

# Cybersecurity

## Cryptography Modes of Operation and Blockchains



# Modes of Operations

- Authenticated
  - Validate the integrity of the ciphertext
- Unauthenticated
  - do not validate the integrity of the ciphertext
- Counter
  - Changes block ciphers into stream ciphers
    - Done by generating successive blocks in the stream using a nonrepeating counter



# Blockchain

- A distributed and immutable public ledger
  - Can store records in a way that distributes records among different systems worldwide
  - All while preventing tampering
- Every block contains a hash of the previous block, a timestamp, and transaction data.
  - Repetitive hashing
  - Highly resistant to data alteration

