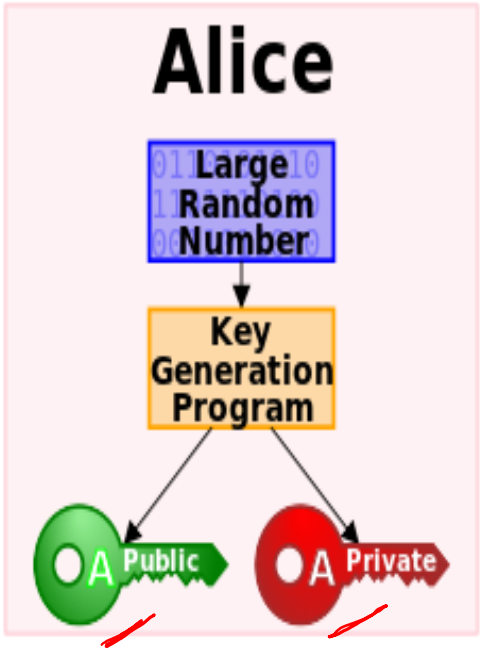
# Bitcoin Blockchain

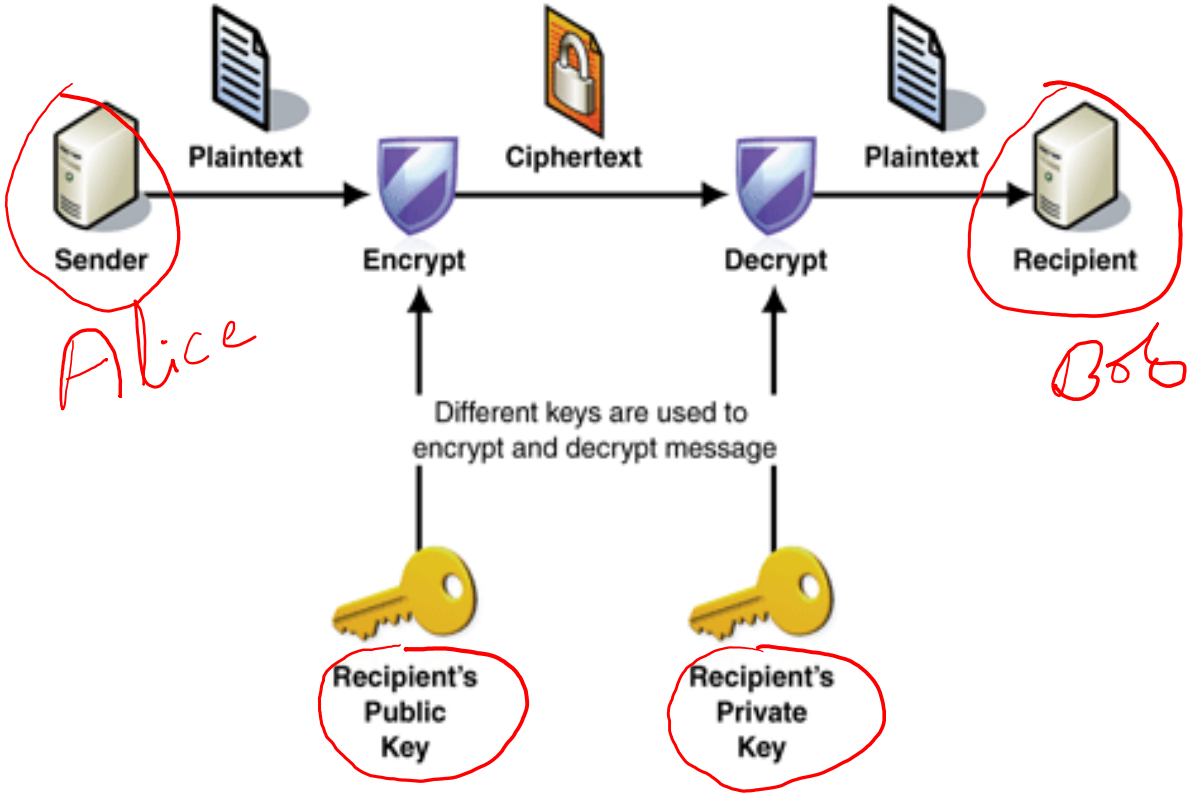
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

