

数字货币和区块链

山东大学网络空间安全学院

钱宸 2023年11月29日

- 共识与区块链

区块链与共识协议

- 简介与历史
- 拜占庭广播与Dolev-Strong协议
- 拜占庭广播（无签名）
- 区块链
- 区块链协议

简介与历史

- 共识协议：
 - 分布式共识协议的优点
 - 能够保证在分布式协议中，恶意或损坏的计算节点不影响最终结果（类似纠错码的作用）
- 历史：
 - 飞机控制系统
 - Google和Facebook的基础设施
 - 2009年以来被用于数字货币等

一些简单的说明

- 共识协议

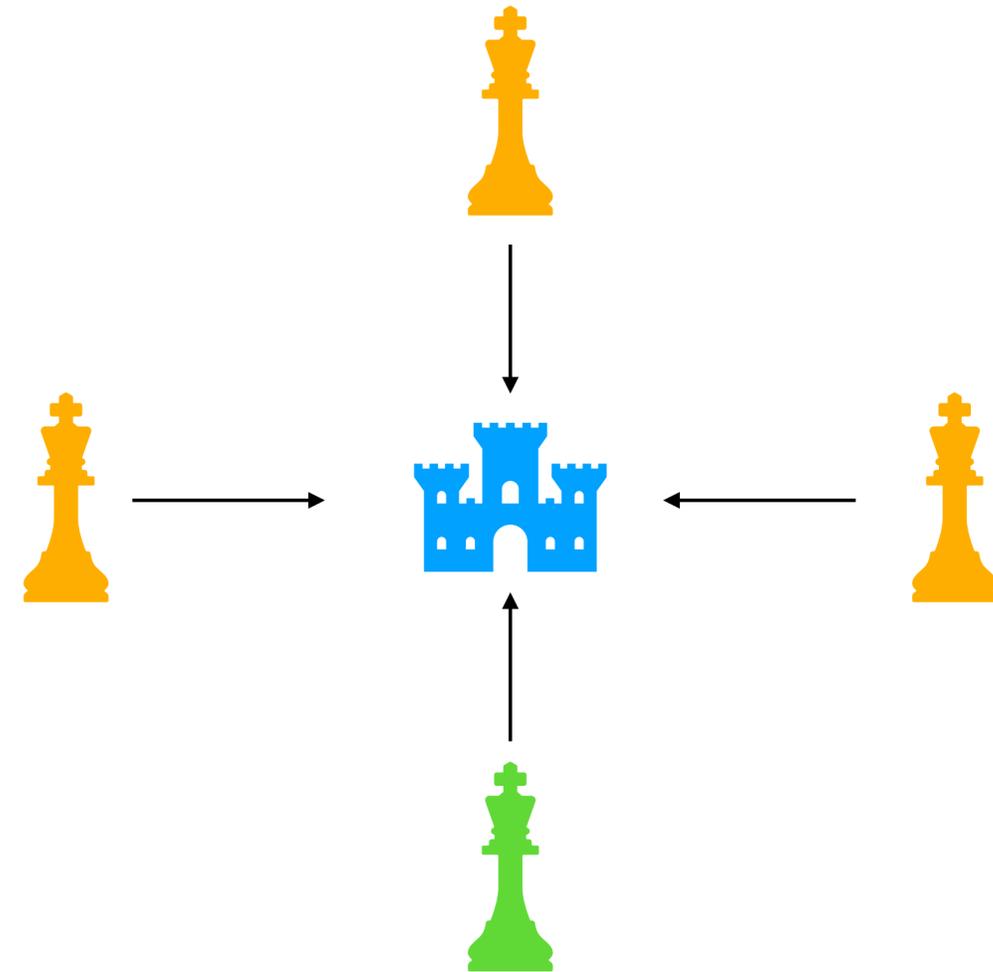
- N 方(P_1, P_2, \dots, P_n)参与计算, 最终获得共识 C

- 攻击者

- 在协议开始之前选定一个集合 $S \subseteq [n]$ 破坏
- $\forall i \in S. P_i$ 不用遵守协议, 可以任意计算发出的值
- 所有 S 集合中的用户, 可以共谋。

拜占庭协议 (Lamport, Shostak, Pease '82)

- 多个将军攻击一个城池
- 只存在两两之间的信息交互
- 有叛徒存在，叛徒可以传递任何信息
- 其中有一个大将军发号施令
- 所以会出现一下三种情况：
 - 所有人都进攻→攻下城池✓
 - 所有人都撤退→无损伤撤退✓
 - 一部分人进攻一部分人撤退→失败✗



拜占庭将军协议 - (拜占庭广播)

