Storing Transactions in Blocks

Stephen Haunts
LEADER, DEVELOPER, SPEAKER AND TRAINER

@stephenhaunts www.stephenhaunts.com

Overview

Blocks with a single transaction

Blocks with multiple transactions

Transaction pools, HMAC and digital signatures

Block versioning

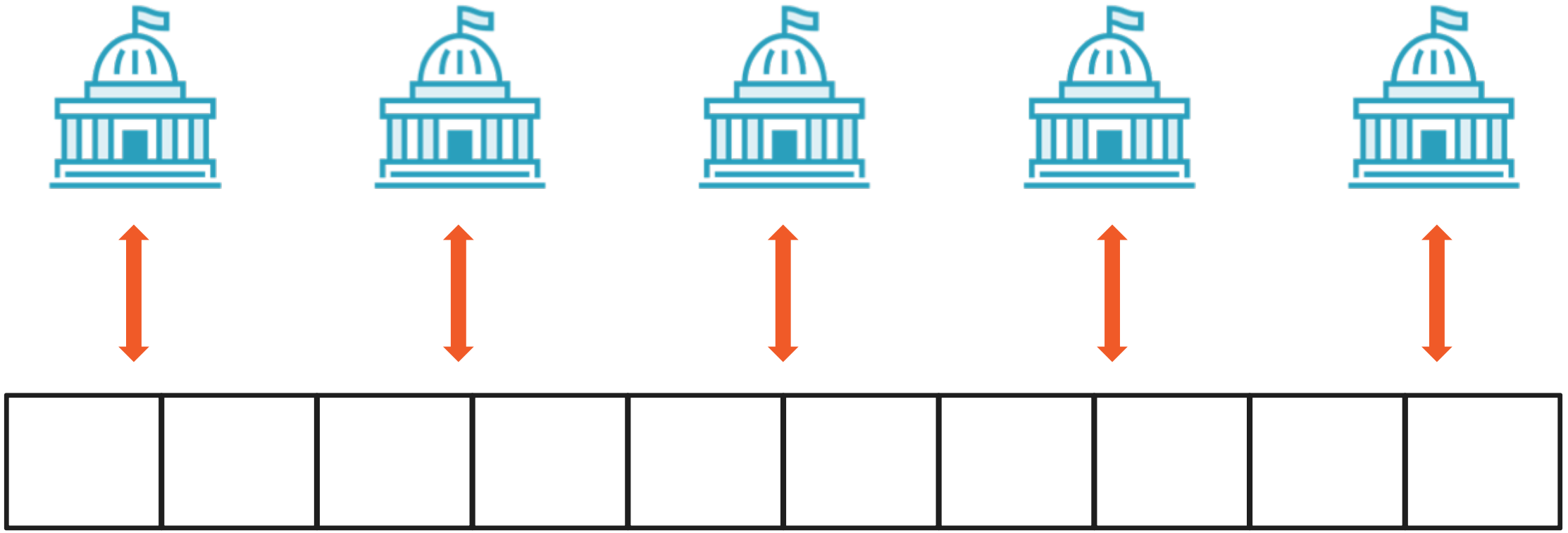

Theory
Practice


Non-developers welcome!


stephenhaunts — BlockWithProofOfWork.dll — -bash — 113×24
Difficulty Level 3 - Nonce = 891969 - Elapsed = 00:00:01.24 - 000Qil4yJtclAq6zfAoaJqBpsUTjWmdLT7+D+6AI9g0=
Difficulty Level 3 - Nonce = 43429 - Elapsed = 00:00:00.06 - 000a70JZc6M3TnorqSXrtCoVFVf9FWoQXmB+j8jSWD4=
Difficulty Level 3 - Nonce = 66050 - Elapsed = 00:00:00.10 - 000F4IiLEIsOxTcPq+xJBBr0+OmkSCg9/z08cNZz+2M=
Difficulty Level 3 - Nonce = 14904 - Elapsed = 00:00:00.02 - 000QqAK7+TcJBk56vv57ce4Zd66Nd/BNO7hzM2hBrfk=
Block Number 0 : PASS VERIFICATION
Block Number 1 : PASS VERIFICATION
Block Number 2 : PASS VERIFICATION
Block Number 3 : PASS VERIFICATION
Blockchain integrity intact.
Block Number 0 : PASS VERIFICATION
Block Number 1 : FAILED VERIFICATION
Block Number 1 : Invalid Digital Signature
Block Number 2 : FAILED VERIFICATION
Block Number 2 : Invalid Digital Signature
Block Number 3 : FAILED VERIFICATION
Block Number 3 : Invalid Digital Signature
Blockchain integrity NOT intact.
Press any key to continue...

.NET Standard 2.0 & .NET Core 2.0

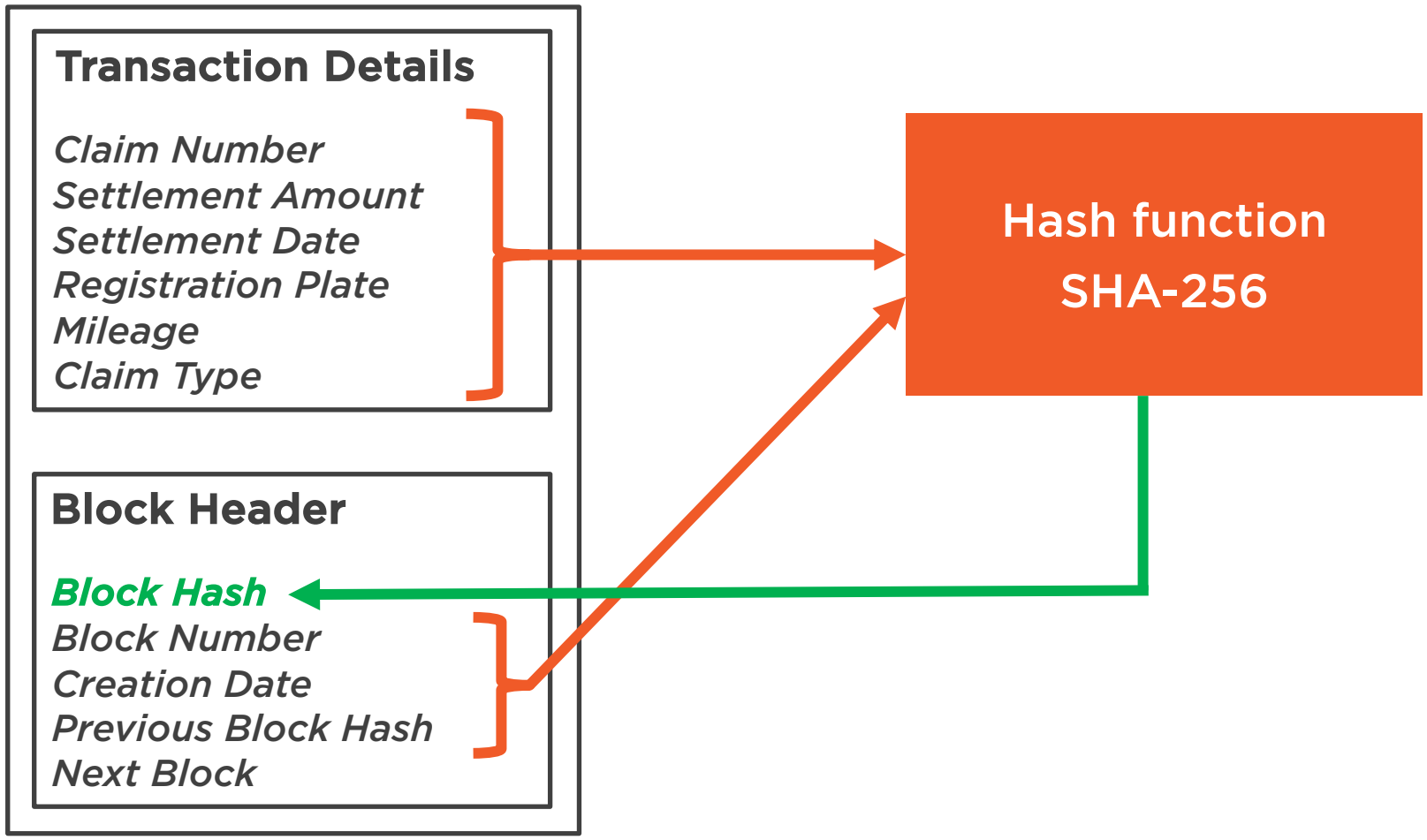
Visual Studio 2017 on Windows
Visual Studio for Mac
JetBrains Rider
Visual Studio Code


Blockchain

Globomantics Data to Record

- Claim number
- Settlement amount
- Settlement date
- Car registration
- Mileage
- Claim type

Blocks with a Single Transaction


Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block
Hash function
SHA-256

Transaction Details

Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type

Block Header

Block Number
Block Hash
Creation Date
Previous Block Hash
Next Block

Transaction Details

Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type

Block Header

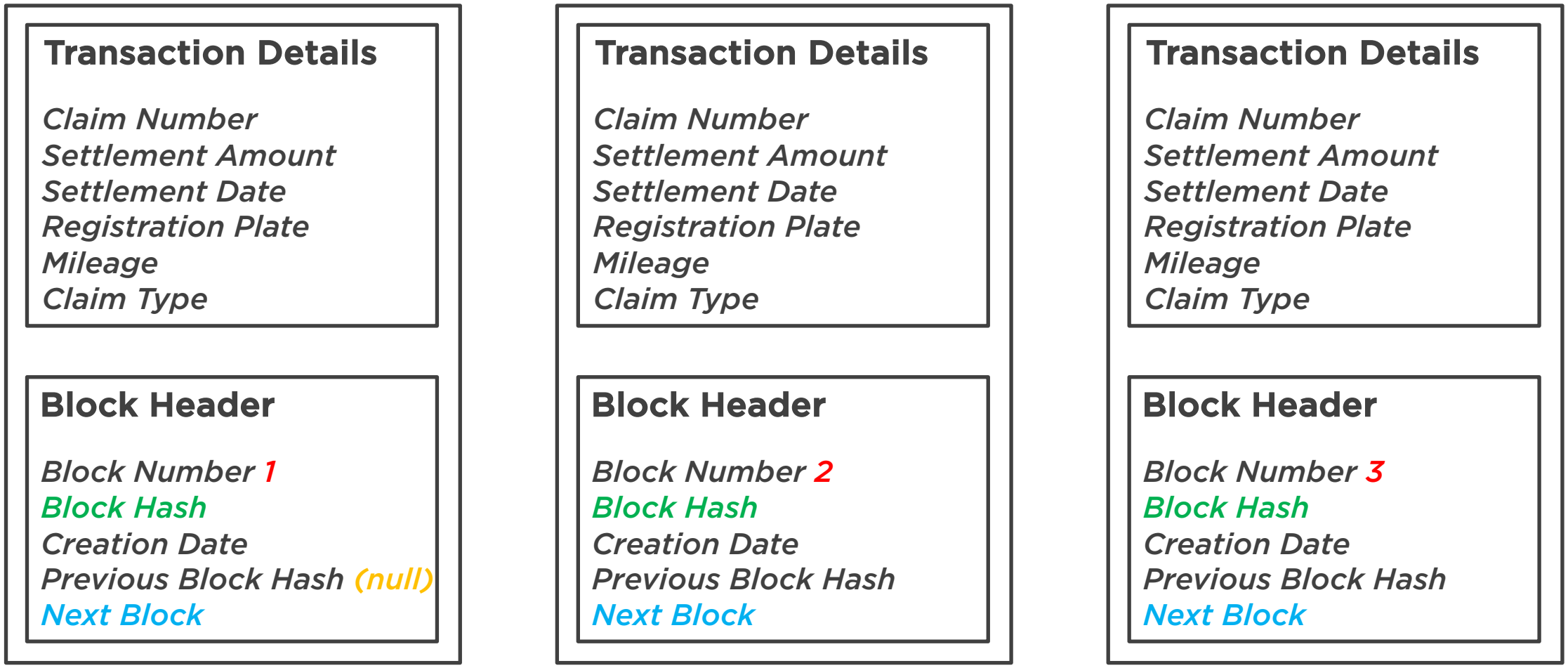
Block Number
Block Hash
Creation Date
Previous Block Hash
Next Block