CHITTOOR, INDIAN

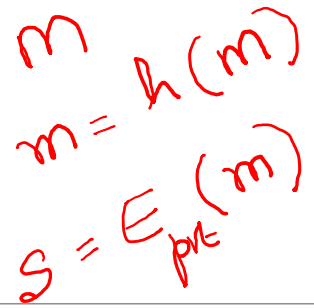
# Public Key Crypto: Encryption

## Key pair: public key and private key

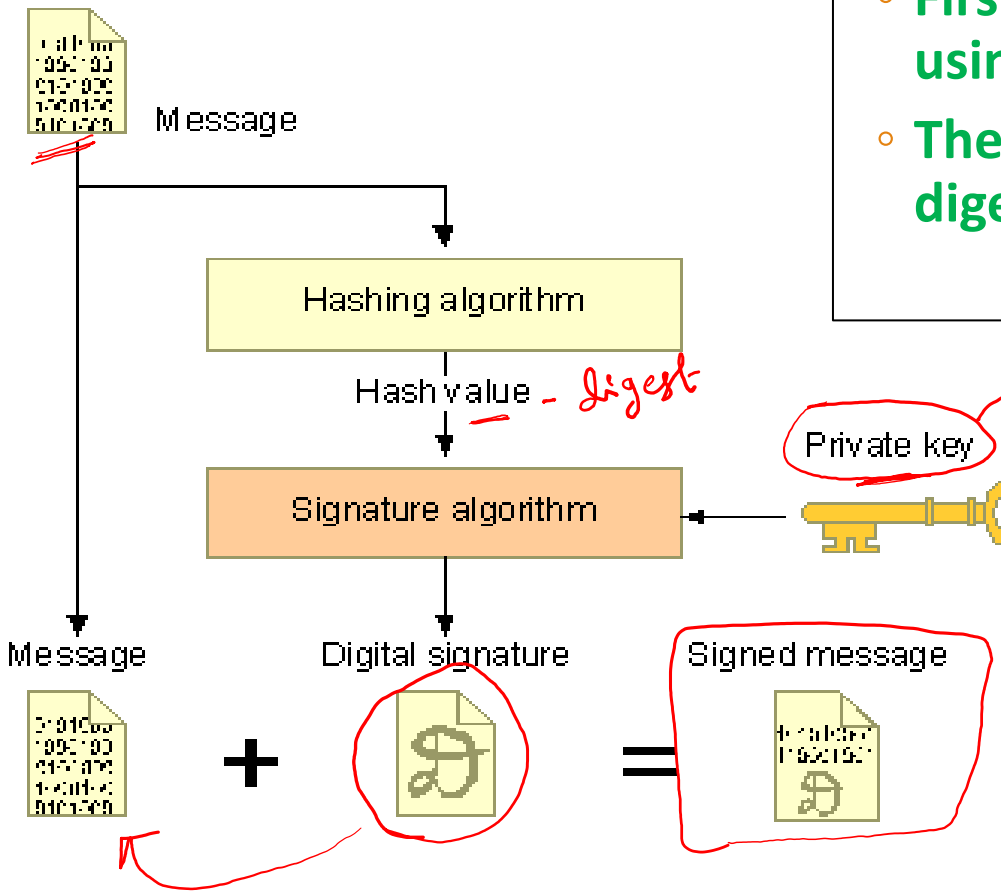


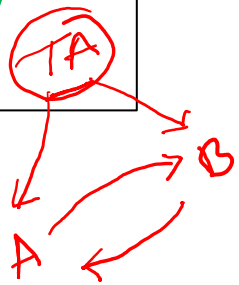



# Public Key Crypto: Digital Signature




- First, create a message digest using a cryptographic hash
- Then, encrypt the message digest with your private key



