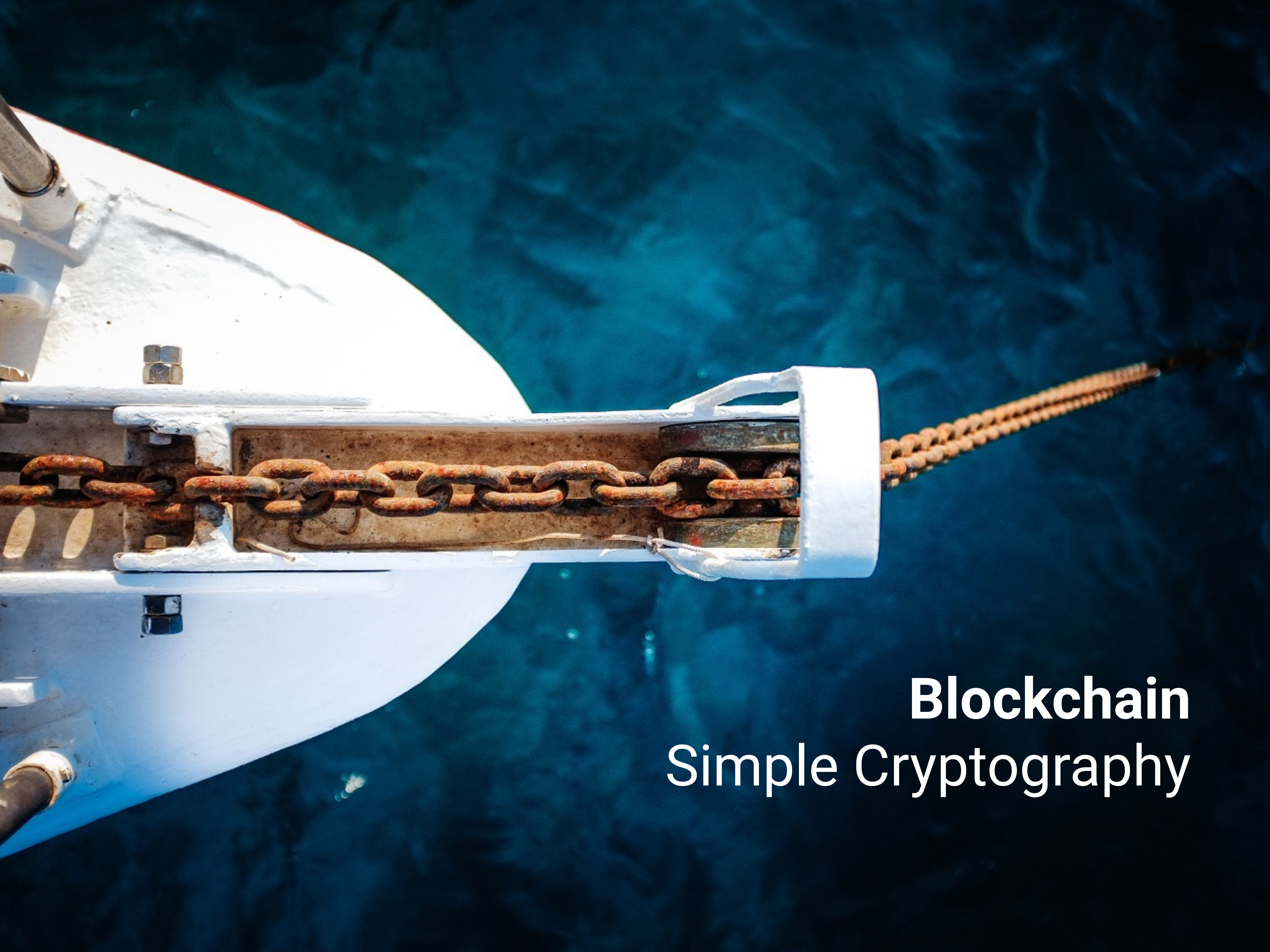


Blockchain

Simple Cryptography

Data Types

- **Cryptographic Hash Functions**

- Merkle Trees

- Elliptic Curve Signature Algorithm (ECDSA)

Data Types

- **Cryptographic Hash Functions**

- SHA256
- RIPEMD160

Arbitrarily long data

Fixed sized hash/digest

- I

- E

Cryptographic Hash Function

- Cryptographic Hash Functions
  - Takes any byte sequence as input
  - Fixed size output
  - Efficiently computable

- Security Properties:
  - Collision-resistance
  - Second pre-image resistance
  - Pre-image resistance
  - Hiding
  - Puzzle-friendly

Example: https://www.pelock.com/products/hash-calculator

Pre-image Resistance

- For any given h in the output space of the hash function, it is hard to find x, s.t. $H(x)=h$

Second Pre-image Resistance

- For a given message x, it is hard to find y s.t. $x \neq y$ and $H(x) = H(y)$

Collision Resistance

- It is hard to find a pair of values, $x \neq y$ and $H(x) = H(y)$

Hiding

- A hash function H is hiding when a secret value r is chosen from a high min-entropy probability distribution, then given H(r || x), it is hard to find x.

