

Giới thiệu về

# Bitcoin



Đặng Quang Huy

<https://huydq.dev>

# Bitcoin (BTC) là gì?

- Là một loại tiền tệ kỹ thuật số phân cấp
- Phát hành bởi [Satoshi Nakamoto](#) năm 2009.
- Có thể trao đổi qua Internet mà **không cần thông qua một tổ chức tài chính trung gian nào.**

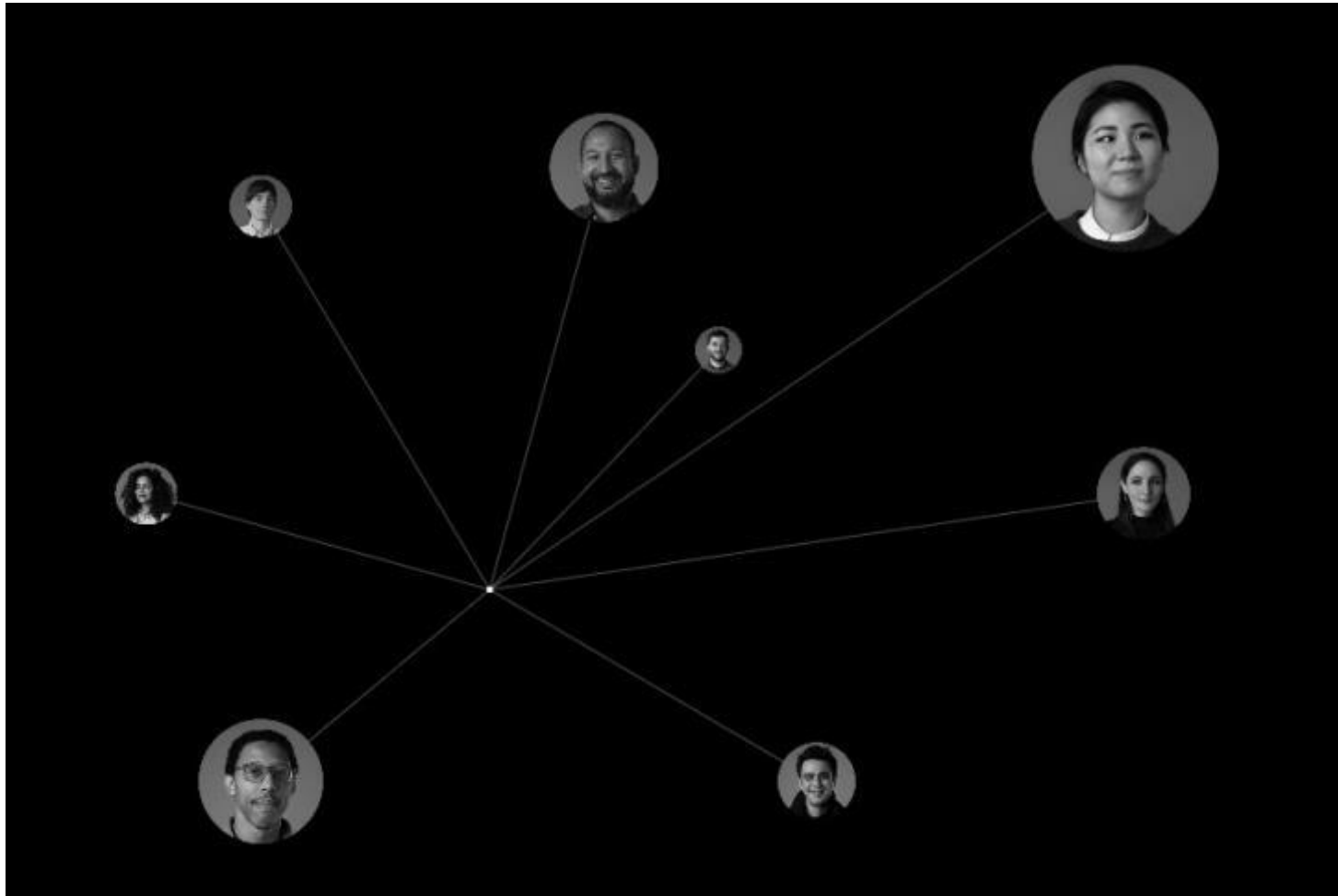
# Giao dịch trực tuyến

- Cần một bên trung gian thứ ba mà ta tin tưởng:

