On a calculation from the Bitcoin white paper

Matthew F. Lapa
mflapa1234@gmail.com

I. INTRODUCTION

In this note we explore in more detail an interesting calculation from the Bitcoin white paper by Satoshi Nakamoto [1]. The reader should keep in mind that this note is for educational purposes only, and we do not make any claims that the contents of this note represent original research.

In Section 11 of the Bitcoin white paper, Nakamoto presents a calculation of the probability that an attacker can successfully attack the blockchain when he is z blocks behind the chain built by the honest nodes. Nakamoto first derives a formula for the probability that the attacker succeeds, and then he writes a C program to evaluate this formula numerically in several examples. The output of this numerical calculation seems to indicate that the attacker's probability of success decays *exponentially* with z (the number of blocks he is behind), provided that the honest nodes have more CPU power (more computational resources) than the attacker.

In this short note we examine Nakamoto's formula for the probability that the attacker succeeds, and we present a rigorous mathematical proof that this probability does indeed decay exponentially with z when the honest nodes have more CPU power than the attacker. Therefore, at least within this simple model, we can be confident of the security of the blockchain as long as the honest nodes control more than 50 percent of the total computational resources.

II. NOTATION

Let q denote the fraction of the total CPU power that is controlled by the attacker. We have $0 \leq q \leq 1$. Then $p = 1 - q$ is the fraction of the total CPU power that is controlled by the honest nodes. In our calculation we assume that $q < p$, which means that

$$q < 0.5 \ . \tag{2.1}$$

In other words, we assume that the honest nodes control more CPU power than the attacker. We also assume that $q > 0$, so that the attacker controls some non-zero amount of the total CPU power. Finally, the positive integer z represents how far behind (in blocks) the attacker is compared to the blockchain built by the honest nodes.

Given this notation, we define $P(z;q)$ to be the probability that the attacker will succeed. Nakamoto's expression for $P(z;q)$ can be written in the form

$$P(z;q) = \sum_{k=0}^{z} e^{-\lambda} \frac{\lambda^k}{k!} \left(\frac{q}{p}\right)^{z-k} + \sum_{k=z+1}^{\infty} e^{-\lambda} \frac{\lambda^k}{k!} \ , \tag{2.2}$$

where

$$\lambda = z \frac{q}{p} \tag{2.3}$$

is the parameter in the Poisson distribution that describes the attacker's potential progress.

To close this section, note that if $q = p = 0.5$, then $P(z;q) = 1$, so the security of the blockchain will be compromised if the attacker controls half (or more) of the total computational resources.

III. MAIN RESULT AND EXPLANATION

In this note we prove the following theorem.

Theorem 1. *Suppose that $q < p$, so the attacker controls less than half of the total CPU power. Then the probability $P(z;q)$ that the attacker succeeds is bounded from above as*

$$P(z;q) \leq c_1(q) e^{-c_2(q) z} \ , \tag{3.1}$$

where $c_1(q)$ and $c_2(q)$ are given by

$$c_1(q) = 1 + e\frac{q}{p} \tag{3.2a}$$

$$c_2(q) = \frac{q}{p} - 1 - \ln\left(\frac{q}{p}\right) . \tag{3.2b}$$

If $q < 0.5$, then $c_2(q) > 0$, and so $P(z;q)$ decays exponentially *with z when the attacker controls less than half of the total CPU power.*

To understand the last sentence in this theorem, note that for all $x \in (0,1)$ the natural logarithm obeys the strict inequality

$$\ln(x) < x - 1 . \tag{3.3}$$

Therefore, if $q < p$ (which holds for $q < 0.5$), then $\frac{q}{p} < 1$ and $c_2(q)$ is positive, and so $P_2(z;q)$ decays exponentially with z.

As a side note, we can prove the inequality (3.3) by using the fundamental theorem of calculus to write

$$\ln(x) = -\int_x^1 dy\, \frac{1}{y} . \tag{3.4}$$

Next, we note that for $y \in (x,1)$ (with $x > 0$ and $x < 1$) we have $-\frac{1}{y} < -1$, and so

$$\ln(x) < -\int_x^1 dy\, 1 . \tag{3.5}$$

Then, since $-\int_x^1 dy\, 1 = x - 1$, we arrive at the inequality (3.3).

