周汇报——

多方授权、门限签名、DVT和ZenGo SAML

汇报人： 王田

2023年4月9日

20230409

一 多方授权

二 TSS、DVT 和 Zengo SAML初步模型

三 模型完善

三 Demo演示

多方授权

- 本文观点：
- 授权在网络空间主要体现为签名，所以多方授权可解释为由多方签名，具体可通过多签或门限实现
- 门限签名是私钥守护神

硬核科普：一文读懂数字化契约守护神“多方门限签名”的妙用

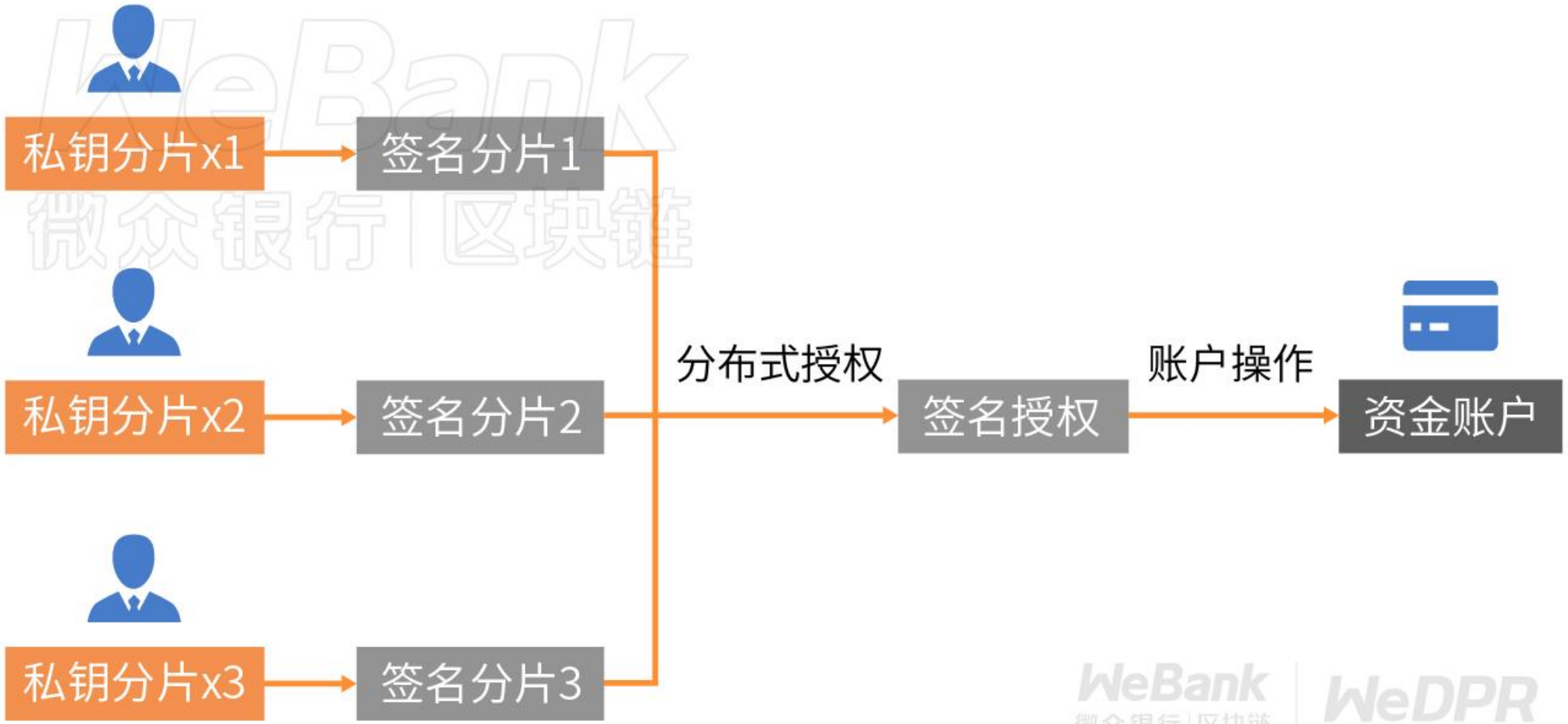
微众银行区块链　2020-07-16　热度: 19648

原标题：数字化契约如何守护？解析多方门限签名的妙用

数字签名是否只能由单一主体签署？在涉及多方授权的场景中，如何实现多方联合签名？多方联合签名是否支持决策权重分配？其背后的门限签名技术除了支持多方授权功能之外，还有哪些神奇之处？