- 目标：
 - 所有诚实的将军都会做同样的决定
 - 如果发号施令的大将军是诚实的，则所有诚实的将军都会遵守相同的决定
- 注意：
 - 如果大将军肯定是诚实的，那么问题是显然的
 - 所有人只要遵守大将军的指令即可

可信分布式系统

- 对应到分布式系统中
 - 每一个节点都有可能失败
 - 通信都是1对1发送
 - 最终要达成共识

现实中的例子

- 考试开卷还是闭卷？
- 最简单的方法是老师来发布通知。（“诚实大将军”情况）
- 班长一对一通知，
 - 可能有部分同学不想考试。。所以，会不诚实遵守协议（“非诚实将军”）
 - 也有可能班长自己也不想考试（“非诚实大将军”）
 - **目标：**所有想考试的同学都能达成共识

具体定义

- **计算节点**：假设一共有 n 个计算节点，被定义为 $P = \{1, 2, \dots, n\}$ 。
 - 定义其中1号为“大将军”，信息发布者 s
 - 遵循协议的用户被称为诚实的
 - P 中有一部分用户 $T \subseteq P$ ，不遵守协议可以在任意时间，发送给任意用户任意信息。被称为叛徒。且叛徒也可以共谋，信息共享。
 - 通常可以模拟成为一个用户控制所有叛徒
 - 我们不知道谁是叛徒，否则的话协议也是简单的

具体定义

- 通信模型：
 - 一对一通信
 - 每一个用户都有自己的签名公私钥，保证通信传输不会被更改
 - $\langle m \rangle_i$ 表示 (m, σ) 其中 σ 是 m 能被用户 i 的公钥验证的签名
- 通信模式：
 - 同步通信模型，每一次信息发出都会在一轮内到达（本课程默认模式）
 - 非同步通信模型

具体定义

- 叛徒模型：
 - 叛徒必须是在协议开始执行之前就选定 - 静态叛徒模型（本课程默认设定）
 - 叛徒可以在协议执行期间选定 - 动态叛徒模型

拜占庭广播协议

- 运行：
 - 由信息发布者 s 收到一个比特 $b \in \{0,1\}$
 - 所有的用户集合 P 分成叛徒集合 T 和诚实用户集合 H 。即： $P = T \cup H$ 且 $T \cap H = \emptyset$
 - 开始运行协议，协议结束后每一个诚实的用户都输出一个比特 b_i
- 保证以下性质：
 - 一致性： $\forall i, j \in H. b_i = b_j$
 - 正确性：如果所有信息发布者 s 是诚实的且收到的信息是 b ，则 $\forall i \in H. b_i = b$

尝试

- 最简单的尝试：
 - 第一轮： P_1 随机选择一个比特 b ，并将 $\langle b \rangle_1$ 发送给所有用户（包括他自己）
 - 第二轮： 所有用户输出自己收到的比特。
- 一致性？
 - 如果 $1 \in H$ (P_1 是诚实的)，则协议保证一致性
 - 如果 $1 \in T$ (P_1 是叛徒)，则无法保证协议一致性

再次尝试

- 总结上述，发现要让诚实的用户达成一致→加入投票机制
- 想法：假设一共有 $2k + 1$ 个人，其中最多 k 个叛徒，那么投票产生结果
- $(2k+1)$ 个用户
 - 第一轮： P_1 随机选择一个比特 b ，并将 $\langle b \rangle_1$ 发送给所有用户（包括他自己）
 - 第二轮：所有用户将自己收到的比特发送给所有人
 - 第三轮：每个用户发送自己收到最多的比特
- 这个协议满足一致性要求么？ ❌

再次尝试

- $(2k+1)$ 个用户
 - 第一轮: P_1 随机选择一个比特 b , 并将 $\langle b \rangle_1$ 发送给所有用户 (包括他自己)
 - 第二轮: 所有用户将自己收到的比特发送给所有人 (包括用户自身)
 - 第三轮: 每个用户发送自己收到最多的比特
- 攻击: 将 $(2, \dots, 2k+1)$ 的 $2k$ 个用户分成 S_0 和 S_1 两个不同的集合
 - P_1 发送 $\langle 0 \rangle_1$ 给所有 S_0 中的用户; P_1 发送 $\langle 1 \rangle_1$ 给所有 S_1 中的用户
 - P_1 投票 $\langle 0 \rangle_1$ 给所有 S_0 中的用户; P_1 投票 $\langle 1 \rangle_1$ 给所有 S_1 中的用户

