NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Bitcoin

Mechanics of Blocks and Transactions

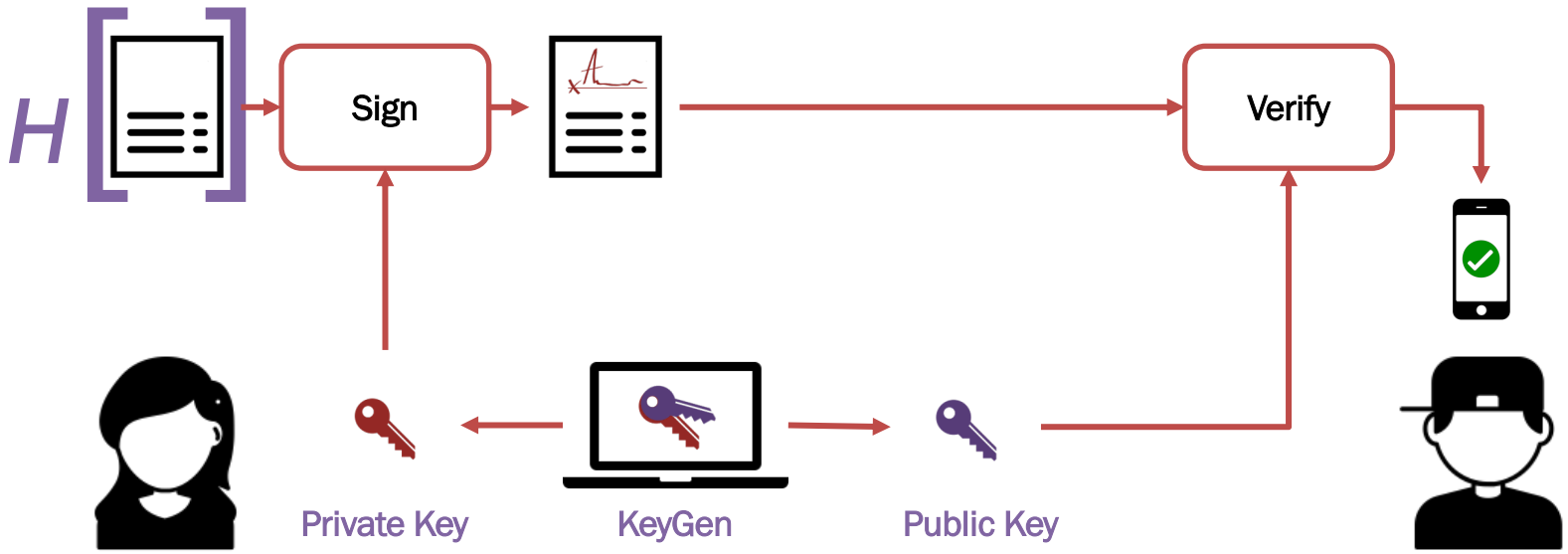
Dr Sourav SEN GUPTA
Lecturer, SCSE, NTU

Bitcoin Transactions

Keys, Addresses and Ownership

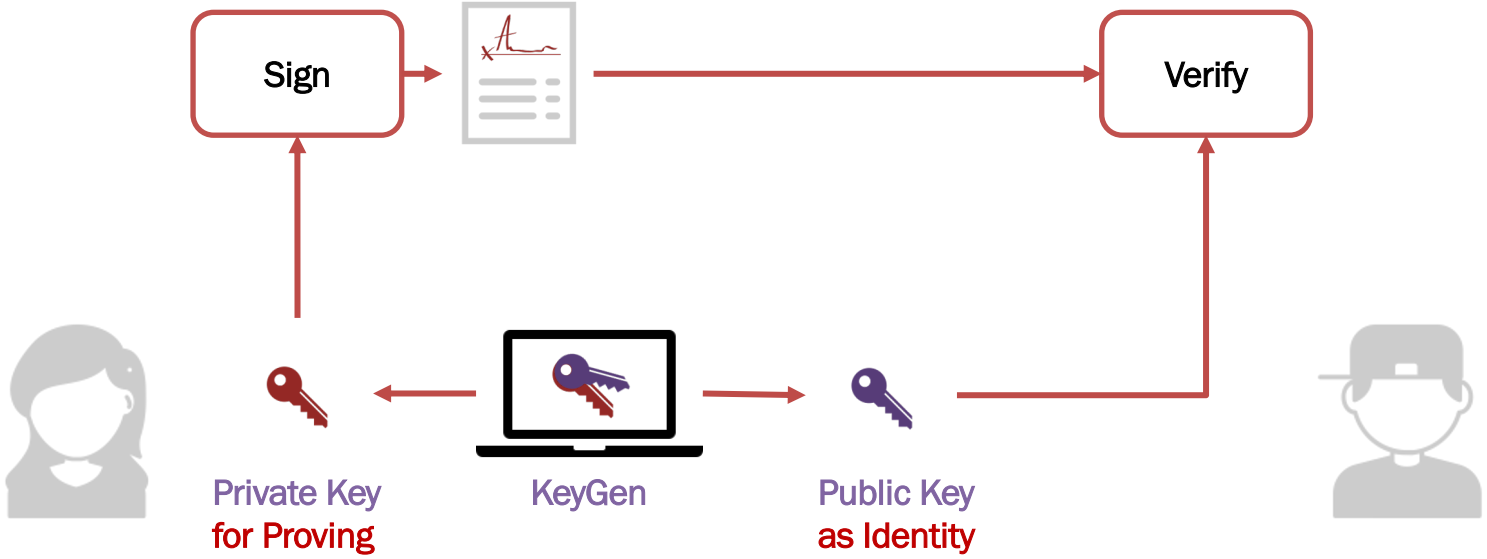
Recall : Digital Signatures

Comprises of two stages : **Sign and Verify**



Recall : Identity and Authentication

Claim identity as PubKey → **Prove** identity by PriKey → **Verify** identity by PubKey



“Anonymous” Identity

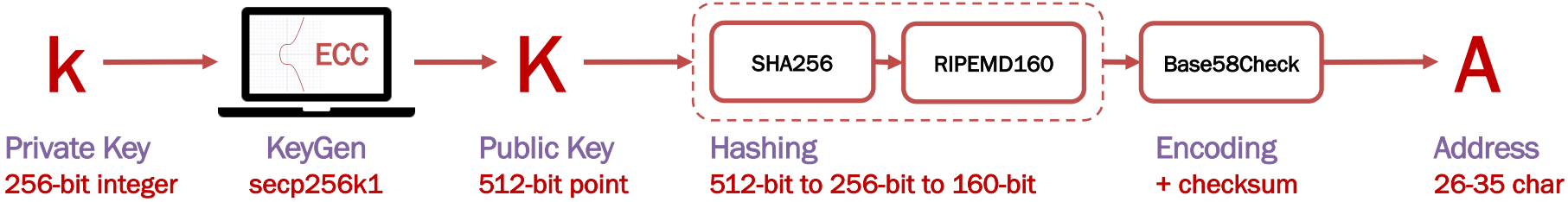
Public-Private Key Pair allows for verifiable “anonymous” Identities

- **Publish** your Public Key (or hash of it) as your “anonymous” identity
- **Sign** digital records with your Private Key when you want to prove it
- **Verification** of the claim (identity) and the proof (signature) entails:
  - Checking that your Public Key is correct (or the hash of it matches)
  - Checking that your signature can be verified using your Public Key

Bitcoin generally uses hashed-and-encoded Public Key as identity.

Bitcoin Addresses [1]

Key Generation : Elliptic Curve Cryptography (curve secp256k1)
Address Generation : SHA256 and RIPEMD160 (hash functions)



Food for thought : What if someone can derive backwards, A → K → k?