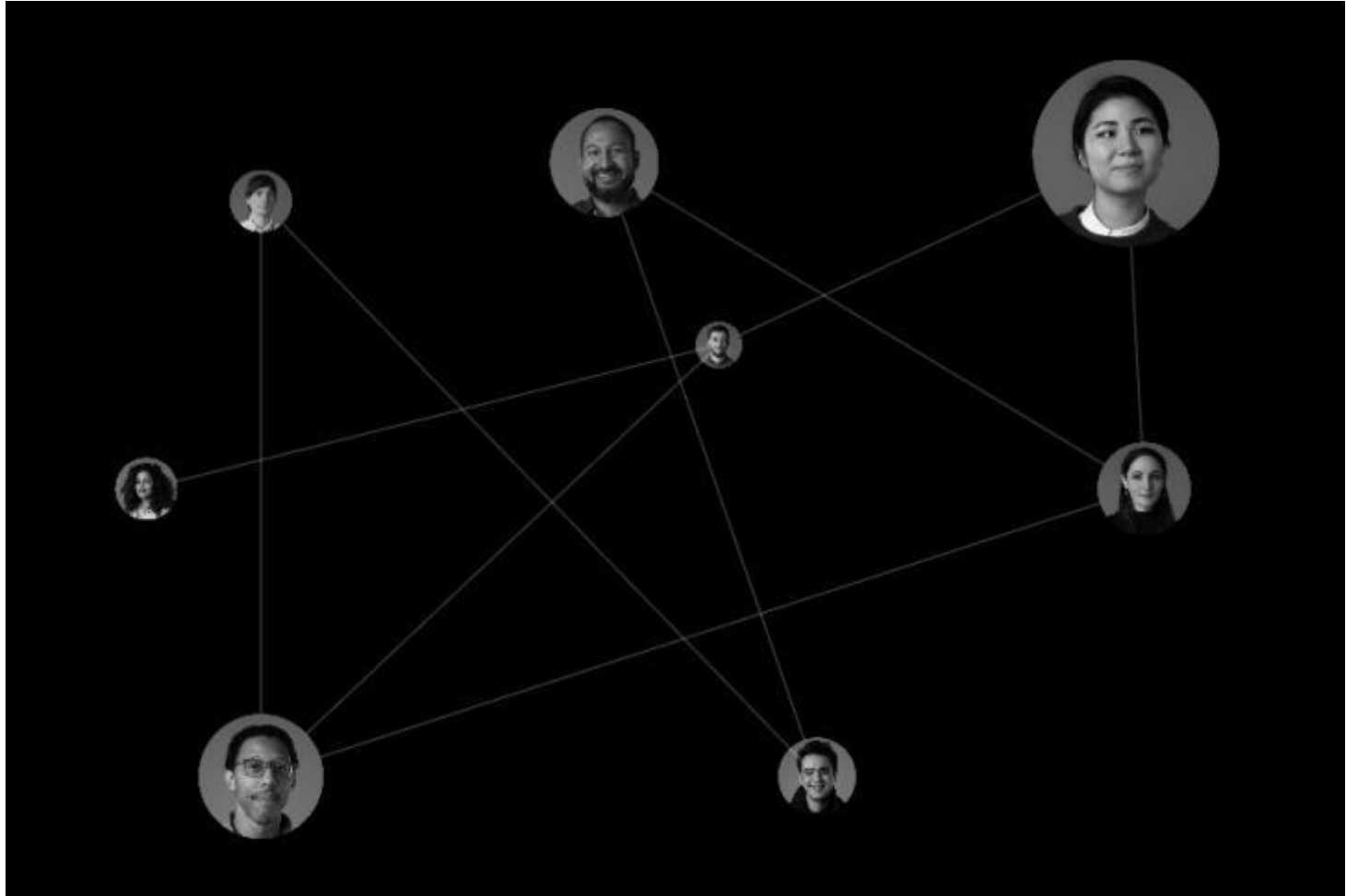


- Cơ sở dữ liệu (CSDL) tập trung để xác minh giao dịch.

