Bayesian Neural Networks

Ava, Conor, & Taylor

Reed College

March 21, 2024

A Brief History

1979 — The patent a 'Method of providing digital signatures' is filed by Ralph C. Merkle [4].

1999 — The original patent expires.

2009 — Bitcoin uses Merkle Trees for 'block header commitment.' [3]

2023 — Twenty students taking a cryptography class .

Applications

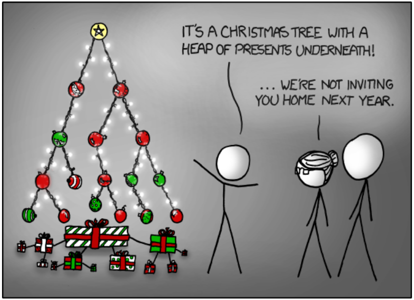

Figure: XKCD: " *Tree*" [6]

Merkle trees are secured data structures whose operations can be used to prove/verify membership of a node in $\mathcal{O}(\log(n))$ hashes.

Proving Membership (*singular*)

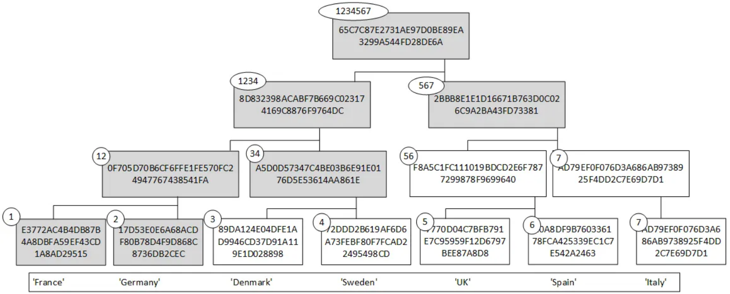

Figure: Show Germany exist in the tree [2]

Proving Membership (*multiple*)

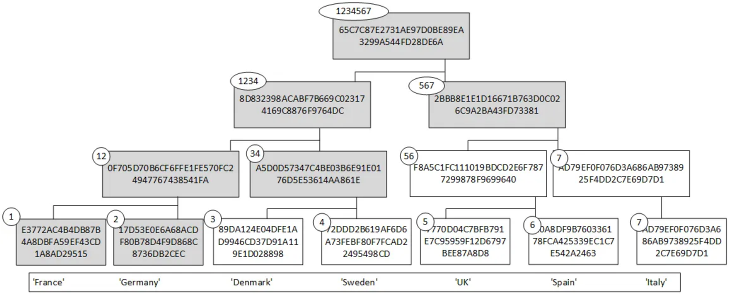

Figure: Show Germany **and** France exist in the tree [2]

Joining trees

See blackboard

Figure: Create a new root node and connect trees A and B [1]

Equality

See blackboard

Figure: Show trees A and B are equal.

Is it a secure authenticated data structure

> *We next define security. We say that an adversary defeats the scheme if it can output a hash*

We assume the underlying hash function h is collision resistant.

Authenticated data structure scheme syntax

An authenticated data structure scheme $\mathcal{D} = (H, P, V)$ defined over $(\mathcal{X}^n, \mathcal{Y})$ is a tuple of three efficient deterministic algorithms:

- H is an algorithm that is invoked as $y \leftarrow H(T)$, where $T := (x_1, \ldots, x_n) \in \mathcal{X}^n$ and $y \in \mathcal{Y}$.
- P is an algorithm that is invoked as $\pi \leftarrow P(i, x, T)$, where $x \in \mathcal{X}$ and $1 \leq i \leq n$. The algorithm outputs a proof π that $x = x_i$, where $T := (x_1, \ldots, x_n)$.
- V is an algorithm that is invoked as $V(i, x, y, \pi)$ and outputs accept or reject.
- We require that for all $T := (x_1, \ldots, x_n) \in \mathcal{X}^n$, and all $1 \leq i \leq n$, we have that

$$V(i, x_i, H(T), P(i, x_i, T)) = \text{accept}$$

Attack Game

For Merkle tree $D = (H, P, V)$ defined over $(\mathcal{X}^n, \mathcal{Y})$, and a given adversary $\mathcal{A}$:

> *The adversary A outputs a $y \in \mathcal{Y}$, a position $i \in \{1, \ldots, n\}$, and two pairs (x, π) and (x', π') where $x, x' \in \mathcal{X}$.*

$\mathcal{A}$ wins the game if $x \neq x'$ and $V(i, x, y, \pi) = V(i, x', y, \pi') =$accept. Define $\mathcal{A}$'s advantage with respect to $\mathcal{D}$, denoted $\mathrm{ADSadv}[\mathcal{A}, \mathcal{D}]$, as the probability that $\mathcal{A}$ wins the game.

Merkle hash tree scheme is a Secure Authenticated Data Structure Scheme

The Merkle hash tree scheme is a secure authenticated data structure scheme, assuming the underlying hash function h is collision resistant.

Lessons from Bitcoin

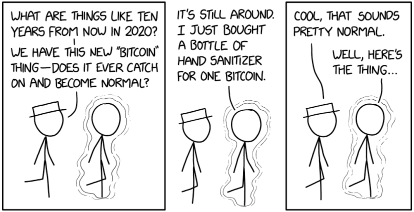

Figure: XKCD: "*2010 and 2020*" [7]

- ~~All cryptocurrencies are Ponzi schemes~~
- The *chain* is actually collection of root nodes.
- Bitcoin incorrectly implemented their merkle trees and it resulted in DOS attacks due to over hashing and duplicate nodes (CVE-2012-2459).

BitTorrent Data Integrity

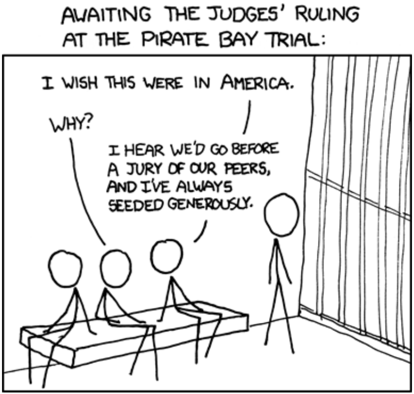

Figure: XKCD: "*Pirate Bay*" [5]

- Finding errors in $\mathcal{O}(\log(n))$!
- Only needing to compare nodes below incorrect nodes.

References I

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.*

Monroe, R. (2009, March). Xkcd: Pirate bay.

Monroe, R. (2010, December). Xkcd: Tree.

Monroe, R. (2020, March). Xkcd: 2010 and 2020.