[1] reading: Chapter 4 of the book "Mastering Bitcoin"

Transfer of Assets

Bitcoin Keys and Addresses allow for verifiable Transfer of Assets

- **Receiving** : Digital Assets “assigned” to receiver’s Bitcoin address
- **Sending** : Sign with corresponding Private Key to “reassign” Asset
- **Verification** of the asset transfer and the ownership proof entails:
  - Checking that recipient’s Public Key matches the Bitcoin address
  - Checking that sender’s Signature is verified using that Public Key

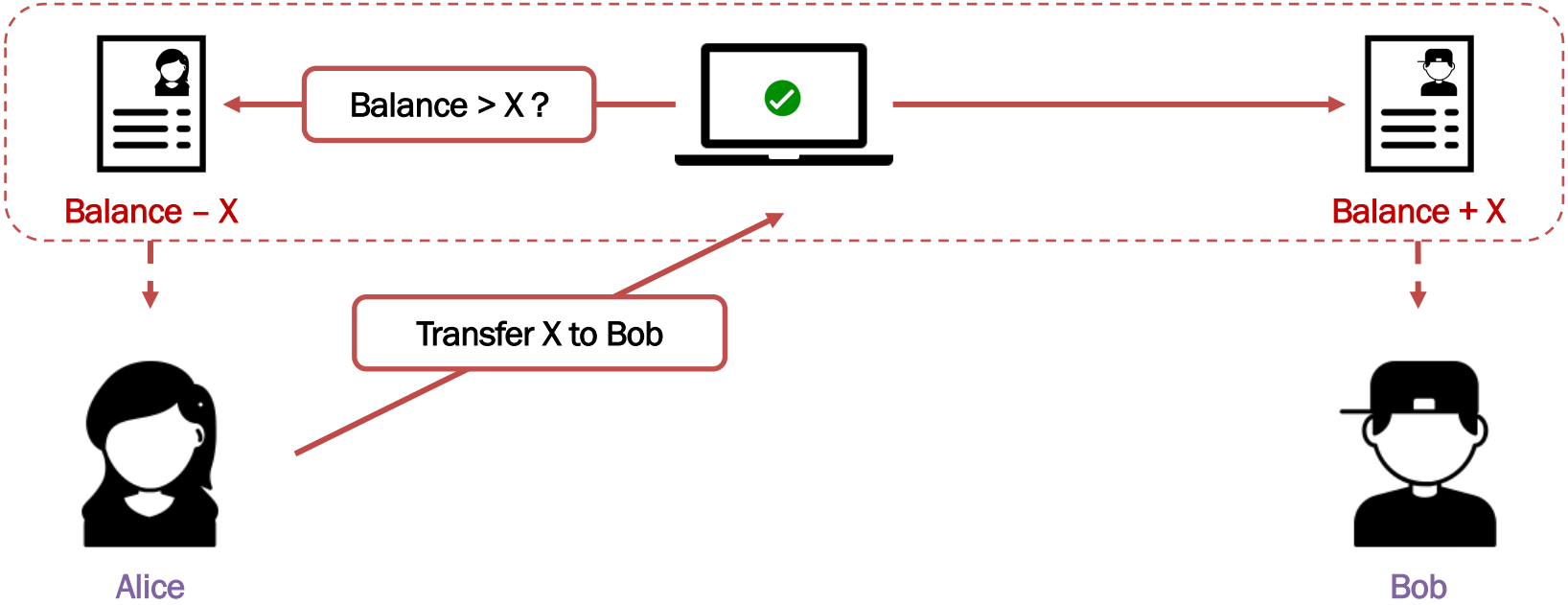
Sender must prove ownership (receipt) of Asset before a transfer.

Bitcoin Transactions

Motivation and Construction

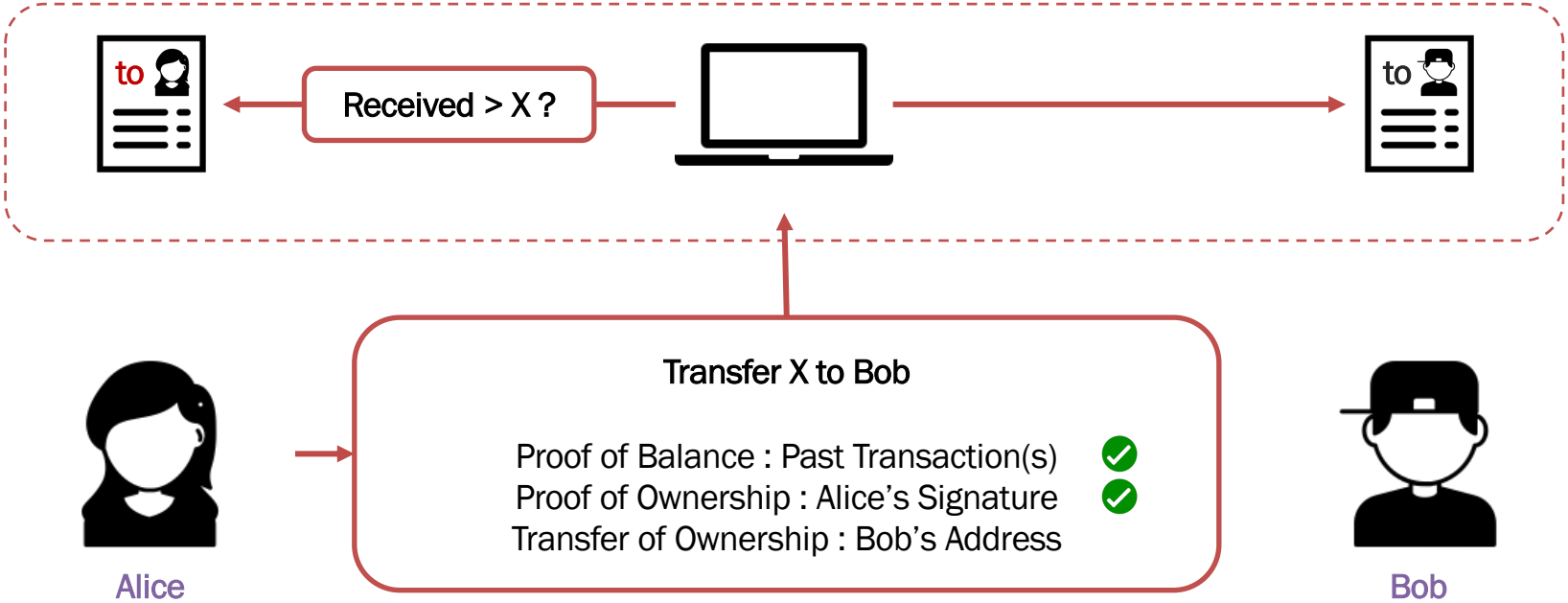
Account-based Ledger

Ledger keeper verifies Accounts and Balances for correctness of Transaction



Transaction-based Ledger

Ledger keeper verifies Signature and Receipts for correctness of Transaction



Bitcoin Transaction [2]

Verifiable data structure created by the Sender

- **Proof of Balance** : Pointer to a past Transaction within the Ledger
- **Proof of Ownership** : Signature corresponding to that Transaction
- **Transfer of Ownership** : State Bitcoin address(es) of Recipient(s)

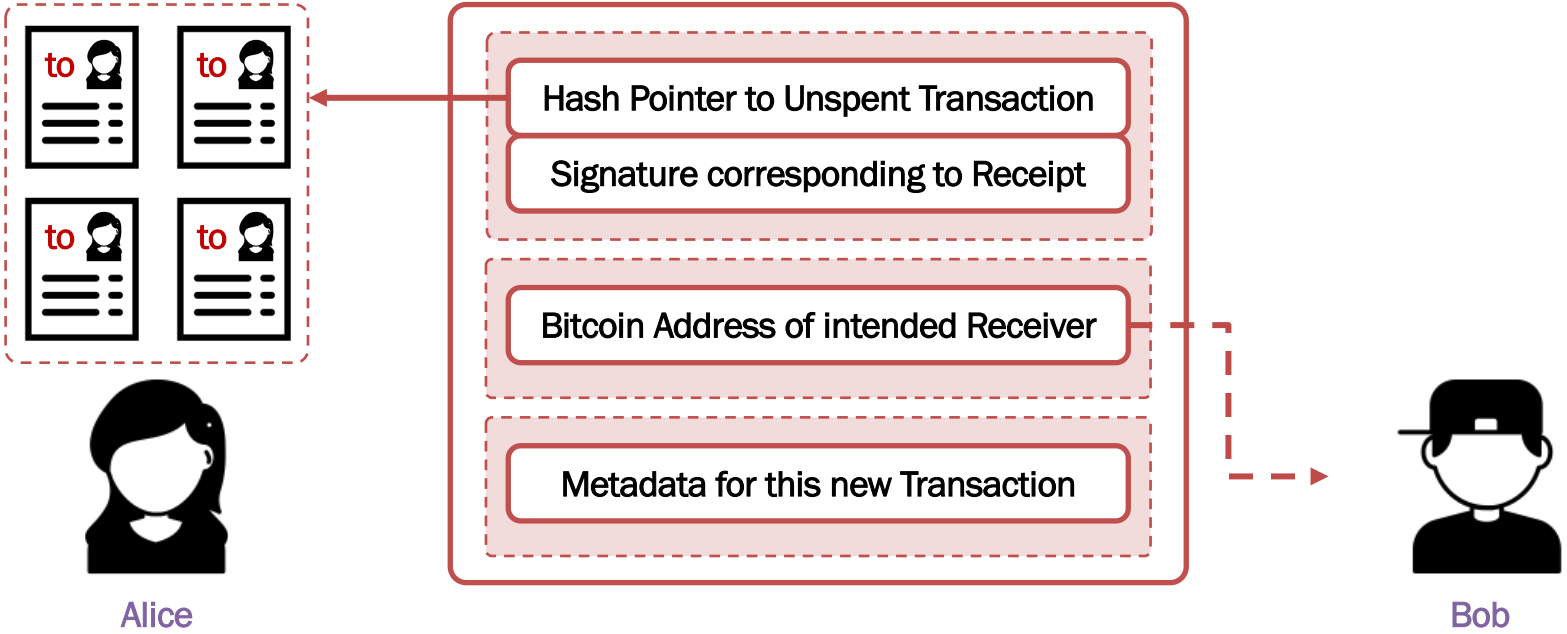
Verification of a Transaction requires two checks

1. Check that the past transaction is valid and unspent on record.
2. Check that the signature matches recipient of past transaction.