多方授权

- 多方授权可解释为由多方签名，具体可通过多签或门限实现



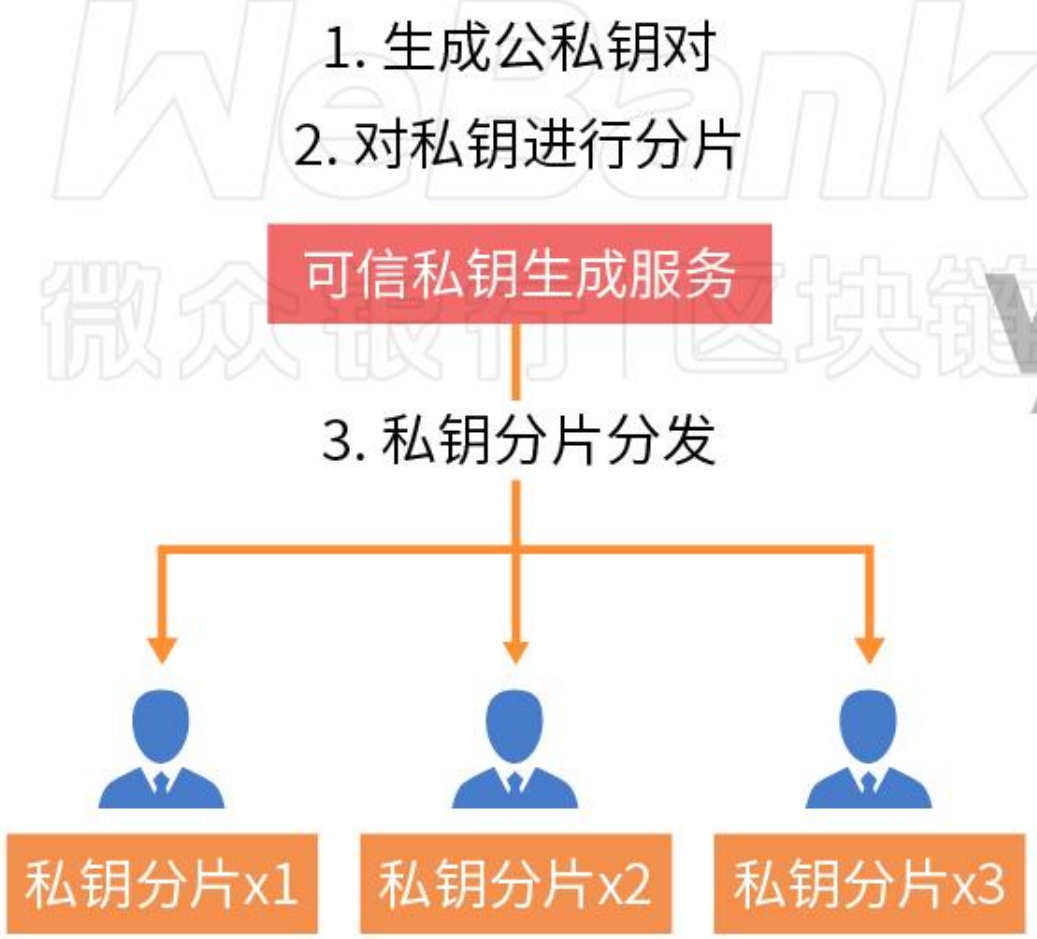
多方授权

- 门限签名相比于多签的优势

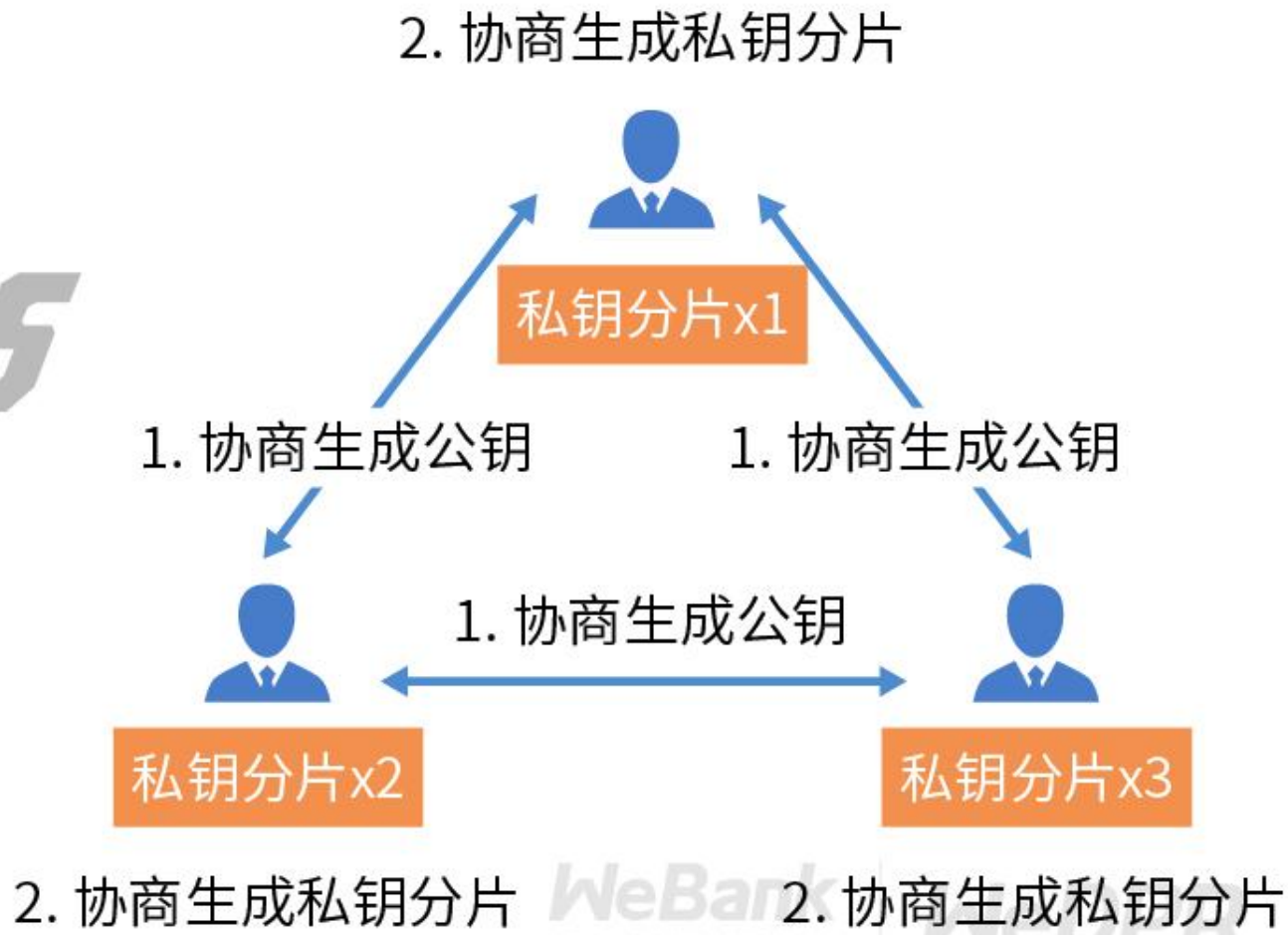
	多重签名	门限签名
签名方人数与签名大小、验证时间的关系	随签名方人数线性增长	固定大小
签名方身份是否匿名	否	是
签名验证使用的公钥	所有签名方的公钥	单个合并公钥
是否可实现门限特性	是	是
签名值	所有的签名进行级联或者一个签名列表	一个合并的门限签名
公私钥对的初始化	各个参与方可以独立完成公私钥对的初始化	各个参与方需要协商完成公私钥对的初始化

多方授权

- 门限签名的两种实现方式：有第三方、无第三方（引入DKG技术）



VS



多方授权

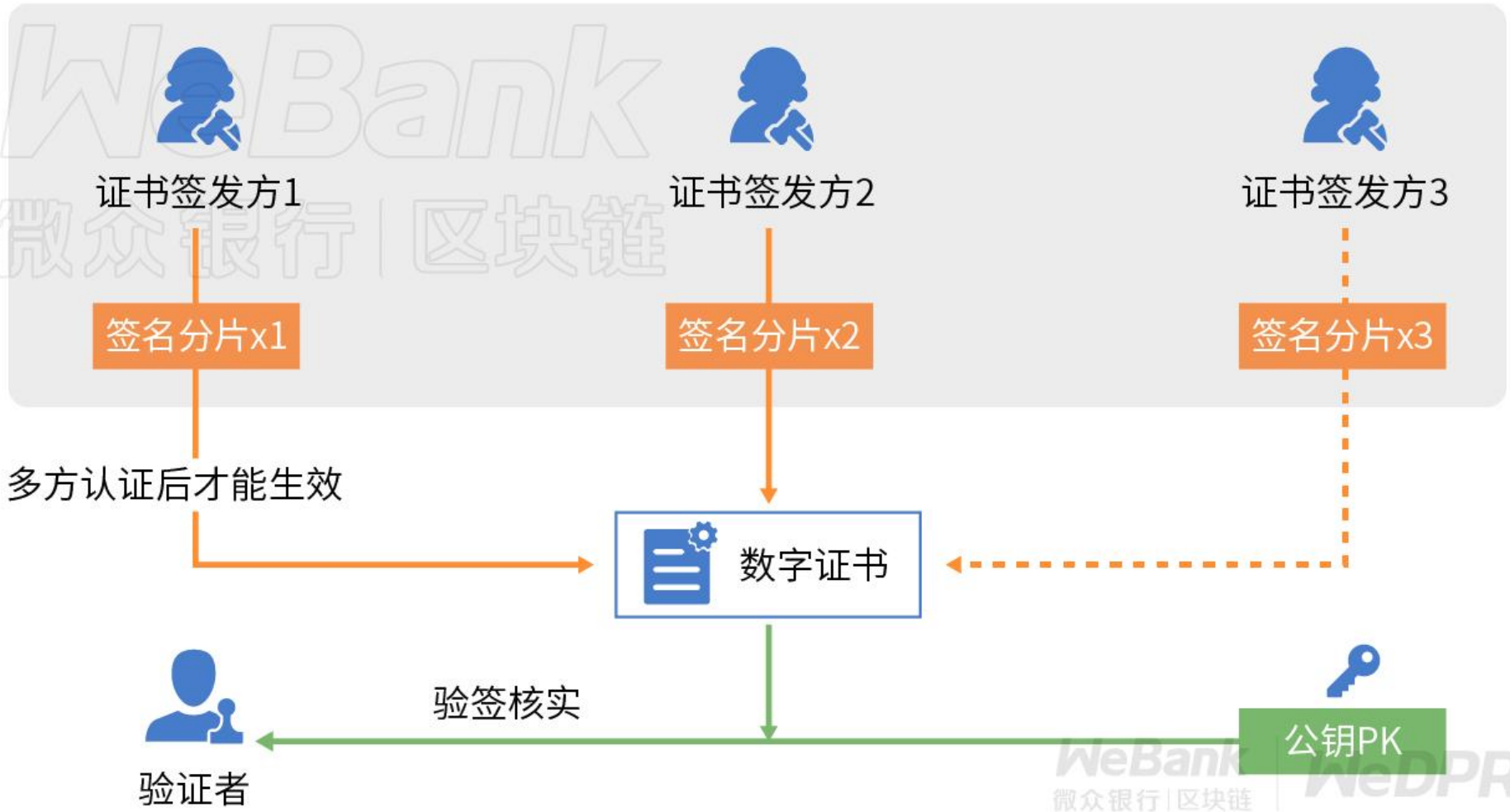
- 门限签名是私钥守护神

传统PKI面临的不足之处主要体现在，传统PKI证书签发机构在签发和管理证书的过程中，可能存在单点脆弱性，即出现单一证书签发机构的证书签发私钥泄露或被窃取，从而导致重大声誉和财务损失。

