Cameleonica

- Safety
  - Versioning
  - Snapshots
  - Consistency / Durability / Atomicity / Isolation ?
- Crypto
  - Confidentiality
    - Shaving secrets master key
    - Freezing volume wiping keys
  - Authenticity
- Stego
  - Plausible deniability
- Advanced
  - Performance
    - Low delays
    - High throughput
  - Security
    - Permanent deletion
  - Functionality
    - Instantenous copying
      - Reverse is actually deduplication
  - Utilisation
    - Transparent compression
      - Selective/Adaptive
  - Integration
    - Transparent hashing
      - enables deduplication

Cameleonica 2.0

- Redundancy
  - Copies on remote backends
- Capacity
  - Only copies moved to remote backends
    - Glacier storage?
- Computation
  - Remote execution of code on remote files
    - Remote execution of arbitrary unmodified codes
- Redistribution
  - Third party can download files given a ticket
    - Retrievability
      - Proofs of
- Pluggability
  - Can use heterogeneous backends
    - Amazon EBS
    - Amazon S3
    - Any file/block storage on local/remote node

- Moveability
  - Select ones of backend to move data out of
- Transferability
  - Move files between remote backends by just issuing tickets

idea #3

thanks to Bruce Schneier

Self-destruct subsystem

- Freeze volume
  - at activation
  - wipe master key from RAM
  - Also trigger screen lockout
- After 10-15 min
  - wipe master header from hard disk
  - unless disarmed
    - if rebooted during countdown
      - wipe now
- Triggered by keyshortcut
  - or some external event
  - eg. external website or IM status
  - or a certain password
  - or a TOR hidden service
- Make a backup beforehand
  - store it at unknown location
  - Divide it among parties
    - eg. 2 of 3 needed to recover