数字货币和区块链

- 共识与区块链

山东大学网络空间安全学院

钱宸 2024年12月25日

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

中本聪区块链的安全性分析

- 现实区块:
  - (h_{-1}, η, txs, h)
- 理想化模型:
  - 每个区块(txs)
  - 每个计算节点可以询问向可信第三方$\mathcal{F}_{tree}$询问:
    - 挖矿请求: Mine$(chain, txs)$ 随机以概率p接收挖矿请求, 将$chain||txs$记录
    - 验证请求: Verify$(chain)$ 验证链是否成立

中本聪区块链

- 架设:每个诚实节点在第r轮见到一个消息,那么所有诚实节点都能在$r + \Delta$时间看见这个消息
- 理想化模型
  - 每个计算节点记录见过最长的链
  - 每一轮中,每一个诚实节点接收所有网络上的消息,如果任意看到的链满足
    - $\mathcal{F}_{tree}.\text{Verify}(chain') = 1$
    - $chain'$比$chain$长, 则替换$chain$并广播$chain'$
    - 请求$\mathcal{F}_{tree}.\text{mine}(chain, txs)$ 并将$chain \| txs$广播
    - 忽略最后k个区块作为最终区块链结果

简单标记

- 挖矿成功概率: p
- 总人数: n
- 敌手比例: ρ
- 每一轮诚实用户挖到区块的概率: $\alpha = p \cdot (1 - \rho)n$
- 每一轮敌手挖到区块的概率: $p \cdot \rho n$

收敛窗口

- 定义一个特殊的模式: 收敛窗口$[T-\Delta . T+\Delta]$
  - 对于任意$t \in [\max(0, T-\Delta), T)$ 没有诚实节点挖矿得到区块
  - 一个诚实的节点在T轮挖矿得到一个区块
  - 没有诚实节点在$t \in (T, T+\Delta]$得到一个节点
- 将收敛窗口简写成T. $C[t' : t]$为一个随机变量表示区间$[t' : t]$中有多少收敛窗口.

收敛窗口的发生概率

- 定理:
  - 对于任意η和关于λ的超指数κ, 下列事件发生概率大于$1 - negl(\lambda)$:
    - 对于任意$t_0, t_1 \geq 0$, 且$t := t_1 - t_0 > \frac{\kappa}{\alpha}$, 有
    - $C[t_0 : t_1] > (1 - \eta)(1 - 2pn\Delta)\alpha t$
    - 其中每一轮诚实用户挖到区块的概率: $\alpha = p \cdot (1 - \rho)n$

链增长率

- 如果收敛窗口发生, 最短的诚实链会至少增长1.
- 定理:
  - 对于任意轮数$t_0 \leq t_1$, 记录两个链$chain^{t_0}$, $chain^{t_1}$满足
  - $C[t_0 + \Delta : t_1 - \Delta] \leq |chain^{t_1}| - |chain^{t_0}|$

链增长率

- 对于任意时刻t, t_0
- 满足$|chain^{t_0+t}| - |chain^{t_0}| > (1-\varepsilon')(1-2pn\Delta)\alpha t$
- 简要说明:
  - $$\begin{aligned} & |chain^{t_0+t}| - |chain^{t_0}| \\ > & (1-\varepsilon)(1-2pn\Delta)\alpha(t-2\Delta) \\ \geq & (1-\varepsilon')(1-2pn\Delta)\alpha t \end{aligned}$$