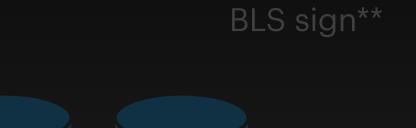
# Key Discovery / Pay Username

Proposal

wallet Prove ownership of email/phone number user





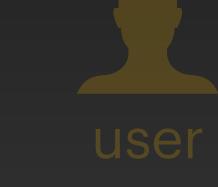


Light weight crypto operation

wallet crypto material Prove ownership Transaction of email/phone modified crypto number material user user Light weight crypto operation

BLS sign\*\*





BLS sign\*\* Smart contract verify modified crypto material wallet crypto material Prove ownership Authorities Transaction of email/phone modified crypto number material user user user Light weight crypto Light weight crypto operation operation

## Setup









wallet



 $n_{A}$ 

 $t_1 = H_1(n_A)^w \in G_1$  $t_2 = H_2(n_A)^w \in G_2$ 



user

$$a \leftarrow Z_q$$

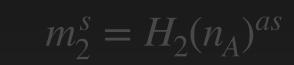
 $BLS.vrfy(\sigma_1, m_1, pk_{w_1})$  $SLB.vrfy(\sigma_2, m_2, pk_{w_2})$  BLS sign in G1 and G2

BLS sign with hash function



$$m_1^s = H_1(n_A)^{as}$$







$$k_1 = H_1(n_A)^s = (m_1^s)^{-a}$$

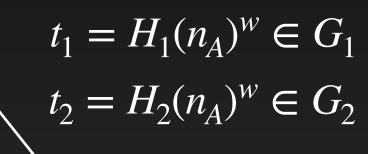
$$k_2 = H_2(n_A)^s = (m_2^s)^{-\alpha}$$