Puzzle-friendly

- A hash function H is puzzle friendly if for every possible n-bit output value h, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x such that H(k || x) = h in time significantly less than 2^n.

Search puzzle

- A hash function H
- A value, id, chosen from a high min-entropy distribution
- A target set Y

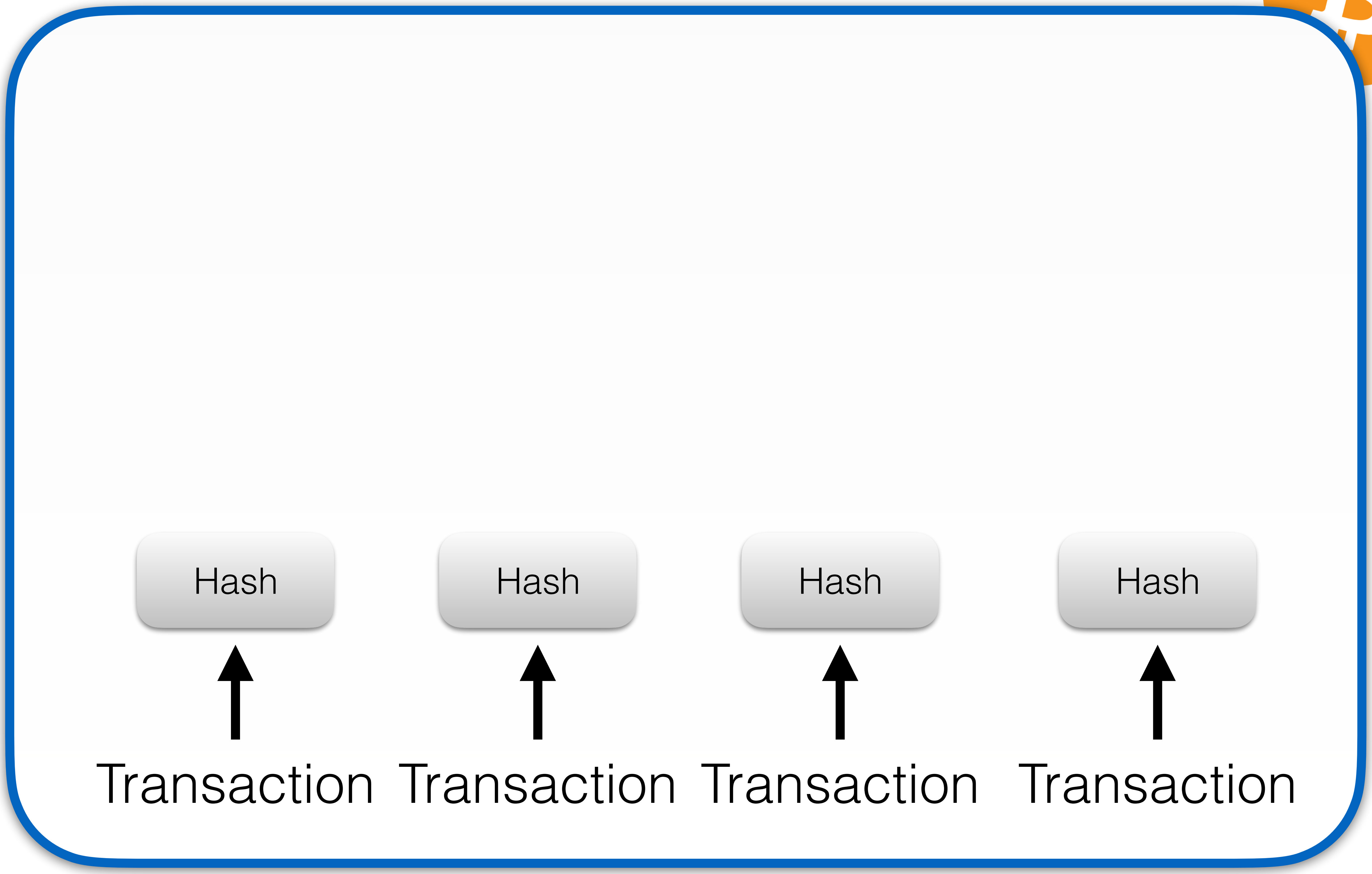
A solution to the puzzle is a value x, s.t.

