Bitcoin:
Programming the Future of Money

Topics in Computer Science - ITCS 4010/5010, Spring 2025

Dr. Christian Kümmerle

Lecture 19

Merkle Trees

What is the problem that Bitcoin can solve?

WHAT IS THE PROBLEM?

Video by Joe Bryan
https://www.youtube.com/watch?v=YtFOxNbmD38&t=2157s

WHAT IS THE PROBLEM?

Questions:

- Explain the presented relationship between the “big red button” / money printing and wealth inequality.
- What is the relationship between the “big red button” and the breakdown of the nuclear family and declining birth rates?
- In which sense does the presented analysis present a “vicious cycle”?
- How are even the wealthy suffer from the Fiatello standard?

Merkle Trees

Consider following setup:

- Mohammed, a company owner in Dubai, operates an import/export business; he wishes to construct a company capital account with flexible rules. The scheme he creates requires different levels of authorization depending on timelocks. The participants in the multisig scheme are Mohammed, his two partners Saeed and Zaira, and their company lawyer.

  The three partners make decisions based on a majority rule, so two of the three must agree. However, in the case of a problem with their keys, they want their lawyer to be able to recover the funds with one of the three partner signatures.

  Finally, if all partners are unavailable or incapacitated for a while, they want the lawyer to be able to manage the account directly after he gains access to the capital account’s transaction records.

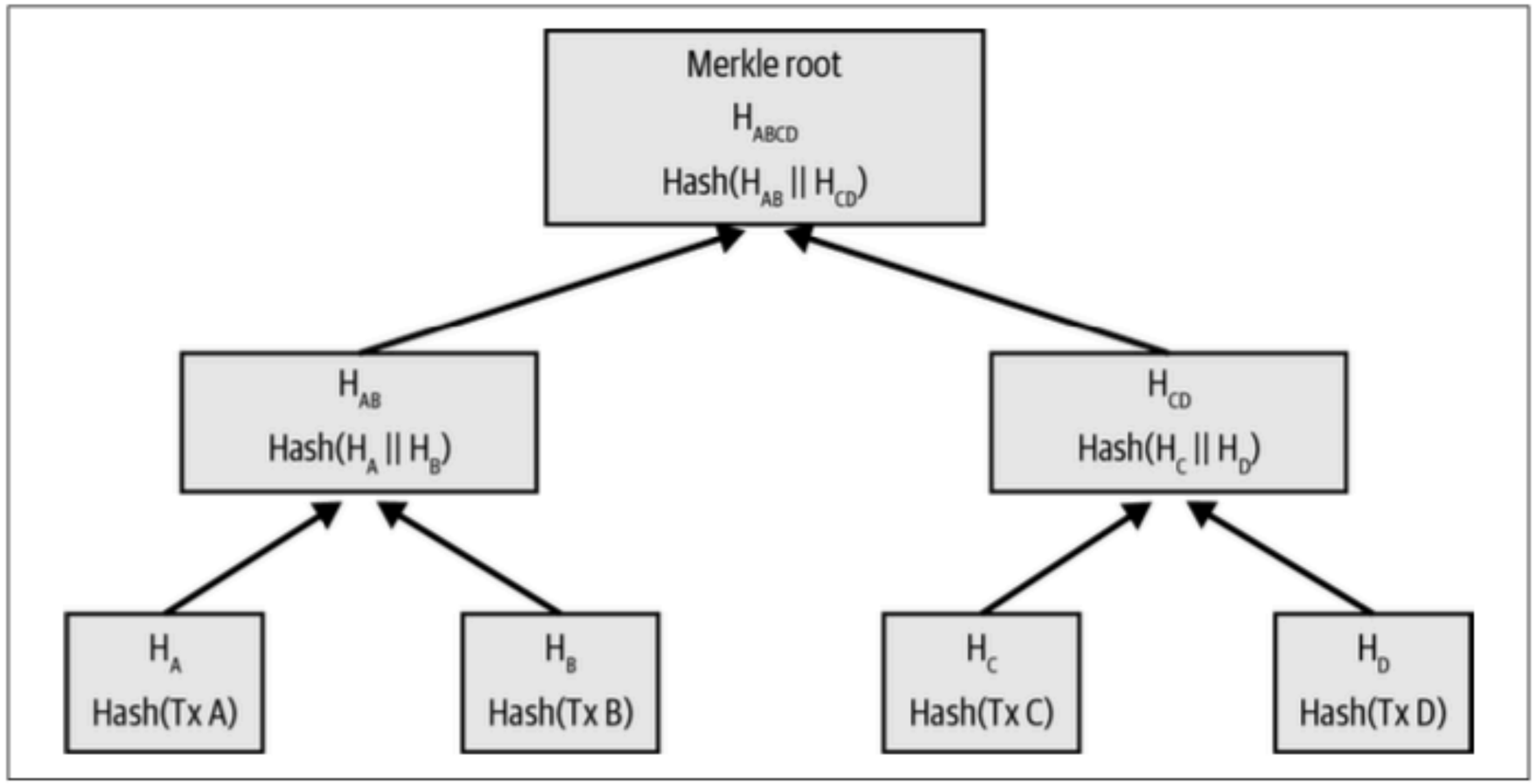
A MORE COMPLEX P2SH EXAMPLE

Redeem script of example above:

```
01  OP_IF
02    OP_IF
03      2
04    OP_ELSE
05      <30 days> OP_CHECKSEQUENCEVERIFY OP_DROP
06      <Lawyer's Pubkey> OP_CHECKSIGVERIFY
07      1
08    OP_ENDIF
09    <Mohammed's Pubkey> <Saeed's Pubkey> <Zaira's Pubkey> 3 OP_CHECKMULTISIG
10  OP_ELSE
11    <90 days> OP_CHECKSEQUENCEVERIFY OP_DROP
12    <Lawyer's Pubkey> OP_CHECKSIG
13  OP_ENDIF
```

Q: How to encode script such that only the spending condition that is used needs to be revealed?