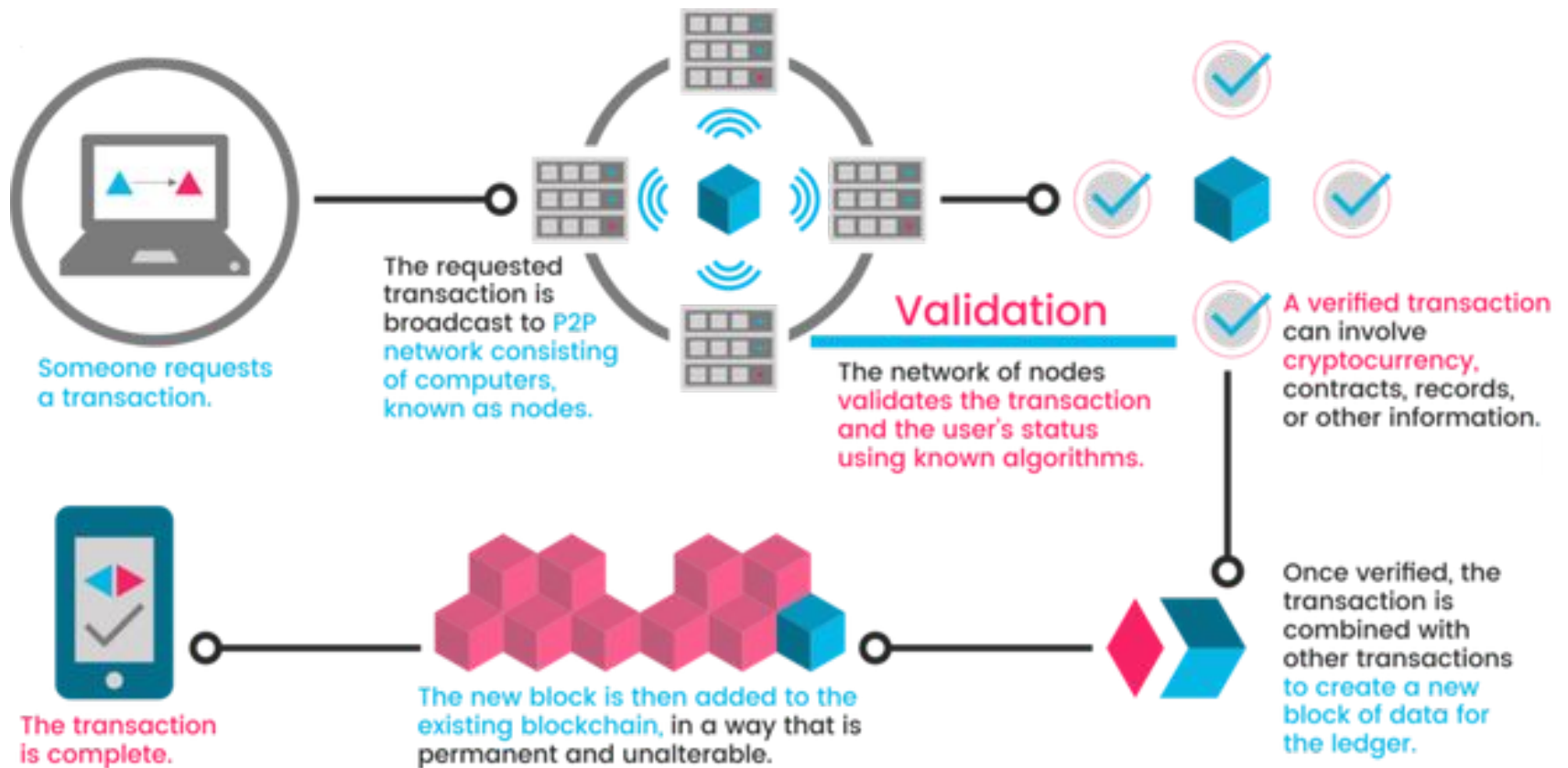
# Centralized



# Decentralized

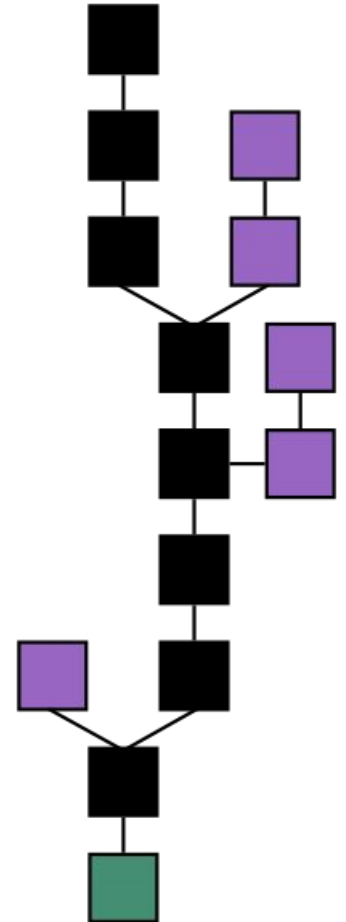


# Bitcoin transaction



# Blockchain (CSDL phân tán)

- Là một danh sách các khối thông tin (block) được liên kết bằng mã hóa và mở rộng theo thời gian.
- Mỗi block đều chứa thông tin về thời gian khởi tạo và thông tin về block tạo ra trước đó.
- Blockchain được thiết kế để chống lại việc thay đổi dữ liệu.



