SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 7:

Bitcoin – Part 2

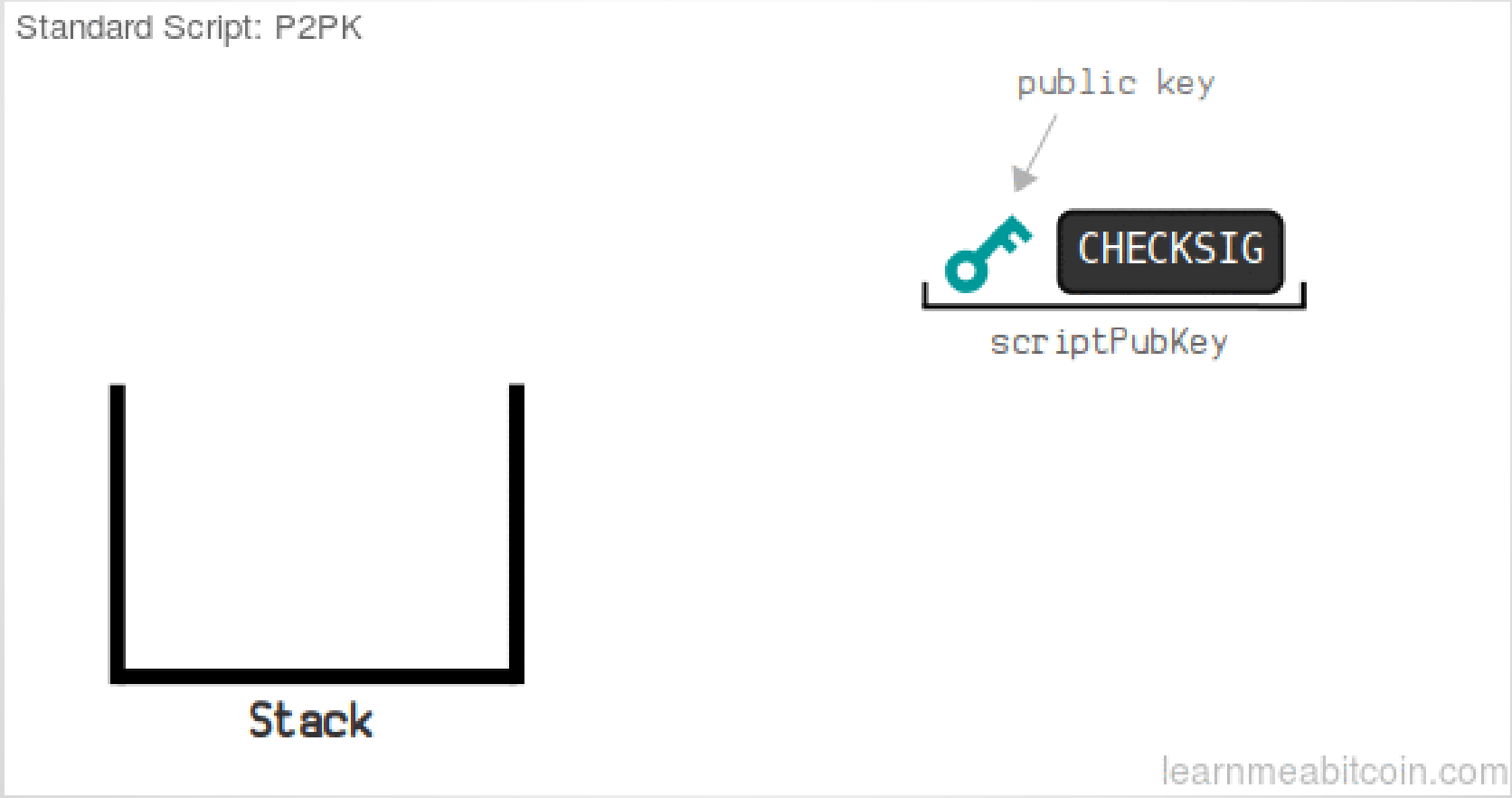
Module 2 – P2PK, P2PKH, P2SH and Multisig Transaction Types

There are Different Bitcoin Transaction Types

- Pay-to-Public Key (P2PK)
- Pay-to-Public-Key-Hash (P2PKH)
- Multisig Transactions
- Pay-to-Script-Hash (P2SH)
- Pay-to-Witness-Public-Key-Hash (P2WPKH)
- Pay-to-Witness-Script-Hash (P2WSH)
- OP_RETURN Transactions

