Bitcoin Script

Thierry Sans

The language

Input and Output addresses are actually scripts

- Stack based language (simplistic)
- Cryptography primitives
- No loop (no halting problem)

See all instructions
https://wiki.bitcoinsv.io/index.php/Opcodes_used_in_Bitcoin_Script

The mechanics

`scriptPubKey` (transaction output)

the locking script that specified the condition that needs to be fulfilled to use the UTXO

`scriptSig` (transaction input)

the unlocking script (transaction input) provided by the user who wants to use the UTXO

Op Codes

Op Code	Description
`OP_CHECKSIG`	Takes (i.e pull) public key and signature and returns (i.e push) **`TRUE`** or **`FALSE`** if the signature match
`OP_DUP`	Duplicates the element at the top of the stack
`OP_EQUAL`	Takes two inputs and returns **`TRUE`** or **`FALSE`** if the two values are equal
`OP_VERIFY`	Marks the transaction as valid if the top of the stack is **`TRUE`**
`OP_EQUALVERIFY`	Same as **`OP_EQUAL`** combine with **`OP_VERIFY`**
`OP_CHECKMULTISIG`	Similar to **`OP_CHECKSIG`** but checking multiple in a row
`OP_HASH256`	Takes an input and returns it hash
`OP_MAX`	Takes two values and returns the biggest one

Pay to Public Key Hash (P2PKH)

The payer sends bitcoin to another address

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash?> OP_EQUALVERIFY OP_CHECKSIG
scriptSig:    <sig> <pubKey>
```

✓ The UTXO does not reveal Alice's public key

Null Data

This script is used to store arbitrary data (limit 40 bytes)

```
scriptPubKey: <OP_RETURN> <DATA>
```

Pay to Script Hash (P2SH)

The payer can specify a redeeming script (BIP16)

```
scriptPubKey: OP_HASH160 <redemptionScriptHash> OP_EQUAL
scriptSig:     [<sign>...<sig>] <redeemScript>
```

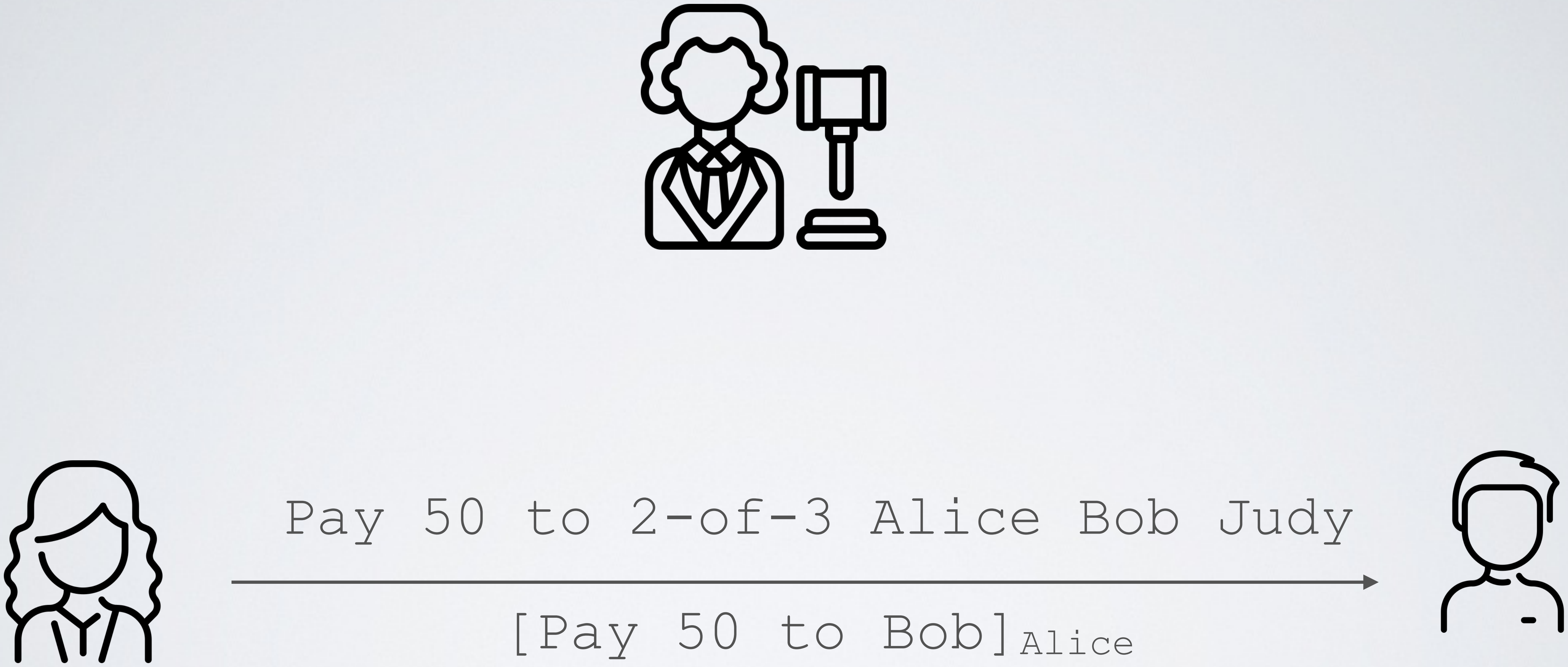
✓ Can specify complex conditions for when UTXO can be spent

Example of P2SH : Multi-Signature

Spending a UTXO requires t-out-of-n signatures

