

# WeHeart

基于区块链的慈善共创平台

**FinTechathon** - 2021

微众银行第三届金融科技高校技术大赛

# 目录

01 社会现状

DATA SCAN 100%

02 平台设计

DATA SCAN 100%

03 亮点总结

DATA SCAN 100%

04 系统展示

DATA SCAN 100%

# 目录

01 社会现状

DATA SCAN 100%

02 平台设计

DATA SCAN 100%

03 亮点总结

DATA SCAN 100%

04 系统展示

DATA SCAN 100%

# 社会现状—慈善的价值



帮助贫困、弱势群体，  
让他们感受到社会的关爱

今报网 JINBW.COM.CN 首页 > 新闻频道 > 河南 新闻线索在线提交

## 10余天募集善款13.64亿元，郑州水灾背后的慈善引领

| 首页 > 慈善新闻

捐款7000万元，111万人参与 郑州慈善“99公益 爱满绿城”硕果累累 助力灾后重建(图文)

2021-09-16 505J-06-09

面对重大灾难时慈善的力量

# 社会现状—慈善的公众参与

2015 - 2020 公众捐款比重变化表

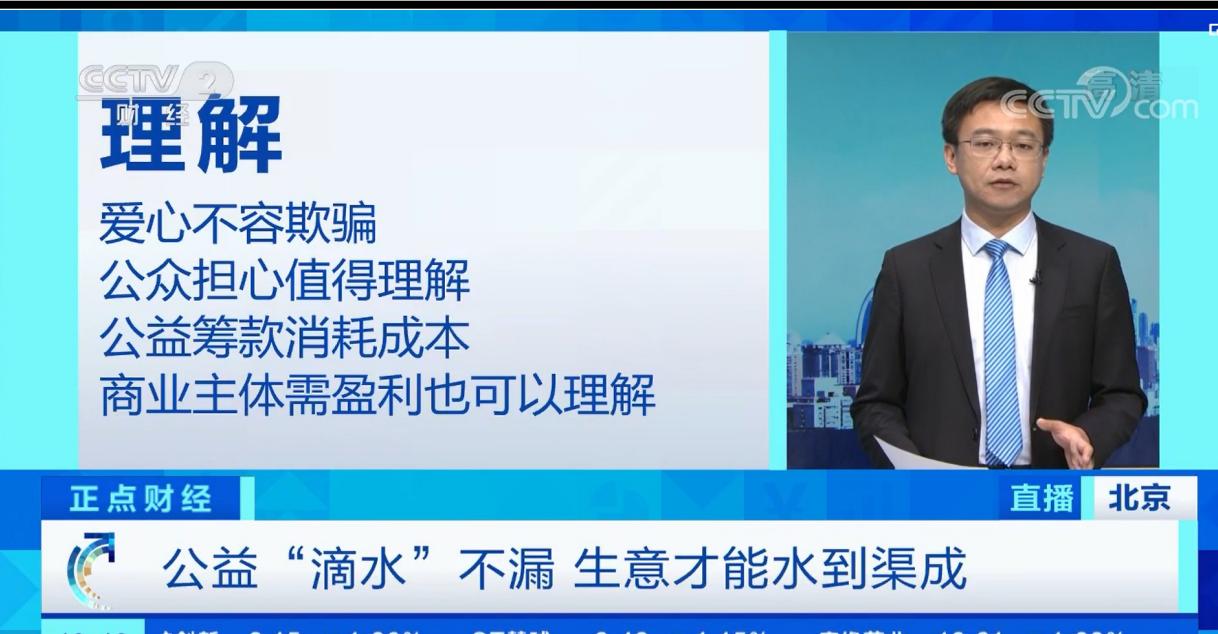


2015-2020 “99 公益日”