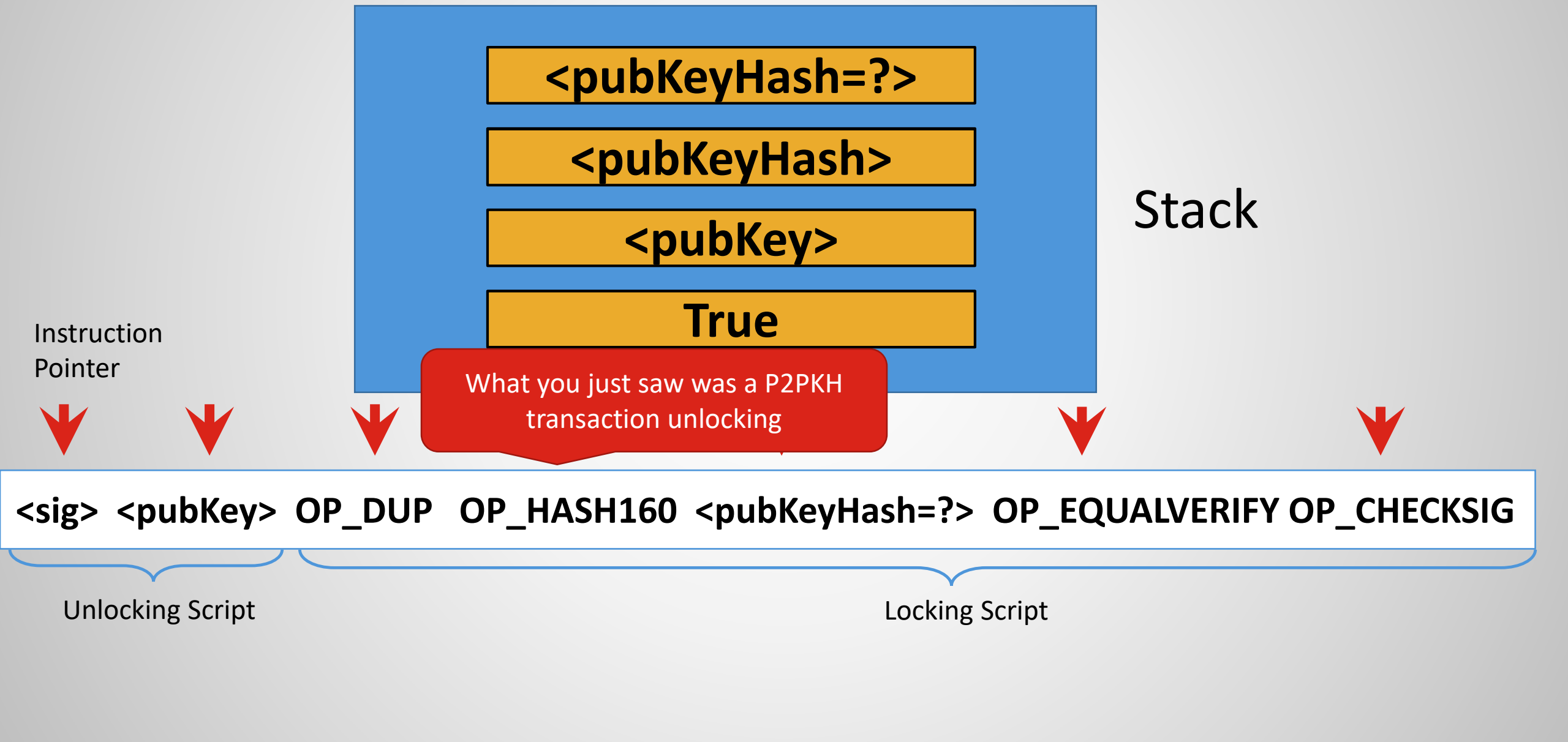
Pay to Public Key (P2PK) Transaction Type

Locking Script: <public key> CHECKSIG
Unlocking Script: <signature>



(Greg Walker, from learnmeabitcoin.com)

Recall: Bitcoin Language Stack in a Spending Transaction



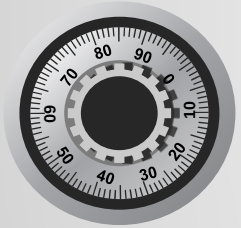
```
{
   "txid": "a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d",
   "version": 1,
   "size": 23620,
   "vsize": 23620,
   "weight": 94480,
   "locktime": 0,
   "vin": [
      {
         "txid": "867da54b0fd0a9429d30471af3fcf069e069141fcc544583f3103ac3948f2e0d",
         "vout": 0,
         "scriptSig": {
            "asm":
"3046022100bc57dc26f46fecc1da03272cb2298d8a08b22d865541f5b3a3e862cc87da4b47022100ce1fc72
771d164d608b15065832542a0e9040cfdf28862c5175c81fcb0e0b655[ALL]
0434417dd8d89deaf0f6481c2c160d6de0921624ef7b956f38eef9ed4a64e36877be84b77cdee5a8d92b7d9
3694f89c3011bf1cbdf4fd7d8ca13b58a7bb4ab0804",
},
...
"vout": [
      {
         "value": 10000,
         "n": 0,
         "scriptPubKey": {
            "asm": "OP_DUP OP_HASH160 46af3fb481837fadbb421727f9959c2d32a36829 OP_EQUALVERIFY
OP_CHECKSIG",
            "hex": "76a91446af3fb481837fadbb421727f9959c2d32a3682988ac",
            "address": "17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ",
            "type": "pubkeyhash"
         }
      }
   ]
}
```


The 10,000-BTC pizza was paid for by a P2PKH TX on May 22, 2010

(Laszlo Hanyecz)

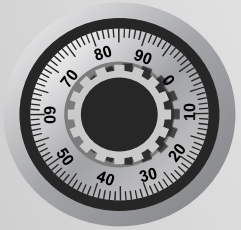
Multisig Transaction Type

- If a transaction is of Multisig type, the output can be unlocked by the joint signature of **k** (out of **n**) people whose public keys have been mentioned in the locking script.



