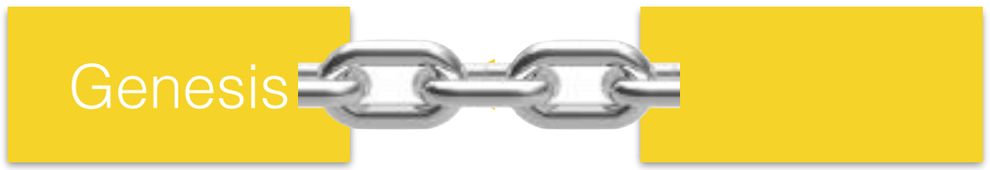
L6

abhi shelat
17f-money

What is a blockchain

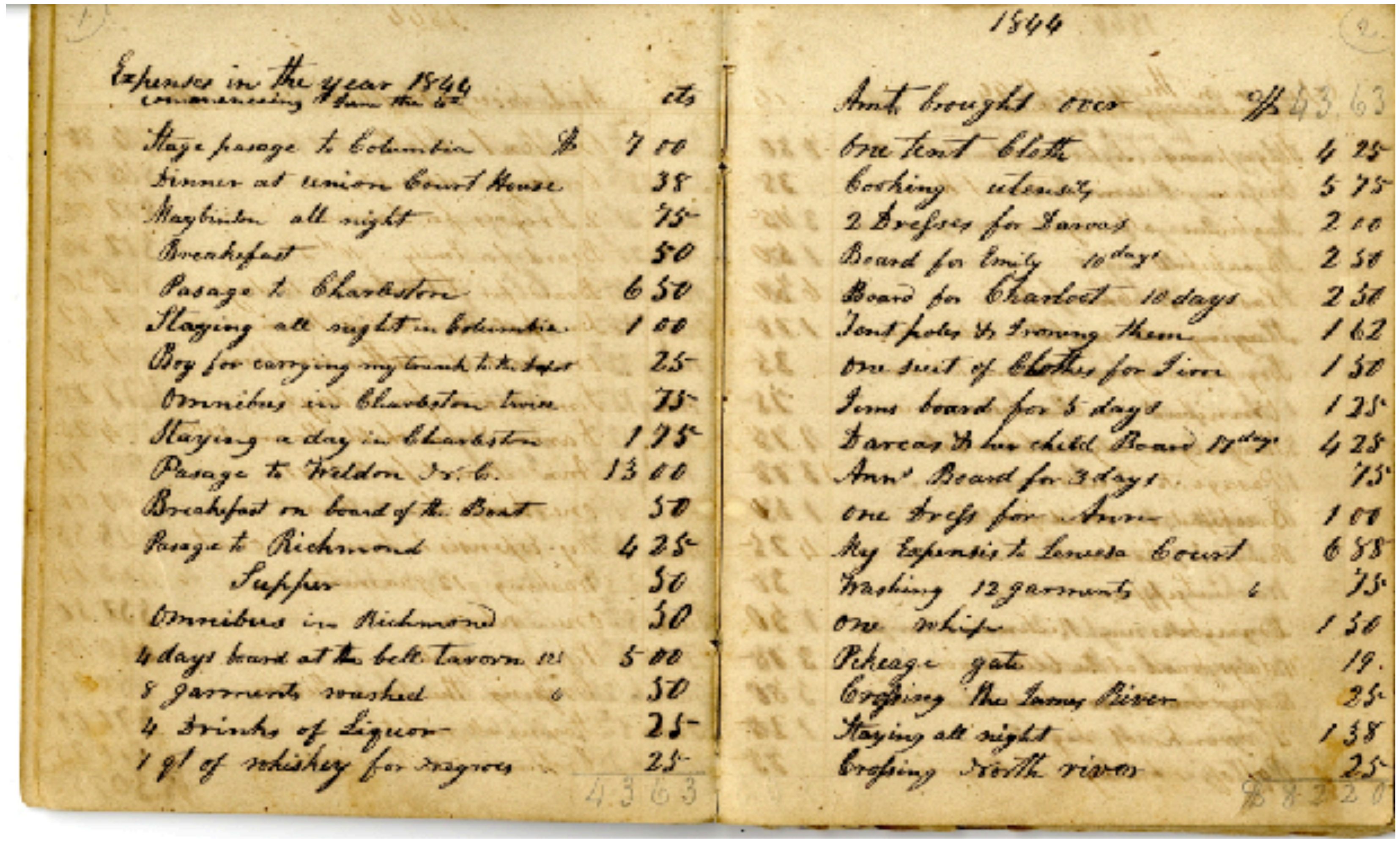
Genesis

What is a blockchain



What is a blockchain

What does it do?

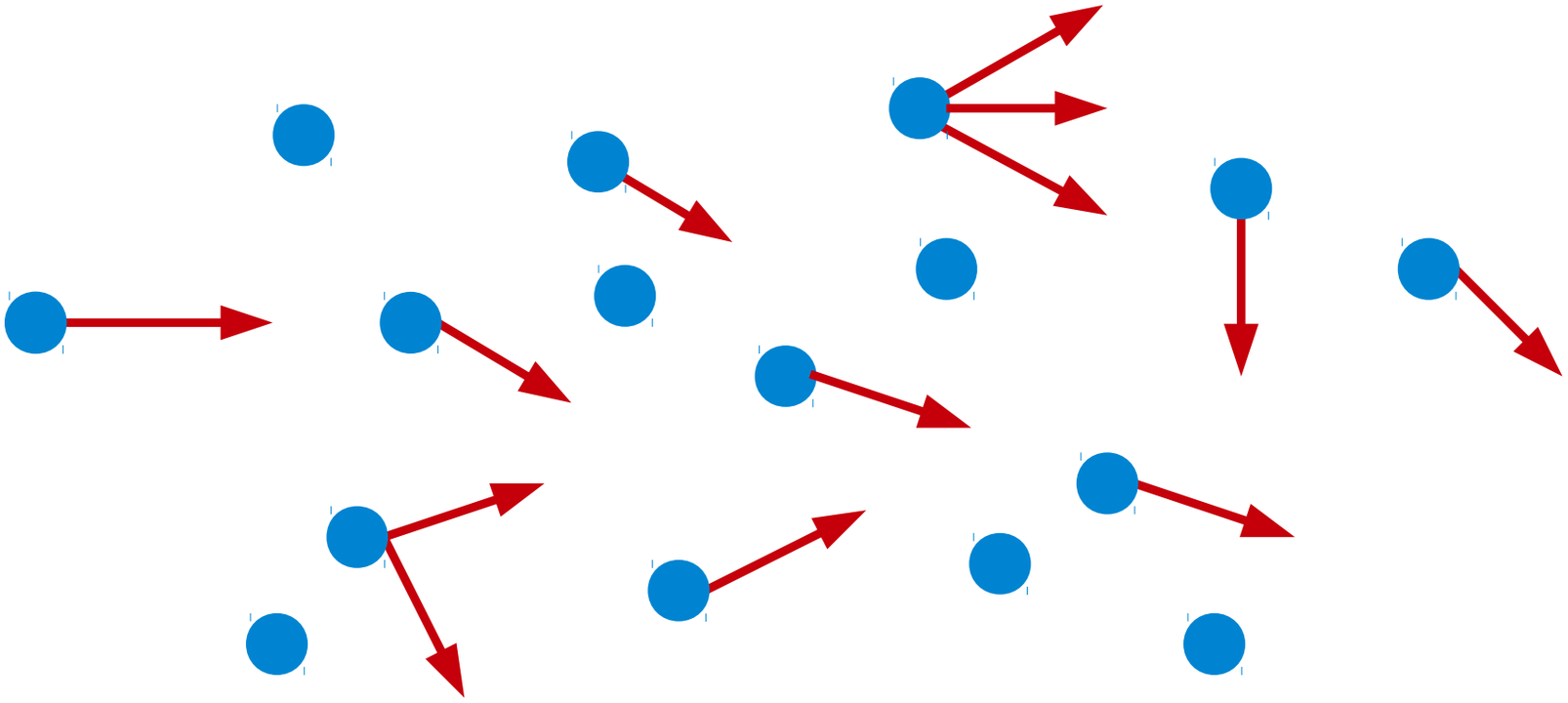


Expenses in the year 1844
commencing from the 6th

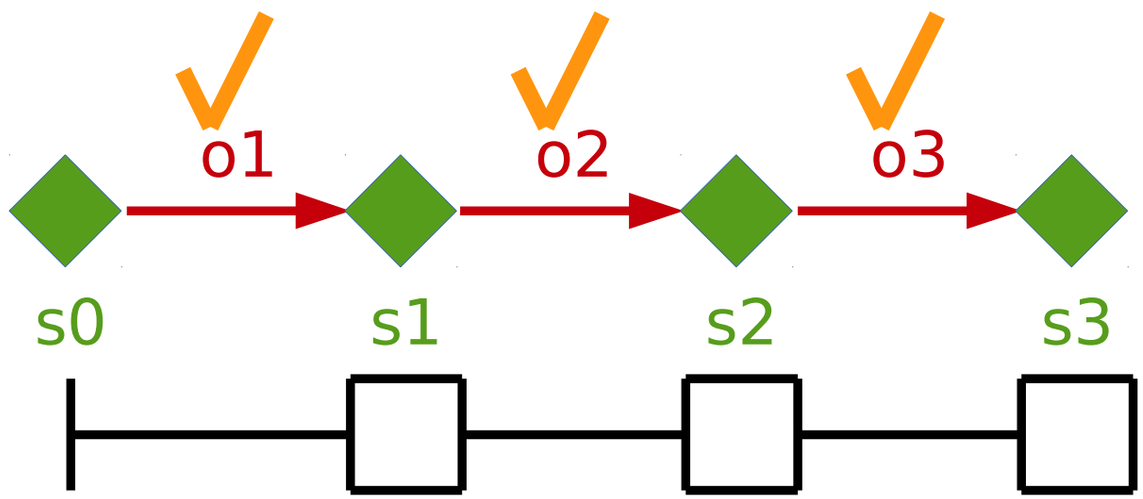
	$	cts
Stage pasage to Columbia	7	00
Dinner at union Court House		38
Staying all night		75
Breakfast		50
Pasage to Charleston	6	50
Staying all night in Columbia	1	00
Boy for carrying my trunk to the depot		25
Omnibus in Charleston twice		75
Staying a day in Charleston	1	75
Pasage to Weldon N. C.	13	00
Breakfast on board of the Boat		50
Pasage to Richmond	4	25
Supper		50
Omnibus in Richmond		50
4 days board at the bell Tavern 125	5	00
8 garments washed 6		50
4 Drinks of Liquor		25
1 qt of whiskey for negroes		25
	43	63

1844

	$	cts
Amt brought over	43	63
One tent Cloth	4	25
Cooking utensils	5	75
2 Dresses for Darcas	2	00
Board for Emily 10 days	2	50
Board for Charlott 10 days	2	50
Tent poles & Ironing them	1	62
One suit of Clothes for Jim	1	50
Jims board for 5 days	1	25
Darcas & her child Board 17 days	4	25
Ann's Board for 3 days		75
One Dress for Ann	1	00
My Expenses to Laneesta Court	6	88
Washing 12 garments 6		75
One whip	1	50
Pikeage gate		19
Crossing the James River		25
Staying all night	1	38
Crossing North river		25
	88	20



Nodes
produce
transactions



Nodes
Run a protocol to construct the public ledger

Slide from Christian Cachin.