例如，黑客从中心化的证书签发机构获得签名证书并窃取私钥，然后对恶意软件进行签名，生成看似安全的签名认证软件，但这实际是一个恶意软件，非常容易导致网络安全事故。

多方授权

- DPKI要求多方授权才能签发数字证书，不再依赖单一实体对签名私钥的保护能力



多方授权

- 背书链应用于私钥保护的研究价值：
  - DVT相比于门限签名有无增量
  - 背书链有无增量

20230409

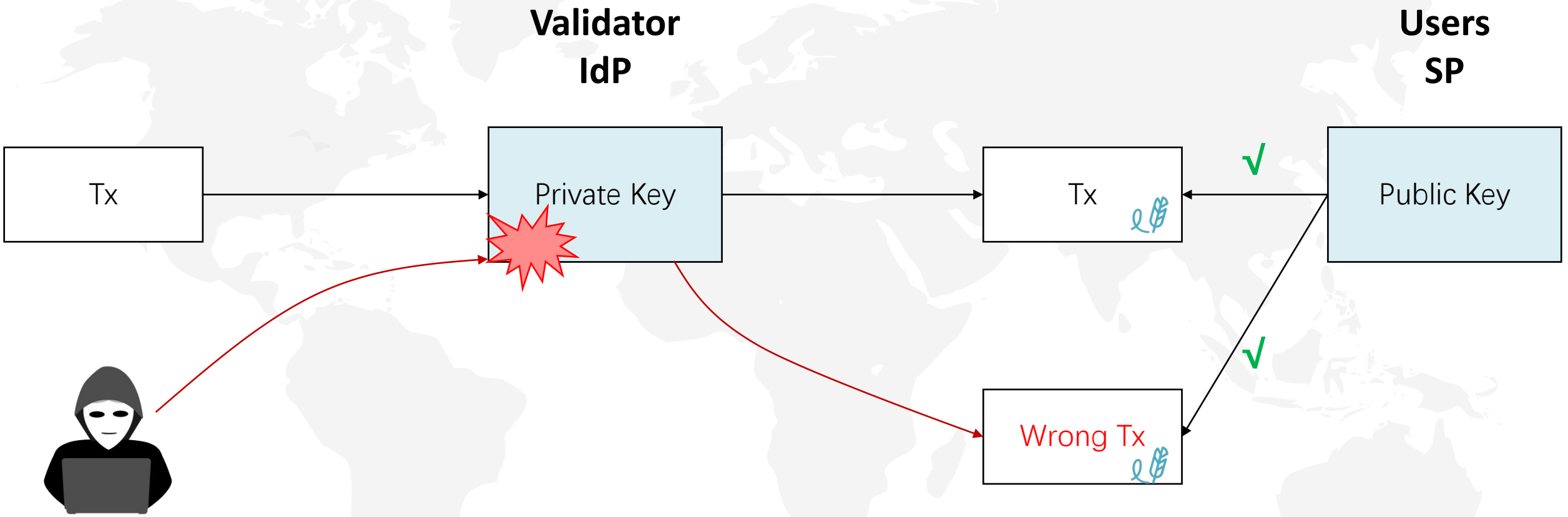
一 多方授权

二 TSS、DVT 和 Zengo SAML初步模型

三 模型完善

三 Demo演示

私钥验证



门限签名（TSS）

SSS

$k \rightarrow k_1, \ldots, k_n$

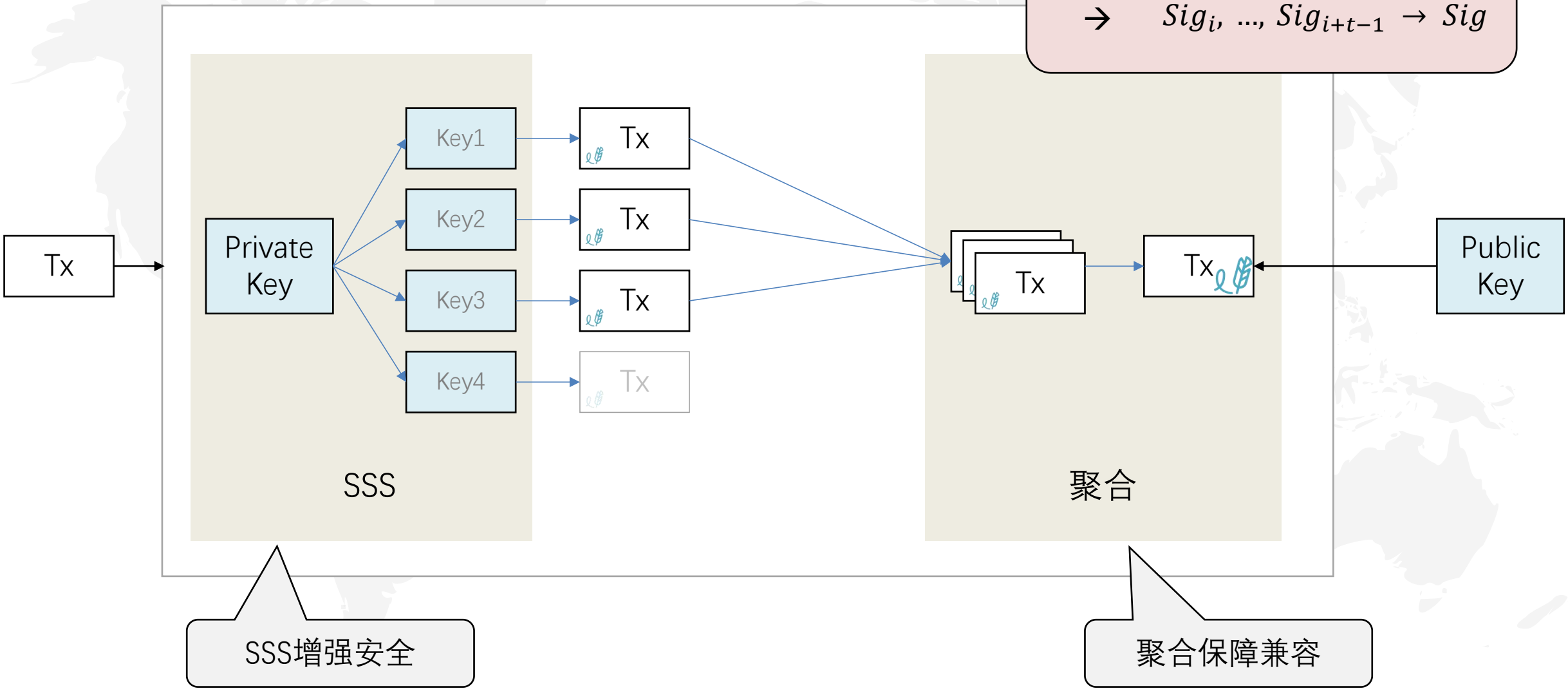
$k_i \ldots k_{i+t-1} \rightarrow k$

聚合

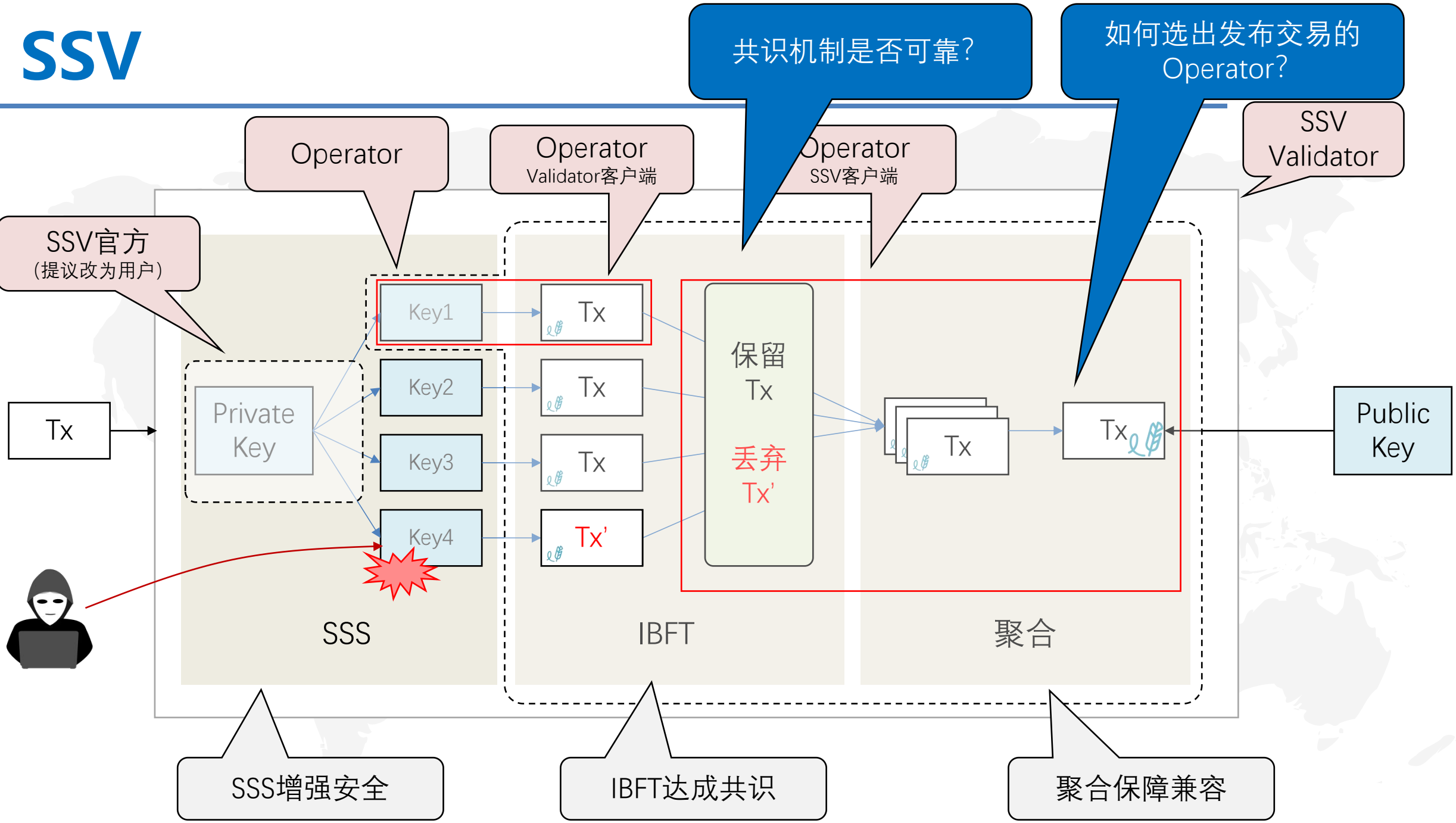
$sign_{Agg}(k_i, M) \rightarrow Sig_i$