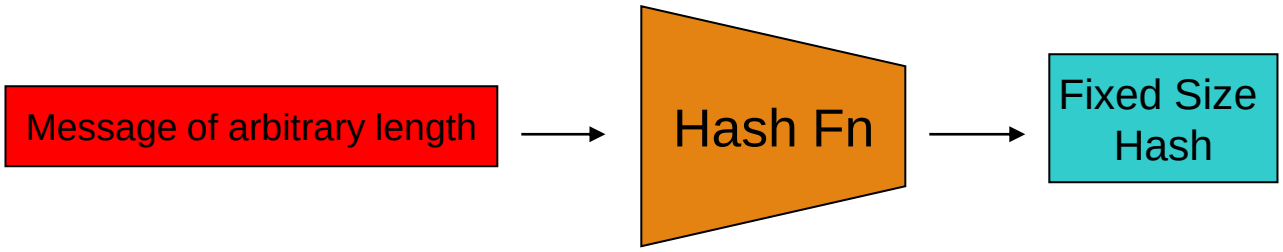

Authentication

Integrity

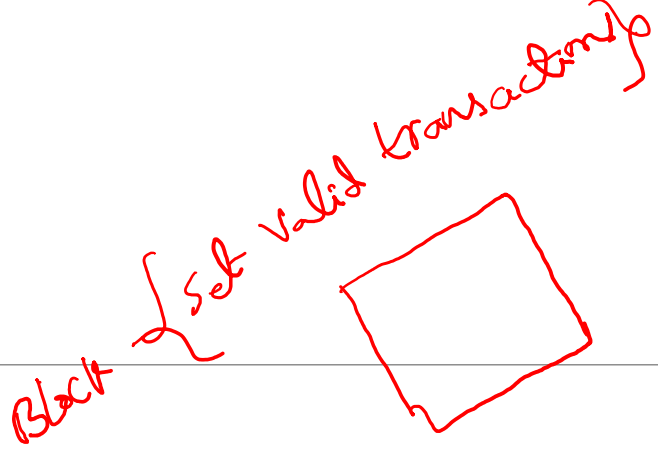
Non-repudiation

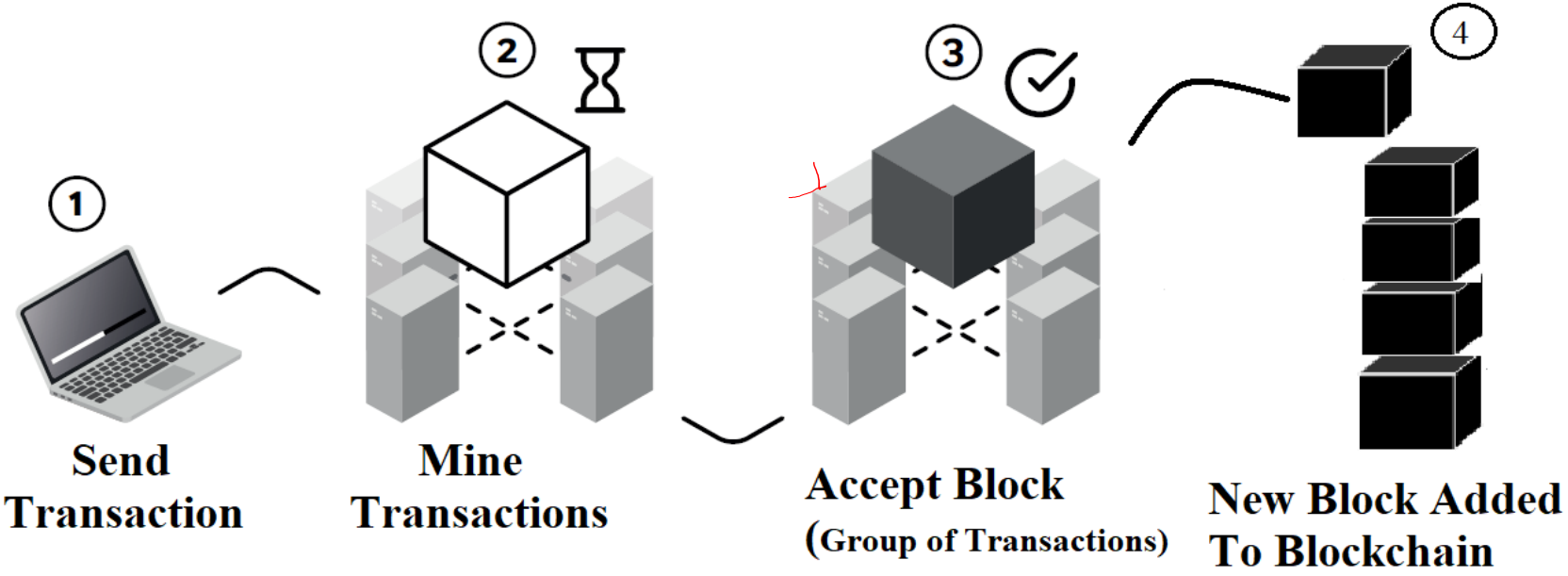
# Cryptographic Hash Functions

- Consistent: H(x) always yields same result
- One-way: given y, hard to find x s.t. H(x) = y
- Collision resistant: given H(w) = z, hard to find x such that H(x) = z

