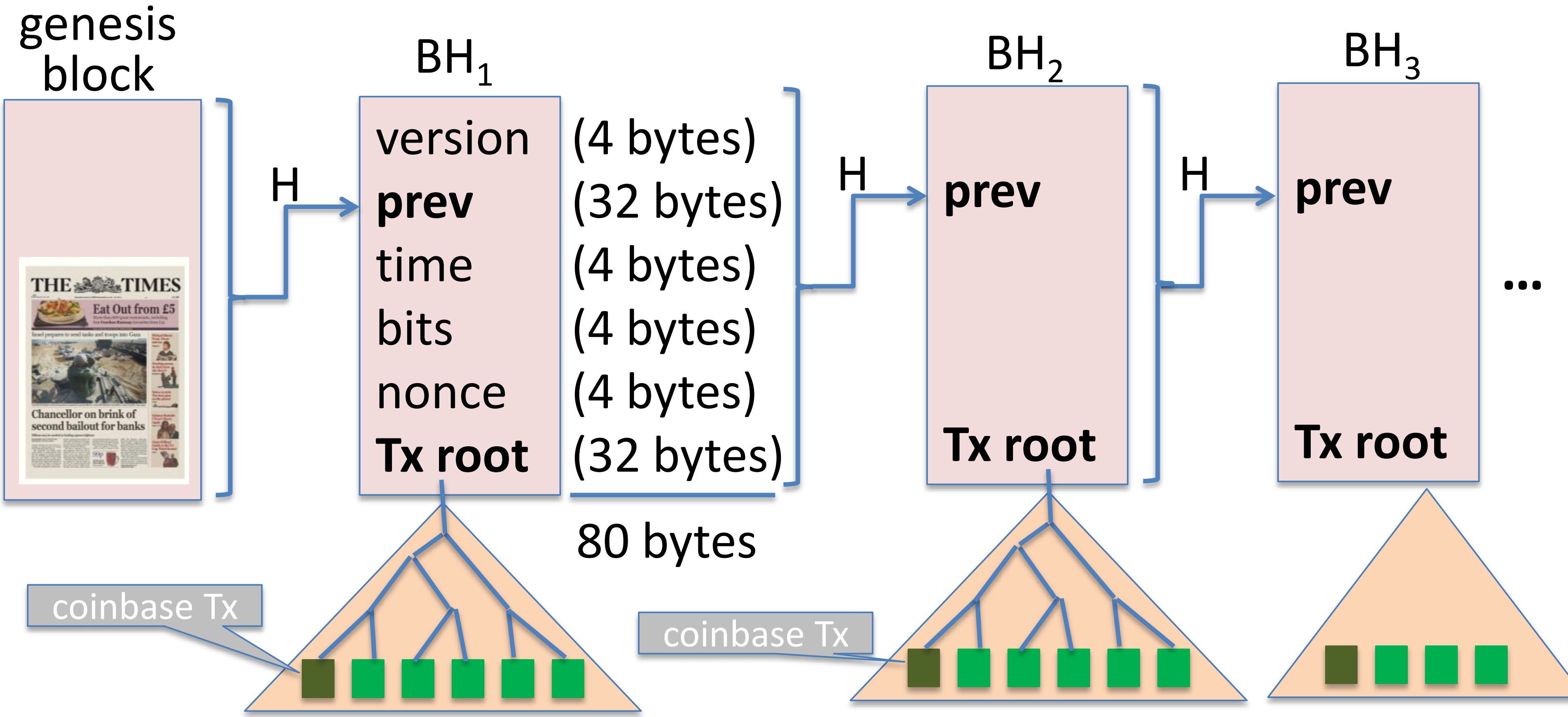
Bitcoin Scripts and Wallets

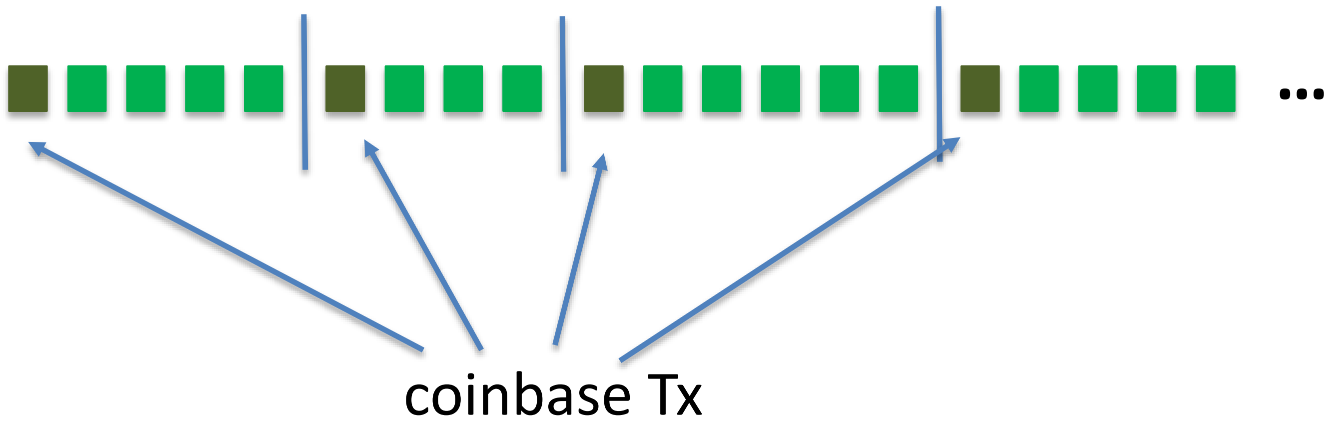
比特币脚本与钱包