Height	Age	Relayed By
382148	4 minutes	BTCC Pool
382147	6 minutes	Eligius
382146	10 minutes	KnCMiner
382145	20 minutes	F2Pool
382144	40 minutes	BitFury
382143	42 minutes	BTCC Pool

Latest Transactions	
c42b3e34126db1e65e37e9413...	0.4106 BTC
ae328c6591f5054f4676df95d...	0.02970983 BTC
0b6e60fc852b43d48e57e68fe...	0.5613794 BTC

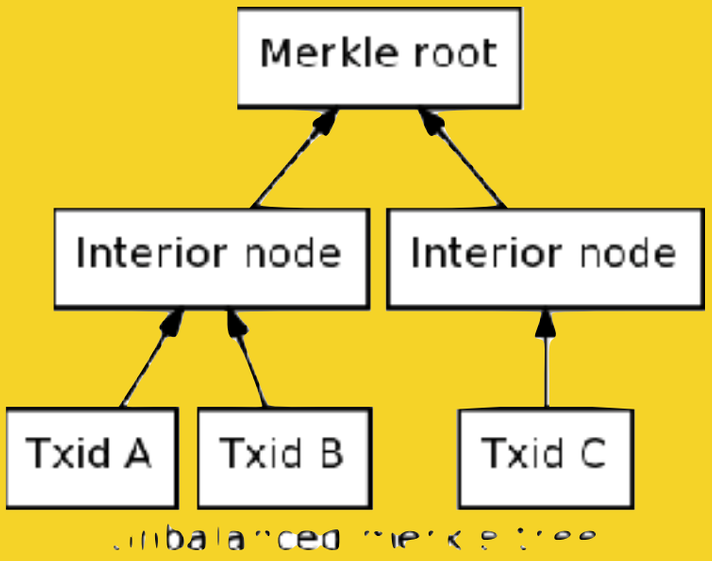
Height	Age	Relayed By
382148	4 minutes	BTCC Pool
382147	6 minutes	Eligius
382146	10 minutes	KnCMiner
382145	20 minutes	F2Pool
382144	40 minutes	BitFury
382143	42 minutes	BTCC Pool

Latest Transactions	
c42b3e34126db1e65e37e9413...	0.4106 BTC
ae328c6591f5054f4676df95d...	0.02970983 BTC
0b6e60fc852b43d48e57e68fe...	0.5613794 BTC

Blockchain datastructure

Blockchain datastructure

4	Version
32	previousBlockHash
32	MerkleRoot of Transactions
4	Time
4	Bits
4	Nonce



4 Version

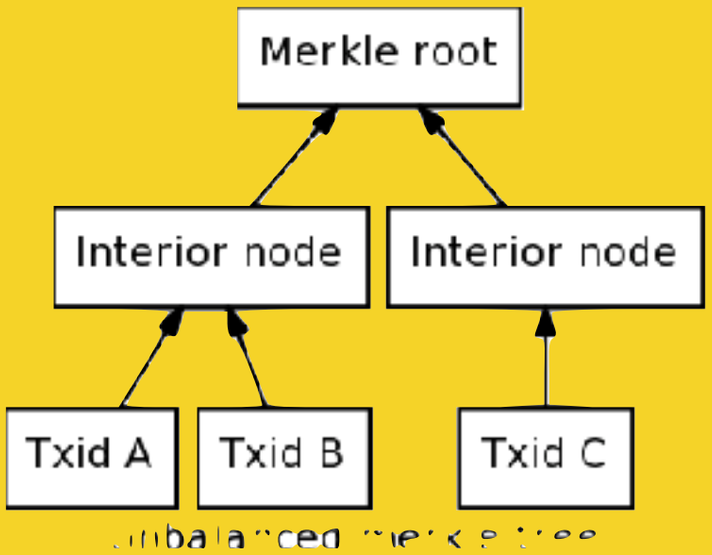
32 previousBlockHash

32 MerkleRoot of Transactions

4 Time

4 Bits

4 Nonce



Each block is named by:

SHA256(SHA256(Vers || Prev || Merkle || Time || Bits || Nonce)

4 Version

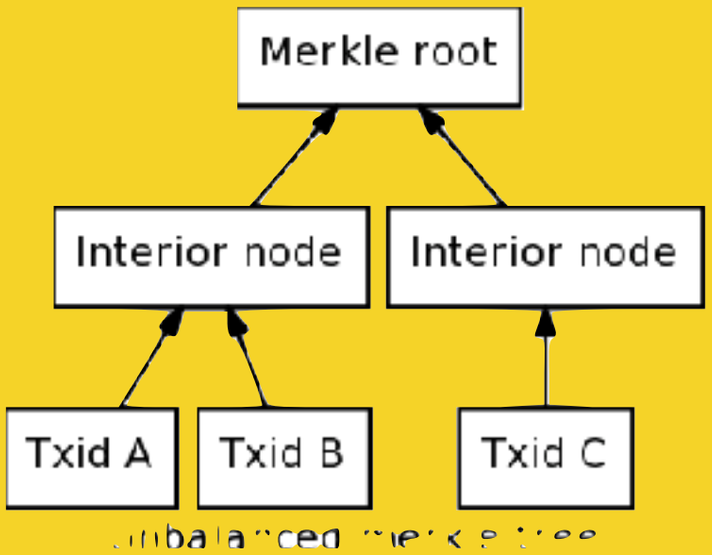
32 previousBlockHash

32 MerkleRoot of Transactions

4 Time

4 Bits

4 Nonce

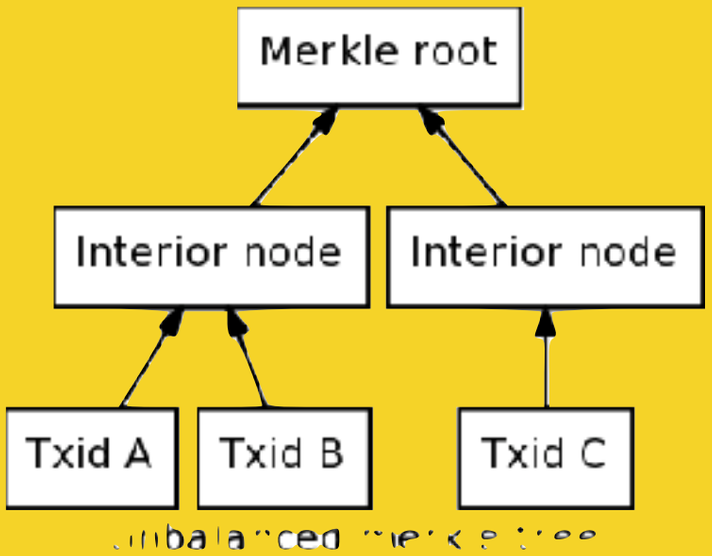


Each block is named by:

SHA256(SHA256(Vers || Prev || Merkle || Time || Bits || Nonce)

Only blocks with Name < D_{time} are valid.

4	Version
32	previousBlockHash
32	MerkleRoot of Transactions
4	Time
4	Bits
4	Nonce



Transactions can be any ledger entry.

In Bitcoin, they represent transfers of coin assets.

Block #443888

Summary	
Number Of Transactions	444
Output Total	424.3016726 BTC
Estimated Transaction Volume	85.74330564 BTC
Transaction Fees	0.16513254 BTC
Height	443888 (Main Chain)
Timestamp	2016-12-17 20:29:03
Received Time	2016-12-17 20:29:03
Relayed By	SlushPool
Difficulty	310,153,855,703.43
Bits	402885509
Size	238.131 kB
Weight	952.272 kWU
Version	0x20000002
Nonce	777617094
Block Reward	12.5 BTC

Hashes	
Hash	000000000000000000cdc0d2a9b33c2d4b34b4d4fa8920f074338d0dc1164dc
Previous Block	0000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214
Next Block(s)	000000000000000002cc08d842aa0156b466c300a7bd756448d22ec337d4692c
Merkle Root	87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

What is a hash function?

goal of a hash function

many bits

hash function *h*

fewer bits

a hash function is a function

$$h : \{0,1\}^d \longrightarrow \{0,1\}^r$$

such that *h* is easy to evaluate and $r < d$

useful in data structures

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785
```

collisions should be rare

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}


abhi$ java test HHHHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785

abhi$ java test “hello world”
1794106052
```

java hash function

$$h(s) = \sum_{i=0}^{n} s[i]31^{n-i}$$

java hash function

$$h(s) = \sum_{i=0}^{n} s[i]31^{n-i}$$

it is thus easy to find a pair s_1, s_2 such that $h(s_1) = h(s_2)$

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}

abhi$ java test HHHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785
```

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}

abhi$ java test HHHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785

abhi$ java test HHHHHHHHHHHHHHHHHHHHHGGGCc
-1644493785
```