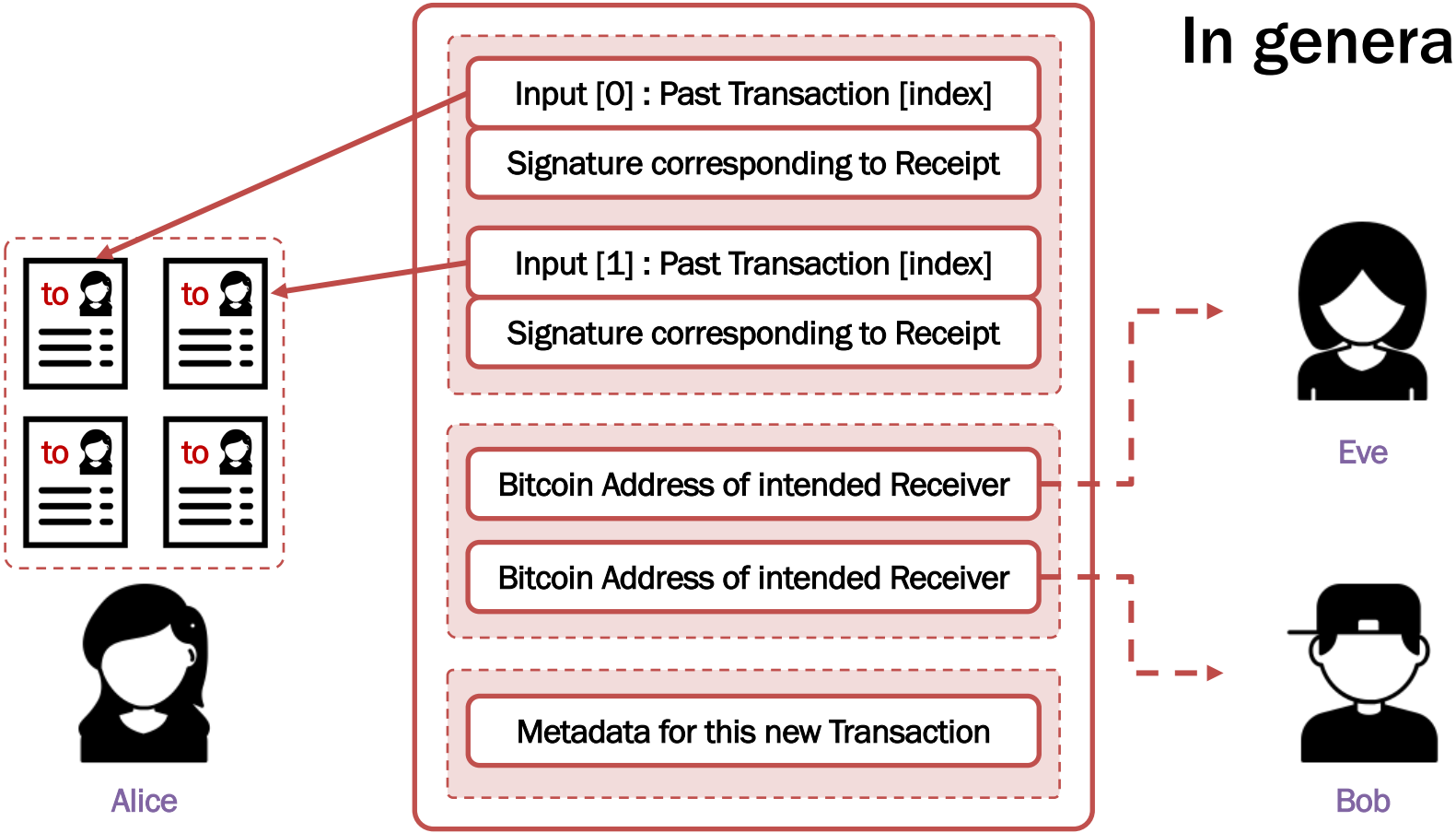
[2] reading: Chapter 5 of the book "Mastering Bitcoin"

Constructing a Transaction

Verifiable data structure created by the Sender

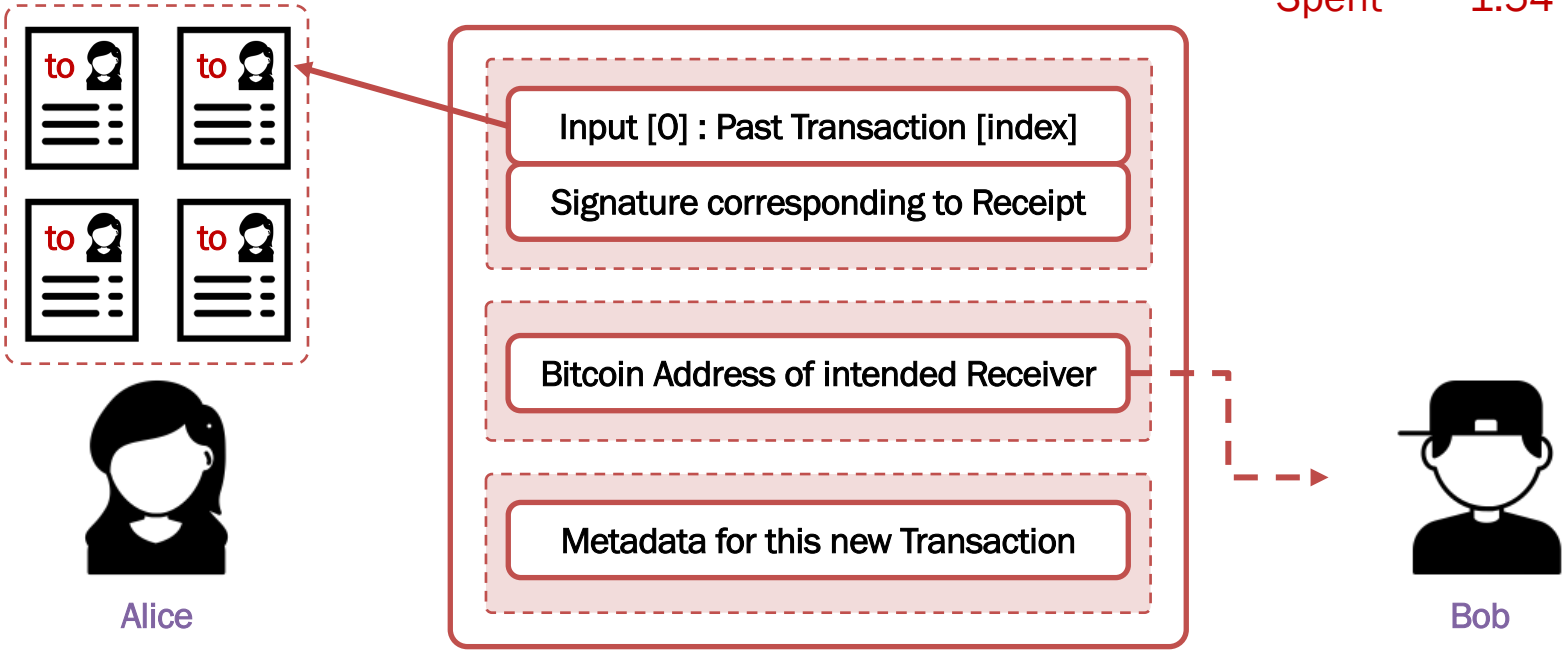


In general ...


to
to
to
to
Alice
Input [0] : Past Transaction [index]
Signature corresponding to Receipt
Input [1] : Past Transaction [index]
Signature corresponding to Receipt
Bitcoin Address of intended Receiver
Bitcoin Address of intended Receiver
Metadata for this new Transaction
Eve
Bob

