This doc was written by andytoshi on Jan 8 2013.

1 The Birthday Paradox

Suppose you have n people in a room, none of whom were born on February 29th. What is the likelihood that two of them will share a birthday?

The answer is easy to calculate, and may surprise you. To do the calculation, consider each person in order (any order you want, just be consistent). The first person might have a birthday on any of the 365 days of the year without conflict, so we have a 365/365 chance of no conflict.

The second person has 364 days his birthday might be to avoid a conflict, so he has a 364/365 chance of no conflict.

The third person has 363 days to choose from, if there is to be no conflict, and so on. We see that the chance of there *not* being a conflict is

$$\frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \cdots \times \frac{(365-n+1)}{365} = \frac{365!}{365^n (365-n)!}$$

and the chance of there being a conflict is one minus this quantity. We hack together some code to check:

```
(defun fact (n) (if (zerop n) 1 (* n (fact (1- n)))))
(defun birthday (n) (/ (fact 365) (fact (- 365 n)) (expt 365 n)))

(- 1.0 (birthday 1))
(- 1.0 (birthday 5))
(- 1.0 (birthday 10))
;;; and so on
```

With one person, the chance of collision is 0, as expected. With two people, it is 1/365, or 0.0027, also as expected. But it grows quickly:

n	Probability of collision
5	0.027135551
10	0.11694819
20	0.4114384
30	0.70631623
50	0.9703736

Wow! With only 30 people, there is a 7 in 10 chance of a collision. With 50 people, the chances grow to 97%.

2 Bitcoin Addresses

Now, what are the chances that two people will wind up using the same bitcoin address? There are 2^{160} bitcoin addresses in the universe, which is a fair bit larger than the 365

birthdays in the universe, but the problem is essentially the same. Our formula becomes

$$\text{chance of collision} = 1 - \frac{2^{160}!}{2^{160n}(2^{160}-n)!}$$

By inspection, we see that the chances are going to be zero for any n less than a million or so, and we have no hope of calculating with any larger n. So what can we do?

Well, thanks to famous mathematicians Abraham de Moivre and James Stirling, we have *Stirling's formula*, an easy-to-compute approximation to the factorial function. It looks like

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

We use this as

$$\begin{aligned}
\frac{2^{160}!}{2^{160n}(2^{160}-n)!} &\approx 2^{-160n}\frac{(2^{160}/e)^{2^{160}}}{((2^{160}-n)/e)^{2^{160}-n}} \\
&= 2^{-160n}e^{-n}\frac{2^{160\times 2^{160}}}{(2^{160}-n)^{2^{160}-n}} \\
&= e^{-n}\frac{2^{160\times(2^{160}-n)}}{(2^{160}-n)^{2^{160}-n}} \\
&= e^{-n}\left(\frac{2^{160}}{2^{160}-n}\right)^{2^{160}-n} \\
&= \exp\left[(2^{160}-n)\log\left(\frac{2^{160}}{2^{160}-n}\right)-n\right]
\end{aligned}$$

So our chance of collision is

$$1 - \exp\left[(2^{160}-n)\log\left(\frac{2^{160}}{2^{160}-n}\right)-n\right]$$

When will this exceed some threshold ϵ? We solve

$$\epsilon = 1 - \exp\left[(2^{160}-n)\log\left(\frac{2^{160}}{2^{160}-n}\right)-n\right]$$

If n is smaller than 2^{159} or so, the quantity inside the logarithm will be very close to 1, so we do a Taylor expansion about 1 to get a second-order approximation. (Notice that $(1-2^{160}/(2^{160}-n))$ is bounded between 0 and 1, so our error is on the order $O(1)$ in n. But that doesn't really tell us anything.)

$$\begin{aligned}
\epsilon &= 1 - \exp\left[(2^{160}-n)\left(\left(\frac{2^{160}}{2^{160}-n}-1\right)-\frac{1}{2}\left(\frac{2^{160}}{2^{160}-n}-1\right)^2\right)-n\right] \\
&= 1 - \exp\left[(2^{160}-n)\left(\left(\frac{n}{2^{160}-n}\right)-\frac{1}{2}\left(\frac{n}{2^{160}-n}\right)^2\right)-n\right] \\
&= 1 - \exp\left[-\frac{1}{2}\frac{n^2}{2^{160}-n}\right]
\end{aligned}$$

Okay, so

$$\log(1-\epsilon) = -\frac{1}{2}\frac{n^2}{2^{160}-n} + \frac{1}{3}\frac{n^3}{(2^{160}-n)^2}$$

$$n^2 - 2n\log(1-\epsilon) + 2^{161}\log(1-\epsilon) = 0$$

$$n = \log(1-\epsilon) \pm \sqrt{[\log(1-\epsilon)]^2 - 2^{161}\log(1-\epsilon)}$$

It's obvious that the second term will dominate, so we have our estimate:

$$n = \sqrt{[\log(1-\epsilon)]^2 - 2^{161}\log(1-\epsilon)}$$

For $\epsilon = 50\%$, this gives $n = 1.41 \times 10^{24}$. For $\epsilon = 90\%$, we get roughly twice this amount.

3 Should I be worried?

Using this result, we calculate that for a 0.1% probability of collision, we would need 5.4×10^{22} addresses in existence. For a 99.9999% chance, we would need 6.35×10^{24} addresses.

So, even if there were 10^{22} bitcoin addresses generated, a collision simply will not happen. But if there were 10^{25} addresses generated, a collision absolutely would happen.

Should we worry about this? **No**, for four independent reasons.

- The chance of getting a *specific* collision, say, a collision with one of your addresses, is still 1 in 2^{160} or 1 in 10^{48}. So even if you've got a million million million addresses, nobody has a chance of colliding with you.

- At the time of this writing, there are less than 10^7 addresses in use in the network. So anyone with 10^{25} addresses would only be colliding their own addresses.

- Each address takes around 100 bytes to store. (Actually about half that, but we only care about orders of magnitude.) So for the network to support 10^{25} addresses, it would take 10 million million terabytes of storage just to record them.

  This is not even touching the problem of searching such a huge data store.

  Further, according to sipa, if the current mining network (which is at 25 THash, and the most powerful computing network in the history of the world) were switched over to address generation, the network could generate 2.5×10^{12} addresses per second (one address generation corresponding to roughly 10 hashes). At that rate, it would take 127,000 years to get so many addresses. It is debatable whether *homo sapiens sapiens* has walked the earth for so long.

- With 21 million bitcoins ever existing, and 8 decimal places of divisibility, at most 2.1×10^{14} can possibly have money on them at once.

  But in a space of 10^{24} addresses, this means that only one in 10^{12} addresses could possibly have money on them. So an attacker, after doing the physically impossible a

trillion times over, has only a one in a trillion chance of getting even one satoshi out of it.