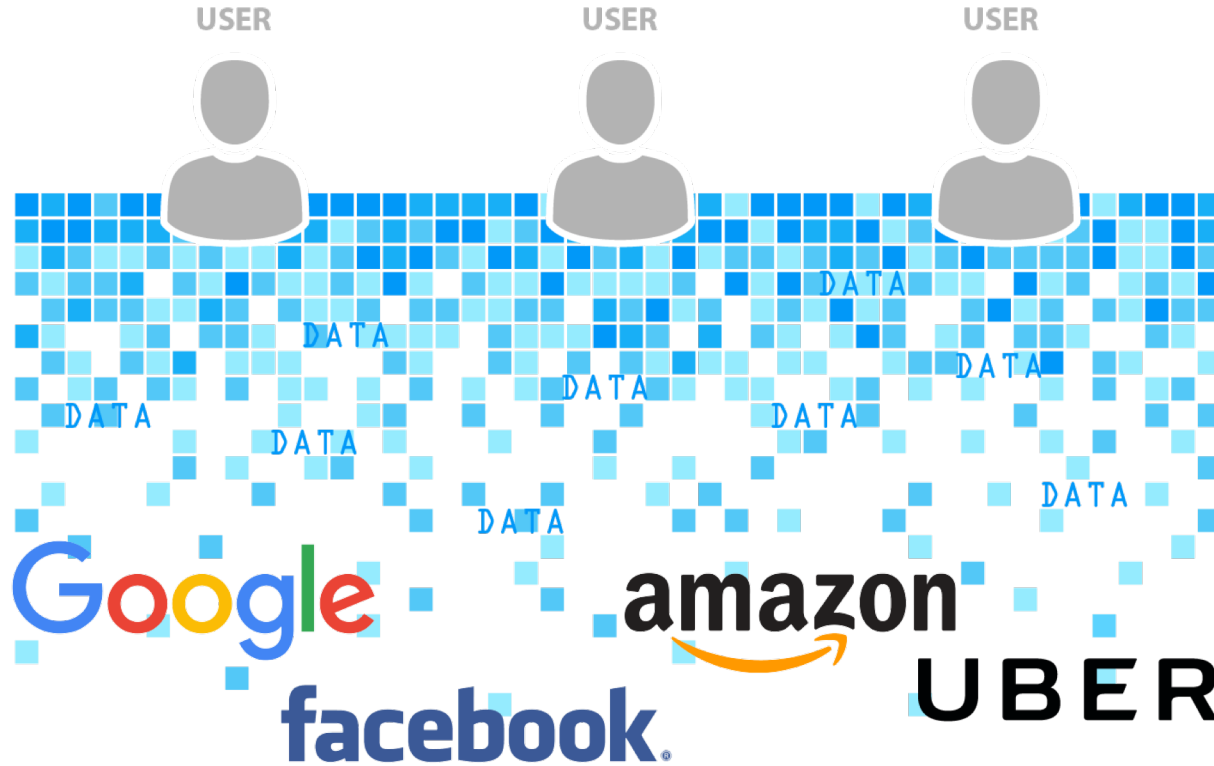




LinkChains: Trusted Personal Linked Data

Allan Third and John Domingue
{allan.third,john.domingue}@open.ac.uk

Motivation



Motivation



Motivation



The FAIR Principles

- **F**indable
 - Globally persistent IDs and metadata
- **A**ccessible
 - Retrievable in a standard way (with auth?)
- **I**nteroperable
 - Formal & machine-readable representation
- **R**eusable
 - Licences, attributes, and provenance

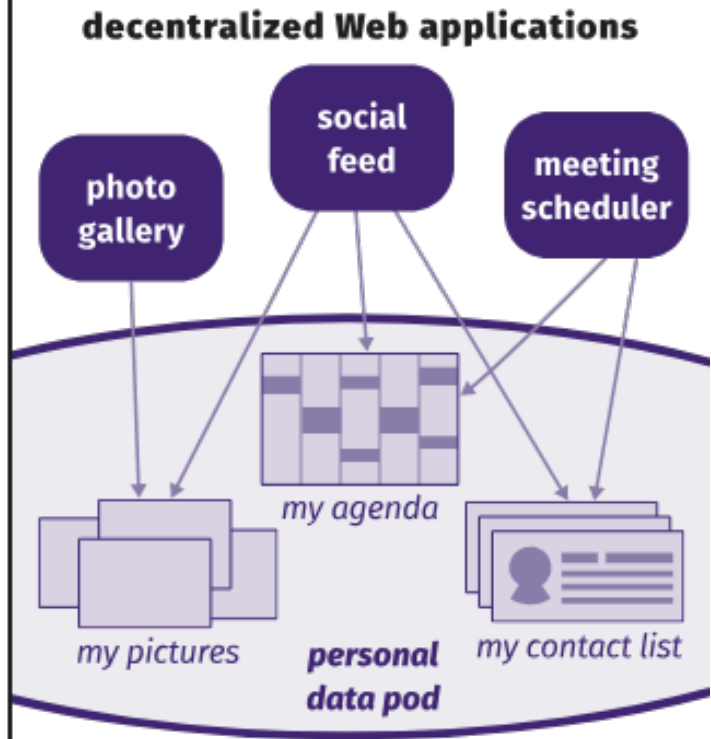
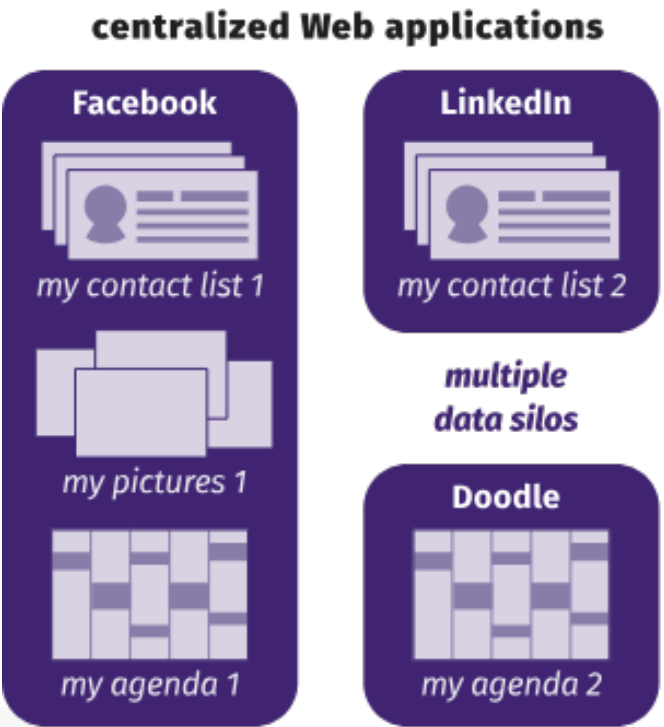
TRADE Principles