活动累计募集善款 90.89 亿元  
1.55+亿人次参与捐款。

在捐赠主体方面，公众捐款是善款的**第一大来源**，且公众捐款在总善款中的占比呈现上升趋势。

# 社会现状



但是，在慈善事业发展过程中，浮现出  
一些引起社会广泛关注的问题



# 目录

01 社会现状

DATA SCAN 100%

02 平台设计

DATA SCAN 100%

03 亮点总结

DATA SCAN 100%

04 系统展示

DATA SCAN 100%

# 平台设计—方案架构

## WeHeart 慈善共创平台



# 平台设计——设计初衷



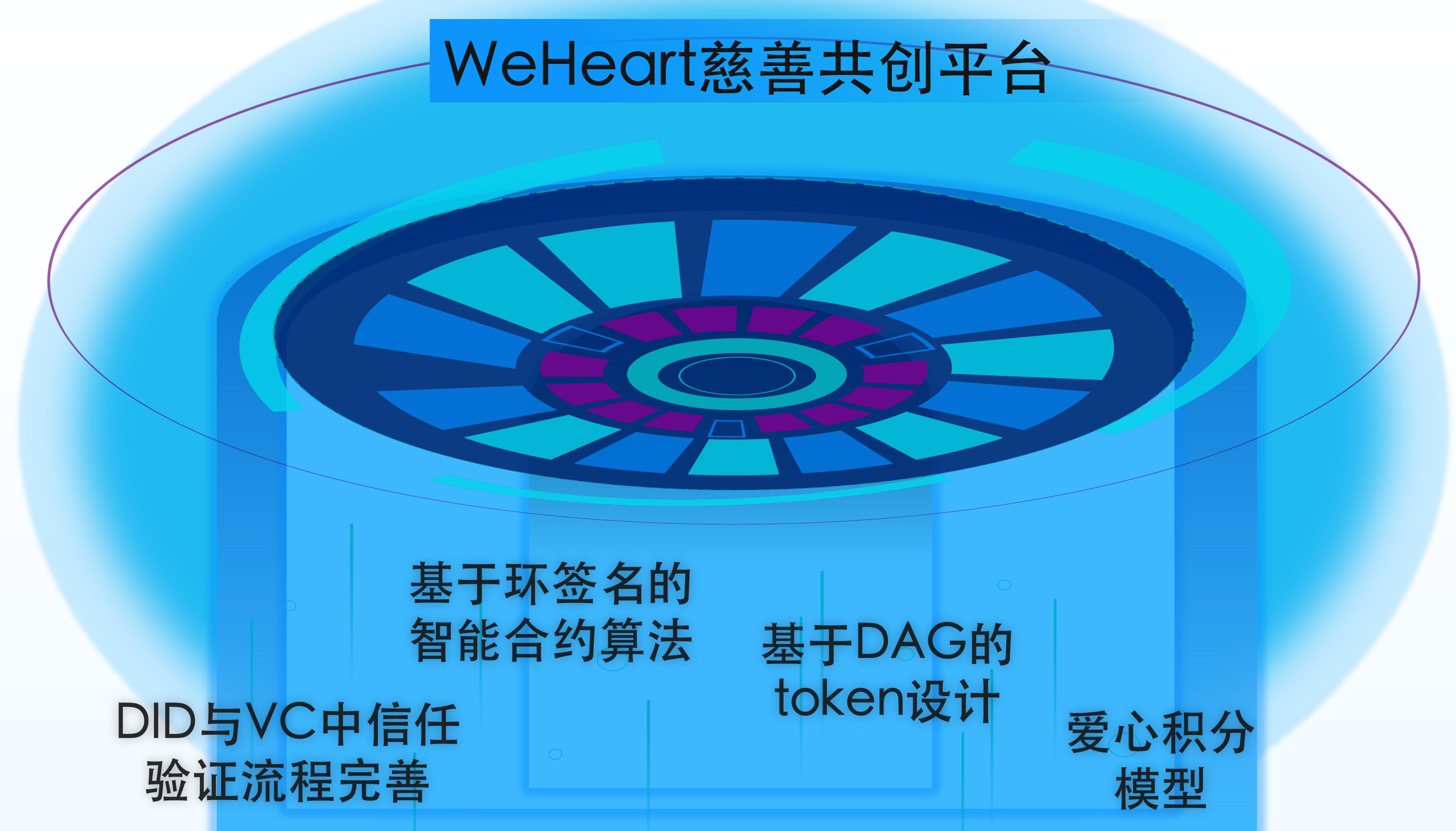
针对大众的**质疑**，保护  
个人**隐私**，传承“**好人  
有好报**”

