Finding the probability of linking twitter user a to bitcoin public key b, assuming a 1-to-1 mapping.

Carolyn Atterbury

May 2, 2019

Suppose we have a set A of n users from Twitter, and a set B of m users in Bitcoin, we can come up estimate of the probability $P(a_i, b_j)$ of user $a_i \in A$ in Twitter having public key $b_j \in B$ in Bitcoin, assuming there is a one-to-one mapping between the two sets.

Proof:

Let A be the set of Twitter Users, such that $|A| = n$. Let $a \in A$.

Let B be the set of Bitcoin Public Keys, such that $|B| = m$. Let $b \in B$ Suppose $m > n$.

We want to find $P(a, b)$, the probability of user a having the public key b, where

$$P(a, b) = \frac{\text{The number of mappings where } f(a) = b}{\text{Total number of mappings}}$$

Let $F(A, B) = \{f : A \to B \text{ such that f is an injection}\}$.

We know that $|F(A, B)| = \binom{m}{n} \cdot n! = \frac{m!}{(m-n)!}$.

If we fix a and b such that $f(a) = b$,

then let $F(A', B') = \{f' : A' \to B' | A' = A - \{a\}, B' = B - \{b\}\}$.

Since $|A - \{a\}| = m - 1$ and $|B - \{b\}| = n - 1$, then $|F(A', B')| = \binom{m-1}{n-1} \cdot (n-1)! = \frac{(m-1)!}{(m-n)!}$.

So,

$$\begin{aligned} P(a,b) &= \frac{\text{The number of mappings where } f(a)=b}{\text{Total number of mappings}} \\ &= \frac{|F(A',B')|}{|F(A,B)|} \\ &= \frac{(m-1)!}{(m-n)!} \Big/ \frac{m!}{(m-n)!} \\ &= \frac{(m-1)!}{m!} \\ &= \frac{1}{m} \end{aligned}$$

Assuming there is a one-to-one mapping between set the Twitter users in set A and the Bitcoin users in set B, then the probability of a Twitter user a having the public key b is $P(a,b) = \frac{1}{m}$.