→

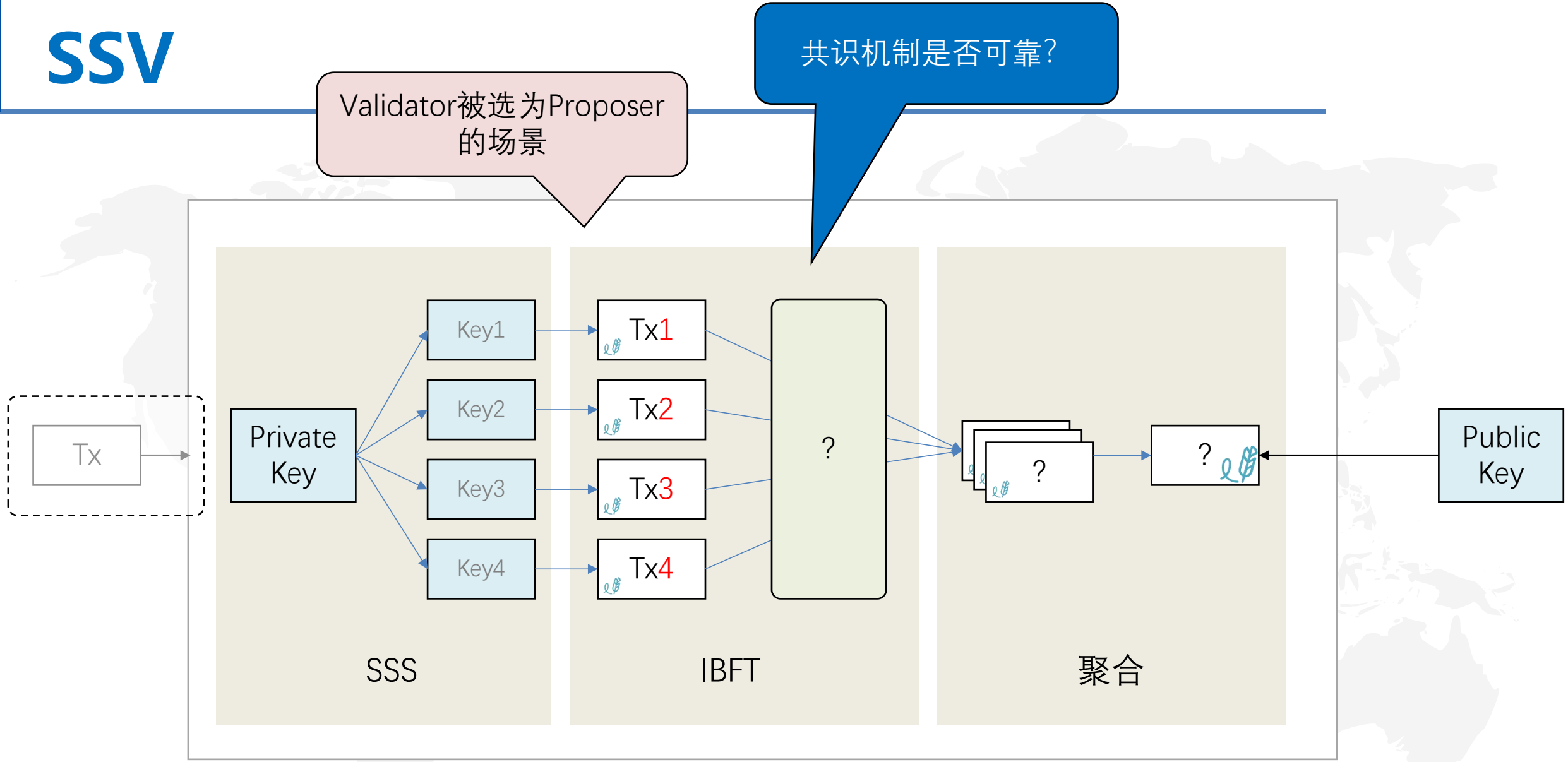
$Sig_i, \ldots, Sig_{i+t-1} \rightarrow Sig$



SSV


共识机制是否可靠?
如何选出发布交易的Operator?
SSV Validator
Operator
Operator
Validator客户端
Operator
SSV客户端
SSV官方
(提议改为用户)
Key1
Key2
Key3
Key4
Tx
Tx
Tx
Tx'
Private Key
保留Tx
丢弃Tx'
Tx
Tx
Public Key
SSS
IBFT
聚合
SSS增强安全
IBFT达成共识
聚合保障兼容

SSV

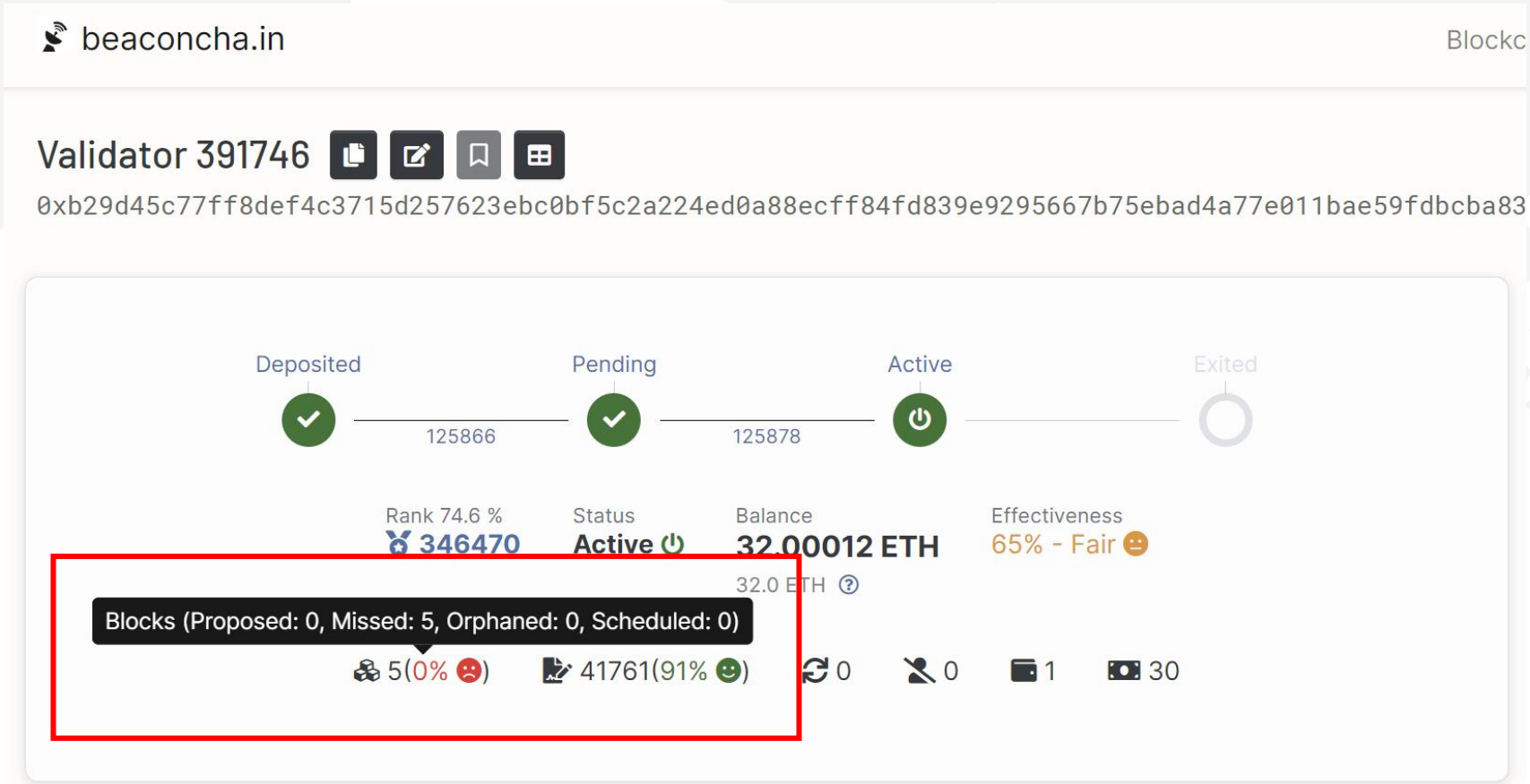

Validator被选为Proposer的场景
共识机制是否可靠?
Tx
Private Key
Key1
Key2
Key3
Key4
Tx1
Tx2
Tx3
Tx4
?
?
?
Public Key
SSS
IBFT
聚合

