有关本文的背景，请参阅《二次方投票和二次方资助》。 在这篇文章发表一个月后，BSC基金会在DoraHacks开发者平台HackerLink上执行了BSC生态第一轮的平方资助在随后的15天里，我收到了全球60多个开发人员团队提交的项目。 [xy 002] [xy001]在Shuming hao123 @ QQ.com上，我介绍了Vitalik博客《Quadratic Payments》提到的三个问题：身份伪造攻击(Identity Bribery)、共谋、合理忽视问题(Rational Ignorance)。。
这三个问题其实并不局限于平方投票，而是链上治理机制面临的共同问题。 因此，这些问题的解决方案不仅可以使平方投票更规模化、更安全，而且可以惠及更多的链上治理机制。

本文的目标是为设计“不合作平方投票”或“抗共谋平方投票”的机制做准备。 在这种场合，投票者无法相互合作，没有勾结的可能性。
这个机制的基本框架之一是，Vitalik Buterin在Ethresear上发表的文章《Minimal anti-collusion infrastructure》 [1] (MACI)。 因此，首先说明MACI的机制因此，这是为了进一步探讨如何使用MACI改进平方投票，消除串通的可能性。

[xy001] maci :最小化协同框架。 背景资料见Vitalik Buterin的博客https://ethresear.ch/t/minimal-anti-collusion-infrastructure/5413、以及Shuming hao123 @ QQ.com https://vitalik.ca/general/2019/04/03/collusion.html [xy 002] [xy001]许多链中的管理APP案例但同时，也需要通过区块链执行和防范交易，保证隐私保护。 投票是有这种需要的重要场合。 在投票中显然需要抗共谋，同时对执行结果的准确性要求较高，需要保护投票过程，最后必须防止对投票者的审查。

设置假设存在智能协议(r)、公钥列表(k_1...k_n)和可以注册智能协议的所需函数。 另外，其他的中选择所需的族。 只有满足以下两个条件的参与者的公钥才能访问

帐户属于“合法”参与者(独立人、社区成员)例如，某个国家的国籍，在论坛中享有充分的声誉，拥有某个数量以上的Token...)

帐户的所有者个人控制密钥(例如，可根据需要打印证明)

每个用户都需要钱在stake上。如果每个人泄露了自己的私钥，得到私钥的人可以直接拿走这笔钱，该帐户将从列表中删除。
这个机制抑制了任何人把私钥交给别人。

还有假设您有一个操作符(“操作符”)。 假设他有私钥(k_omega)和相应的公钥(k_omega).[xy 002] (xy001)最后，机制(m)。
那是函数)是action^n

ightarrowoutputs] (其中函数的输入是(n
)个参加者的行为，输出是该函数定义的某种输出结果。
例如，简单的投票机制是基于输入的值的函数输出出现次数最多的值。

运行开始时间(T_{start}))。(operator)开始实际状态(s _ { start }=(I :)
key=k_I，action=phi) }，i in 1.n).

)在

开始时间(T_{start})和结束时间(T_{end}
)之间，任何注册参与者可将由该参与者自己的私钥) k)加密的消息传输到r。

约定行为：如投票。 参与者必须发送加密消息(enc(msg=(I，sign)
msg=action，key=k_i))、pubkey=K_omega)。 其中) k_i
)是此参与者的当前私钥、I)是参与者的(r)中的id

更新密钥：参与者加密了的消息(enc) msg=(I，sign) msg=newk_I，key=k_i))

此时，操作者的工作是按照消息上的链接优先级处理每个消息。
具体处理过程：使用

操作符的私钥解密消息。 如果解密失败，或者无法解密对应的信息，则为上述两种信息、使用state[i].key验证消息的签名

解码消息的约定行为(例如中选择所需的族。
(如果设置了state[i]=action，并且解码的消息是新的公钥，则) state [I
].key=newk _ I] [xy 002] [xy001]为) T_{end}、运营商必须公布输出状态((m)
state[n].action，state[n].action))))，同时ZK-SNARK

为什么这个机制抗共谋？ 假设参与者想证明他们做了什么。 例如(action)) a)
)。另外，他可以引用链上的交易(enc) msg=(I，sign) msg=a，key=k_i)
)，并提供知识零的证明另外，验证该交易确实是包含(a)的加密信息。
但是他不能证明他没有发行其他交易。 例如，之前的证明也变得没有意义，因为他可能发行了更早的交易，将公钥更换为新的(NewK_i
)因为，如果他交换过钥匙，他可能已经做了别的动作。

参与者也可以将私钥传递给其他人，这样该人就可以获得私钥并立即尝试修改密钥。 这样做的话1)有50%的成功率2)得到钥匙的人会直接拿走以前stake的存款。

[xy 001]如果maci的未解决问题的接收者位于受信任的硬件环境中，或者接收者具有受信任的多符号，则出售私钥[xy 002]

传统私钥在可信硬件环境中的攻击。 在第一种情况下，该环境可以防止攻击者将私钥改变为他们事先不知道的私钥。通过特别设计的复杂签名机制，该环境对可信硬件和多个签名不友好。 但是，该设计需要保证验证函数对ZKP友好。

第二种情况可以用“面对面零知识证明”解决。 例如，参与者可以将私钥分解为(x y=k_i)。、(X=x*G)和) Y=y*G)并分别向验证者展示包含(x)和(y)的两个信封。验证者打开一个，检查并检查公开的(y)是否正确(X Y=K_i)。

不合作平方投票这一机制可用于改善包括投票在内的各种链上的管理机制。 平方资助中，如果资金池规模非常大，或者平方资助用于更大场景(例如选举、国会批准预算等场景))。串通成为一个必须解决的问题。
因此，可以设计抗串通的平方投票(Anti-collusion quadratic funding)机制，扩大规模，平方资助资金。