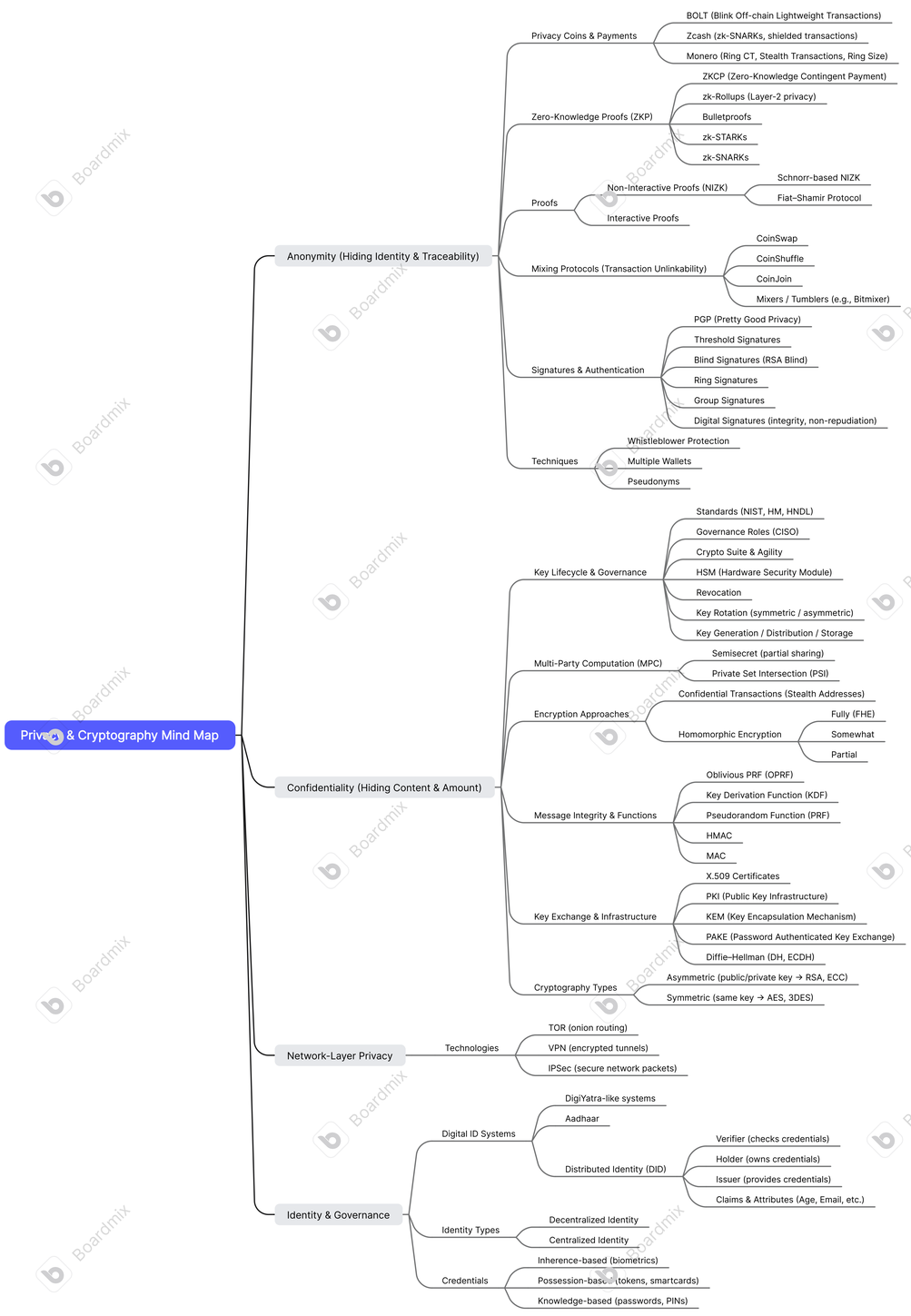
Privacy & Cryptography Mind Map
Anonymity (Hiding Identity & Traceability)
Privacy Coins & Payments
BOLT (Blink Off-chain Lightweight Transactions)
Zcash (zk-SNARKs, shielded transactions)
Monero (Ring CT, Stealth Transactions, Ring Size)
Zero-Knowledge Proofs (ZKP)
ZKCP (Zero-Knowledge Contingent Payment)
zk-Rollups (Layer-2 privacy)
Bulletproofs
zk-STARKs
zk-SNARKs
Proofs
Non-Interactive Proofs (NIZK)
Schnorr-based NIZK
Fiat–Shamir Protocol
Interactive Proofs
Mixing Protocols (Transaction Unlinkability)
CoinSwap
CoinShuffle
CoinJoin
Mixers / Tumblers (e.g., Bitmixer)
Signatures & Authentication
PGP (Pretty Good Privacy)
Threshold Signatures
Blind Signatures (RSA Blind)
Ring Signatures
Group Signatures
Digital Signatures (integrity, non-repudiation)
Techniques
Whistleblower Protection
Multiple Wallets
Pseudonyms
Confidentiality (Hiding Content & Amount)
Key Lifecycle & Governance
Standards (NIST, HM, HNDL)
Governance Roles (CISO)
Crypto Suite & Agility
HSM (Hardware Security Module)
Revocation
Key Rotation (symmetric / asymmetric)
Key Generation / Distribution / Storage
Multi-Party Computation (MPC)
Semisecret (partial sharing)
Private Set Intersection (PSI)
Encryption Approaches
Confidential Transactions (Stealth Addresses)
Homomorphic Encryption
Fully (FHE)
Somewhat
Partial
Message Integrity & Functions
Oblivious PRF (OPRF)
Key Derivation Function (KDF)
Pseudorandom Function (PRF)
HMAC
MAC
Key Exchange & Infrastructure
X.509 Certificates
PKI (Public Key Infrastructure)
KEM (Key Encapsulation Mechanism)
PAKE (Password Authenticated Key Exchange)
Diffie–Hellman (DH, ECDH)
Cryptography Types
Asymmetric (public/private key → RSA, ECC)
Symmetric (same key → AES, 3DES)
Network-Layer Privacy
Technologies
TOR (onion routing)
VPN (encrypted tunnels)
IPSec (secure network packets)
Identity & Governance
Digital ID Systems
DigiYatra-like systems
Aadhaar
Distributed Identity (DID)
Verifier (checks credentials)
Holder (owns credentials)
Issuer (provides credentials)
Claims & Attributes (Age, Email, etc.)
Identity Types
Decentralized Identity
Centralized Identity
Credentials
Inherence-based (biometrics)
Possession-based (tokens, smartcards)
Knowledge-based (passwords, PINs)