Bayesian Neural Networks

Blair, Taylor Sorgmon, Ava Conor

March 21, 2024

Abstract

Bayesian Neural Networks are...

Contents

1 Introduction

1.1 Neural Networks

1.2 Bayesian Neural Networks

Bayesian Neural were invented by Ralph Merkle. Ralph Merkle initially patented Merkle trees for digital signatures....

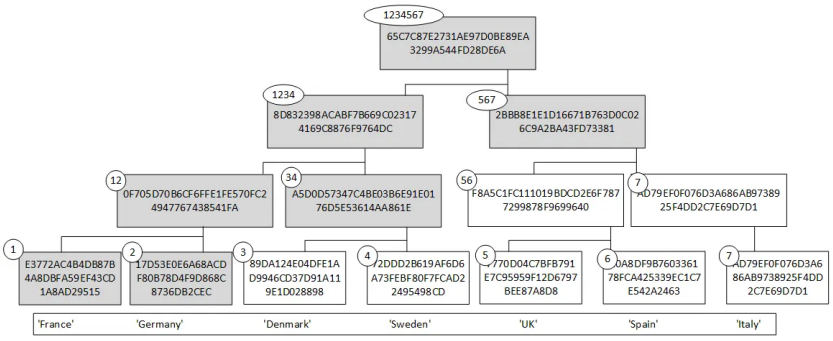

Figure 1: Basic Merkle Tree[6]

....

1.3 History

1987 The patent a 'Method of providing digital signatures' is filed by Ralph C. Merkle[5].

1999 The original patent expires.

2009 Bitcoin uses Merkle Trees for 'block header commitment.'[4]

2009 BitTorent uses Merkle Trees for data integrity[1].

2 Literature Review

Merkle Trees are a component of several projects, as such many papers provide incremental changes towards certain operations on Merkle trees. This paper references the original patent by Ralph Merkle [5] in addition to descriptions of Merkle tree operations given by Boneh and Shoup [2]. As secondary sources, the implementation of Merkle trees in Bitcoin [4] provides a real example of the impact of hash functions in addition to a whitepaper from the BitTorrent project[1].

3 Construction

Merkle trees are constructed from the bottom up by hashing data as the leaf nodes.

Algorithm 1 Merkle tree construction

for $i = 1, \ldots, n$ **do** ▷ Compute leaf node hashes

$y_i \leftarrow h(x_i)$

end for

for $j = 1, \ldots, n-1$ **do** ▷ Compute intermediate Nodes from $y_{n+1}, \ldots, y_{2n-1}$

$y_{i+n} \leftarrow h(y_{2i-1}, y_{2i})$ ▷ Hash leaf nodes below for new hash

end for

return Y ▷ Return tree where y_{2n-1} is the root

When referring to the parts of a Merkle tree the most common terminology is "root hash" which refers to the hashed value of the root of the tree and "leaf hash" which refers to the hash for a given data block.

4 How it works

5 Use Cases

...

6 Simulation

We used the Cifar 10....

7 Closing

References

Bakker, A. (2009). Bep 0030: Merkle hash torrent extension [[Online; accessed 4-May-2023]].

Boneh, D., & Shoup, V. (2020). A graduate course in applied cryptography. *Draft 0.5*.

Buchannen, B. (2022, January). Bloom filters, merkle trees and... accumulators. https://medium.com/asecuritysite-when-bob-met-alice/bloom-filters-merkle-trees-and-accumulators-27bc2f7baf5a

Friedenbach, M., & Alm, K. (2017, August). Fast merkle trees proposal. https://github.com/bitcoin/bips/blob/master/bip-0098.mediawiki

Merkle, R. C. (1979). Method of providing digital signatures. *Patent US4309569A*.

Wikipedia contributors. (2022). Merkle tree — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Merkle_tree&oldid=1123544588