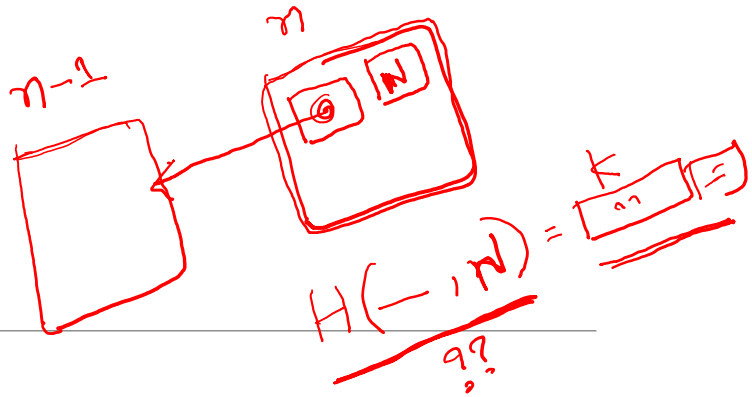


# Bitcoin Network



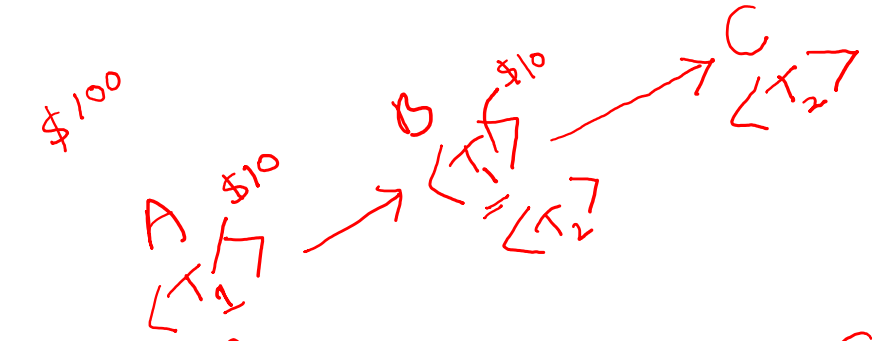
# BitCoin

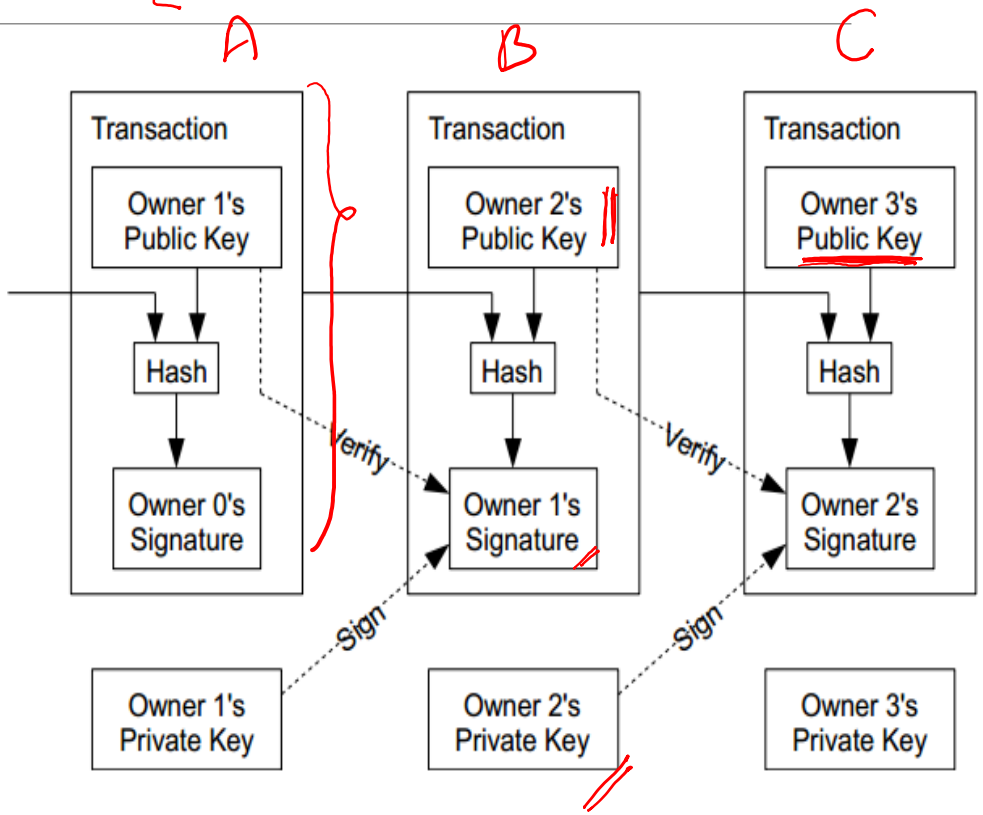


- **Validation**
  - Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending? → Broadcast to all nodes
- **Creation of a virtual coin/note**
  - How is it created in the first place? → Provide incentives for miners