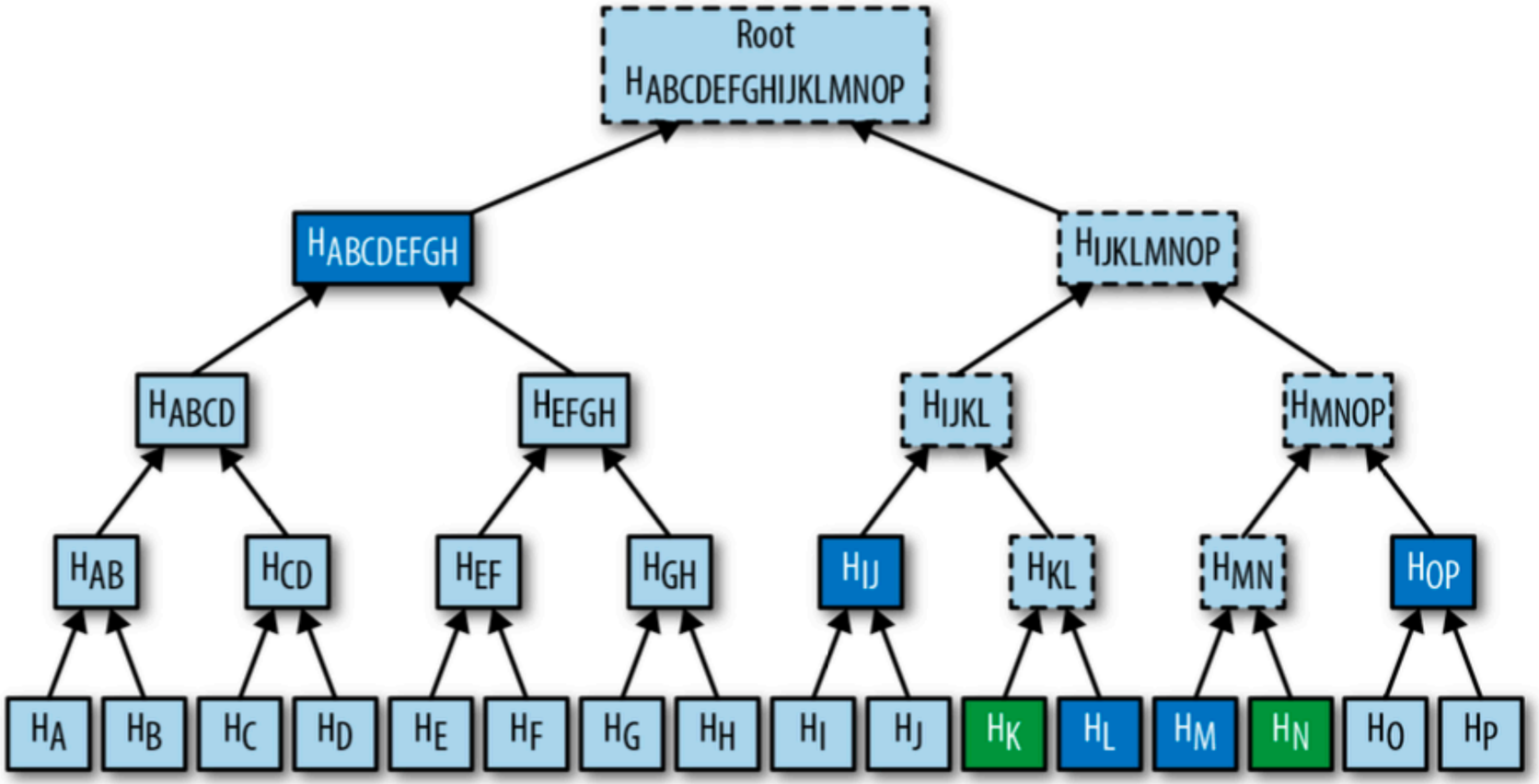
RECAP: MERKLE TREES FOR CONSTRUCTING MERKLE ROOT IN BITCOIN BLOCKS



- Verify membership of transaction in block in O(log n) time by providing “Merkle proof” of size O(log n), where n number of transactions in block.
- Sorted variant can prove non-membership of data in tree in O(log n)

MERKLE TREES AND MERKLE PROOFS

Setup:



- H_K and H_N are hashes of two data pieces K and N (e.g., representing two transactions)
- By providing the values in dark blue, the fact that K and N are indeed part of Merkle tree summarized by Merkle root $H_{ABCDEFGHHIJKLMNOP}$ can be proven (**"Merkle proof"**)

Applications of Merkle Trees in the Bitcoin protocol:

- Efficient Transaction Verification
- Data integrity
- Block header compactness
- Enables Merklized Alternative Script Trees (in Taproot)

MERKLE TREES

MERKLE TREES