**CS251: Cryptocurrencies and Blockchain Technologies**

Assignment #1

**Problem 1. A broken proof of work hash function**:

Với là cố định thì là cố định. Do vậy với yêu cầu , ta có thể làm như sau: Thử tất cả mọi trường hợp cho đến khi tìm được thỏa mãn .

Với có được này, khi mỗi được phát hành thì ta có thể tìm ra ngay lập tức bởi phép toán . Nên nhớ rằng là cố định vì vậy ta sẽ dùng thêm rất nhiều lần nữa, do đó hàm băm với là không an toàn cho cơ chế *proof-of-work*.

**Problem 2. Beyond binary Merkle tree:**

1. Ta sẽ tính với . Từ đó

Như vậy, để chứng minh nằm trong thì ta cần các giá trị .

Mô hình hóa quá trình tính như sau:

Hình vẽ sẽ update sau.

1. Gọi là hàm biểu diễn độ dài proof để chứng minh .

Ta có là chiều cao của Merkle tree. Ở mỗi độ sâu của Merkle tree, ta lại cần giá trị để tính được giá trị băm. Do vậy:

1. Với như trên và điều kiện đủ lớn, ta sẽ so sánh và .

Tức là ta so sánh và . Dễ thấy rằng với n đủ lớn cho nên lựa chọn dùng binary tree là tối ưu hơn.

**Problem 3. Bitcoin script:**

1. có dạng như sau:

Trong đó *Redeem Script* sẽ có dạng như sau:

1. Với mật khẩu chỉ có sáu ký tự thì hoàn toàn có thể bị tấn công vét cạn mật khẩu . Như vậy mật khẩu không làm yên tâm hơn so với khi không dùng mật khẩu này.

**Problem 4. BitcoinLotto:**

1. Để tránh trường hợp như trên, thì ta sẽ thiết kế lại để sao cho người chơi A nhận được đúng private key thì đồng thời sau locktime và được bên ban tổ chức ký thì mới có thể chứng minh rằng anh ta đã thắng cuộc.

Vậy với *ScriptPublicKey* chứa public key của jackpot theo cơ chế P2PK thì *ScriptSig* phải có dạng như sau:

Như vậy *ScriptPublicKey* có dạng:

**Problem 5. Lightweight clients:**

1. Giả sử transaction Alice gửi một khoản Bitcoin cho Bob nằm ở Block thứ kể từ Block gần nhất.

Do Bitcoin client mà Bob đang sử dụng chỉ cho Bob biết Block Header gần nhất, do đó, để Alice chứng minh được cô ấy đã chuyển tiền cho Bob thì cô ấy cần cho Bob biết được Block Header nào chứa transaction trên và chứng minh transaction đó thực sự nằm trong Block ấy.

Như vậy, Alice cần gửi cho Bob thông tin hash pointer của Block Header ở giữa để Bob biết được transaction này ở Block nào. Để chứng minh transaction nằm trong Block ấy thì Alice cần đưa cho Bob proof của Merkle tree cho transaction này.

Tòm lại, Alice cần gửi thông tin các hash pointer của Block Header ở giữa cùng với proof của Merkle tree trên Block ấy.

1. Gọi là hàm biểu diễn độ dài proof tính bằng byte biểu diễn theo và .

Mỗi hash pointer dài bit, tương đương với byte và mỗi nút trong Merkle cũng có đọ dài byte do đều dùng hàm băm .

Như vậy, kết hợp với câu a, ta được với và với .

Vậy bytes

1. Chưa hiểu tính như nào ??