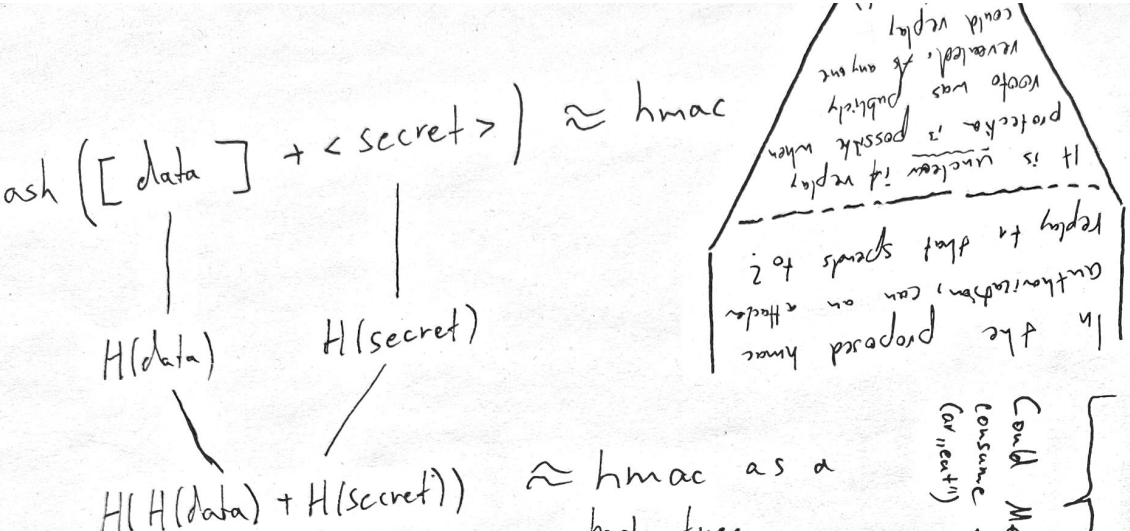
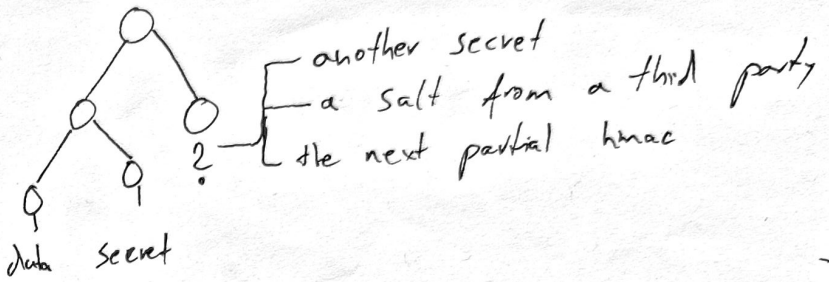
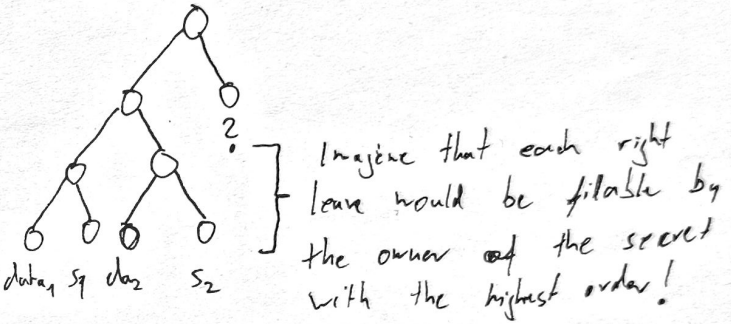
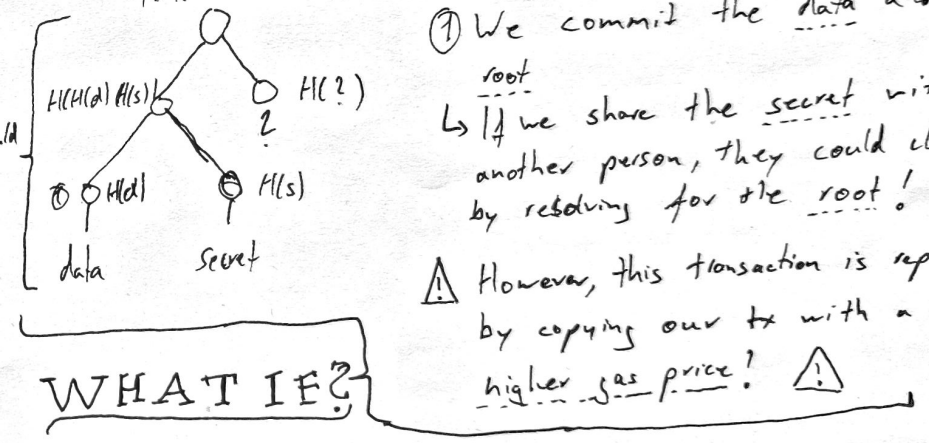
May 12, 2021



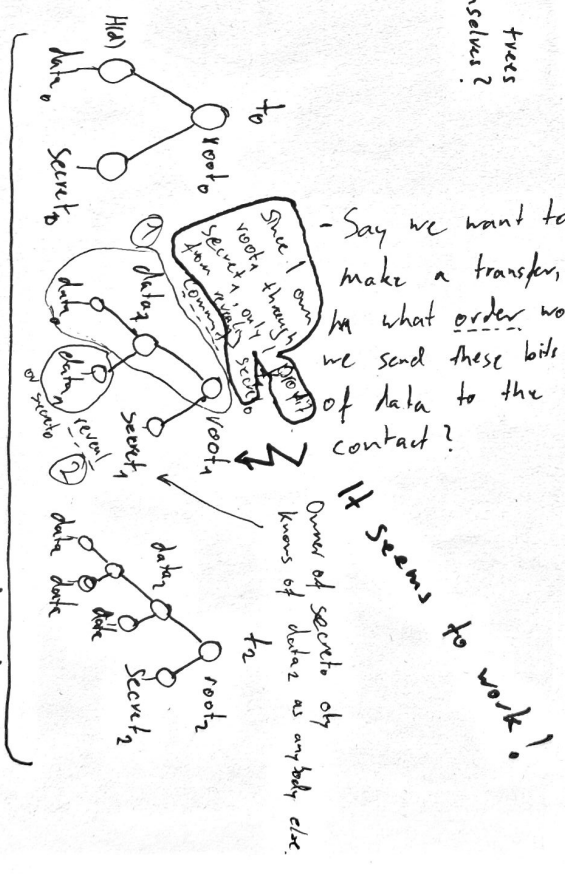






WHAT IF?

- ② was a nonce?
- the old merkle tree "ate" the old one?



- What is public here? A: data, root
- private ??? A: secret

How to spend to?
① Commit(tx, secret0) to reveal root1 which becomes data1, commitment is fulfilled.
② Send secret to another person along with H(data1).

Useful as alternative authorization schema for signatures.
- generating hashes in the EVM is cheap
- it seems only three 32 bytes values are necessary
- Construction is simple to evaluate and implement

① commit
② reveal
} To avoid a replay attack!