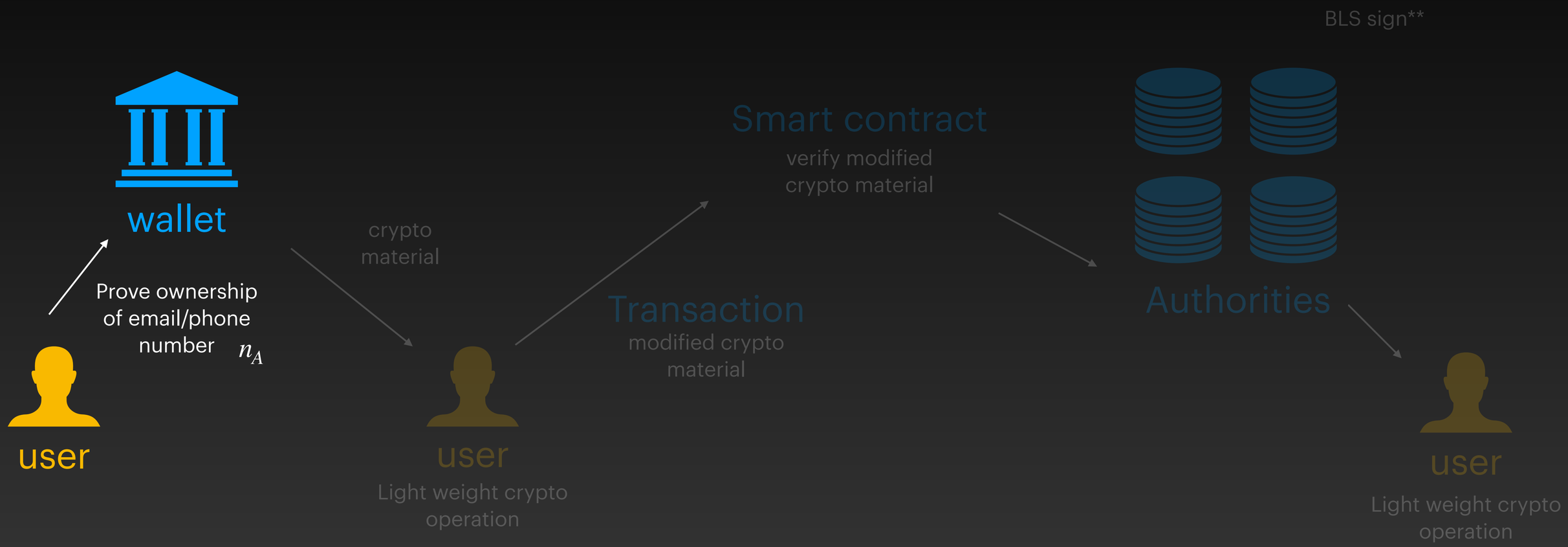
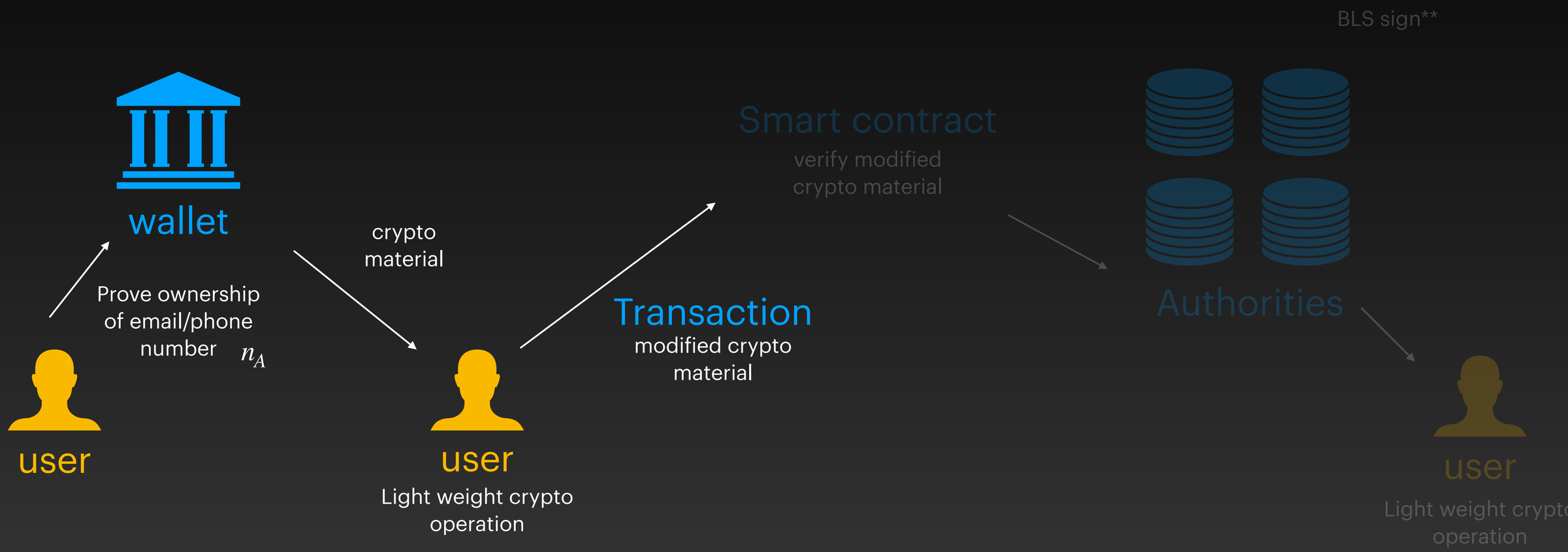
Key Discovery / Pay Username

