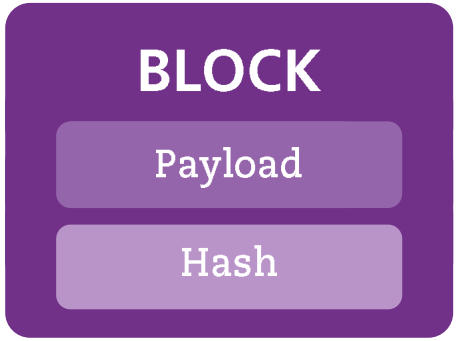
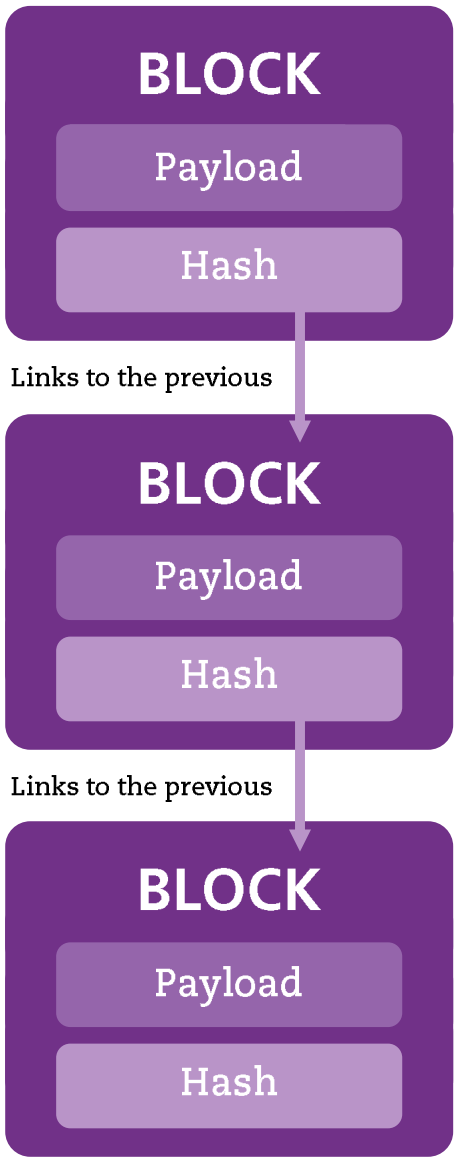
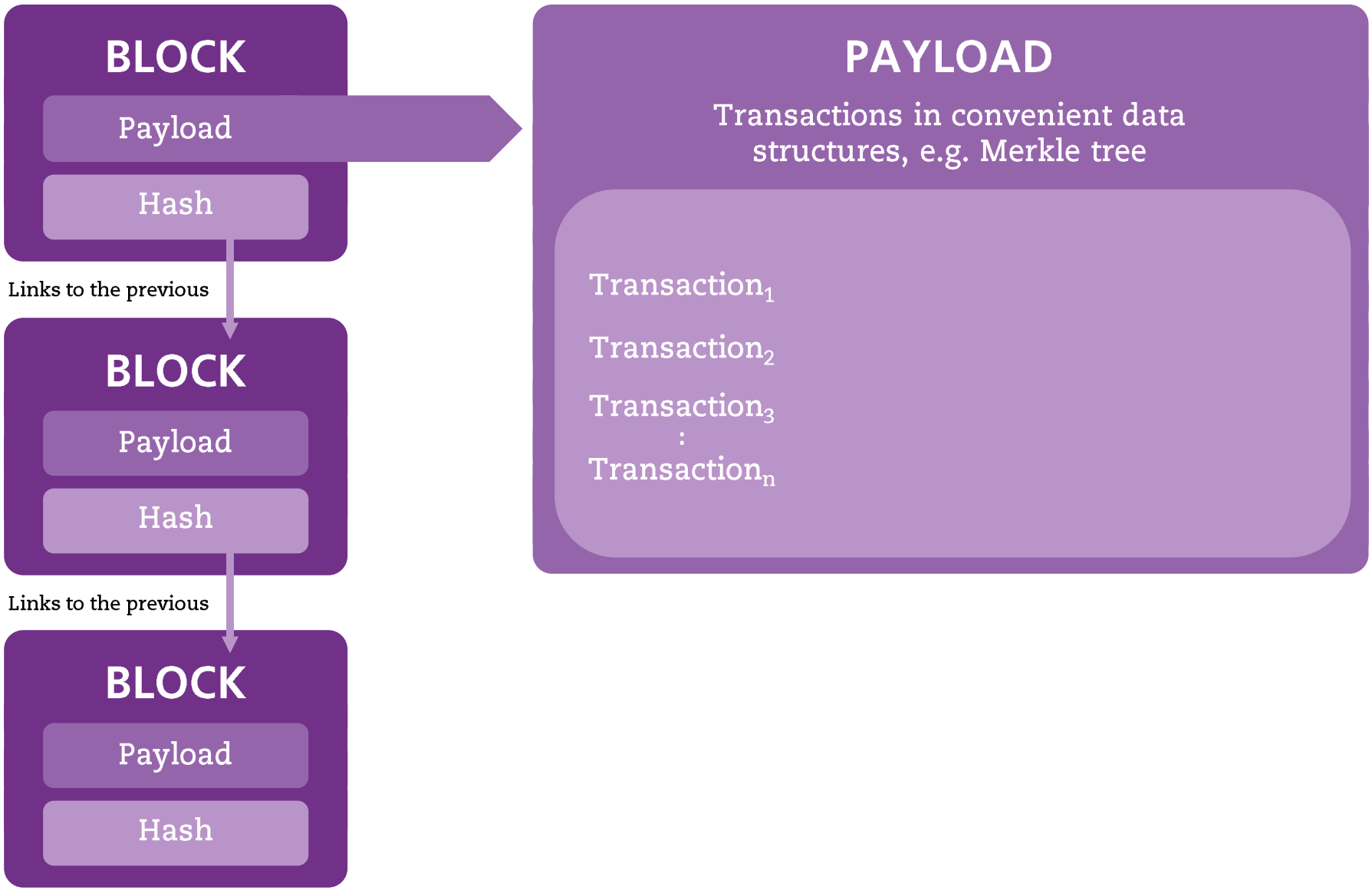
Inside of a blockchain



