Công nghệ Blockchain

Bài 1. Nguyên tắc, sự phát triển và ứng dụng

Gv: TS. Nguyễn Thành Huy

Khoa Công nghệ thông tin kinh doanh

Nội dung môn học

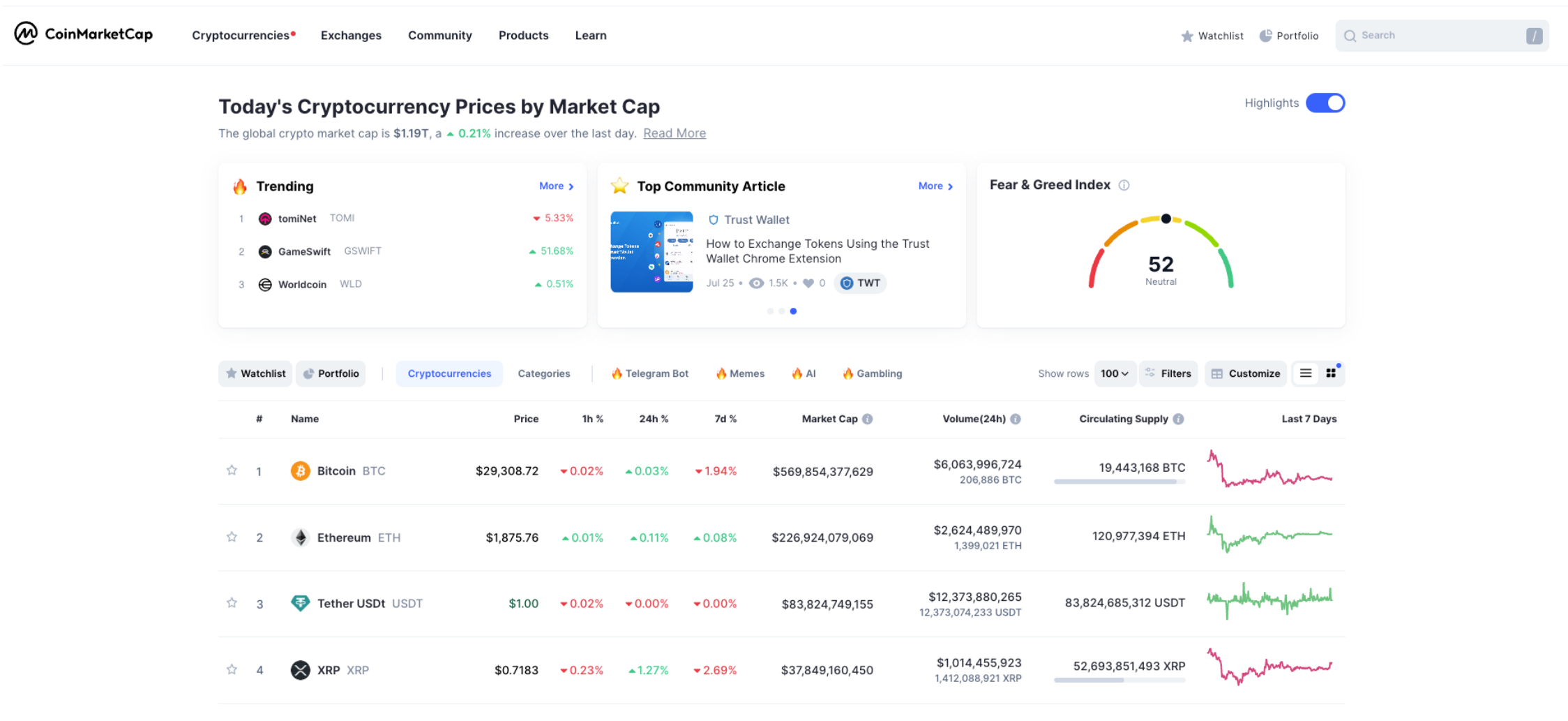
- Chương 1: Khái niệm cơ bản Blockchain
- Chương 2: Tổng quan về Blockchain: Lịch sử & Phát triển
- Chương 3: Kiến trúc nền tảng Blockchain
- Chương 4: Pháp lý của Blockchain
- Chương 5: Thảo luận về các mô hình Blockchain cho bài toán kinh tế
- Chương 6: Các ứng dụng thực tiễn của Blockchain
- Chương 7: Metaverse
- Chương 8: Metaverse và tương lai của ngành thông tin truyền thông
- Chương 9: Báo cáo chuyên đề

Nội dung

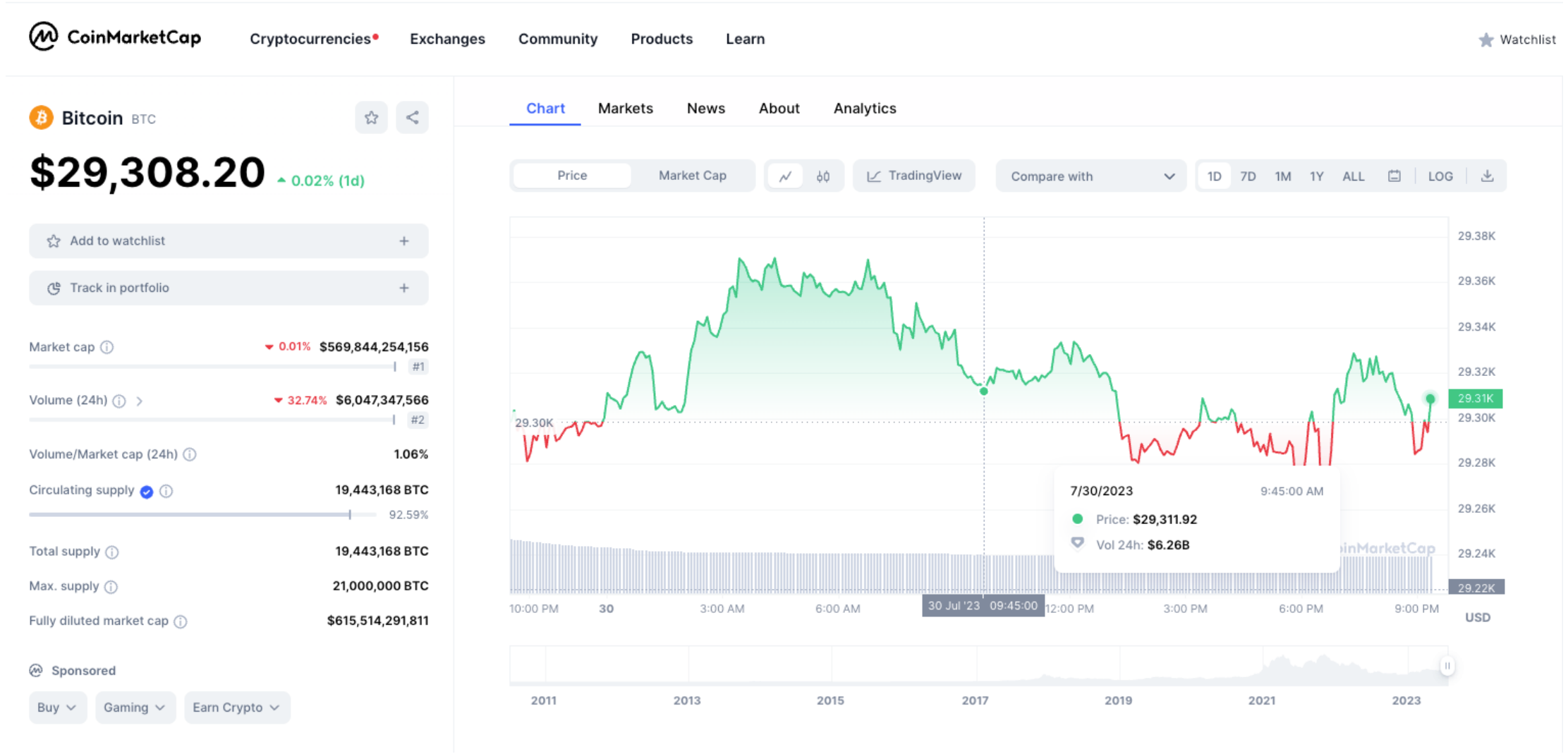
- Blockchain là gì?
- Ứng dụng của Blockchain
- Hoạt động của Blockchain
- Các khía cạnh về kỹ thuật của Blockchain

Intersting Look

- https://coinmarketcap.com



Bitcoin


CoinMarketCap
Cryptocurrencies
Exchanges
Community
Products
Learn
Watchlist
Bitcoin BTC
$29,308.20
0.02% (1d)
Add to watchlist
Track in portfolio
Market cap
0.01%
$569,844,254,156
#1
Volume (24h)
32.74%
$6,047,347,566
#2
Volume/Market cap (24h)
1.06%
Circulating supply
19,443,168 BTC
92.59%
Total supply
19,443,168 BTC
Max. supply
21,000,000 BTC
Fully diluted market cap
$615,514,291,811
Sponsored
Buy
Gaming
Earn Crypto
Chart
Markets
News
About
Analytics
Price
Market Cap
TradingView
Compare with
1D
7D
1M
1Y
ALL
LOG
29.38K
29.36K
29.34K
29.32K
29.31K
29.30K
29.28K
29.26K
29.24K
29.22K
29.30K
7/30/2023
9:45:00 AM
Price: $29,311.92
Vol 24h: $6.26B
10:00 PM
30
3:00 AM
6:00 AM
30 Jul '23
09:45:00
12:00 PM
3:00 PM
6:00 PM
9:00 PM
USD
2011
2013
2015
2017
2019
2021
2023

