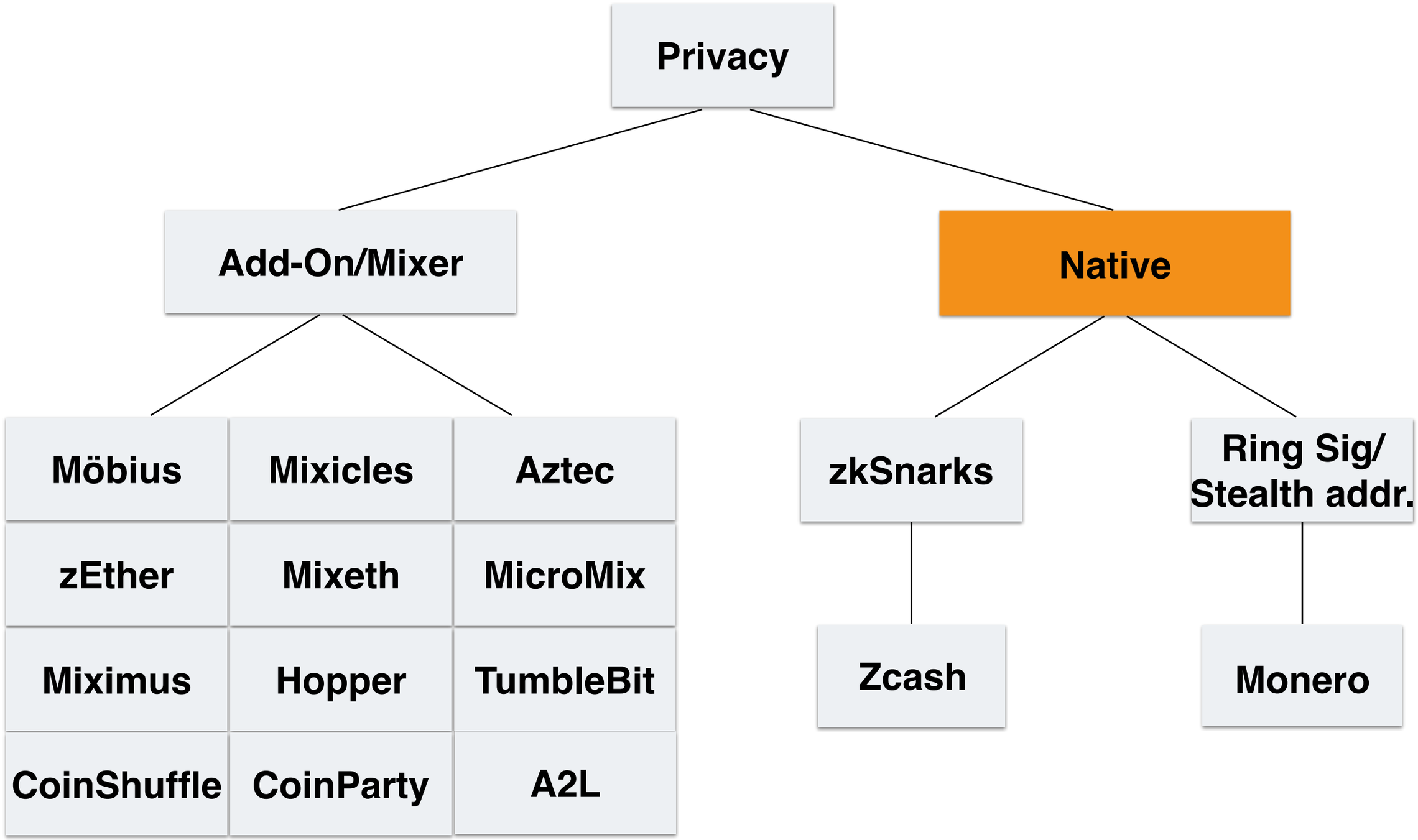

Blockchain Privacy
Native Privacy Blockchain

Blockchain Privacy Solutions



Privacy Preserving Blockchains - Different Approaches

Decoy of k-anonymity Privacy

- Monero, CoinJoin

N-anonymity Privacy

- ZCash

ZCash

- Bitcoin Fork

- Privacy Features:
  - Transparent Transactions (t-addr)
  - Shielded Transactions (z-addr)

- z-addr Transactions
  - # coins entering
  - # coins exiting
  - ZKP that the transaction is valid

	Shielding	**De-shielding**	**Shielded**
Source	t-addr	z-addr	z-addr
Destination	z-addr	t-addr	z-addr
Amount	Public	Public	Private

- zkSNARK
  - Non-interactive, Succinct proofs of knowledge
  - Requires trusted setup

Monero Privacy Features

- Unlinkability (destination): Stealth Addresses
- Untraceability (source): Ring Signatures/RingCT