Recap: the Bitcoin blockchain



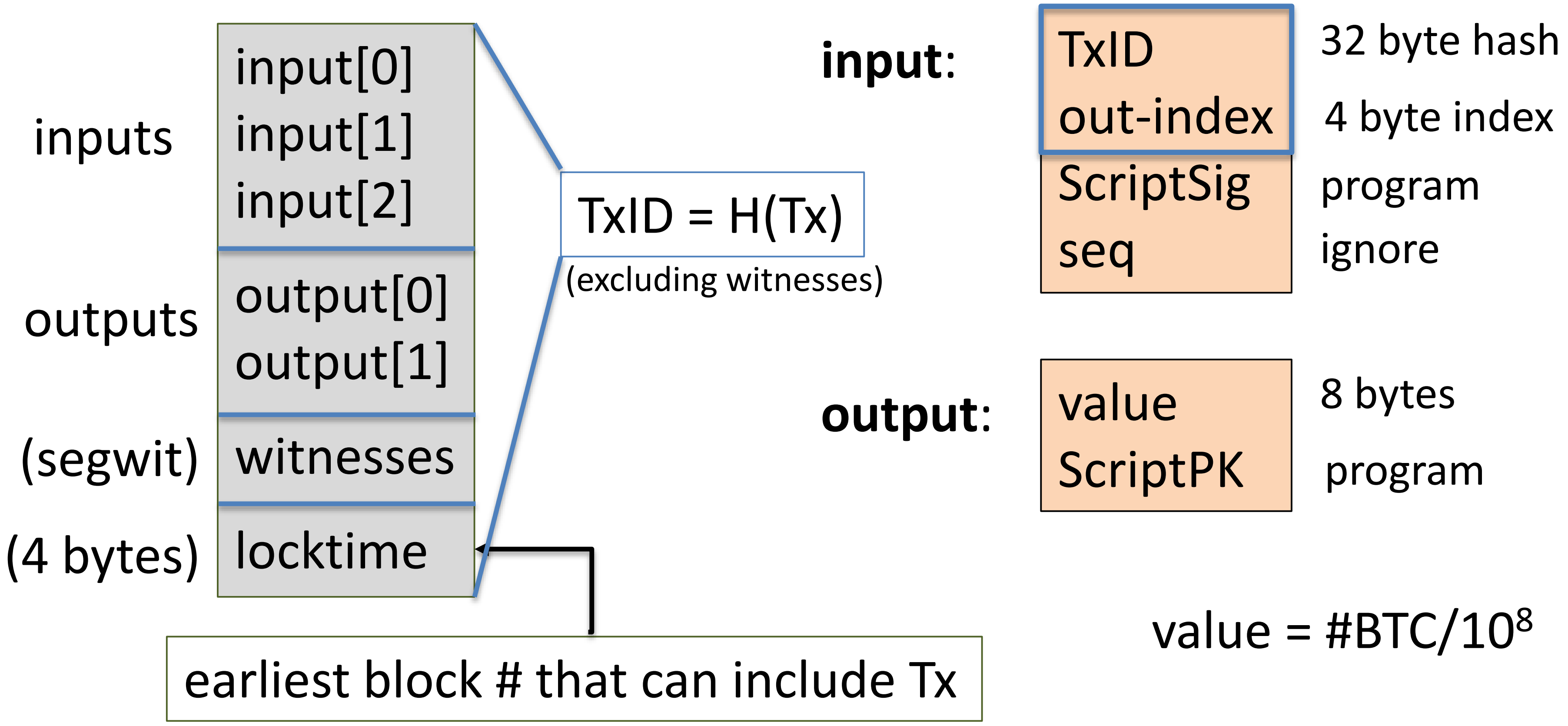
Tx sequence

View the blockchain as a sequence of Tx (append-only)