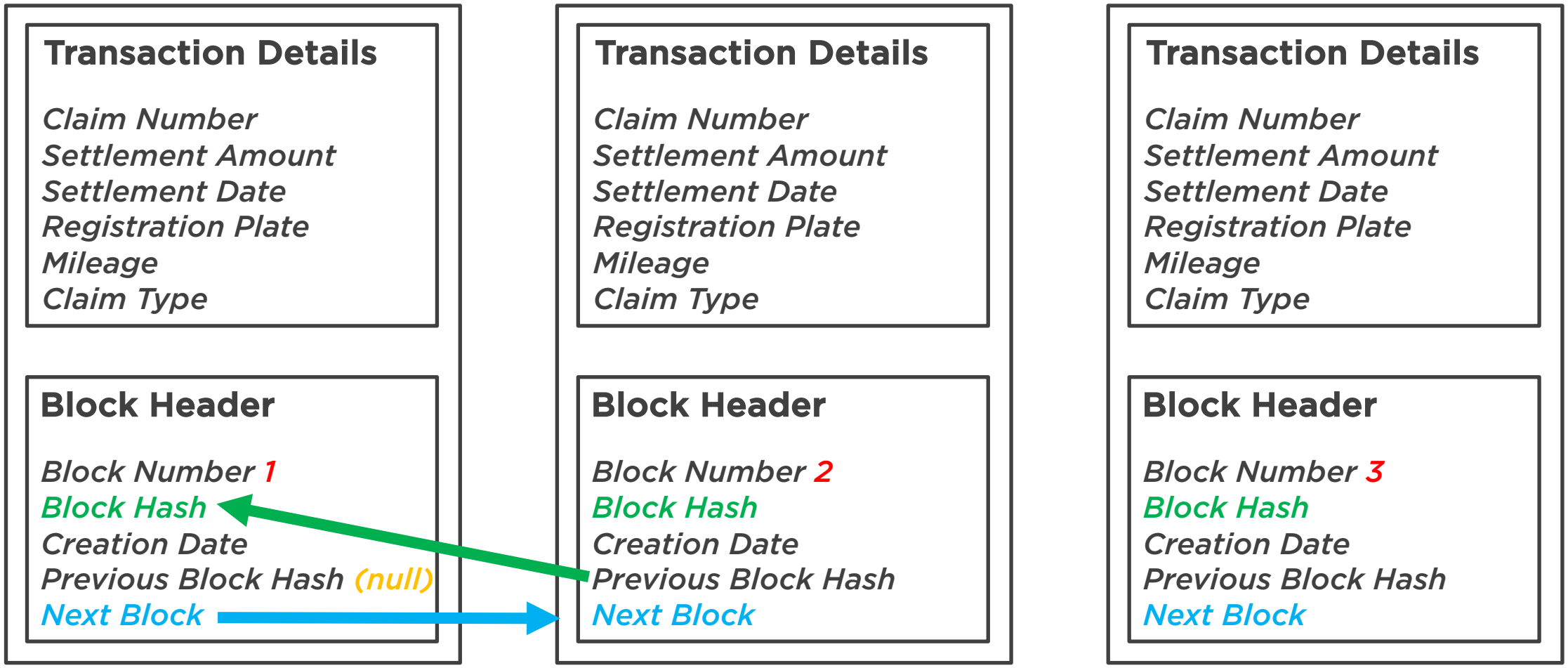
Transaction Details

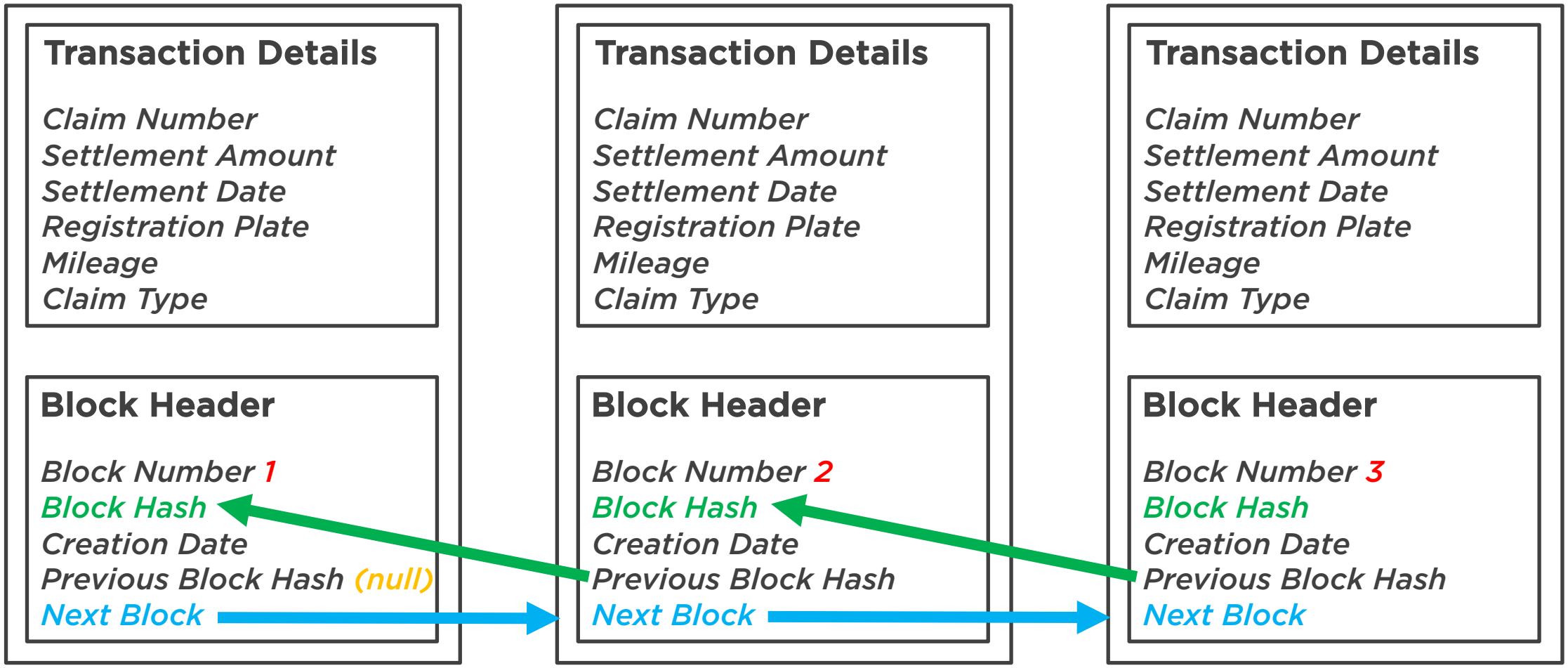
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type

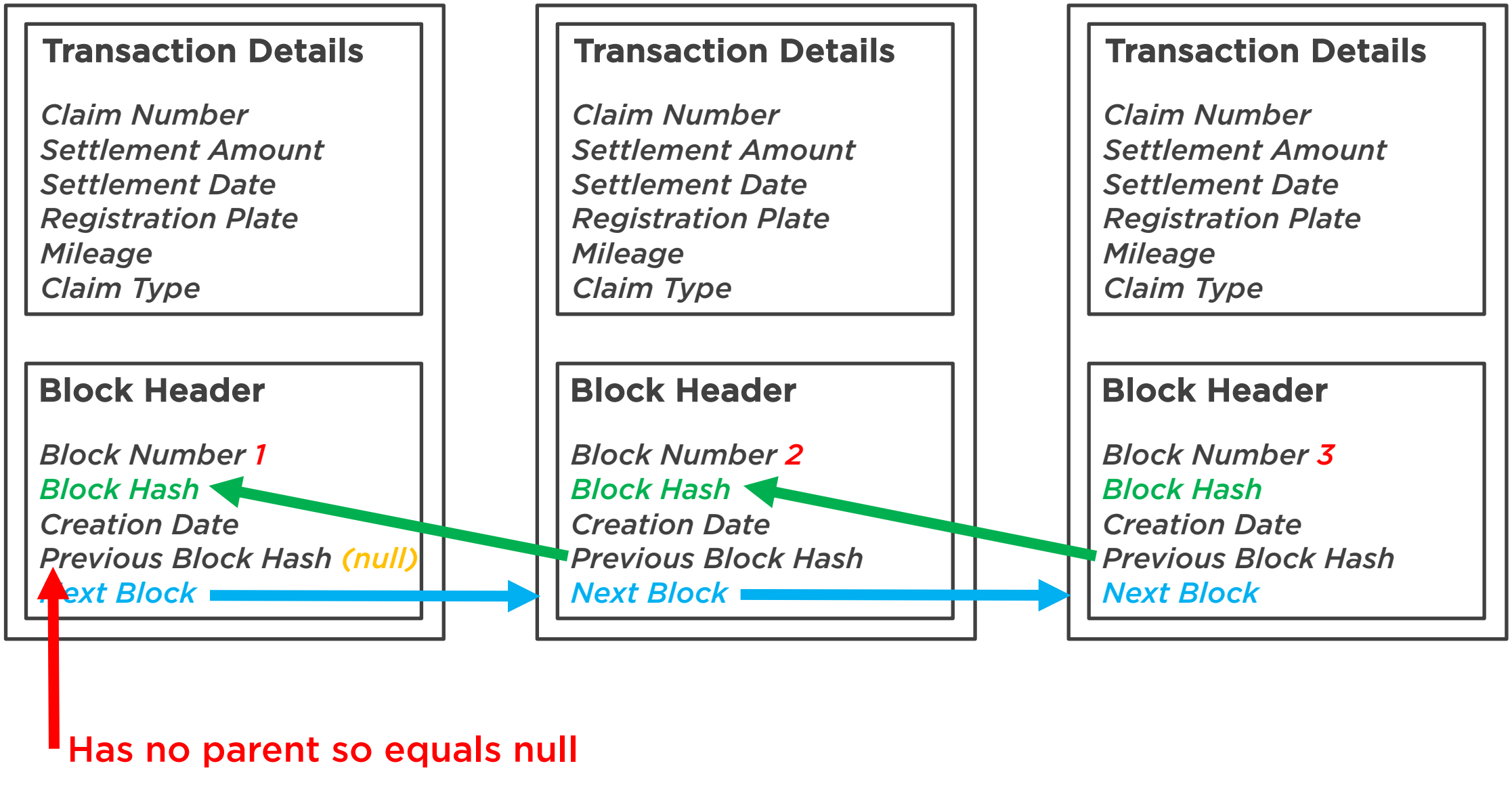
Block Header

Block Number
Block Hash
Creation Date
Previous Block Hash
Next Block

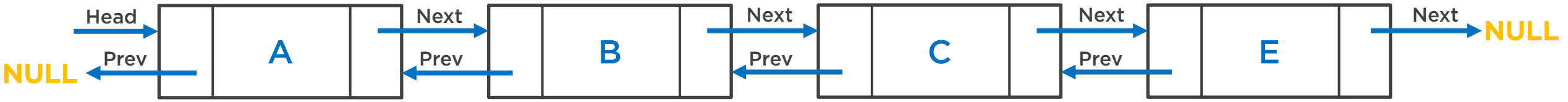

Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 1
Block Hash
Creation Date
Previous Block Hash (null)
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 2
Block Hash
Creation Date
Previous Block Hash
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 3
Block Hash
Creation Date
Previous Block Hash
Next Block


Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 1
Block Hash
Creation Date
Previous Block Hash (null)
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 2
Block Hash
Creation Date
Previous Block Hash
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 3
Block Hash
Creation Date
Previous Block Hash
Next Block

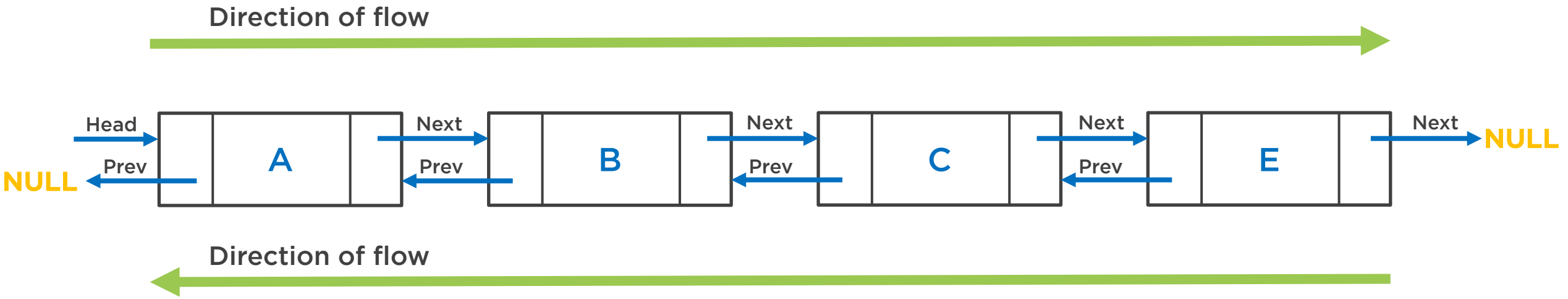

Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 1
Block Hash
Creation Date
Previous Block Hash (null)
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 2
Block Hash
Creation Date
Previous Block Hash
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 3
Block Hash
Creation Date
Previous Block Hash
Next Block


Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 1
Block Hash
Creation Date
Previous Block Hash (null)
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 2
Block Hash
Creation Date
Previous Block Hash
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 3
Block Hash
Creation Date
Previous Block Hash
Next Block
Has no parent so equals null