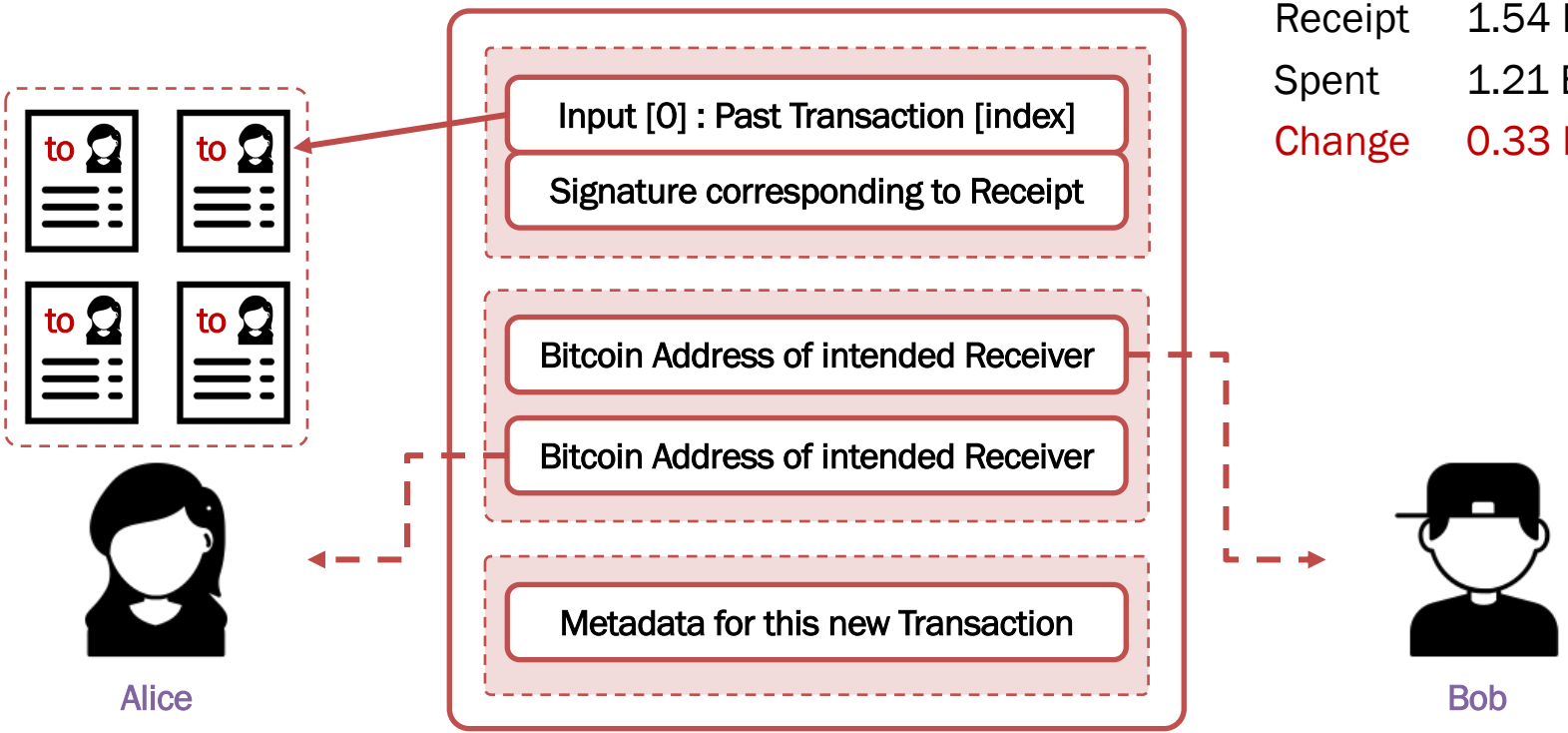
Example #1

Receipt	1.54 Bitcoin
Spent	1.54 Bitcoin



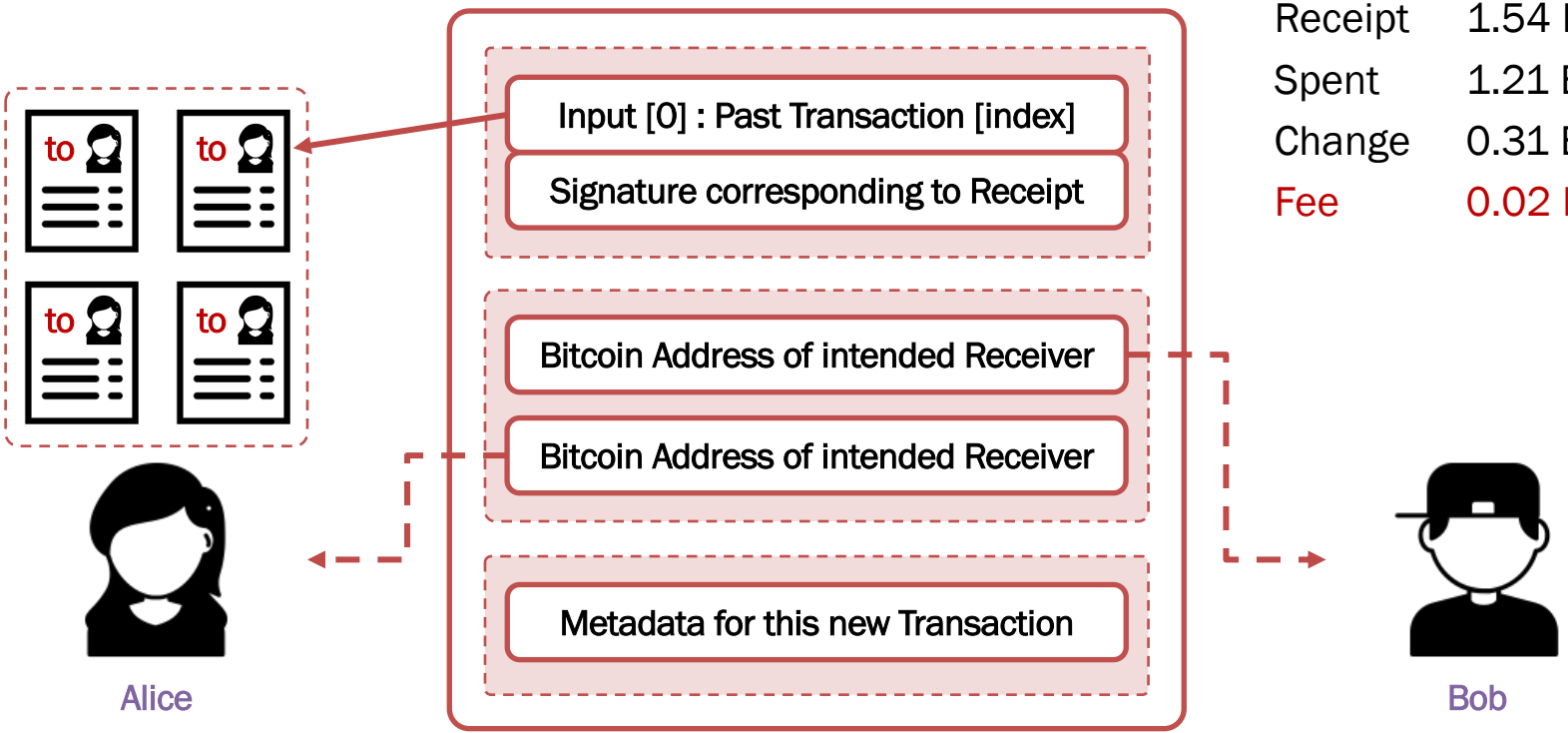
Example #2

Receipt	1.54 Bitcoin
Spent	1.21 Bitcoin
Change	0.33 Bitcoin

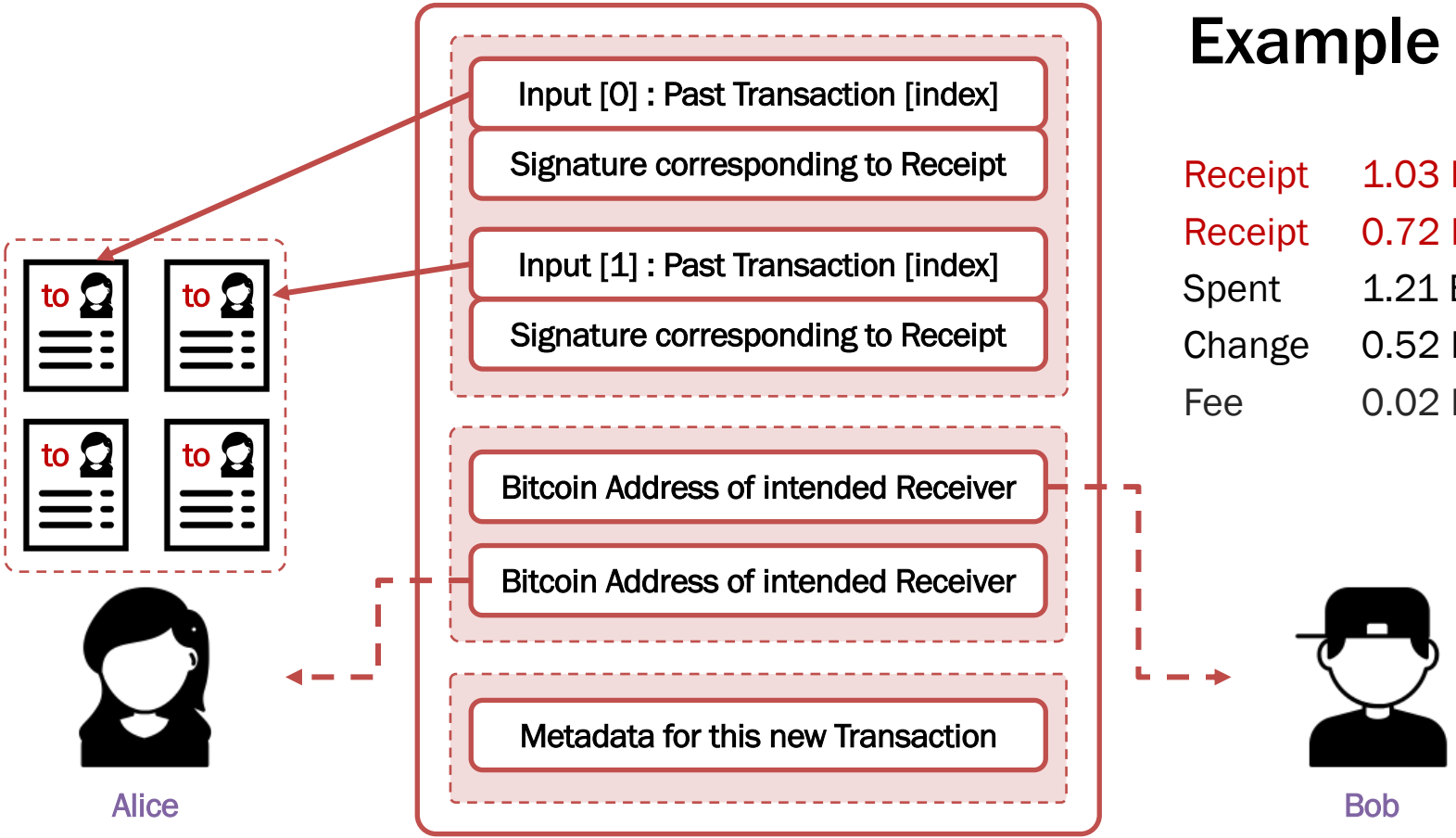


Example #3

Receipt	1.54 Bitcoin
Spent	1.21 Bitcoin
Change	0.31 Bitcoin