Locking Script

k <public key #1> <public key #2> … <public key #n> **n** CHECKMULTISIG

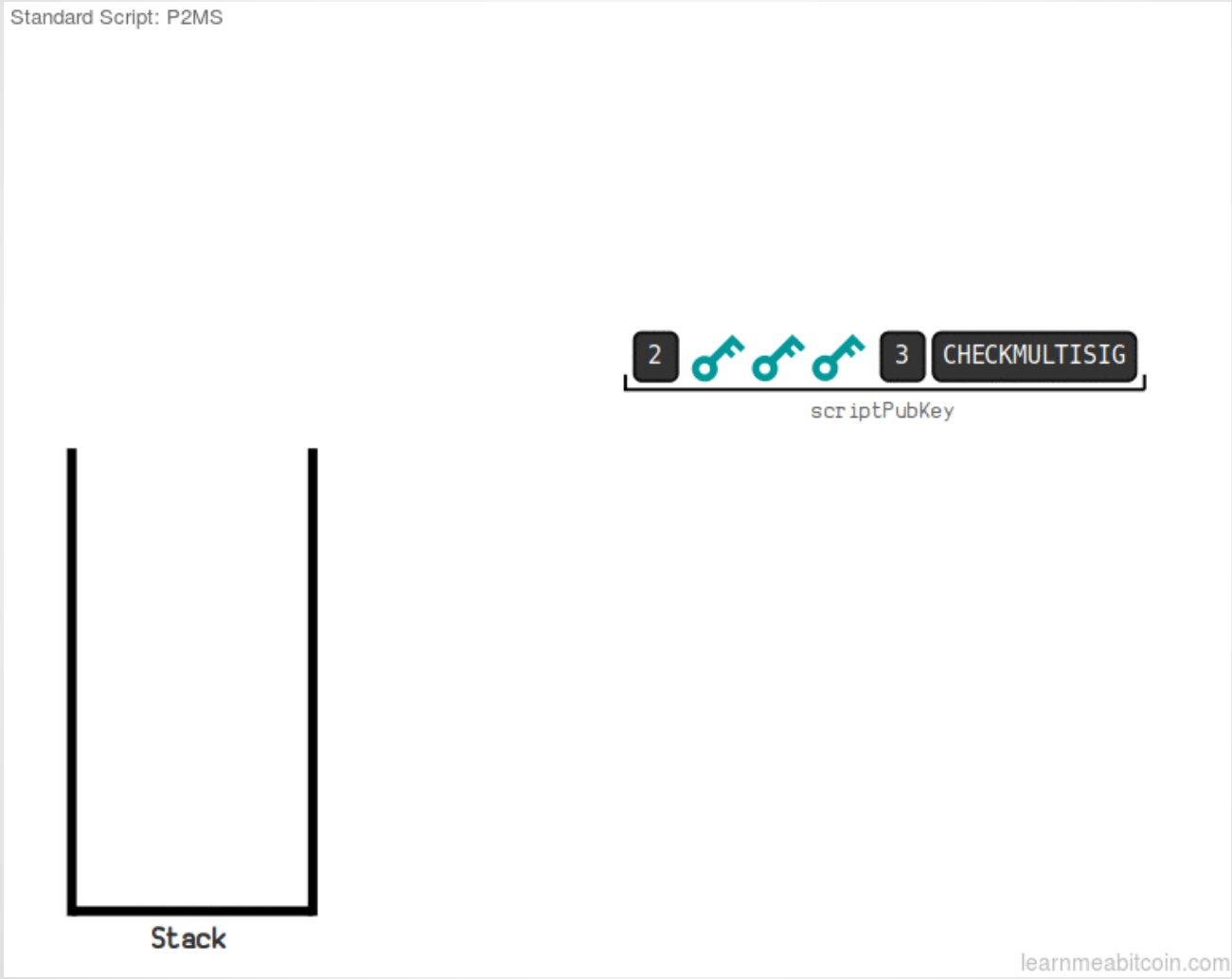


Unlocking Script

<signature x> …. <signature z>

k signatures

Visual Presentation: Unlocking a 2-out of-3 Multisig Transaction



(Greg Walker, from learnmeabitcoin.com)

Multisig Stats

- Pay to Multisig transactions are rare (<<1%, mostly 2-of-2 or 2-of-3).
  - “Pay to Scripthash” has replaced “Pay to Multisig”.
  - The first Multisig transaction issues on Jan 30, 2012

    (TXID: 60a20bd93aa49ab4b28d514ec10b06e1829ce6818ec06cd3aabd013ebcdc4bb1)

Real Example:

TXID: 581d30e2a73a2db683ac2f15d53590bd0cd72de52555c2722d9d6a78e9fea510


```
...
   "vout": [
      {
         "value": 0.0169,
         "n": 0,
         "scriptPubKey": {
            "asm": "2 04d81fd577272bbe73308c93009eec5dc9fc319fc1ee2e7066e17220a5d47a18314578be2faea34b9f1f8ca078f8621acd4bc22897b03daa422b9bf56646b342a2
04ec3afff0b2b66e8152e9018fe3be3fc92b30bf886b3487a525997d00fd9da2d012dce5d5275854adc3106572a5d1e12d4211b228429f5a7b2f7ba92eb0475bb1
04b49b496684b02855bc32f5daefa2e2e406db4418f3b86bca5195600951c7d918cdbe5e6d3736ec2abf2dd7610995c3086976b2c0c7b4e459d10b34a316d5a5e7 3 OP_CHECKMULTISIG",
            "hex":
"524104d81fd577272bbe73308c93009eec5dc9fc319fc1ee2e7066e17220a5d47a18314578be2faea34b9f1f8ca078f8621acd4bc22897b03daa422b9bf56646b342a24104ec3afff0b2b66e8152
e9018fe3be3fc92b30bf886b3487a525997d00fd9da2d012dce5d5275854adc3106572a5d1e12d4211b228429f5a7b2f7ba92eb0475bb14104b49b496684b02855bc32f5daefa2e2e406db4418f
3b86bca5195600951c7d918cdbe5e6d3736ec2abf2dd7610995c3086976b2c0c7b4e459d10b34a316d5a5e753ae",
            "type": "multisig"
         }
....
```

The Problem with Multisig

? But this means longer TXs for me and more TX fees.

I want to buy cloths

We only support 2-out of-3 multisig TXs

The Generation of Pay to Script Hash (P2SH)

- P2SH was introduced as a standard in **April 2012.**
- The idea was to specify a redemption script as the output and pay to an script instead of multiple public keys.
- The script is defined by the merchant, and its hash is used in the TX output created by the customer.
  - The customer pays the money to the hash of a script, whose size is fixed and small.

Steps Taken in a P2SH Lifecyle (A→ B→ C)

Merchant (B):

1. **Makes a redemption script (with the Bitcoin instruction set),**
2. **Calculates the script hash,**
3. **Gives the hash to the customer (A).**

This can support the construction of k-out of-n multisig transactions.

Customer (A):

1. **Makes a P2SH TX in which the output is the merchant's script hash value.**

- The merchant can spend the money (and send it to e.g. **C**) by crafting a transaction that includes the original script and signature.
- Network nodes can hash the script and see it is equal to the ID the money has been sent to by **A**.
  - If the signatures are valid, they accept it as an input to another transaction.

Wait a Minute!

Doesn’t this mean that the same overhead regarding big TXs in Multisig transactions is transferred to the merchant in P2SH?

- Yes, but when the merchant wants to spend the money collected, it creates one transaction with all the inputs received, and only one copy of the script. Including the script happens only once (in contrast to customers’ multiple TXs).

