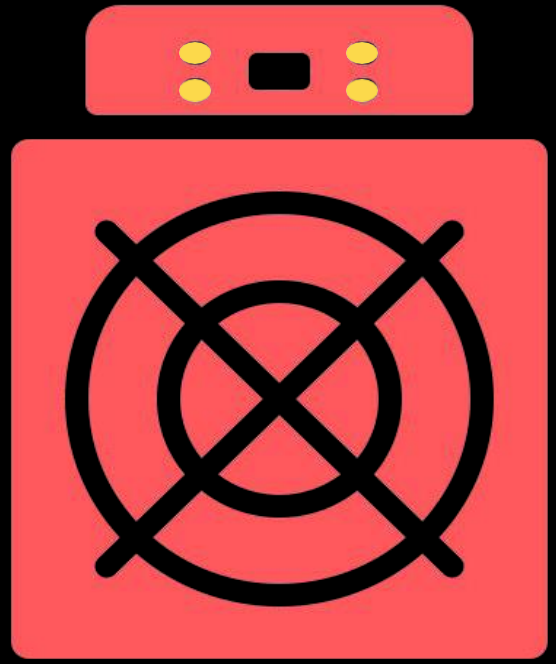
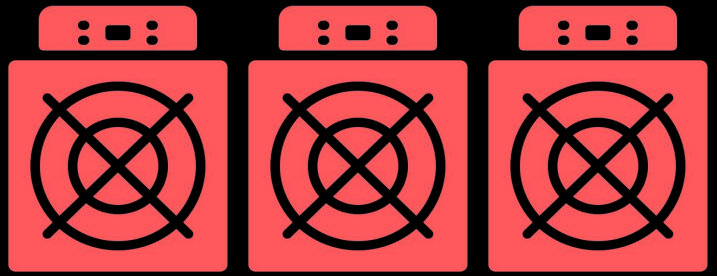
BẰNG CHỨNG KHAI THÁC

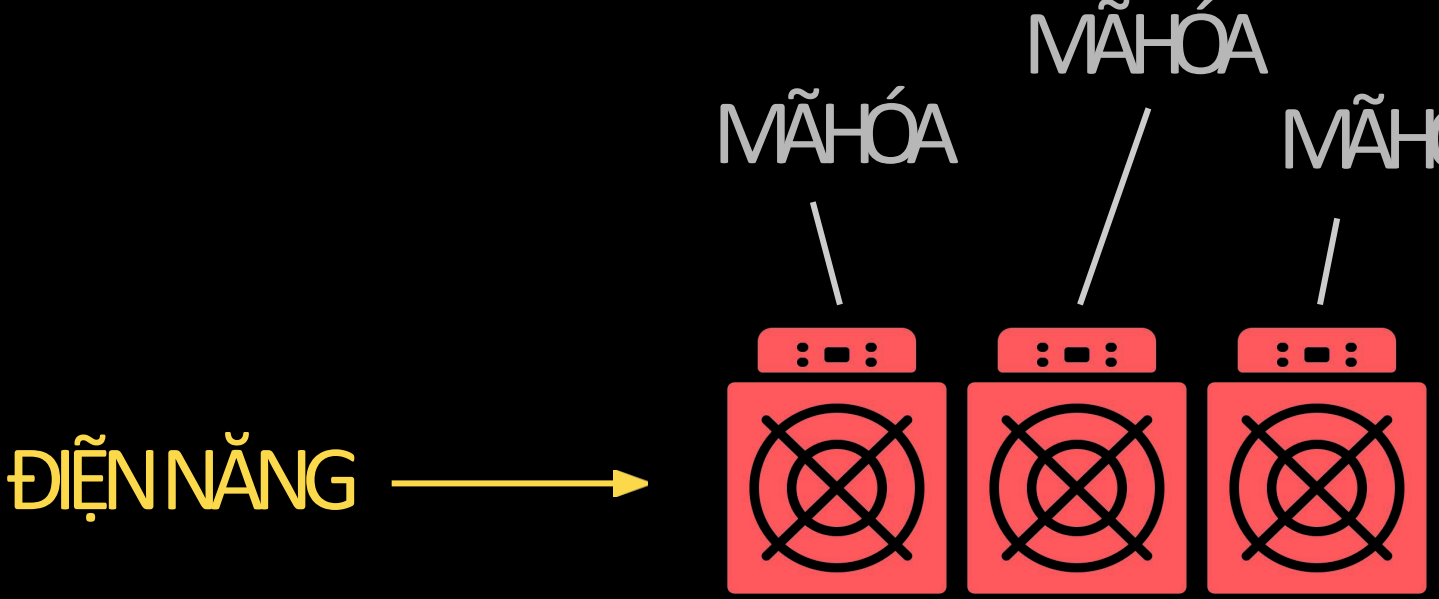
[Proof of work]