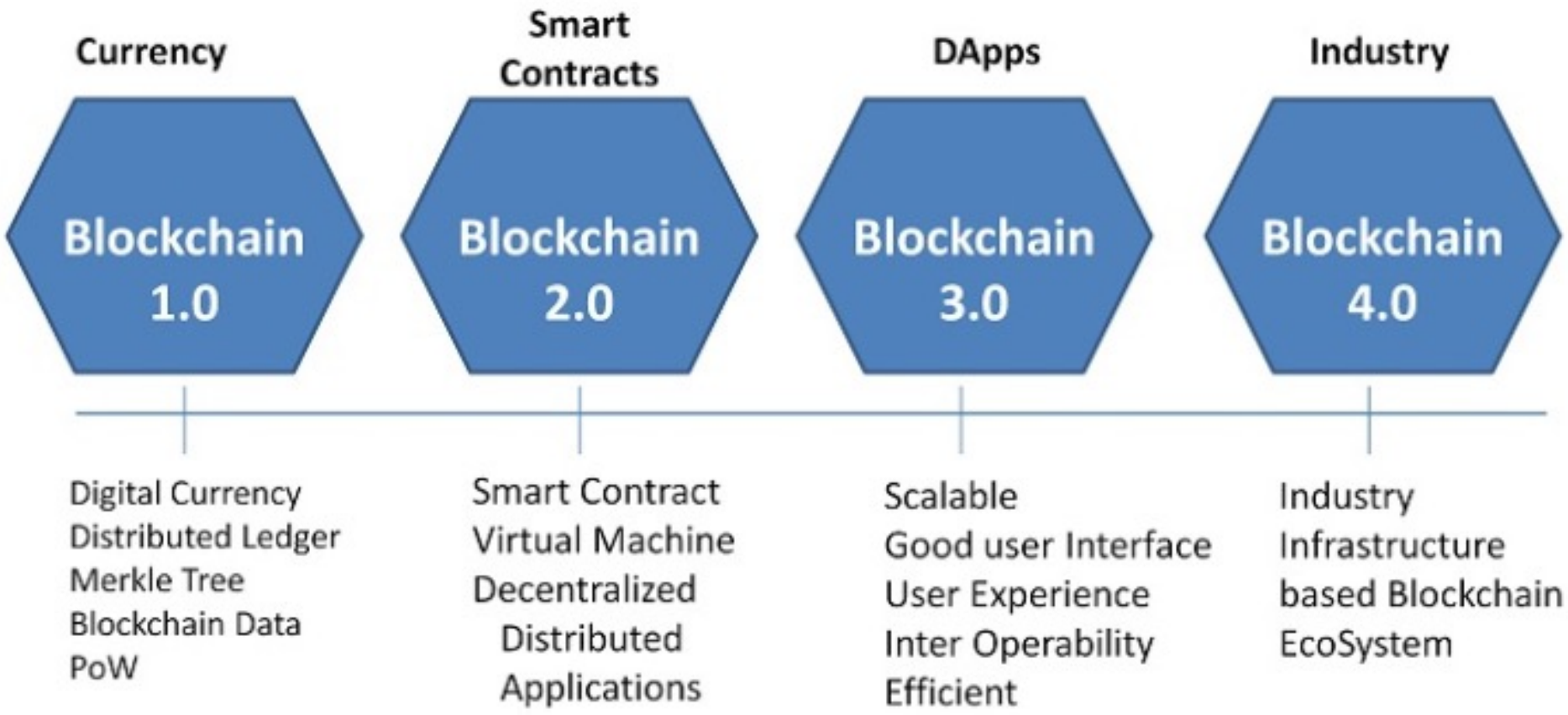
Blockchain là gì?

- Có nhiều định nghĩa:
  - Là một công nghệ dùng cho bitcoin
  - Wiki: Là một cơ sở dữ liệu phân tán duy trì một danh sách các bản ghi lớn dần liên tục gọi là khối (Block) và được bảo vệ khỏi giả mạo và chỉnh sửa.
  - Blockchain là một giao thức an toàn cho phép trao đổi ngang hàng (p2p) trong một mạng phân tán một cách an toàn, công khai, được công nhận.

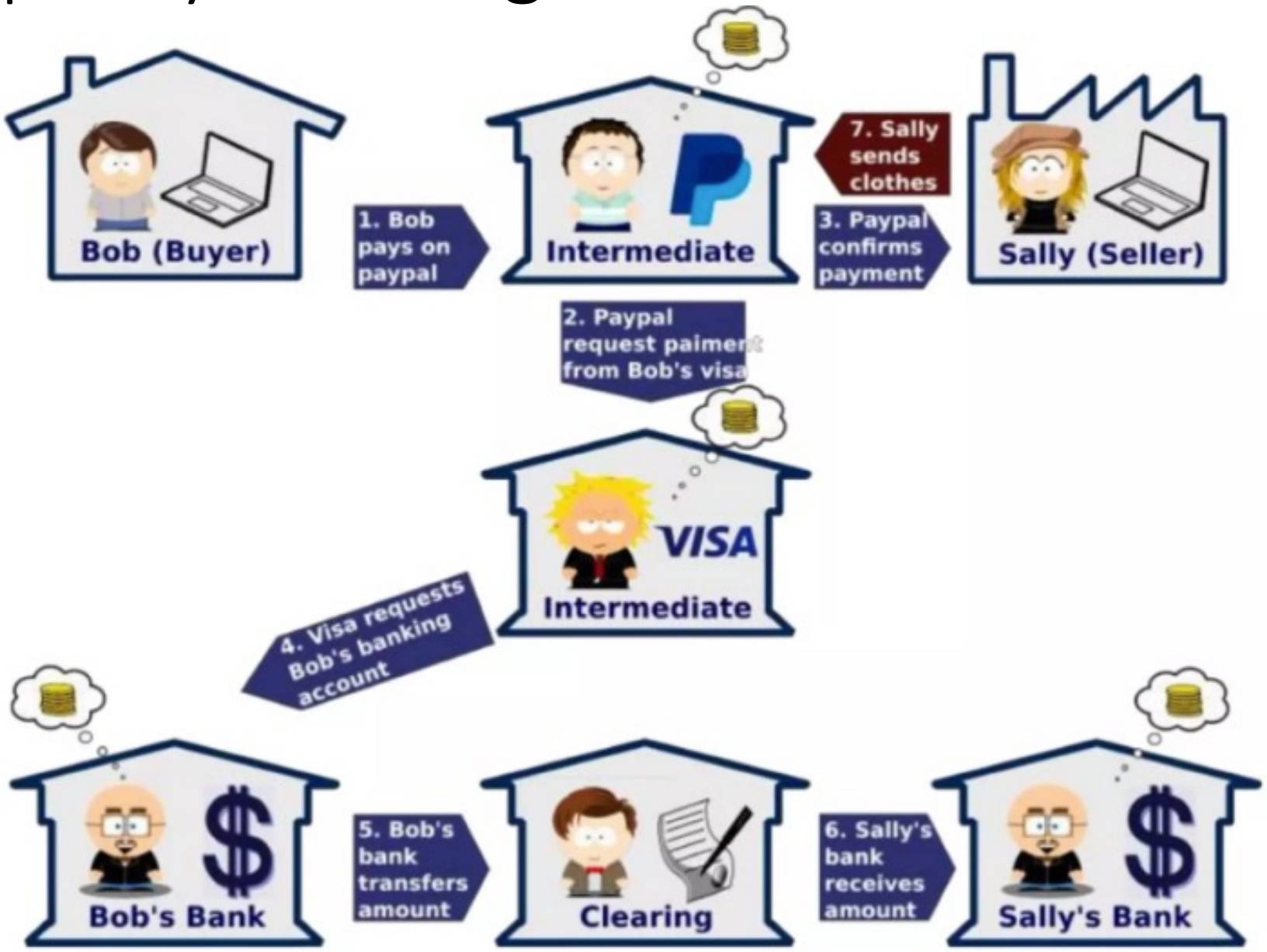
Lịch sử Blockchain

- Hình thành năm 2008
- Thực hiện triển khai trong năm 2009
- Năm 2014: Ra đời blockchain 2.0
  - Là cuộc cách mạng so với phiên bản đầu tiên
  - Từ các giao dịch đơn giản tới các chương trình phần mềm
  - Từ dạng 1 sổ cái giao dịch phân tán tới phân tán toàn cục, không thể sở hữu, điện toán số.

Sự phát triển của Blockchain



Giải pháp truyền thống



Giải pháp truyền thống

- Hệ thống đóng và thiếu minh bạch
- Các bên trung gian không phải tình nguyên viên và làm việc vì tiền
- Các giao dịch có nhiều lỗ hỏng
  - Mất cắp thông tin thẻ tín dụng
  - Lỗi nhân viên ngân hàng
- Chủ tài khoản về bản chất không phải người sở hữu thực sự tài khoản
  - Ngân hàng là người sở hữu thực sự tài khoản
  - Các tài khoản dễ dàng bị đóng băng, thay đổi
  - Ngân hàng hoặc các tổ chức xử lý giao dịch có thể từ chối xử lý vì một số thực thể pháp luật khác.
- Giao dịch thực hiện chậm: sec có thể mất vài ngày.

Bộ phận thanh toán bù trừ/ Clearing House

- Đứng giữa 2 thực thể ngân hàng, nhằm giảm rủi ro, đảm bảo giao dịch.
- “Thanh toán bù trừ” là một nghiệp vụ, mà ở đó, một nhóm các ngân hàng (Hay các giao dịch) giữa sec, hối phiếu hay các chứng từ của nhau khi đưa chúng vào thanh toán sẽ tham gia vào quá trình bù trừ của nhau.
- Việc này mỗi ngân hàng sẽ là con nợ/chủ nợ và sẽ thanh toán qua tổ chức bù trừ bằng cách chuyển số dư tới ngân hàng trung ương.

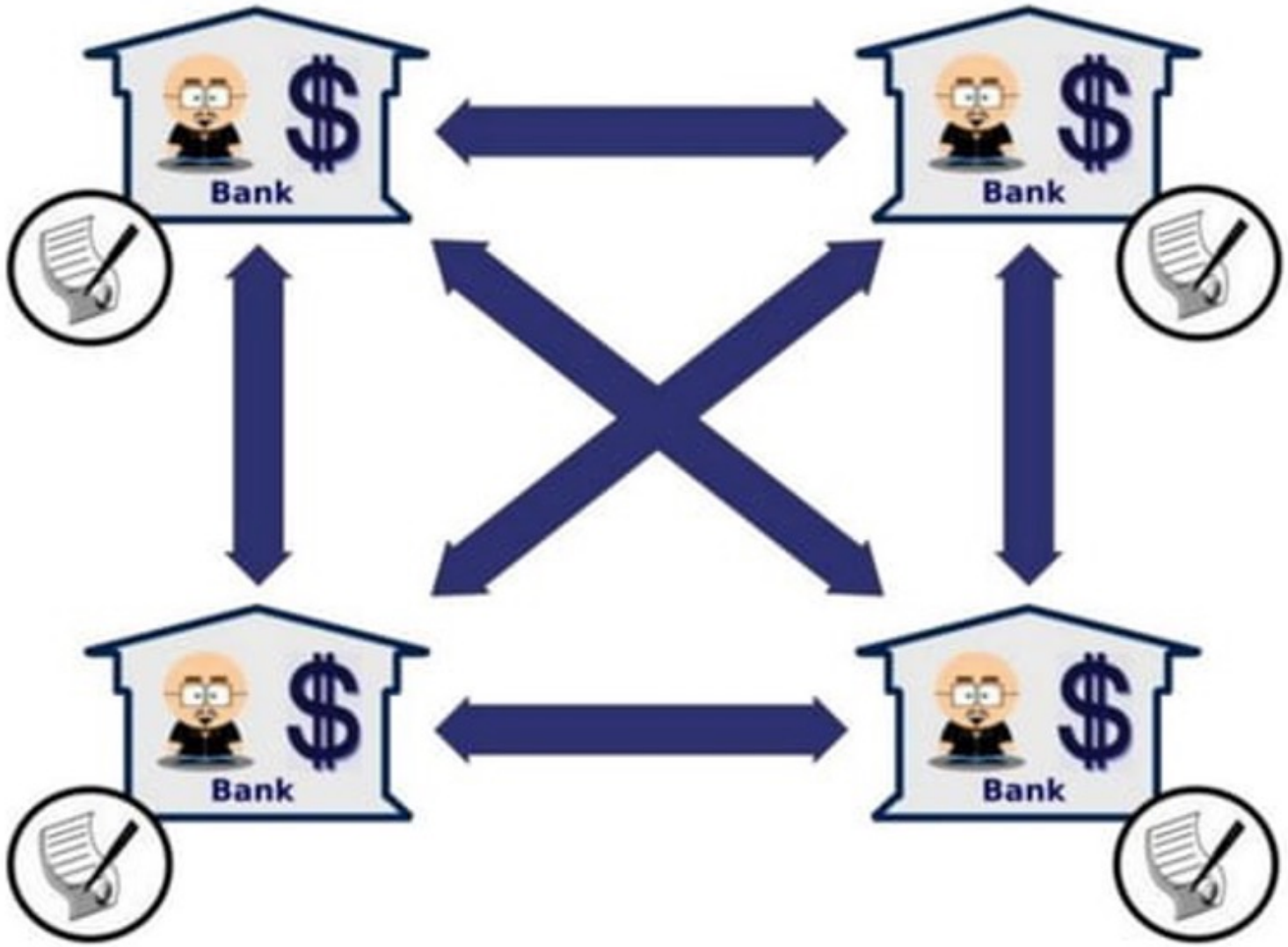
Clearing housing problems

- Các ngân hàng sử dụng sổ cái tập trung để giám sát giao dịch
  - Hệ thống thiếu hiệu quả
  - Tốn thời gian, tăng chi phí
- Là mục tiêu tấn công, gian lận
- Tốn chi phí đảm bảo an toàn, bảo mật