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHHGGGCc
-1644493785
```

‘D’ - ‘c’ + 31(‘D’-‘C’) = 0

hashing is also important for cryptographic applications

finding a collision should be intractable

definition

in addition to being easy to compute,
it should be “hard” for an adversary
to find a hash collision, i.e. two different
strings s1, s2 such that

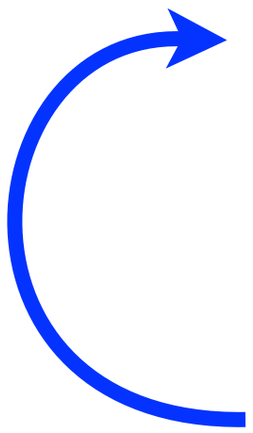
$$h(s1) = h(s2)$$

general attacks

$$H_n = \{h_i : \{0,1\}^d \to \{0,1\}^n\}_{i \in I, n}$$

general attacks

$$H_n = \{h_i : \{0,1\}^d \to \{0,1\}^n\}_{i \in I, n}$$

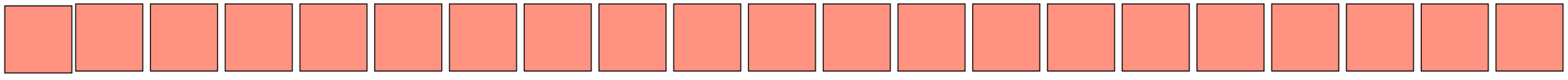


pick a pair *x*,*y* from domain

if $h(x)=h(y)$ and $x \neq y$ output (x,y)

else repeat

domain of size *d*



range of size *r*

md4 1990

md5 1992

sha1 1994

sha256 2005

md4	1990	128 bit
md5	1992	128 bit
sha1	1994	160 bit
sha256	2005	256 bit

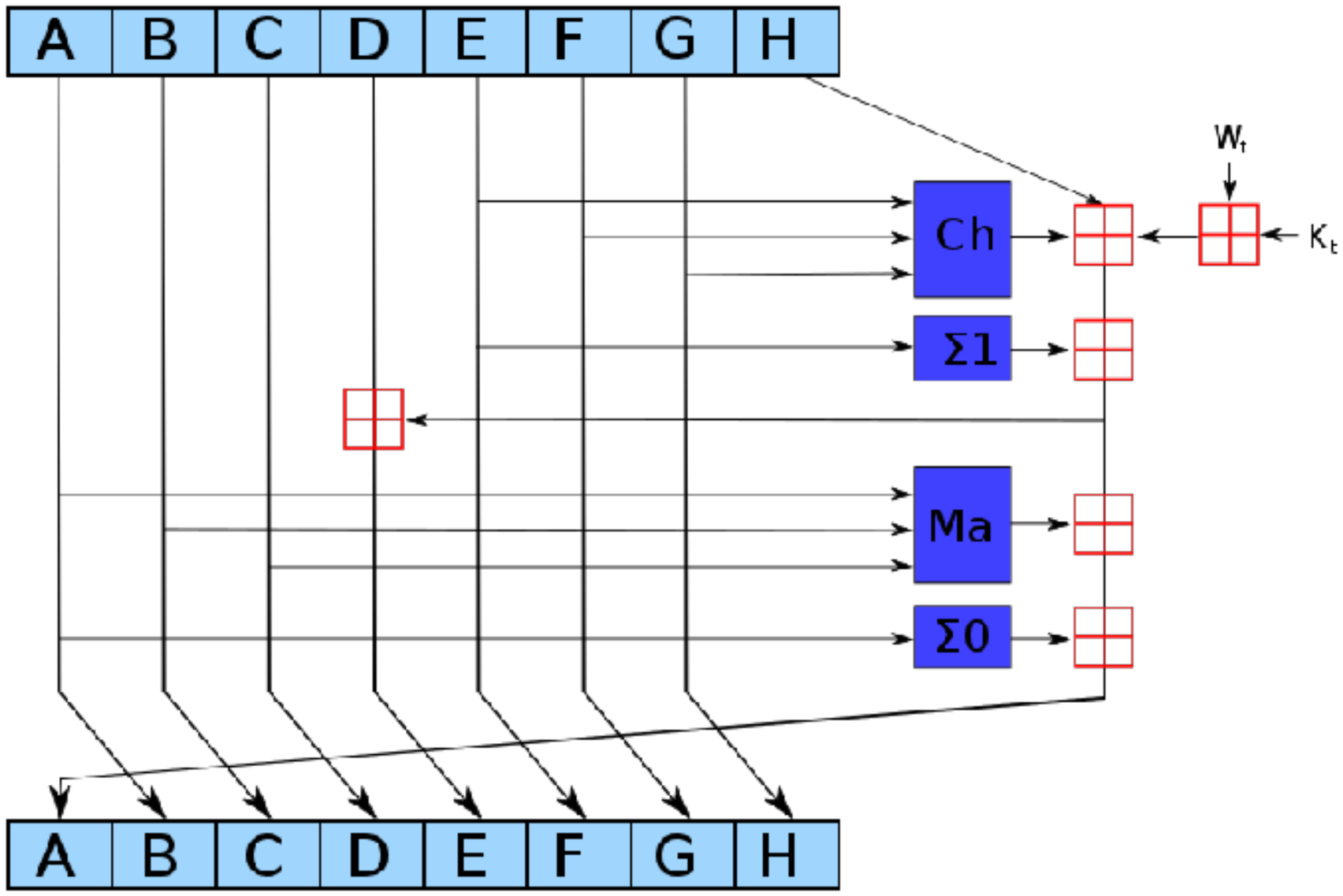
md4	1990	128 bit	1995
md5	1992	128 bit	1998
sha1	1994	160 bit	2005*
sha256	2005	256 bit	

512 bits

Sha256

256 bits

Sha256



Examples

```
ab2017:17f-money$ shasum -a 256 README.md
6e7407cea997f98b6962a4ac3a2b15fb703209dc74b0ce
cb566d59bd7a6ba813  README.md
```

Block #443888

Summary	
Number Of Transactions	444
Output Total	424.3016726 BTC
Estimated Transaction Volume	85.74330564 BTC
Transaction Fees	0.16513254 BTC
Height	443888 (Main Chain)
Timestamp	2016-12-17 20:29:03
Received Time	2016-12-17 20:29:03
Relayed By	SlushPool
Difficulty	310,153,855,703.43
Bits	402885509
Size	238.131 kB
Weight	952.272 kWU
Version	0x20000002
Nonce	777617094
Block Reward	12.5 BTC

Hashes	
Hash	000000000000000000cdc0d2a9b33c2d4b34b4d4fa8920f074338d0dc1164dc
Previous Block	0000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214
Next Block(s)	000000000000000002cc08d842aa0156b466c300a7bd756448d22ec337d4692c
Merkle Root	87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

4 Version

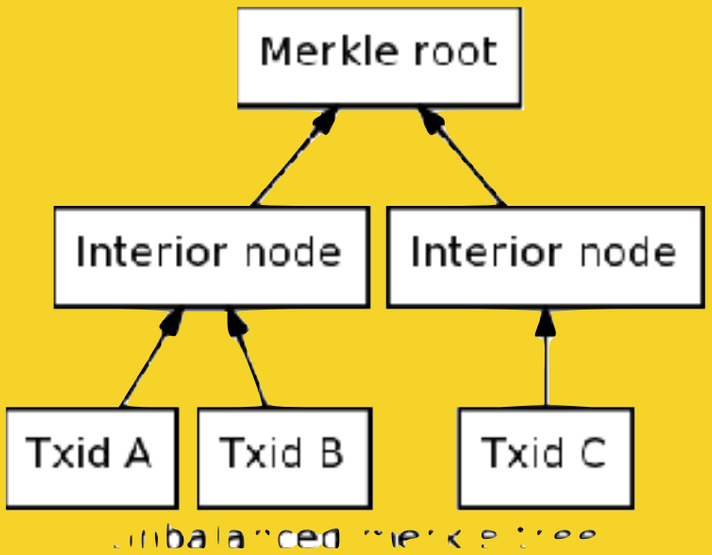
32 previousBlockHash

32 MerkleRoot of Transactions

4 Time

4 Bits

4 Nonce



Each block is named by:

SHA256(SHA256(Vers || Prev || Merkle || Time || Bits || Nonce)

4 Version

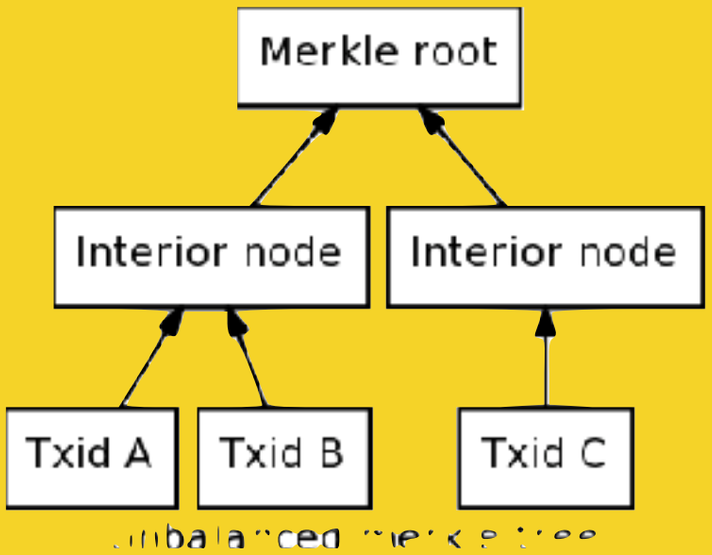
32 previousBlockHash

32 MerkleRoot of Transactions

4 Time

4 Bits

4 Nonce



Each block is named by:

SHA256(SHA256(Vers || Prev || Merkle || Time || Bits || Nonce)

Only blocks with Name < D_{time} are valid.

Block 443888

20000002

0000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03

402885509

777617094

Block 443888

20000002

0000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03 1482006543 0x5855A00F

402885509 0x18038B85

777617094 0x2E597EC6

Block 443888

20000002

0000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03 1482006543 0x5855A00F

402885509 0x18038B85

777617094 0x2E597EC6

```
02000020
14c2a9b75c44c656d5720f694c32d97aa3354d2d926a80010000000000000000
c28a2cdd8aeb39b66bcf7906b26c9b1b865dc50ed99243b152f4a498e883f687
0FA05558
858B0318
C67E592E
```

Block 443888

20000002

0000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03 1482006543 0x5855A00F

402885509 0x18038B85

777617094 0x2E597EC6

```
02000020
14c2a9b75c44c656d5720f694c32d97aa3354d2d926a80010000000000000000
c28a2cdd8aeb39b66bcf7906b26c9b1b865dc50ed99243b152f4a498e883f687
0FA05558
858B0318
C67E592E
```

↓ sha256

99d1364a650f0f7e60803989d0d7bbca9be11c675d1271d075617668a8c8434f

Block 443888

20000002

0000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03 1482006543 0x5855A00F

402885509 0x18038B85

777617094 0x2E597EC6

