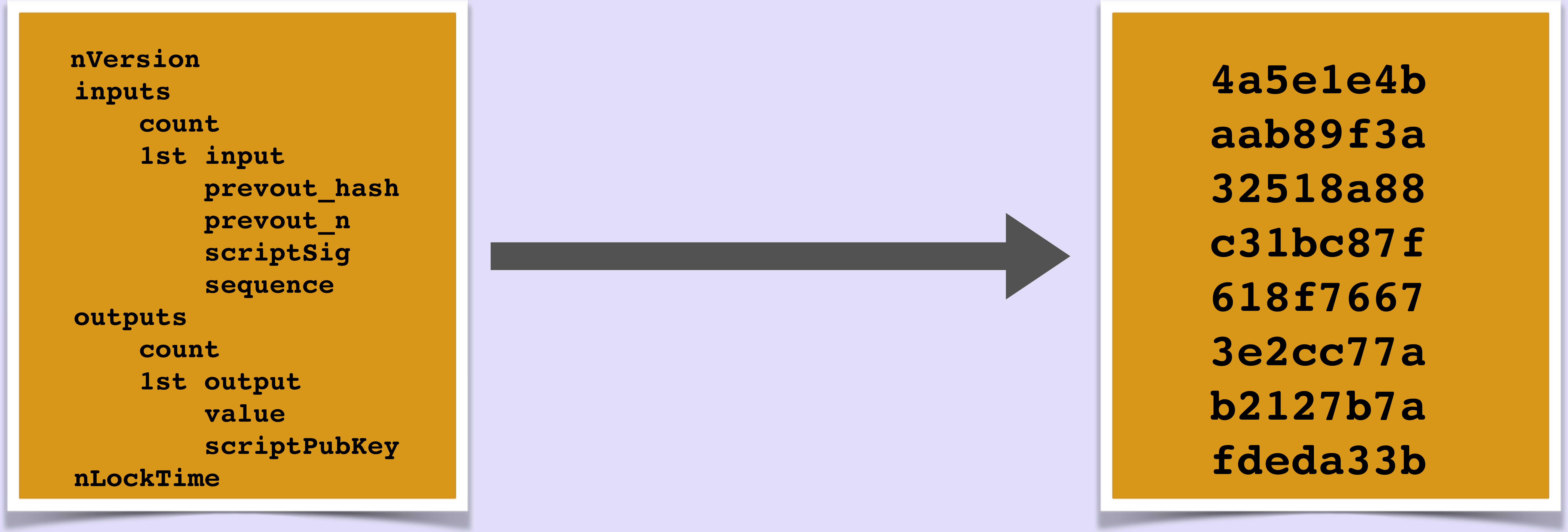
mobilefish.com

BLOCKCHAIN TUTORIAL 27

Bitcoin Raw TX & TXID



```
nVersion
inputs
    count
    1st input
        prevout_hash
        prevout_n
        scriptSig
        sequence
outputs
    count
    1st output
        value
        scriptPubKey
nLockTime
```

```
4a5e1e4b
aab89f3a
32518a88
c31bc87f
618f7667
3e2cc77a
b2127b7a
fdeda33b
```

mobilefish.com

BITCOIN RAW TRANSACTION

- A raw transaction is a way to construct a transaction by specifying the UTXO (which bitcoins to spend) and where to send them.

- This raw transaction can be signed with your private key, and the signed transaction can be broadcasted to the Bitcoin network.

- It is intended for developers or very sophisticated end-users for low-level access to transaction creation and broadcast.

BITCOIN RAW TRANSACTION DEMO

- For the demo, the following 3 links are used:
  - http://www.mobilefish.com/download/cryptocurrency/bitcoin_genesis_raw_tx.txt
  - https://en.bitcoin.it/wiki/Protocol_documentation#tx
  - https://blockchain.info/

BIG ENDIAN VS LITTLE ENDIAN

- Big Endian - Machine stores the most significant bytes first.

A5	23	09	CD	F5	77

- Little Endian - Machine stores the least significant bytes first.

77	F5	CD	09	23	A5

mobilefish.com

SATOSHI

- A Satoshi is the smallest unit of Bitcoin.
- 1 $ = 100 cent
- 1 cent = 0.01 $
- 1 BTC = 100,000,000 satoshi (10^8)
- 1 satoshi = 0.000000001 BTC

BITCOIN TRANSACTION ID

- A transaction id (TXID) or transaction hash is a long string of hexadecimal numbers: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

- A transaction id can be used to look up a transaction on the blockchain.

- Transaction ids are also used to create a Merkle Tree (more about this in a later video)

- A Bitcoin transaction id is always 32 bytes (64 characters) and contains hexadecimal values.

BITCOIN TRANSACTION ID

- To calculate the transaction id of a transaction:
  - Create the raw transaction: raw_tx
  - Convert raw_tx hex string into the corresponding unicode:
    data = raw_tx.decode(“hex”)
  - Apply the sha256 hash function twice:
    hash = sha256(sha256(data))
  - Take the little endian order of the hash:
    hash_little_endian = little_endian(hash)

mobilefish.com

BITCOIN TRANSACTION ID DEMO

- For the demo, the following link is used:
  - http://www.mobilefish.com/download/cryptocurrency/calculate_txid.py.txt