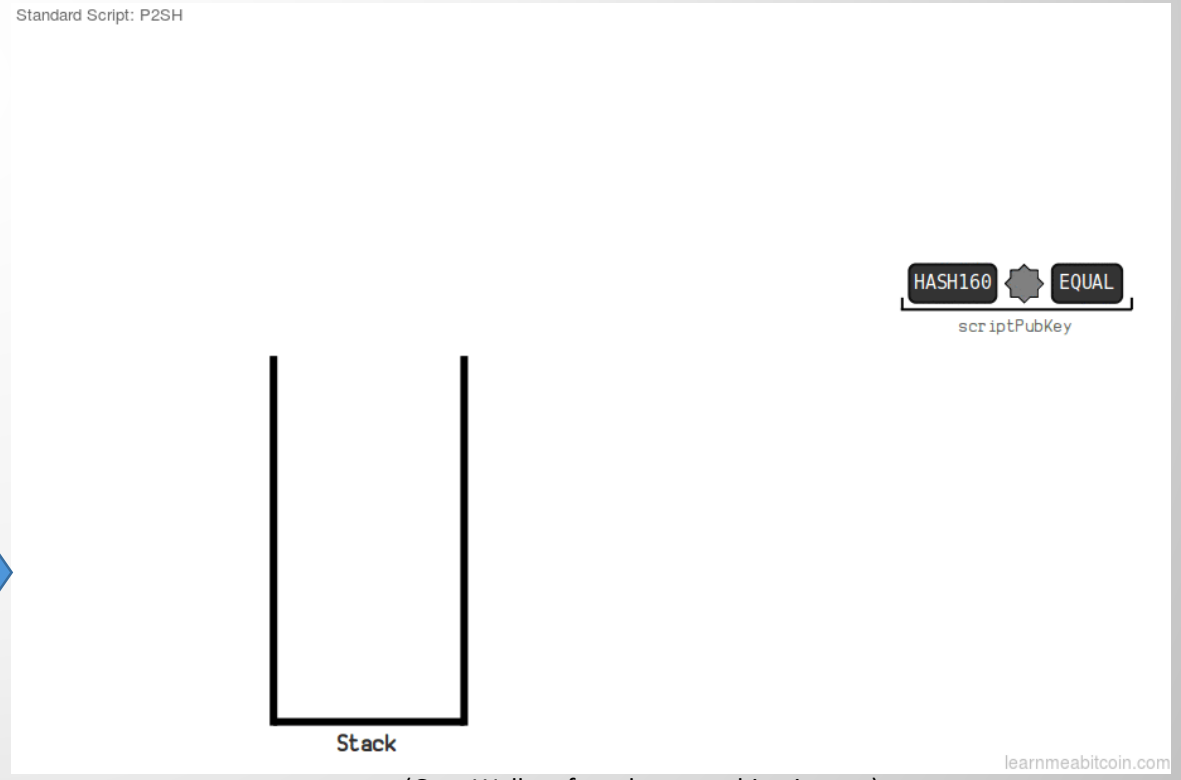
MultiSig

Locking Script:
2 <public key #1> <public key #2> <public key #3> **3** CHECKMULTISIG
Unlocking Script:
<signature x> …. <signature z>

P2SH

Locking Script:
HASH160 <hash of the redeem script> EQUAL
Unlocking Script:
<signature #1> <signature #2> <Redeem Script>

Redeem script = 2 <public key #1> <public key #2> <public key #3> 3 CHECKMULTISIG

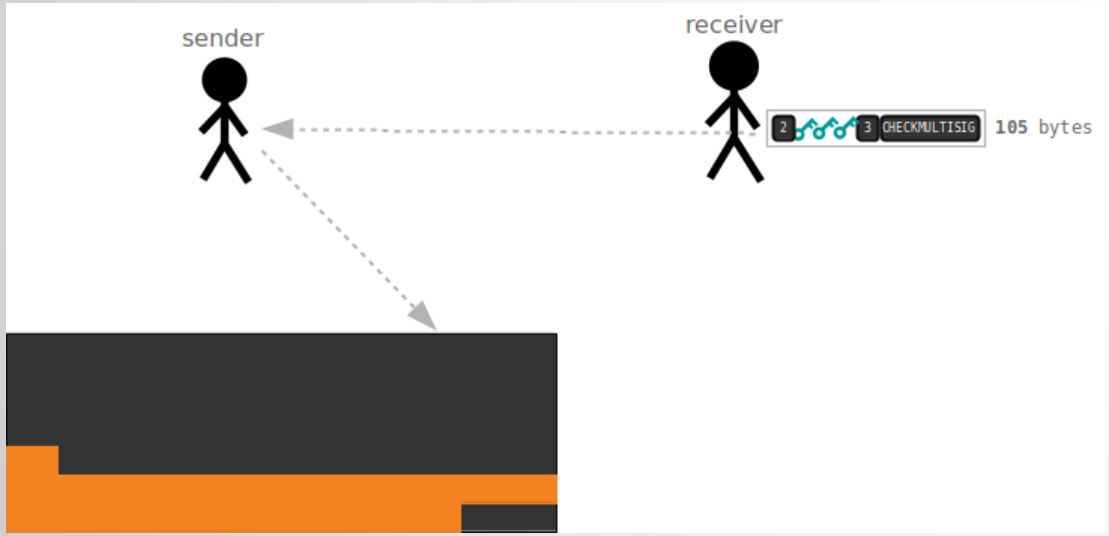


(Greg Walker, from learnmeabitcoin.com)

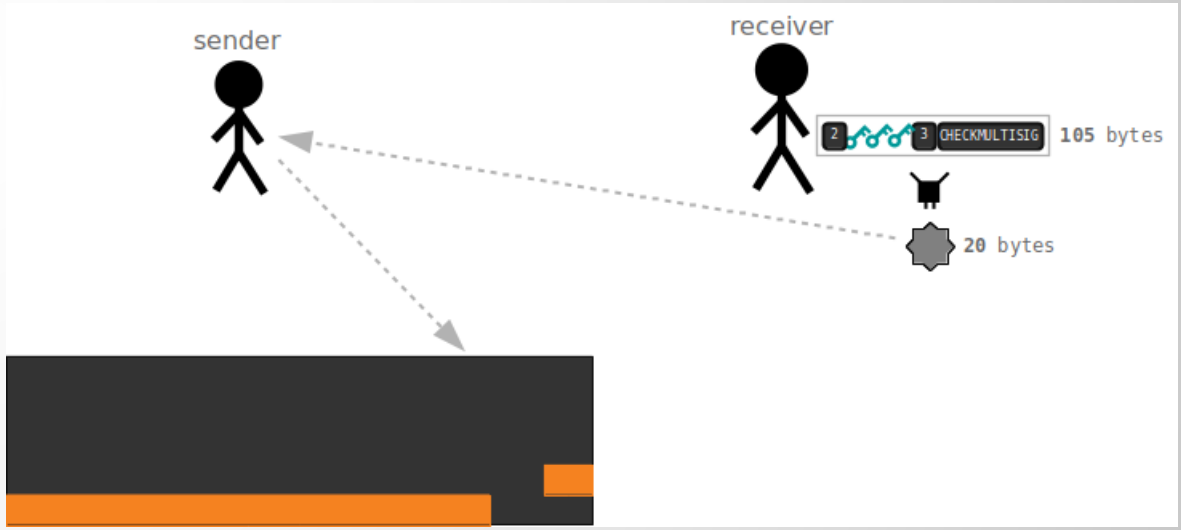
Advantages of P2SH

1. **Cheaper transaction costs for the sender.**

   Larger locking scripts increase the size of the transaction data, so the sender will have to pay more in TX fees to include your script.