Double Linked List



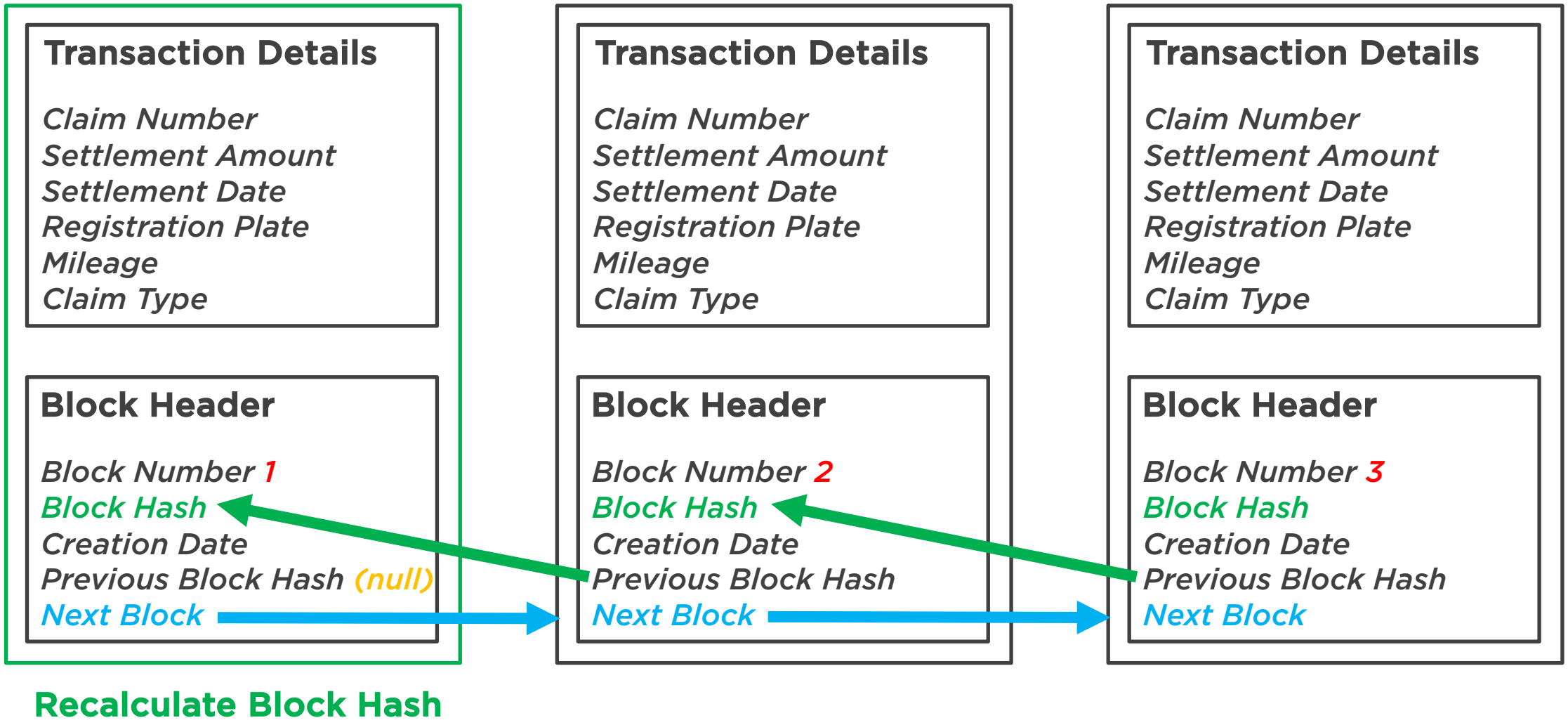
Double Linked List



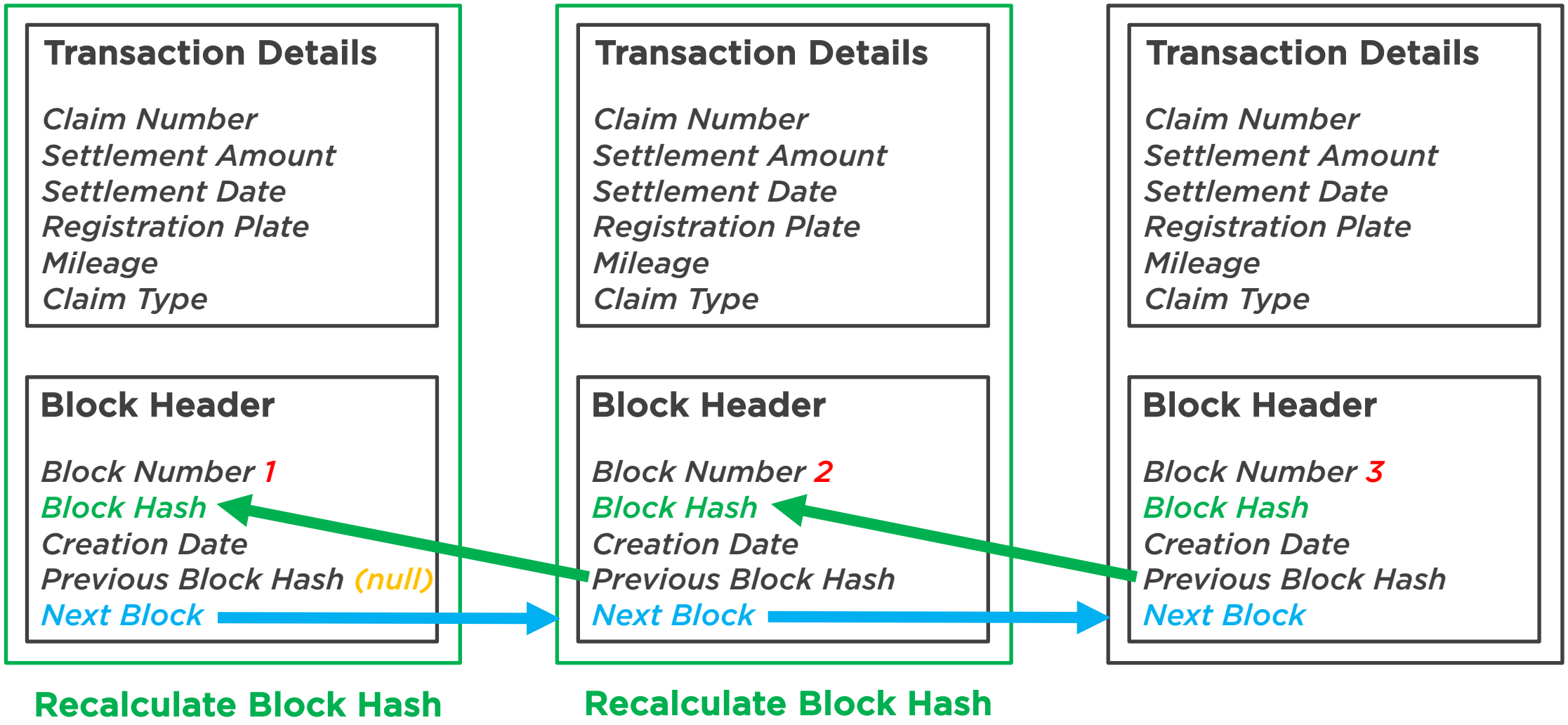
Blockchain flows in one direction


confirm
substantiate
prove
verify
justify
attest
check
clarify
inspect
document
authen
cate

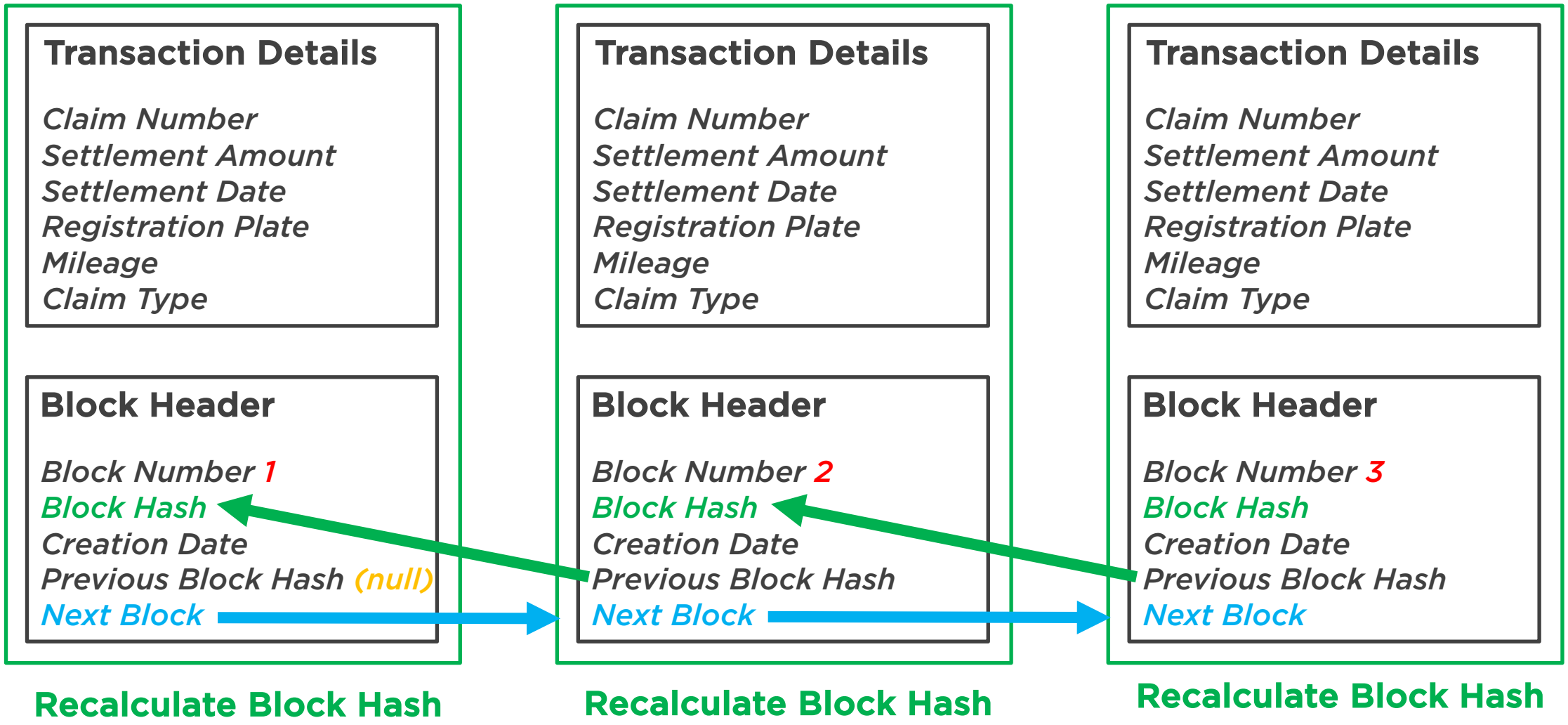
Happy Path


Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 1
Block Hash
Creation Date
Previous Block Hash (null)
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 2
Block Hash
Creation Date
Previous Block Hash
Next Block
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 3
Block Hash
Creation Date
Previous Block Hash
Next Block
Recalculate Block Hash

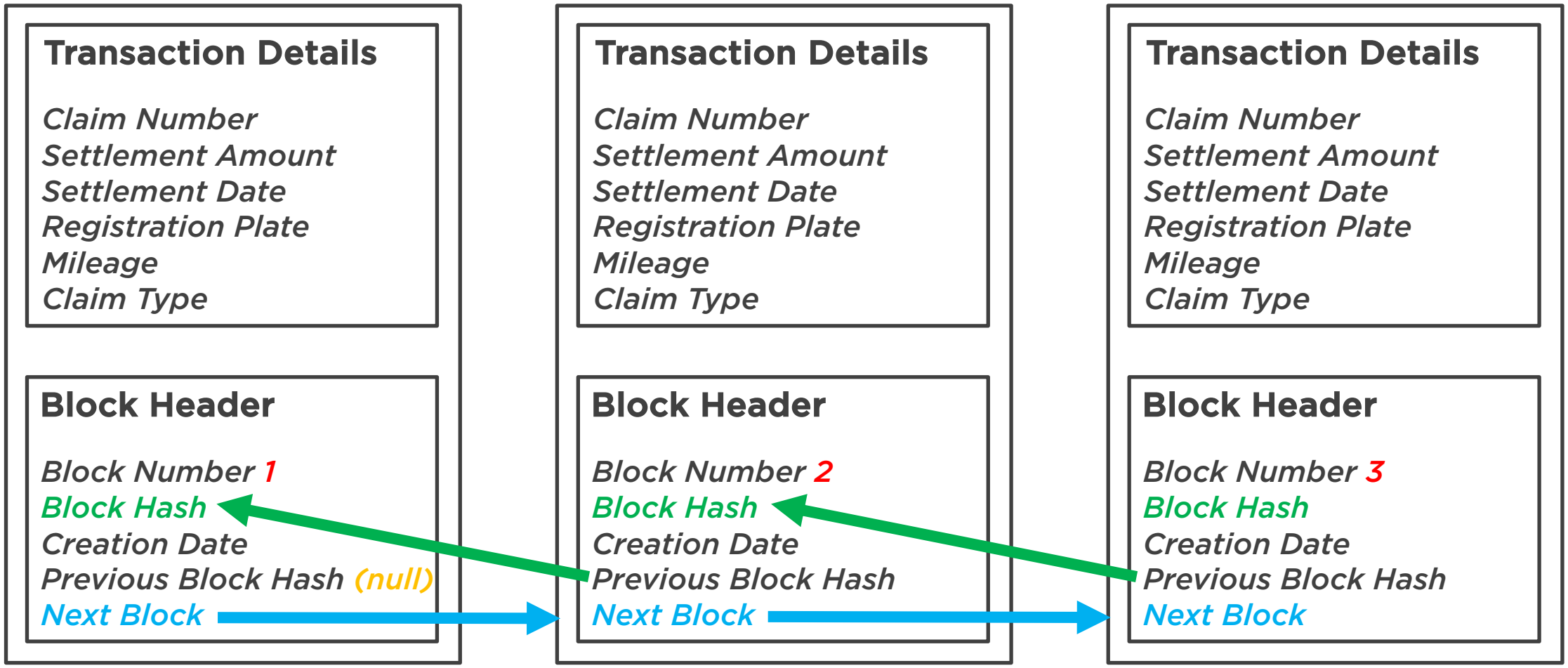
Happy Path


Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 1
Block Hash
Creation Date
Previous Block Hash (null)
Next Block
Recalculate Block Hash
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 2
Block Hash
Creation Date
Previous Block Hash
Next Block
Recalculate Block Hash
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 3
Block Hash
Creation Date
Previous Block Hash
Next Block

