<https://www.youtube.com/watch?v=6woL9jh_6jM&ab_channel=FPTEduTV>

**Góc nhìn về Blockchain qua bài trình bày “Blockchain is eating you” của Giáo sư David Trần, Đại học Massachusetts, USA**

1. Lời mở đầu:
2. Khái quát các nội dung chính của bài trình bày:

* Giới thiệu về quỹ Andreessen Horowitz (a16z) và người sáng lập Marc Andreessen: 2011 Software is eating the world in all sectors
* Cty chuyển dần kinh doanh từ Hardware sang Software: HP, Google từ 2011
* Blockchain is eating finances: blockchain lấy người dùng khỏi các dịch vụ tài chính truyền thống
* A16z quỹ dành riêng cho blockchain, crypto và web3
* Bài toán tung đồng xu: 1 người tung, 1 người đoán gián tiếp, ví dụ qua online, làm sao để xác định đoán đúng sai trong môi trường ko trung thực => bài toán cực lớn trong xã hội: ví dụ các giao dịch thì cần 1 người trung gian đáng tin cậy ví dụ ngân hàng…
* Blockchain là 1 hệ thống rất nhiều máy tính, vai trò trung gian thực hiện các giao dịch
* Sự to lớn của blockchain: niềm tin là rào cản lớn nhất cho sự phát triển của xã hội, và blockchain giúp giải bài toán niềm tin này
* AI như bộ não, blockchain như cơ thể
* Blockchain là sự phát triển tự nhiên:
  + Ngày xưa sử dụng máy tính cục bộ: desktop computing
  + Bây giờ: cloud computing: máy tính đc sở hữu bởi các tổ chức, và thuê để sử dụng
  + Tương lai: next generation of computing: blockchain computing: máy tính được chia sẻ phân tán bởi người dùng, ko do tổ chức nào nắm giữ
  + Blockchain computer: chạy các ứng dụng blockchain
* Ngày càng nhiều job, doanh nghiệp yêu cầu kiến thức về blockchain
* Ngày càng nhiều các sản phẩm chạy trên blockchain
* Là cơ hội để chúng ta tạo ra giá trị
* Nhiều cơ sở toán học đứng sau blockchain:
  + Hàm băm: input độ dài tùy ý, output độ dài cố định
  + Khó để giải đc hàm băm
  + 2 người trao đổi: đổi tiền, bài toán Runaway: đại diện giao dịch ko cần đơn vị trung gian
    - Alice và Bob mỗi người tạo ra 1 cái két, và chung mật khẩu, khi Alice mở két của Bob thì bob nhìn đc mật khẩu và sẽ mở két của Alice: ATOMIC SWAP
  + Để đảm bảo Privacy: Bài toán của những người triệu phú: chứng minh A > B mà ko biết giá trị của A, B
    - Khi chuyển tiền, có thể xác định đc giao dịch hợp lệ mà ko cần biết tài khoản gửi/nhận có bao nhiêu tiền
    - Dùng hàm hash, tính hash-A và hash-B
  + Mật mã học: cánh cửa bí mật: ông A biết mật khẩu, còn ông B muốn ông A chứng mình, ông A ko muốn đưa mất khẩu cho ông B, thì chỉ cần mở cửa nào mà ông A yêu cầu: zero knowledge proof
    - Tìm đc F(x) = C mà ko cần nói ra x
    - Zkp là khái niệm essential trong blockchain: có thể giúp tăng tốc độ blockchain cả trăm, nghìn lần…
  + Fear chung: 1 trong số các em có bùn trên trán, ai nghĩ có bùn thì tự bước lên đây…
    - Thuật toán consensus protocol
    - Chọn ra 1 hội đồng: 1 bài toán khó, áp dụng trong blockchain

1. Các khái niệm chính về Blockchain:
2. Vai trò và tiềm năng của Blockchain tới cuộc sống con người:
3. Kết luận:

**Các tài liệu tham khảo:**

<https://en.wikipedia.org/wiki/Blockchain>

**Một số hình ảnh của ngày hướng nghiệp:**