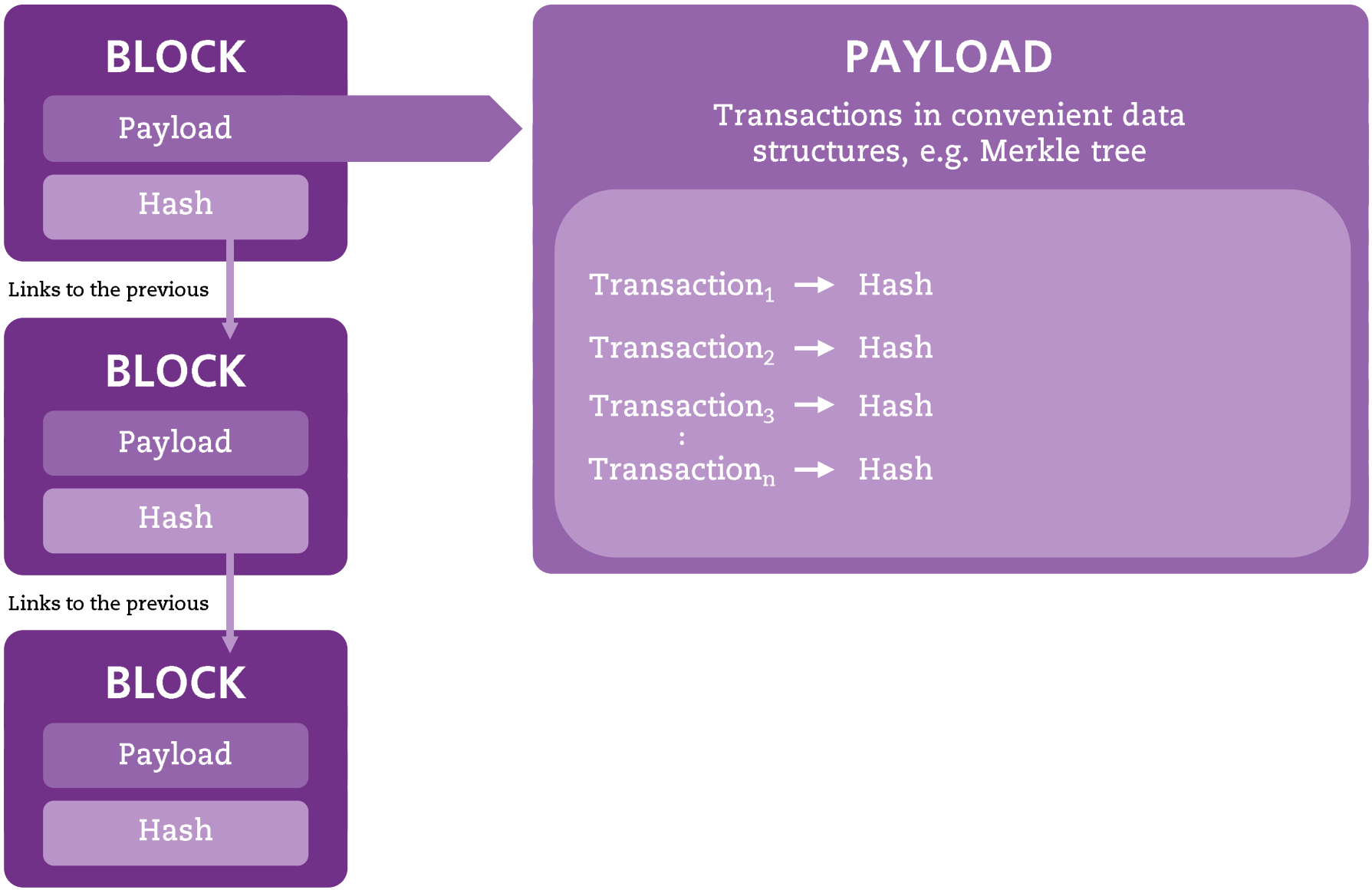
Inside of a blockchain



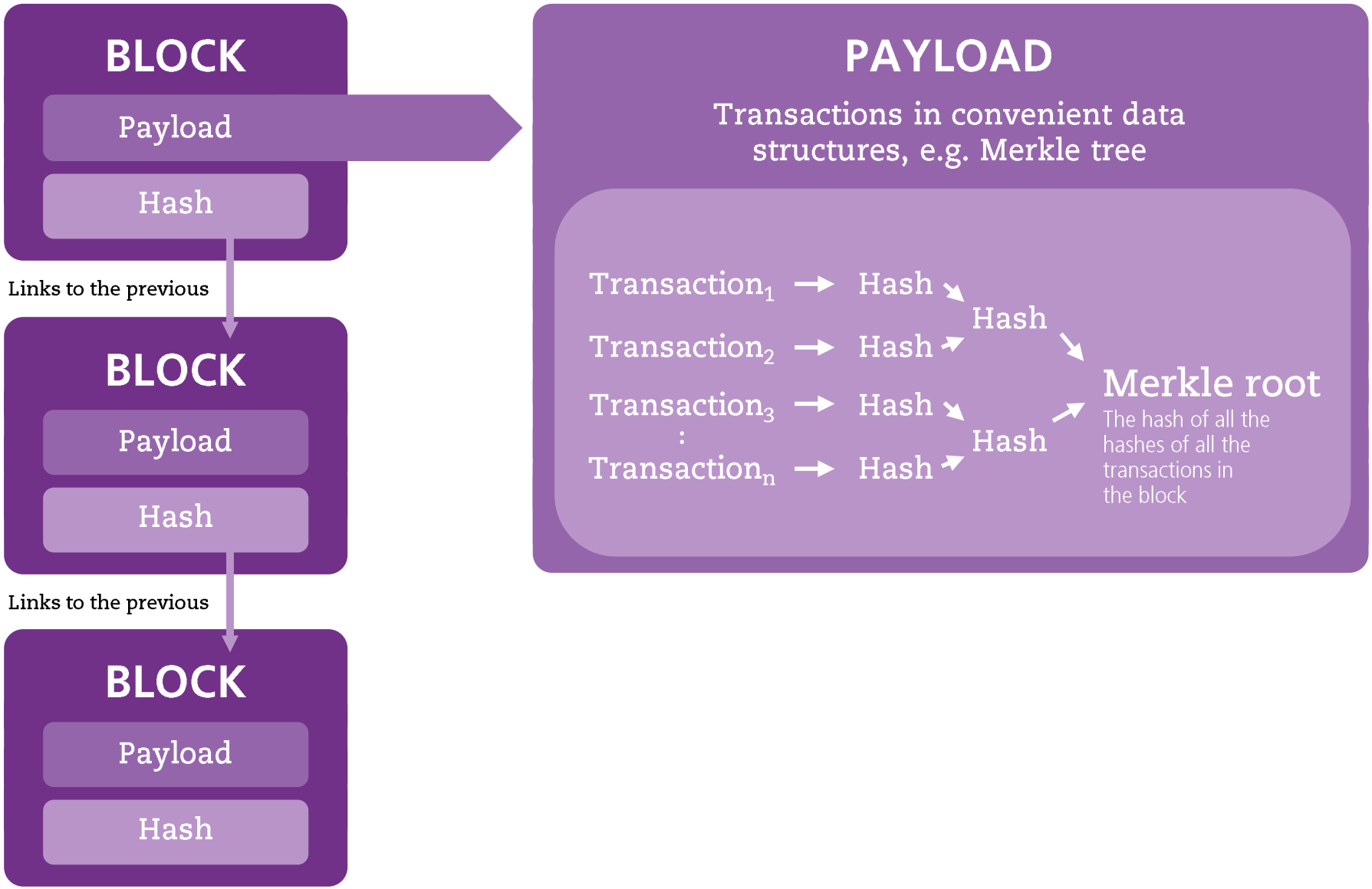
Inside of a blockchain



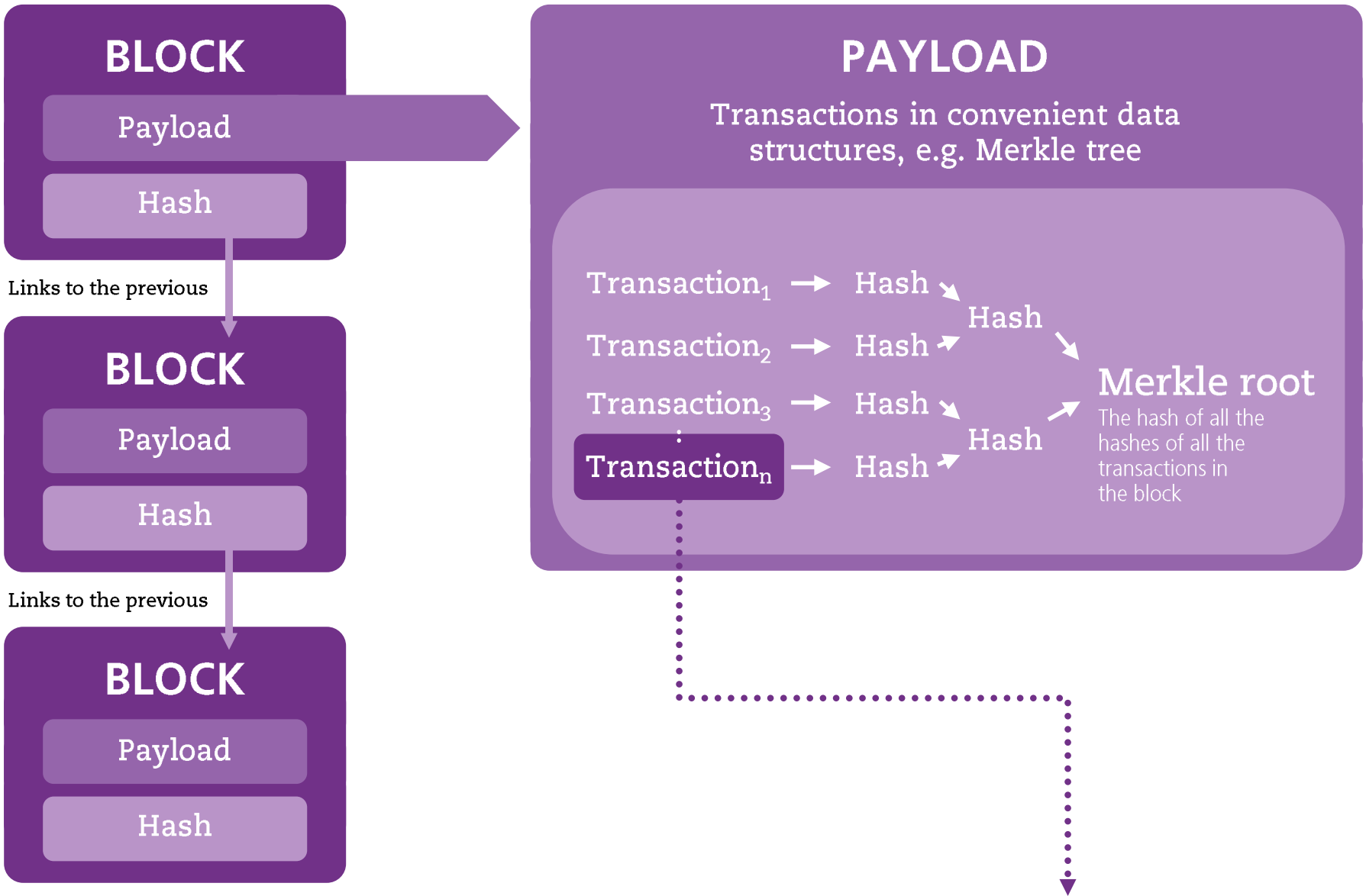
Inside of a blockchain



Inside of a blockchain



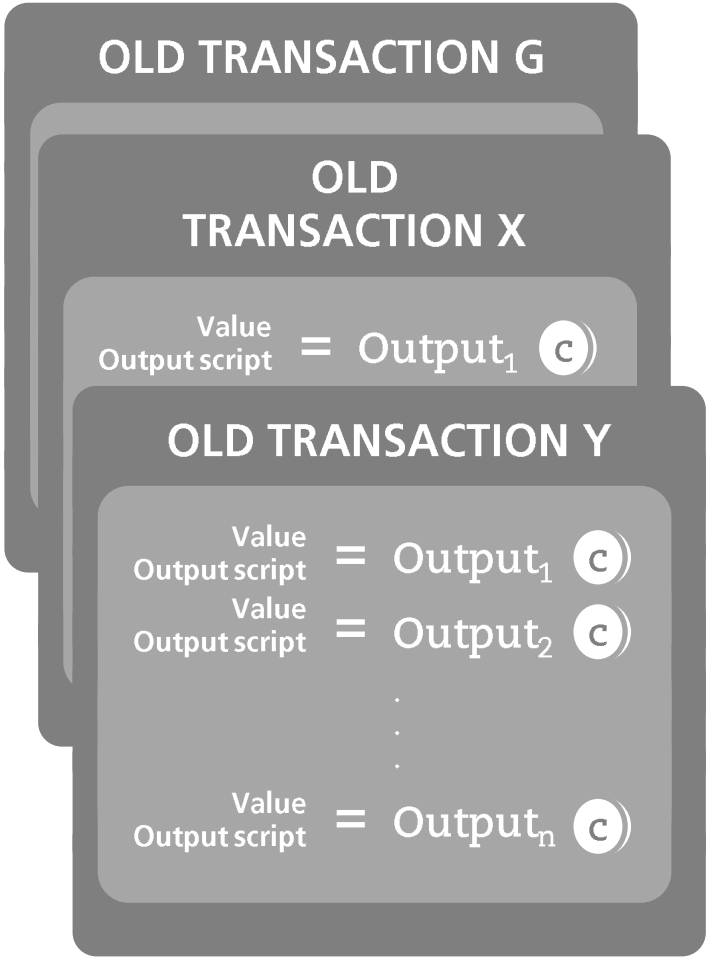
Inside of a blockchain



Transaction