```
02000020
14c2a9b75c44c656d5720f694c32d97aa3354d2d926a80010000000000000000
c28a2cdd8aeb39b66bcf7906b26c9b1b865dc50ed99243b152f4a498e883f687
0FA05558
858B0318
C67E592E
```

↓ sha256

99d1364a650f0f7e60803989d0d7bbca9be11c675d1271d075617668a8c8434f

↓ sha256

dc6411dcd03843070f92a84f4d4bb3d4c2339b2a0ddc0c00000000000000000

Block 443888

20000002

0000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03 1482006543 0x5855A00F

402885509 0x18038B85

777617094 0x2E597EC6

02000020
14c2a9b75c44c656d5720f694c32d97aa3354d2d926a80010000000000000000
c28a2cdd8aeb39b66bcf7906b26c9b1b865dc50ed99243b152f4a498e883f687
0FA05558
858B0318
C67E592E

↓ sha256

99d1364a650f0f7e60803989d0d7bbca9be11c675d1271d075617668a8c8434f

↓ sha256

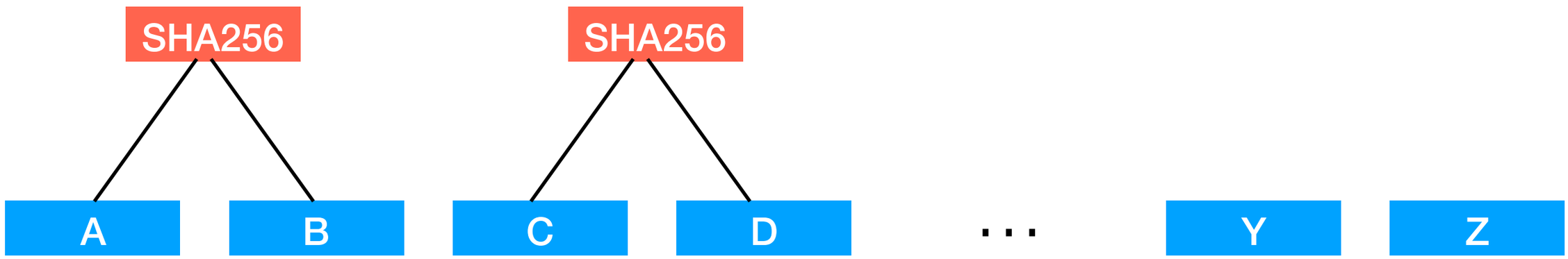
dc6411dcd03843070f92a84f4d4bb3d4c2339b2a0ddc0c0000000000000000

0000000000000000cdc0d2a9b33c2d4b34b4d4fa8920f074338d0dc1164dc

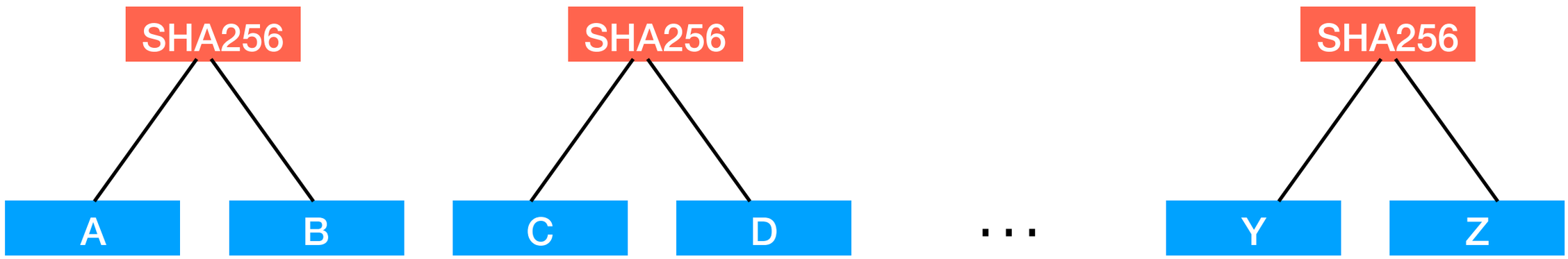
Merkle Tree

Merkle Tree

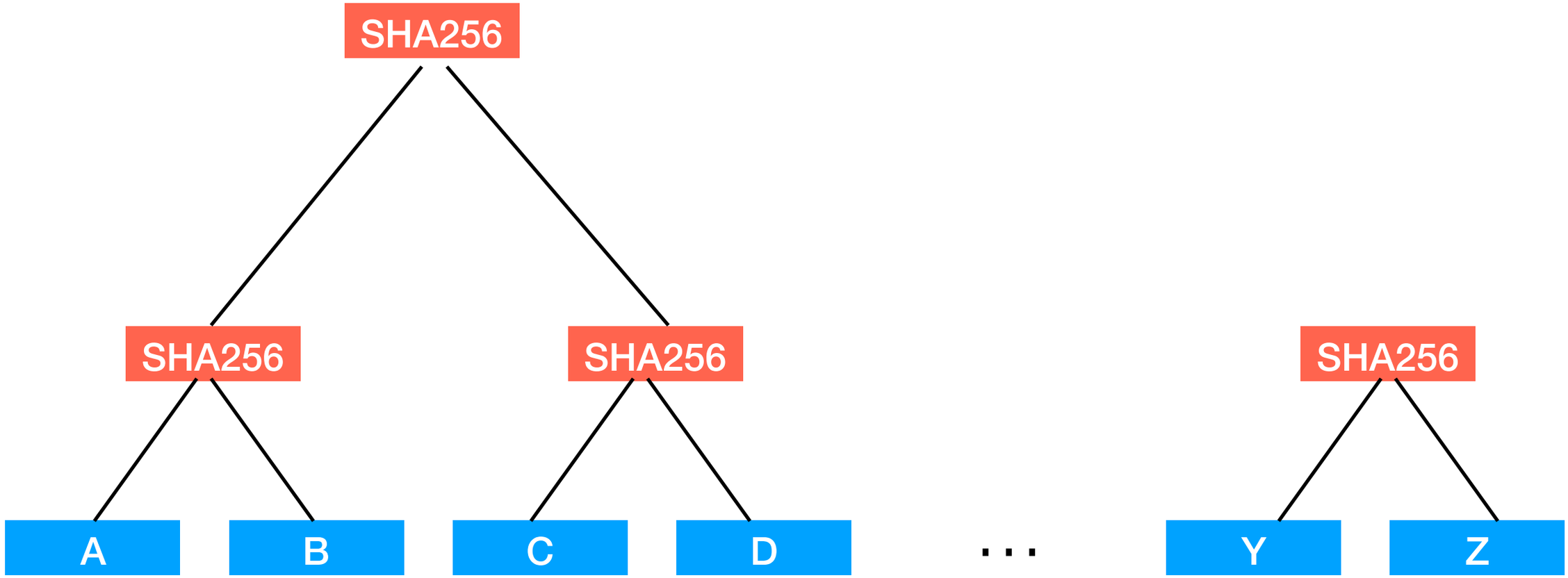
Merkle Tree



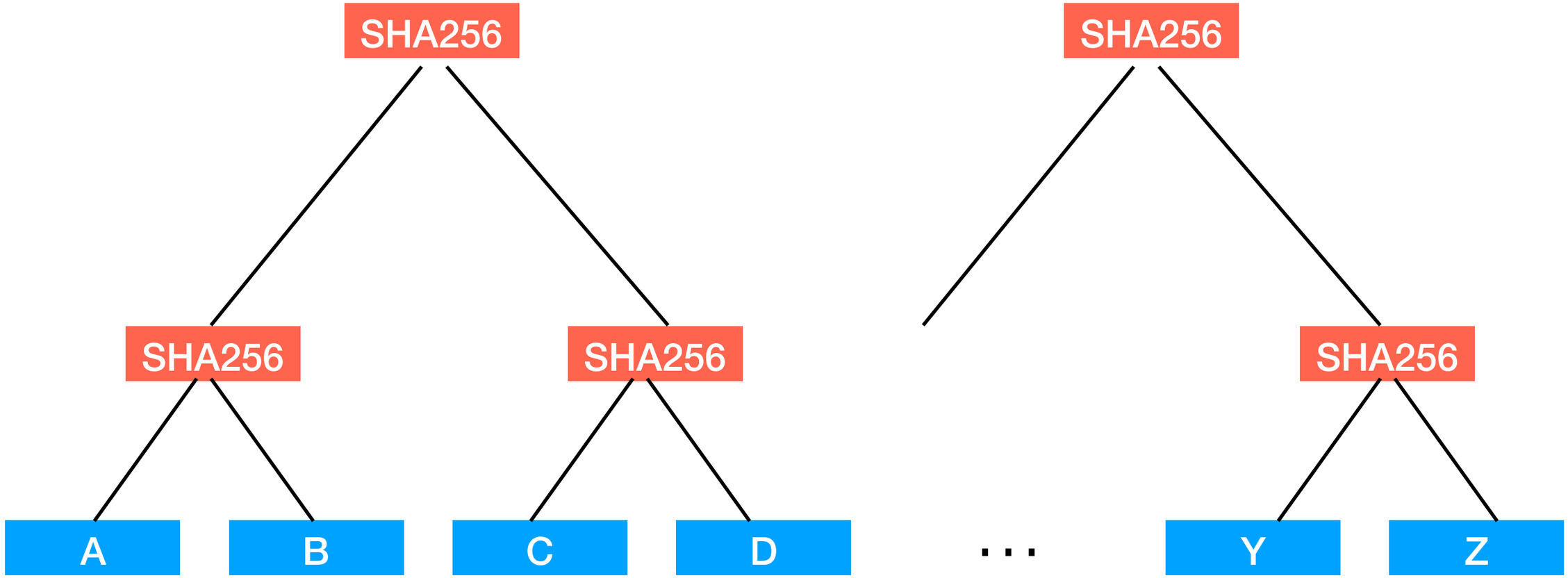
Merkle Tree



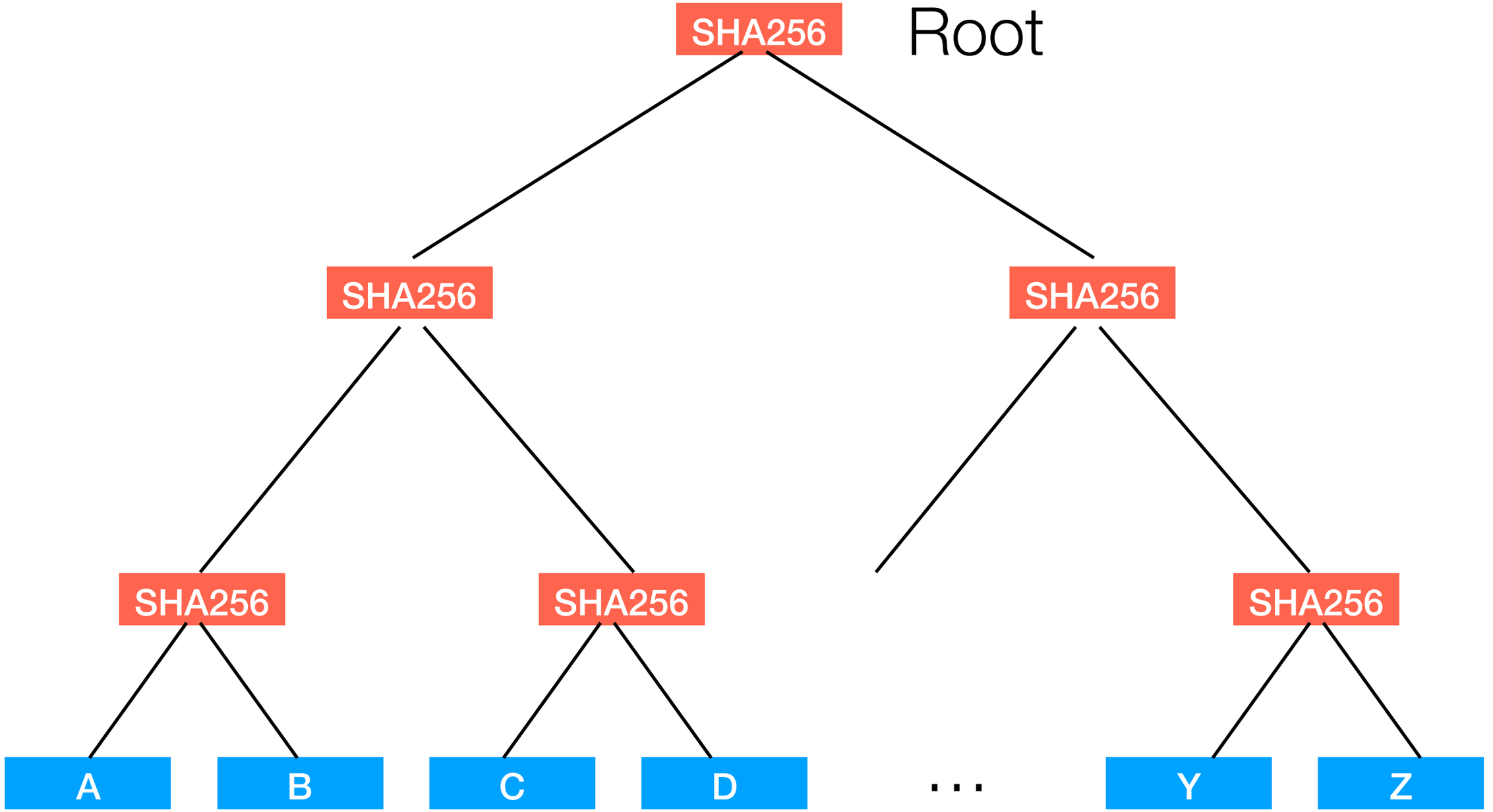
Merkle Tree



Merkle Tree



Merkle Tree



Bitcoin Block

4	Version
3	previousBlockHash
3	MerkleRoot of Transactions
4	Time
4	Bits
4	Nonce

# of transactions

Tx1

Tx2

. . .

Txn

Transactions

List of Inputs

ref to previous output
signature script

List of Outputs

value
spending script

value
spending script

Transactions in a Bitcoin Block

Tx1

4 Version

1-9 # of inputs

_ Input transactions

1-9 # of outputs

_ Output transactions

Transactions in a Bitcoin Block

Tx1

4 Version

1-9 # of inputs

_ Input transactions

1-9 # of outputs

_ Output transactions

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Transactions in a Bitcoin Block

Tx1

4 Version

1-9 # of inputs

_ Input transactions

1-9 # of outputs

_ Output transactions

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Amount
ScriptPubKey

How do we know if a transaction is valid?

How do we know if a transaction is valid?

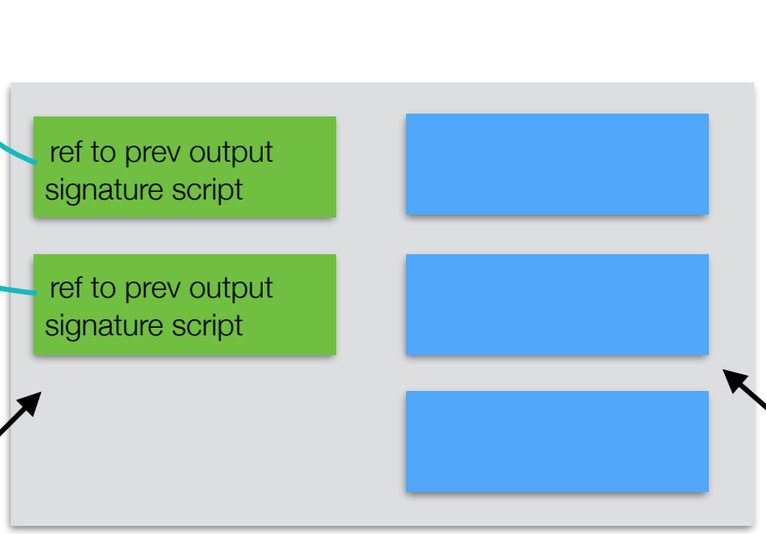
Sum(inputs) < Sum(outputs)

Inputs are not already spent

Inputs are “authorized”

Past tx in earlier blocks

New tx



“Spending witness for previous outputs of transactions”

“Ledger entries of new owners, and their policy on how to spend this coin.”

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0   Index of input
c05b56702943c5342901000000 8b
483045022100b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver

Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c5342901000000 8b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Index of input

Length

scriptsig

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver

Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c5342901000000 8b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Index of input

Length

scriptsig

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver

Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c5342901000000 8b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d000000 1976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac 80e7c63f
00000000 1976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac 00000000
```