- **T**rusted
 - Data & claims, publisher, timestamp verifiable
- **A**utonomous
 - Access to & use of data controlled by owner
- **D**istributed
 - Storage & computation spread across network
- **D**Ecentralised
 - Open, nodes are independent

Valuable Personal Data is...

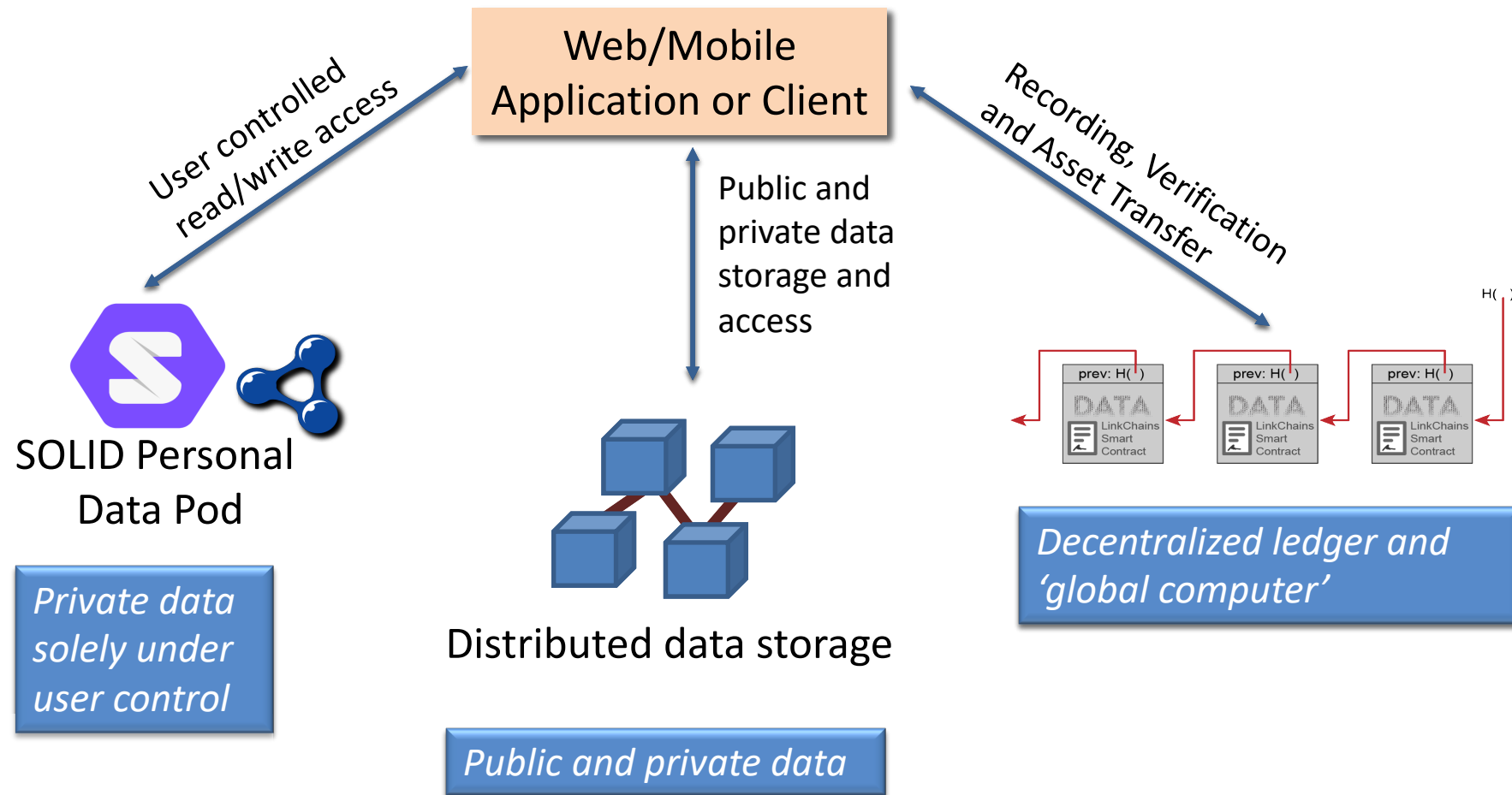
- Personal or sensitive
 - Potentially misusable
 - Damaging if overshared
- Leads to gains when shared selectively
 - **when accurate!**

