代码思路

模型构建

节点

构建 `Node` 结构体表示节点。其属性包括：

- `id` ：节点ID
- `cnt` ：该节点挖出的区块
- `tail` ：该节点本地存储的区块链数据
- `evil` ：指示是否为恶意节点

用无限循环的 `Run` 函数模拟节点的运行，只在接收到Round开始的信号时进行该轮工作。诚实节点的一轮工作包括：

1. 接收广播，将广播的区块链数据存入本地。
2. 尝试创建新区块（通过访问Random Oracle）。若在限定尝试次数内创建成功且是该Round内首个成功的节点，则将该区块加入本地区块链数据，并通过全局变量 `r_block` 公布给全局的区块链。
3. 结束这轮工作。

如果是恶意节点，则只以本地的区块链数据为准，不接收广播数据，也不会主动公布自己的新创建区块。由于恶意节点通常不会和诚实节点在一条链上工作，故用另一个全局变量 `evil_r_block` 指示恶意节点新创建的区块。

因为恶意节点间可以通信，相互之间不会竞争，所以这里将恶意节点抽象成一个节点。它的算力是所有恶意节点的算力总和（通过改变尝试次数实现）。

区块链

构建 `block` 结构体表示区块。其属性包括：

- `id` ：区块ID
- `source` ：产生该区块的节点
- `length` ：以该区块为尾部的区块链长度
- `time` ：产生该区块的时间（Round数）
- `previous` ：指示上一个区块

以其组成的链表来表示区块链。

初始化

0. 实现工具函数 `Random` 和 `length_of_chain` 。
1. 设置参数：节点数、每轮尝试次数、尝试成功率、恶意节点占比、恶意节点攻击方法
2. 初始化变量： `round` 、 `r_block` 、广播通道 `tail_chan` 和 `round_chan` 、异步工具 `WaitGroup` 和 `Mutex` 等。
3. 创建创世块：设置创世块的 `source` 为 -1 ， `length` 为 1 。
4. 启动节点：利用goroutine初始化并启动所有节点，节点ID为 0,1,2,... 。如果有恶意节点，则默认恶意节点ID为 0 。

模拟全诚实节点运行

1. 将区块链数据和Round开始的信号广播至各节点。
2. 等待各节点本轮运行结束（利用 `WaitGroup` ）。
3. 检查 `r_block` 。若有区块数据，则检查其作为尾部的区块链长度是否比现在的链更长。若是，则更新区块链数据。

模拟恶意节点分叉攻击

让诚实节点正常运行，产生5个区块之后恶意节点再展开攻击。

1. 记录当前区块链长度，更新恶意节点链的数据。
2. 将区块链数据和Round开始的信号广播至各节点。
3. 等待各节点本轮运行结束（利用 `WaitGroup` ）。
4. 检查 `r_block` 。若有区块数据，则检查其作为尾部的区块链长度是否比现在的链更长。若是，则更新区块链数据。
5. 检查 `evil_r_block` 。若有区块数据，则更新恶意节点链的数据。
6. 若某个链已比开始时记录的长度多了6个区块，则进行结算：诚实节点/恶意节点取得胜利。

模拟恶意节点自私挖矿攻击

让诚实节点正常运行，产生5个区块之后恶意节点再展开攻击。

1. 更新恶意节点链的数据，开始记录恶意节点的收益。
2. 将区块链数据和Round开始的信号广播至各节点。
3. 等待各节点本轮运行结束（利用 `WaitGroup` ）。
4. 等待恶意节点成功创建区块，否则正常运行。
5. 若某轮恶意节点成功创建区块，则保留该区块。下一产生新区块的轮次里，
    - 若恶意节点产生区块，则恶意节点收益+2。
    - 若诚实节点产生区块且恶意节点未产生区块，则进行竞争：50%的概率选择恶意节点保留的区块，恶意节点收益+1；否则，恶意节点无收益。

实验结果分析

设置参数：

- 节点数 `node_num` = 100
- 每轮尝试次数 `chances_per_round` = 10
- 尝试成功率 `hash_probability` = 1e-6
- 恶意节点占比 `evil_node_ratio` = 0.1/0.2/0.3/0.4
- 恶意节点攻击方法：分叉攻击 / 自私挖矿攻击

各运行约30万轮，得到以下结果。

模拟恶意节点分叉攻击

```
Round: 294130
Tail Block: N61-B2
Chain Length: 297
Average Growing Speed: 990 rounds per block

Round: 295517
Tail Block: N99-B9
Chain Length: 298
Average Growing Speed: 991 rounds per block

Round: 295527
Tail Block: N84-B3
Chain Length: 299
Average Growing Speed: 988 rounds per block

Round: 295968
Tail Block: N71-B2
Chain Length: 300
Average Growing Speed: 986 rounds per block

Round: 296063
Tail Block: N81-B2
Chain Length: 301
Average Growing Speed: 983 rounds per block

Round: 296168
Tail Block: N49-B4
Chain Length: 302
Average Growing Speed: 980 rounds per block

Round: 298064
Tail Block: N84-B4
Chain Length: 303
Average Growing Speed: 983 rounds per block

Round: 298650
Tail Block: N12-B5
Chain Length: 304
Average Growing Speed: 982 rounds per block
```

区块链的增长速度约为980 rounds/block。

模拟恶意节点分叉攻击

恶意节点占比	0.1	0.2	0.3	0.4
分叉攻击成功率	0	0	0.09	0.32

分叉攻击的成功率随着恶意节点的占比降低而急速降低。即使恶意节点占比40%，分叉攻击成功的概率也不高。

模拟恶意节点自私挖矿攻击

恶意节点占比	**0.1**	**0.2**	**0.3**	**0.4**
区块链长度	267	268	250	244
自私挖矿攻击收益	13	49	65	80
收益比例	0.05	0.18	0.26	0.33

恶意节点自私挖矿收益占总区块链长度的比例总体不高。但由于恶意节点连续生成2个块就会公布到区块链系统里，因此比分叉攻击更容易成功。