Lead Golang Software Engineer

The candidate will prepare a presentation and accomplish a small coding assignment.

Agenda

- Presentation of the assignment (15 min)
- Technical presentation (20 min)
- Q&A on the presentation (10 min)

Scope of the presentation

You are expected to give a technical presentation of about 20 minutes on cryptographic hash functions, Merkle-trees and sparse Merkle-tree. The presentation may cover the security aspect of these constructions and their use-cases.

As the scope of the presentation is somewhat wide, you are free to deep dive in the areas where you feel the most competent. The audience is researchers and developers. Please let us know if you have any questions about this exercise.

Coding assignment

Implement a Merkle-tree in go. The candidate is free is to use a hash function of its choice provided the hash function provides 128 bits of security and has the correct properties.
 The implementation should allow for usual operations over Merkle-trees (generating a Merkle-proof, verifying a Merkle-proof and updating a leaf etc…).