Decentralized web apps share access to personal data stores



<https://itsfoss.com/solid-decentralized-web/>

LinkChain Components

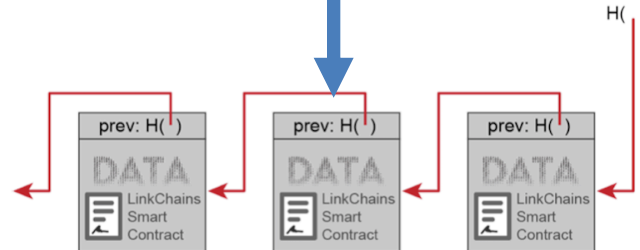


Anchoring data on a blockchain

```
{ ou:student1 :recipient ou:jstrange2323 ;  
  :badge "Magic 101"^^xsd:string. }
```

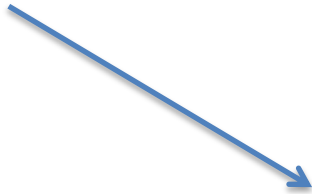


ab8d0f09b90bf9080080de



Federation

```
{ ou:student1 :recipient ou:jstrange2323 ;  
  :badge "Magic 101"^^xsd:string. }
```

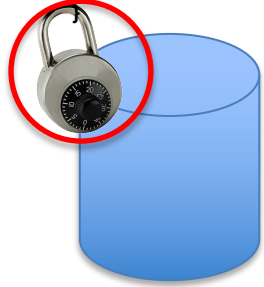


```
{ ou:student1 :recipient ou:jstrange2323 ;  
  :badge "Magic 101"^^xsd:string. }
```

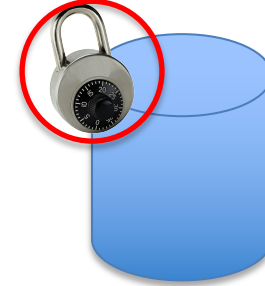


Federation

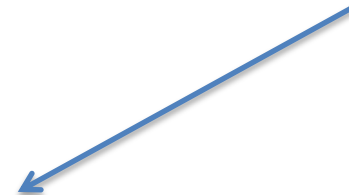
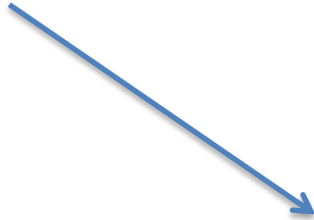
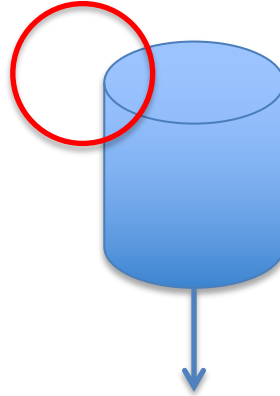
```
{ ou:student1 :recipient ou:jstrange2323 ;  
  :badge "Magic 101"^^xsd:string.
```



```
{ :landowner1212 gov:ownerIn gov:herefordshire .  
}
```



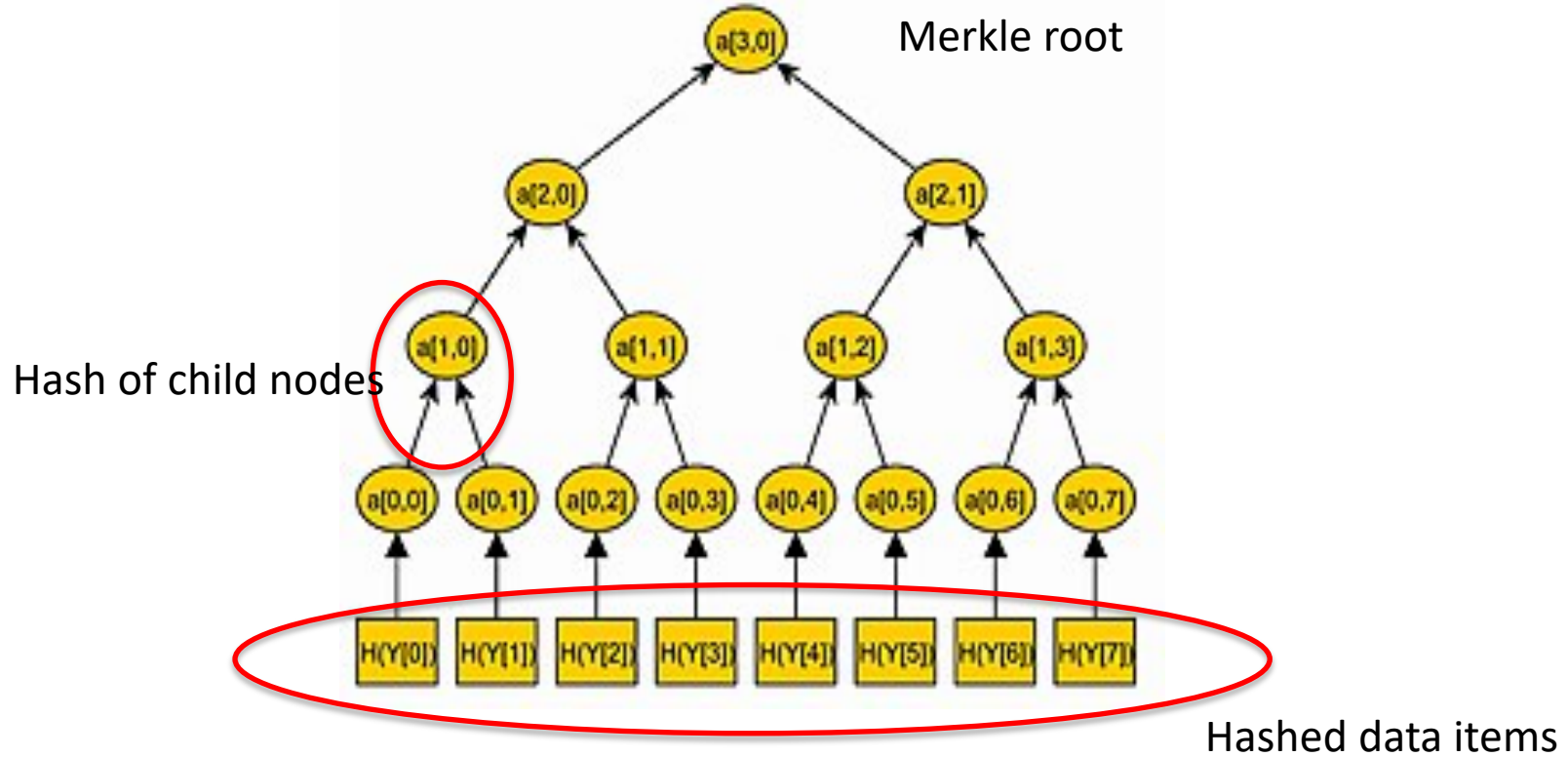
```
{ ou:jstrange2323 owl:sameAs :landowner1212 . }
```



```
{ ou:student1 gov:ownerIn gov:herefordshire . }
```