Proposal

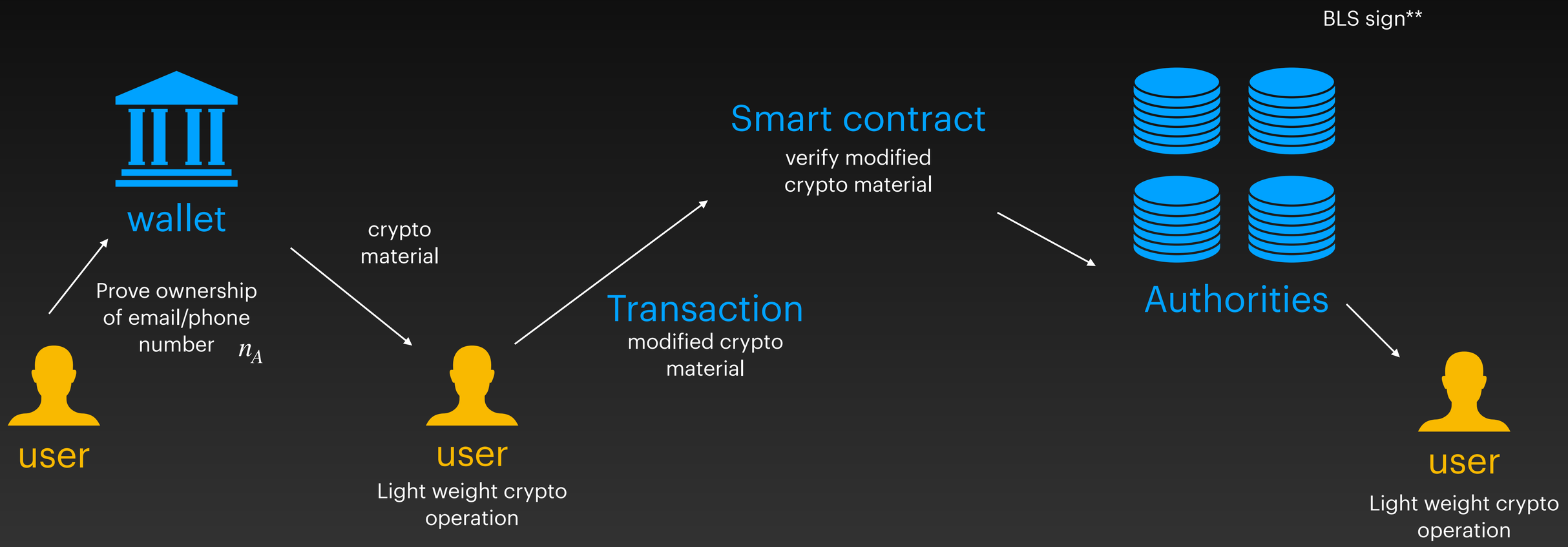
Setup
Sui Transaction



Setup
Sui Transaction



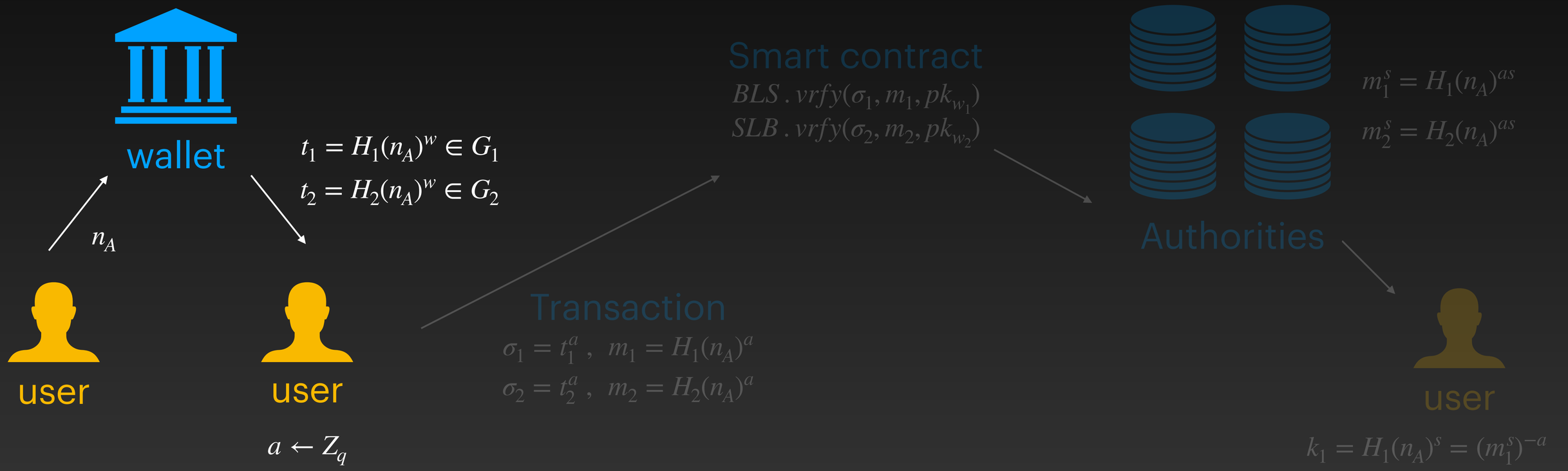
Setup