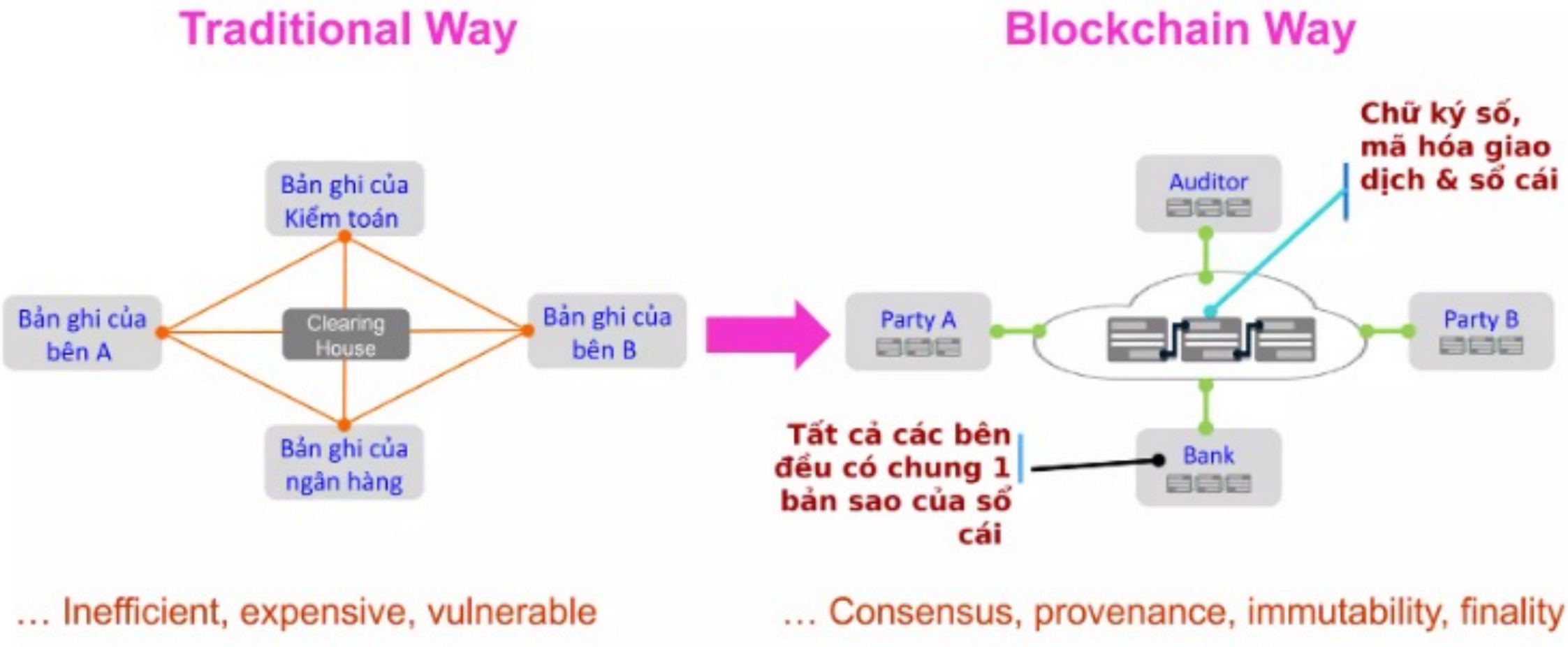
Sổ cái phân tán (distributed ledgers)

- Sổ cái phân tán (Sổ cái chia sẻ) là dữ liệu được **chia sẻ, đồng thuận, nhân bản và đồng bộ** giữa nhiều thực thể.
- Mọi node trong mạng phân tán đều có bản sao của sổ cái này.
- Không có cái gọi là “bản chính thức” hay thực thể nào đáng tin cậy hơn thực thể nào.
- Một sổ cái phân tán của Blockchain bao gồm những dữ liệu số được ghi nhận không thể thay đổi và được đóng gói thành những khối (Block)

Sổ cái phân tán tập trung

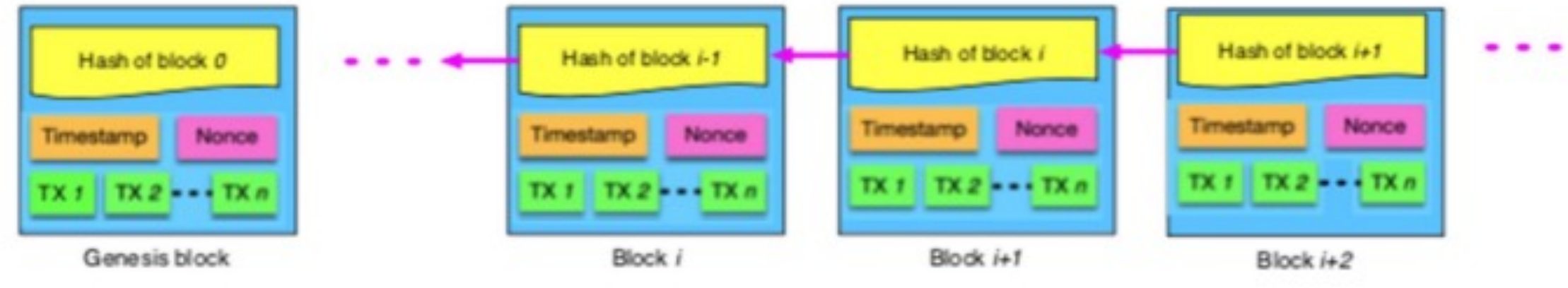


So sánh blockchain vs. Mô hình truyền thống

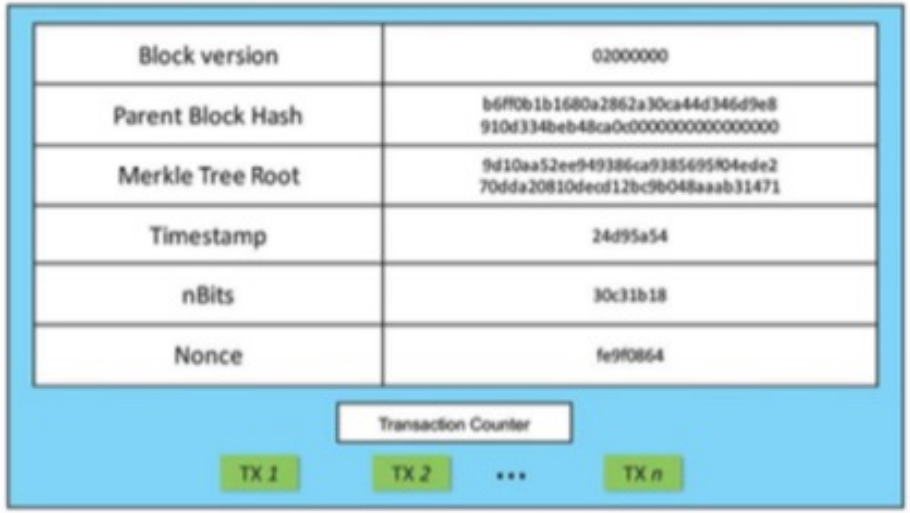


Kiến trúc của Blockchain

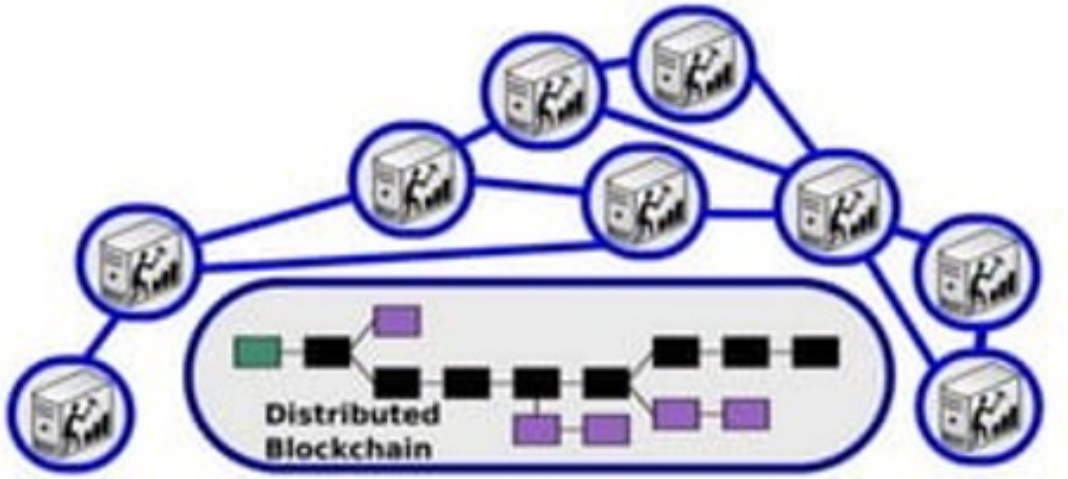
- Blockchain bao gồm một danh sách các blocks:
  - Mỗi block chứa dữ liệu của nó (Ví dụ giao dịch) và giá trị băm (Hash) mã hoá của nó
- Mỗi block chứa giá trị băm (Hash) của khối trước đó trong block. Điều này đảm bảo toàn bộ dữ liệu trong blockchain không bị giả mạo và không bị thay đổi.
- Việc tạo ra block hiện tại từ block nguyên thuỷ
  - Mỗi block được đảm bảo tạo ra sau block trước đó theo trình tự thời gian.