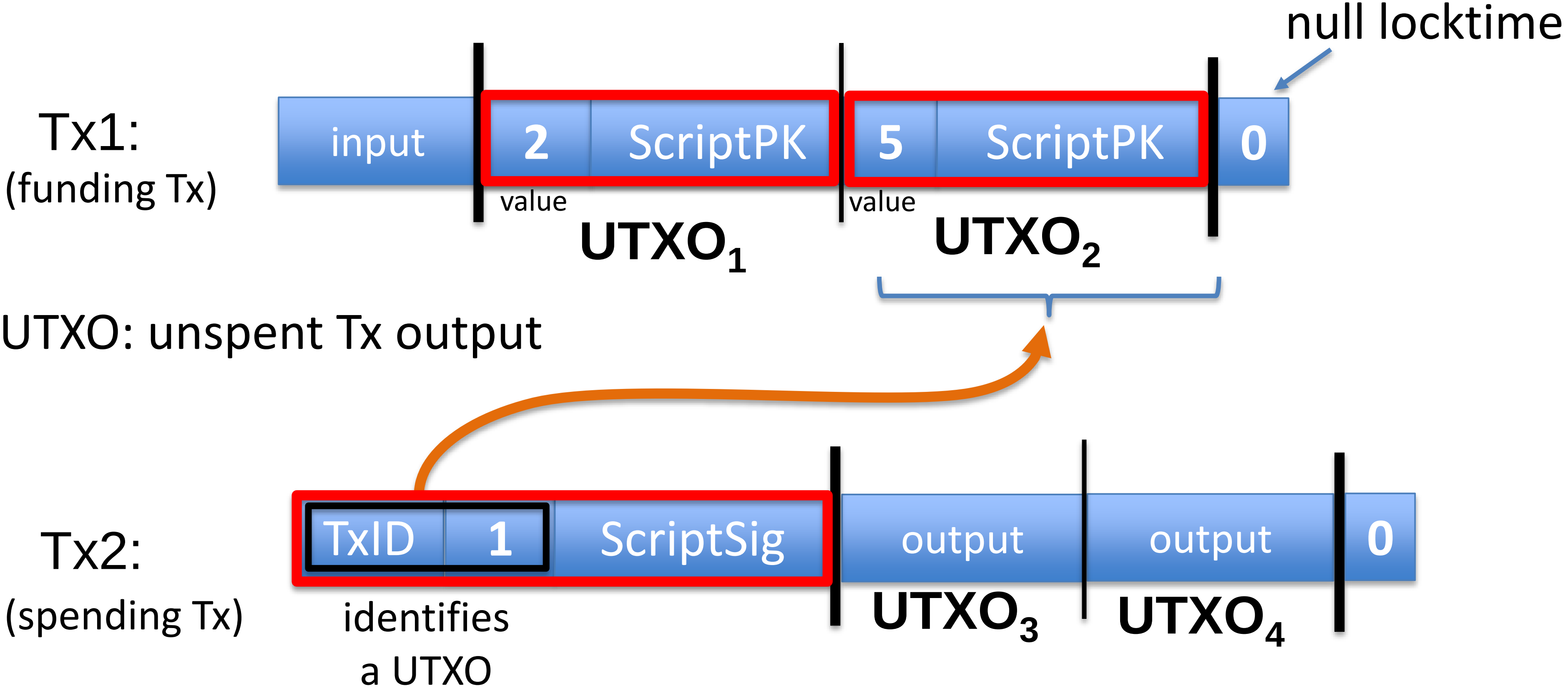


Tx cannot be erased: mistaken Tx $\Rightarrow$ locked or lost of funds

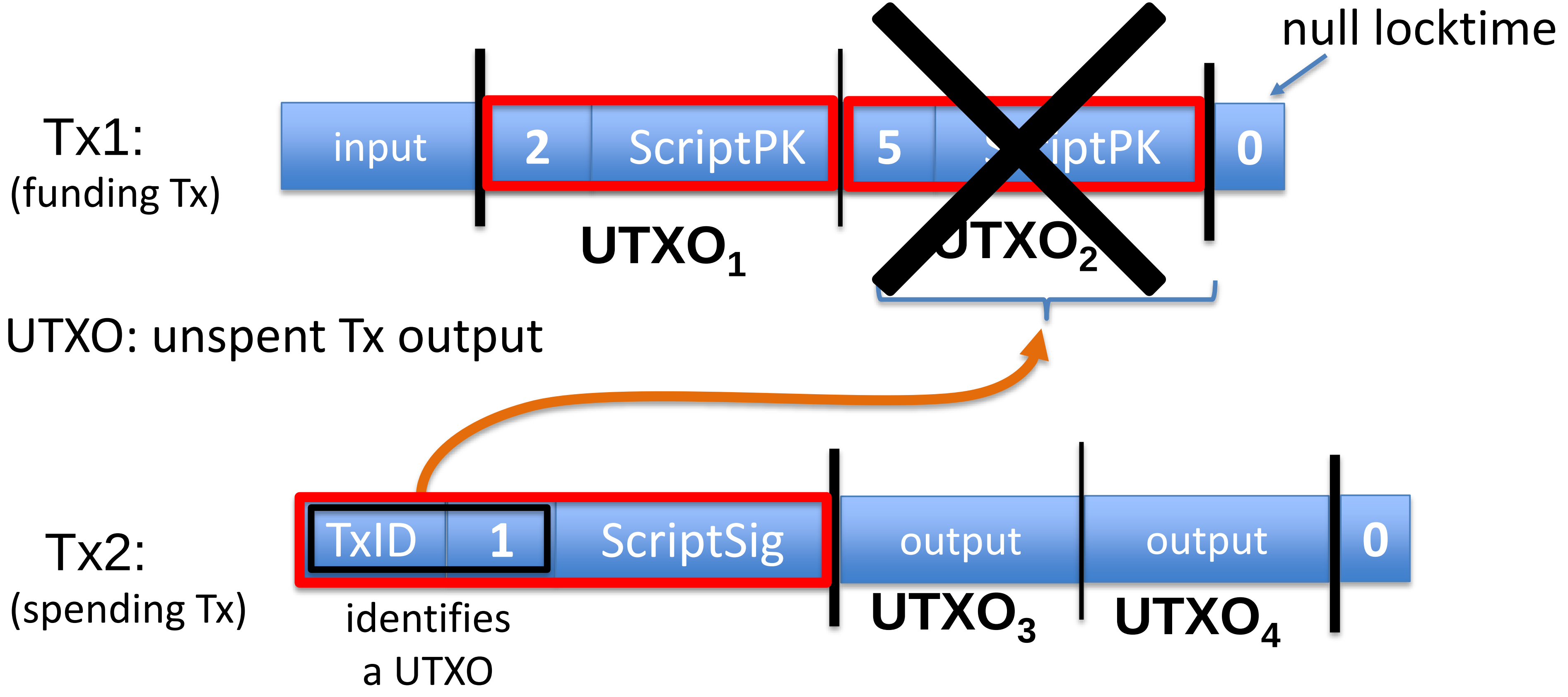
Tx structure (non-coinbase)