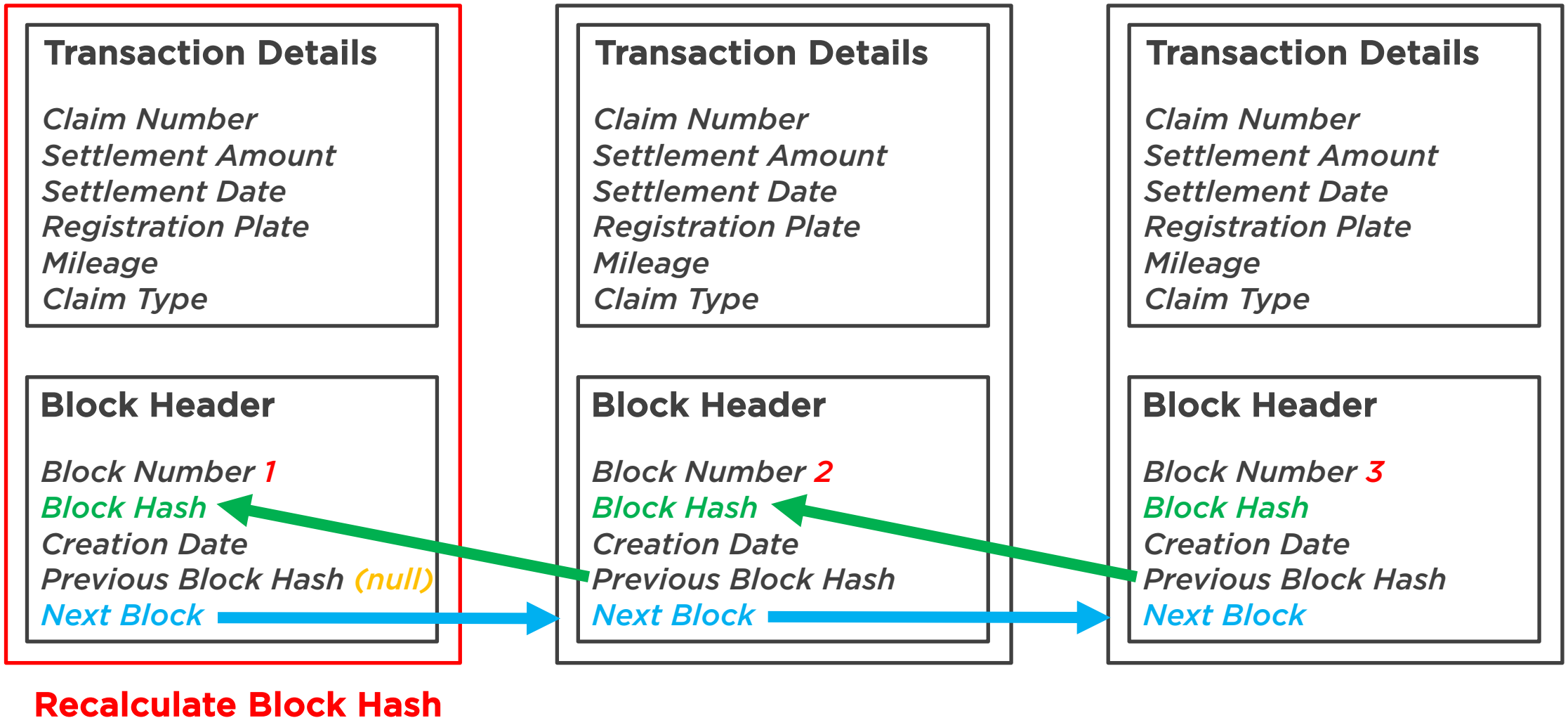
Happy Path


Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 1
Block Hash
Creation Date
Previous Block Hash (null)
Next Block
Recalculate Block Hash
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 2
Block Hash
Creation Date
Previous Block Hash
Next Block
Recalculate Block Hash
Transaction Details
Claim Number
Settlement Amount
Settlement Date
Registration Plate
Mileage
Claim Type
Block Header
Block Number 3
Block Hash
Creation Date
Previous Block Hash
Next Block
Recalculate Block Hash

