Merkle Tree

Paolo Bettelini

Contents

1 Definition

```
                          ┌─────────────┐
                          │    Root     │
                          │ hash($_1^0$) │
                          └─────────────┘
                         ╱               ╲
              ┌──────────────┐        ┌──────────────┐
              │      0       │        │      1       │
              │ hash($_{01}^{00}$) │        │ hash($_{11}^{10}$) │
              └──────────────┘        └──────────────┘
               ╱          ╲            ╱          ╲
        ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐
        │   00    │ │   01    │ │   10    │ │   11    │
        │ hash(A) │ │ hash(B) │ │ hash(C) │ │ hash(D) │
        └─────────┘ └─────────┘ └─────────┘ └─────────┘
             │           │           │           │
        ┌────────┐  ┌────────┐  ┌────────┐  ┌────────┐
        │ Data A │  │ Data B │  │ Data C │  │ Data D │
        └────────┘  └────────┘  └────────┘  └────────┘
```
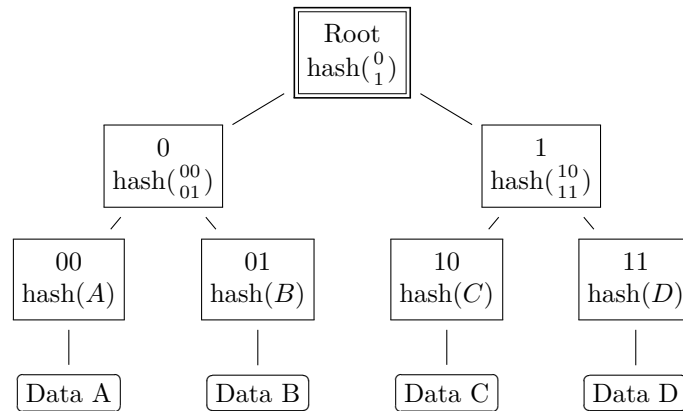
A Markle tree or hash tree is a tree where each node contains the hash of its children, and every leaf contains the hash of a data block.