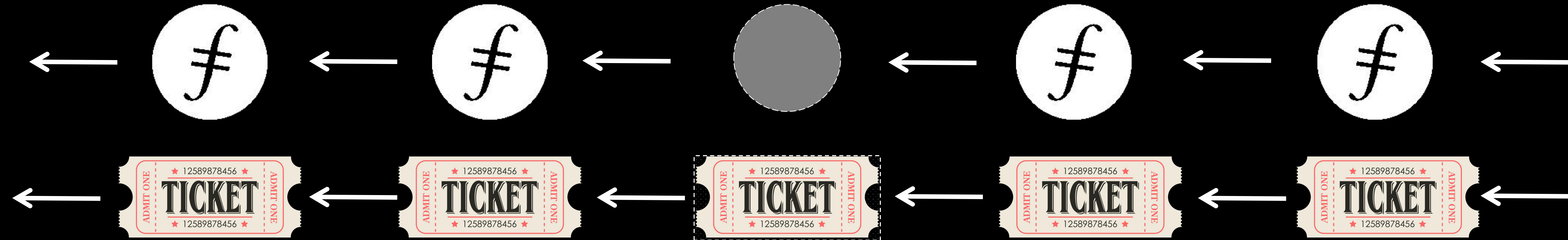
In `go-filecoin/consensus/expected.go`

```
func CreateTicket(proof types.PoStProof, signerPubKey []byte, signer TicketSigner) (types.Signature, error) {  
  
    var ticket types.Signature  
  
    signerAddr, err := signer.GetAddressForPubKey(signerPubKey)  
    if err != nil {  
        return ticket, errors.Wrap(err, "could not get address for signerPubKey")  
    }  
    buf := append(proof[:], signerAddr.Bytes()...)  
    // Don't hash it here; it gets hashed in walletutil.Sign  
    return signer.SignBytes(buf[:], signerAddr)  
}
```

- VDF函数还在实现中，目前采用 `sleep`
 - 很容易实现网络攻击？

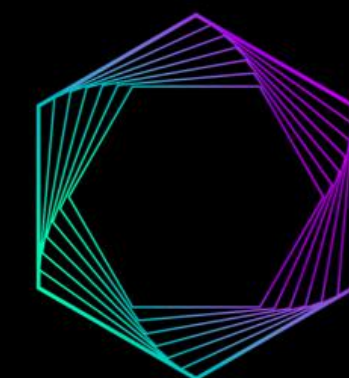


Lossing Ticket

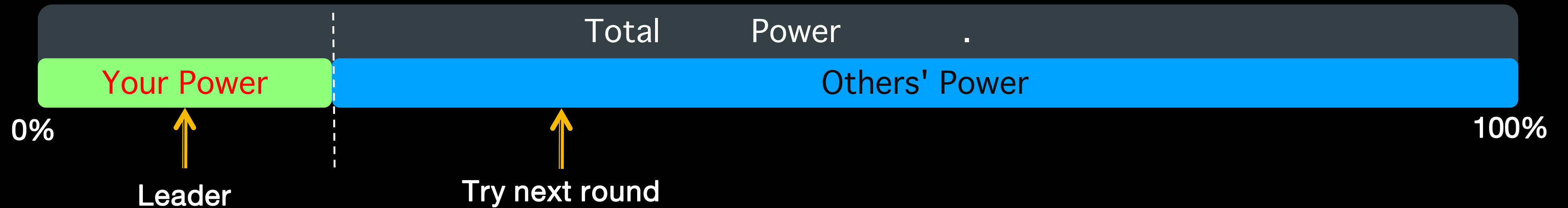


问题： 当一个高度出现空块怎么办？ Ticket如何计算？

- 如果没有收到合法的区块，矿工自动加入空块进行计算 (lossing ticket)
- 也就是说，下一个有效矿工实际上计算了两个或更多连续的 tickets
- 每一轮中，Tipset可以空缺，但Ticket不会