ĐIỆN NĂNG



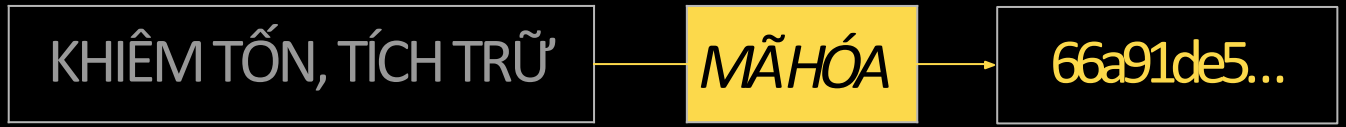
Máy sản xuất sử dụng điện từ mạng lưới điện hoặc từ nguồn năng lượng tại chỗ.

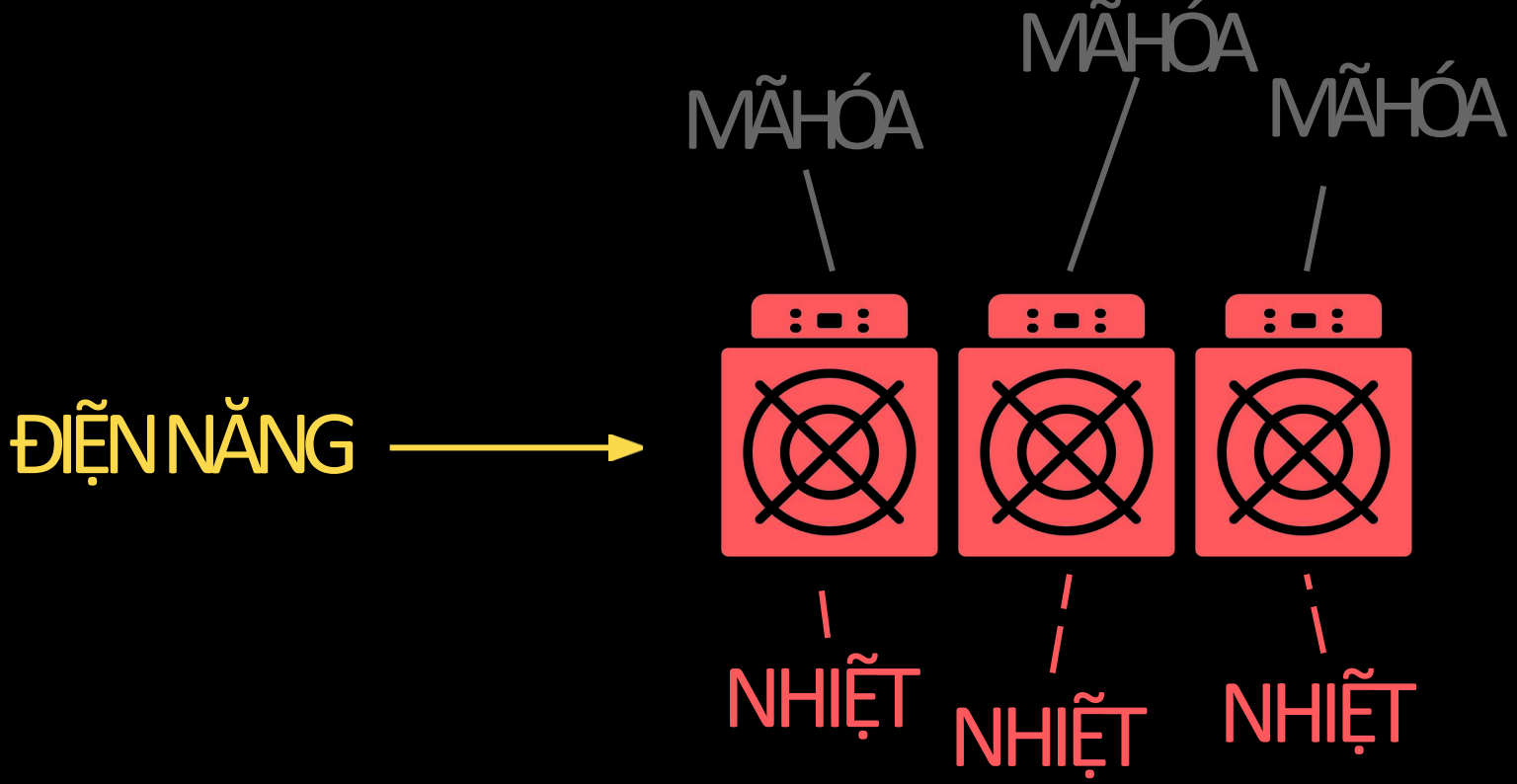


Những máy này được biết đến là thợ đào, tham gia vào quá trình “Mã hóa" với mục đích tạo ra một định dạng dữ liệu mã hóa ở đầu ra.