再再次尝试 - Dolev-Strong (SIAMCOMP '83) 协议

- 假设有 k 个叛徒，一共有 n 个用户参与协议：
- 运行：每个用户都有一个集合 extr_i ，初始状态为空集
 - 第0轮： P_1 随机选择一个比特 b ，并将 $\langle b \rangle_1$ 发送给所有用户（包括他自己）
 - 第 r 轮（ $r = 1$ 到 $k+1$ ）：
 - 收到消息 $\langle \bar{b} \rangle_{1,j_1,\dots,j_{r-1}}$ ，如果 $\bar{b} \notin \text{extr}_i$ ，则 $\text{extr}_i = \text{extr}_i \cup \{\bar{b}\}$
 - 并将 $\langle \bar{b} \rangle_{1,j_1,\dots,j_{r-1},i}$ 发送给每一个用户
 - 结束的时候如果 $|\text{extr}_i| = 1$ ，则输出该比特，否则输出0

Dolev-Strong协议

- 为什么Dolev-Strong协议安全？为什么Dolve-Strong协议需要 $k+2$ 轮？
- 几个想法：
 - 签名保证即使是叛徒也无法更改信息内容
 - 假设只有 k 轮：
 - (错误) ~~两个诚实的用户 (其中之一是信息发送者)~~， k 个叛徒
 - (正确) 一共有 k 个叛徒，包含信息发送者。
 - 第0轮，发送 $\langle 1 \rangle_1$ 给每个用户
 - 第 k 轮，伪造一个 $\langle 0 \rangle_{1,j_1,\dots,j_{k-1}}$ 发送给一个诚实的用户
 - 一个诚实的用户输出0，其他输出1

Dolev-Strong协议

- 一致性、正确性
- 正确性：
 - 如果信息发送者是诚实的
 - 那么 $\langle 1 - b \rangle_1$ 中的签名从来没有出现过
 - 所以，所有的诚实用户都会返回 b

Dolev-Strong协议

- 一致性：
 - 证明两个性质
 - 引理1: 令 $r \leq k$ 。如果第 r 轮结束的时候，某个诚实的用户 i ，对应的 extr_i 中有 \bar{b} ，则在第 $r + 1$ 轮结束的时候，每个诚实的用户的 extr_i 中都有 \bar{b} 。
 - 引理2: 如果第 $k + 1$ 轮结束的时候，某个诚实的用户 i ，对应的 extr_i 中有 \bar{b} ，则在第 $k + 1$ 轮结束的时候，每个诚实的用户的 extr_i 中都有 \bar{b} 。

Dolev-Strong 协议

- 引理1: 令 $r \leq k$ 。如果第 r 轮结束的时候, 某个诚实的用户 i , 对应的 extr_i 中有 \bar{b} , 则在第 $r + 1$ 轮结束的时候, 每个诚实的用户的 extr_i 中都有 \bar{b} 。
- 证明:
 - 挑选第一次 \bar{b} 进入 extr_i 的时候, 假设为第 t 轮。
 - 则在第 $t + 1$ 轮结束的时候所有诚实用户的 extr_i 中都有 \bar{b} 。

Dolev-Strong 协议

- 引理2: 如果第 $k + 1$ 轮结束的时候, 某个诚实的用户 i , 对应的 extr_i 中有 \bar{b} , 则在第 $k + 1$ 轮结束的时候, 每个诚实的用户的 extr_i 中都有 \bar{b} 。
- 证明: 分两种情况讨论。
 - 第一种: 假如 extr_i 在第 k 轮的时候就已经包含了 \bar{b} , 则根据引理1可得
 - 第二种: 如果 \bar{b} 实在第 $k+1$ 轮的时候新加入 extr_i 的:
 - 则我们观察可知, 第 r 轮加入的信息都包含 r 个签名。
 - 即: 新加入的 \bar{b} 包含 $k+1$ 个签名, 其中至少有一个是诚实的用户 j 。
 - 所以诚实用户 j 的 extr_j 在第 k 轮的时候就包含 \bar{b} , 所以由引理1可得。

Dolev-Strong 协议

- 一致性：
 - 引理1: 令 $r \leq k$ 。如果第 r 轮结束的时候，某个诚实的用户 i ，对应的 extr_i 中有 \bar{b} ，则在第 $r + 1$ 轮结束的时候，每个诚实的用户的 extr_i 中都有 \bar{b} 。
 - 引理2: 如果第 $k + 1$ 轮结束的时候，某个诚实的用户 i ，对应的 extr_i 中有 \bar{b} ，则在第 $k + 1$ 轮结束的时候，每个诚实的用户的 extr_i 中都有 \bar{b} 。
 - 所以，第 $k+1$ 轮结束的时候，所有诚实用户的 extr_i 都是相同的。
- 一致性可证。

一些讨论

- Dolev-Strong同时证明了任意确定性拜占庭广播都必须有 $k + 1$ 轮 (k 个叛徒)
- 但是在实际中，因为不知道叛徒人数，所以必须得 $n + 1$ 轮。
- 某些情况中十分低效：
 - 加入随机数可以降低轮数