Sui Transaction



Setup
Sui Transaction

BLS sign in G1 and G2

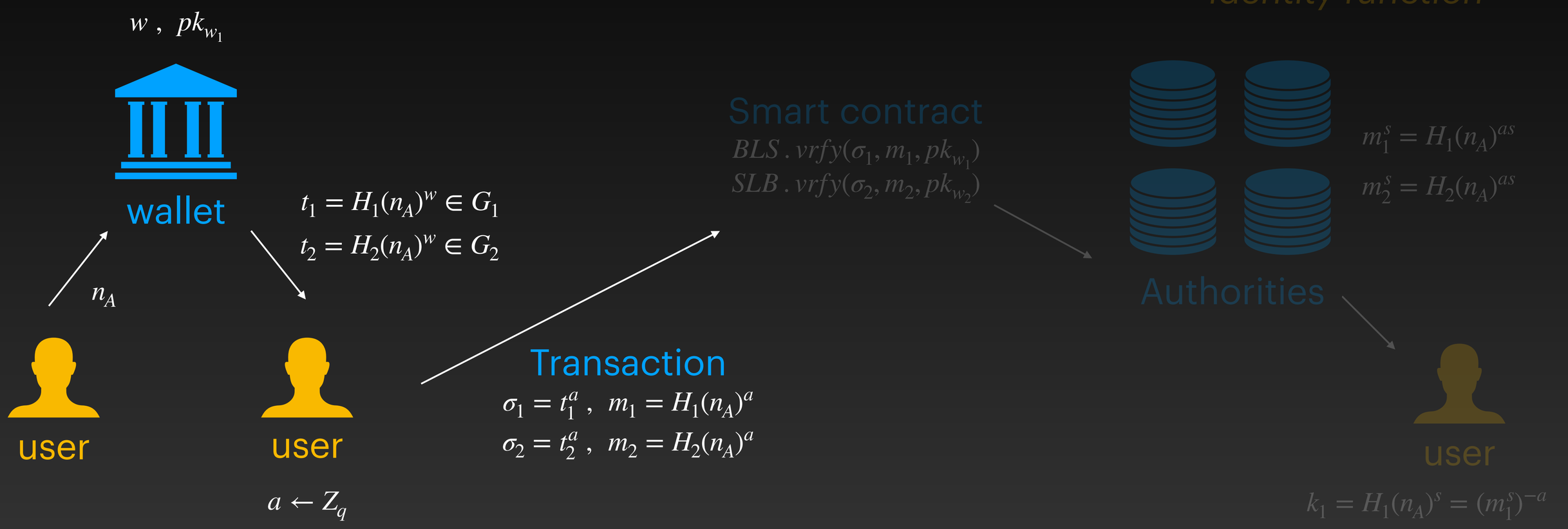
BLS sign with hash function = identity function