MÃ HÓA *(hash)*

Dùng thuật toán để chuyển đổi một phần dữ liệu thành một chuỗi có độ dài cố định và duy nhất.





Máy sản xuất tạo ra nhiệt trong quy trình mã hóa.

NHIỆT ĐỘNG HỌC *Định lý 1*

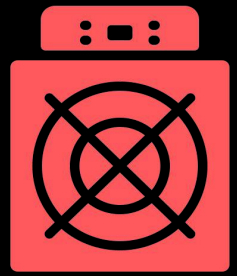
Năng lượng không thể được tạo ra hoặc phá hủy trong các hệ thống cô lập. Nó chỉ có thể được chuyển đổi từ dạng này sang dạng khác.

Các máy sản xuất sử dụng sức mạnh tính toán (biến đổi điện thành các chuỗi dữ liệu mã hóa) và tạo ra nhiệt.

MÃHÓA

26a03cad6cef052e
5772286e18d7986d
e1b3d2d9f959c56d
fce04ca7b469449e

ĐIỆN NĂNG



Các máy sản xuất tìm một hằng số ngẫu nhiên (được gọi là 'nonce') để tạo ra một loại dữ liệu mới thỏa mãn độ khó hiện tại (# số lượng chữ số 0 đầu tiên).

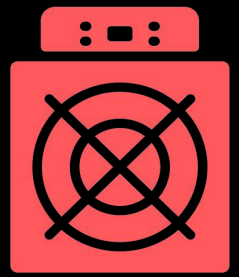
HẰNG SỐ NGẪU NHIÊN

(nonce)

Một hằng số ngẫu nhiên được kết hợp để tạo ra một loại dữ liệu mới đáp ứng các yêu cầu cụ thể (ví dụ, các số 0 đầu tiên) khi kết hợp với dữ liệu hiện có.

MÃ HÓA

/



ĐIỆN NĂNG

0000000000000000
00077d7e94ea7787
80e2d6138d4e38eb
091932e6c6ca4004

THẮNG !

@anilsaidso

Người thắng có quyền yêu cầu phí giao dịch và tự sản xuất ra Bitcoin mới. Việc này được thực hiện bằng cách đề xuất một khối dữ liệu mới cho mạng lưới bitcoin và thực hiện một giao dịch để trả tiền cho chính họ qua sàn giao dịch (ví dụ, coinbase).

Người sản xuất cạnh tranh cho cái gì?

0

21 Triệu

@anilsaidso

Phí giao dịch

từ lưu chuyển trong tổng cung

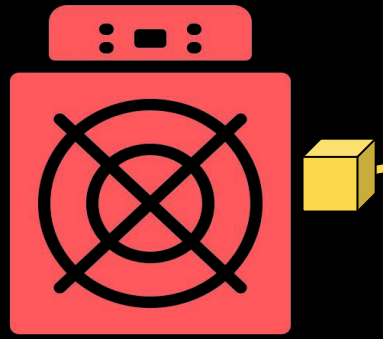
Bitcoin còn lại

Sẽ được sản xuất qua khối dữ liệu mới

PHẦN THƯỞNG
(block subsidy)

Một lượng Bitcoin được xác định trước mà mỗi máy sản xuất thành công được phép tạo ra với mỗi khối dữ liệu.

50BTC	25BTC	12.5BTC	6.25BTC	3.125BTC



Một khối dữ liệu mới nếu hợp lệ sẽ được đề xuất phát tán và lan truyền trên mạng, tạo thành đỉnh mới của chuỗi.