系统旨在通过**公益凭  
证**、**智能合约**、**慈善激励  
机制**，达到**倡导全民慈  
善**、**促进社会担当的目的**

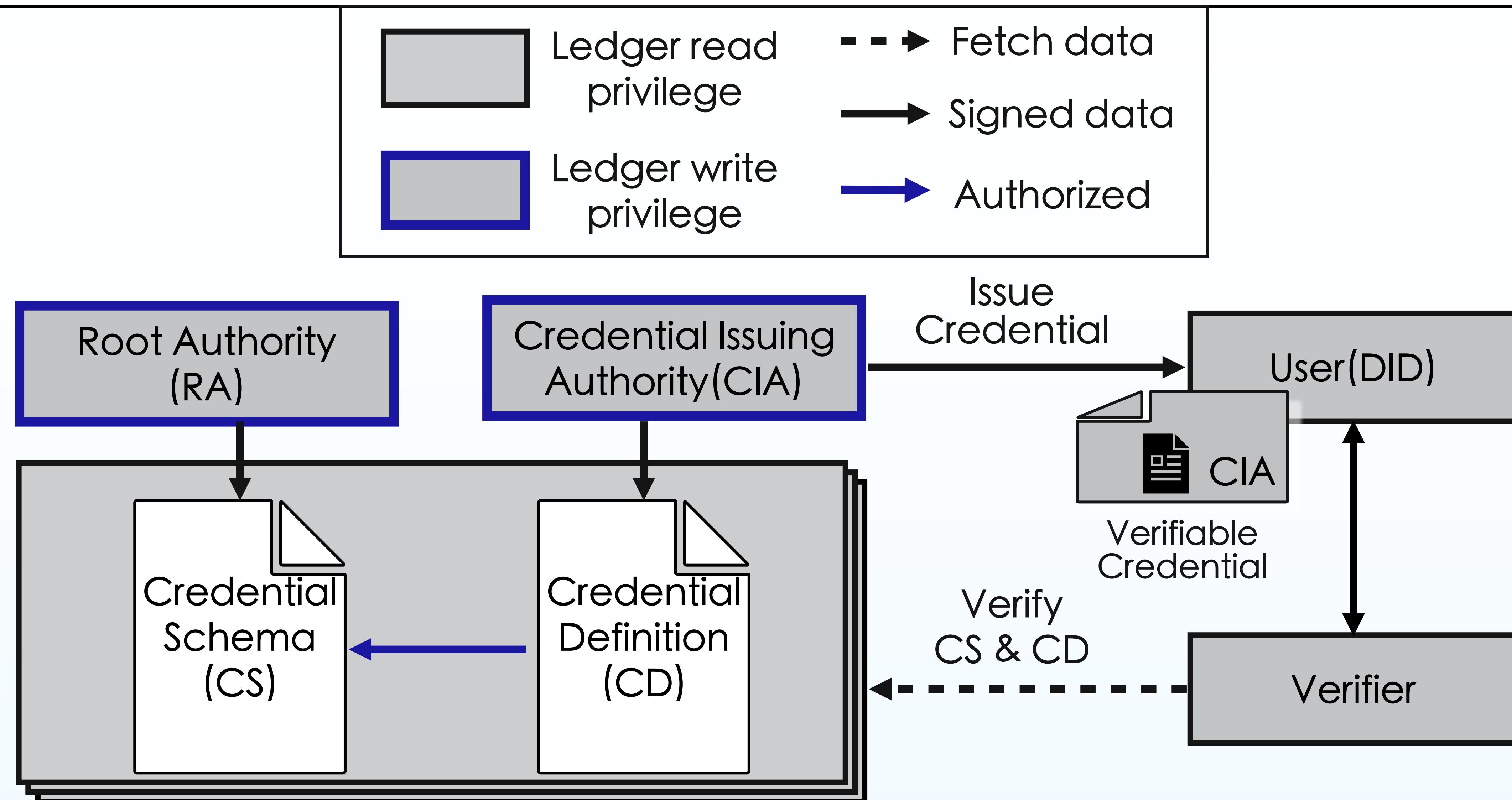
# 平台设计——设计理念



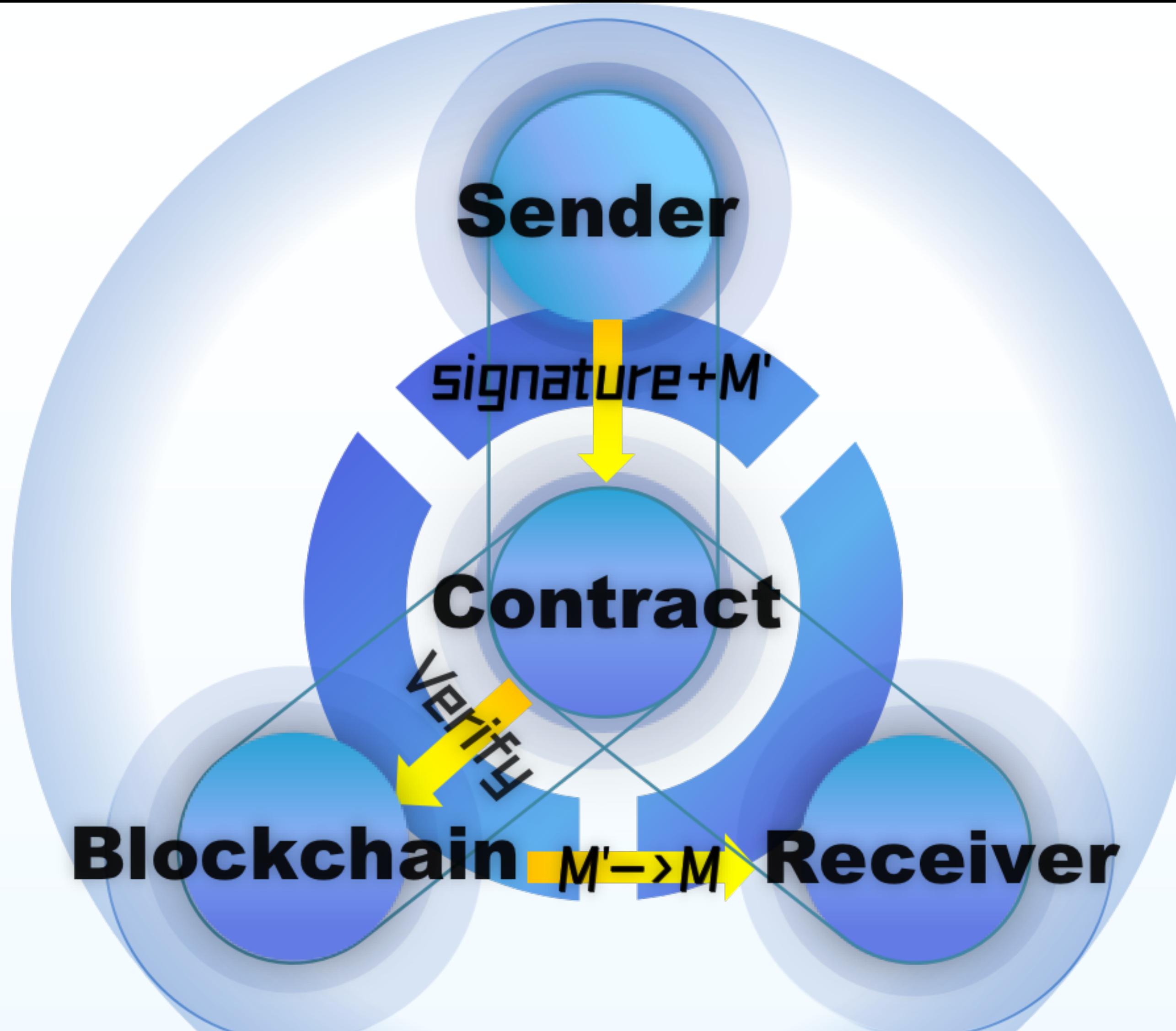
# 平台设计—解决方案



# 平台设计—DID与VC



# 平台设计—基于环签名的智能合约算法



$$P = B + G * H(B * r)$$