Setup
Sui Transaction

BLS sign in G1 and G2

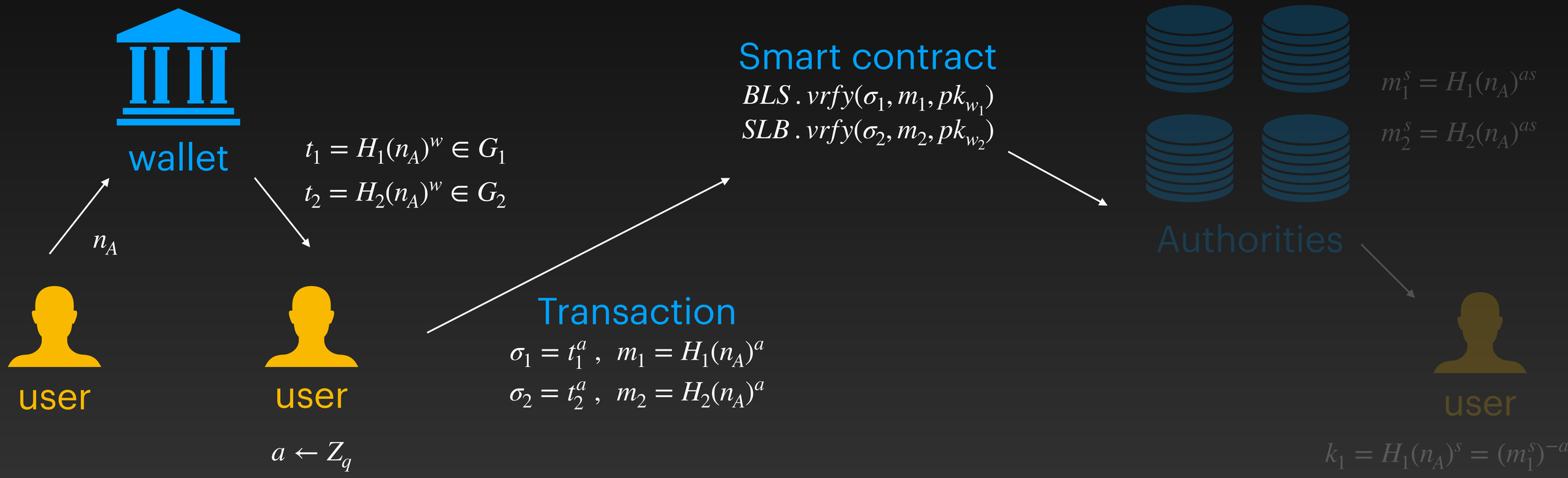
BLS sign with hash function = identity function