Fee	0.02 Bitcoin

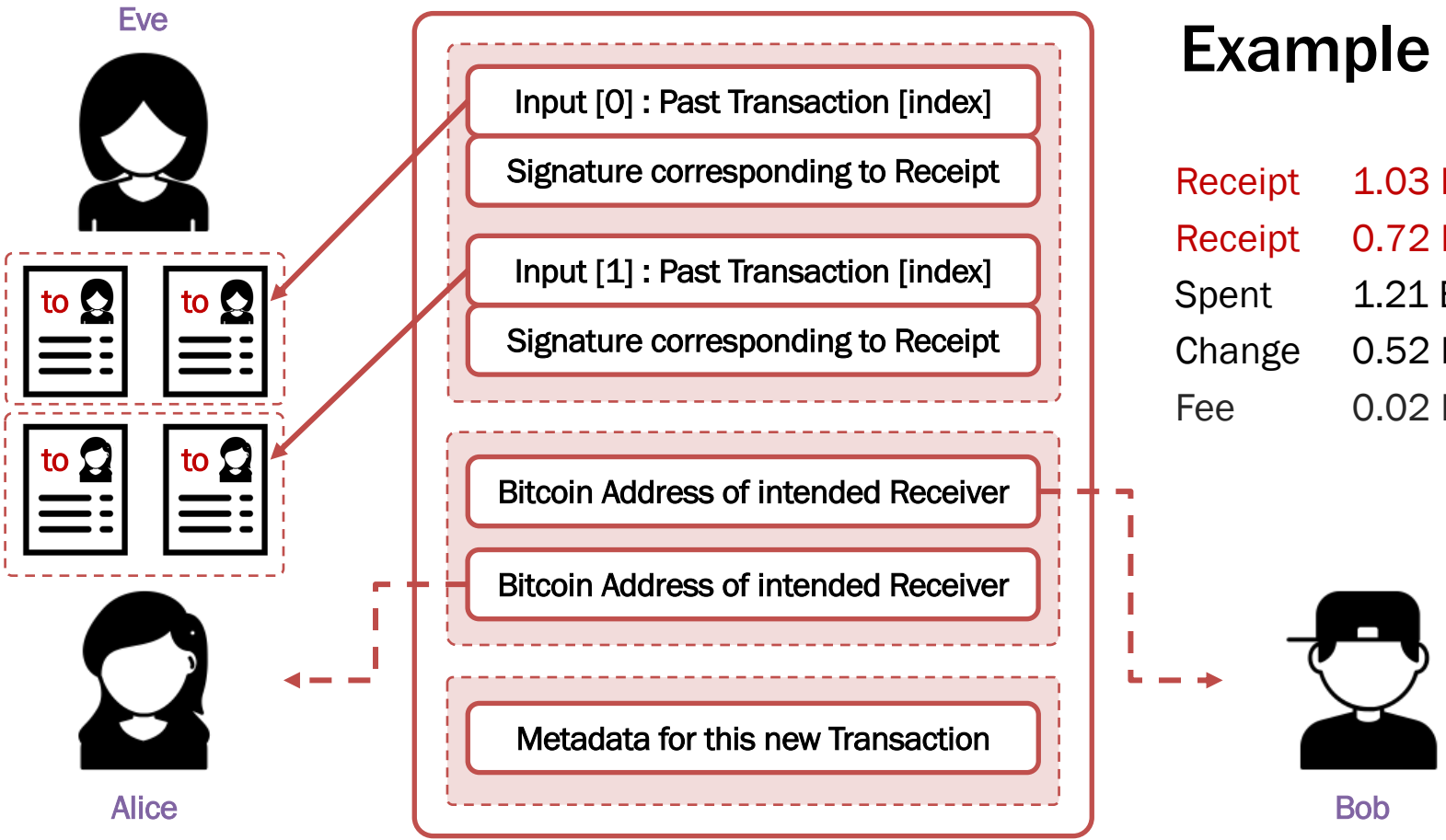


Example #4



Receipt	1.03 Bitcoin
Receipt	0.72 Bitcoin
Spent	1.21 Bitcoin
Change	0.52 Bitcoin
Fee	0.02 Bitcoin

Example #5



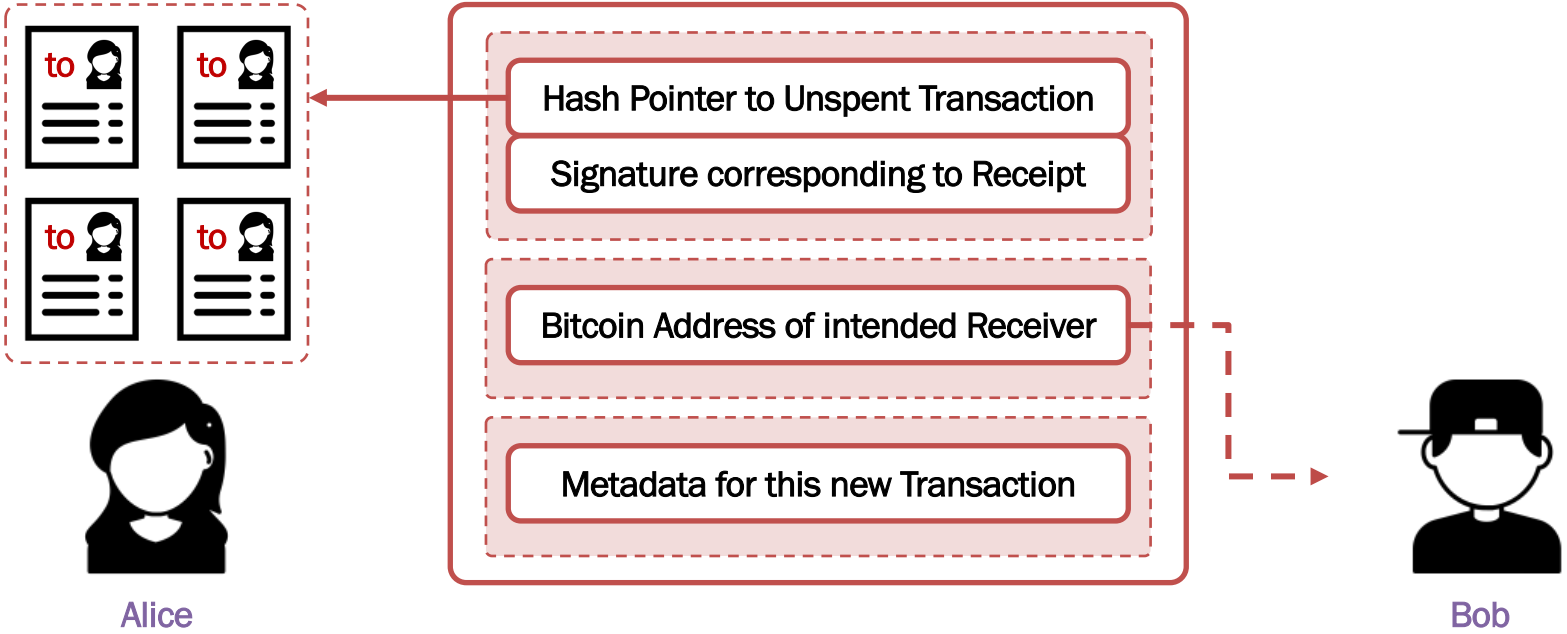
Receipt	1.03 Bitcoin
Receipt	0.72 Bitcoin
Spent	1.21 Bitcoin
Change	0.52 Bitcoin
Fee	0.02 Bitcoin