$$B = b * G \quad R = r * G$$

$$B + G * H(r * b * G)$$

$$P' = B + G * H(R * b)$$

# 平台设计—爱心积分模型



# 目录

01 社会现状

DATA SCAN 100%

02 平台设计

DATA SCAN 100%

03 亮点总结

DATA SCAN 100%

04 系统展示

DATA SCAN 100%

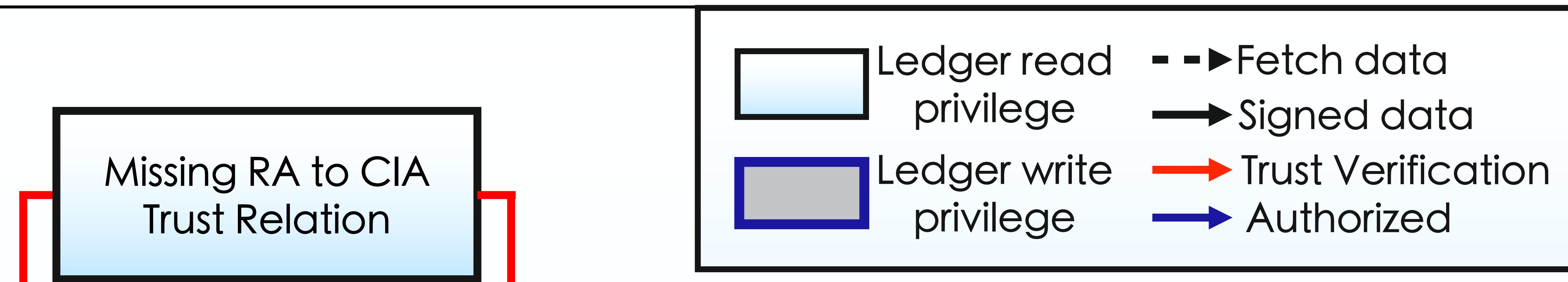
# 亮点总结—研究现状

现有token设计缺乏检索历史信息的**有效途径**，且检索效率**低下**[1][2]，随着区块链增长**性能降低**

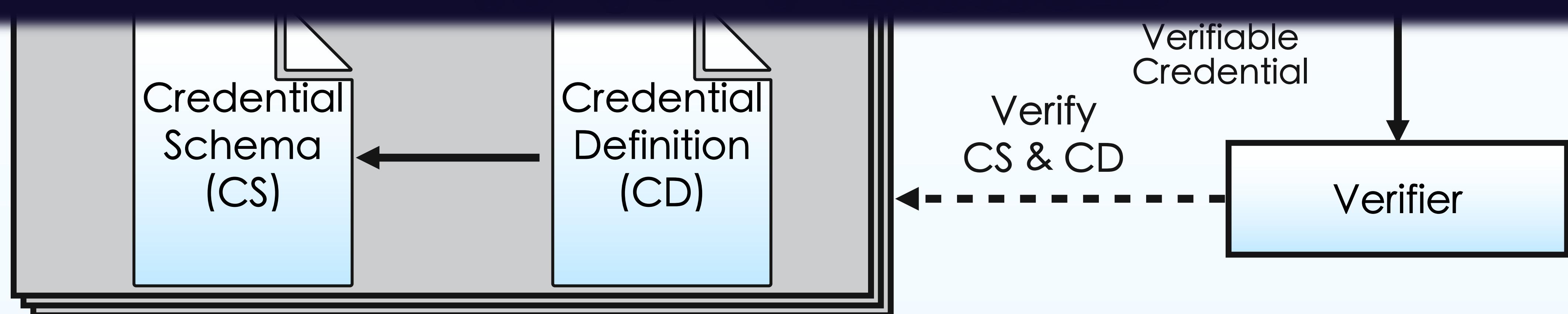
凭证持有者和验证方都难以验证凭证颁发的**合法性**[3][4]，  
确保凭证信息的**机密性和隐私保护**