vs



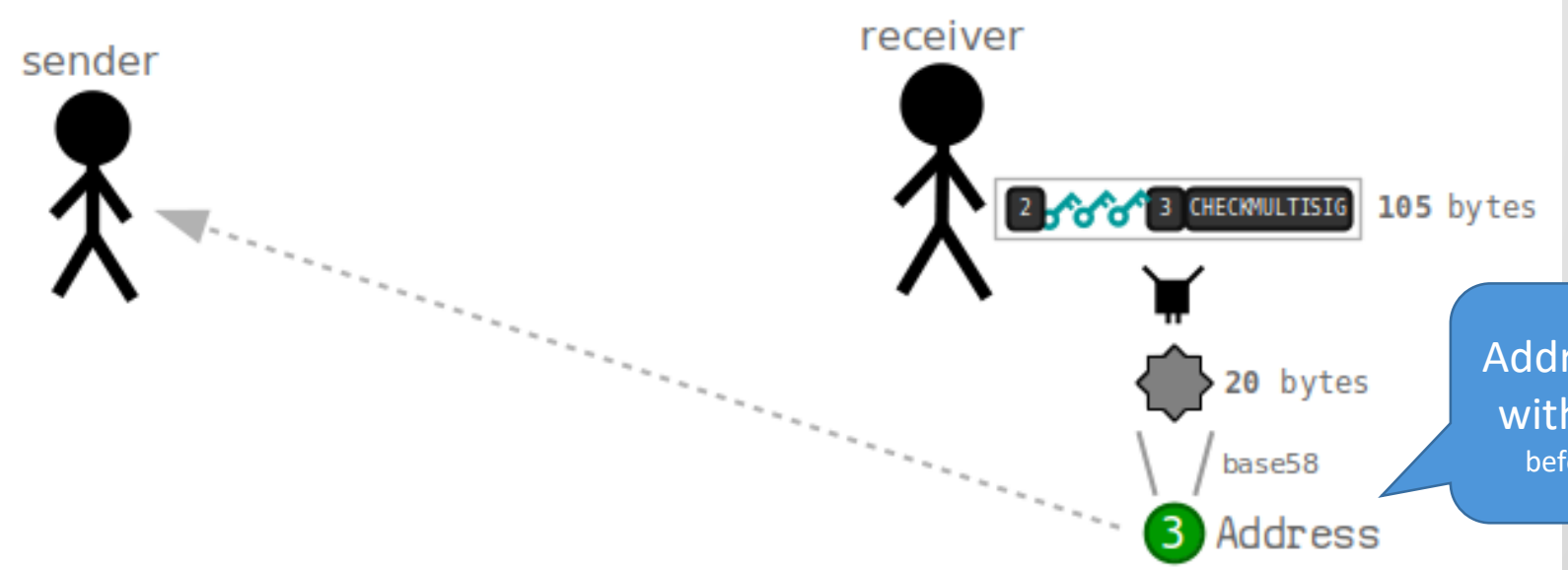
Multisig **P2SH**

(Images from https://learnmeabitcoin.com)

Advantages of P2SH

2. **We can use 160-bit addresses for P2SH locking scripts.**

   Since every P2SH locking script has a fixed structure (thanks to the fixed-size hash, we can have a standard address format for it (similar to the P2PKH address format).