Bitcoin Transactions

Spending a Transaction

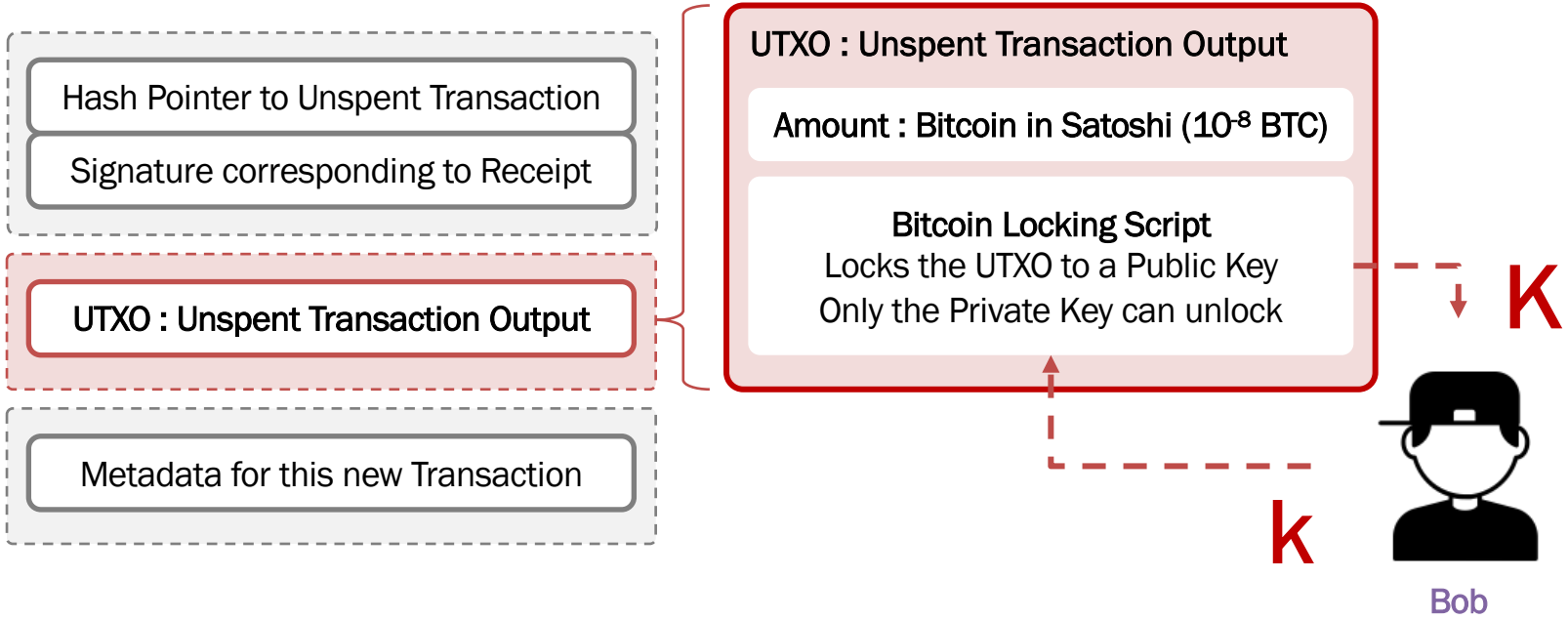
Recall : Receiving Bitcoin

Sender “specifies” the Receiver’s Bitcoin Address in Transaction Output



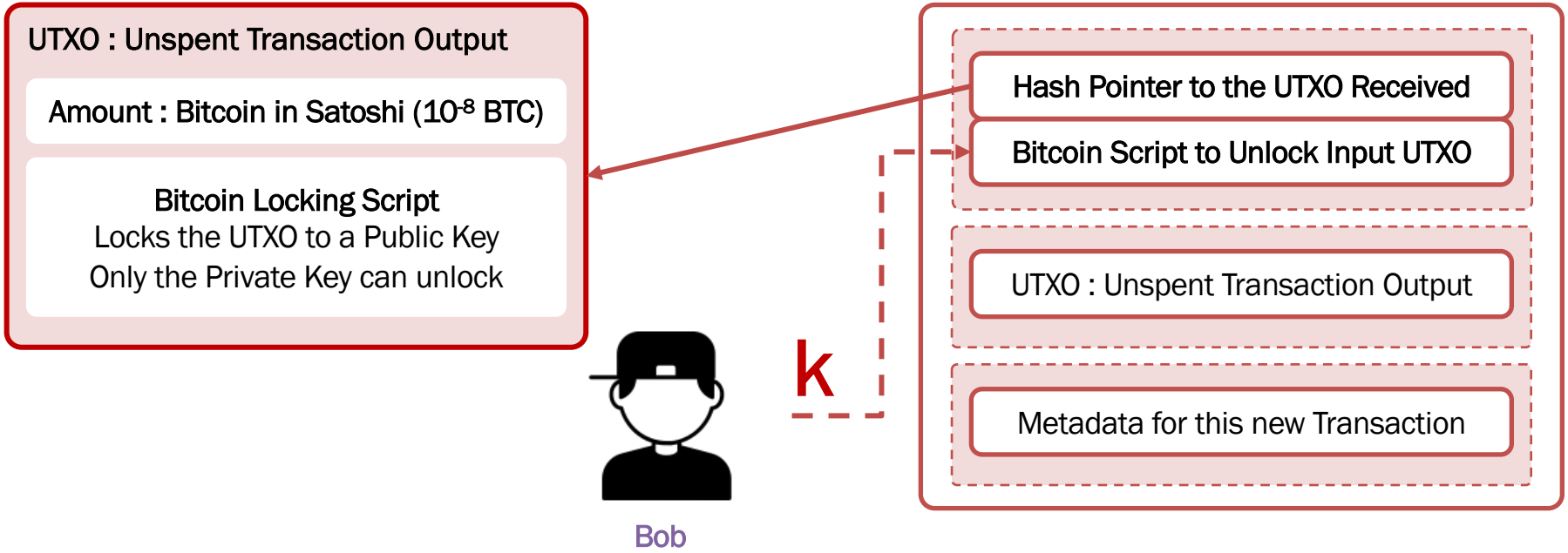
UTXO : Unspent Transaction Output

Sender “locks” certain Bitcoin amount to the Receiver’s Public Key



Spending Bitcoin UTXO [2]

Sender "specifies" the Receivers' Bitcoin Address(es) as Transaction Output



[2] reading: Chapter 5 of the book "Mastering Bitcoin"

Bitcoin Transaction in Practice

Single-input to two-output Transaction with “anonymous” Bitcoin Addresses

Hash	8a39aa4c73cb4b87904db0f0b8c27f24b0b8b9d17bd8087b7db...				2020-08-23 18:52
	11LjtJgf8AS7misuBjHPJLCE8p6bjG7GT	1.60493224 BTC	→	1Nr4GgADbyxaD2MvRGaoEEpxCgLWjhuAjM	0.75760000 BTC
				1P8TWBf3RyojFBXEnFLnJ2vBFFEs9nmre5	0.84684905 BTC
Fee	0.00048319 BTC (214.751 sat/B - 53.688 sat/WU - 225 bytes)				1.60444905 BTC
					5 Confirmations

Total Input	1.60493224 BTC
Total Output	1.60444905 BTC
Fees	0.00048319 BTC

Fee is never specified in the Transaction

Fee is the gap between Input and Output

ref : https://www.blockchain.com/btc/tx/8a39aa4c73cb4b87904db0f0b8c27f24b0b8b9d17bd8087b7dba7342ab8a0be8

Bitcoin Transaction Inputs and Outputs

Inputs

HEX ASM

Index	0	Details	Output
Address	11LjtJgf8AS7misuBjHPJLCE8p6bjG7GT	Value	1.60493224 BTC
Pkscript	76a91400107a44cb1c3957cc23a87ffc5a1de458d1827788ac		
Sigscript	47304402201743b29c473f2fc3a0f36edd87bd479a46f0f4c94e7c29fa3bb1704f8b75cdd1022065f3c3e655671a82dc70f311da7535c402f76bc1e91e2be452ee6dcf5511fbfc012102f3a3fdba423cf1b094ebcf5f87158ffc427ea0c24b4a68d82b7c5b7deaae49fe		
Witness	N/A		