IV. THE PROOF

To prove our theorem we first split $P(z;q)$ into two pieces as $P(z;q) = P_1(z;q) + P_2(z;q)$, where

$$P_1(z;q) = \sum_{k=0}^{z} e^{-\lambda}\frac{\lambda^k}{k!}\left(\frac{q}{p}\right)^{z-k} \tag{4.1}$$

and

$$P_2(z;q) = \sum_{k=z+1}^{\infty} e^{-\lambda}\frac{\lambda^k}{k!} . \tag{4.2}$$

We first bound $P_1(z;q)$. Using the fact that $\lambda = z\frac{q}{p}$, we can rewrite $P_1(z;q)$ in the form

$$P_1(z;q) = e^{-\lambda}\left(\frac{q}{p}\right)^z \sum_{k=0}^{z}\frac{z^k}{k!} . \tag{4.3}$$

Then, since $\sum_{k=0}^{z}\frac{z^k}{k!} \le e^z$, we have

$$P_1(z;q) \le e^{-\lambda}\left(\frac{q}{p}\right)^z e^z . \tag{4.4}$$

Finally, we can use $\lambda = z\frac{q}{p}$ and the identity $a^z = e^{z\ln(a)}$ to rewrite this bound in the form

$$P_1(z;q) \le e^{z - z\frac{q}{p} + z\ln\left(\frac{q}{p}\right)} . \tag{4.5}$$

Next, we derive a bound on $P_2(z;q)$. This term is actually equal to a *tail probability* for the Poisson distribution, and it can be bounded from above using a *Chernoff bound*. However, in this note we do not directly use the Chernoff bound. Instead, we use an equivalent method that allows us to avoid introducing too much of the notation of probability theory.

To bound $P_2(z;q)$ we note that, for any real number α satisfying $\alpha \geq 1$, we have the upper bound

$$P_2(z;q) \leq \sum_{k=z+1}^{\infty} e^{-\lambda} \frac{\lambda^k}{k!} \frac{\alpha^k}{\alpha^{z+1}} \,, \tag{4.6}$$

which holds because $\alpha^k \geq \alpha^{z+1}$ if $k \geq z+1$ and $\alpha \geq 1$. Then, since $\sum_{k=z+1}^{\infty} \frac{(\alpha\lambda)^k}{k!} \leq e^{\alpha\lambda}$, we have

$$P_2(z;q) \leq \frac{1}{\alpha^{z+1}} e^{-\lambda} e^{\alpha\lambda} \,, \tag{4.7}$$

which can be rewritten in the form

$$P_2(z;q) \leq e^{-\lambda+\alpha\lambda-(z+1)\ln(\alpha)} \,. \tag{4.8}$$

To proceed from here, we find the value of $\alpha \geq 1$ that minimizes the function

$$f(\alpha) = \alpha\lambda - (z+1)\ln(\alpha) \,. \tag{4.9}$$

If we plug this special value of α back into our bound, then this will give us the tightest bound on $P_2(z;q)$. To find this minimizing value we examine the first derivative of $f(\alpha)$ with respect to α and search for solutions to $\frac{df(\alpha)}{d\alpha} = 0$. We have

$$\frac{df(\alpha)}{d\alpha} = \lambda - \frac{z+1}{\alpha} \,, \tag{4.10}$$

and so $f(\alpha)$ has an extremum at $\alpha = \alpha_*$, where

$$\alpha_* = \frac{z+1}{\lambda} \,. \tag{4.11}$$

Recall that we required $\alpha \geq 1$ to obtain our first bound on $P_2(z;q)$. Since $\lambda = z\frac{q}{p} < z$, this condition is obeyed by α_*, and so our solution is valid. In addition, one can check that α_* is a minimum (and not a maximum or other critical point) of $f(\alpha)$.

If we now plug α_* back into our bound on $P_2(z;q)$, then we find that

$$P_2(z;q) \leq \left(\frac{e\lambda}{z+1}\right)^{z+1} e^{-\lambda} \,. \tag{4.12}$$

Then, since $\lambda = z\frac{q}{p}$ and $z \leq z+1$, we have

$$P_2(z;q) \leq \left(e\frac{q}{p}\right)^{z+1} e^{-\lambda} \,. \tag{4.13}$$

Finally, by extracting a factor of $e\frac{q}{p}$, we obtain the bound

$$P_2(z;q) \leq \left(e\frac{q}{p}\right) e^{z - z\frac{q}{p} + z\ln\left(\frac{q}{p}\right)} \,. \tag{4.14}$$

Combining this bound with our bound on $P_1(z;q)$ then completes the proof of the theorem.

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf (2008).