Index of input

Length

scriptsig

1st out

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver

Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c5342901000000 8b
```

Index of input

Length

```
483045022100b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
```

scriptsig

```
ffffff02807080b80d000000 1976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac 80e7c63f
00000000 1976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac 00000000
```

1st out

2nd out

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Ver

Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c5342901000000 8b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d000000 1976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac 80e7c63f
00000000 1976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac 00000000
```

Index of input

Length

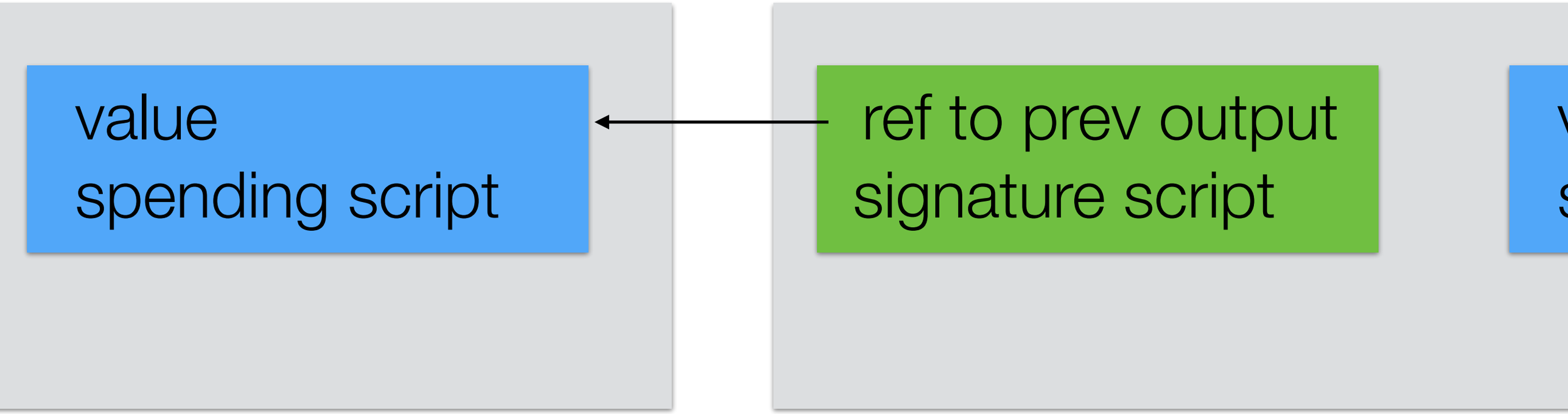
scriptsig

1st out

2nd out

locktime

01000000827ec3b8a540016c5fd18492dec0eec01836aaa280e4fabbf901000000000000b6ecaa535691a4d88e2a24fa0957e66e5ed87cbcfcb0c280addba9738a38dd72ca498150ef75051a0fdafe1408010000000100000000000000000000000000000000000000000000000000000000000000000000ffffffff0f042c498150024d15062f503253482fffffffff01a078072a010000002321**02ef15f4f9ae8b0f5a48992bcfa556ec1dc6fc62a85beef450004a0376d4004d**4dac00000000010000000105f03ccf2cf648bd81865c608685600f8f16229608e0c05b56702943c53429010000008b483045022100b232d83cc379df6f4d6b423871f2e3015085726a03135bae0bcfce5dd44526ed022040811b91eb053adfaa5a63d221da5ea702efc92e98d08d6ca7bbefa1ab857cce014104ef75b5750b34e5e845004e29af1e70ac0333095afa6ebae4eed9e5610f17b358578700492d16bf6fa379e962421f5c38812972399a8b3c27adc4532a7ea9957dfffffff02807080b80d0000001976a9141f585f53479b0a2918895ebc41e09db4f171fe3888ac80e7c63f000000001976a9142d04eee9e30ae8b732bbf56f0dfa83d5d1af33d988ac00000000100000004a11d06da6ec09a64fa8e7cb34133db48d27c013a7596b77a9e1a273e5fe2929401000000**6b483045022064022e28a0101d1b028f7ac2e700cdfa3335eeaecd5579b9eb2e5269357d63990221008fe424620e1b7d9502e03fb579c0ace3b7f6a8eda3ab05afaa9ffba57d**27d88e012102064cb5385061c860733863c0bc5e51492bdd27240c8c4541c16167f37cb50b04ffffffff5d482b4dcd8d2a320d2e59cf67bc2937df41ce7dd302939f15795510c264cda8010000006a47304402203e5f4d034631baea32a989fb0a46296b356c0f1a8568481809b53de4d9879a2802202d81bb212835faf3fc96c4001d8bc58acb5d293df4698482d4805c83ad2707eb012102064cb5385061c860733863c0bc5e51492bdd27240c8c4541c16167f37cb50b04fffffffffa27256ca4d12eb8747b9bd439a4d8c8b8f69d385458a655909ba6424a9b3079a000000006c493046022100e7f3047d7821fd7eaa3ad5a0ffa434698051995e280f364d94d68d580f5acdf90221009ad6b88ff42a3544cdde3fbca9cd4e4420d3753147c44568d3eb9296e1abf7c7012103060332accf032db8a4f4621ab0942eba8b8411a2fafef0355e7e6f8082bc7326ffffffff8543f55556439e7356665ffde4acc2e3e441dc0700504d68cfb098547f9165db000000006a4730440220130e8310a0c2b12b92493cdfbbff7226aeea5523ccf34f019862d22209613dfa02200e5780421382bb7d57e3e9d7afb50266ed8b9918e0b7a2cc0a0cbd0b1062c21c0121020b549cdddd1dbf0c71f98348a21f365534bca423d25bc5832d3ecb9200f9b16dffffffff01c0da905902000000**1976a914c88ed470692d0c11a671685595cad039bcce359988ac00000000010000000875f3f23c38f1028bbae82790b9c09588df6ece07cfb763ee5472c8c374f0518e010000008c493046022100989ba93aabdc1af5895e629509caae169bd2ad0d9fa94fff8d51580ee0b10544022100ffa3d089aca8a70b7892b5ec5a29bb066e4e43fd33b8e0318079f2d903e69df0014104c41cbd6dea2817393aec3bb80cbd148c16f0630be703ef0fd6289604a809eb21241451b31fa317d39cea4e26793265e1305c34d3b6750945764d680278f171b1ffffffff8452454ff5800a84d8717a17859ed260cc61cbd14773ca648ea677674afc90ae000000008c493046022100da4df82fbb585228a5384f1fe9ddbdc37182e8ac125c6c8550ad9197cc3182a2022100b65e9b9055c90a104829603e06995e14dcf54e0a28cef22b35f5405e673e266e014104378b8beea9b92c6055f90845172a7a5e5d7eee27d29b65cd715dfed345d1b015beda2fa30e1d12ba7ee354fd1ca313df59c4b32b29e4403ebae26563c2aa0253ffffffff4a1426c4b6312e08ce7f4402fd994fd98dc41ed62076be6bf2cb5f6921f3edd4000000008a473044022019 03e3394b486e4b39be9502cfd90872d70fe0164dbdaa4578793a4650587b8f02205d65342c76e8ee1935eddd6a018c2f58f5e25ecc8a4ee6ffd8a9eb5c88732e76014104ff0dcf5d1645ddd7fb318ecf0335ba65300184136422d00627b24bf61f7d86914f22e767baffd18c6d46b4482f04a07902cbcbfd0b71550a706d2565b1a261d2ffffffffa6290f5d0f27272a79053929799b01887c7e4e4293ce792d9914daed40bf8248000000008c493046022100951 25a342561f43b4eccb87c1e72d81b5f4c0fe4b91c73de30f7b89e590e17440221008d92787d96d52242c61fa0afe649f5025c14bf9d56df31cf92c518652f4d823401410439698e8e2218c7a73c9ab86859eb7273337cf34d867a955b7f0df9b432fab2ad54824352eb69ef9331042d8d3080118884ddaacac60fa732b21c8c0035c83ff1ffffffffad3bdc2b4657afd28f73b0472165144340717 