Class 23: Sidechains

Schedule

Each team will have an opportunity to present their project the last three classes (April 20, 22 and 27). Teams will sign up for presentation slots at Monday's class. Final projects are due by 11:59pm on Sunday, 3 May.

Thursday, 6pm Commerce School 223. *Entrepreneurial and Career Ventures in the world of Digital Currency* Panel.

Friday, 10:45am Rice 242. Suman Jana, *Rise of the Planet of the Apps: Security and Privacy in the Age of Bad Code.*

Bloom Filters

Burton Bloom, *Space/Time Trade-offs in Hash Coding with Allowable Errors*, Communications of the ACM, July 1970.

Conventional Hash Table

Store collection of N b-bit elements, using $k > N$ cells.

H is pseudorandom function, $H(x) \leftarrow [0, k)$.

Bloom Filter

Tradeoff: shrink size of array to store, accept false matches.

m = number of bits in array
k = number of hash functions
n = number of elements

What is the probability a given element of the array is not selected by a particular hash function?

What is the probability a given element of the array is not selected for a particular element by any of the k hash functions?

After n elements, what is the probability that an array bit is 0?

Probability of false match:

$$(1-(1-1/m)^{kn})^k$$

How big should m be to have less than 0.01% false positive rate for a block with 1000 addresses?

How much privacy does using a bloom filter provide to an SPV wallet?