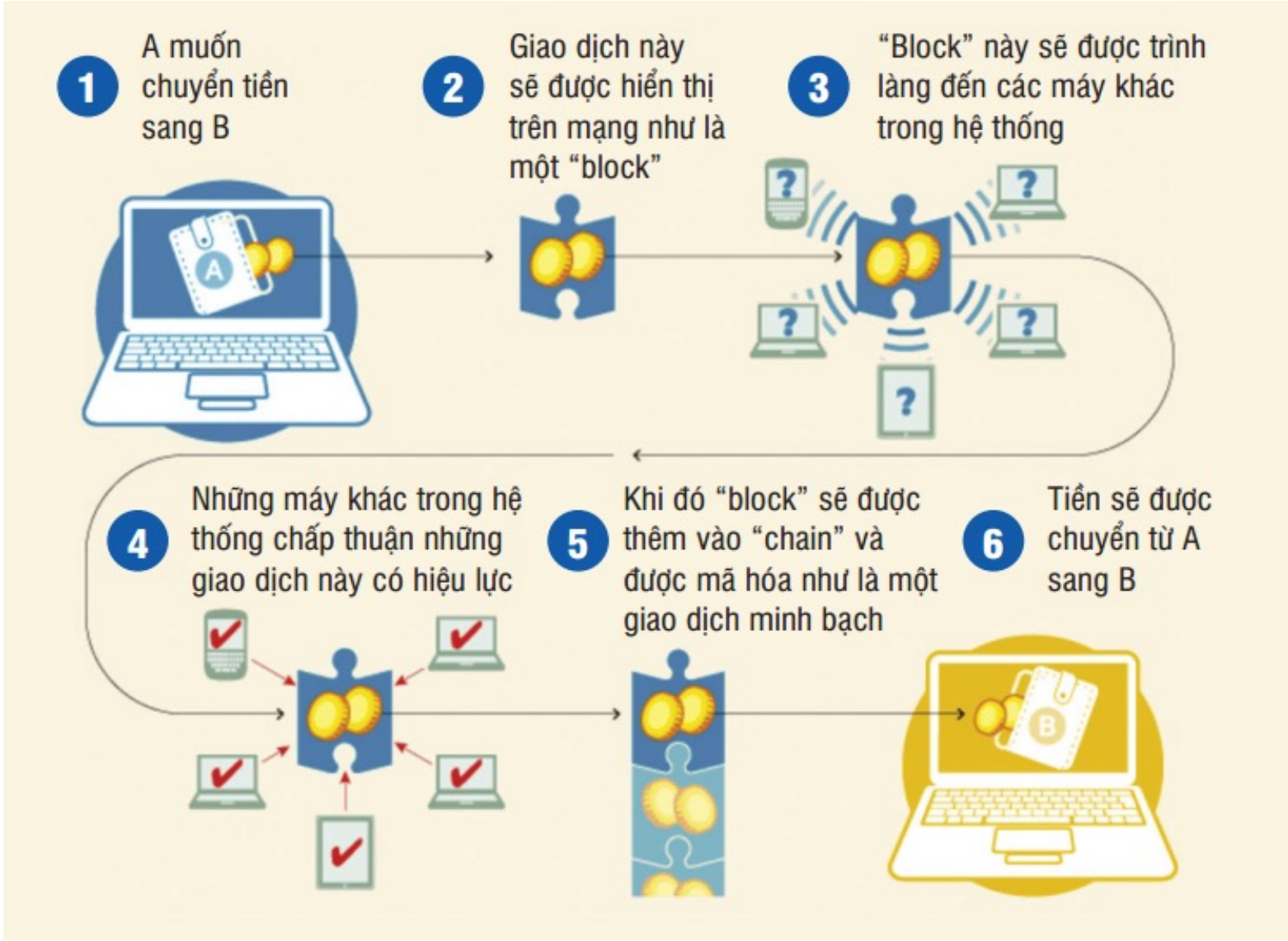
Cấu trúc một khối (block)



- Mạng Blockchain là một mạng ngang hàng gồm nhiều node độc lập. Trao đổi thông tin bằng truyền thông quảng bá.
- Một node không nhất thiết giao tiếp với mọi node khác nhưng cần giao tiếp với một vài node.



Cách hoạt động của một Blockchain



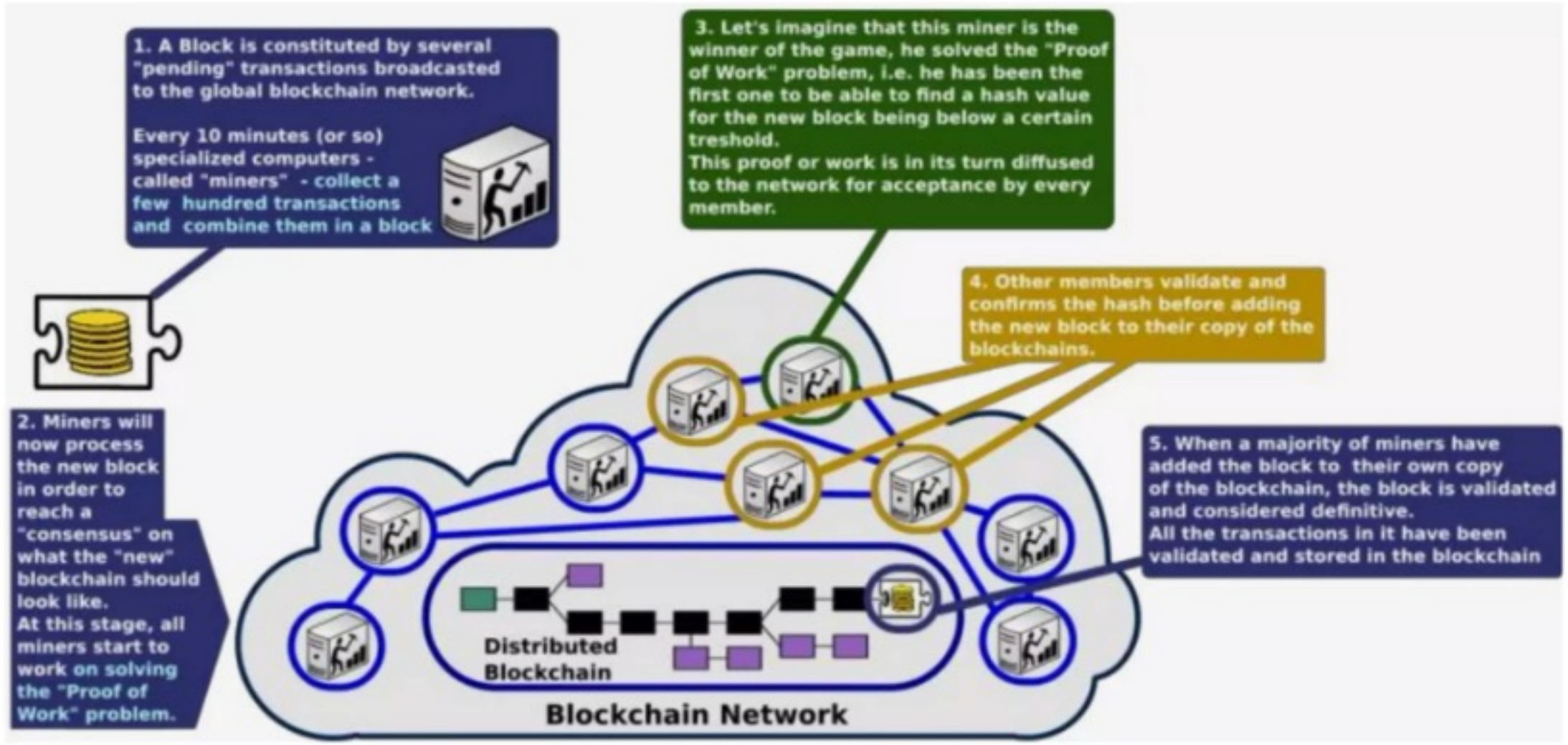
Proof of work

- Để một block được chấp nhận bởi các thành viên trong mạng, những miner phải hoàn thành “Chứng minh công sức” – proof of work chứa tất cả các dữ liệu trong 1 block:
  - “minh chứng công sức” là một phần dữ liệu trong block mà rất khó để tạo ra (tốn kém thời gian và năng lượng/cpu) nhưng lại dễ dàng có thể kiểm tra tính đúng đắn và phải đạt được một số yêu cầu cụ thể.
  - Việc tạo ra một “minh chứng công sức” này giống như một quá trình ngẫu nhiên với xác suất xảy ra thấp, đòi hỏi thử và sai nhiều lần trước khi tạo ra được nó.
  - Bitcoin sử dụng hệ thống hashcash proof of work.
- Một block được coi là hợp lệ phải có giá trị băm nhỏ hơn một giá trị đích hiện có (current target). Đặc điểm này nhằm chứng tỏ proof of work đã được thực hiện.