05e6338d63b82fabe6a271a0247000000008b483045022100cdb30a3b5458b57ae33b2c0e89dc6b8202b72e4c92275cd53e1a0426038fd26e02203bad69005bd590c8985727338e0090dc7375896c93b614811d249d5377edb39301410400099fdec541569162c57f41b61374a1e3a6a5f10d754601b1e7fe163829928d01cba8dc2f656ae084eb458fbfa9a7cd77f864ecaef8563ae94f2b3b96351053ffffffff6ee3ee42a78cd4d8923177790d2e946bc5c6d46180d4925def966dde073675390e0000008b483045022100ec63c82cca7991aa25998909ee0e34e4af831b018500140e83ce73f0f4acc9d002202c5cdfa34279cbf32c305c870d84a3e199d7f522dc034d3aba7d12dbb6af8a94014104ad67b0c87a621124d404ff0380d3325e8dc2eebc26afeb786e9ead2be0a95092d3463cc674e8fc34078ed14843c39ecaebd72c5aef1432e23a226db200a73f19ffffffffeaec680ae472e49f1aac407f1f4a043119cc1f3b2556750401a3835920158a37010000008b48304502204f572ce18c1accdf4347196ebcbebfc3a4758ecca819d83ac9040f9ee0e41b1102210082ada1d7a30615df8fc3552daec4a64199312862f7c87b643f9752d2daa33f84014104c41cbd6dea2817393aec3bb80cbd148c16f0630be703ef0fd6289604a809eb21241451b31fa317d39cea4e26793265e1305c34d3b6750945764d680278f171b1ffffffffff58b4611713a07f9f1324df27c48511171b663802ece8aa9823ff2227dd5a285010000008b48304502200840ab6b79393e26179e44f70e0e6bebf0b64608575b614c027a767a43edde99022100df879ad3651c03446f3324a967e2f77b2958e255890e9c78631ace13b415b945014104c41cbd6dea2817393aec3bb80cbd148c16f0630be703ef0fd6289604a809eb21241451b31fa317d39cea4e26793265e1305c34d3b6750945764d680278f171b1ffffffff02f0450f00000000001976a914dc11899967e3df3bbd0bc9dce7a876008d88c7ae88ac00ca9a3b000000001976a9148f0e19a7ad9abd62b285363bdb170d7f5d28943288ac00000000100000001e82989e72c6a36bec1bd8cf5f23fafda18ad274606573ea27f652575877319370100000008c4930460221009b231470fd42c91125d09c1641be7da4272c5fc4cfc392350b27ae828d7e6779022100d5637cad76d0d230e111892c9dbbe78d34268bf4fc729b94e764f5de468d8438014104b4e2c30a7ca121695b1ad2fef4c7b836b361b5989412fb7eaff0aac0461f3bb49bd0d884e74c02b6ba6467b310964513def9dc2107f352aaec8ee6d2a9ba2208ffffffff02916f4b170200000019**76a91445a0df49818c9f693d12c917302620c476905dd488acaf14f114030000001976a914432e9ab5f86f6c7120fa8930c015b623168832c988ac00000000100000001177b6577fdb8e42a5b9701cc0b041c7781b671fb8d4c96b127a5848c7de548c4000000008c493046022100c69d9f08157d81dd59421e9bd1d5d32f2eb9cd5eee9ee4eaefd3d16a5a324e15022100813b6f987f7c256ae78aa58d195516f7ea94ac6ffcfb54c426bb0b66ead59e4f014104cca2dc809ece7324c6fb1b6006c12492559746a96611982f31977dc65a33a6b744ebcafa20e5ecadfd428cea8a4b60b3073ada6c1da657893a50418c24555959ffffffff020027b929000000001976a9144b1b8e06ebe63f8cb92a34060124ead51dc68b7588ac2ee71c6a010000001976a914050d1959dfb23a463a43a44f2b4b764e075efc9888ac00000000010000000012cf494c7c716423e82e6666922e0c90d6691330a600c454ad1c8ed0a2b40dcee010000008a47304402205b5872cc59e1157c4b050dfbf9419d03a12ee1d7432dc158161db967df6853f702205c64df50255c522361b97e786ffdaa2f249fa97aa69d6ca38046f21615dc3571014104e1371e6c530cd0442a04a2efdcb2a00c485fd6df49e9f07b6b05cbdd0e8a2cd3b3f2792742effbc5136abf91bb6ab77ff5222f36285a6174be380fe448992942ffffffff021f51d15c000000001976a91437c7d6233b197c6e547ac5701bfdf8b45e49cb2088ac7189c8d8010000001976a914a5534677ce6abac2627396f7dae0860b33d8f1be88ac00000000100000001705ffefd13bbfbdd4a8ef31434334d0fa8218a19938d4c289265d16afb10f1df0000000048473044022020dd07aadfe4a973ed0cd0352f0573c2948ce439a50ba8cc50437937242d6c85102202121b6d3840eb8eb9267f6f9949b153983f56d7b6aa23f3916a6dbd888706d5101ffffffff01b5124f2a010000001976a9140568015a9facccfd09d70d409b6fc1a5546cecc688ac00000000



Spending Script

A program, P, that when executed after executing the signature script, returns “Valid”

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

Duplicate top value on the stack

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

Duplicate top value on the stack

Hash top value on stack

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

Duplicate top value on the stack

Hash top value on stack

push this constant onto stack

Standard spending script

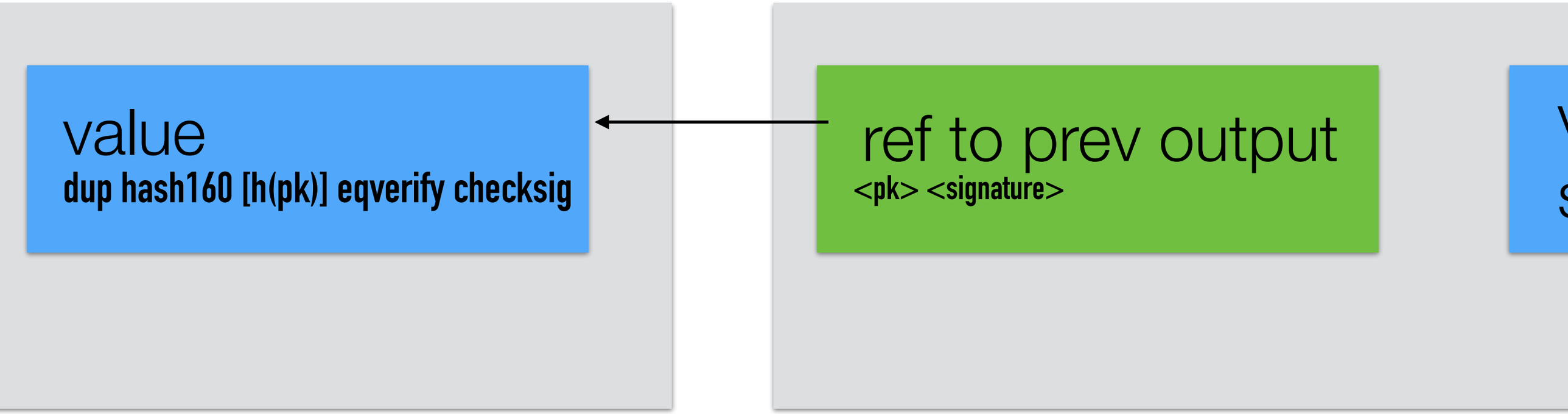
DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

↑	↑	↑	↑
Duplicate top value on the stack	Hash top value on stack	push this constant onto stack	check equality of top two stack values

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

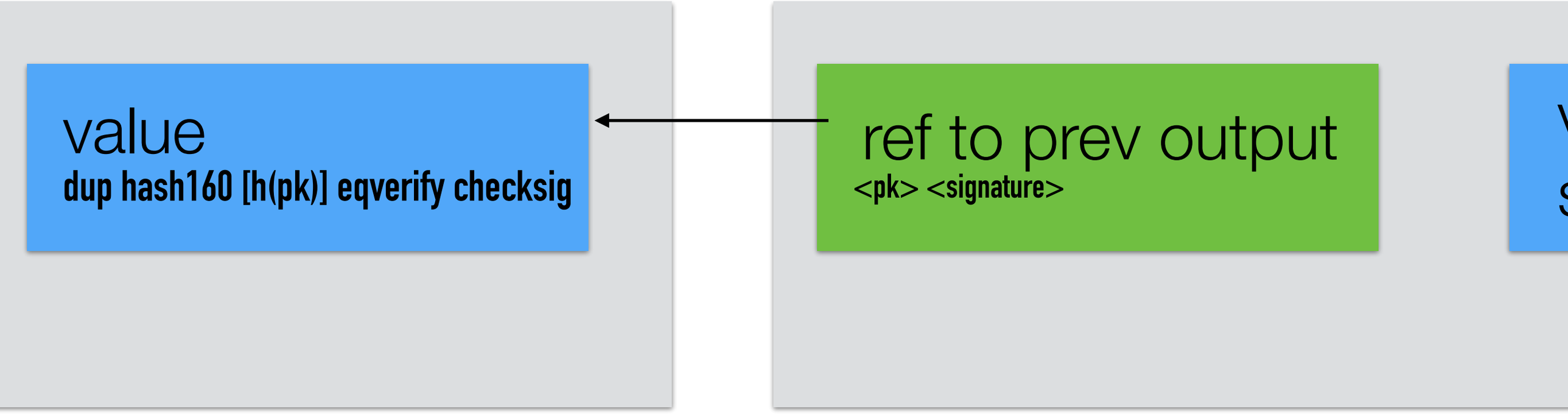
Duplicate top value on the stack	Hash top value on stack	push this constant onto stack	check equality of top two stack values	check whether next two values are pk,sig for the tx



Spending Script

A program, P, that when executed after executing the signature script, returns “Valid”

01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
48304502210 0b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
*88ac*00000000