Example


null locktime
Tx1:
(funding Tx)
input
2
ScriptPK
value
5
ScriptPK
value
0
UTXO1
UTXO2
UTXO: unspent Tx output
Tx2:
(spending Tx)
TxID
1
ScriptSig
output
output
0
UTXO3
UTXO4
identifies
a UTXO

Example


null locktime
Tx1:
(funding Tx)
input
2
ScriptPK
5
ScriptPK
0
UTXO1
UTXO2
UTXO: unspent Tx output
Tx2:
(spending Tx)
TxID
1
ScriptSig
output
output
0
identifies
a UTXO
UTXO3
UTXO4

Validating Tx2

Miners check (for each input):

1. The program ScriptSig | ScriptPK returns true
2. TxID | index is in the current UTXO set
3. sum input values ≥ sum output values

program from funding Tx: under what conditions can UTXO be spent

program from spending Tx: proof that conditions are met

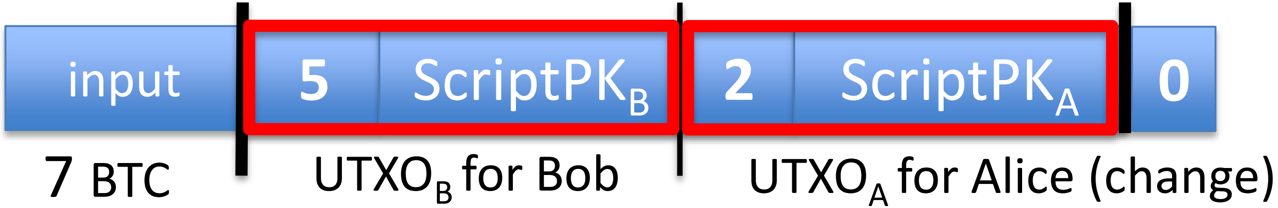
After Tx2 is posted, miners remove $UTXO_2$ from UTXO set

Transaction types: (1) P2PKH

pay to public key hash

Alice want to pay Bob 5 BTC:

- step 1: Bob generates sig key pair $(pk_B, sk_B) \leftarrow$ Gen()
- step 2: Bob computes his Bitcoin address as $Addr_B \leftarrow H(pk_B)$
- step 3: Bob sends $Addr_B$ to Alice
- step 4: Alice creates Tx:

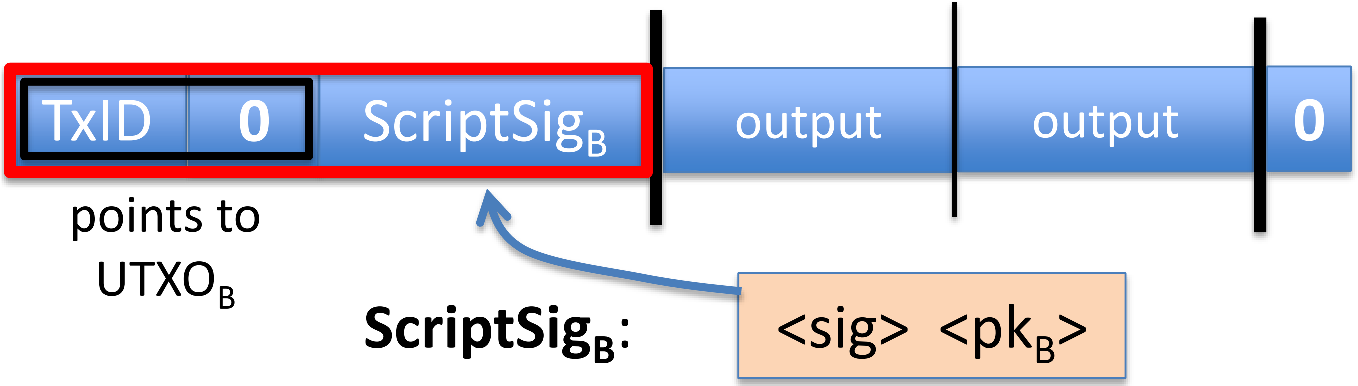


$ScriptPK_B$: DUP HASH256 **<$Addr_B$>** EQVERIFY CHECKSIG

Transaction types: (1) P2PKH

Later, when Bob wants to spend his UTXO: create a Tx_{spend}

Tx_{spend}:



<sig> = Sign(sk_B, Tx) where Tx = (Tx_{spend} excluding all ScriptSigs) (SIGHASH_ALL)

Miners validate that $ScriptSig_B$ | $ScriptPK_B$ returns true

Segregated Witness

ECDSA malleability:

- given (m, sig) anyone can create (m, sig') with sig ≠ sig'

⇒ miner can change sig in Tx, and change TxID = H(Tx)

⇒ Tx issuer cannot tell what TxID is, until Tx is posted

⇒ leads to problems and attacks

Segregated witness: signature is moved to witness field in Tx

TxID = Hash(Tx without witnesses)

Transaction types: (2) P2SH: pay to script hash

(pre SegWit in 2017)

Let’s payer specify a redeem script (instead of just pkhash)

Usage: (1) Bob publishes hash(redeem script) ⟵ Bitcoint addr.

(2) Alice sends funds to that address in funding Tx

(3) Bob can spend UTXO if he can satisfy the script

ScriptPK in UTXO: HASH160 <H(redeem script)> EQUAL

ScriptSig to spend: $<sig_1>$ $<sig_2>$ … $<sig_n>$ <redeem script>

payer can specify complex conditions for when UTXO can be spent

P2SH

Miner verifies:

(1) <ScriptSig> ScriptPK = true ⟵ spending Tx gave correct script

(2) ScriptSig = true ⟵ script is satisfied

Example P2SH: multisig

Goal: spending a UTXO requires t-out-of-n signatures

Redeem script for 2-out-of-3: (chosen by payer)