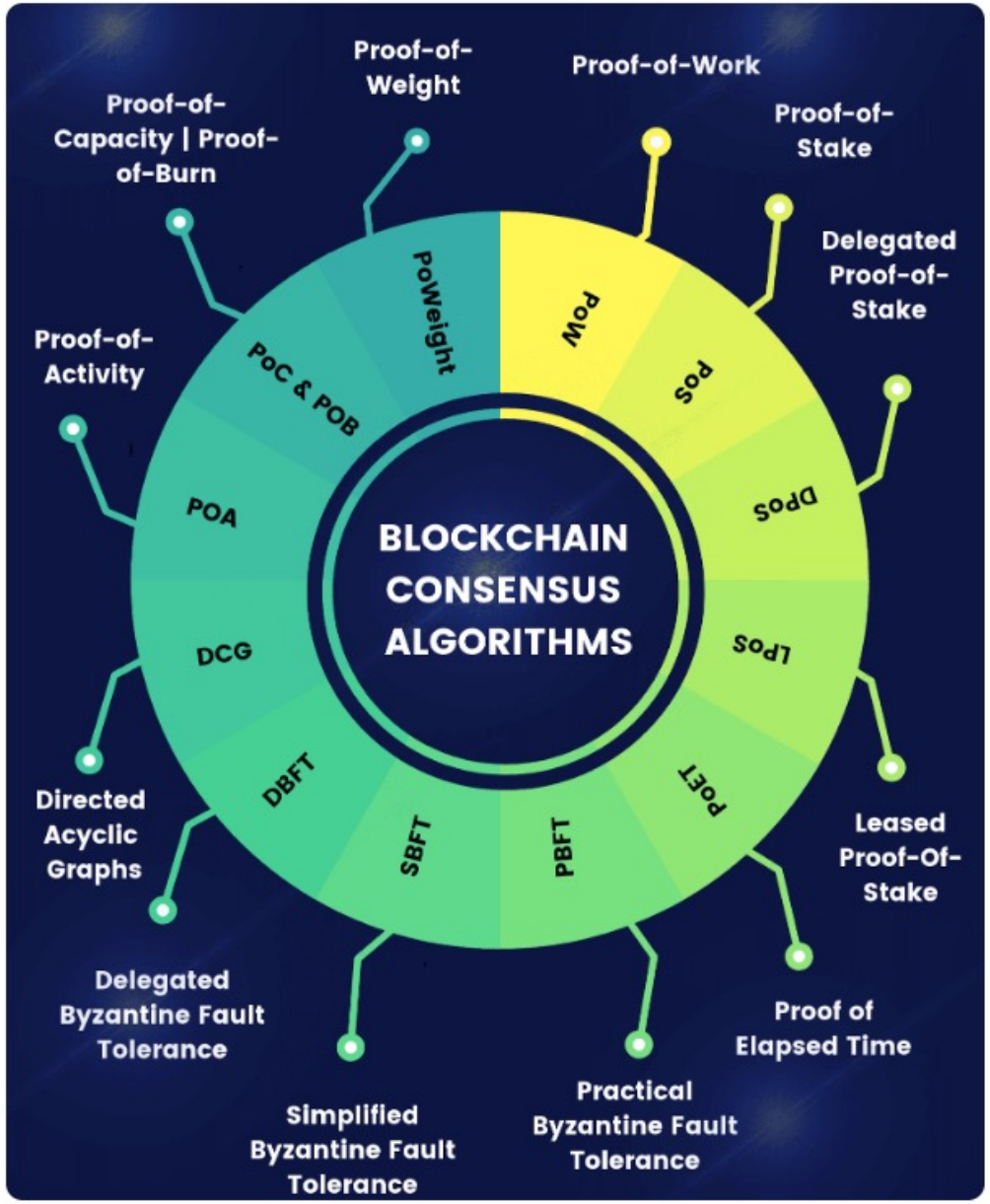
Proof of work

- Mỗi block cũng chứa giá trị băm của block trước đó. Do đó, mỗi block chứa thông tin của một chuỗi các blocks – chứa một lượng lớn các proof of work.
- Thay đổi một block cũng đồng nghĩa yêu cầu thay đổi toàn bộ các block kế tiếp (successors) và làm lại toàn bộ các proof of work của nó.
  - Điều này sẽ giúp blockchain khỏi việc giả mạo.
  - Số lượng các successors liên quan tới việc đánh giá tính hợp lệ của một block: Cần ít nhất 6 successors để khẳng định 1 block là hợp lệ.

Proof of work

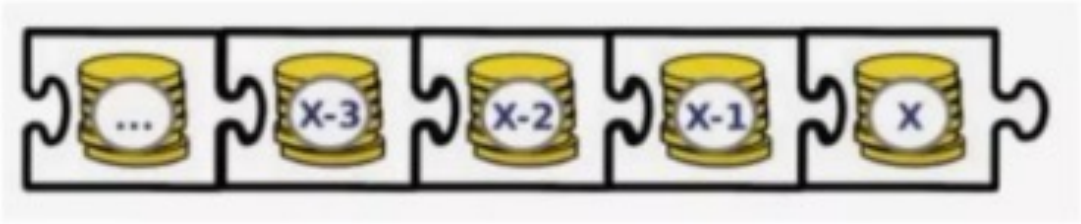


Các blockchain phổ biến hiện nay

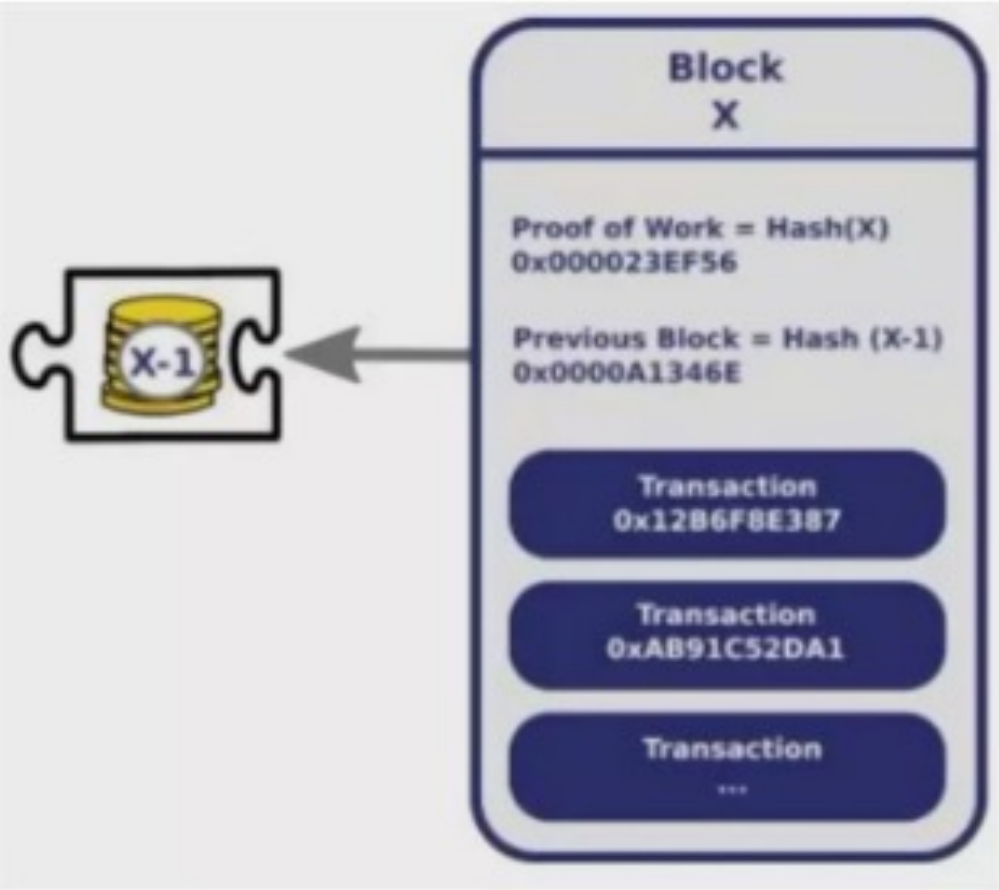


Cấu trúc dữ liệu

- Blockchain là một danh sách tuần tự có liên kết ngược của các block trong đó gồm các giao dịch
- Mỗi khối khi đã được đưa vào chuỗi thì độ phức tạp tính toán để thay đổi khối đó rất lớn và nó dẫn tới phải tính toán lại thay đổi toàn bộ các khối sau nó. Việc tính toán này là không thực tế.
- Các giao dịch mới được các thợ đào (miners) bổ sung vào các block và được đưa và cuối của blockchain, khi được chấp nhận bởi mạng thì không thể thay đổi, xoá bỏ nó.



Thông tin trong 1 block trong proof of work

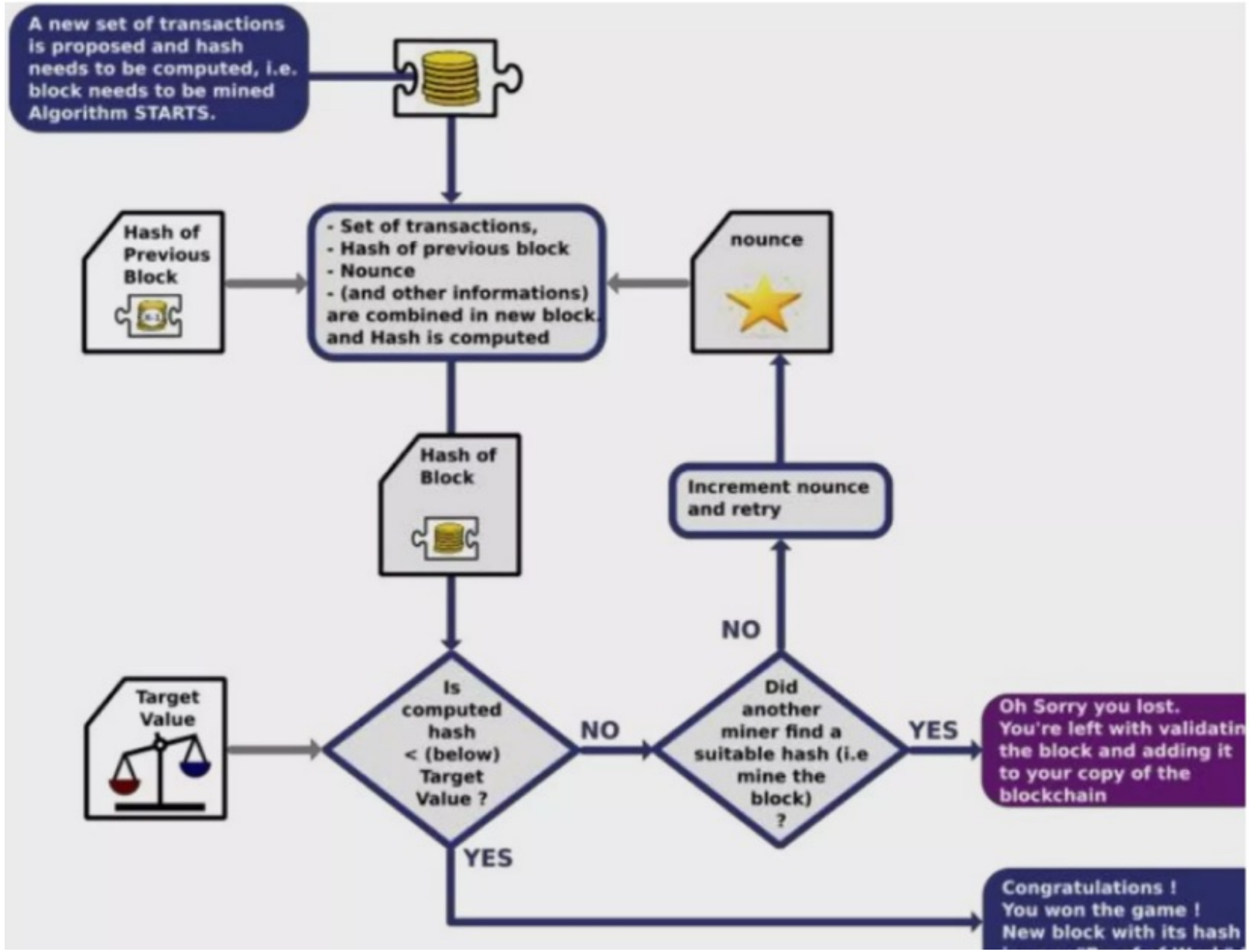


- Các transaction gần đây.
- Giá trị băm của block trước đó
- Lời giải của bài toán khó (Proof of work)