Who is the Winner



左：根据ticket和矿工签名计算的看结果

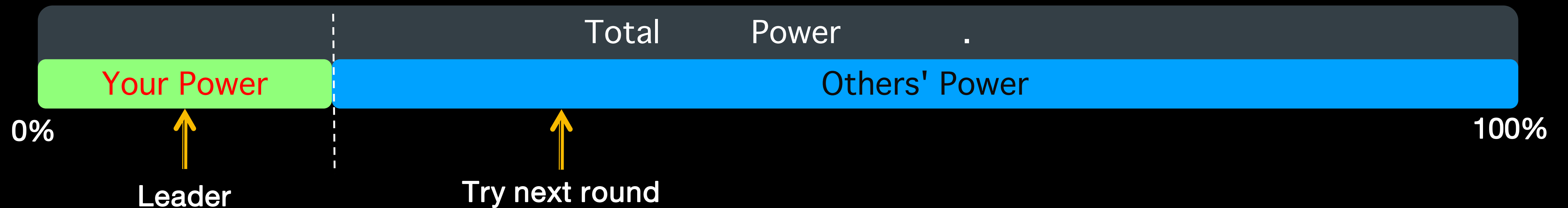
$$\mathcal{H}(\langle t || \text{rand}(t) \rangle_{\mathcal{M}_i}) / 2^L \leq \frac{p_i^t}{\sum_j p_j^t}$$

右：矿工算力占全网算力的比例

- 对一个矿工而言，如果在一轮中上面不等式成立，即成为 Leader
- 不等式右边是矿工的算力占比，代表了矿工成为leader的可能性
- 不等式左边是一个无法预测的 0 ~ 1 之间的随机数；代表了矿工的运气



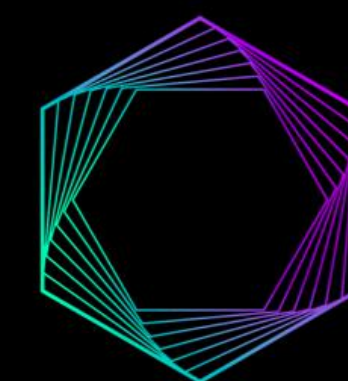
如何验证?



$$\mathcal{H}\left(\langle t || \text{rand}(t) \rangle_{\mathcal{M}_i}\right) / 2^L \leq \frac{p_i^t}{\sum_j p_j^t}$$

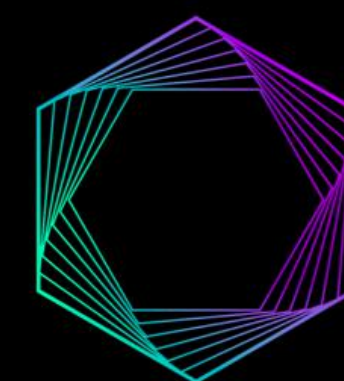
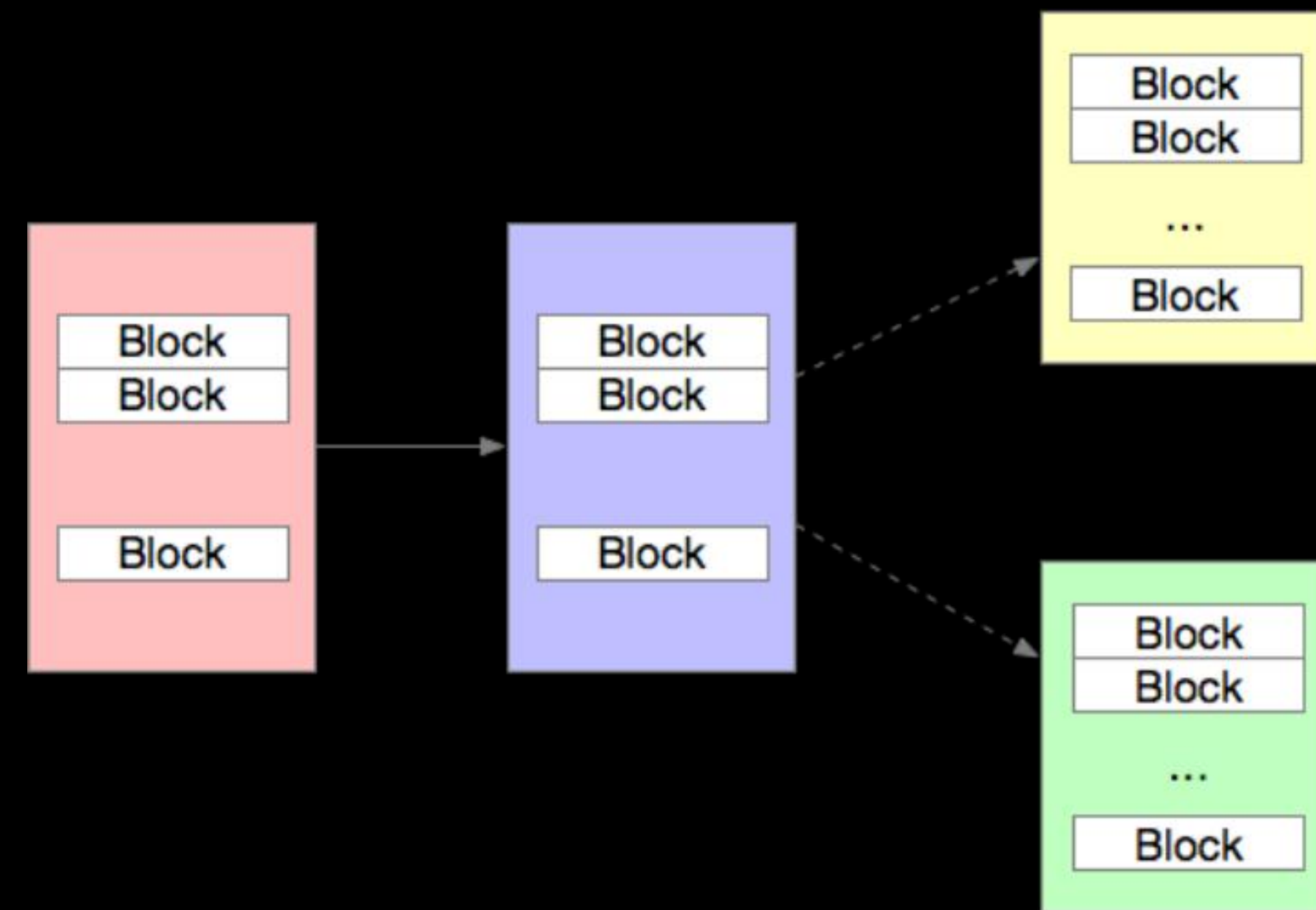
$$\langle m \rangle_{\mathcal{M}_i} := \left((m), \text{SIG}_{\mathcal{M}_i}(\mathcal{H}(m)) \right)$$