Includes chaincode script that determines

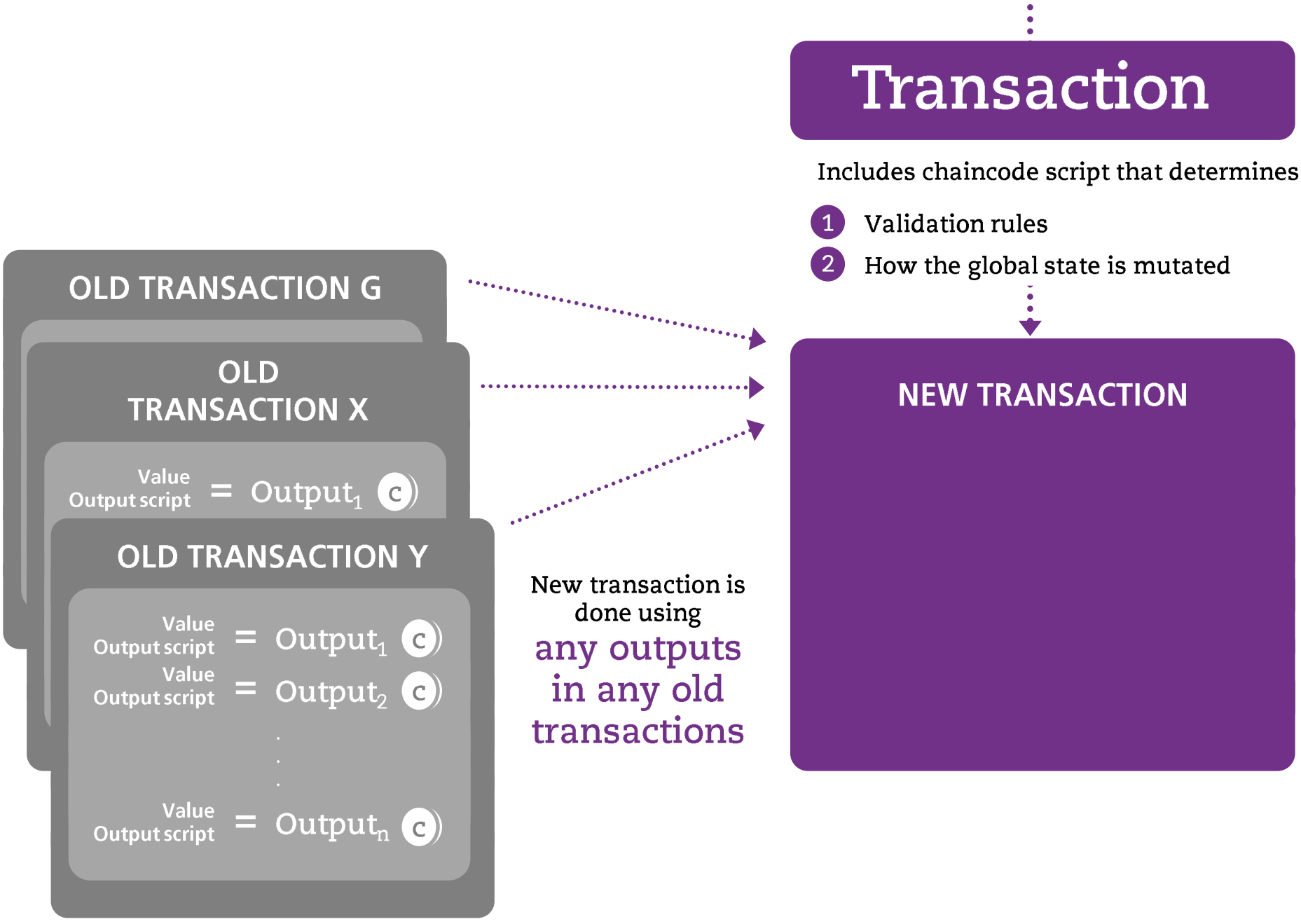
1. Validation rules
2. How the global state is mutated



Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated


Transaction
Includes chaincode script that determines
1 Validation rules
2 How the global state is mutated
NEW TRANSACTION
OLD TRANSACTION G
OLD TRANSACTION X
Value
Output script = Output1
OLD TRANSACTION Y
Value
Output script = Output1
Value
Output script = Output2
Value
Output script = Outputn
New transaction is done using
any outputs in any old transactions

Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

NEW TRANSACTION

OLD TRANSACTION G

OLD TRANSACTION X

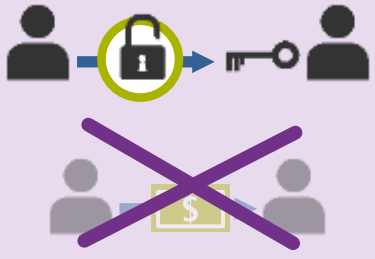
Value
Output script = $Output_1$ c

OLD TRANSACTION Y

Value
Output script = $Output_1$ c

Value
Output script = $Output_2$ c

Defines how that output can be spent (and by whom): Money does not change the owner but the PERMISSION to use it.



Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

OLD TRANSACTION G

OLD TRANSACTION X

Value
Output script = $Output_1$ C

OLD TRANSACTION Y

Value
Output script = $Output_1$ C

Value
Output script = $Output_2$ C

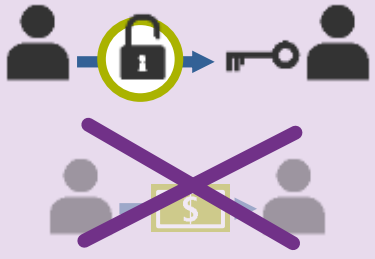
NEW TRANSACTION

C $Input_1$

C $Input_2$

C $Input_n$

Defines how that output can be spent (and by whom): Money does not change the owner but the PERMISSION to use it.



Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

NEW TRANSACTION

Output reference
Signature script = C $Input_1$

Output reference
Signature script = C $Input_2$

.
.
.

Output reference
Signature script = C $Input_n$

OLD TRANSACTION G

OLD TRANSACTION X

Value
Output script = $Output_1$ C

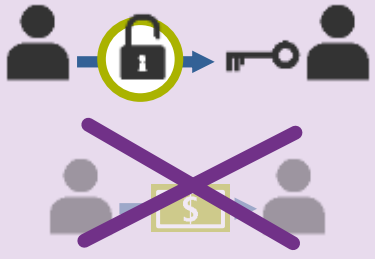
OLD TRANSACTION Y

Value
Output script = $Output_1$ C

Value
Output script = $Output_2$ C

.

Defines how that output can be spent (and by whom): Money does not change the owner but the PERMISSION to use it.