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins

# Bitcoin

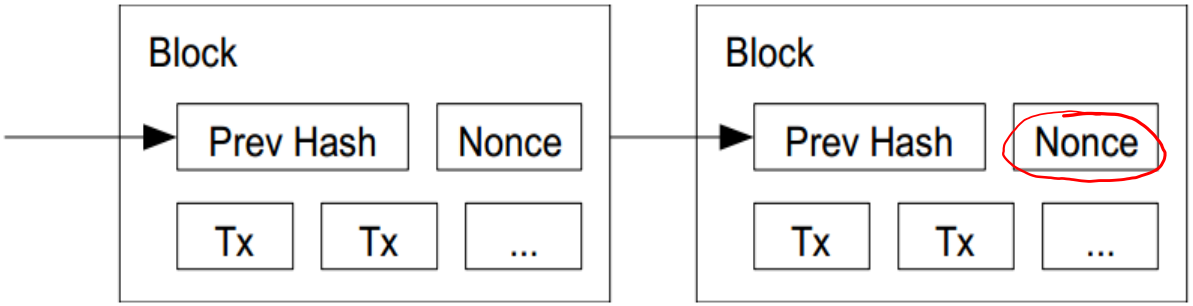
- Electronic coin == chain of digital signatures
- BitCoin transfer: Sign(Previous transaction + New owner's public key)
- **Anyone can verify (n-1)th owner transferred this to the nth owner**
- **Anyone can follow the history Given a BitCoin**