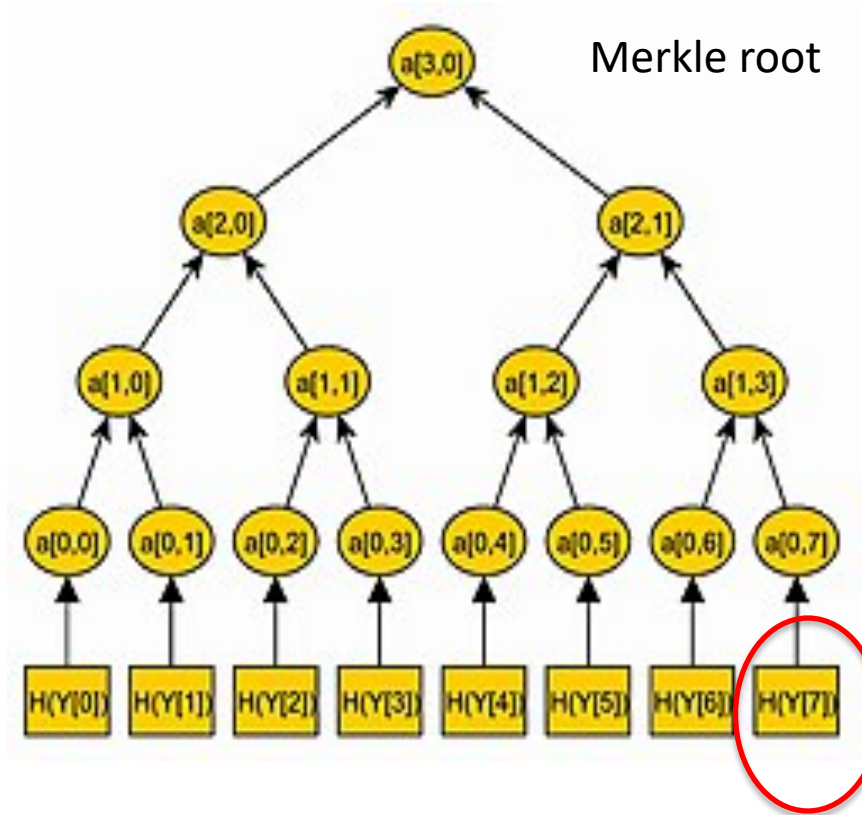
Merkle tree



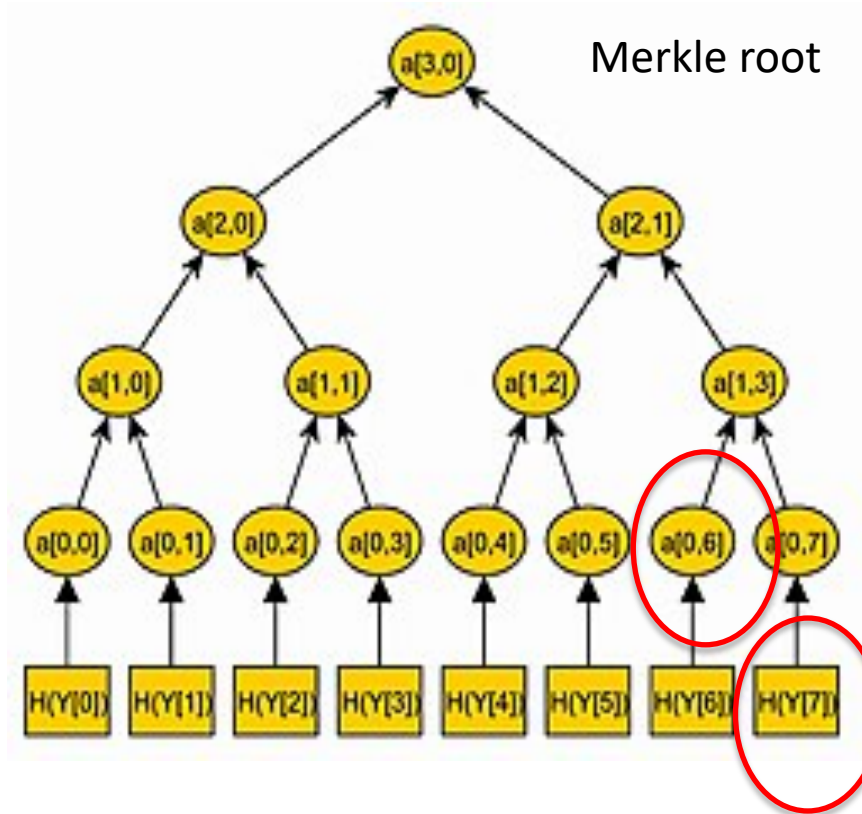
<https://commons.wikimedia.org/wiki/File:MerkleTree1.JPG>