```
scriptPubKey: <m> <pubKey> [<pubKey> ... ] <n> <OP_CHECKMULISIG>
scriptSig:    <sig> [<sig>...<sig>] <redeemScript>
```

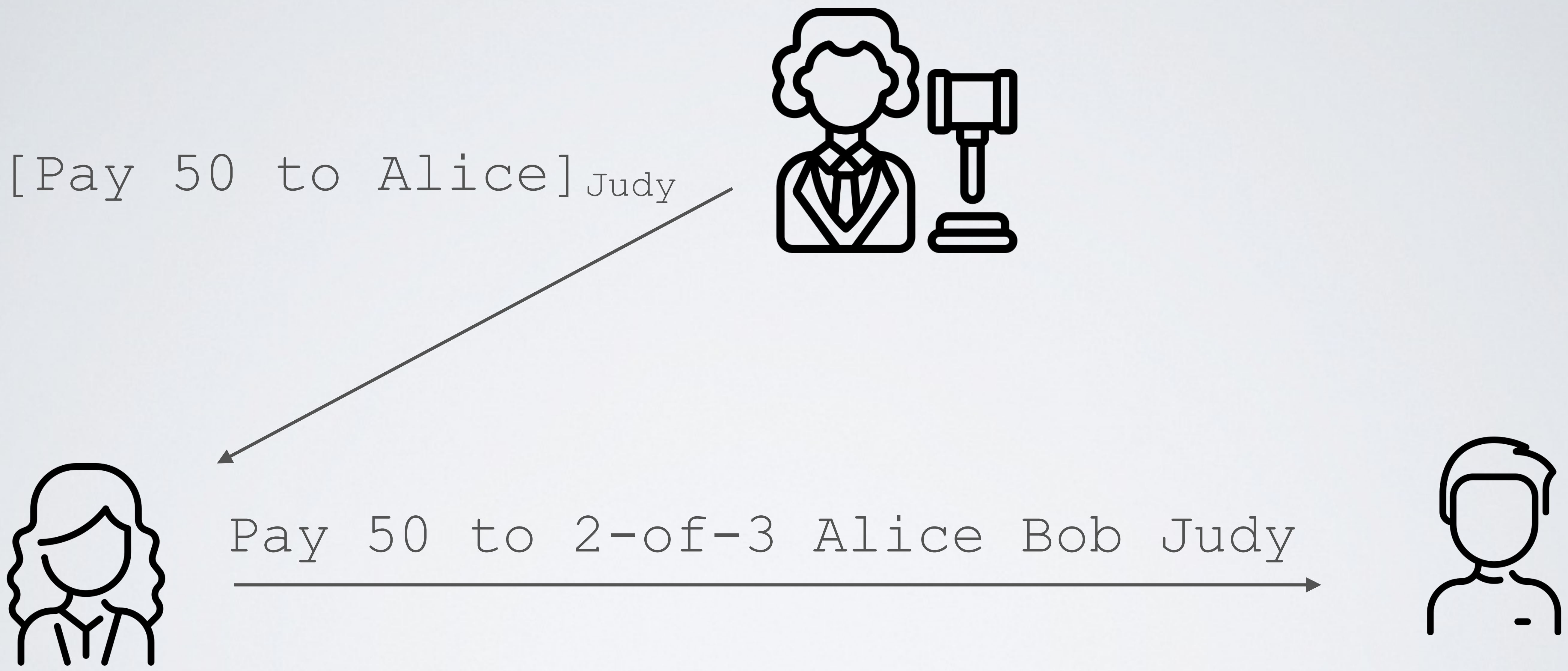
Escrow Transactions



```
Pay 50 to 2-of-3 Alice Bob Judy
```

[Pay 50 to Bob]$_{\texttt{Alice}}$

Escrow dispute


[Pay 50 to Alice]$_{\text{Judy}}$
Pay 50 to 2-of-3 Alice Bob Judy