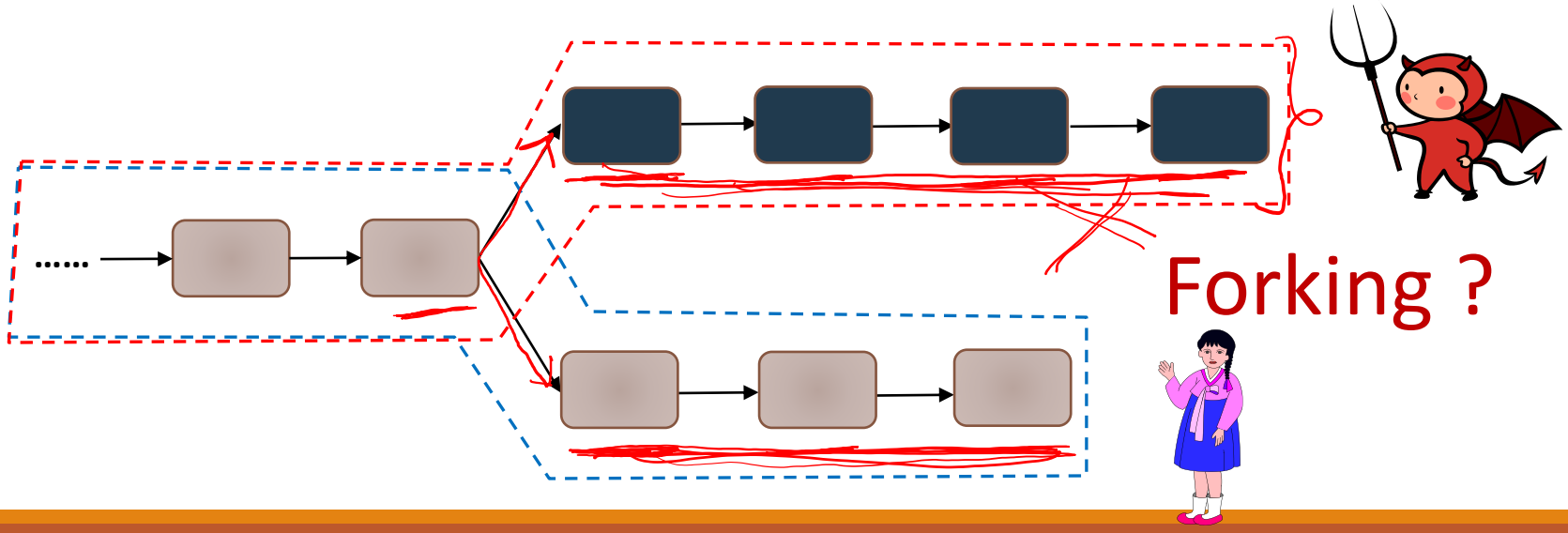
# Use of Cryptographic Hashes

- **Proof-of-work**
  - Block contains transactions to be validated and previous hash value.
  - Pick a nonce such that **H(prevhash, nonce, Tx) < E**.
    - E is a variable that the system specifies. Basically, this amounts to finding a hash value who's leading bits are zero.
    - The work required is exponential in the number of zero bits required.
  - Verification is easy. **But, proof-of-work is hard.**



# Preventing Double-spending

- The only way is to be aware of all transactions.
- Each node (miner) verifies that this is the first spending of the Bitcoin by the payer.
- Only when it is verified it generates the proof-of-work and attach it to the current chain.