Georg987 [CC BY-SA 3.0]

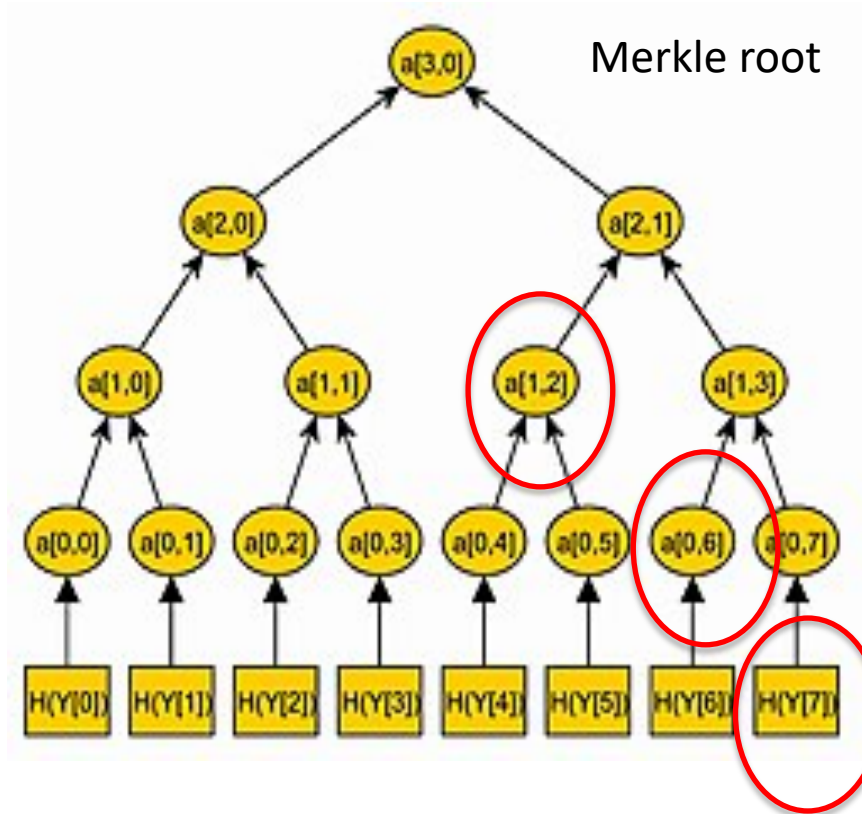
Merkle proofs



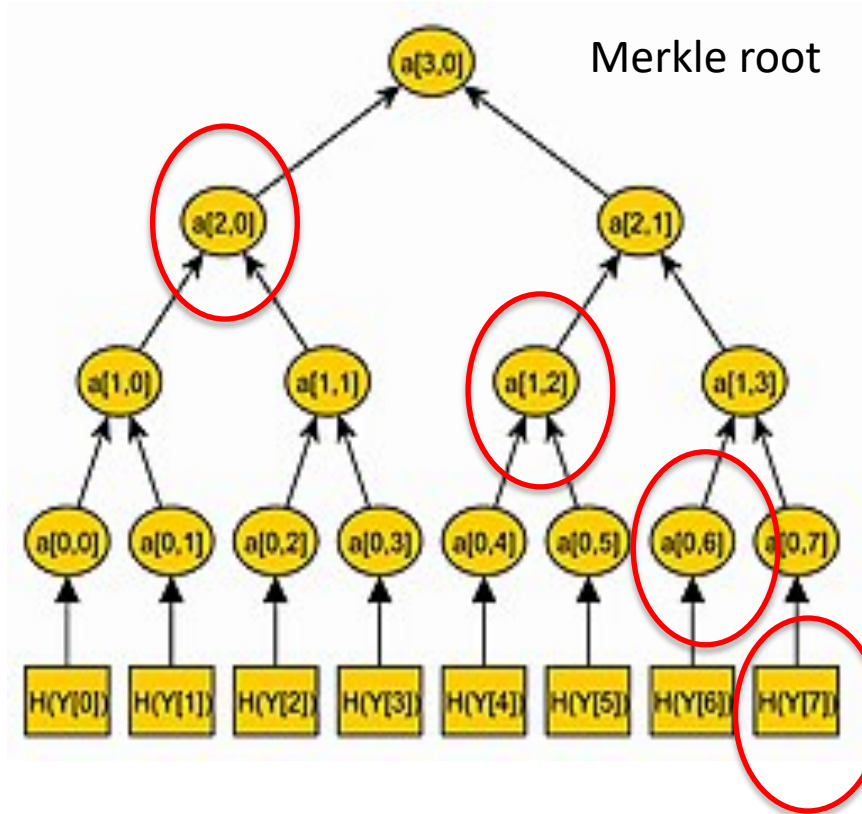
Merkle proofs



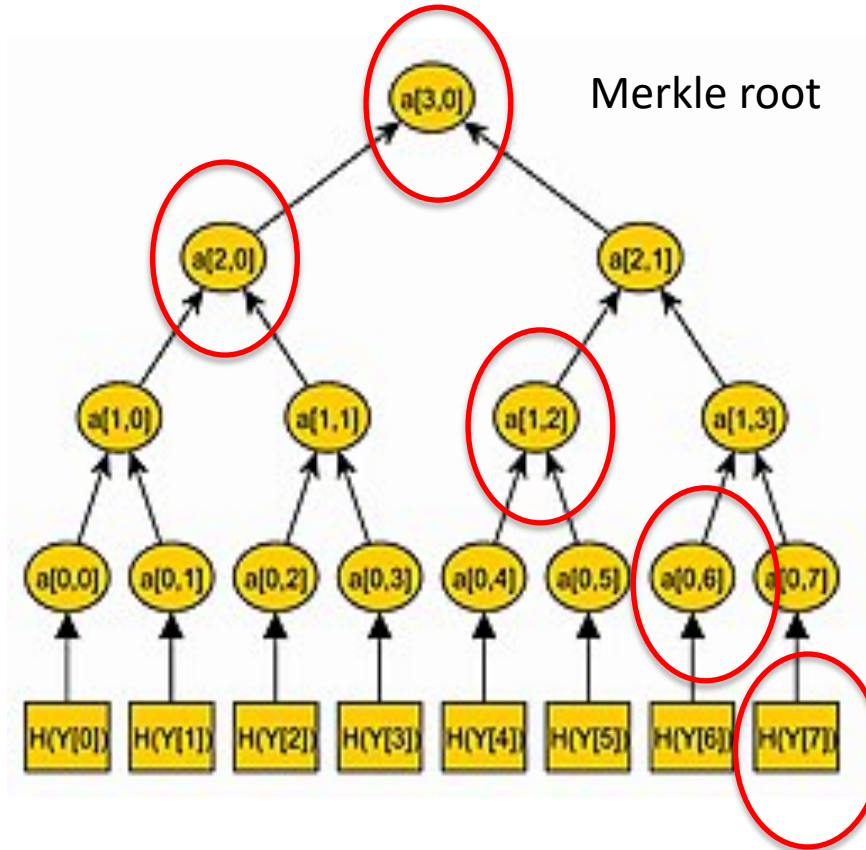
Merkle proofs



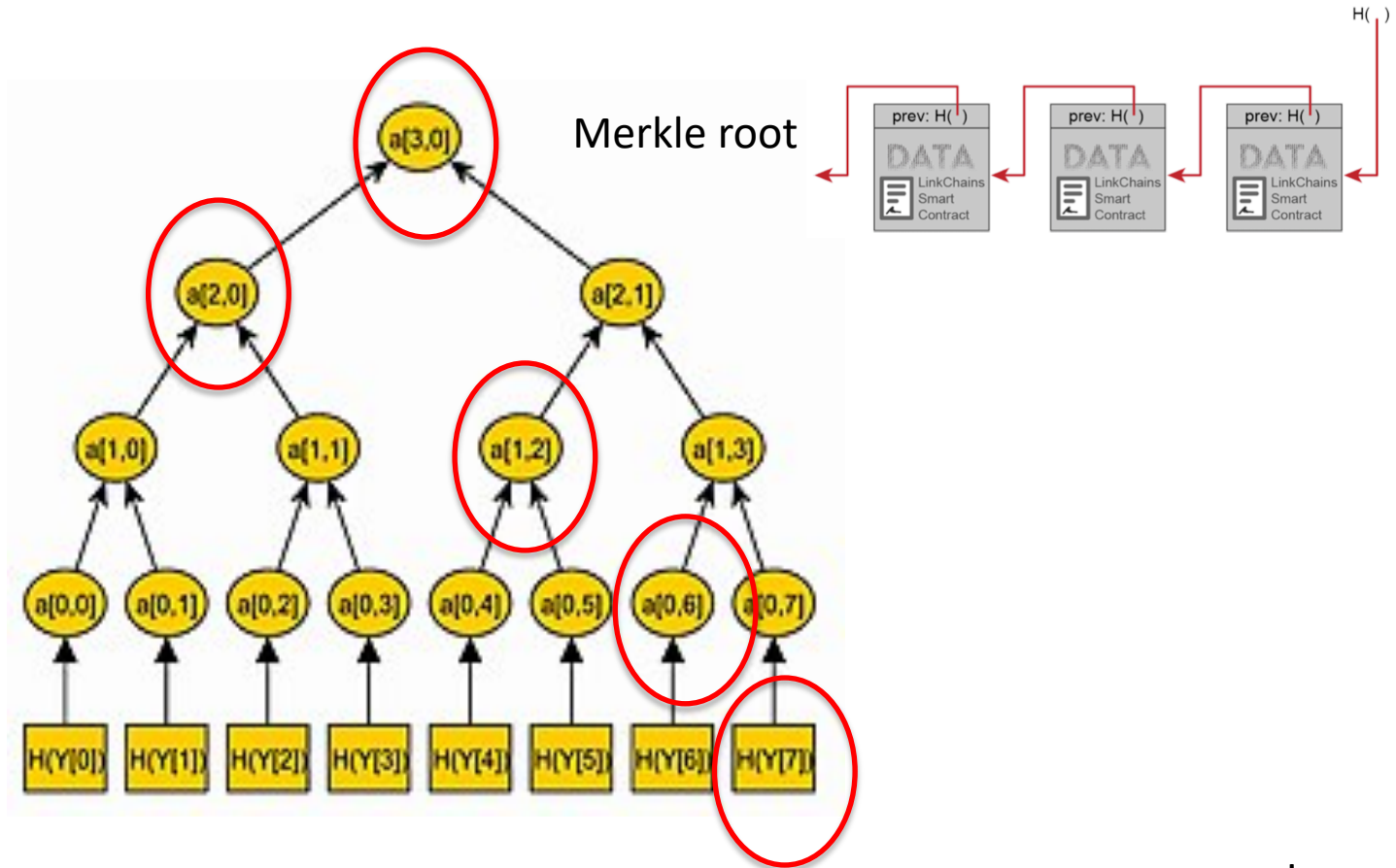
Merkle proofs



Merkle proofs



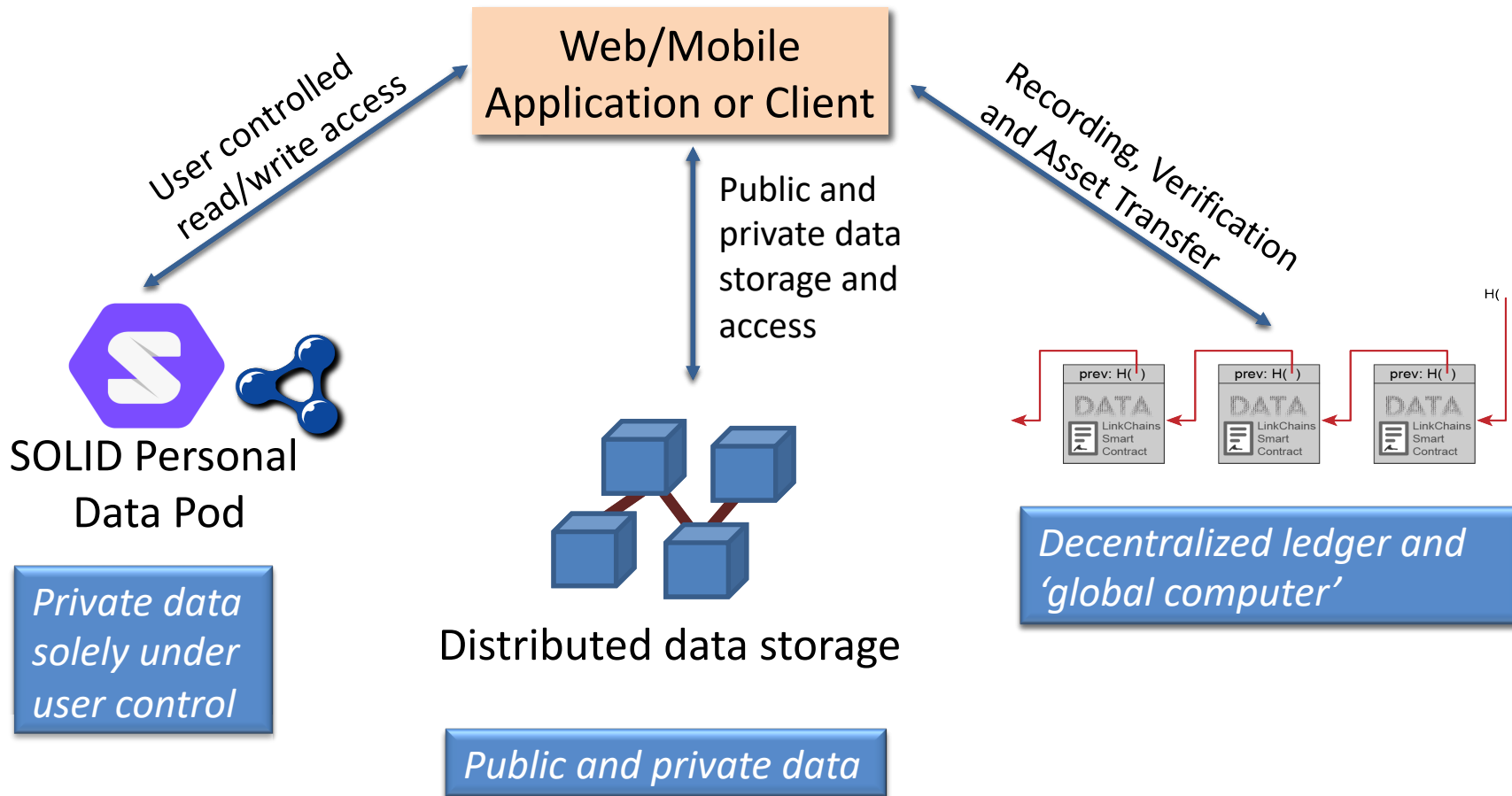
Merkle proofs



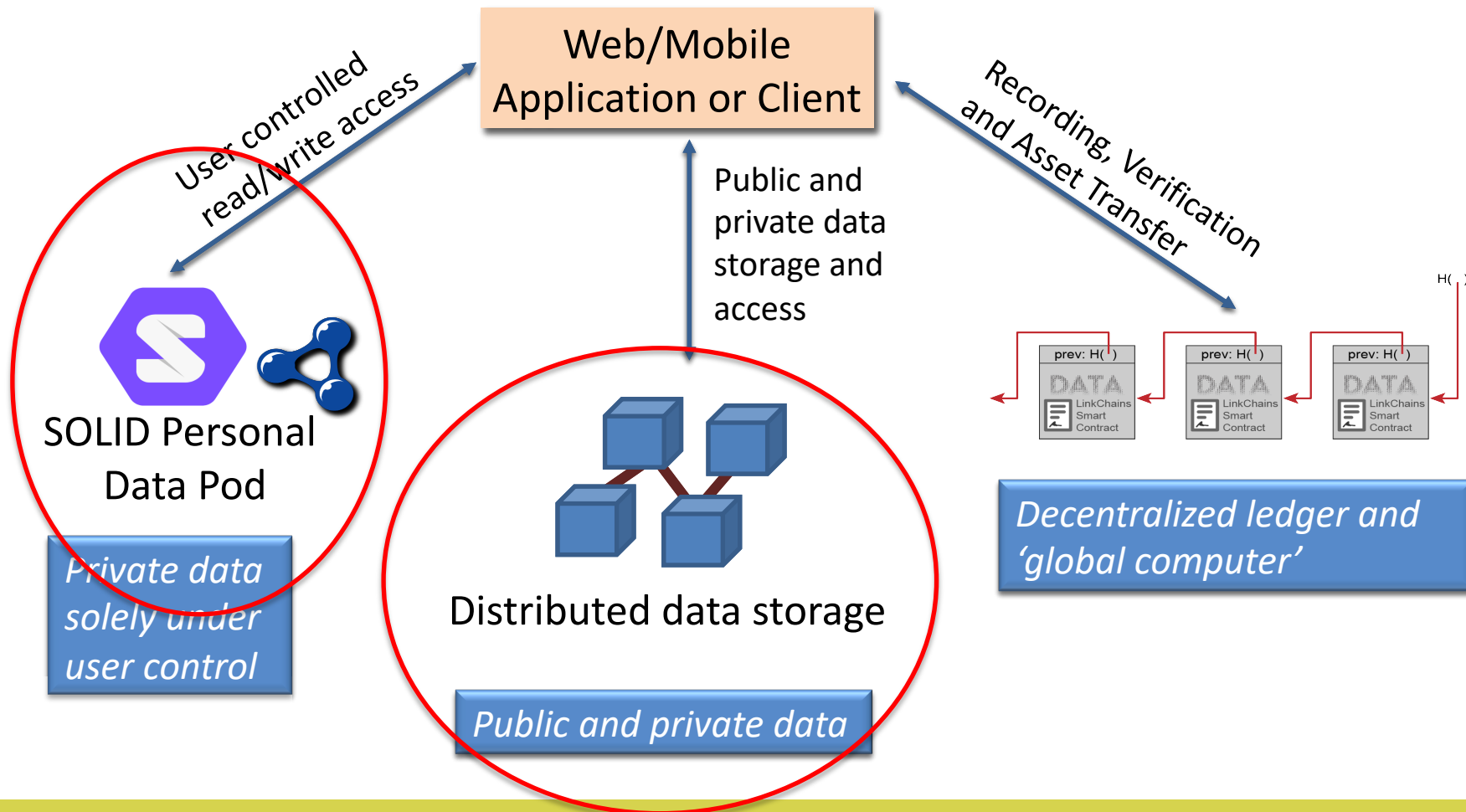
Per-quad/triple validation

```
{
  "status": "passed",
  "proof": {
    "merkleRoot": "5b134b80c0b992e056922be56c599d340c9d5276dda54d1445471c38f3dced84",