# Đào Bitcoin

- Bitcoin được cung ứng một cách **tự động, hạn chế và phân chia theo lịch trình có sẵn** dựa trên các thuật toán.
- Để có Bitcoin, các máy tính "đào" Bitcoin (miner) cần tìm được một số gọi là **nonce** thỏa mãn điều kiện của thuật toán để tạo ra một block mới.





# Mỏ đào Bitcoin

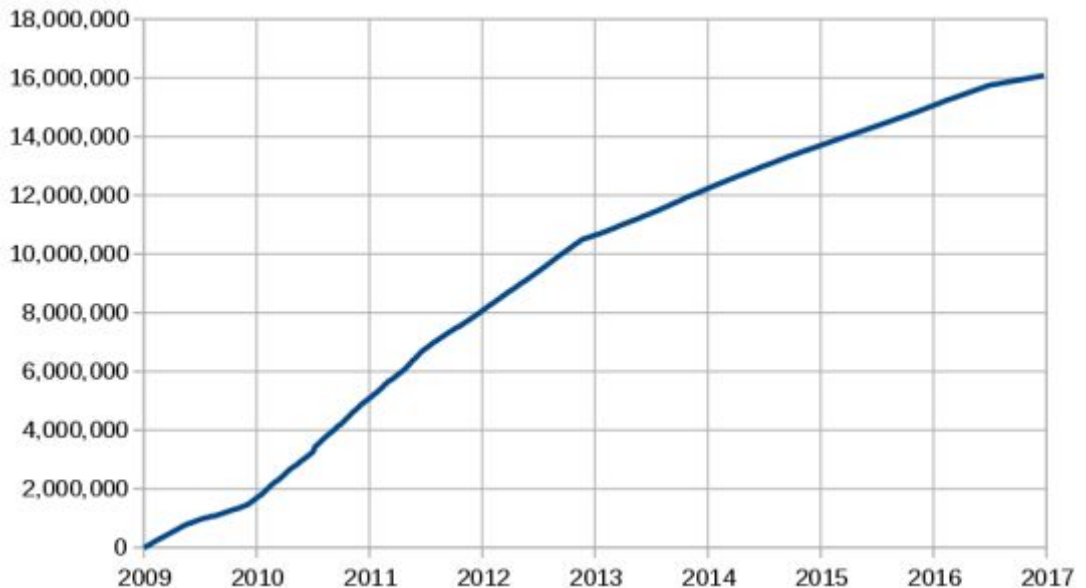


<https://www.youtube.com/watch?v=ueUTStzpbHo&feature=youtu.be>

# Số lượng Bitcoin

- Tổng cộng có **21 triệu Bitcoin**.
- Trung bình mỗi 4 năm, số Bitcoin "đào" được sẽ giảm đi  $\frac{1}{2}$

và đến năm **2140**  
thì sẽ đạt đến  
giới hạn.



# Tỉ giá Bitcoin

- Năm 2009, lần đầu lên sàn giao dịch:  
**1 Bitcoin = 0.00076 USD**
- Năm 2010, lần đầu tiên Bitcoin được dùng để mua hàng hóa:  
**10.000 Bitcoin = 1 ổ Pizza (25 USD)**
- Tháng 8 năm 2017, giá Bitcoin đang ở mức:  
**1 Bitcoin ~ 4.500 USD**

# Ưu điểm của Bitcoin

- Không có ngân hàng trung ương, số lượng có hạn nên không bị lạm phát (lạm dụng in tiền).
- Không cần giao dịch qua kênh trung gian, giảm bớt chi phí giao dịch và có thể thực hiện tại bất kỳ thời điểm nào.
- Giao dịch an toàn, không bị làm giả và không tốn chi phí kiểm định.

# Nhược điểm của Bitcoin

- Hơi khó sử dụng và chưa phổ biến.
- Có tính rủi ro nhất định vì không có người đứng đầu hay tổ chức đại diện nào. Có thể bị lừa đảo hoặc bị ăn cắp (mã khóa địa chỉ bitcoin).
- Nạn tin tặc và rửa tiền. Có thể bị dùng vào mục đích xấu do tính ẩn danh khi giao dịch và không có bên trung gian quản lý.

# Link tham khảo

## ■ Blockchain:

- <https://en.wikipedia.org/wiki/Blockchain>
- <http://www.goldmansachs.com/our-thinking/pages/blockchain/index.html>

## ■ Bitcoin:

- <https://en.wikipedia.org/wiki/Bitcoin>