- 参见右式，矿工会在发送的区块信息中包含右式中的信息
- 即，包含合法的Ticket（一个全网可验证的随机数），
- 以及自己的签名，可以公开被验证



分叉？

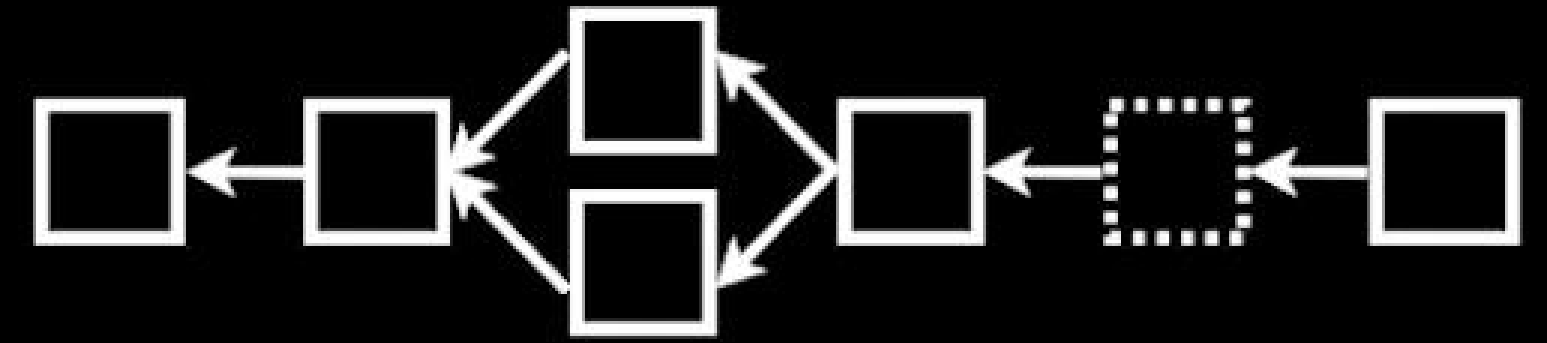
- 每一轮可能出现多个Leader
- 会出现多个区块，每个区块可以有选择性地打包消息
- Tipset 是区块的组合，当有多个区块时，组合可能有多种
 - 每一种都是合法的
- 分叉就出现了，。。。。



分叉处理 - 最重链法则

- 最重链法则
 - 当出现分叉时，挑选最重的一条链
- 每一个区块都会为链增加重量
 - 最重链法则保证了更多的消息被处理
- 每个矿工每一轮只能选择一条链
 - 如果同时延展两条链，则会遭到严厉惩罚 - 取缔挖矿资格