#### Smart contract

BLS.  $vrfy(\sigma_1, m_1, pk_{w_1})$ SLB.  $vrfy(\sigma_2, m_2, pk_{w_2})$ 





# user

 $n_{A}$ 



 $a \leftarrow Z_q$ 

#### Transaction

$$\sigma_1 = t_1^a , \ m_1 = H_1(n_A)^a$$

$$\sigma_2 = t_2^a , \ m_2 = H_2(n_A)^a$$

### BLS sign in G1 and G2

### BLS sign with hash function = identity function



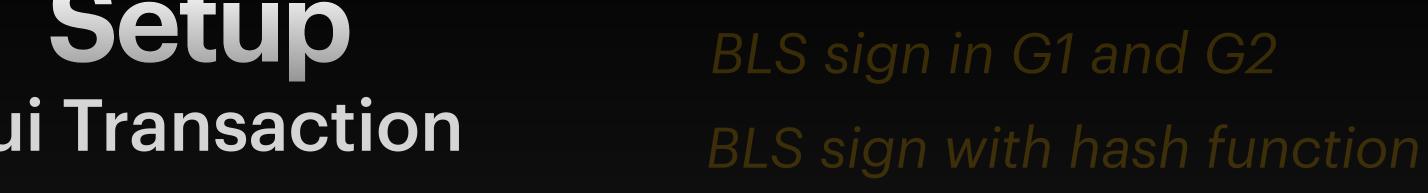
Authorities

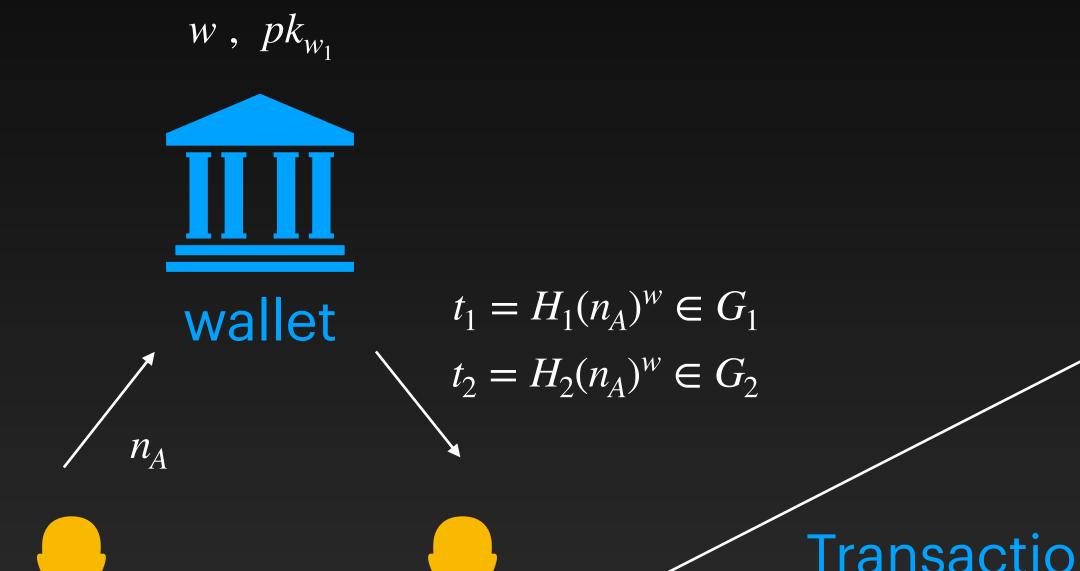


$$k_1 = H_1(n_A)^s = (m_1^s)^{-\alpha}$$

## Setup







#### Smart contract

 $BLS.vrfy(\sigma_1, m_1, pk_{w_1})$  $SLB.vrfy(\sigma_2, m_2, pk_{w_2})$ 







user

$$a \leftarrow Z_q$$

#### Transaction

$$\sigma_1 = t_1^a , \ m_1 = H_1(n_A)^a$$

$$\sigma_2 = t_2^a , \ m_2 = H_2(n_A)^a$$

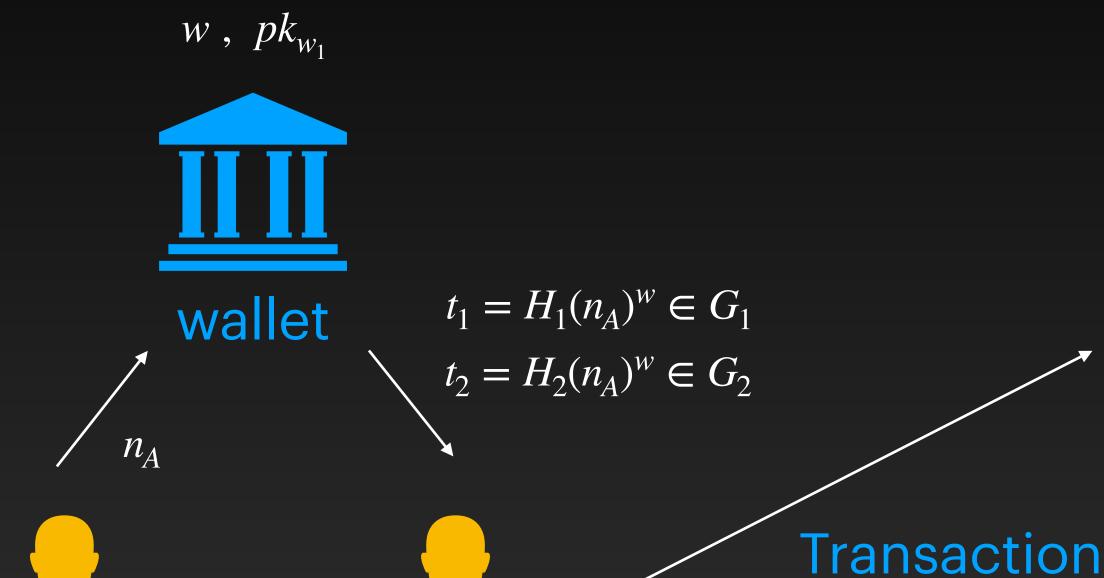


$$k_1 = H_1(n_A)^s = (m_1^s)^{-a}$$
  
 $k_2 = H_2(n_A)^s = (m_2^s)^{-a}$ 

 $\sigma_1 = t_1^a , \ m_1 = H_1(n_A)^a$ 

 $\sigma_2 = t_2^a$ ,  $m_2 = H_2(n_A)^a$ 

BLS sign in G1 and G2
BLS sign with hash function
= identity function



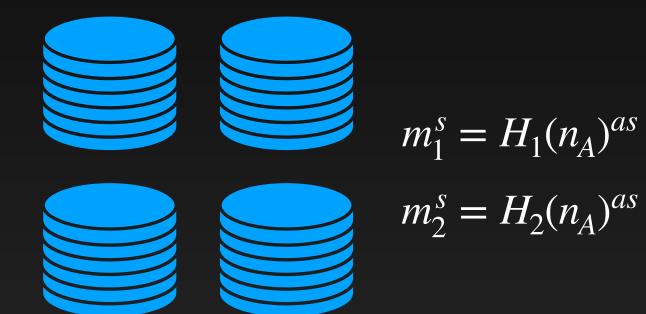
user

 $a \leftarrow Z_a$ 

user