Transaction

Includes chaincode script that determines

1. Validation rules
2. How the global state is mutated

NEW TRANSACTION

Output reference
Signature script = Input$_1$

Output reference
Signature script = Input$_2$

Output reference
Signature script = Input$_n$

Reference to
an output of
the old transaction

OLD TRANSACTION G

OLD TRANSACTION X

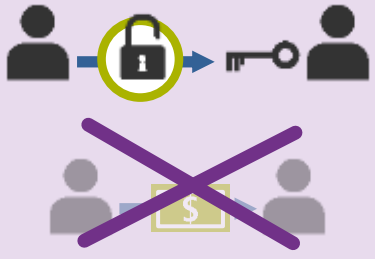
Value
Output script = Output$_1$

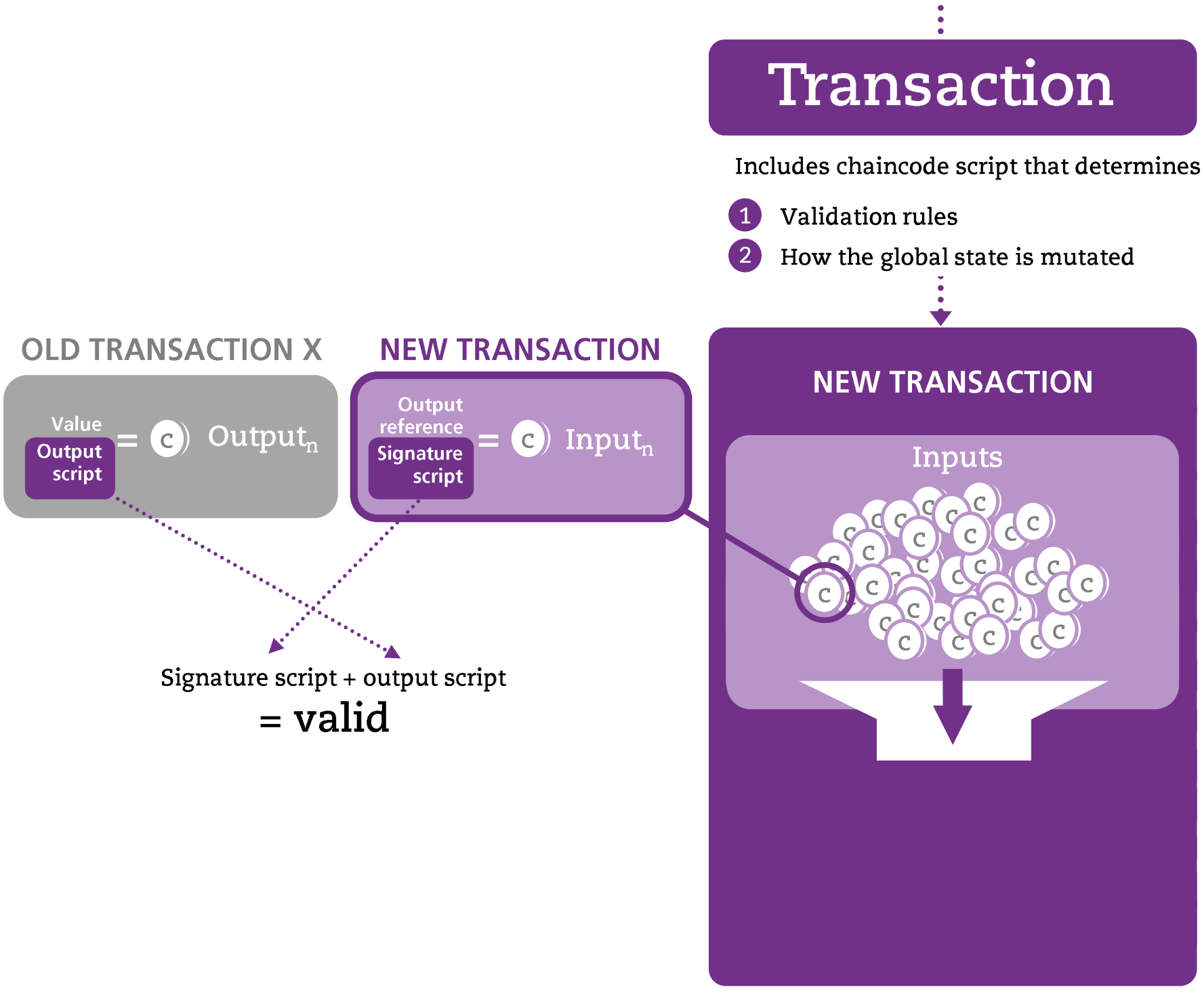
OLD TRANSACTION Y

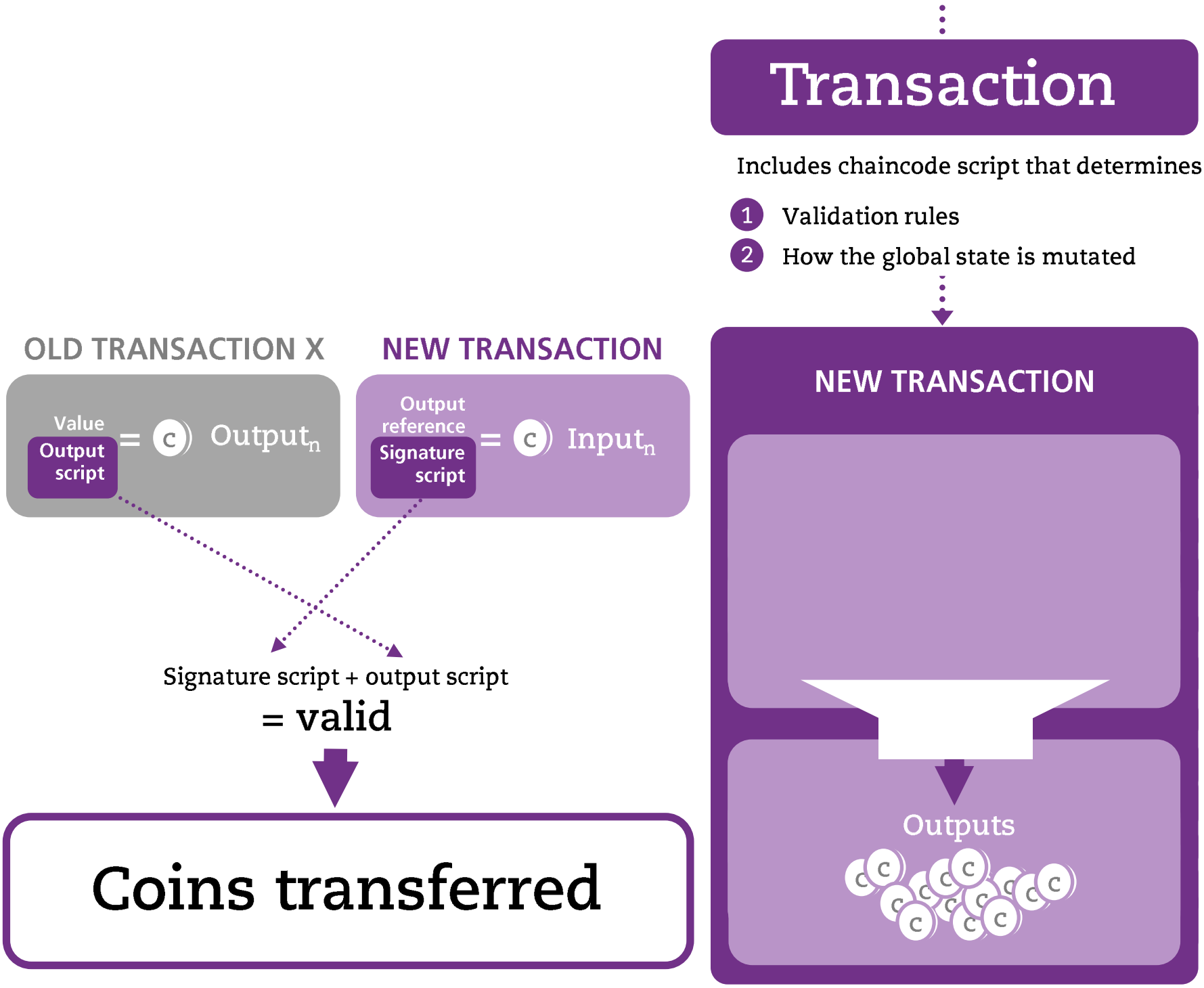
Value
Output script = Output$_1$

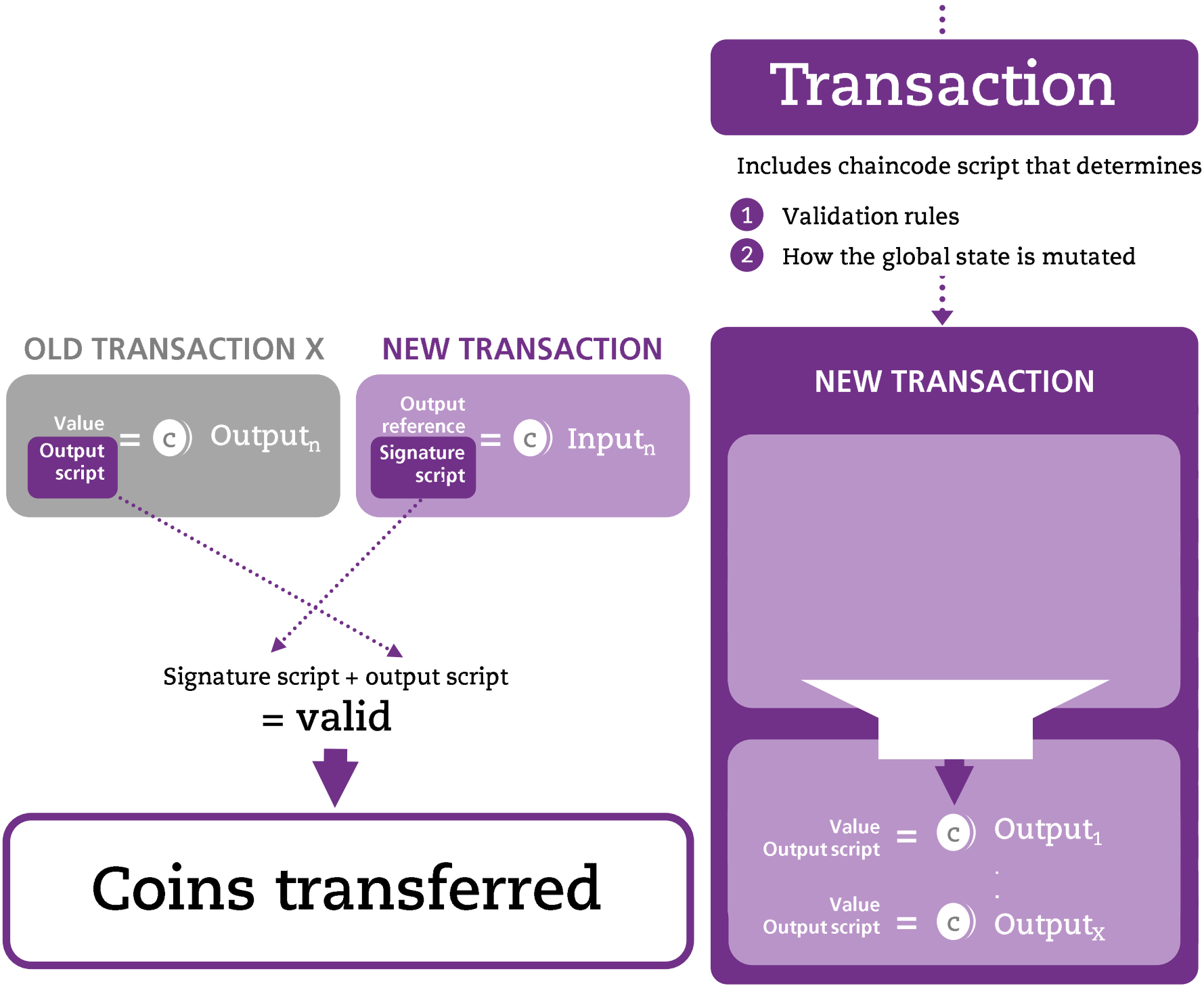
Value
Output script = Output$_2$

Defines how that
output can be spent
(and by whom):
Money does not change
the owner but the
PERMISSION to use it.




Transaction
Includes chaincode script that determines
1 Validation rules
2 How the global state is mutated
OLD TRANSACTION X
NEW TRANSACTION
Value
Output script
= Output$_n$
Output reference
Signature script
= Input$_n$
NEW TRANSACTION
Inputs
Signature script + output script
= valid


Transaction
Includes chaincode script that determines
1 Validation rules
2 How the global state is mutated
OLD TRANSACTION X
NEW TRANSACTION
Value
Output script
= C Output$_n$
Output reference
Signature script
= C Input$_n$
Signature script + output script
= valid
Coins transferred
NEW TRANSACTION
Outputs


Transaction
Includes chaincode script that determines
1 Validation rules
2 How the global state is mutated
OLD TRANSACTION X
NEW TRANSACTION
Value
Output script
= c Output$_n$
Output reference
Signature script
= c Input$_n$
Signature script + output script
= valid
Coins transferred
NEW TRANSACTION
Value
Output script
= c Output$_1$
Value
Output script
= c Output$_x$