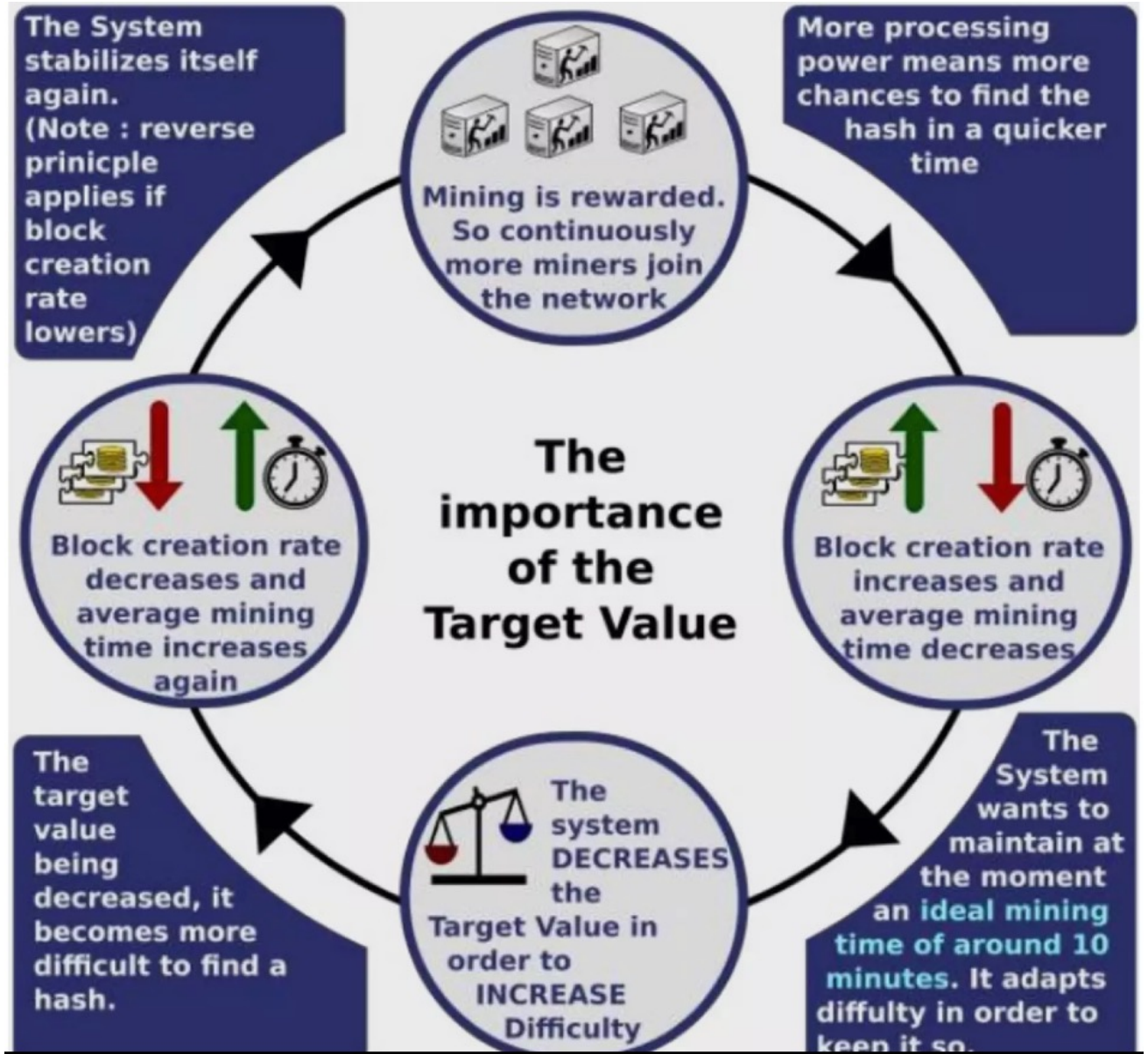
Khai thác / Mining

- Trong bitcoin, một giao dịch được quảng bá vào mạng bởi người tạo giao dịch. Tất cả các nút (node) đang tính toán block mới sẽ thu thập các bản ghi giao dịch này để đưa vào block. Quá trình này được gọi là khai thác hoặc đào (mining).
  - Đây là quá trình nhằm đưa giao dịch vào sổ cái của các giao dịch.
  - Quá trình này được thiết kế sao cho nó đòi hỏi tài nguyên lớn, độ khó cao nhằm đảm bảo số lượng block sinh ra trong ngày ổn định.
- Mục tiêu chính là quá trình khai thác là để các node trong mạng hướng tới một sự đồng thuận không thể giả mạo và an toàn.

