目标

1. 一人一票
2. 特定的人群才能有投票权
3. 投票人可以验证自己的选票被最终计算

思路

因为第二点的貌似很难做到真正的匿名，**特定的人群** 即说明需要关联投票人的个人身份，理论上一旦关联了身份就不可能是匿名的了。

但我们可以通过以下两点来曲线保证做到严格匿名：

1. 第三方的验证机构只验证身份的群体有效性，不验证具体某元素。比如：只验证是某公司员工，而不细致到该公司的某个具体的人。
2. 隐私之所以会泄漏根本原因在于它被存储了，只要不存这些信息那么我们就可以做到匿名。

方案

步骤

准备阶段

1. DApp 生成随机字段 str
2. DApp 用身份验证服务器的公钥盲化 str 得到 blindStr

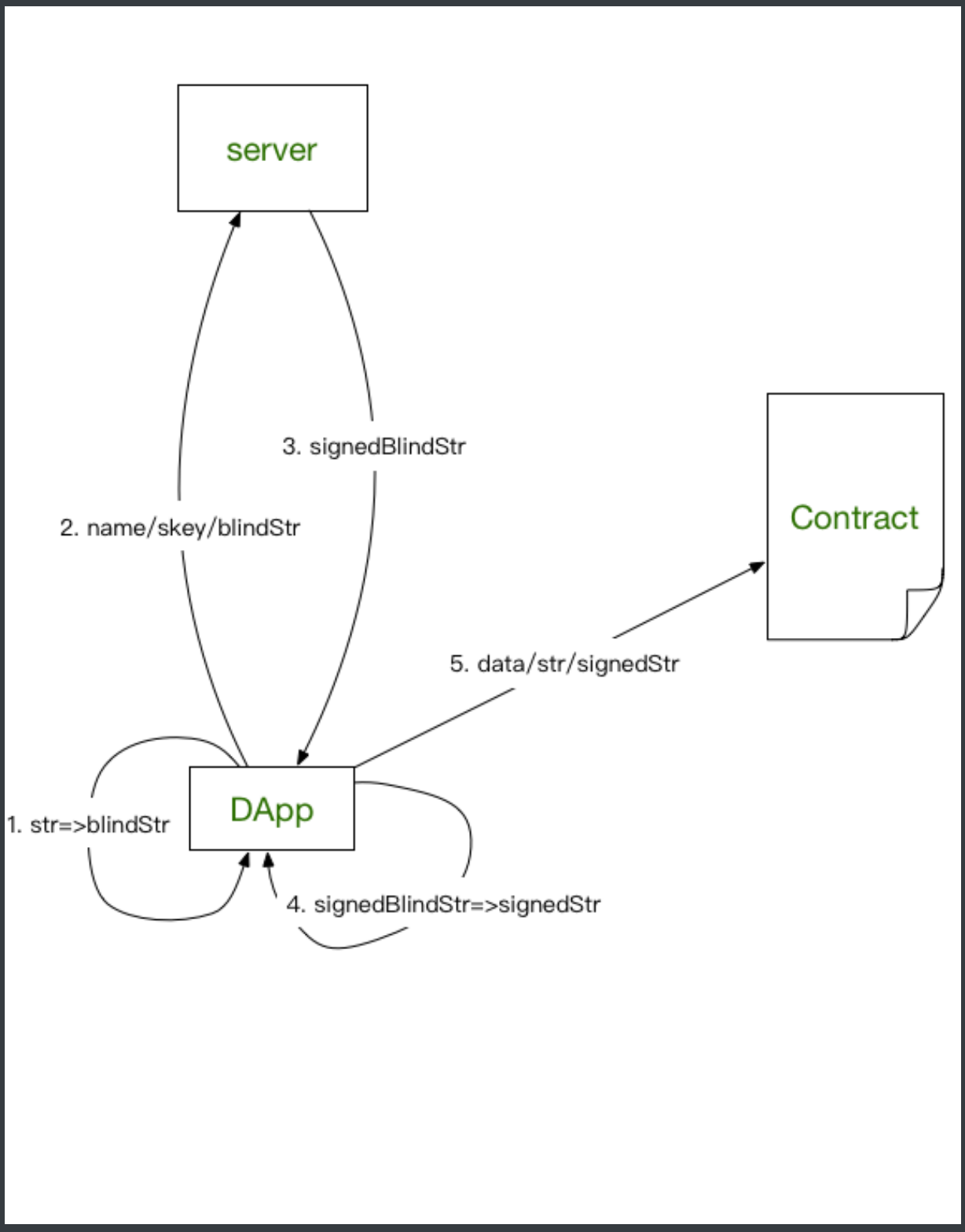
投票阶段

1. DApp 用 http 请求带上 name、skey 和 blindStr 调用第三方的身份验证服务，身份验证服务通过验证后用私钥对 blindStr 签名，返回签名的结果 signedBlindStr
2. DApp 对签名结果做去盲处理得到 signedStr
3. 将投票内容 data、signedStr 和 str 三者一起请求合约发起投票