SSV

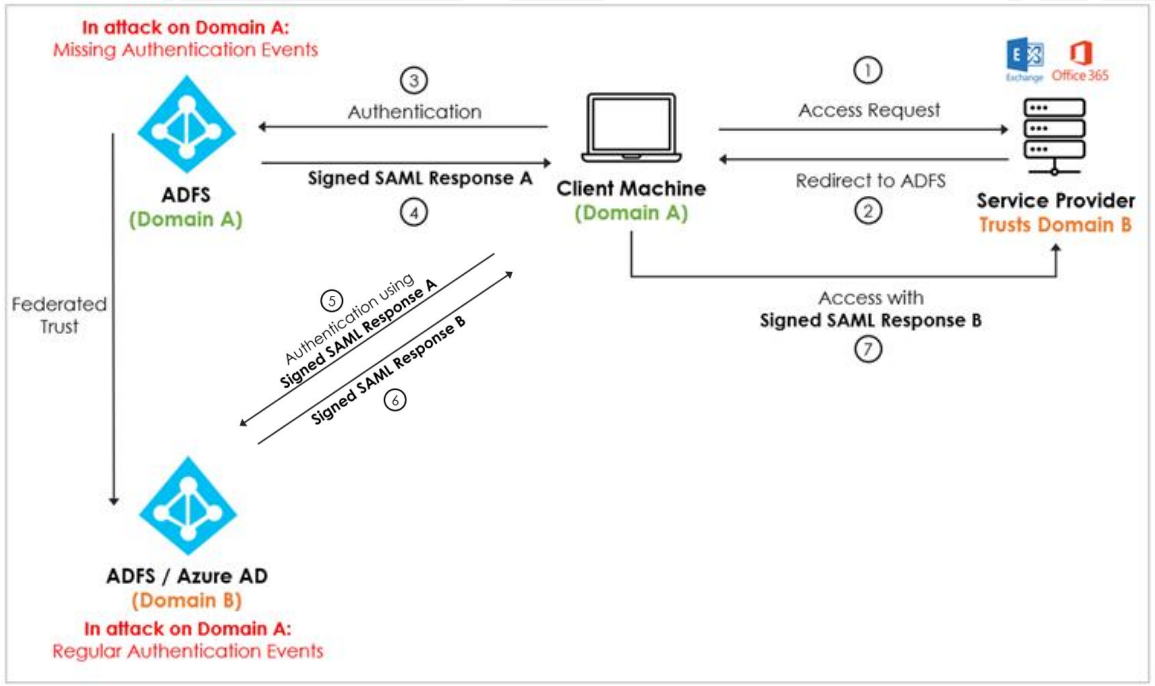
共识机制是否可靠?

不完全可靠

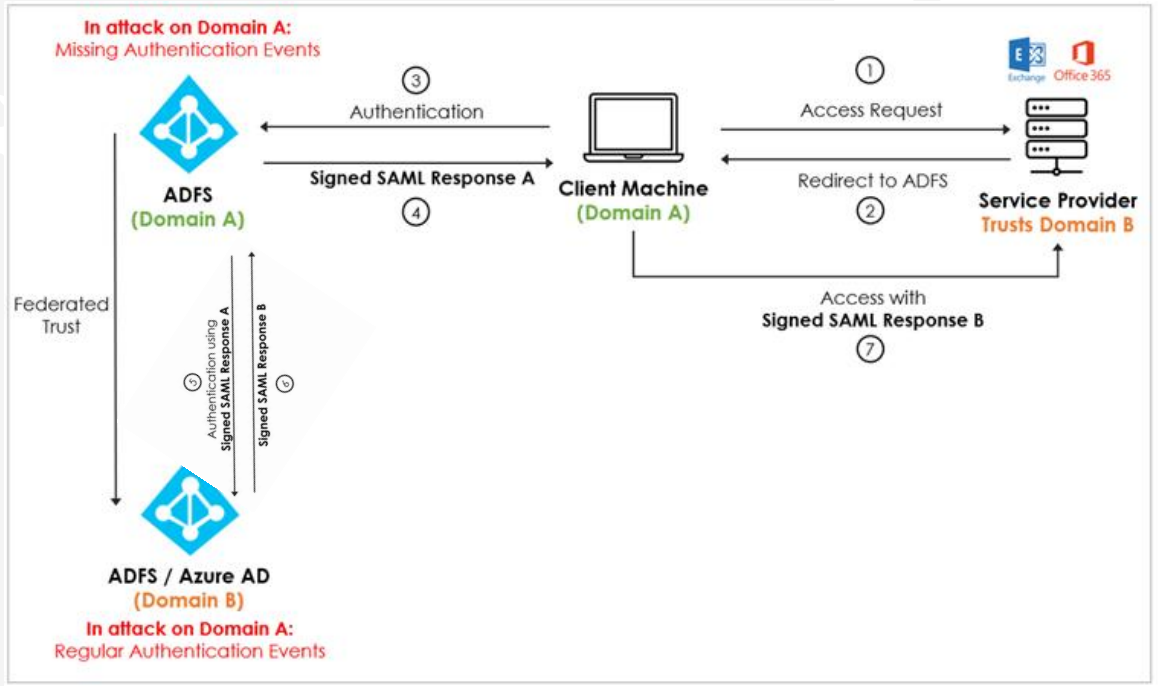
- Lido DVT Pilot: Although both validators have missed a block proposal, this is due to a limitation of the current SSV Network Shifu testnet implementation.
- 尽管两个验证者都错过了区块提议，但这是由于当前 SSV Network Shifu 测试网实施的限制所致。