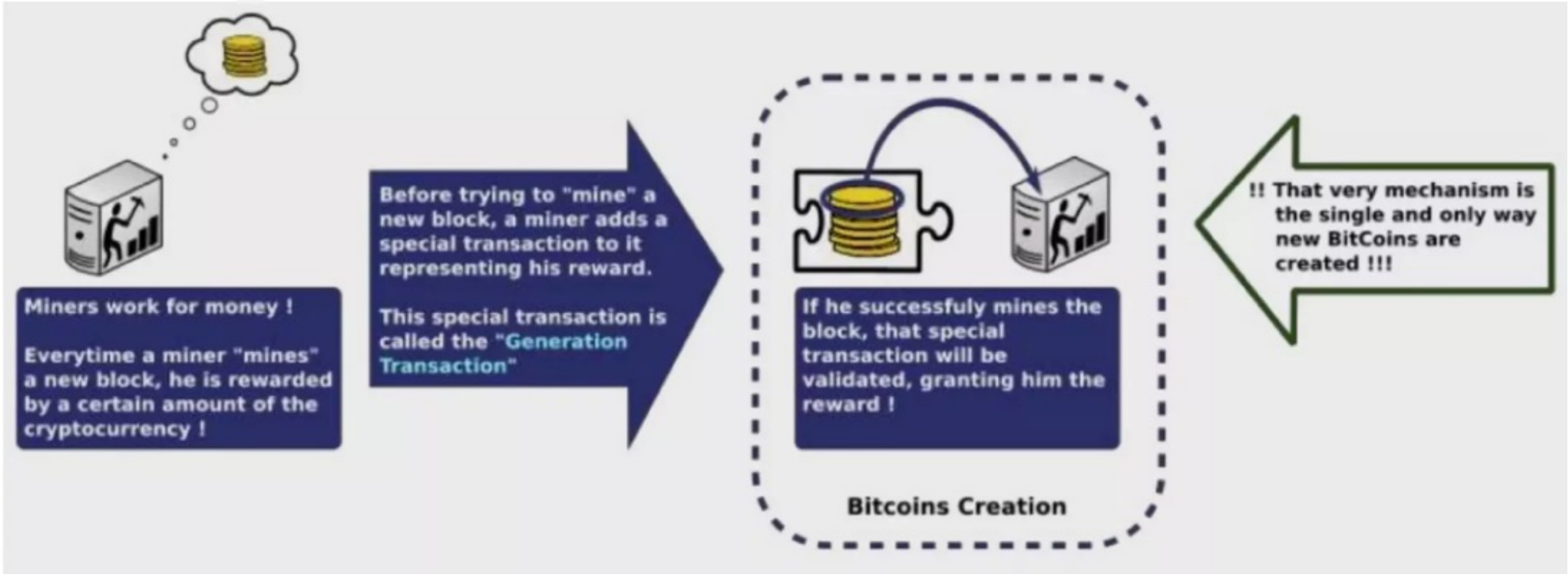
Thuật toán Khai thác/mining



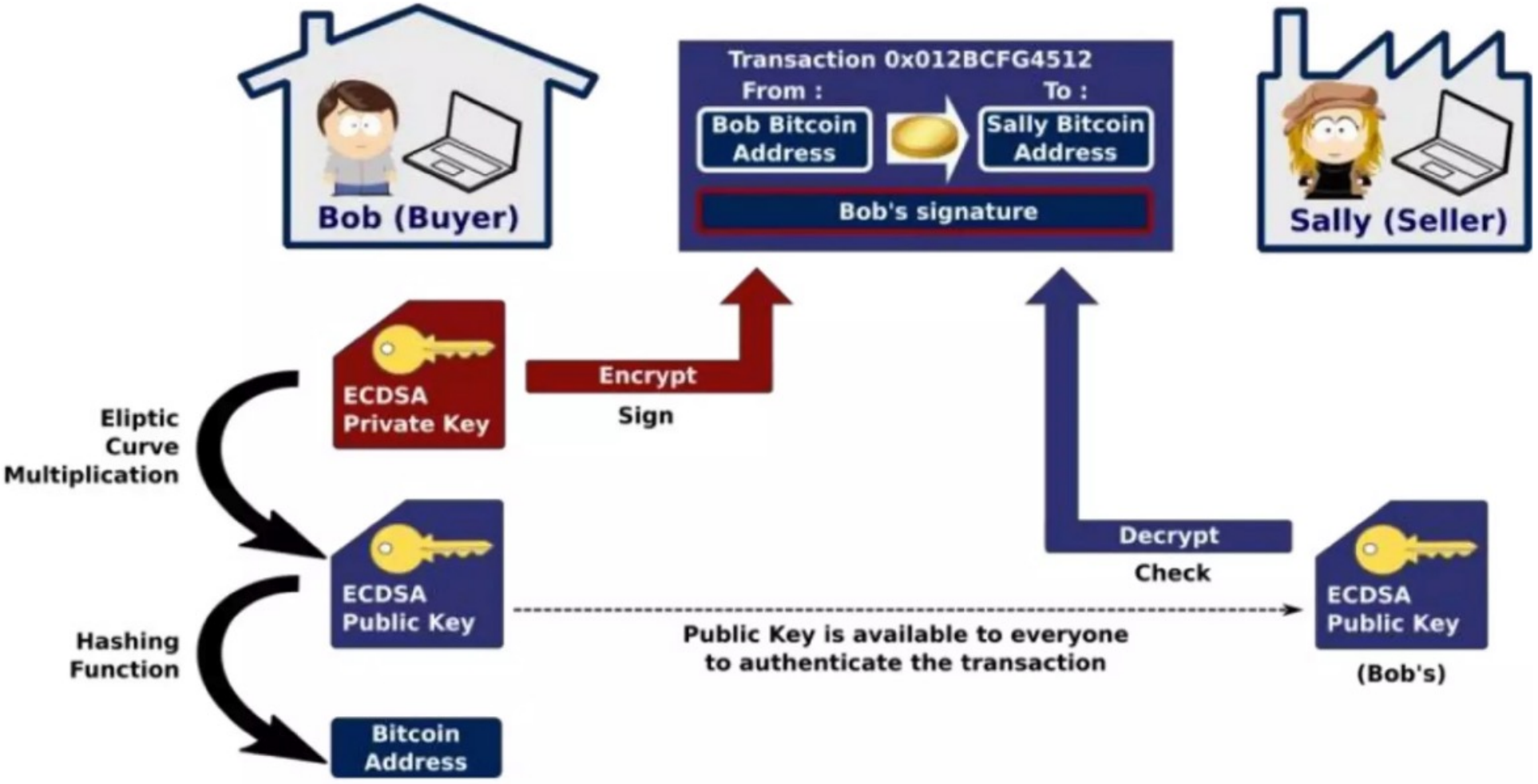
The importance of the target Value



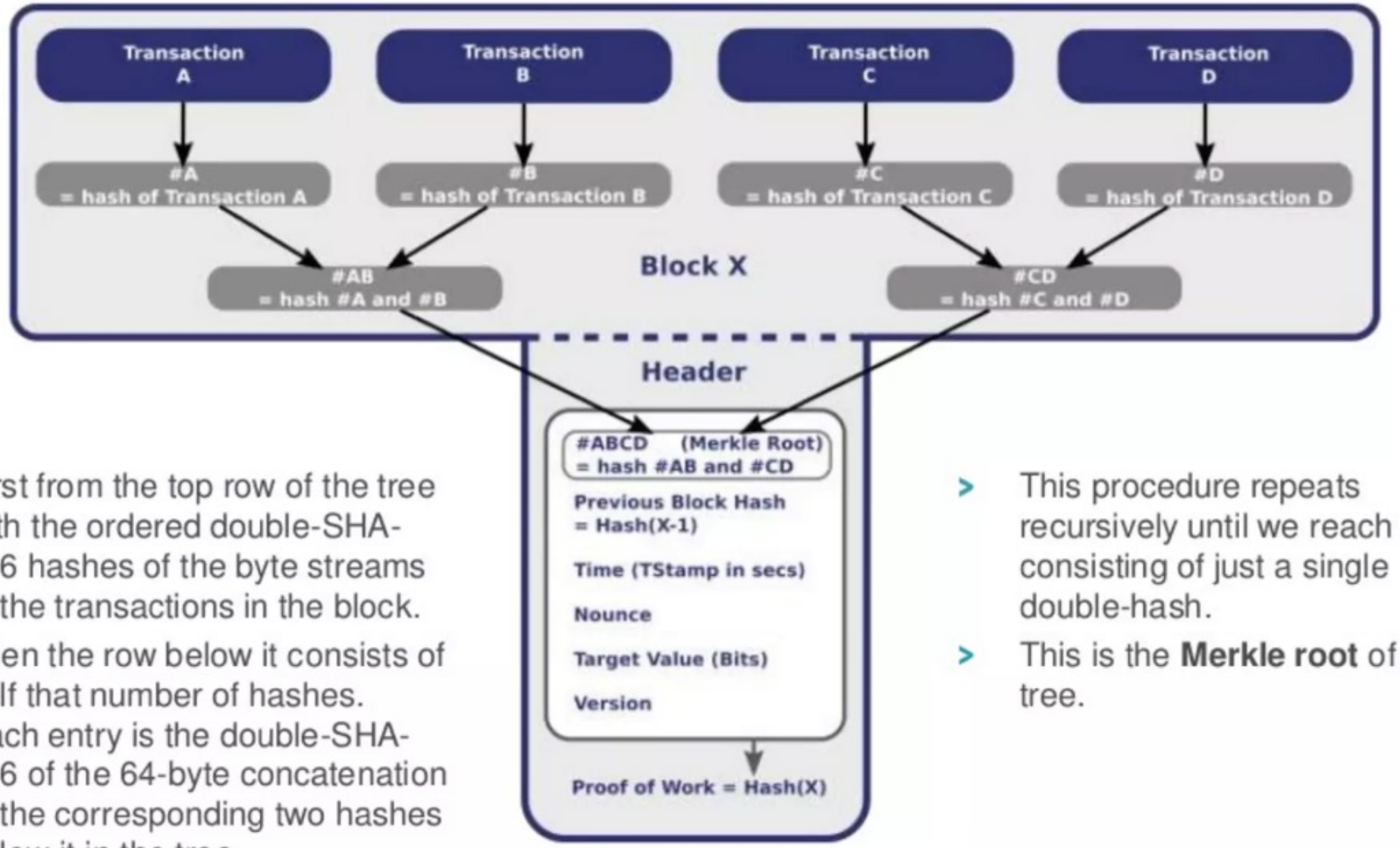
Phần thưởng cho người khai thác (Rewards for Miners)



Ví và cách tạo một giao dịch



Tổ chức thông tin các giao dịch trong 1 block

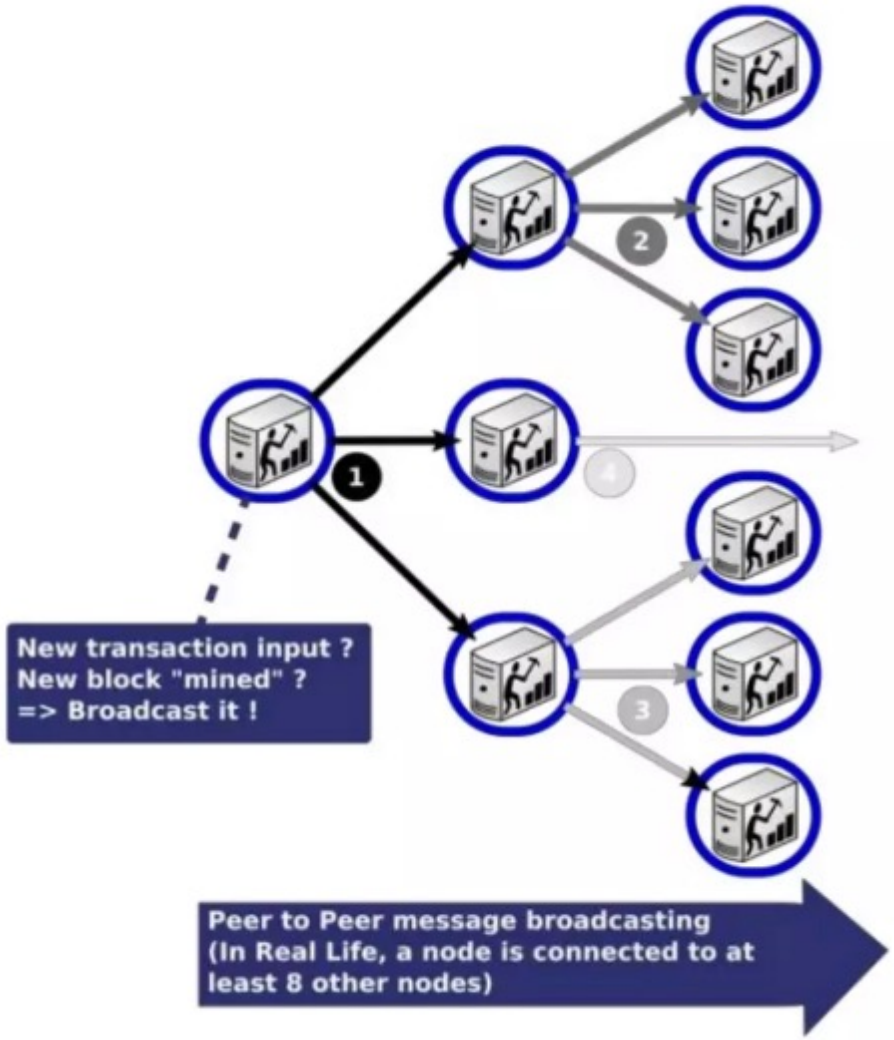


First from the top row of the tree with the ordered double-SHA-256 hashes of the byte streams of the transactions in the block.

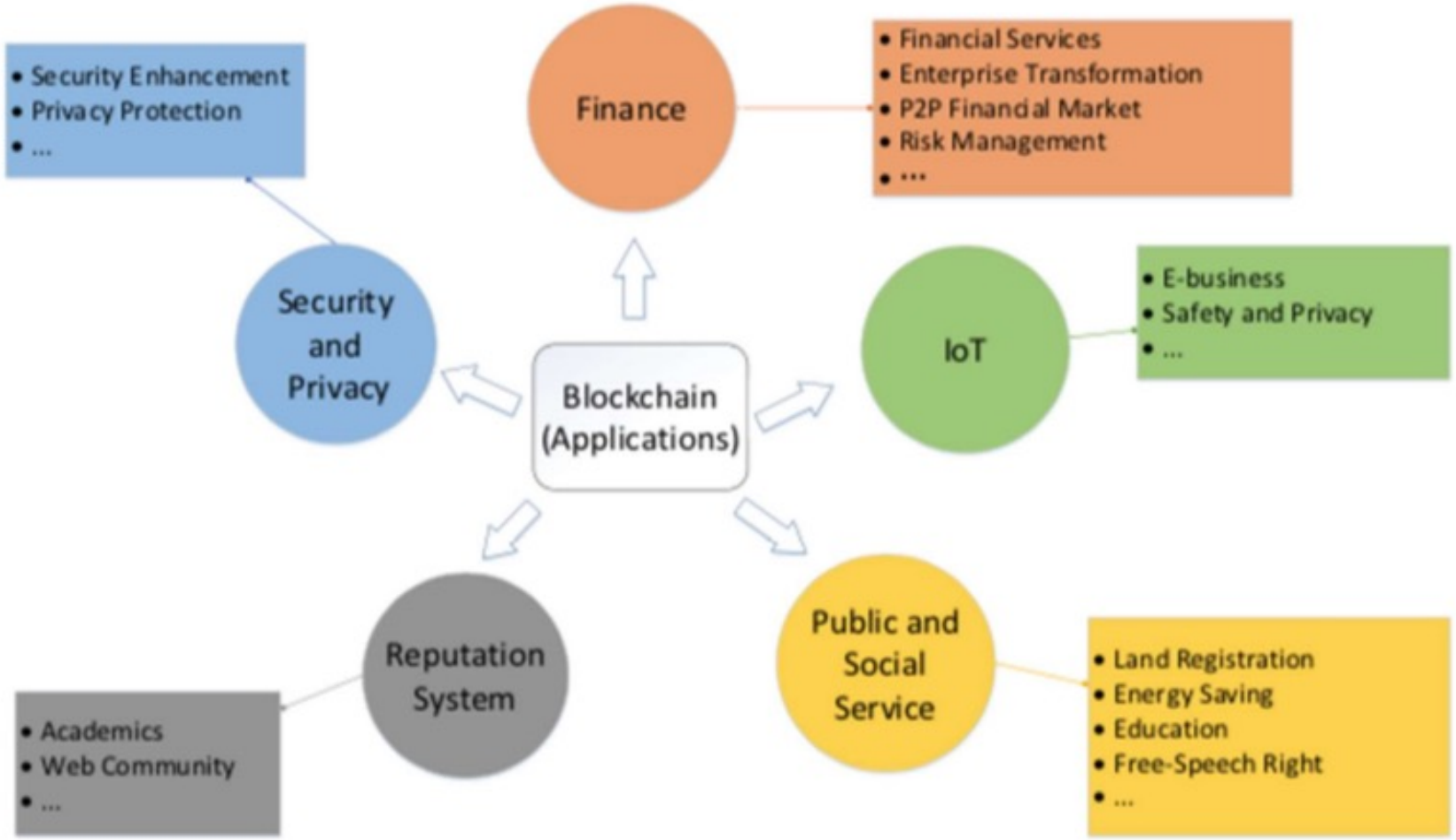
Then the row below it consists of half that number of hashes. Each entry is the double-SHA-256 of the 64-byte concatenation of the corresponding two hashes below it in the tree.

- This procedure repeats recursively until we reach a row consisting of just a single double-hash.
- This is the **Merkle root** of the tree.