<2> <PK_1> <PK_2> <PK_3> <3> CHECKMULTISIG

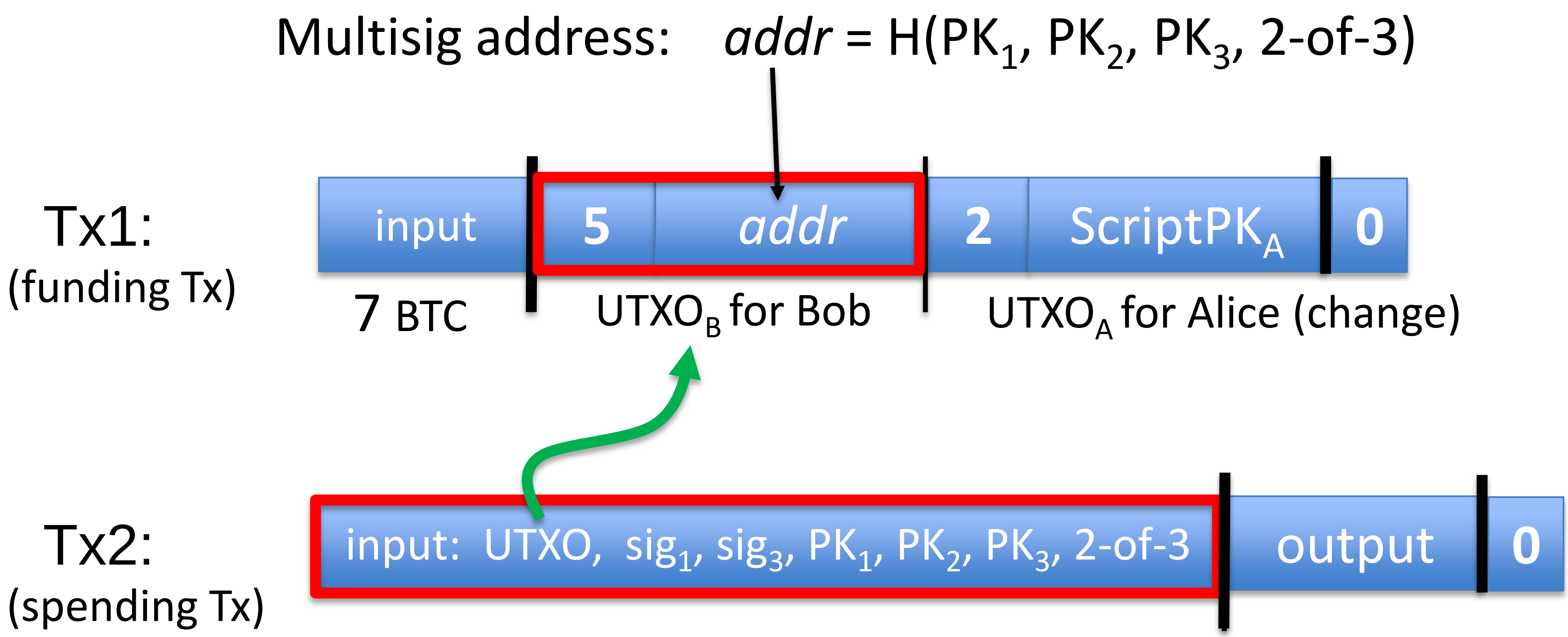
threshold

hash gives P2SH address

ScriptSig to spend: (by payee) <0> <sig1> <sig3> <redeem script>

(in the clear)

Abstractly …

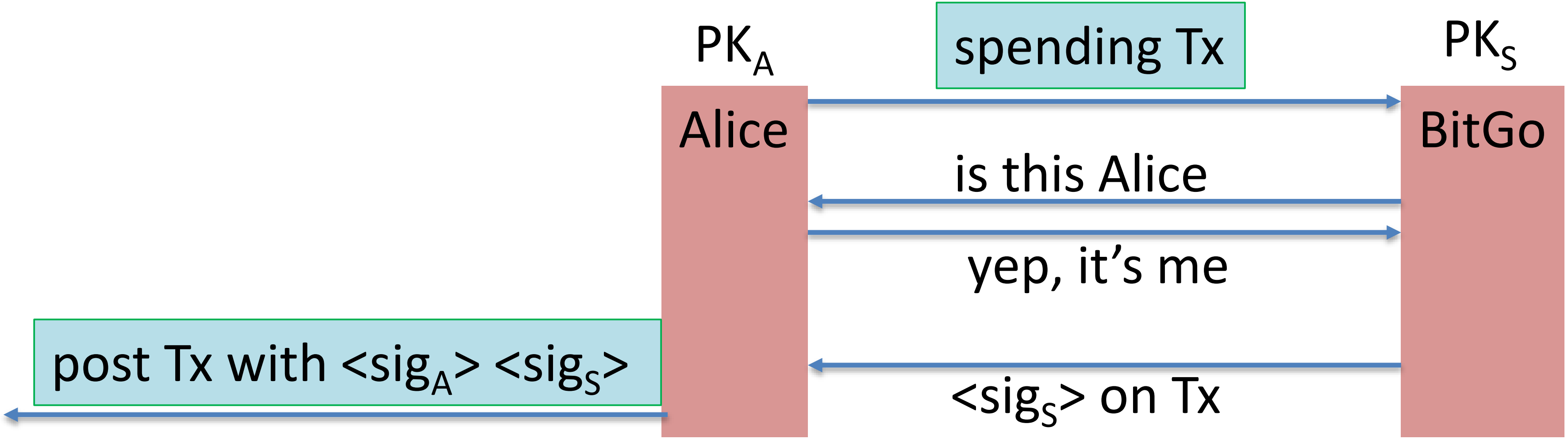


Multisig address: addr = H(PK1, PK2, PK3, 2-of-3)
Tx1:
(funding Tx)
input
5
addr
2
ScriptPKA
0
7 BTC
UTXOB for Bob
UTXOA for Alice (change)
Tx2:
(spending Tx)
input: UTXO, sig1, sig3, PK1, PK2, PK3, 2-of-3
output
0

Example Bitcoin scripts

Protecting assets with a co-signatory

Alice stores her funds in UTXOs for *addr* = **2-of-2(PK_A, PK_S)**



⇒ theft of Alice's SK_A does not compromise BTC

Escrow service

Alice wants to buy a backpack for 0.1Ƀ from merchant Bob

<u>Goal</u>: Alice only pays after backpack arrives, but can't not pay

$$addr = \textbf{2-of-3}(PK_A, PK_B, PK_J)$$

post payment of 0.11Ƀ to *addr*

($UTXO_A$)

Alice

PK_A

want backpack for 0.1Ƀ

once see Tx on chain

mail backpack

backpack arrives

send <sig_A> on Tx:

$UTXO_A \rightarrow (PK_B{:}0.1,\ PK_A{:}0.01)$

Bob

PK_B

redeem using <sig_A> <sig_B> on Tx

Judge

PK_J

Escrow service: a dispute

(1) Backpack never arrives: (Bob at fault)

Alice gets her funds back with help of Judge and a Tx:

Tx: **($UTXO_A \rightarrow PK_A$, sig_A, sig_{Judge})** [2-out-of-3]

---

(2) Alice never sends sig_A: (Alice at fault)

Bob gets paid with help of Judge as a Tx:

Tx: **($UTXO_A \rightarrow PK_B$, sig_B, sig_{Judge})** [2-out-of-3]

---

(3) Both are at fault: Judge publishes <sig_{Judge}> on Tx:

Tx: **($UTXO_A \rightarrow PK_A$: 0.05, PK_B: 0.05, PK_J: 0.01)**

Now either Alice or Bob can execute this Tx.