#### Smart contract

BLS.  $vrfy(\sigma_1, m_1, pk_{w_1})$ SLB.  $vrfy(\sigma_2, m_2, pk_{w_2})$ 



Authorities



$$k_1 = H_1(n_A)^s = (m_1^s)^{-a}$$
  
 $k_2 = H_2(n_A)^s = (m_2^s)^{-a}$ 

BLS sign in G1 and G2
BLS sign with hash function
= identity function





**KYC** 

$$t_1 = H_1(n_A)^w \in G_1$$
  
 $t_2 = H_2(n_A)^w \in G_2$ 

#### Smart contract

BLS. 
$$vrfy(\sigma_1, m_1, pk_{w_2})$$
  
SLB.  $vrfy(\sigma_2, m_2, pk_{w_1})$ 





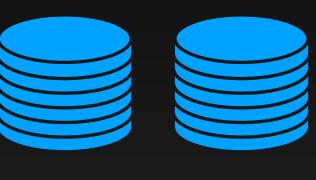
user

$$a \leftarrow Z_a$$

#### Transaction

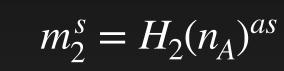
$$\sigma_1 = t_1^a , \ m_1 = H_1 (n_A)^a$$

$$\sigma_2 = t_2^a , \ m_2 = H_2(n_A)^a$$



$$m_1^s = H_1(n_A)^{as}$$





Authorities



$$k_1 = H_1(n_A)^s = (m_1^s)^{-a}$$

$$k_2 = H_2(n_A)^s = (m_2^s)^{-a}$$

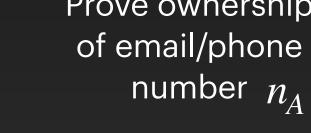
### Setup Crypto



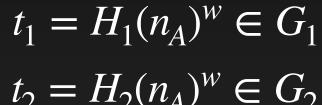


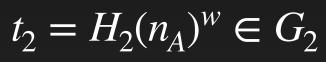
wallet

Prove ownership of email/phone











user

$$a \leftarrow Z_q$$



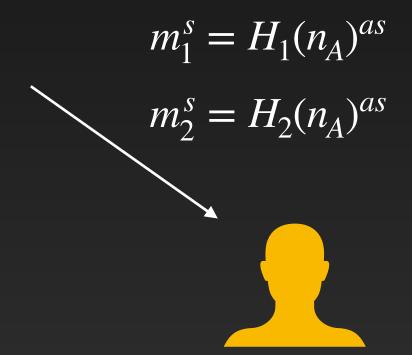




authorities

$$\sigma_1 = t_1^a , \quad m_1 = H_1(n_A)^a$$
 $\sigma_2 = t_2^a , \quad m_2 = H_2(n_A)^a$ 