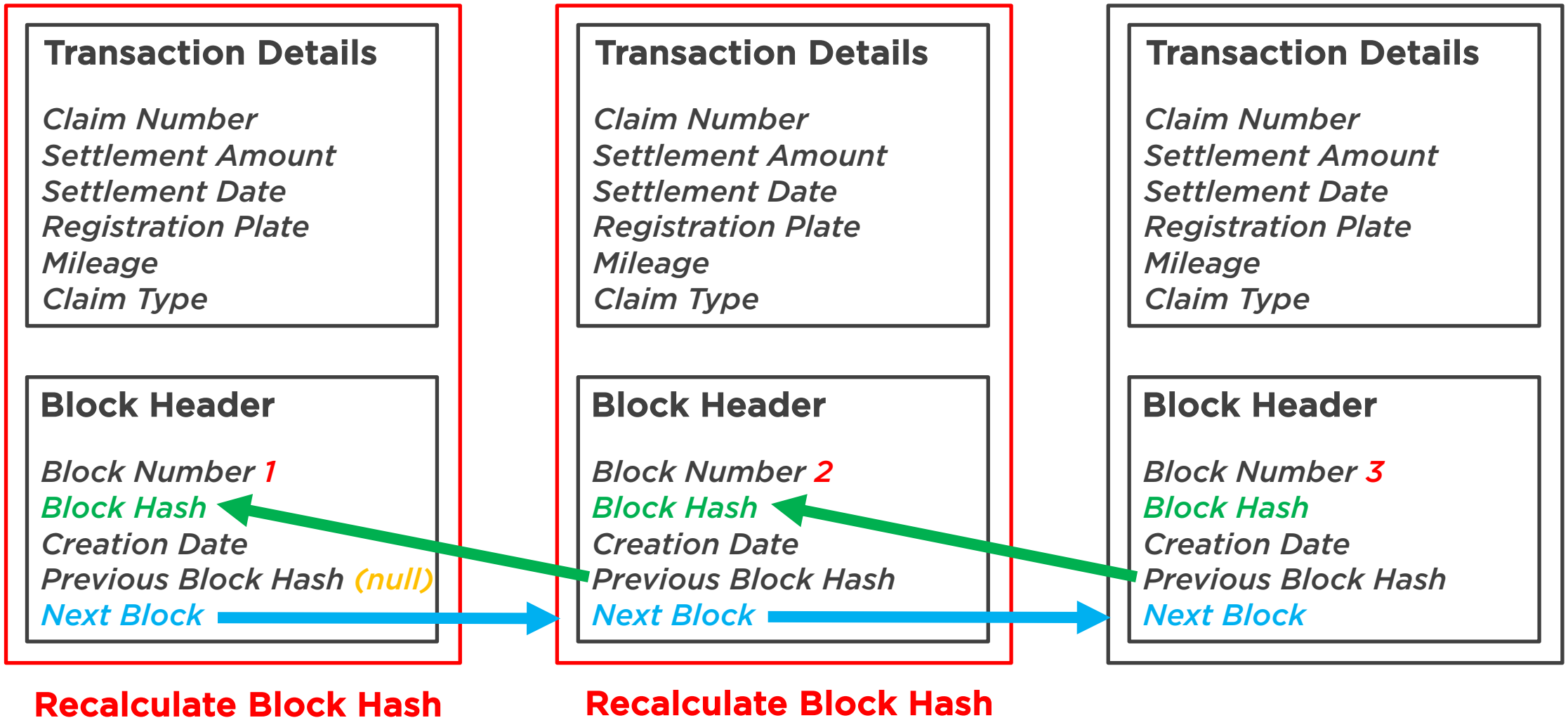
Verification Failure



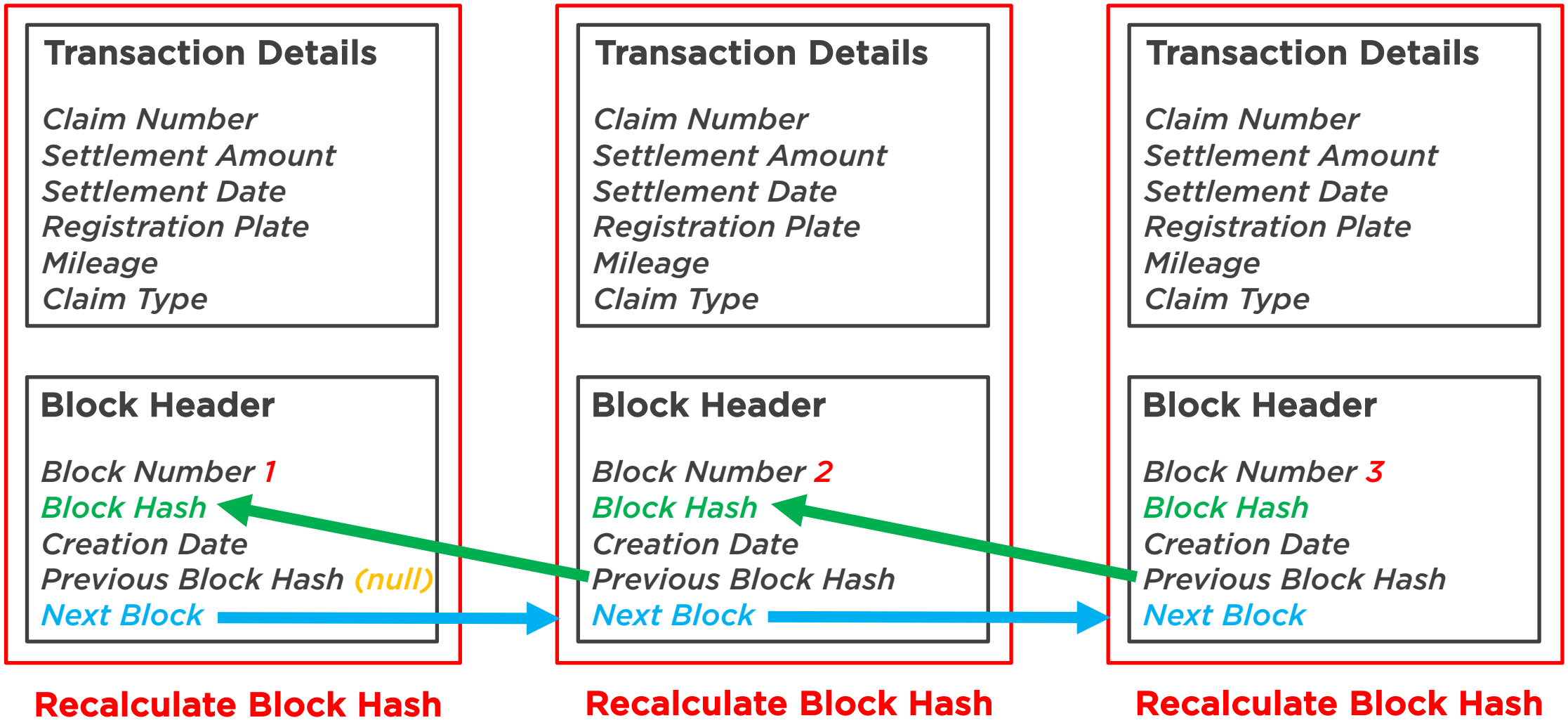
Verification Failure



Verification Failure



Verification Failure



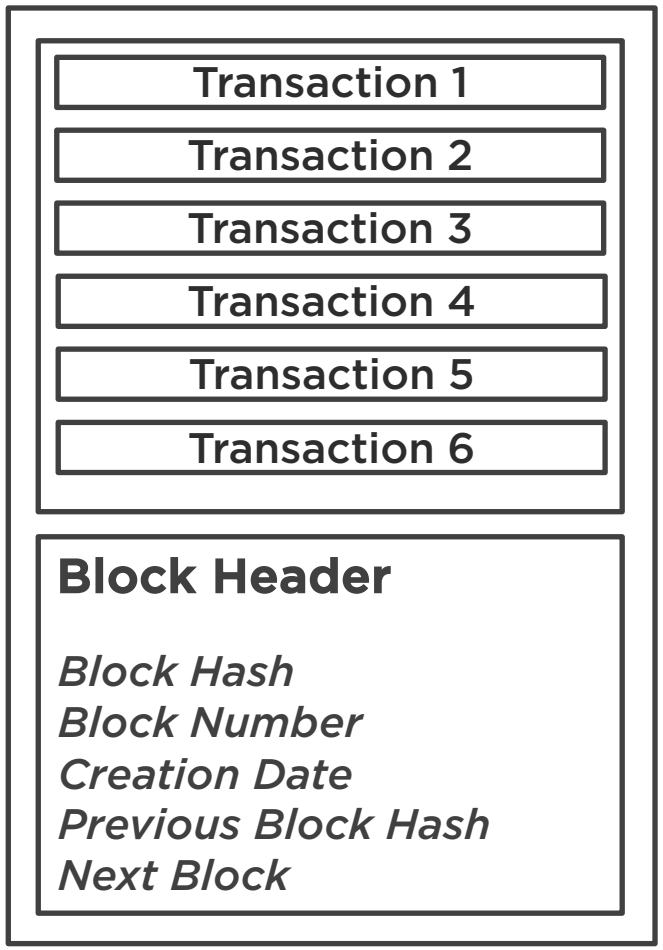
Demo

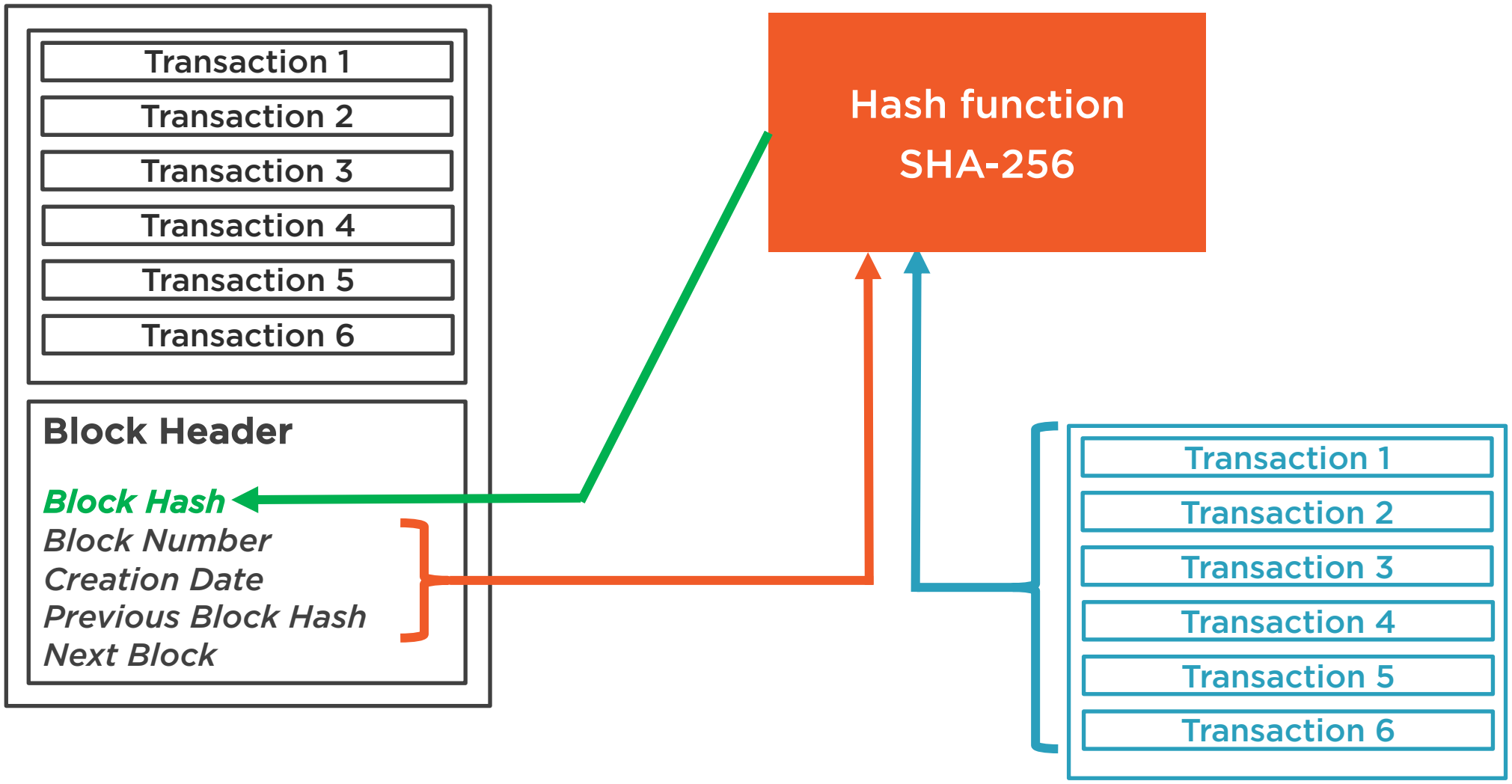
.NET Standard 2.0+ & .NET Core 2.0+

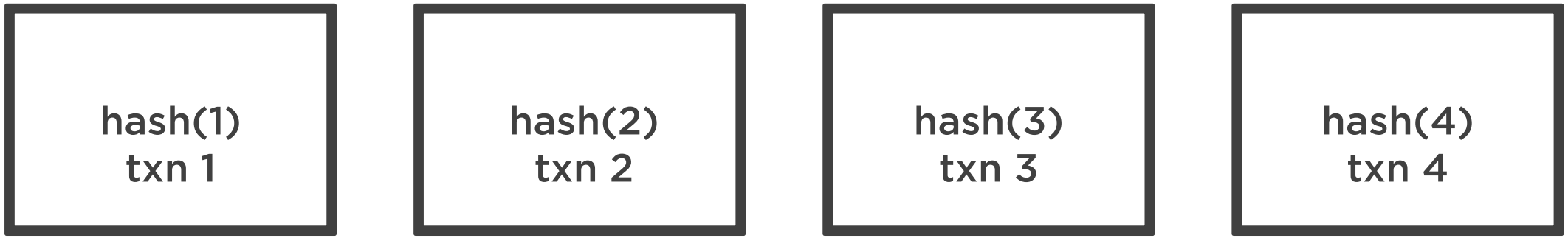
Cross platform

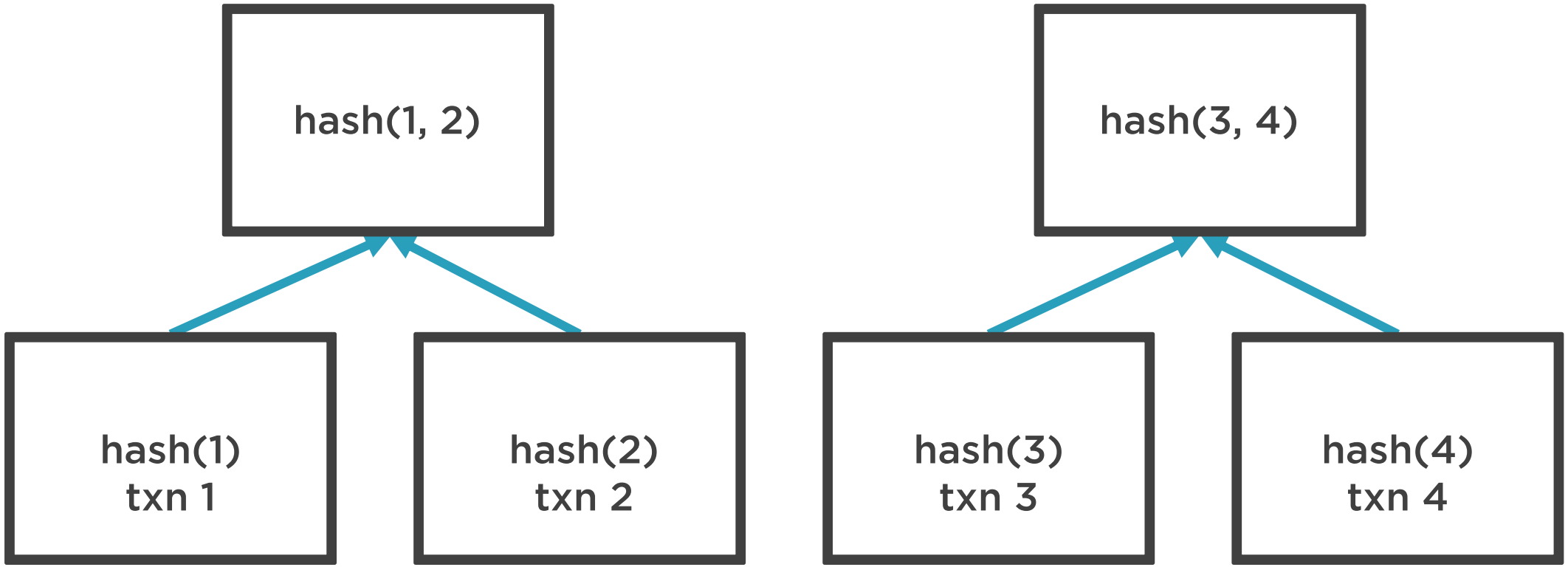
Demos in Visual Studio for Mac

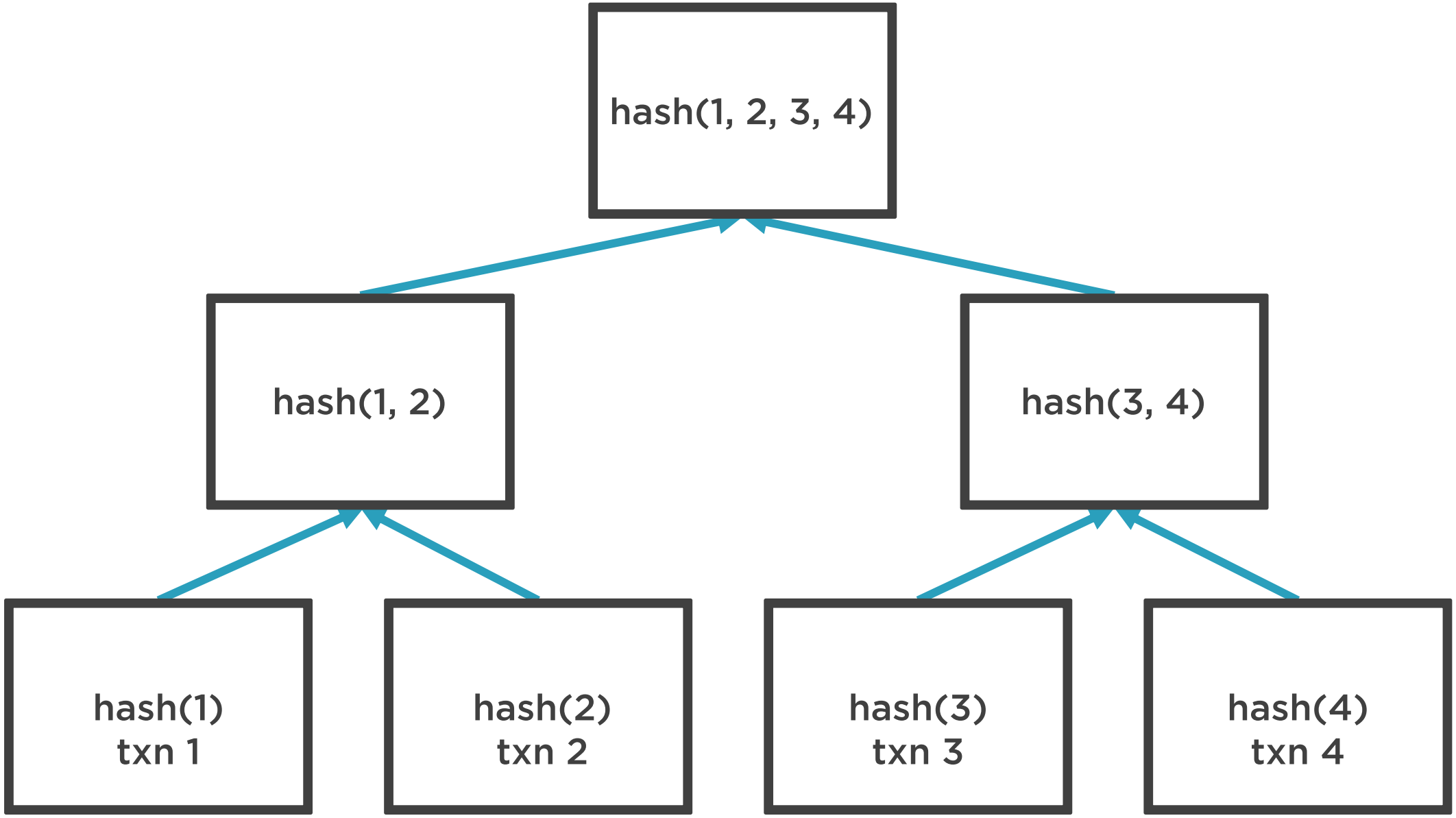
Blocks with Multiple Transactions

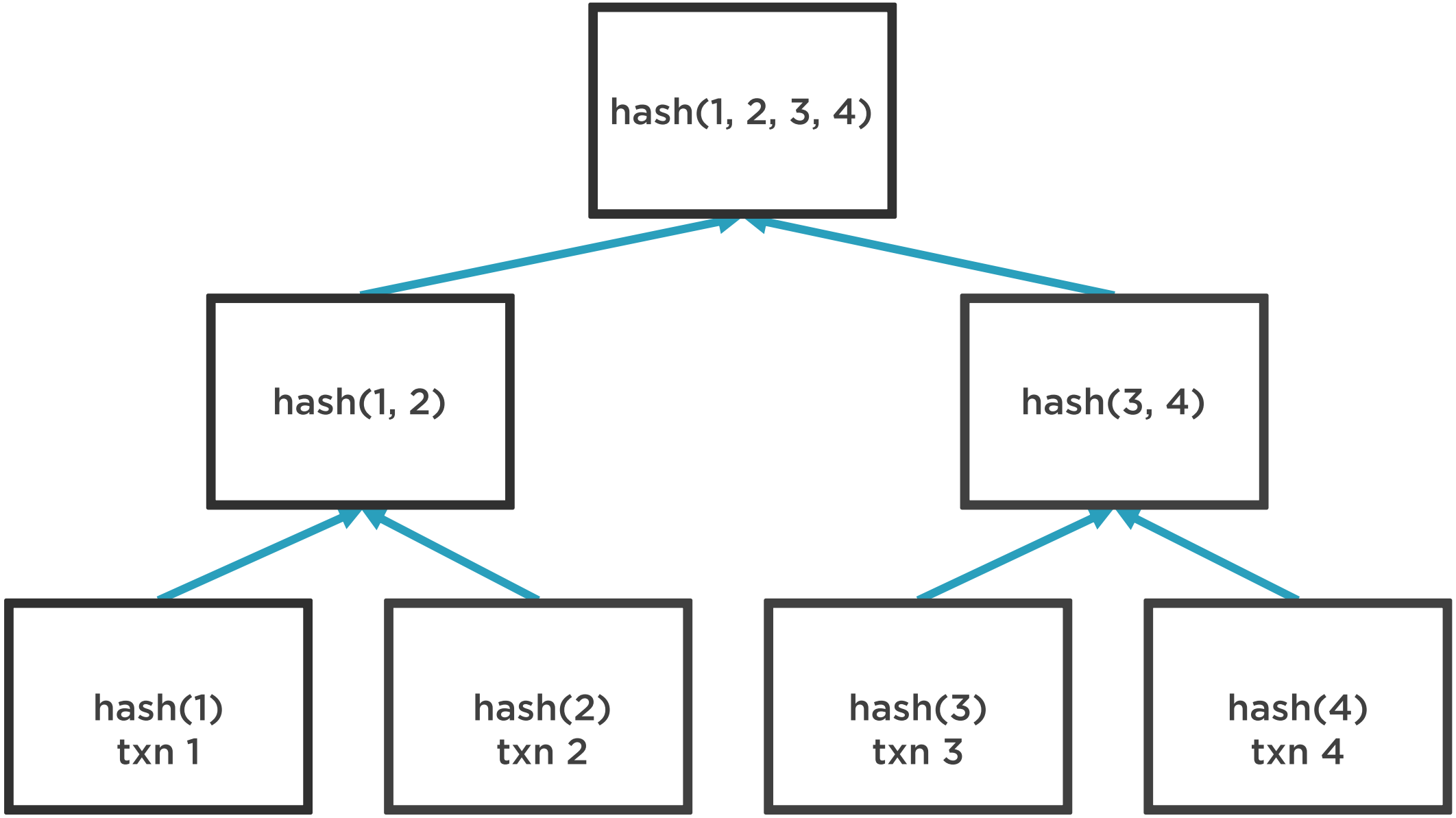

Transaction 1
Transaction 2
Transaction 3
Transaction 4
Transaction 5
Transaction 6
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block

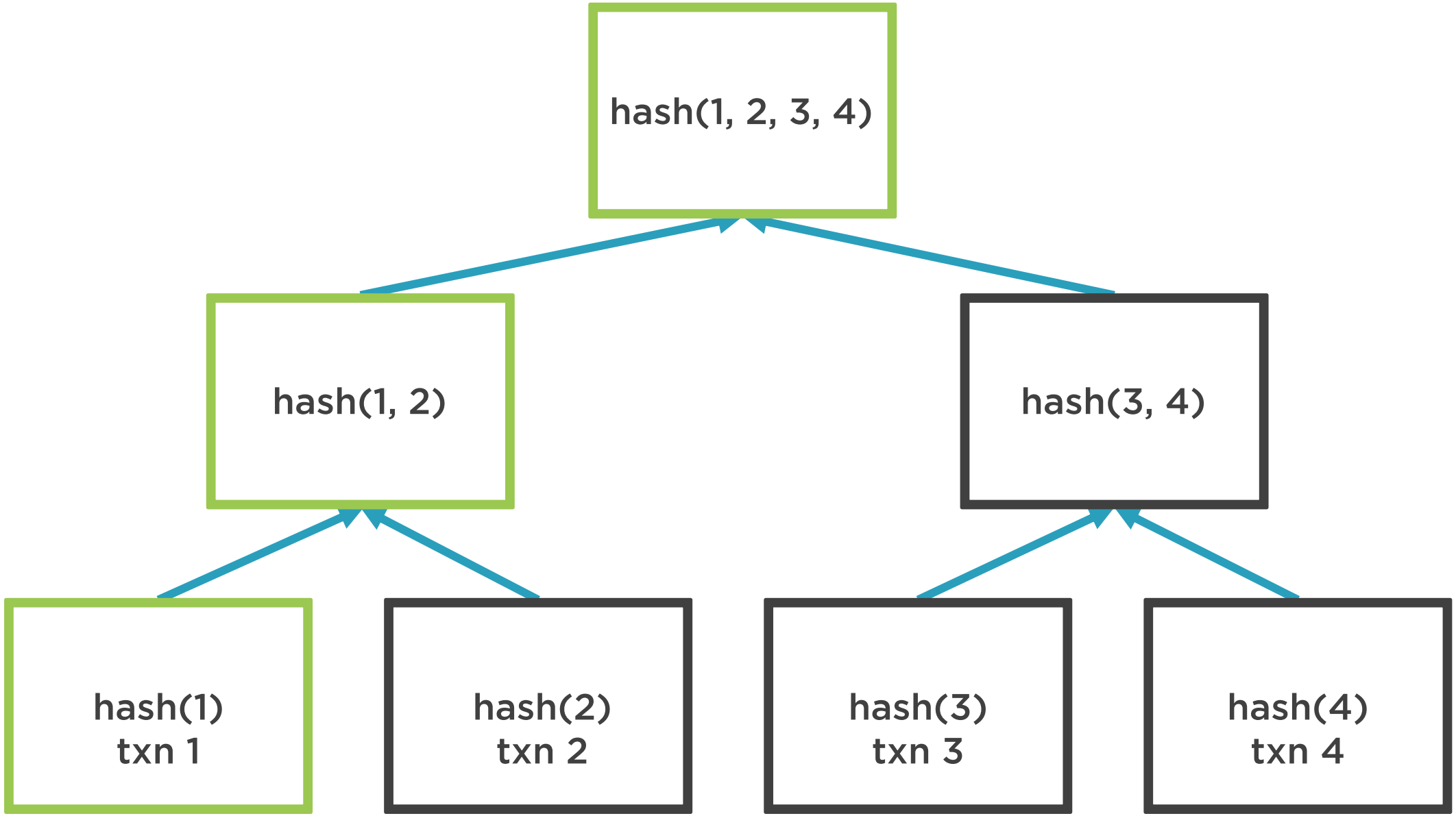

Transaction 1
Transaction 2
Transaction 3