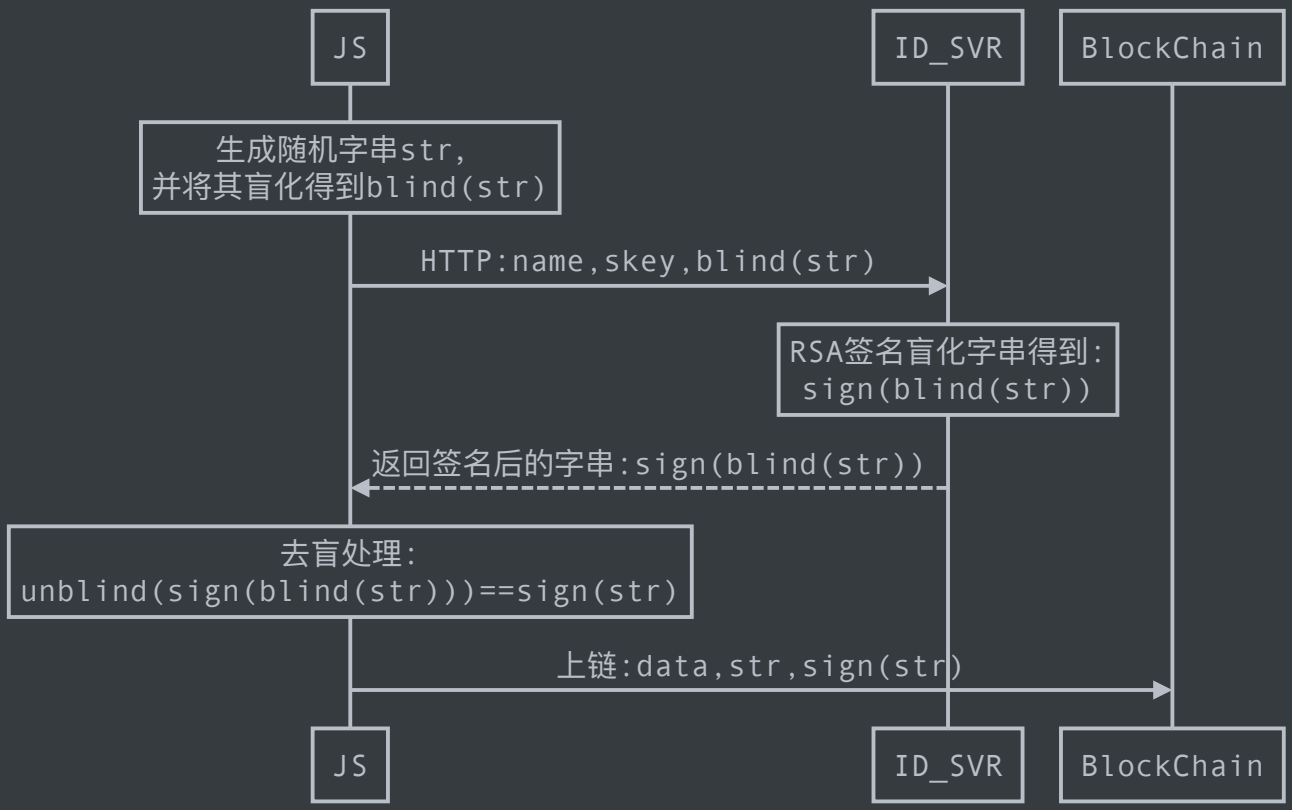
计票阶段

1. 各个 DApp 通过公钥验证 str 和 signedStr，开始常规计票逻辑

架构


server
3. signedBlindStr
2. name/skey/blindStr
Contract
5. data/str/signedStr
DApp
1. str=>blindStr
4. signedBlindStr=>signedStr

时序图


JS
ID_SVR
BlockChain
生成随机字串str,
并将其盲化得到blind(str)
HTTP:name,skey,blind(str)
RSA签名盲化字串得到:
sign(blind(str))
返回签名后的字串:sign(blind(str))
去盲处理:
unblind(sign(blind(str)))==sign(str)
上链:data,str,sign(str)
JS
ID_SVR
BlockChain