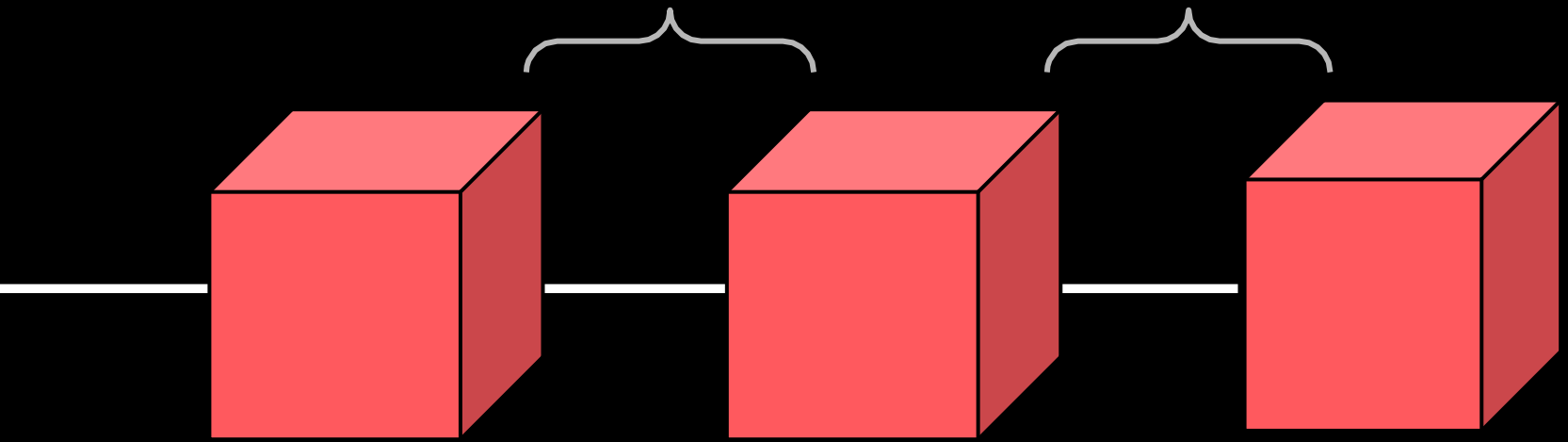
Đỉnh chuỗi

KHỐI
ĐỀ XUẤT

KHỐI
ĐÃ XÁC NHẬN

@anilsaidso

chu kỳ (trung bình.)
10 phút



@anilsaidso

Quy trình sản xuất mỗi khối dữ liệu được lập trình đều đặn một khoảng thời gian cố định. Nếu thời gian tạo khối dữ liệu lâu hơn chu kỳ trung bình là 10 phút, độ khó trong quy trình sản xuất sẽ tự điều chỉnh tăng hoặc giảm.

ĐỘ KHÓ *(difficulty)*

Một phương thức cho biết khả năng tạo ra một khối dữ liệu mới dựa trên một vài thông số nhất định.

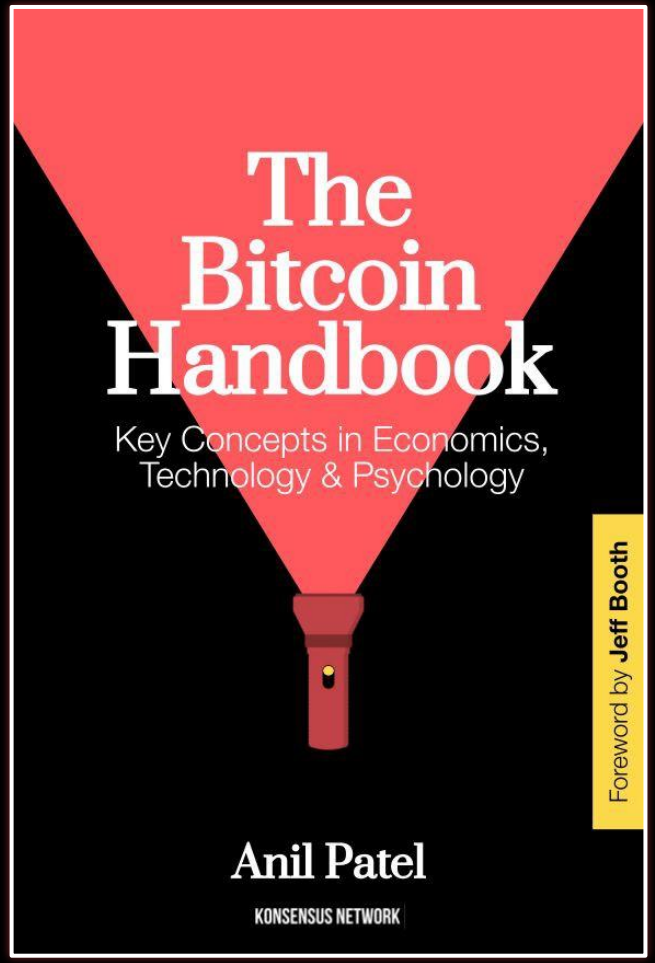
0000000000000000077d7e94ea778780e2d6138d4e38eb091932e6c6ca4004

“Tính bất biến và bền vững của Bitcoin dựa trên định luật nhiệt động học.

Chúng ta chỉ cần duy nhất một sổ cái bất biến được minh chứng qua làm việc.”

—Andreas Antonopoulos

Now available:



Anil

@anilsaidso

Biên dịch

@AnhContact