    "targetHash": "418943f1399ba2bce51cbd60aebb377b0e3671ab9f632afd91bf234411778526",
    "proof": [
      {"right": "418a116ba9a27c549437607dc84d0010cfbce0cb0e32e0e1daa8a6b55e86da00"},
      {"left": "16833b0d5a7cd03f71109b9ca01efcc082c6021d3d35bb364b4451f23aed7fc6"},
      {"right": "fc784afad2bd55058f956d99aadfec98a75d8385498e67948c4d66b912bf203a"},
      {"left": "86590531474fd823b4875a6a0f6c23d58d2a207d7cc35d796a920b935674d30e"},
      {"right": "35a6613975ec0398729ef92b15a314a2a1b8d4844bae398d97043b1e705e60a2"},
      {"left": "f37667d43d694cff2e6ee2ef01dd6362cd22cc3d0e0ed4cc1975bde04e89585f"},
      {"right": "81d227e827bdc630c365c1c3fa1e015f781db07c77f3782f816ca517aa01a6de"},
      {"right": "f3673355c6a2d19ff3a89ce0f937673ae0d7c72fa39f80303f0efcae2f25340"},
      {"right": "84e95530a4f2babab3aa0227c3a5a4cd8e14f9ccc5c2fae0de0c2988340f8ceb"},
      {"right": "1d0dd5373739992f1e19a203d021e053aff0f598bab298cf96c78cb171f6891e"},
      {"right": "7c1e105170ff2cab7a3d5f478c2ced218f2b0259854f1811353843a36d61bbd0"},
      {"left": "f8e9e8b80c20a21ebcc16ab31c7d81c0759ae2501d1ac353ffc471bf65ad8984"},
      {"right": "dc8fdb98d63d66e3c25720fc0b19e82e0324828c20b71bc50270f7449d608786"},
      {"left": "9d5ec06df58d69d9f48044bca72b1687e0cdbc50d1229bb9cab9aa8564e8709d"},
      {"right": "c8f68b0d2f7bcd520749afa065d8bf8158d34f511e9647622dd85e141f482e2"},
      {"right": "5c3e8f2c8147eaae235618fb3b936bf5443880172f7490e91addfd8ef550e6b4"}
    ]
  }
}
```

Verifiable VPD



Verifiable VPD



Thank you!

- Any questions?



<https://adecentweb.org>

Decentralized Web Symposium
Vienna, Austria, Jan 2020