$$H(id||x) \in Y$$

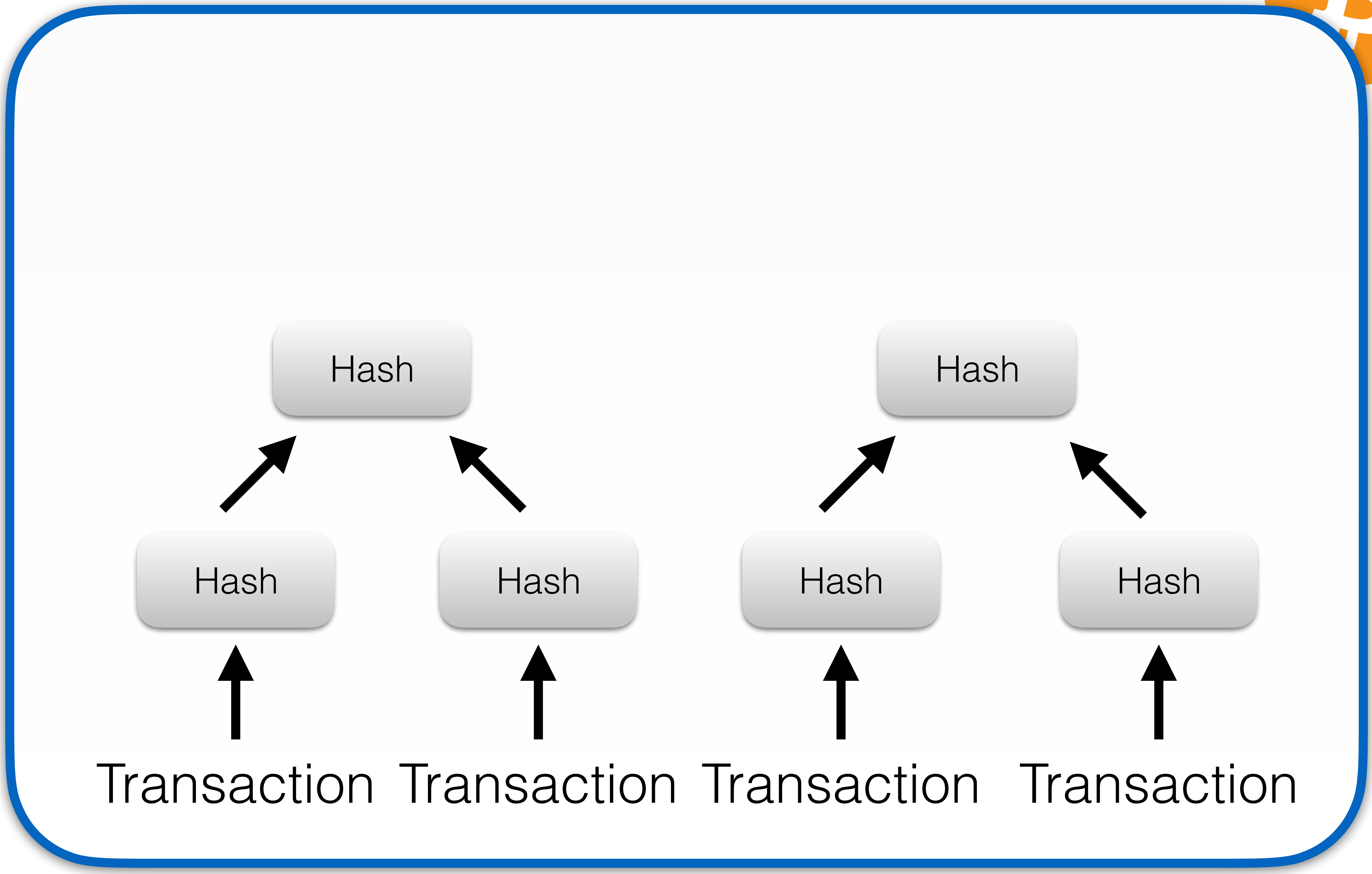
Data Types

- Cryptographic Hash Functions
- **Merkle Trees**
- Elliptic Curve Signature Algorithm (ECDSA)

