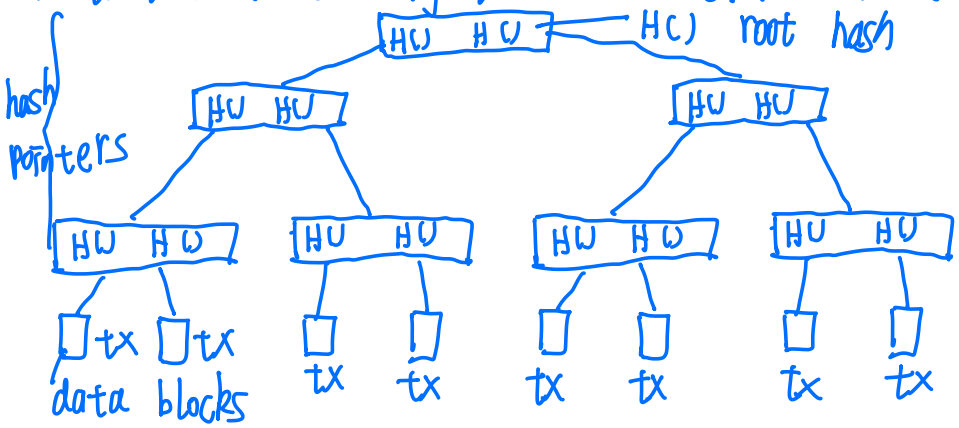
block-chain 示意图

every block has a hash point

every block 的 hash value 是由前一个 block 的所有信息计算而来，因此一旦有某个 chunk 被更改了，那么后续的都不会对上。

只要改一个，那么 most recent block 的 hash 也会改。

Merkle tree：与一般 binary tree 的区别：用 hash 指针代替了 simple 指针。



只 need remember root hash，可得到全树任何部位的修改。

bitcoin 中 every block 所包含的交易由 merkle tree 组织到一起并存储。

即 data block 中存一个 tx 交易

每个区块链分 2 部份：

block header：存 merkle tree 的 root hash 值

block body：存交易列表

merkle tree 提供了 merkle proof

比特币

全结点中包含 block header 与 block body

轻结点只包含 block header.

proof of membership式的证明

proof of non-membership

排序:

sorted merkle tree 证不存在. 但 bitcoin 不need!

只要 data-structure 无环即可用.

有环会出问题的。