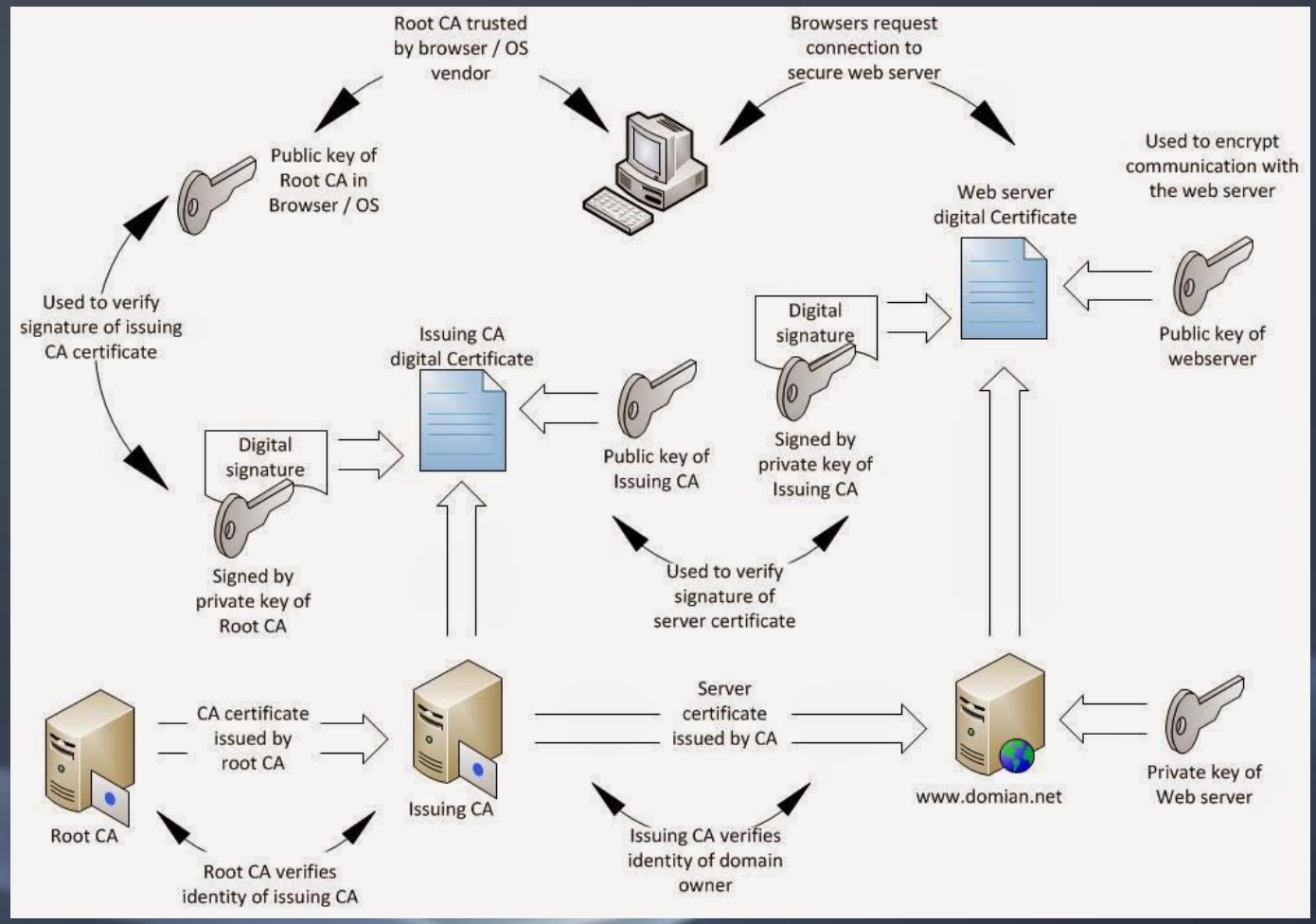
Trust of chain, chain of trust

neomabao

今天互联网的信任体系 - PKI