Cross Chain Atomic Swap

Alice has 5 BTC,   Bob has 2 LTC (LiteCoin).   They want to swap.

Want a sequence of Tx on the Bitcoin and Litecoin chains s.t.:

- either success: Alice has 2 LTC and Bob has 5 BTX,
- or failure: no funds move.

Swap cannot get stuck halfway.

Goal: design a sequence of Tx to do this.

solution: programming proj #1 ex 4.

Managing crypto assets: Wallets

Managing secret keys

Users can have many PK/SK:

- one per Bitcoin address, Ethereum address, …

Wallets:

- Generates PK/SK, and stores SK,
- Post and verify Tx,
- Show balances

Managing lots of secret keys

Types of wallets:

- **cloud** (e.g., Coinbase): cloud holds secret keys (may pay interest)
- **laptop/phone**: Electrum, MetaMask, …
- **hardware**: Trezor, Ledger, …
- **paper**: print all sk on paper
- **brain**: memorize sk (bad idea)

client stores secret keys

Lost key ⇒ lost funds

Simplified Payment Verification (SPV)

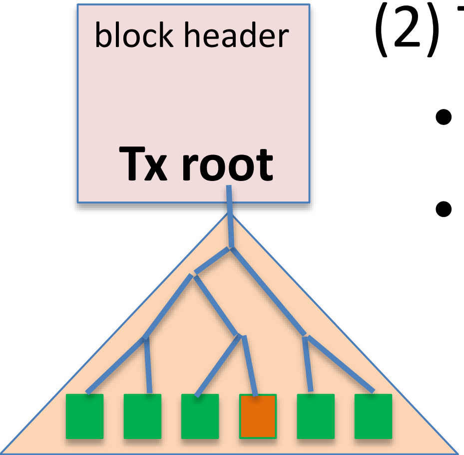
How does a wallet display Alice's current balances?

- Laptop/phone wallet needs to verify an incoming payment
- **Goal**: do so w/o downloading entire blockchain (300 GB)

SPV: (1) download all block headers (52 MB)

(2) Tx download:

- wallet → server: list of my wallet addrs (Bloom filter)
- server → wallet: Tx involving addresses + Merkle proof to block header.



简单支付验证，是一种不用运行全节点、只需保存所有的区块头，就可以验证支付的技术手段。

Simplified Payment Verification (SPV)

Problems:

(1) **Security**: are BH the ones on the blockchain? Can server omit Tx?

- Electrum: download block headers from ten random servers, optionally, also from a trusted full node.

List of servers: electrum.org/#community

(2) **Privacy**: remote server can test if an *addr* belongs to wallet

We will see better light client designs later in the course (e.g. Celo)

Hardware wallet: Ledger, Trezor, …

End user can have lots of secret keys. How to store them ???

Hardware wallet (e.g., Ledger Nano X)

- connects to laptop or phone wallet using Bluetooth or USB
- manages many secret keys
  - Bolos OS: each coin type is an app on top of OS
- PIN to unlock HW (up to 48 digits)
- screen and buttons to verify and confirm Tx

Hardware wallet: backup

Lose hardware wallet ⇒ loss of funds. What to do?

<u>Idea 1:</u> generate a secret seed $k_0 \in \{0,1\}^{256}$

for i=1,2,…: $sk_i \leftarrow HMAC(k_0, i)$, $pk_i \leftarrow g^{sk_i}$ ← ECDSA public key

$pk_1, pk_2, pk_3, \ldots$: random unlinkable addresses (without k_0)

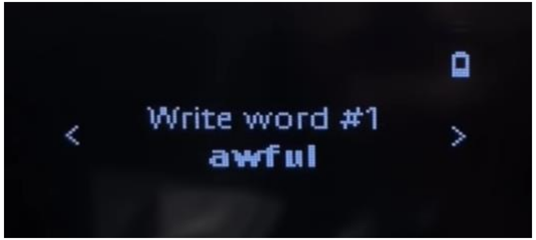
k_0 is stored on HW device and in offline storage (as 24 words)

⇒ in case of loss, buy new device, restore k_0, recompute keys

On Ledger

When initializing ledger:

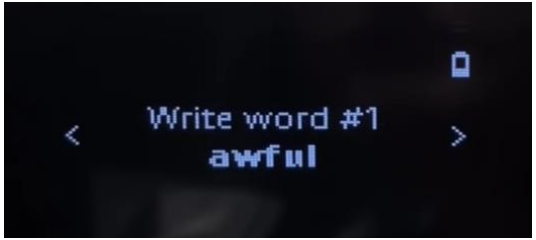
- user asked to write down the 24 words
- each word encodes 11 bits (24 × 11 = 268 bits)
    - list of 2048 words in different languages (BIP 39)