MFA SAML

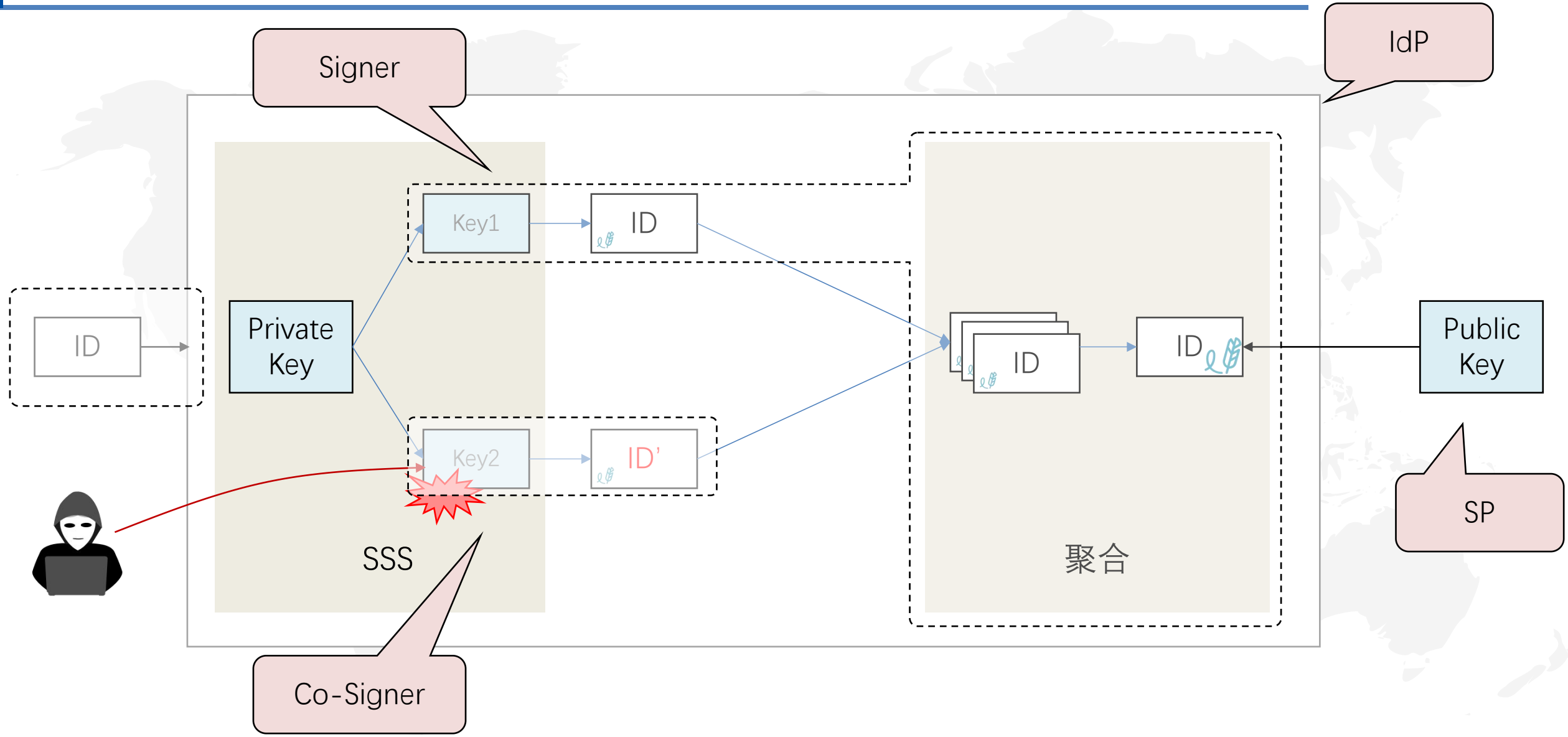


只分割，不聚合
只有安全性，没有兼容性

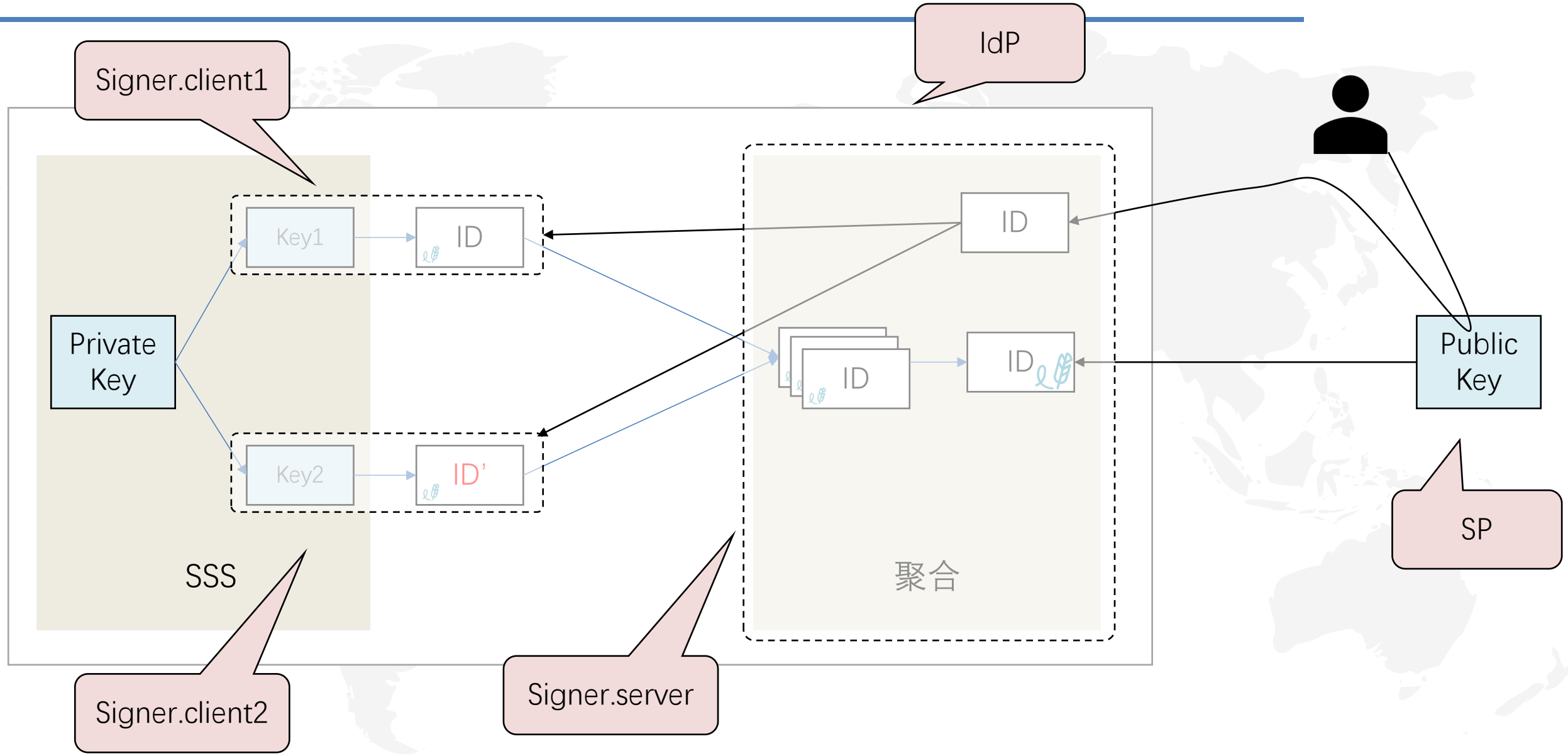


有只分割，有聚合
既有安全性，又有兼容性

MFA SAML


Signer
IdP
Key1
ID
ID
Private Key
Public Key
ID
ID
Key2
ID'
SP
SSS
聚合
Co-Signer

MFA SAML


IdP
Signer.client1
Key1
ID
Private Key
Key2
ID'
SSS
ID
ID
ID
聚合
Public Key
SP
Signer.client2
Signer.server

