Grundlagen

Das Bitcoin-Protokoll definiert vor allem zwei wesentliche Voraussetzungen zum Mining von Bitcoin:

- alle ca. 10 Minuten soll ein neuer Block gefunden werden.
- die Belohnung für einen gefundenen Block beträgt zunächst 50 BTC und wird alle 4 Jahre halbiert.

Durch diese Maßnahmen soll die Gesamtzahl der Bitcoins auf 21 Millionen Einheiten begrenzt bleiben.

Aufgabe 1

(a) Geben Sie eine Funktionsgleichung $b(t)$ an, die die Anzahl der durchschnittlich gefundenen Blöcke nach t Jahren beschreibt.

(b) Die Gleichung der Belohnungsfunktion $r(t)$ lautet $r(t) = \frac{50}{\lceil \frac{t}{4} \rceil}$. Skizzieren Sie den Graphen von $r(t)$.
Hinweis: die Funktion $\lceil x \rceil$ rundet $x \in \mathbb{R} \setminus \mathbb{Z}$ auf die nächstgrößere ganze Zahl auf.

Aufgabe 2

Da die Modellierung mit der Treppenfunktion $r(t)$ umständlich ist, wird überlegt, als Belohnungsfunktion eine stetige Funktion $\hat{r}(t) = \hat{r}_0 \cdot e^{-\lambda \cdot t}$ mit der Anfangsbelohnung $\hat{r}_0$ zu verwenden. Der Parameter λ kann dabei über den Zusammenhang $t_H = \frac{ln(2)}{\lambda}$ aus der Halbwertszeit t_H bestimmt werden.

(a) Bestimmen Sie die Gleichung von $\hat{r}(t)$.

Aufgabe 3

Um die Anzahl der bereits geschürften Bitcoin zu berechnen, wird u.a. das Integral über $r(t)$ benötigt. Wir indizieren dazu die Treppenstufen von $r(t)$ mit den natürlichen Zahlen und definieren A_k als den Inhalt unter der Stufe mit der Nummer k.

(a) Geben Sie die Größe der Fläche A_k an.

(b) Berechnen Sie $\int_0^\infty r(t)\ dt$, indem Sie die Summe der Flächen A_k bestimmen, d.h. den Zusammenhang $\int_0^\infty r(t)\ dt = \sum_{k=0}^\infty A_k$ ausnutzen. (Sie dürfen ohne Beweis verwenden, dass $\sum_{k=0}^\infty \frac{1}{2^k} = 2$ gilt.)

Aufgabe 4

Wir wollen zeigen, dass die Menge der Belohnungen durch die stetige Funktion $\hat{r}(t)$ unterschätzt wird. Dazu verwenden wir die Hilfsfunktion $h(t) = \frac{200}{x+4}$.

(a) Begründen Sie, dass $h(t) \leq r(t)$ für alle $t \geq 0$ gilt.

(b) Weisen Sie nach, dass sich die Funktionen $h(t)$ und $\hat{r}(t)$ im Punkt $S(4|25)$ schneiden.

(c) Zeigen Sie, dass die Fläche unter $\hat{r}(t)$ im Intervall $[0;4]$ kleiner ist als die Fläche der Stufe A_0.

(d) Folgern Sie aus den ersten drei Teilaufgaben, dass die Fläche unter der Funktion $\hat{r}(t)$ kleiner ist als die unter $r(t)$. Beurteilen Sie die Qualität der Eignung von $\hat{r}(t)$ als Modell für die Belohnungsfunktion des Bitcoin.

Aufgabe 5

Sei $B(t) = b(1) \cdot \int_0^t r(x)\ dx$ die Anzahl der Bitcoins, die bis zum Zeitpunkt t (in Jahren) geschürft wurden.

(a) Berechnen Sie mithilfe der Flächen A_k unter den Stufen den Wert $B(8)$.

(b) Zeigen Sie durch Nachrechnen, dass für die Gesamtmenge aller Bitcoins $B = b(1) \cdot \int_0^\infty r(x)\ dx$ näherungsweise $B \approx 21 \cdot 10^6$ gilt.

(c) Nach Angaben im Bitcoin-Protokoll soll der letzte Bitcoin ca. im Jahre 2140 geschürft werden. Überprüfen Sie, dass für $t = 2140 - 2008 = 132$ tatsächlich bereits etwa $B(t) = B$ gilt.