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 $b \in B$

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

We know that $|F(A, B)| = (n)(n-1)(n-2)...(n-m+1) = \frac{n!}{n-m!}$

Let

$$f_{f1}(x) = \begin{cases} b & x = a \\ f'_a(x) & otherwise \end{cases}$$

where, $f' \in F(A_a, B_b) | A_a = A - \{a\}, B_b = B - \{b\}$.

Since $|A - \{a\}| = m - 1$ and $|B - \{b\}| = n - 1$,

then $|F(A_a, B_b)| = \frac{(n-1)!}{((n-1)-(m-1))!} = \frac{(n-1)!}{(n-m)!}$.

So,

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

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 $P(a,b) = \frac{1}{n}$.