20230409

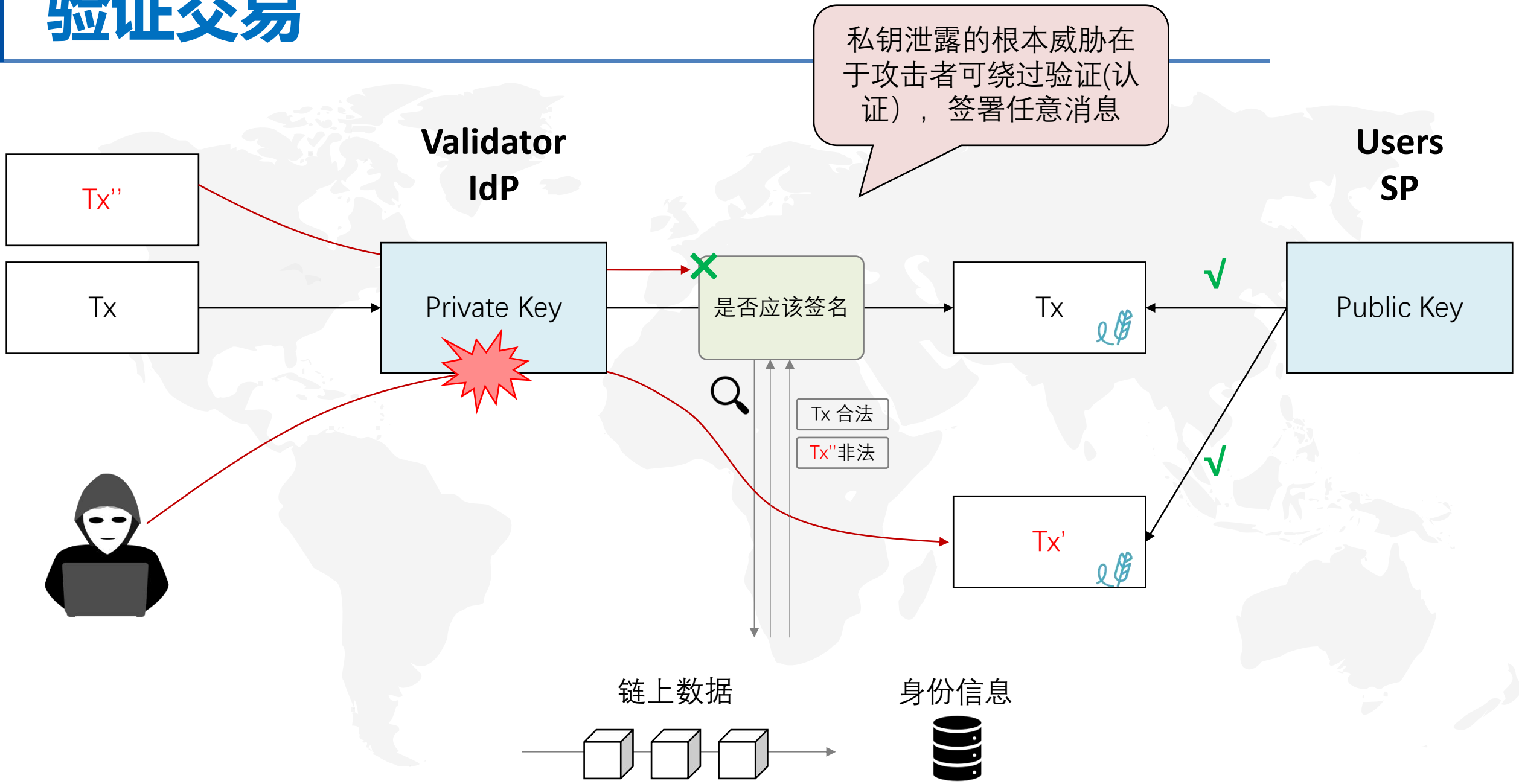
一 多方授权

二 TSS、DVT 和 Zengo SAML初步模型

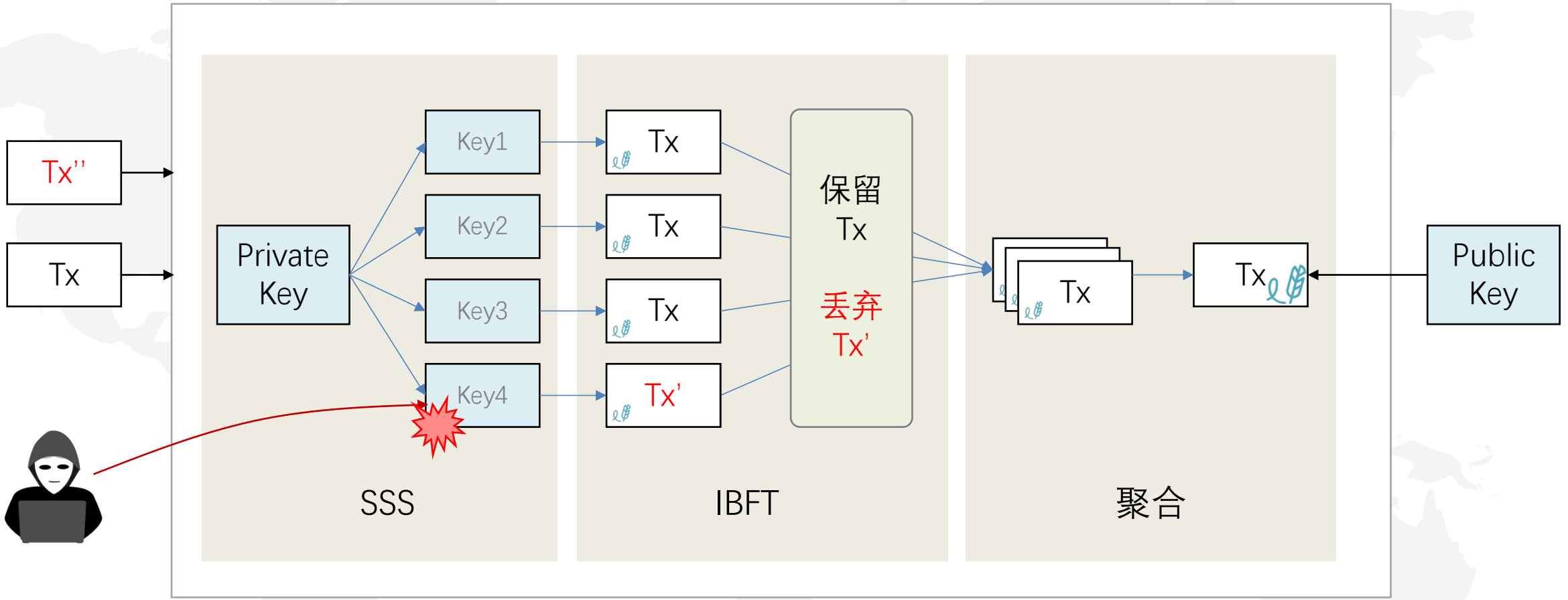
三 模型完善

三 Demo演示

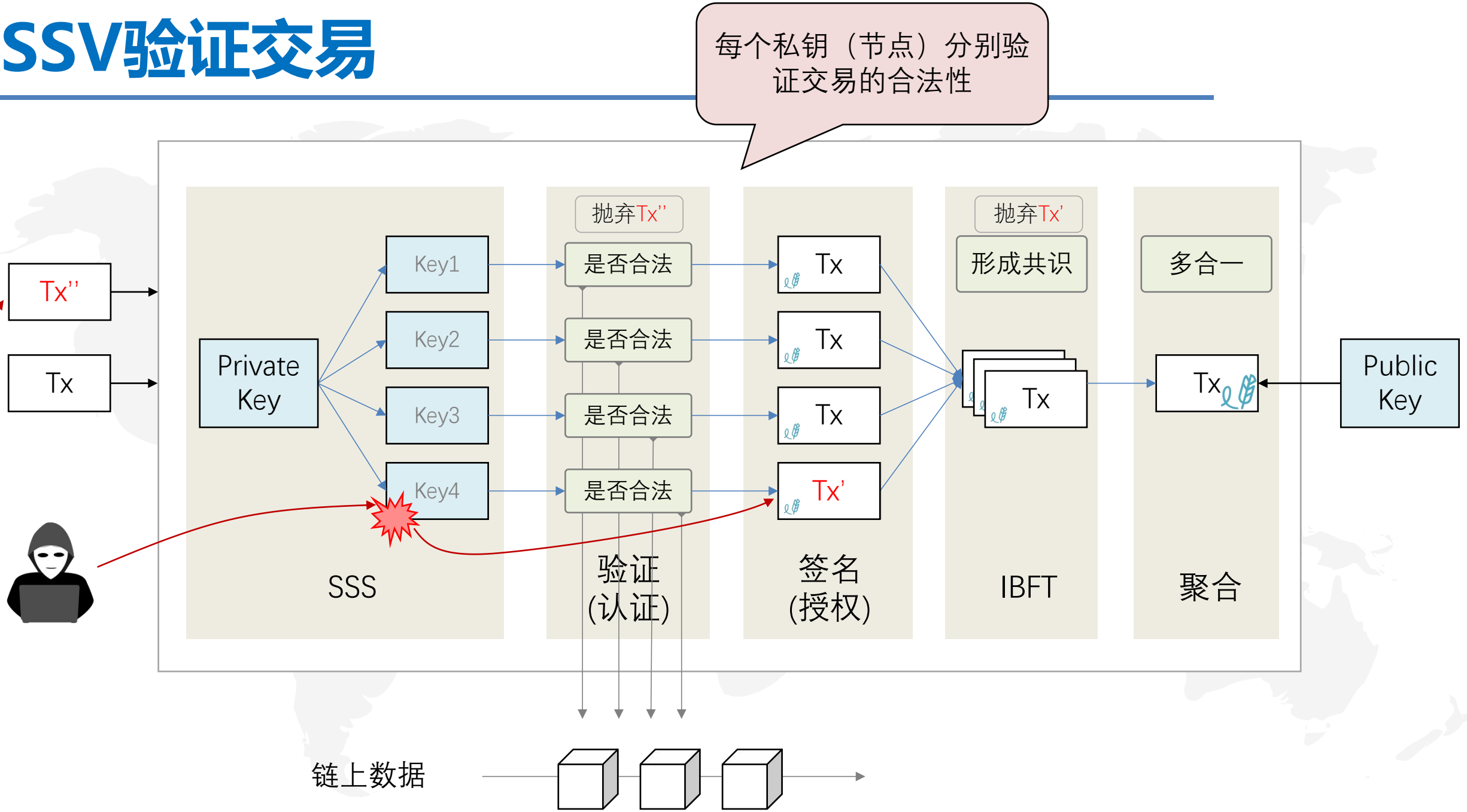
验证交易


私钥泄露的根本威胁在于攻击者可绕过验证(认证），签署任意消息
Validator
IdP
Users
SP
Tx''
Tx
Private Key
是否应该签名
Tx 合法
Tx''非法
Tx
Public Key
Tx'
√
√
链上数据
身份信息

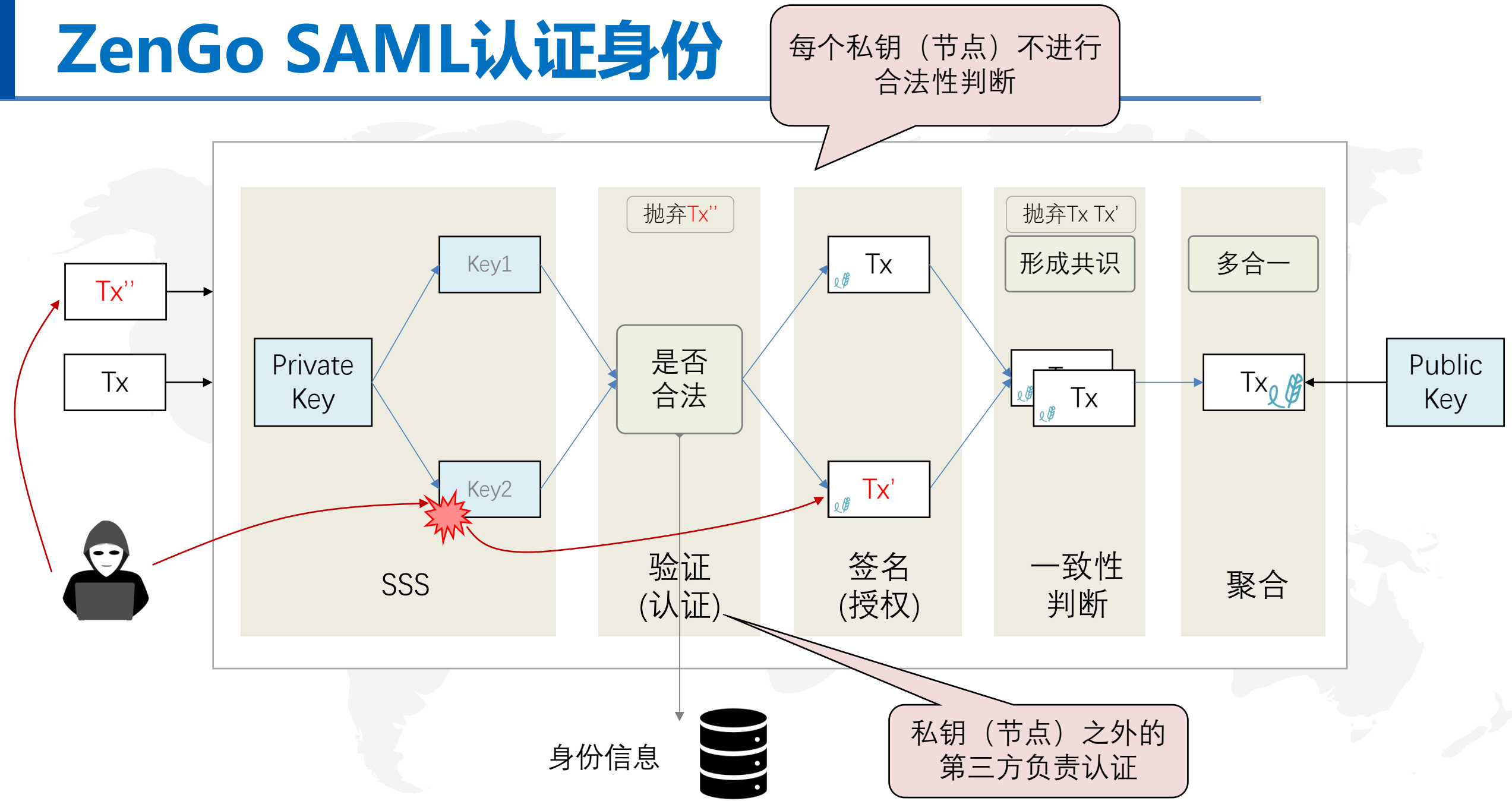
SSV验证交易


Tx''
Tx
Private Key
Key1
Key2
Key3
Key4
Tx
Tx
Tx
Tx'
保留 Tx
丢弃 Tx'
Tx
Tx
Public Key
SSS
IBFT
聚合

