

Bitcoin

Bitcoin a Nepředstavitelné

 Představ si *knihu*, kde každá stránka představuje **jeden možný Bitcoin privátní klíč**.

Těch klíčů je:


$$2^{256} \approx 1,1579 \times 10^{77}$$

Pokud by každá stránka měla tloušťku 1 mm, celá kniha by byla vysoká:

$$\approx 1,1579 \times 10^{74} \text{ m} \approx 1,2 \times 10^{57} \text{ světelných let}$$

Pro srovnání:

- Země: 12 742 km
- Ke Slunci (1 AU): 150 mil. Km
- Nejbližší hvězda: 4,2 ly
- Nejbližší černá díra: 1560 ly
- Mléčná dráha: 100 000 ly
- Pozorovatelný vesmír: 93 miliard ly

 Tvá *Bitcoin kniha* by měla délku více než **milionkrát větší než celý pozorovatelný vesmír**.

A přesto to není největší číslo:

- Možných šachových partií: $\sim 10^{120}$
- Možných her Go: $\sim 10^{360}$
- Atomů ve vesmíru: $\sim 10^{80}$
- Stránek Bitcoin knihy: $\sim 10^{77}$

Bitcoin není jen měna.

Je to **kryptografická báseň vesmíru**.

Prolomit klíč?

Je jako **najít konkrétní atom** v moři miliard vesmírů — **hádat naslepo**.

Bitcoin není jen kryptoměna.

Je to **kryptografická báseň vesmíru**.