Transaction 4
Transaction 5
Transaction 6
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block
Hash function
SHA-256
Transaction 1
Transaction 2
Transaction 3
Transaction 4
Transaction 5
Transaction 6

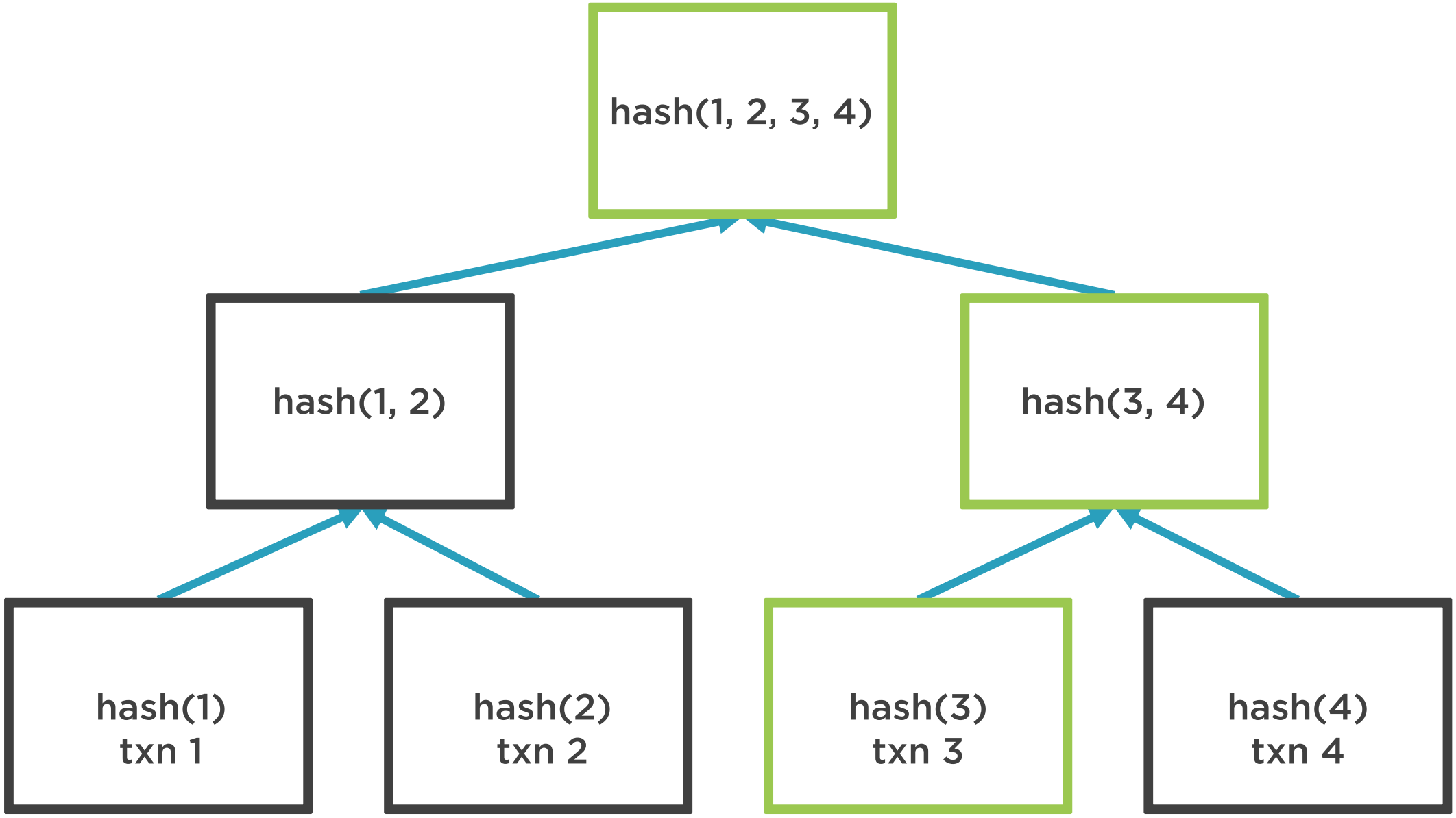

hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 4

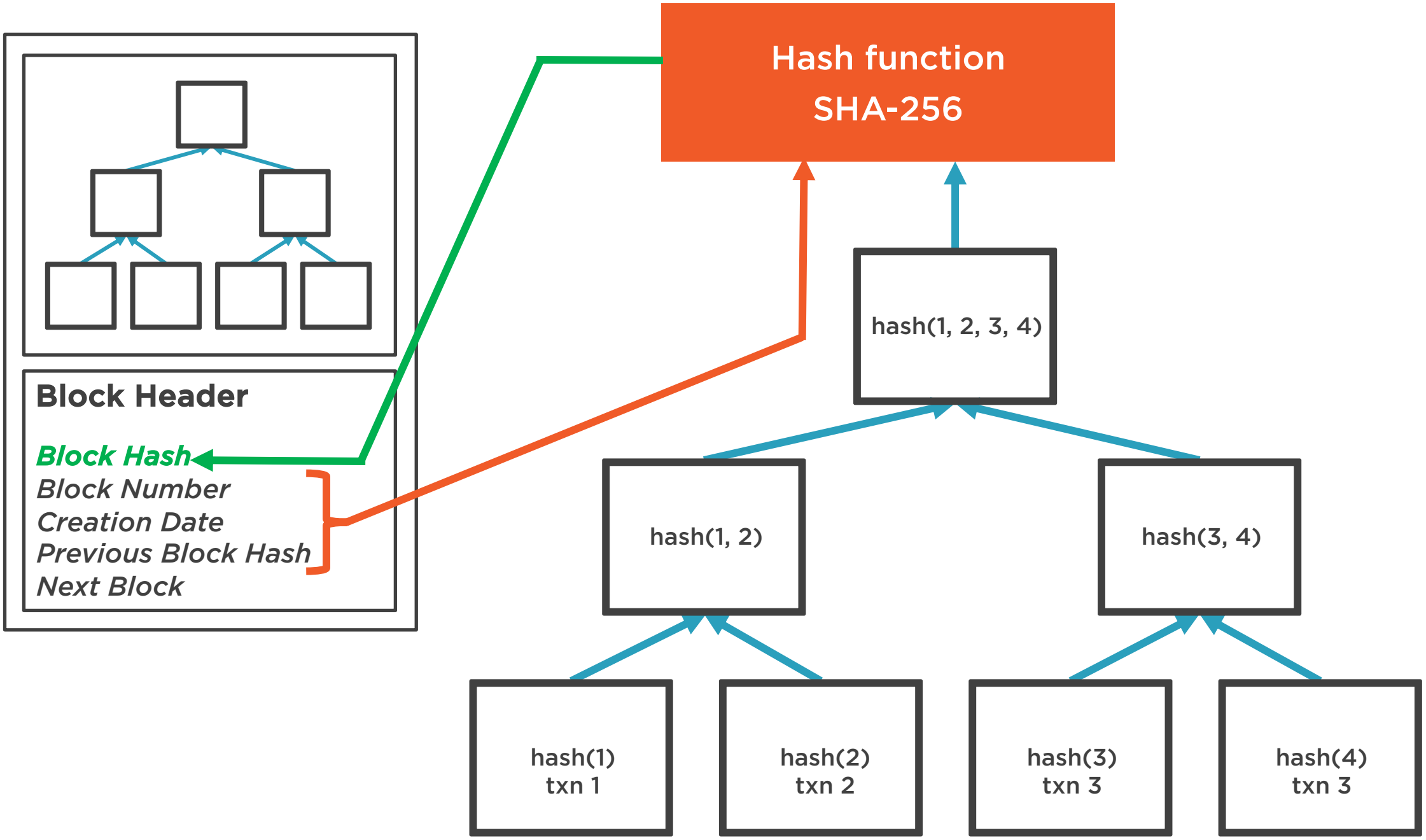

hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 4


hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 4


hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 4


hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 4


hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 4


Hash function
SHA-256
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block
hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 3