SSV验证交易

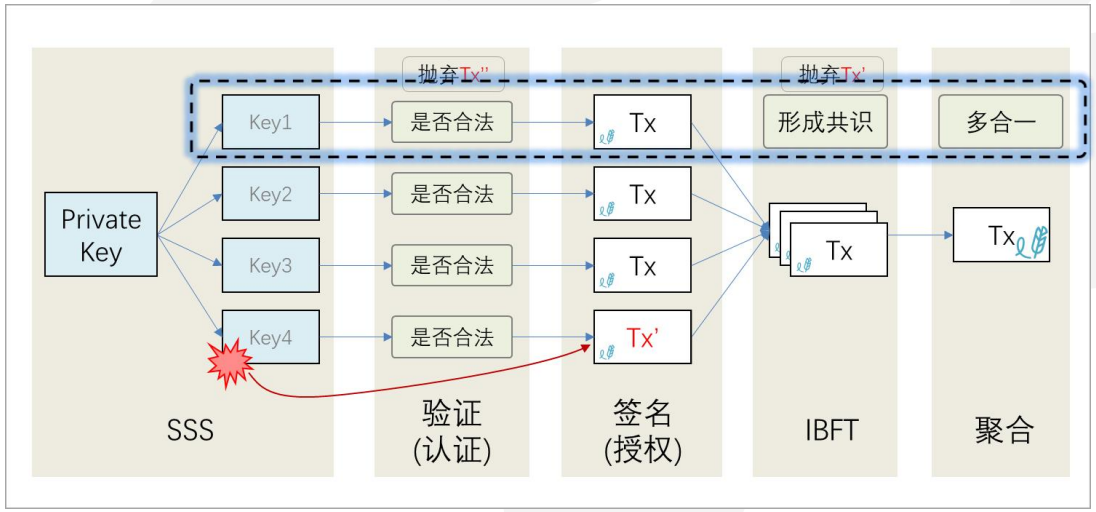

每个私钥（节点）分别验证交易的合法性
Tx''
Tx
Private Key
Key1
Key2
Key3
Key4
抛弃Tx''
是否合法
是否合法
是否合法
是否合法
Tx
Tx
Tx
Tx'
抛弃Tx'
形成共识
多合一
Tx
Tx
Public Key
SSS
验证 (认证)
签名 (授权)
IBFT
聚合
链上数据

ZenGo SAML认证身份

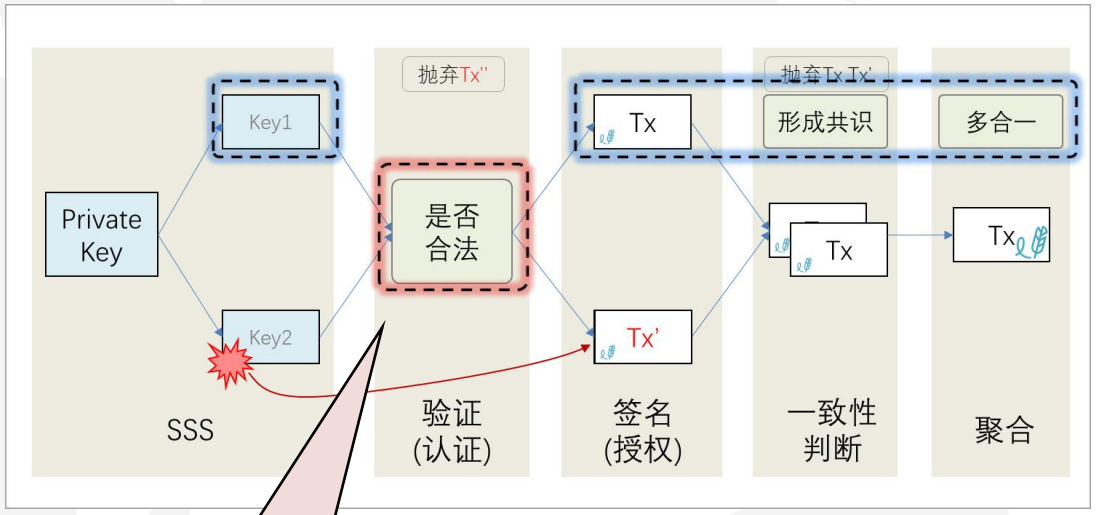


SSV与ZenGo SAML对比

SSV每个节点包含的内容



ZenGo SAML每个节点包含的内容



认证存在单点故障

20230409

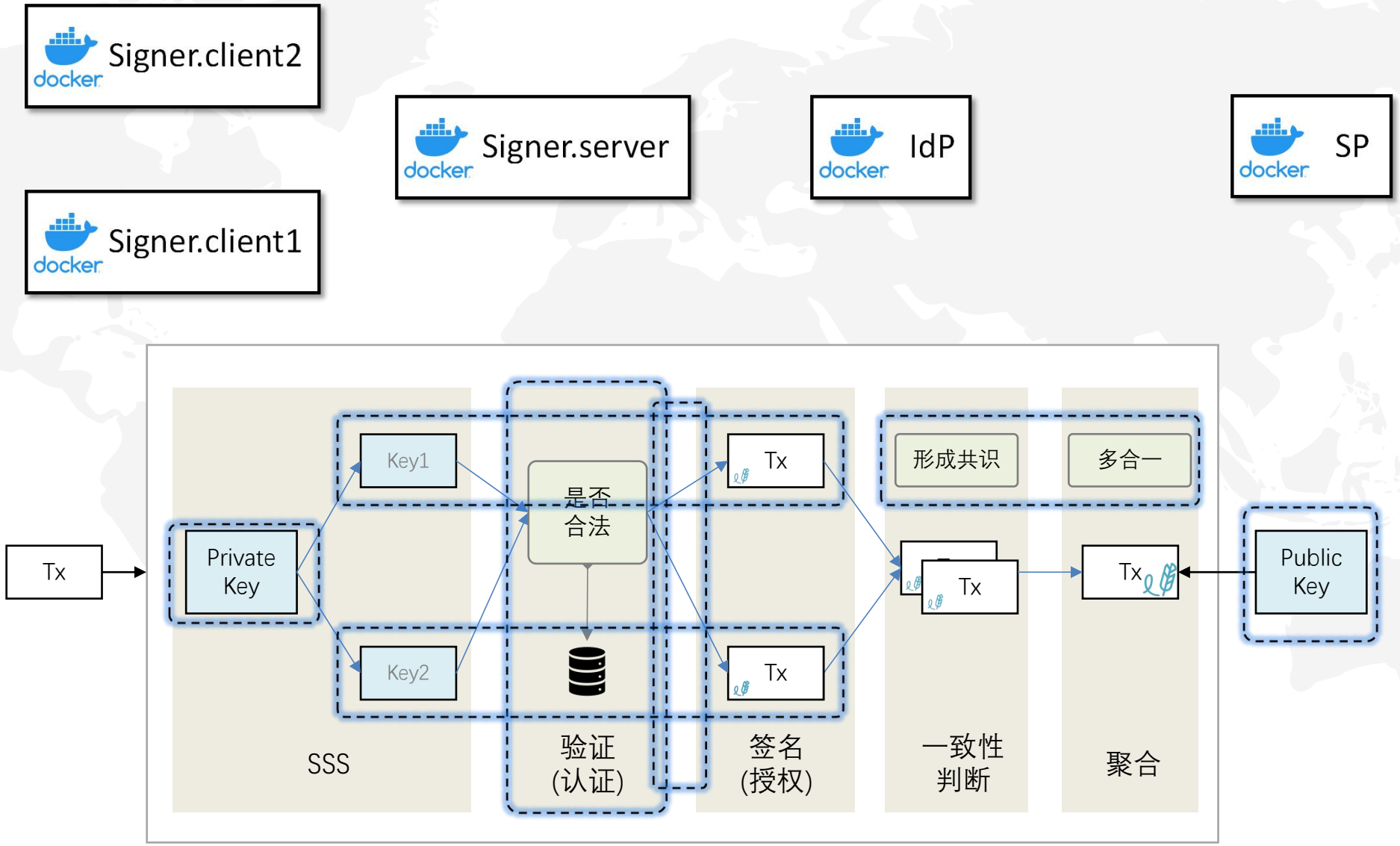
一 多方授权

二 TSS、DVT 和 Zengo SAML初步模型

三 模型完善

三 Demo演示

ZenGo SAML Demo介绍



ZenGo SAML Demo介绍