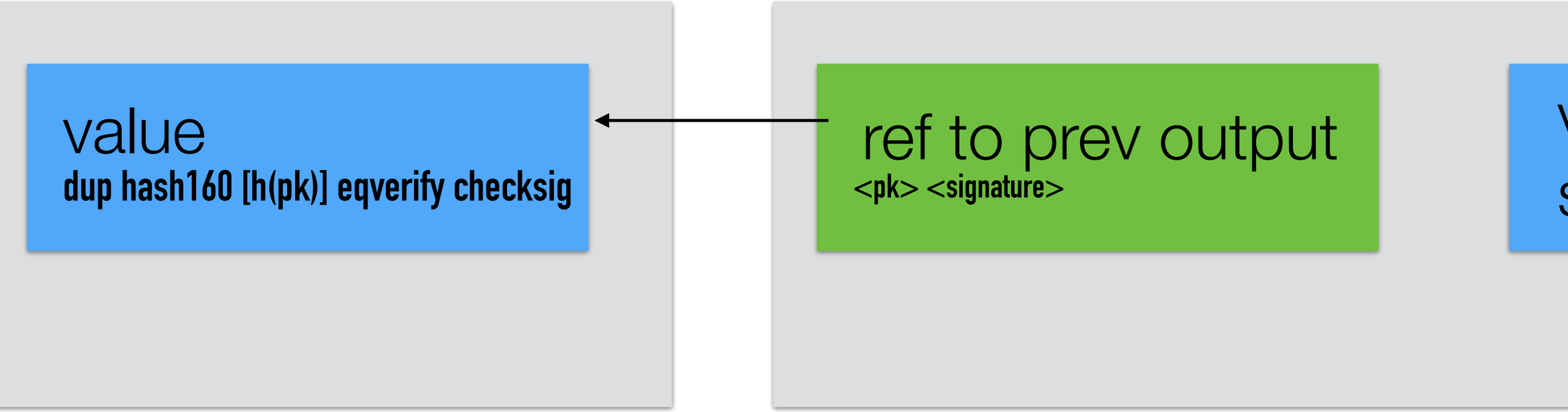


First run this program

483045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc3435022100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d0148044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig



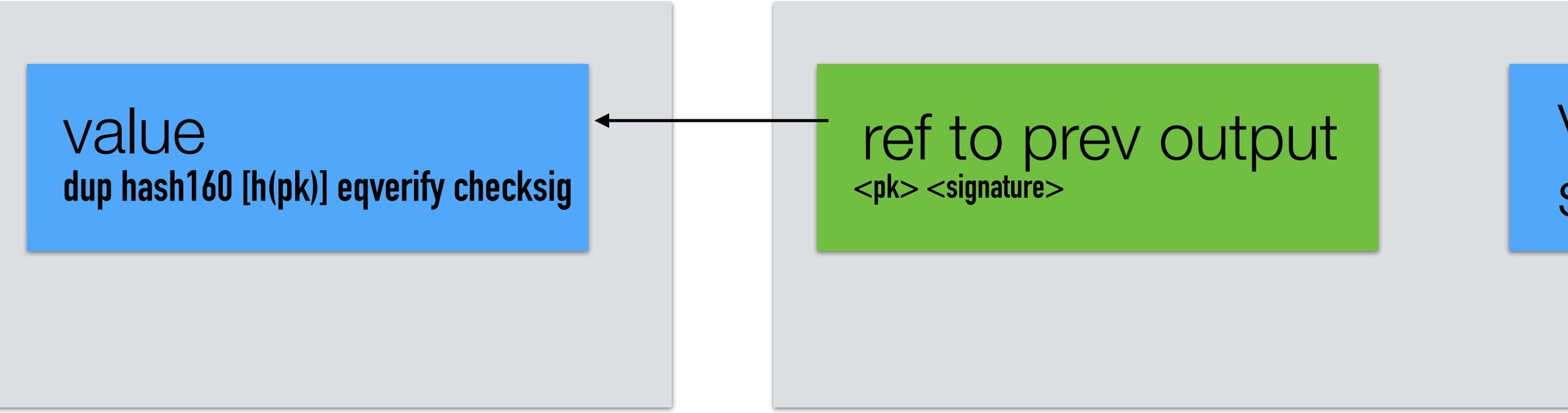
First run this program

PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01

PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig



First run this program

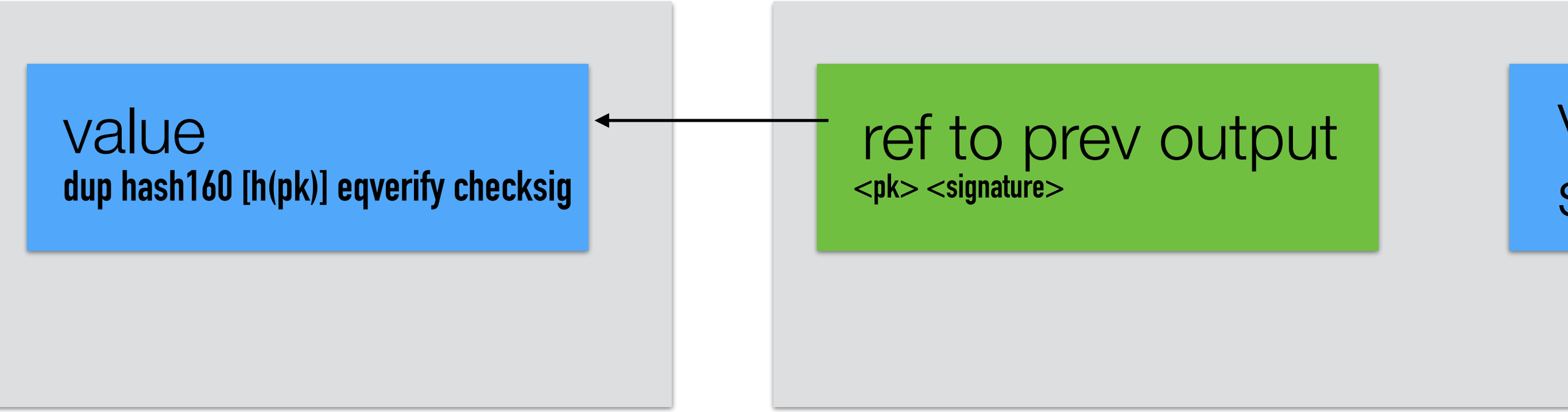
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01

PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

3045022058582…c07d01



First run this program

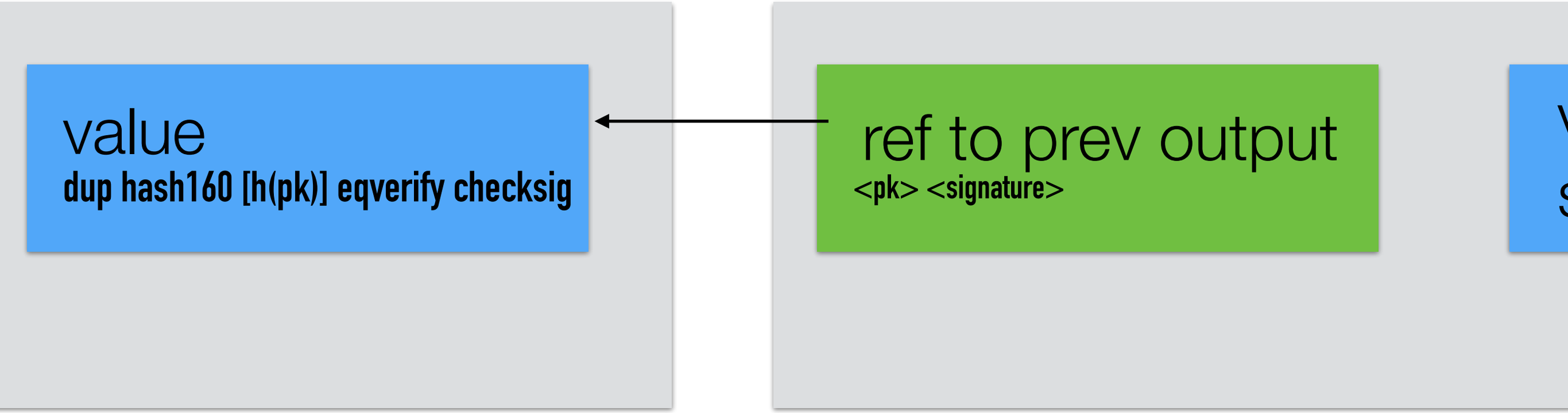
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

044ded81d4fb1…ecccba

3045022058582…c07d01



First run this program

PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01

PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

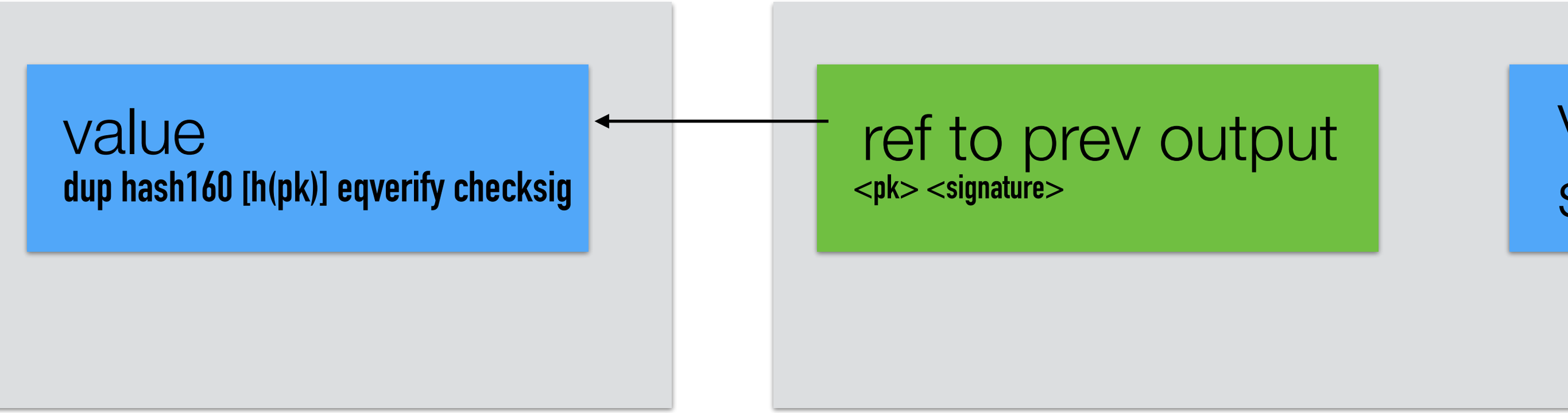
Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