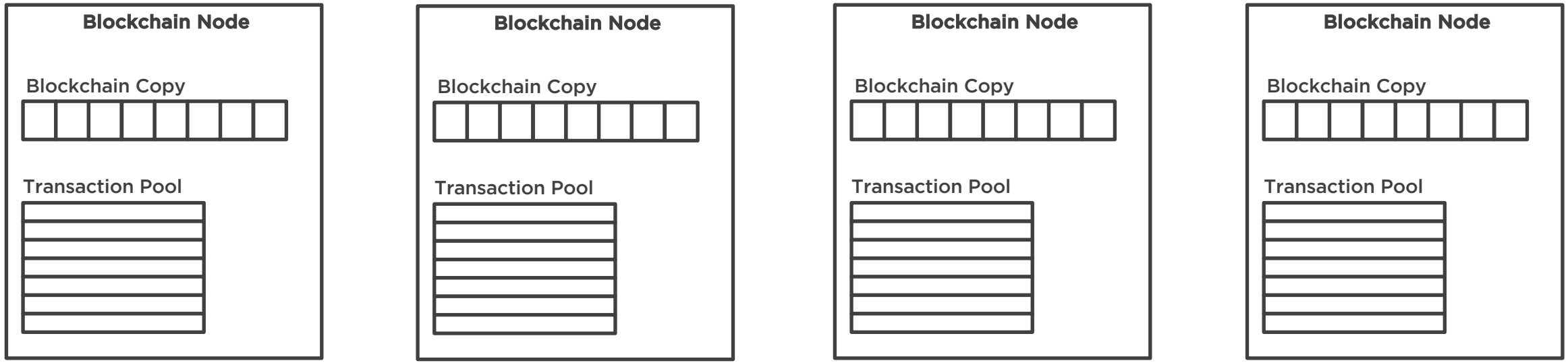
Demo

Incorporate a Merkle tree

We will use an open source Merkle tree

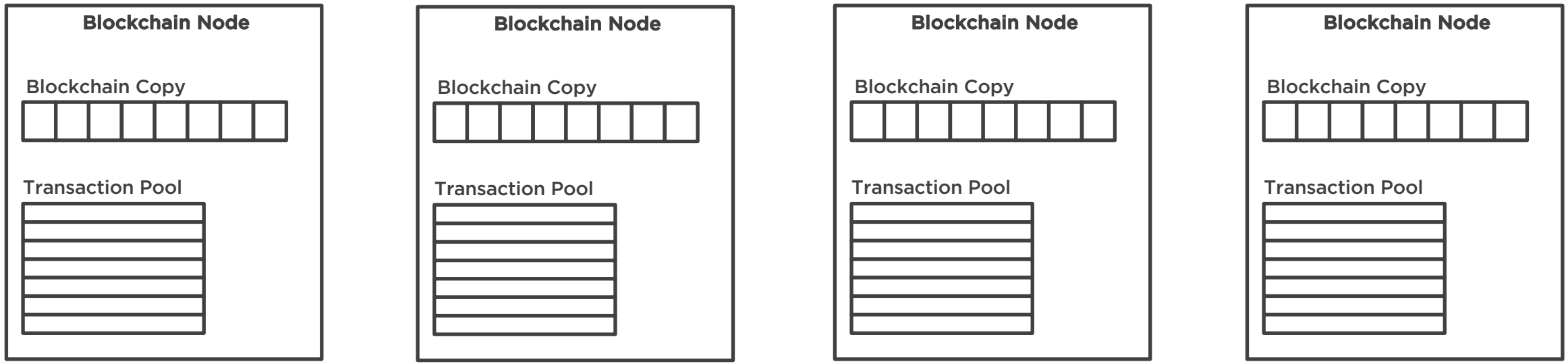
Transaction Pools, Authenticated Hashes and Digital Signatures

Public Fully Distributed Blockchain



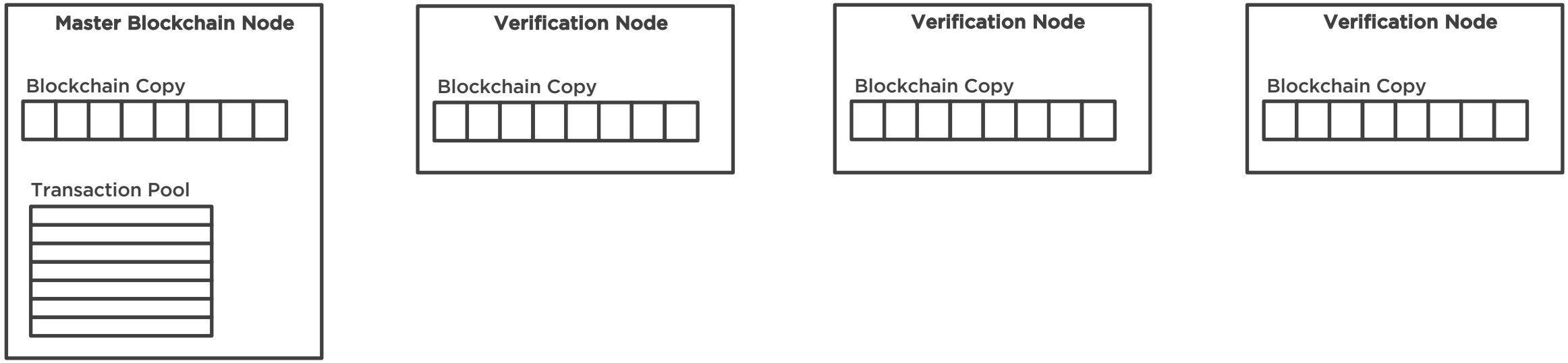
Complete copy of the Blockchain
Complete list of transactions
Transactions sent between all nodes

Private Fully Distributed Blockchain



Same as public Blockchain but access limited
Complete copy of the Blockchain
Complete list of transactions
Transactions sent between all nodes

Private Partial Distributed Blockchain



Transactions managed by central authority
Central authority creates blocks
Nodes contain complete copy of the Blockchain
Nodes perform verification of chain copy