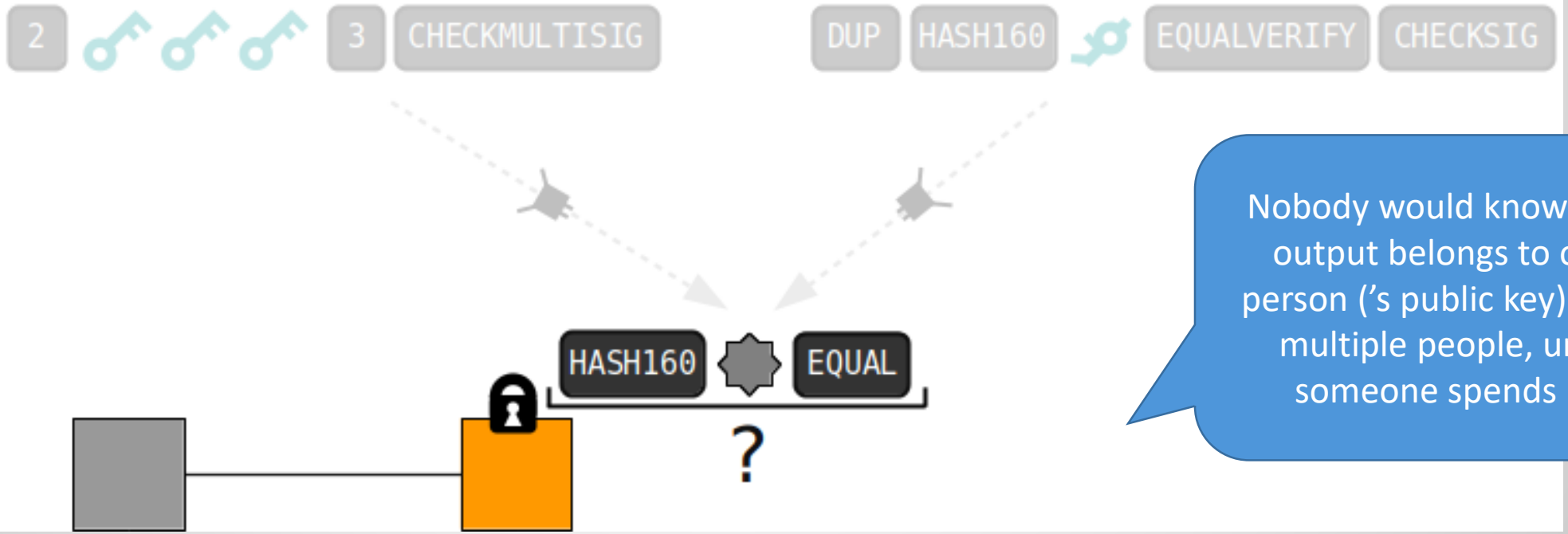


(Image from https://learnmeabitcoin.com)

Advantages of P2SH

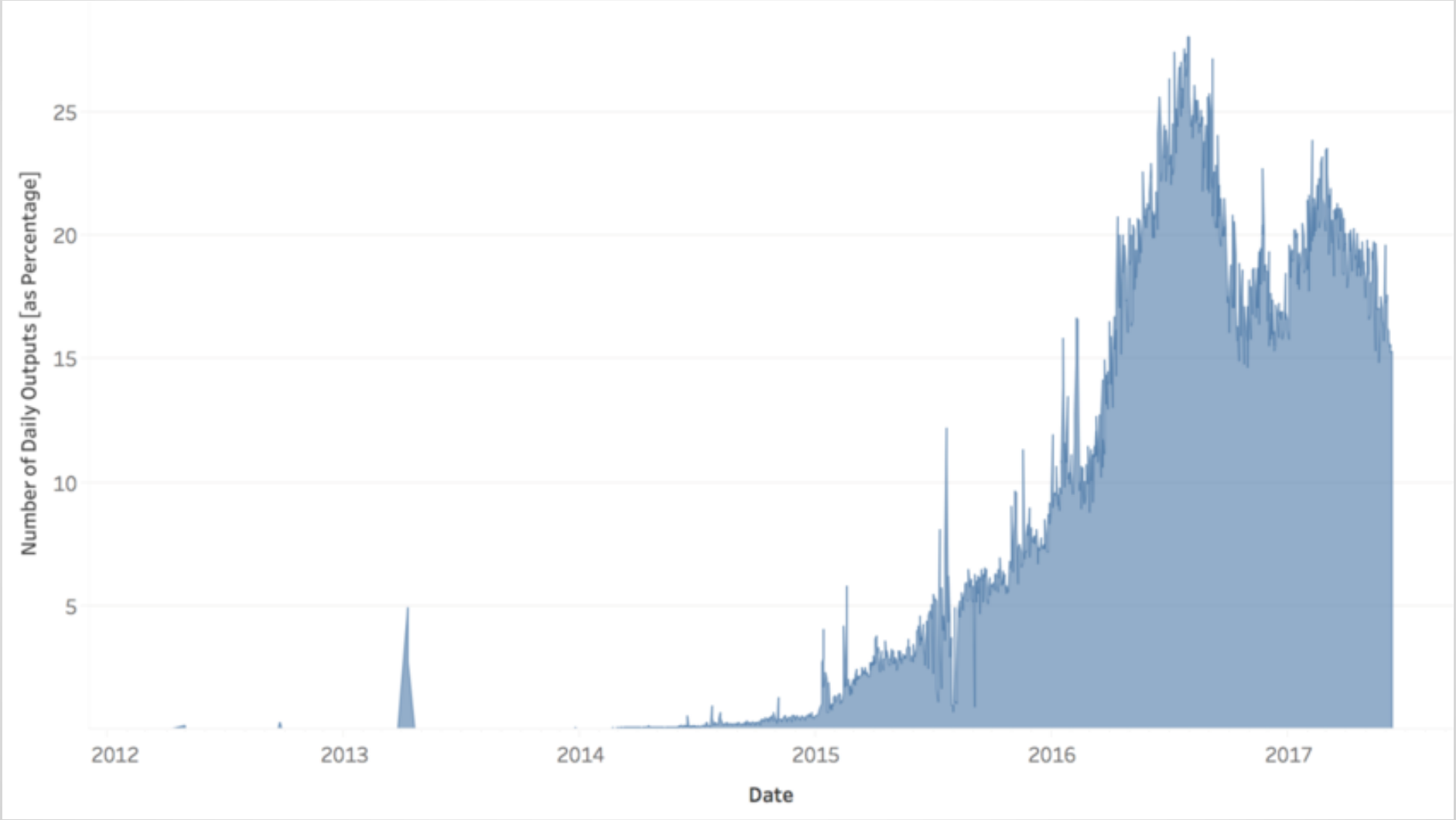
3. P2SH has a little more privacy.