Single Input UTXO
Pkscript Locks
Sigscript Unlocks

Outputs

Index	0	Details	Unspent
Address	1Nr4GgADbyxaD2MvRGaoEEpxCgLWjhuAjM	Value	0.75760000 BTC
Pkscript	76a914efa1c0e2fe35adbb55dba6ff744eab73e46e249688ac		
Index	1	Details	Unspent
Address	1P8TWBf3RyojFBXEnFLnJ2vBFFEs9nmre5	Value	0.84684905 BTC
Pkscript	76a914f2bbcd7e20fd34cfc8fe0840eee704181138b78488ac		

Two Output UTXOs
Pkscript Locks

ref : https://www.blockchain.com/btc/tx/8a39aa4c73cb4b87904db0f0b8c27f24b0b8b9d17bd8087b7dba7342ab8a0be8

Bitcoin Transaction in JSON


```
{
  "ver":2,
  "inputs":[ list of input transactions ],
  "weight":900,
  "block_height":644979,
  "relayed_by":"0.0.0.0",
  "out":[ list of output transactions ],
  "lock_time":644978,
  "size":225,
  "rbf":true,
  "block_index":0,
  "time":1598179958,
  "tx_index":0,
  "vin_sz":1,
  "hash":"8a39aa4c73cb4b87904db0f0b8c27f24b0b8b9d17bd8087b7dba7342ab8a0be8",
  "vout_sz":2
}
```


Check on your own : Entire Transaction Format
Especially, the format for Inputs and Outputs

ref : https://blockchain.info/tx/8a39aa4c73cb4b87904db0f0b8c27f24b0b8b9d17bd8087b7dba7342ab8a0be8?format=json

Bitcoin Coinbase Transaction

Transaction with no Input, meant to Mine new Bitcoin into the ecosystem.

Hash	8785cfd428b67e6f4419db7fb4529eb1216fd936476ceed888f77...			2020-08-23 19:23
	COINBASE (Newly Generated Coins)	→	1MvYASoHjqynMaMnP7SBmenyEWiLsTqoU6	6.39861453 BTC
			OP_RETURN	0.00000000 BTC
			OP_RETURN	0.00000000 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 289 bytes)			6.39861453 BTC
				3 Confirmations

Coinbase Transactions generally go to the Miner of a Block

Coinbase Transactions contain Mining Reward and Tx Fees

ref : https://www.blockchain.com/btc/tx/8785cfd428b67e6f4419db7fb4529eb1216fd936476ceed888f77daaec63fd64

Bitcoin Ledger

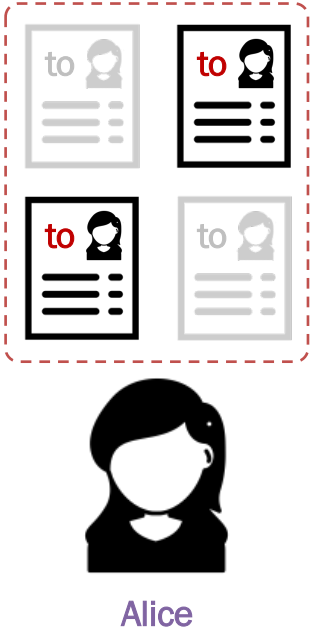
Recording the Transactions

Transaction Lifecycle

Bitcoin Transactions go through **five phases** in the Network

- **Construction** : Sender(s) construct the Transaction and Sign(s) Input(s)
- **Communication** : Transaction sent to any Node in the Bitcoin Network
- **Validation** : Each node listening to the Transaction will check its Validity
  - Check : All input transactions refer to UTXOs with valid signatures
  - Check : Total input is greater than or equal to total output Bitcoin
- **Propagation** : Each node will send valid Transactions to its Neighbors
- **Recording** : Mining nodes will Record the Transaction in local Ledger

Construct



Input [0] : UTXO in own Wallet [index]

Signature Script to “unlock” UTXO

Input [1] : UTXO in own Wallet [index]

Signature Script to “unlock” UTXO

Output [0] : Script to “lock” UTXO

Output [1] : Script to “lock” UTXO

Metadata for this new Transaction

required

UTXOs in own Wallet

Recipient Public Key

input

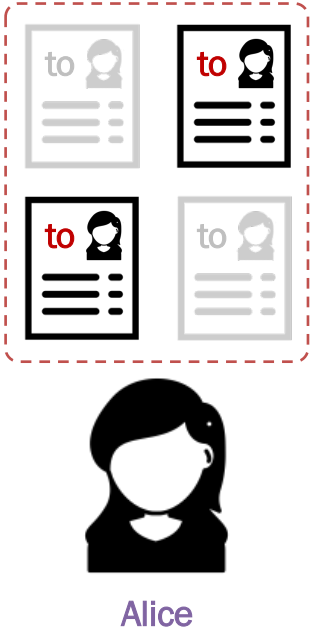
UTXO Hash Pointers

Index of Input UTXO

output

UTXO Locking Script

Communicate



Input [0] : UTXO in own Wallet [index]

Signature Script to “unlock” UTXO

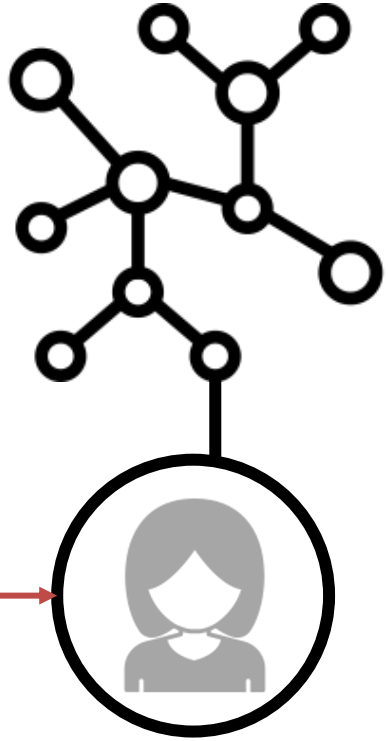
Input [1] : UTXO in own Wallet [index]

Signature Script to “unlock” UTXO

Output [0] : Script to “lock” UTXO

Output [1] : Script to “lock” UTXO

Metadata for this new Transaction



Validate

required

Bitcoin Script Exec

Recipient Public Key

iteration

Validate all Inputs

track

Fee = Input – Output

Input [0] : UTXO in own Wallet [index]

Signature Script to “unlock” UTXO

Input [1] : UTXO in own Wallet [index]

Signature Script to “unlock” UTXO

Output [0] : Script to “lock” UTXO

Output [1] : Script to “lock” UTXO

Metadata for this new Transaction

UTXO [index]

Amount : Bitcoin in Satoshi

Lock : Public Key Script (K)

Unlock : Signature Script (k)

Propagate

if valid transaction

Send to Neighbors

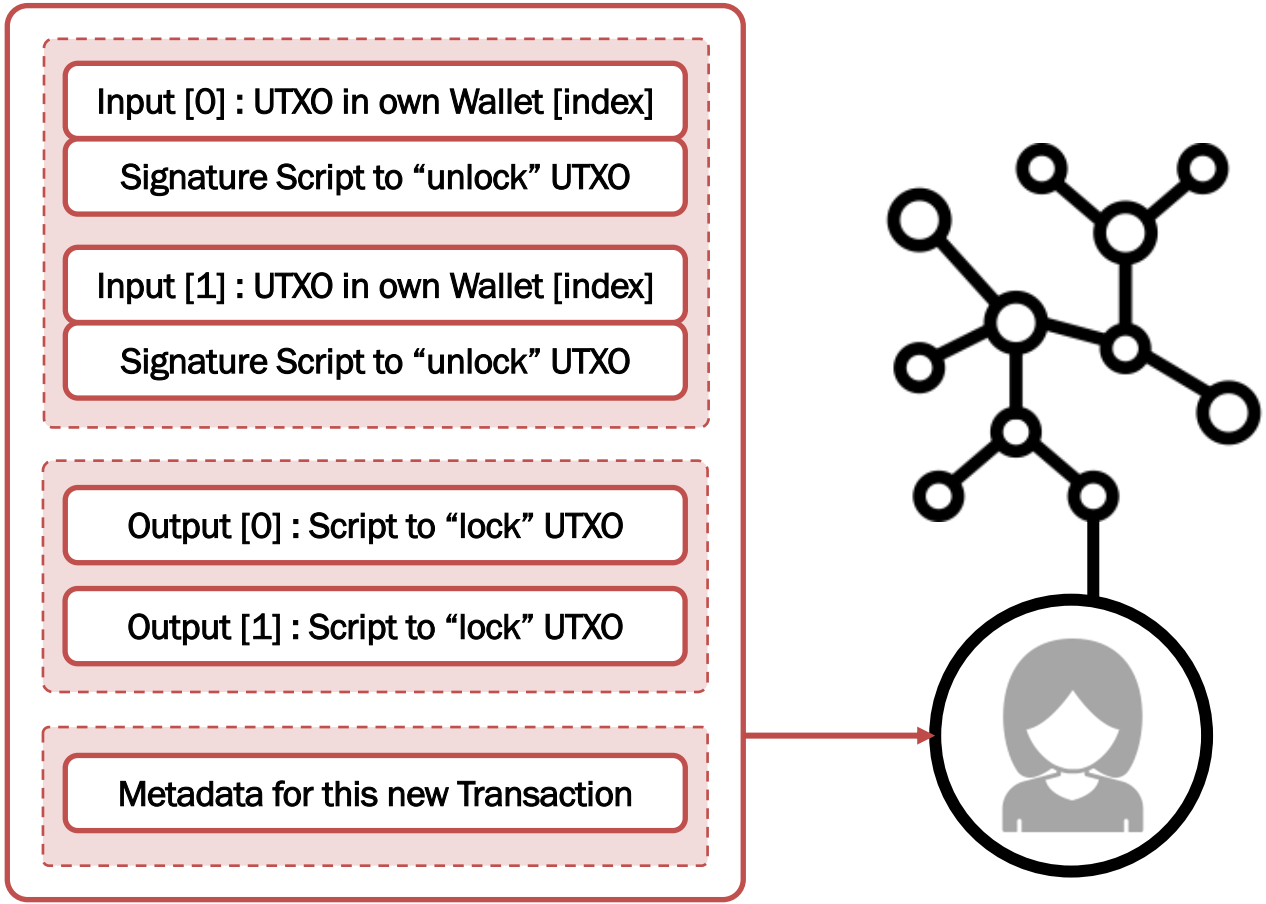
Send forth “Accept”