现有的安全解决方案，难以在不降低智能合约效率  
的情形下[5]实施**动态保护**

# 亮点总结—完善信任验证机制

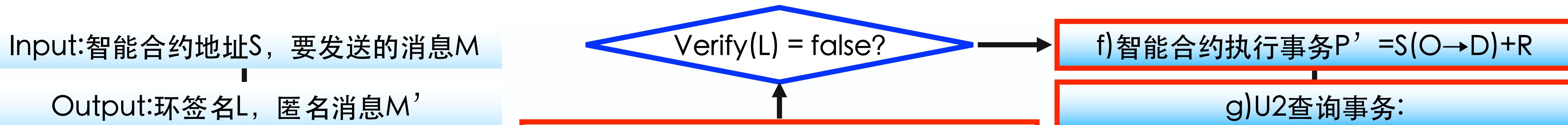


利用**密码学累加器**，支持政府机构（RA）授权慈善机构（CIA）颁发凭证

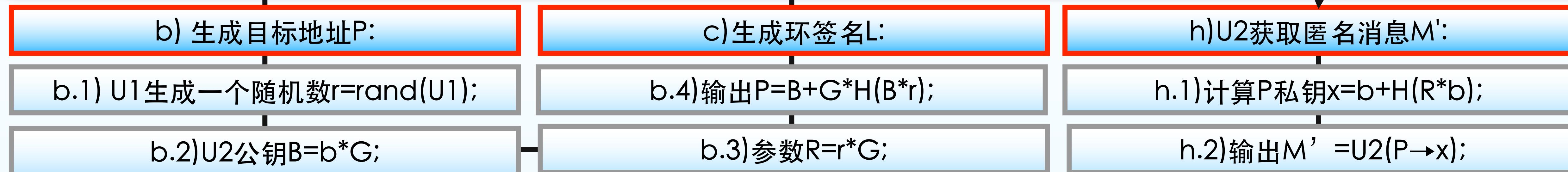


# 亮点总结—基于环签名的智能合约设计

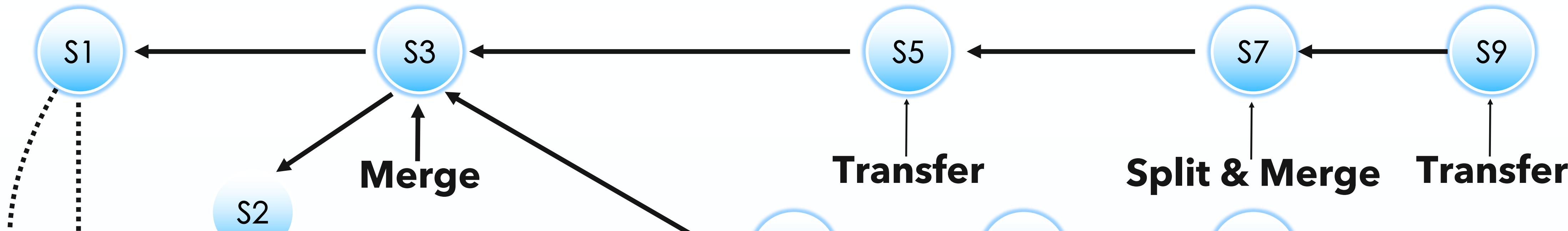
事务发起方:U1,公钥A,私钥a;事务接收方:U2,公钥B,私钥b,H( )为哈希算法,事务为D



提出了一种**基于环签名的智能合约方案**，在交易过程中调用环签名算法来验证发起人的身份



# 亮点总结—基于DAG的token实现快速溯源



针对token状态转换进行建模，并基于DAG的token进行设计，直接从区块链进行搜索。



基于DAG模型的token状态转换

# 亮点总结—积分生成模型

## 参与慈善项目

用户积极参与慈善项目，会得到积分回馈和奖励

$$f(x) = kx_i$$

## 平台活动

平台随机举行各项活动，如慈善知识问答，赢得奖励积分。

$$f(x) = wx = \max[wx_i]$$

## 积分引导

平台针对紧急项目和用户求助，从多维度考虑奖励积分构成，引导用户援助。

$$A = \begin{bmatrix} \frac{w_1}{w_1} & \frac{w_1}{w_2} & \dots & \frac{w_1}{w_n} \\ \frac{w_1}{w_2} & \frac{w_2}{w_2} & \dots & \frac{w_2}{w_n} \\ \vdots & \vdots & \dots & \vdots \\ \frac{w_n}{w_1} & \frac{w_n}{w_2} & \dots & \frac{w_n}{w_n} \end{bmatrix} \quad W_i = \frac{\bar{W}_i}{\sum_{j=1}^n \bar{W}_j}$$

# 亮点总结

利用密码学累加器在政府与权威机构之间补充了一个安全认证协议，以增强用户对于机构的**信任度**

保证数据信息**公开透明**，提出了一种**基于环签名的智能合约**方案，调用环签名算法来验证交易发起人的身份

针对检索效率低下的问题，引入了基于DAG的token机制记录流动情况，实现资金物资的**快速溯源**

# 目录

01 社会现状

DATA SCAN 100%

02 平台设计

DATA SCAN 100%

03 亮点总结

DATA SCAN 100%

04 系统展示

DATA SCAN 100%

# Thanks

*FinTechathon* 2021

微众银行第三届金融科技高校技术大赛

*FinTechathon* 2021

微众银行第三届金融科技高校技术大赛