P2SH locking script just contains the hash of the script. It's impossible to know what kind of locking script that hash came from before its redemption.



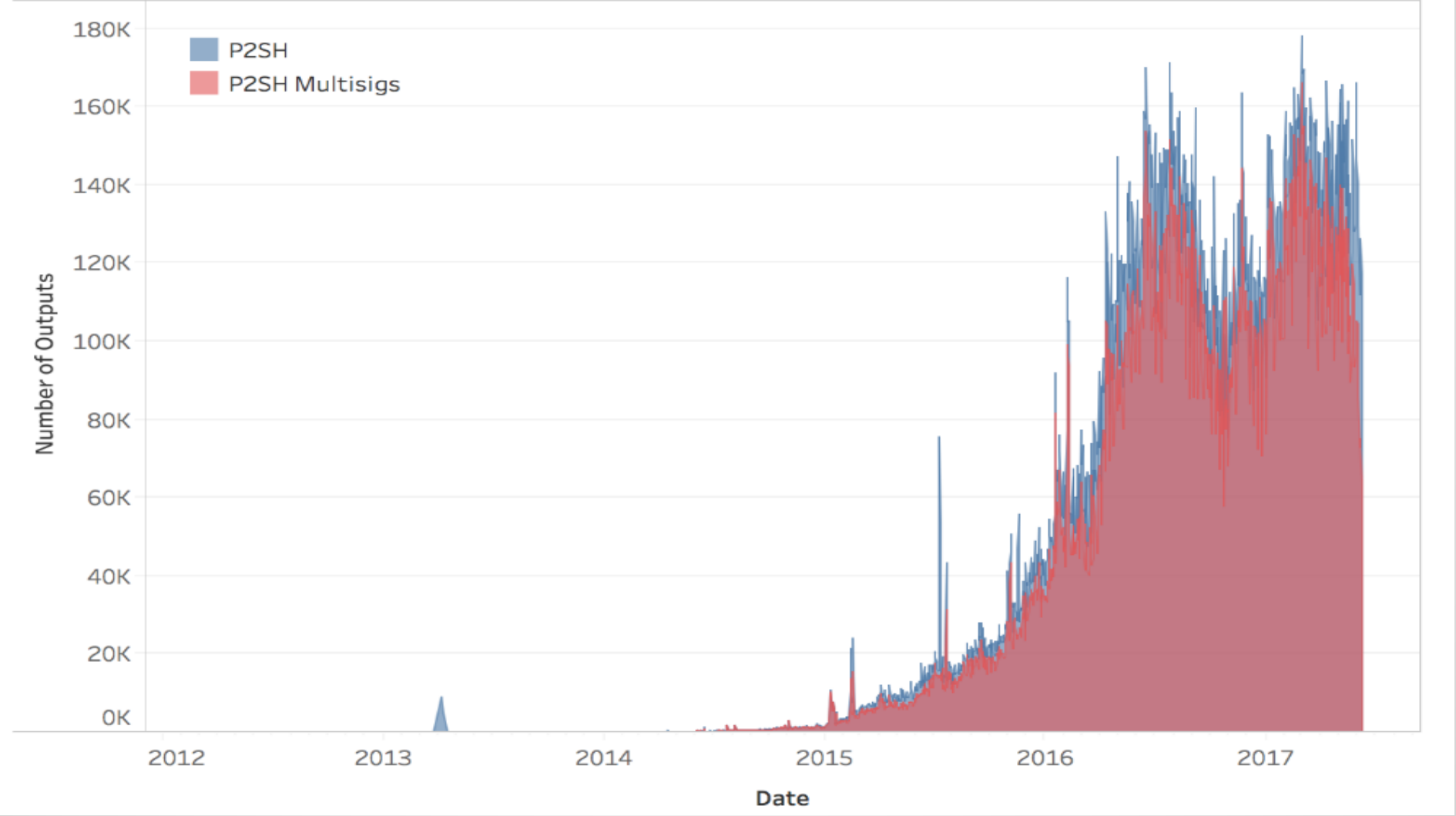
(Image from https://learnmeabitcoin.com)

P2SH TXs over the Time



B. Fabian et al., “Adoption of Security and Privacy Measures in Bitcoin - Stated and Actual Behavior”, SSRN Electronic Journal · May 2018

P2SH TXs over the Time



B. Fabian et al., "Adoption of Security and Privacy Measures in Bitcoin - Stated and Actual Behavior", SSRN Electronic Journal · May 2018

Different Kinds of Bitcoin Addresses

- Addresses starting with a “1”. These are known as Legacy, or P2PKH (Pay-to-pubkey-hash) addresses.
- Addresses starting with a “3”. These are known as P2SH (Pay-to-script-hash) addresses.
- Addresses starting with a “bc1”. These are known as “Native Segwit” or “Bech32”, which we explain later.

What Comes Next …

- We introduced P2PKH, Multisig, and P2SH transactions and mentioned the pros and cons of each.
- We got familiar with the scripts and how they are used in Bitcoin transactions.
- In the next session, we will see some improvements made on top of Bitcoin to make it more efficient.

See you in the next video …