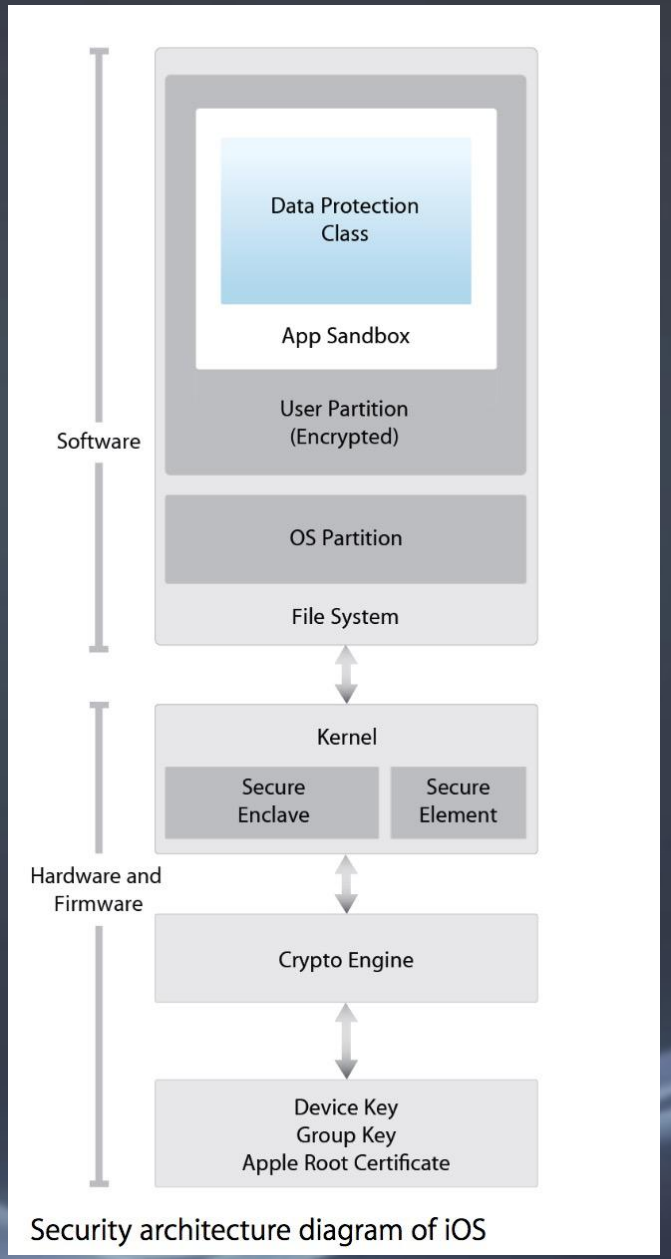
1. 中心化
2. 滥用
3. 盗用
4. 基础开源库



PKI is broken!

大公司都怎么了?