Setup
Sui Transaction

BLS sign in G1 and G2

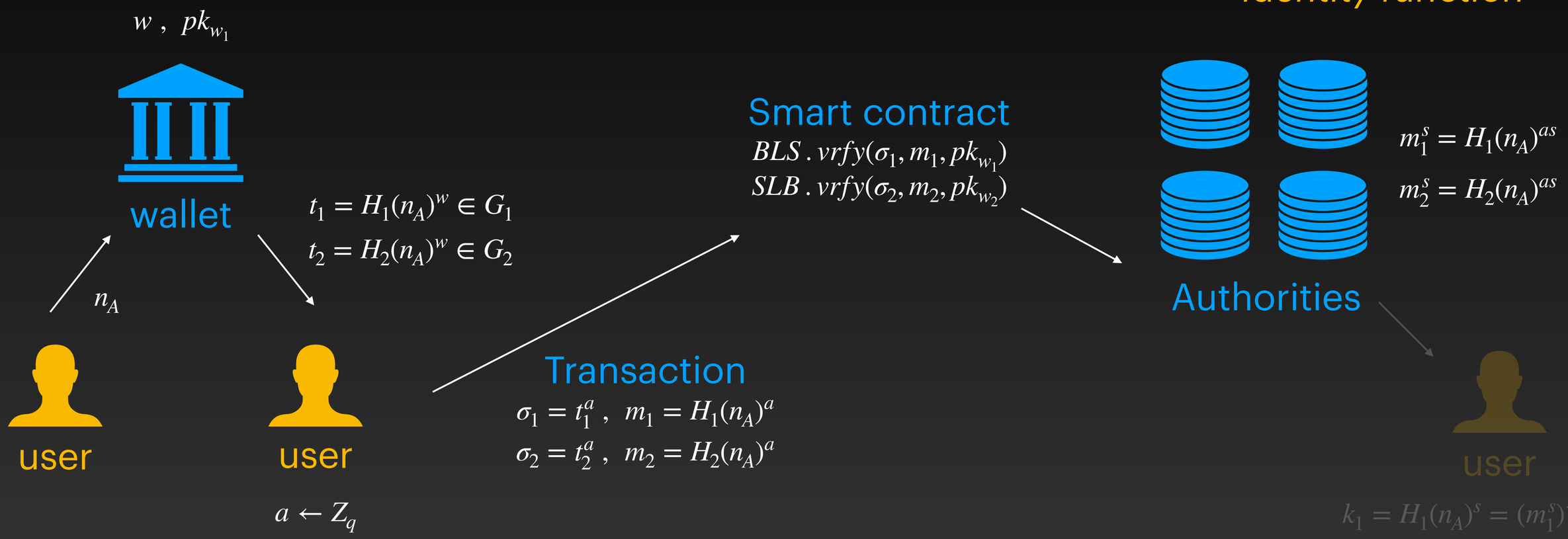
BLS sign with hash function = identity function



