Blockstream

# Introduction to Onion Routing

Dr. Christian Decker

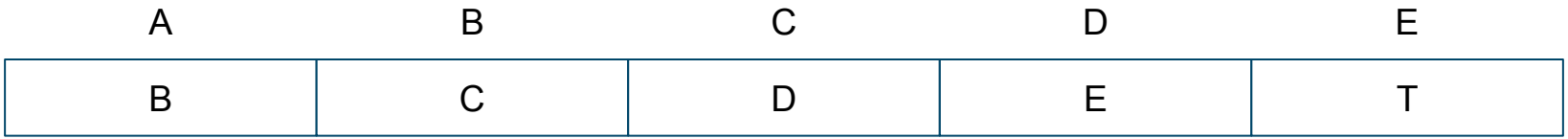
Core Tech Engineer

# Source-based vs Distance Vector Routing

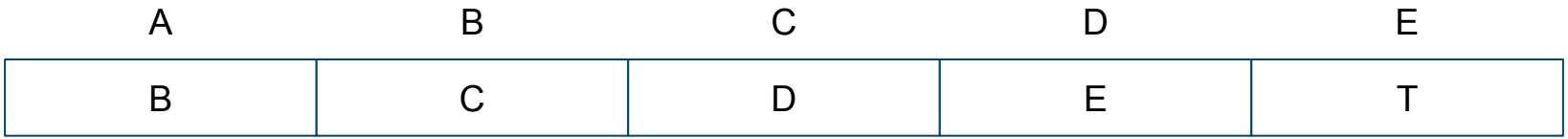
## Distance Vector Routing


## Source-based routing

# Routing with an Onion



# Routing with a Variable Onion



# 1 Simple Onion

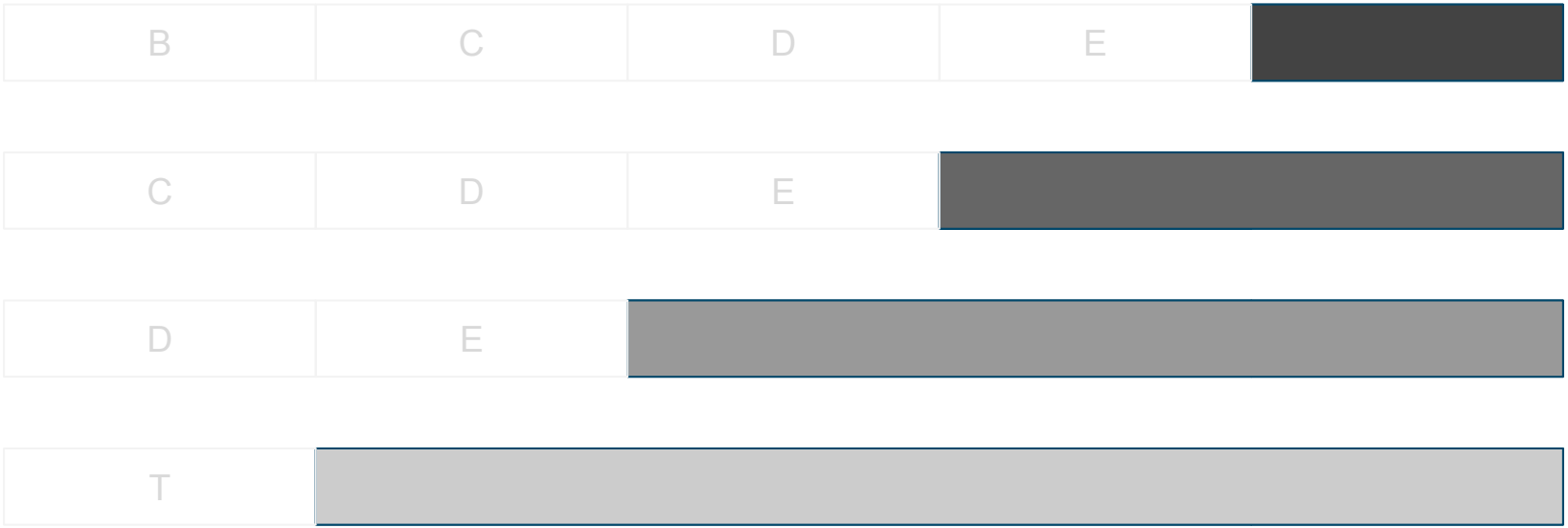
# Simple Onion Routing protocol

# 2 Constant Size Onion

# Constant Size Onion

# 3 Sphinx

# Filler for HMACs



# Sphinx

# Pseudocode

## Unwrapping the onion

- ECDH with ephemeral key and node ID ⇨ shared secret
- Verify HMAC
- Append filler
- Decrypt using shared secret
- Extract hop payload
    - Next HMAC
    - Next hop
    - CLTV delta
    - Forward amount
- Serialize next onion

## Wrapping the onion

- Generate ephemeral key and shared secrets in forwards order with ECDH
- Serialize last hop payload (HMAC = 32 x `0x00` bytes)
- In reverse order for each hop:
    - Right pad to 1365 `0x00` bytes
    - Derive `ChaCha20` stream from shared secret
    - Encrypt Onion using stream
    - Compute the HMAC of the first 1300 bytes
    - Add HMAC to prior hop
    - Right-shift by 65 bytes
    - Serialize previous hop payload into shifted in bytes
- Serialize onion packet

# Sphinx in Lightning

- Encryption Stream: `ChaCha20`
- `HMAC`: `SHA256`
- Shared Secret: `ECDH`
- Key generation: `HMAC` with key-type
  - `rho`
  - `mu`
  - `um`

# 4 Returning an Error

# 5 Recent Developments

# Thank You

@Snyke

@Blockstream

Blockstream.com