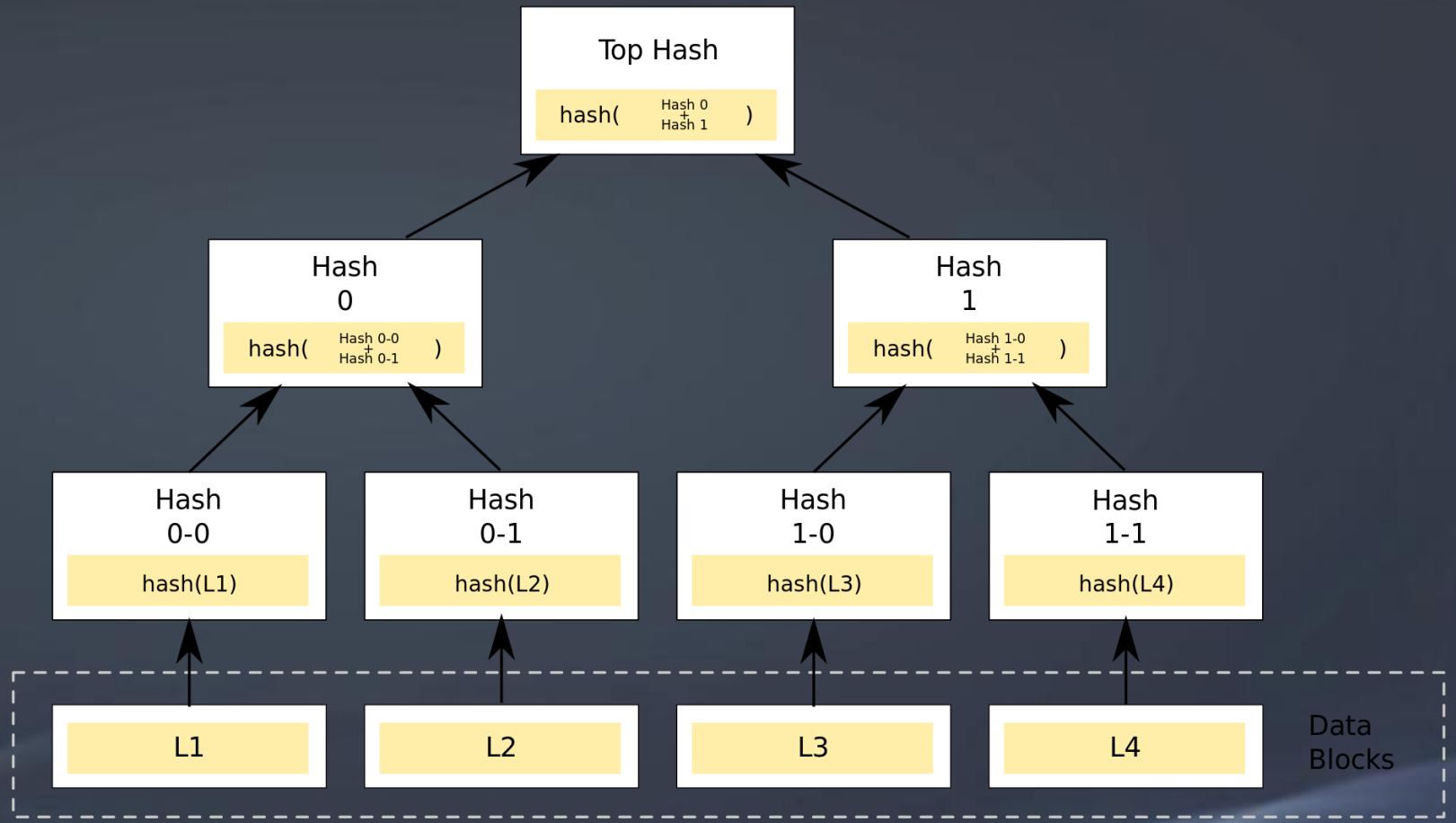
1. Apple, 世界上最安全的操作系统, 曾经
2. macOS High Sierra 空密码root问题
3. Iphone SEP/Intel ME
4. Android, 筛子
5. 英飞凌 ROCA
6. .....



Security architecture diagram of iOS

区块链

1. 信任之链
2. ECDSA, EdDSA, SHA, Merkle Tree...
3. PoW, PoS, dPoS, xBFT
4. 轻节点, 全节点
5. 钱包, 硬件钱包



钱包?!

钱包

1. 公私钥对
2. 推导(轮次)
3. secp256k1, ed25519
4. Brainpass
5. Paperwallet
6. Multi-sig
7. 硬件钱包
8. 热钱包/冷钱包
9. 智能合约
10. …

So?

1. 信任根
2. 随机数
3. Bottom to top安全
4. 补丁, 补丁, 补丁
5. 代码安全审计(fuzzer)
6. 智能合约 - K.I.S.S
7. Multi-sig – 逻辑
8. 离线签名
9. 硬件钱包 != 高枕无忧
10. 生物信息, no
11. 突发状况
12. …

私钥

THANK YOU!