if invalid transaction

Send back “Reject”

track

All Transactions

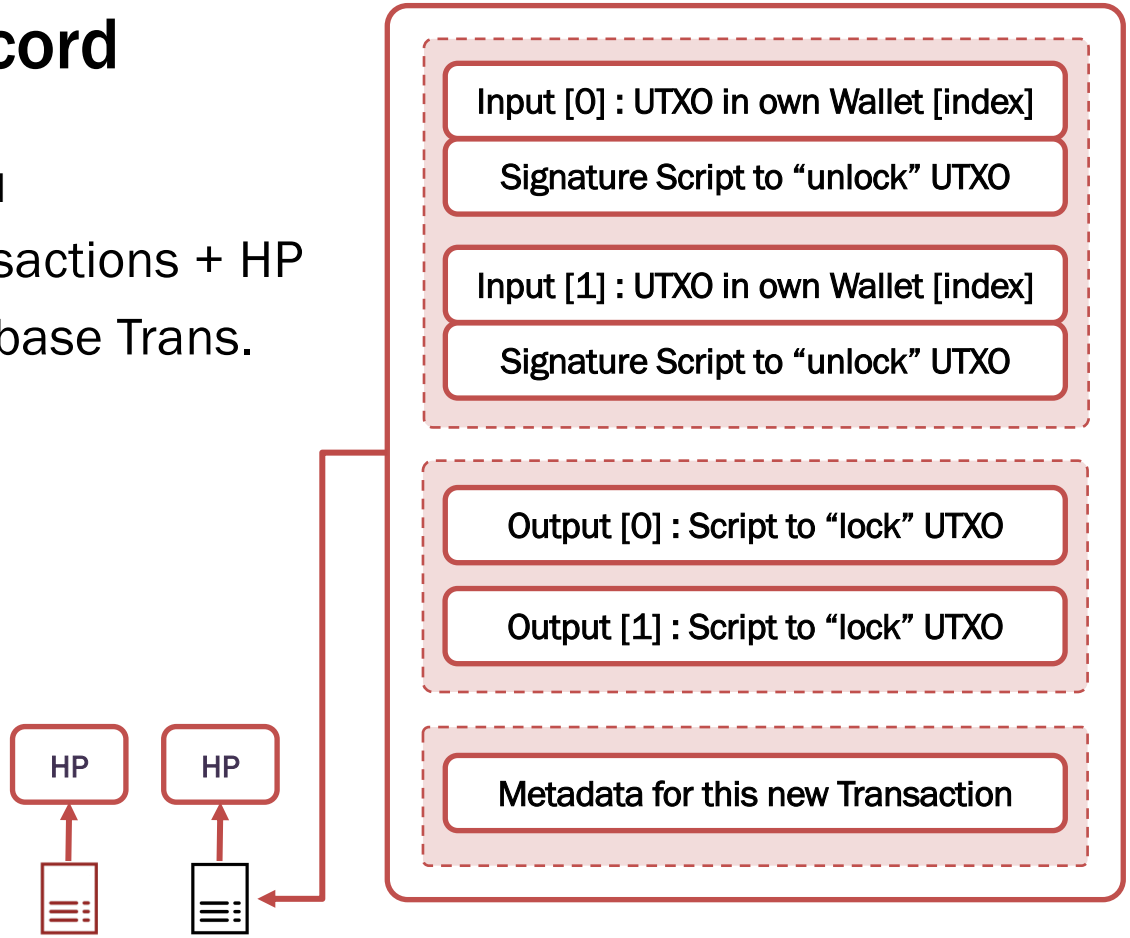


Record

record

Transactions + HP

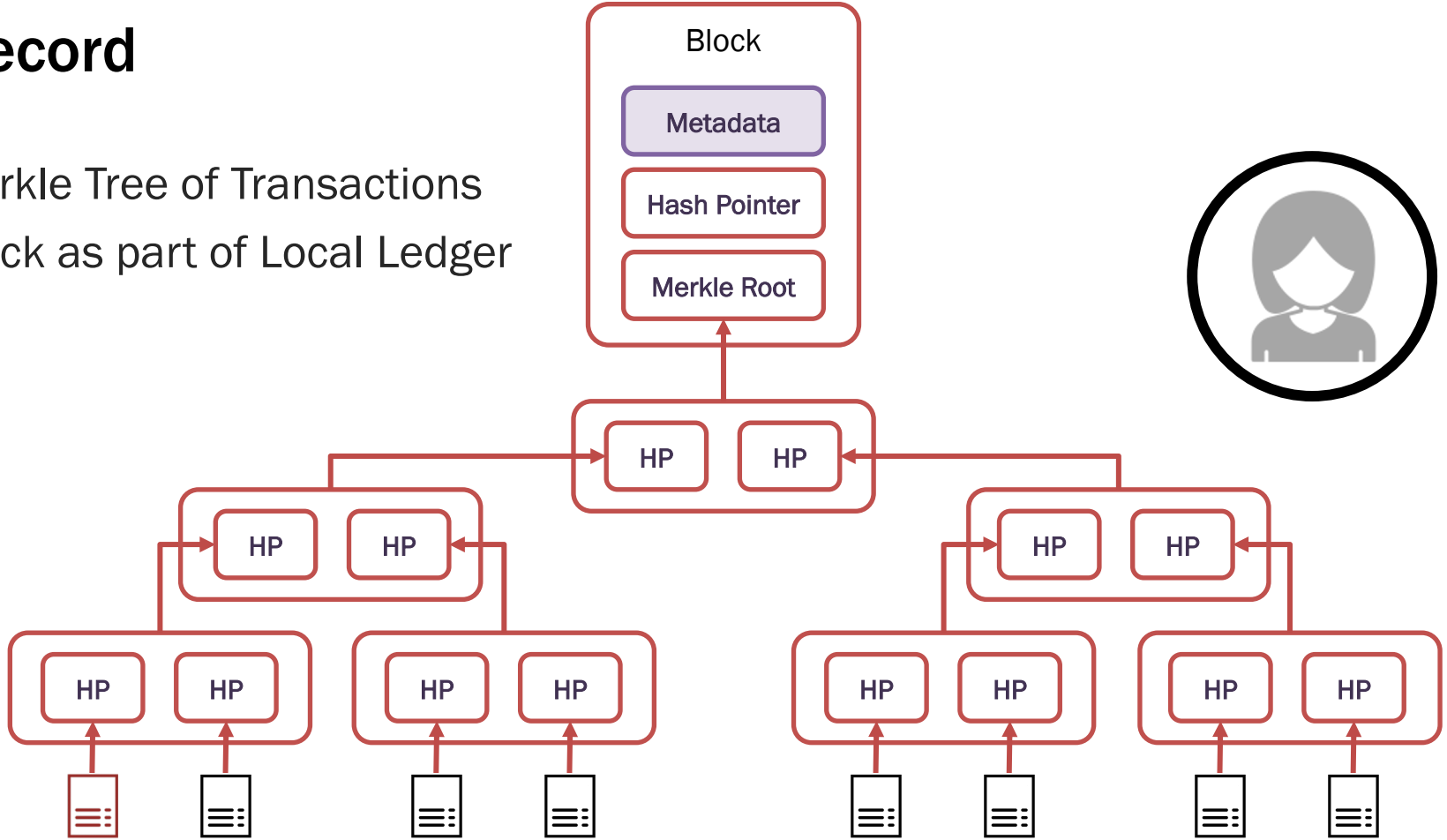
Coinbase Trans.



Record

Merkle Tree of Transactions

Block as part of Local Ledger



Mining

Record in the Global Ledger