Adding Authentication

Confidentiality

Integrity

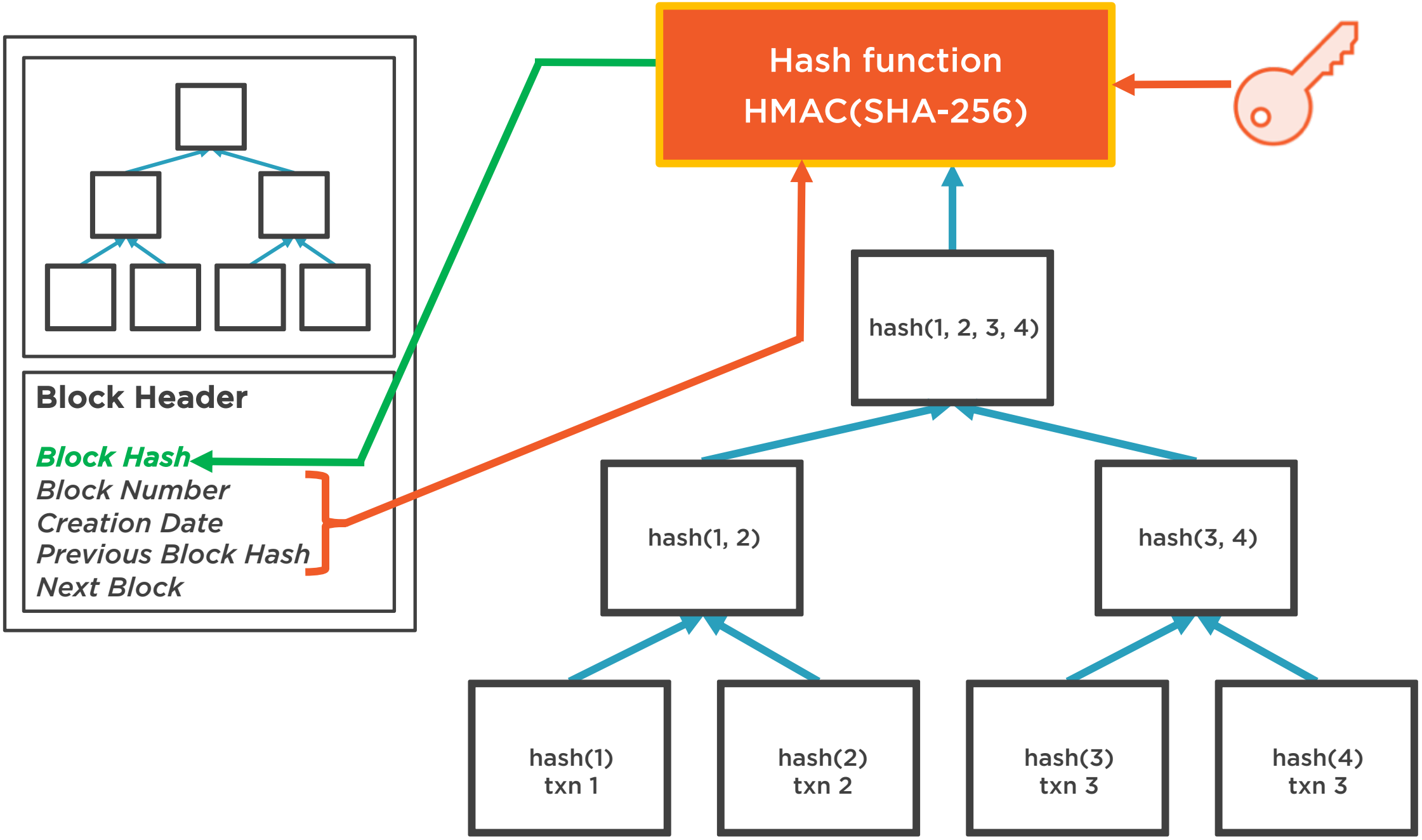
Authentication

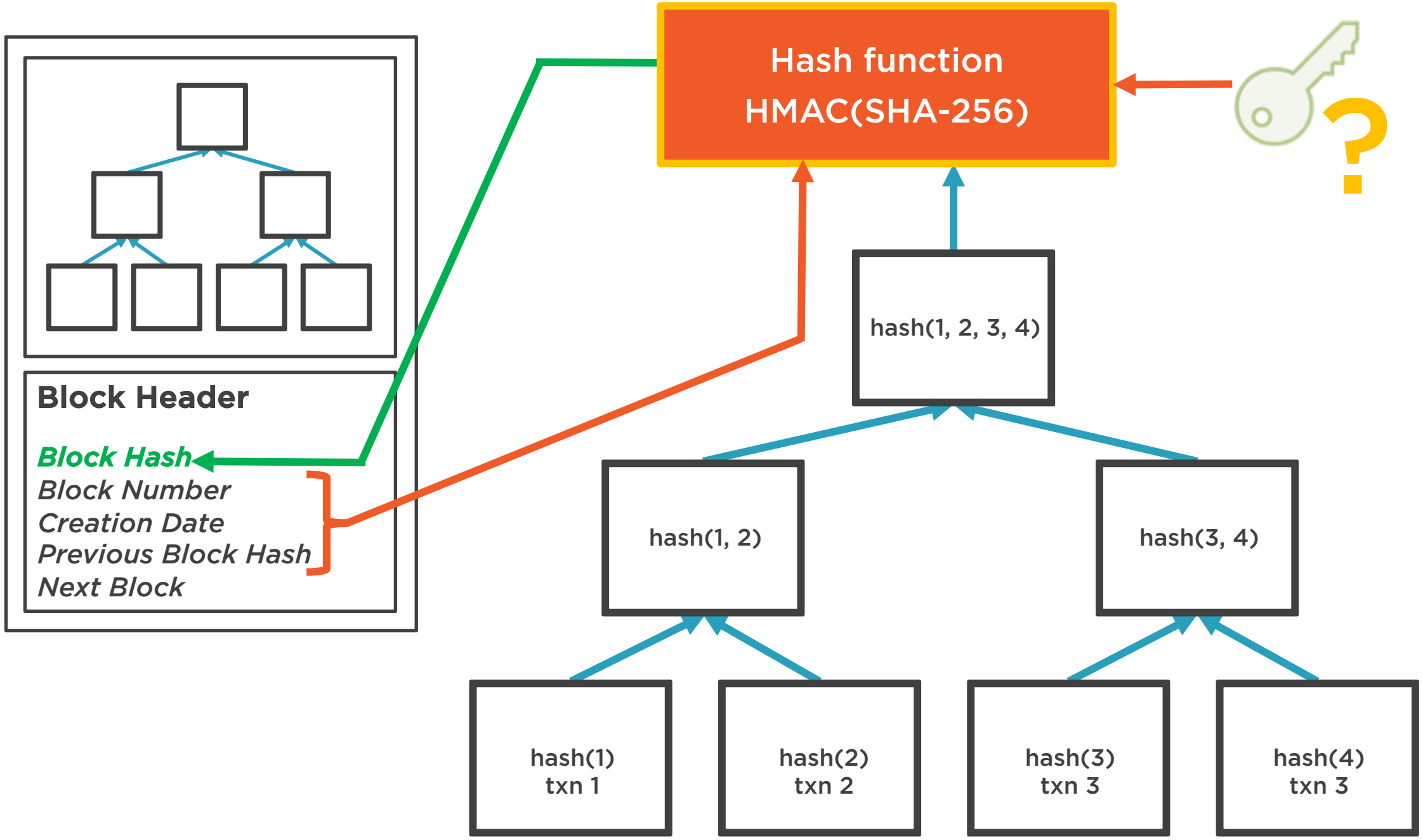
Non-repudiation

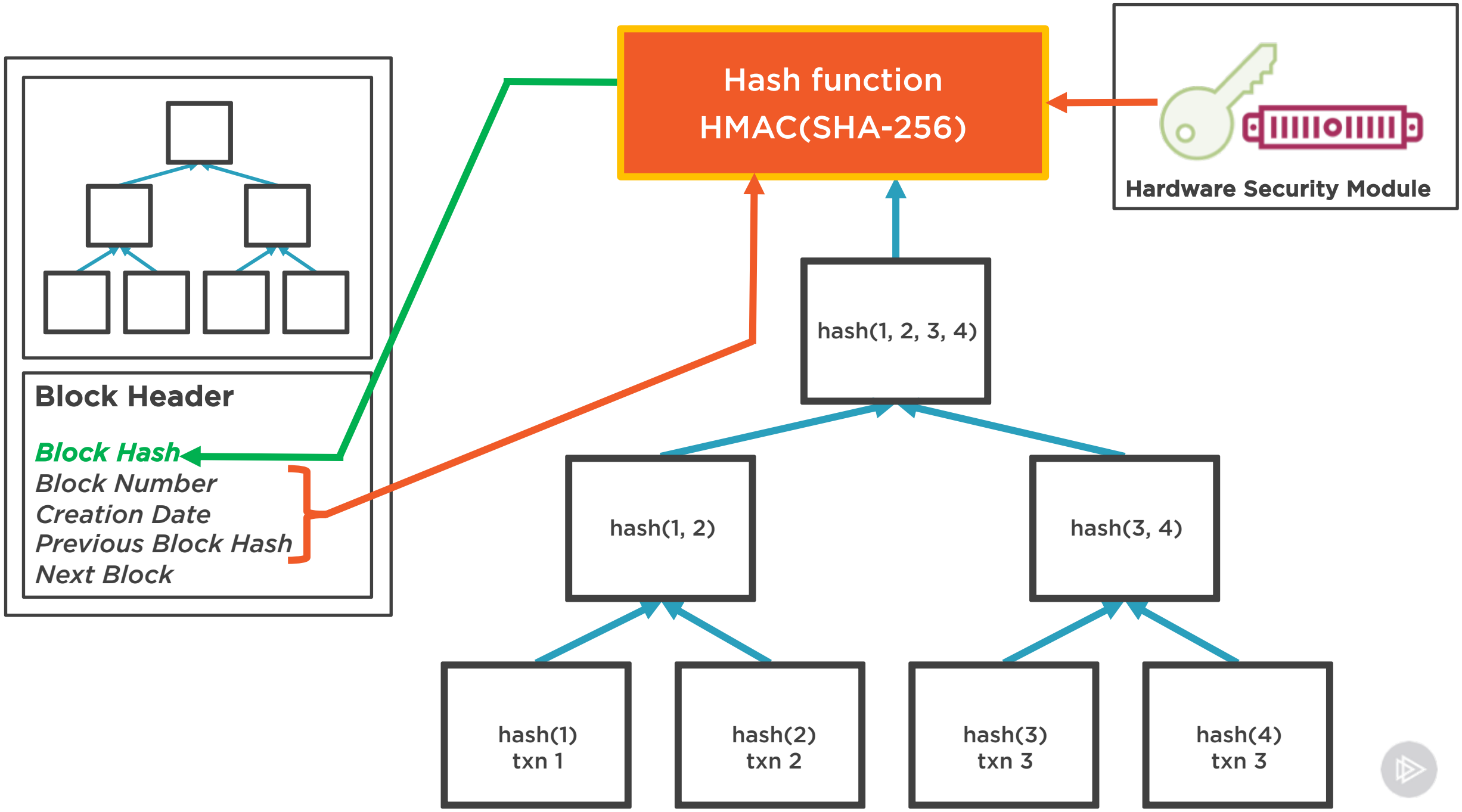
Adding Authentication

Hashing solves integrity

Authenticated hashing solves authentication and integrity


Hash function
HMAC(SHA-256)
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block
hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 3


Hash function
HMAC(SHA-256)
?
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block
hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 3

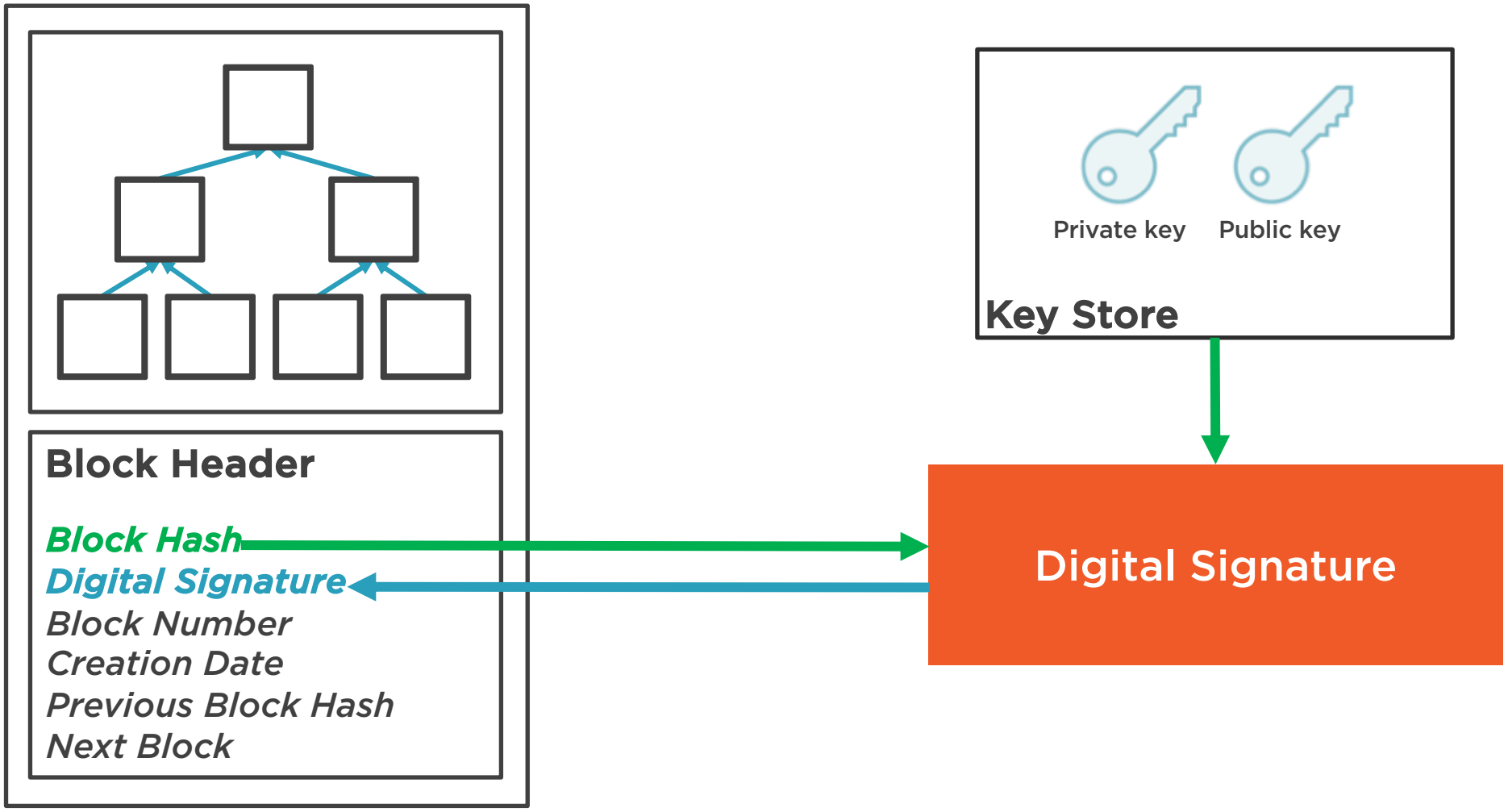

Hash function
HMAC(SHA-256)
Hardware Security Module
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block
hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 3

Practical Cryptography in .NET

Play by Play : Enterprise Data Encryption with Azure Revealed

Adding Non-Repudiation

	Public Key	Private Key
Encryption (RSA)	Encrypt	Decrypt
Digital signatures	Verify signature	Sign message


Block Header
Block Hash
Digital Signature
Block Number
Creation Date
Previous Block Hash
Next Block
Private key
Public key
Key Store
Digital Signature

Blocks

Authentication

Integrity protection

Blockchain validation

Non-repudiation

Non-repudiation = Proof

Key Rotation and Block Versioning

Changing encryption keys over time is good practice

Key Rotation and Block Versioning

Changing encryption keys over time is good practice

Key **A**

Uses Key **A**	Uses Key **A**	Uses Key **A**
Block 998	Block 999	Block 1000

Key Rotation and Block Versioning

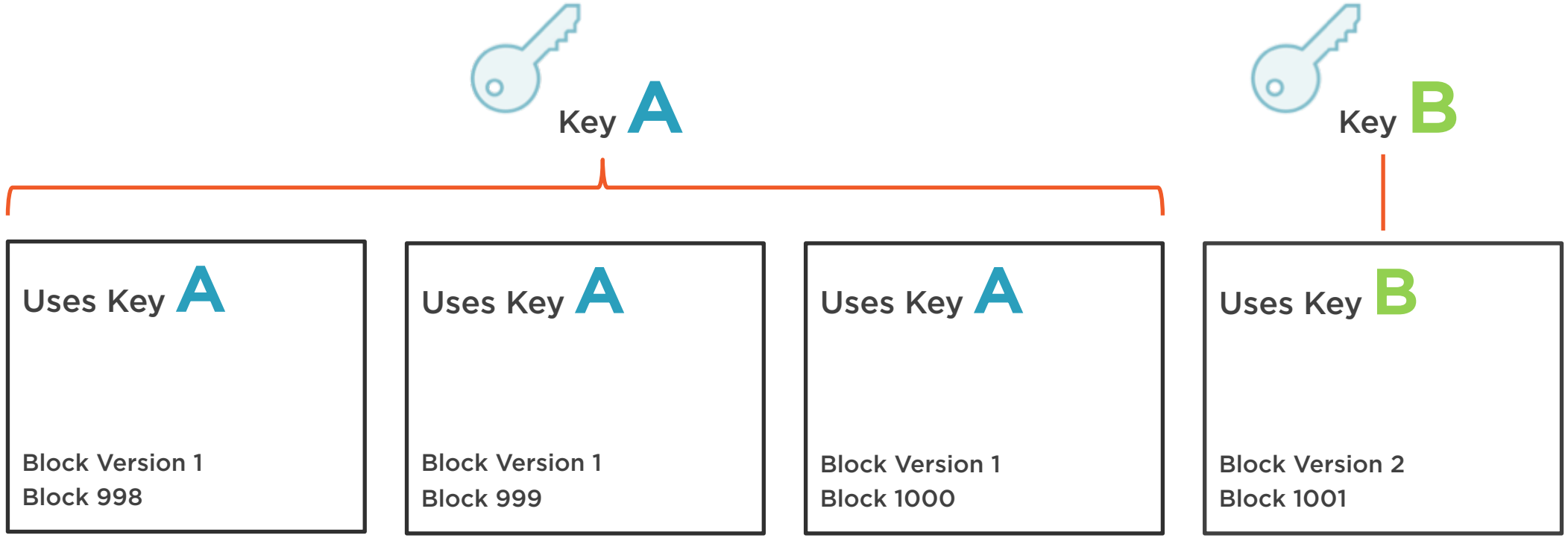
Changing encryption keys over time is good practice

Key **B**

Uses Key **A**	Uses Key **A**	Uses Key **A**	Uses Key **B**
Block 998	Block 999	Block 1000	Block 1001

Key Rotation and Block Versioning

Changing encryption keys over time is good practice



Key Rotation and Block Versioning

Q. Why not just recalculate every block hash?

Key Rotation and Block Versioning

Q. Why not just recalculate every block hash?

A. It's very inefficient!


BUG

Demo

Transaction pool

Message authentication

Digital signatures

Summary

- Blocks containing a single transaction
- Blocks containing multiple transactions
- Merkle trees
- Authentication and non-repudiation
- Block versioning