$$BLS.vrfy(\sigma_1, m_1, pk_{w_1})$$
  
 $SLB.vrfy(\sigma_2, m_2, pk_{w_2})$ 



$$k_1 = H_1(n_A)^s = (m_1^s)^{-a}$$
  
 $k_2 = H_2(n_A)^s = (m_2^s)^{-a}$ 

### Key Derivation



$$S_{AB} = e(k_1, H_2(n_B)) = e(H_1(n_A)^s, H_2(n_B))$$
  
 $S_{BA} = e(H_1(n_B), k_2) = e(H_1(n_B), H_2(n_A)^s)$ 

$$k_{AB} = KDF(S_{AB} \ XOR \ S_{BA})$$

$$key = g_1^{t_{AB}}, t_{AB} = H(s_{AB})$$

$$val = c_{AB} = AEAD_k(addr_A)$$



$$S_{AB} = e(k_1, H_2(n_B)) = e(H_1(n_A)^s, H_2(n_B))$$
  
 $S_{BA} = e(H_1(n_B), k_2) = e(H_1(n_B), H_2(n_A)^s)$ 

$$k_{AB} = KDF(S_{AB} \ XOR \ S_{BA})$$

$$key = g_1^{t_{BA}}, \ t_{BA} = H(s_{BA})$$

$$val = c_{BA} = AEAD_k(addr_B)$$

### Key Derivation



$$S_{AB} = e(k_1, H_2(n_B)) = e(H_1(n_A)^s, H_2(n_B))$$
  
 $S_{BA} = e(H_1(n_B), k_2) = e(H_1(n_B), H_2(n_A)^s)$ 

$$k_{AB} = KDF(S_{AB} \ XOR \ S_{BA})$$

$$key = g_1^{t_{AB}}, t_{AB} = H(s_{AB})$$

$$val = c_{AB} = AEAD_k(addr_A)$$



$$S_{AB} = e(H_1(n_A), k_2) = e(H_1(n_A), H_2(n_B)^s)$$
  
 $S_{BA} = e(k_1, H_2(n_A)) = e(H_1(n_B)^s, H_2(n_A))$ 

$$k_{AB} = KDF(S_{AB} \ XOR \ S_{BA})$$

$$key = g_1^{t_{BA}}, \ t_{BA} = H(s_{BA})$$
 $val = c_{BA} = AEAD_k(addr_B)$ 

### Key Derivation



$$S_{AB} = e(k_1, H_2(n_B)) = e(H_1(n_A)^s, H_2(n_B))$$
  
 $S_{BA} = e(H_1(n_B), k_2) = e(H_1(n_B), H_2(n_A)^s)$ 

$$k_{AB} = KDF(S_{AB} \ XOR \ S_{BA})$$

$$key = g_1^{t_{AB}}, t_{AB} = H(s_{AB})$$
  
 $val = c_{AB} = AEAD_k(pk_A)$ 



$$S_{AB} = e(H_1(n_A), k_2) = e(H_1(n_A), H_2(n_B)^s)$$
  
 $S_{BA} = e(k_1, H_2(n_A)) = e(H_1(n_B)^s, H_2(n_A))$ 

$$k_{AB} = KDF(S_{AB} \ XOR \ S_{BA})$$

$$key = g_1^{t_{BA}}, t_{BA} = H(s_{BA})$$

$$val = c_{BA} = AEAD_k(pk_B)$$

### Sui is special



$$S_{AB} = e(k_1, H_2(n_B)) = e(H_1(n_A)^s, H_2(n_B))$$
  
 $S_{BA} = e(H_1(n_B), k_2) = e(H_1(n_B), H_2(n_A)^s)$ 

$$k_{AB} = KDF(S_{AB} \ XOR \ S_{BA})$$

$$key = g_1^{t_{AB}}, t_{AB} = H(s_{AB})$$

$$val = c_{AB} = AEAD_k(addr_A)$$

- 1. Create a new owned object with owner hash(key)
- 2. The object contains a single field: val
- 3. Readers can gather all objects owned by a public key they know.
- 4. Single-owner object structure remains because there is a single writer for every key