Example: English word list

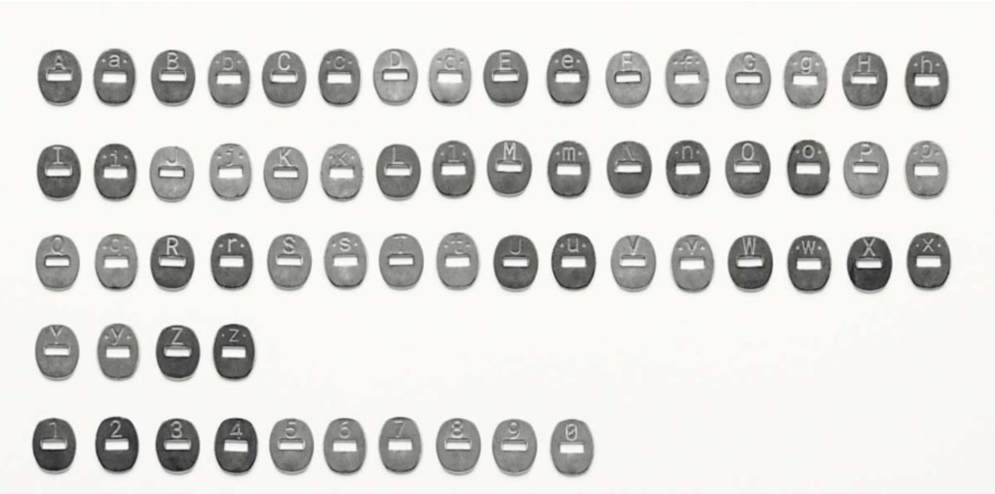
2048 lines (2048 sloc) | 12.8 KB

1	abandon
2	ability
3	able
4	about
5	above
6	absent
7	absorb
8	abstract
9	absurd
10	abuse
⋮	
2046	zero
2047	zone
2048	zoo



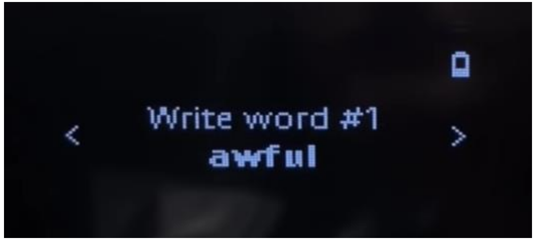
save list of 24 words

Crypto Steel



Careful with unused letters …

On Ledger



When initializing ledger:

- user asked to write down the 24 words
- each word encodes 11 bits (24 × 11 = 268 bits)
    - list of 2048 words in different languages (BIP 39)

Beware of "pre-initialized HW wallet"

- 2018: funds transferred to wallet promptly stolen

How to securely check balances?

With Idea1: need k_0 just to check my balance:

- k_0 needed to generate my addresses $(pk_1, pk_2, pk_3, \dots)$

  … but k_0 can also be used to spend funds

- Can we check balances without the spending key ??

Goal: two seeds

- k_0 lives on Ledger: can generate all secret keys (and addresses)
- k_{pub}: lives on laptop/phone wallet: can only generate addresses (for checking balance)

Idea 2: (used in HD wallets)

secret seed: $k_0 \in \{0,1\}^{256}$; $(k_1, k_2) \leftarrow$ HMAC(k_0, "init")

balance seed: $k_{pub} = (k_2,\ \ h = g^{k_1})$

for all i=1,2,…:

$$sk_i \leftarrow k_1 + \text{HMAC}(k_2, i)$$

$$pk_i \leftarrow g^{sk_i} = g^{k_1} \cdot g^{HMAC(k_2,i)} = \underbrace{h \cdot g^{HMAC(k_2,i)}}_{\text{computed from } k_{pub}}$$

k_{pub} does not reveal sk_1, sk_2, …

computed from k_{pub}

k_{pub}: on laptop/phone, generates unlinkable addresses pk_1, pk_2, …

k_0: on ledger

Paper wallet (be careful when generating)

signing key (cleartext)

Bitcoin address = base58(hash(PK))

base58 = a-zA-Z0-9 without {0,O,l,1}

Managing crypto assets: Exchanges

Hot/cold storage

Coinbase: holds customer assets

Design: 98% of assets (SK) are held in cold storage

<u>cold storage (98%)</u>

$k_0^{(1)}$

$k_0^{(2)}$

$k_0^{(3)}$

k_0

t-out-of-n secret sharing of k_0

<u>hot wallet (2%)</u>

h, k_2	SK_{hot}
used to verify cold storage balances	2% of assets

customers

Problems

Can't prove ownership of assets in cold storage,
without accessing cold storage:

- To prove ownership (e.g., in audit or in a proof of solvency)
- To participate in proof-of-stake consensus

Solutions:

- Keep everything in hot wallet (e.g, Anchorage)
- Proxy keys: keys that prove ownership of assets,
  but cannot spend assets

END OF LECTURE

Next lecture: consensus