044ded81d4fb1…ecccba

044ded81d4fb1…ecccba

3045022058582…c07d01



First run this program

PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01

PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

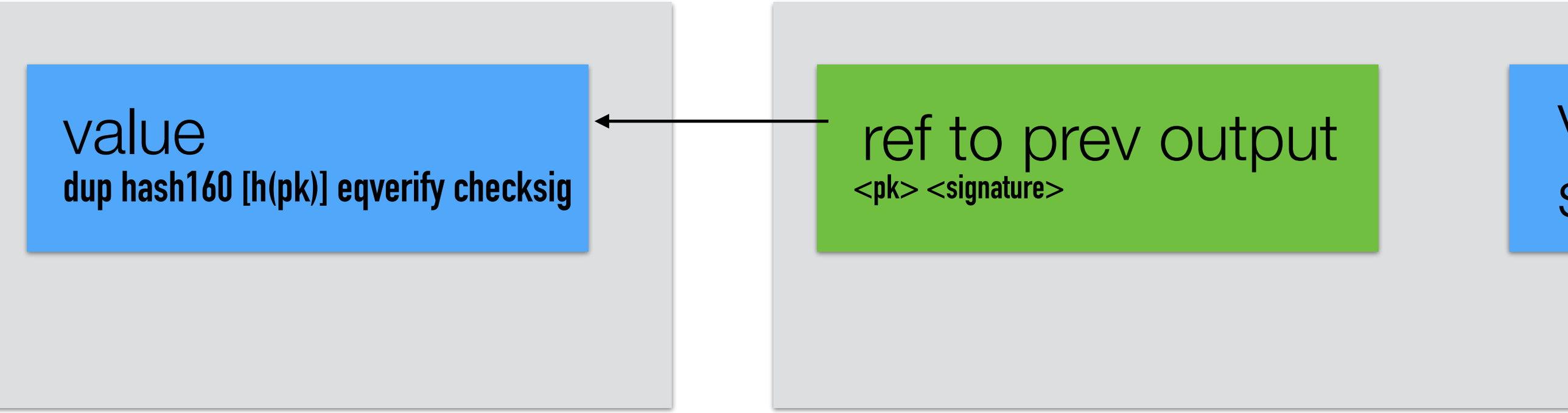
Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

1f585f53479b0a2918895ebc41e09db4f171fe38

044ded81d4fb1…ecccba

3045022058582…c07d01



First run this program

PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01

PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

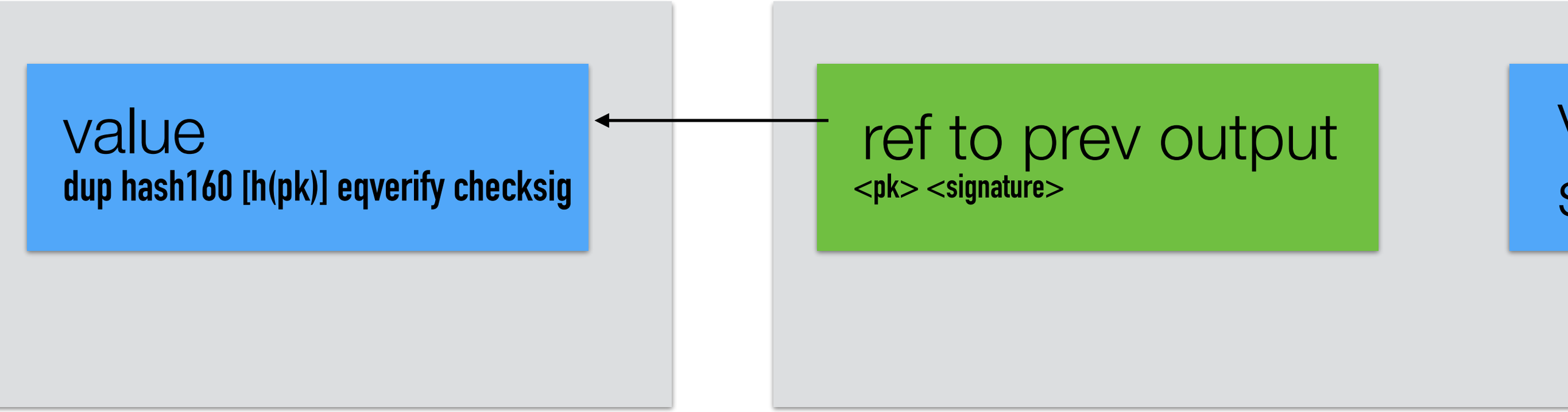
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

1f585f53479b0a2918895ebc41e09db4f171fe38

1f585f53479b0a2918895ebc41e09db4f171fe38

044ded81d4fb1…ecccba

3045022058582…c07d01



First run this program

PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01

PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

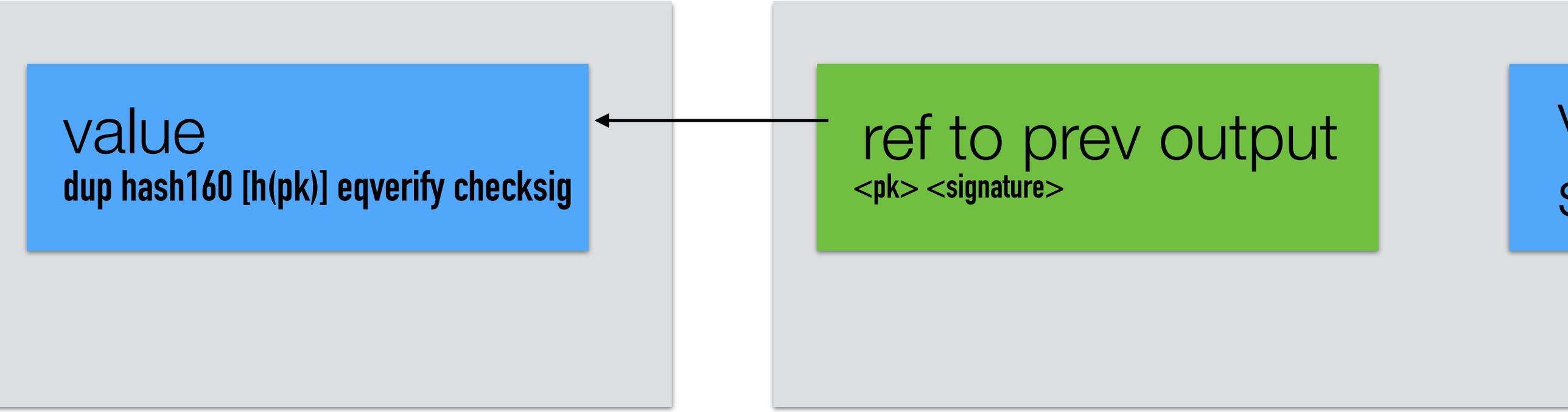
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

1f585f53479b0a2918895ebc41e09db4f171fe38

1f585f53479b0a2918895ebc41e09db4f171fe38

044ded81d4fb1…ecccba

3045022058582…c07d01



First run this program

PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01

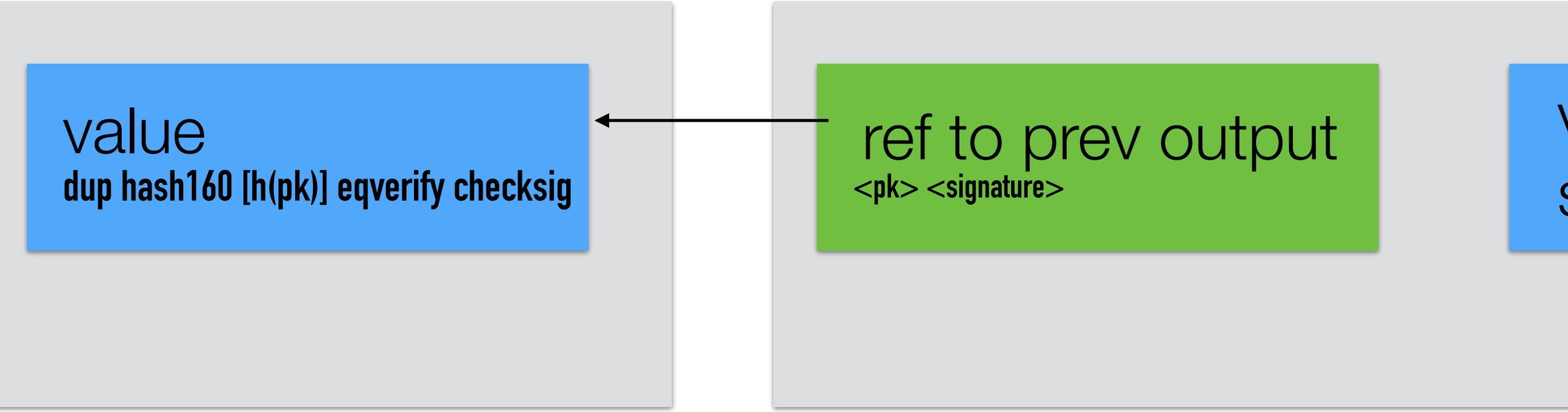
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

044ded81d4fb1…ecccba

3045022058582…c07d01



First run this program

PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba

Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

044ded81d4fb1…ecccba
3045022058582…c07d01

OK

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

Duplicate top value on the stack	Hash top value on stack	push this constant onto stack	check equality of top two stack values	check whether next two values are pk,sig for the tx

"vout_sz": 2,
"confirmations": 9,
"confidence": 1,
"inputs": [
{
"prev_hash":
"f7f380ed4cc8f54982cc2cc04cb372558e62770c5b9bff575161f637bd3ad183",
"output_index": 1,
"script":
"4830450221009f7768bf1d2322b757d3738437741 0f30a5e19d0f6e810d8aae8f4700
f82fd6f0220111ff9684afc84f160a4842cf113487098e84ccab92e3740317b3575f6152
b070121023a24f09e3b1c840946748d6da88e9aa687b9c08e547664c3ec16c0eab3f
505fc",
"output_value": 33311400,
"sequence": 4294967295,
"addresses": ["1PxTVHpG3JagK3oogWeLhUNFYVfgkRLP2b"],
}
],
"outputs": [
{
"value": 32000000,
"script": "76a914c29e48f3c4745986acc9c9c30c23d15f939d842e88ac",
"addresses": [
"1Jk3i3m78bkNMKKyVBmVb1tLvnaQJ8kJCT"
],
},
{
"value": 311400,
"script": "76a914fbcfc189b757194aa237130b0deb09698040c6fa88ac",
"addresses": [

DUP HASH160 c29e48f3c4745986acc9c9c30c23d15f939d842e EQ CHECK

Bitcoin address

1Jk3i3m78bkNMKKyVBmVb1tLvnaQJ8kJCT

a redundant “base-58” encoding of (a hash of) your public key:

DUP HASH160 `c29e48f3c4745986acc9c9c30c23d15f939d842e` **EQ CHECKSIG**

1. `A=Ripemd160(SHA256(pk))`
2. Compute SHA256(SHA256(00A))

c46f8f04db15c58a03027e23528c141c3df329db3cca1339f2a8c6fea790350f

3. Copy first 4 bytes to end

c29e48f3c4745986acc9c9c30c23d15f939d842e c46f8f04

4. Base-58 encode

1Jk3i3m78bkNMKKyVBmVb1tLvnaQJ8kJCT

How to spend

1. Form a valid transaction tx using address
2. Broadcast your tx to the bitcoin network
3. Wait for a miner to include it in a block

How to mine

1. Listen for new {blocks, txs}
2. Organize *valid* txs into a new pre-block
3. Hash pre-block, while changing nonce/time/txs in pre-block in order to find a valid block
4. Broadcast new valid blocks to peers.