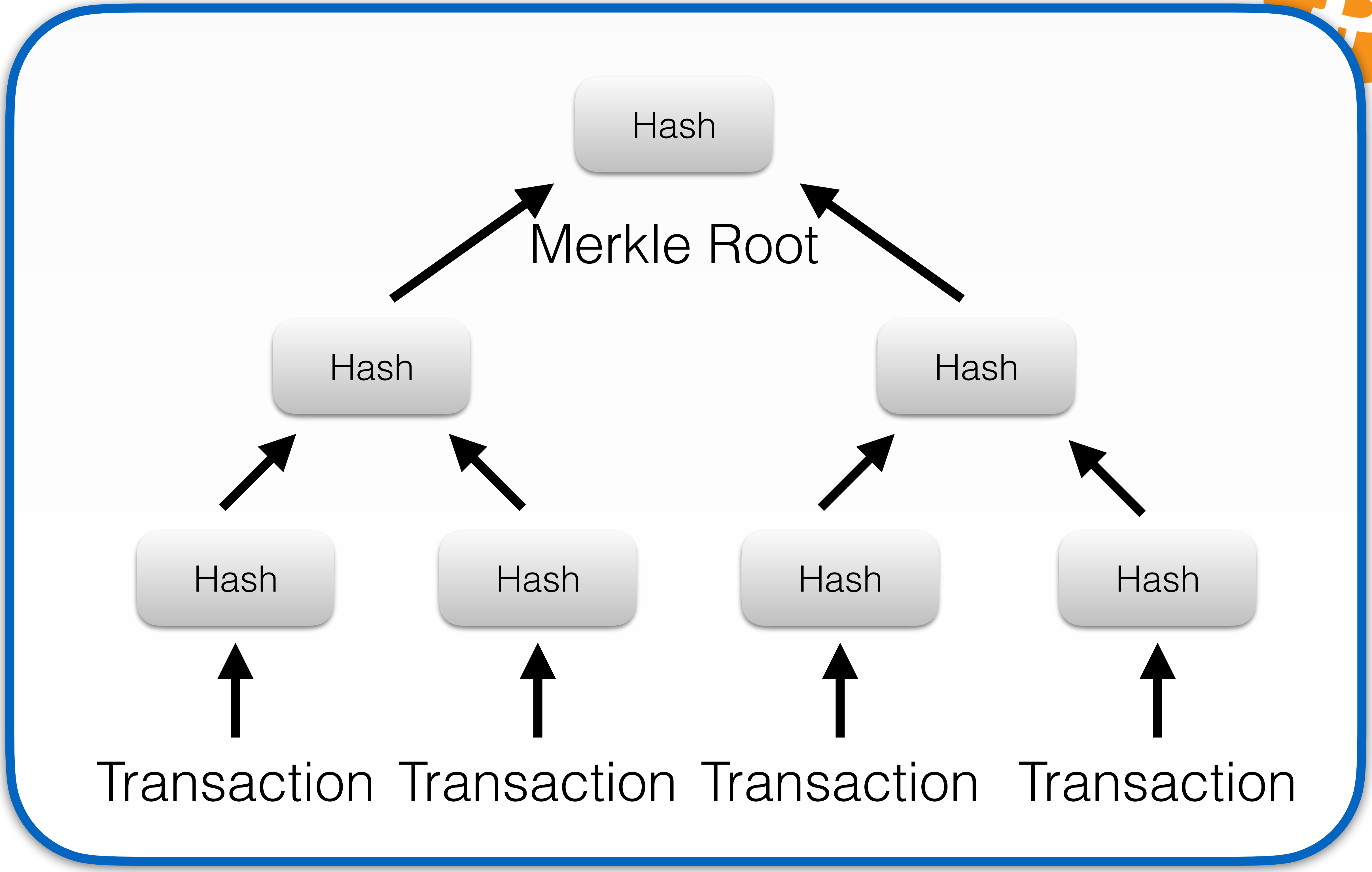
Data Types


Hash
Hash
Hash
Hash
Transaction
Transaction
Transaction
Transaction

Data Types


Hash
Hash
Hash
Hash
Hash
Hash
Transaction
Transaction
Transaction
Transaction

Data Types


Hash
Merkle Root
Hash
Hash
Hash
Hash
Hash
Hash
Transaction
Transaction
Transaction
Transaction

Data Types

- Cryptographic Hash Functions
- Merkle Trees
- **Elliptic Curve Signature Algorithm (ECDSA)**

Data Types

- ECDSA (secp256k1 curve) is used to
  - Sign transactions
  - Verify the signature of transactions
- Nothing in Bitcoin is encrypted ⚠

- **Elliptic Curve Signature Algorithm (ECDSA)**