Setup
Sui Transaction

BLS sign in G1 and G2

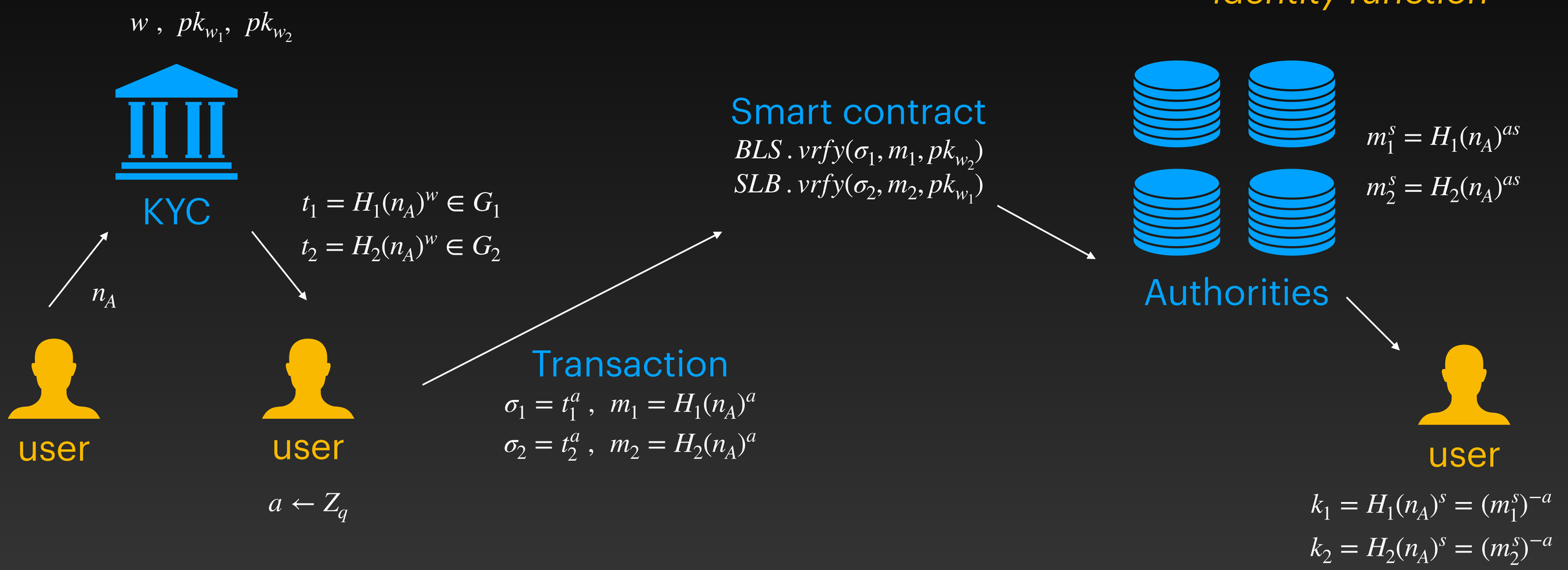
BLS sign with hash function = identity function



Setup
Sui Transaction

BLS sign in G1 and G2

BLS sign with hash function = identity function



Setup
Crypto

$w\ ,\ pk_{w_1} \in G_1\ ,\ pk_{w_2} \in G_2$

wallet

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

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

Prove ownership of email/phone number n_A

user

user

$a \leftarrow Z_q$

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

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

$s\ ,\ pk_{s_1} \in G_1\ ,\ pk_{s_2} \in G_2$

authorities

$BLS\ .\ vrfy(\sigma_1, m_1, pk_{w_1})$

$SLB\ .\ vrfy(\sigma_2, m_2, pk_{w_2})$

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

$m_2^s = H_2(n_A)^{as}$

user

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

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

Key Derivation

user A

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

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

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

user B

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

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

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

Key Derivation

user A

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

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

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

user B

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

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

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

Key Derivation

user A

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

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

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

user B

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

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

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

Sui is special

user A

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

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

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

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