链的重量



$$W_t = W_p + \sum(\alpha + \delta) \text{ with } \begin{array}{l} \alpha \text{ constant} \\ \delta \text{ leader-based tie-breaker} \end{array}$$

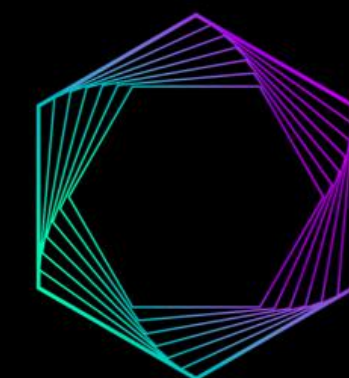
- 链的最新tipset会反映当前链的重量，计算方法：
 - 上一个tipset重量， 加上
 - 每一个区块带来的新的重量： 一个常量 (10) + $\log(\text{TotalPower})$
- 连续的链比跳空的链更重； 包含更多区块的tipset更重



Weight in v0.2.2

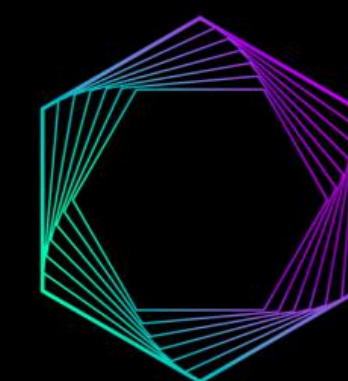
$$\text{Weight} = \text{ParentWeight} + \text{Sum}(\text{ECV} + \text{ECPrM} * \text{miner_power_ratio})$$

- Weight: defined in consensus/expected.go
- Weight at height 0 == 0
- $\text{ECV} = 10$, $\text{ECPrM} = 100$: EC中的常量定义
- It can be estimated that weight increasing by about 10~110



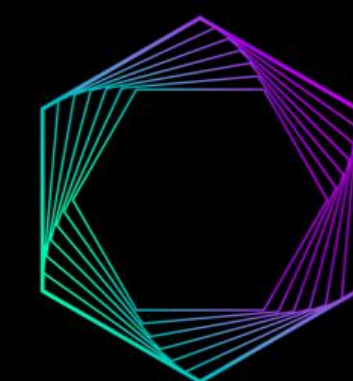
Weight/Height: distribution of network

- Discussion
 - You could find secrets from numbers ...
 - How



Attack the network

- Blank block attack (especially without VDF)
- Weight related Attack, ...
 - Block withholding
 - Large-power miner self-mining ...



Open Questions

- Parameter K, Parameter L
- Checkpointing Strategy
- Block confirmation time
- When selecting between two forks of equal weight, one strategy might be to select the 'Tipset' with the lowest number of linked tickets for a given block height and weight.

Should there be a minimum power required to participate in the consensus process?

How long should 'valid' candidate blocks be kept around? Essentially the question is: when is finality?

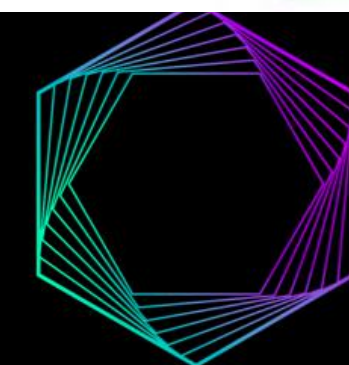
How should block rewards be assigned in the expected consensus setting?

VDF difficulty adjustment

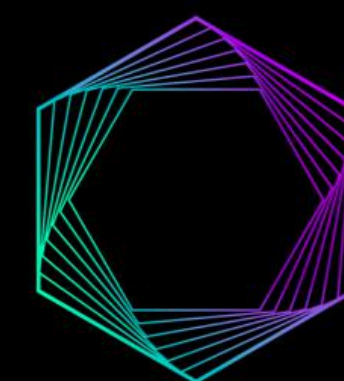


共同探讨学习

- [Filecoin共识机制的探索](#)
- [对Filecoin-0.2.2开发网络的攻击手法的分析?](#)
- [【IPFS/Filecoin】存储交易的达成和收费](#)
- [【Filecoin】理解预期共识 - 及它的优缺点](#)
- [Filecoin 存储证明 浅析](#)
- [Filecoin 挖矿 远比 Bitcoin 复杂](#)
- [【协议学院】Filecoin 存储封印和证明初步解析](#)



谢谢



ProtoSchool
Shanghai Chapter