# Merkle Trees



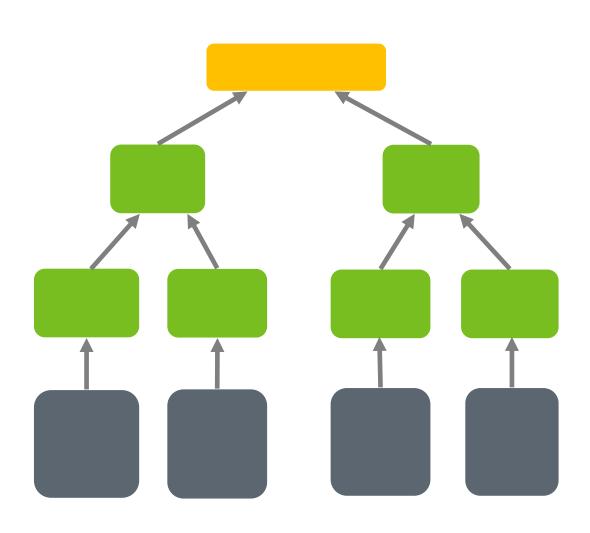
# Objective



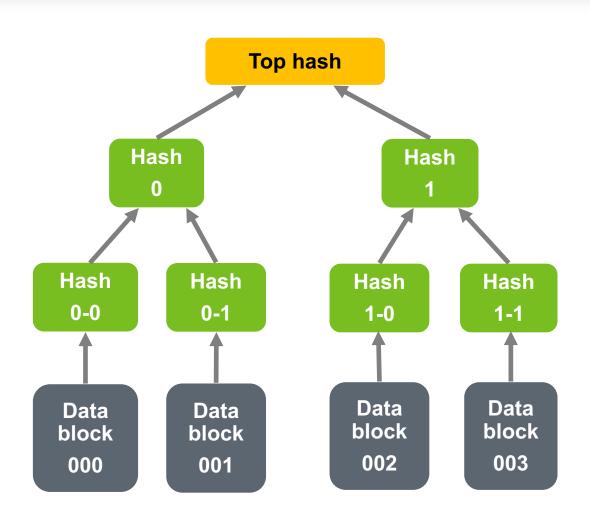
#### **Objective**

Evaluate the validity of Merkle proofs as applied to Simple Payment Verification (SPV) wallets

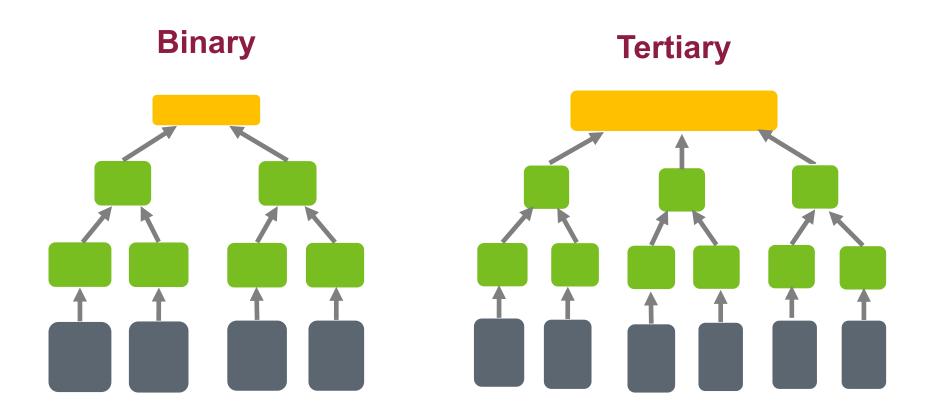
### What is a Merkle Tree?



### Merkle Tree Structure

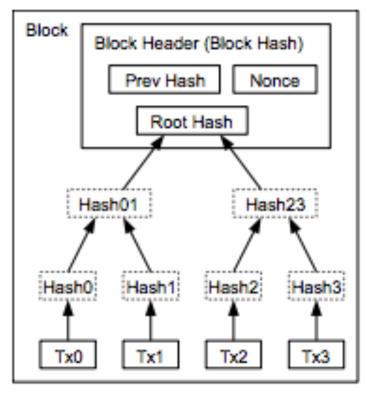


# Types of Merkle Trees

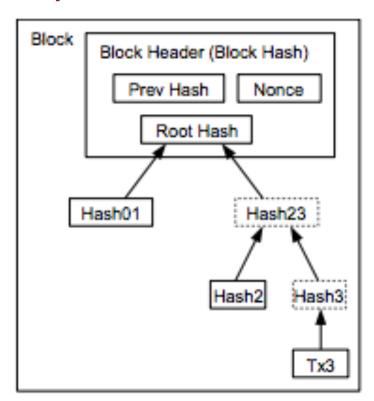


#### Merkle Proof

#### **Bitcoin Example**



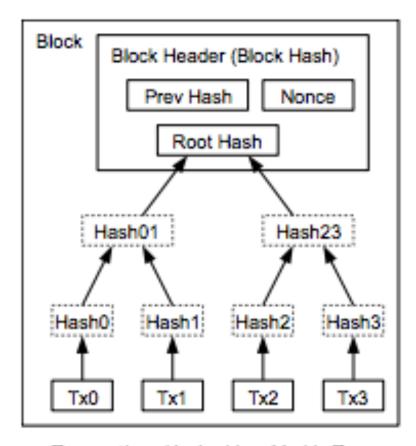
Transactions Hashed in a Merkle Tree



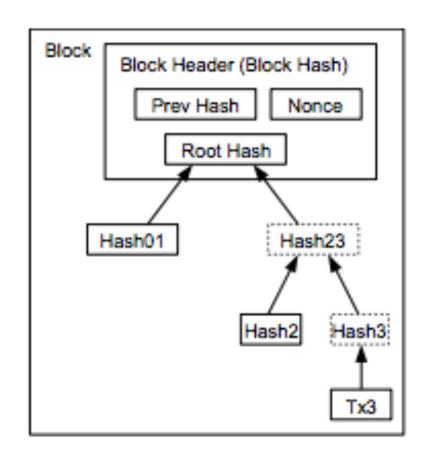
After Pruning Tx0-2 from the Block

SOURCE: Satoshi Nakamoto, "Bitcoin a Peer-to-Peer Electronic Cash System"

## Merkle Tree Properties



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

## Conclusion

Security

Efficiency