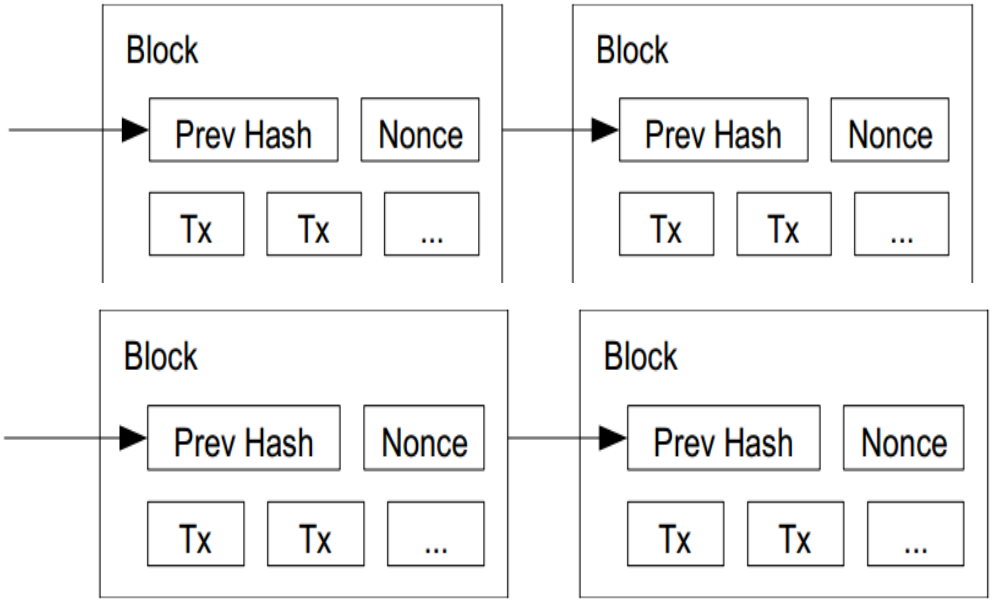


# Tie breaking

**Two nodes may find a correct block simultaneously.**

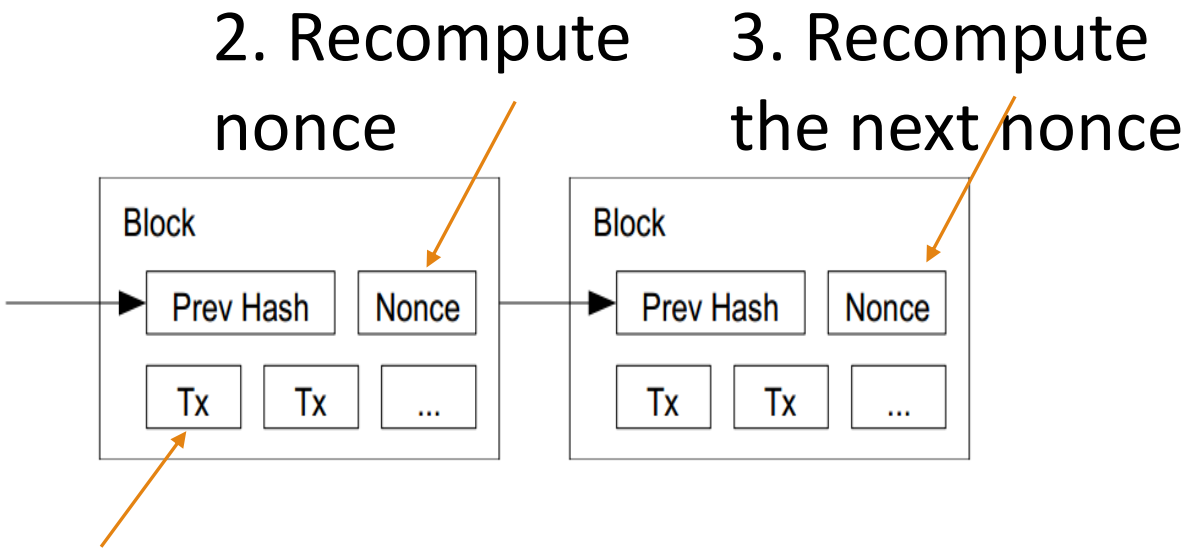
- Keep both and work on the first one
- If one grows longer than the other, take the longer one

Two different block chains (or blocks) may satisfy the required proof-of-work.



# Reverting is Hard

**Reverting gets exponentially hard as the chain grows.**



# Practical Limitation

- **At least 10 mins to verify a transaction.**
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - **But, for a large transaction ($$$) wait longer.**
  - **Because, if you wait longer it becomes more secure.**
  - **For large $$$, you wait for six blocks (1 hour).**

# Acknowledgement

Some of the slides, content, or pictures are borrowed from the following resources, and some pictures are obtained through Google search without being referenced below:

L24-BitCoin and Security; UMASCS660-Secure Digital Currency: Bitcoin, many of the slides borrowed from this presentation with modifications.

**Ian Miers,** Zerocoin: Anonymous Distributed E-Cash from Bitcoin, IEEE S&P slides

# THANK YOU