Quảng bá block/Giao dịch – Giao thức Flood

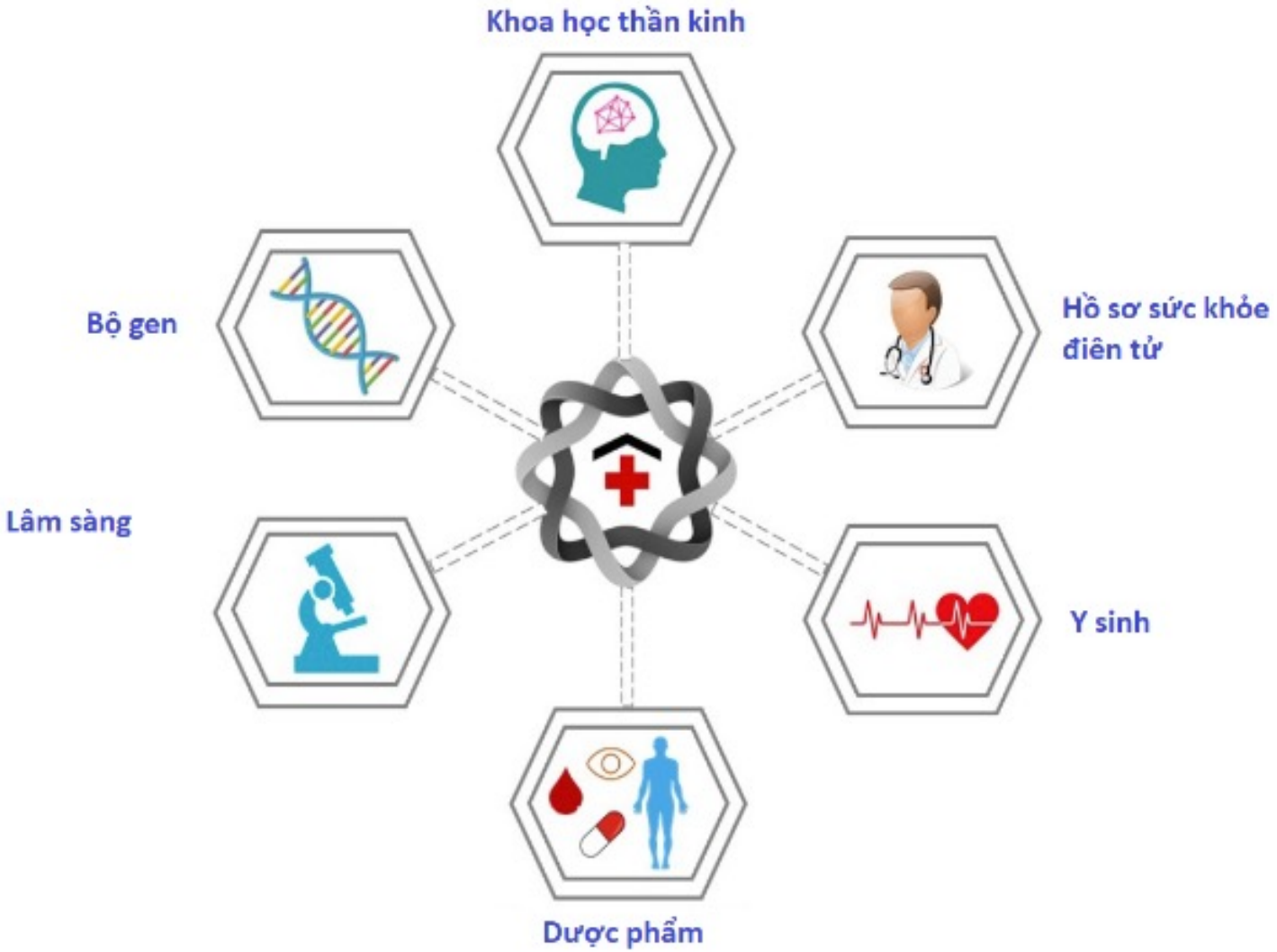


Ứng dụng của Blockchain

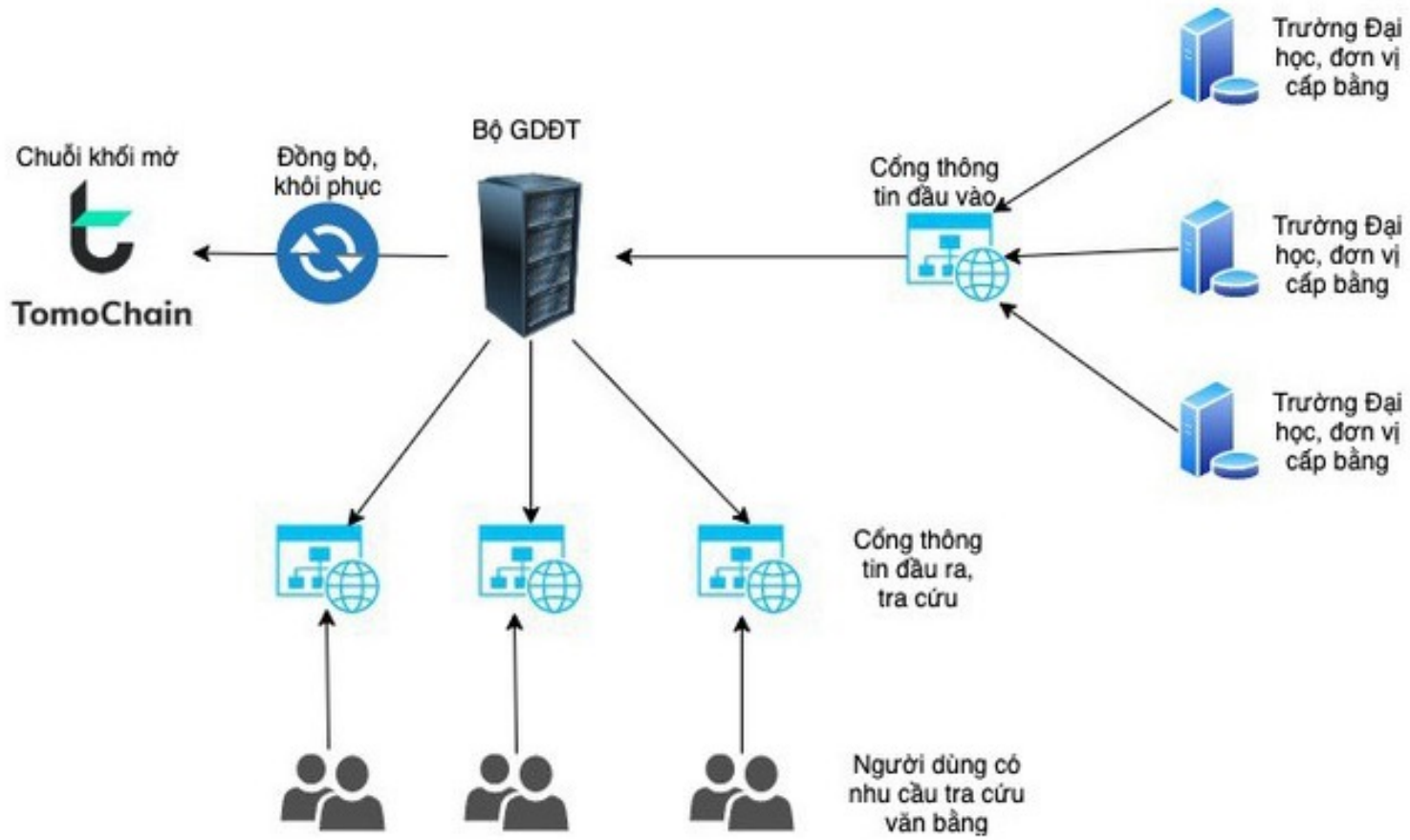


Mô hình Blockchain trong nông nghiệp

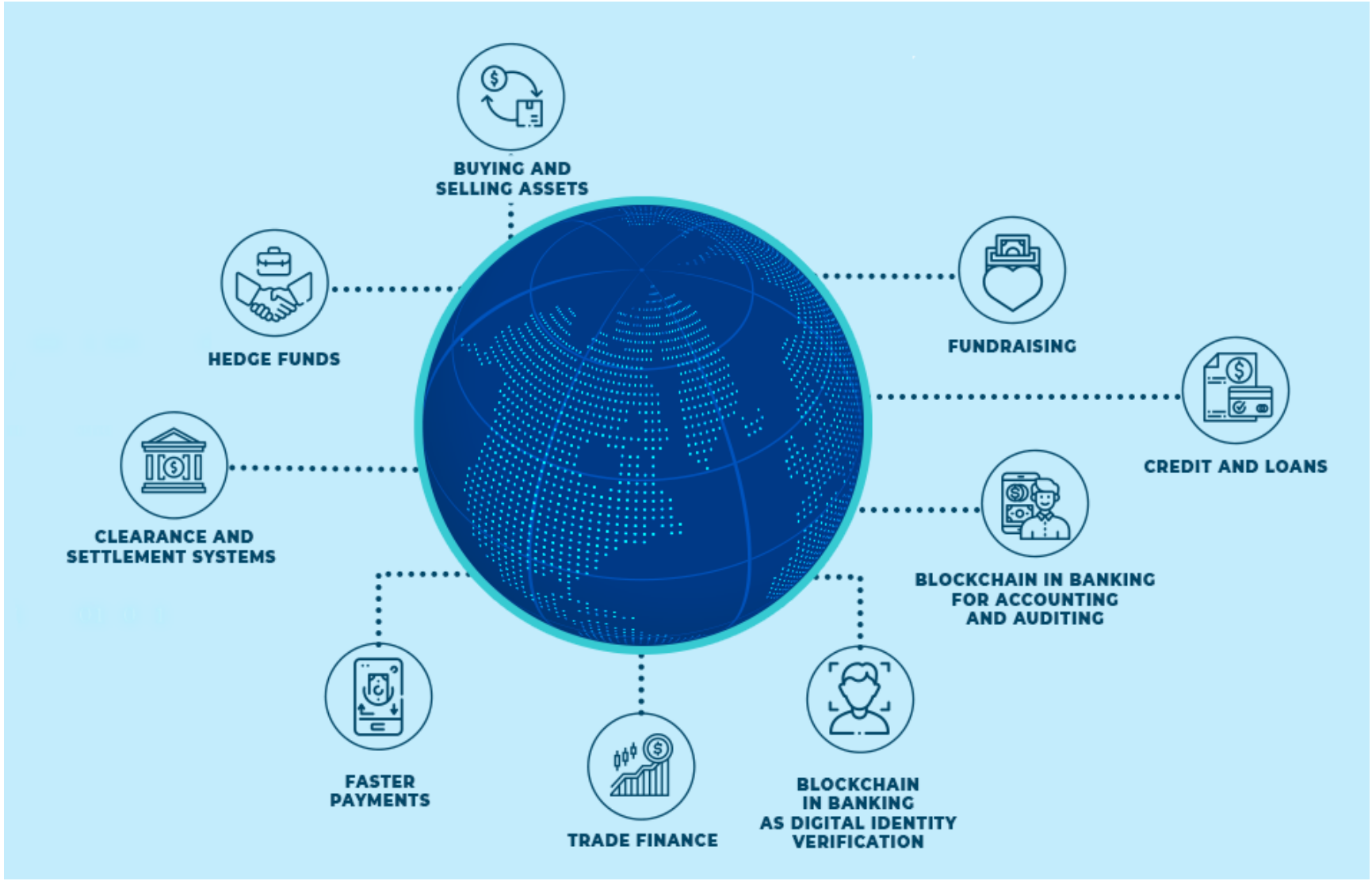
Ứng dụng Blockchain trong y tế



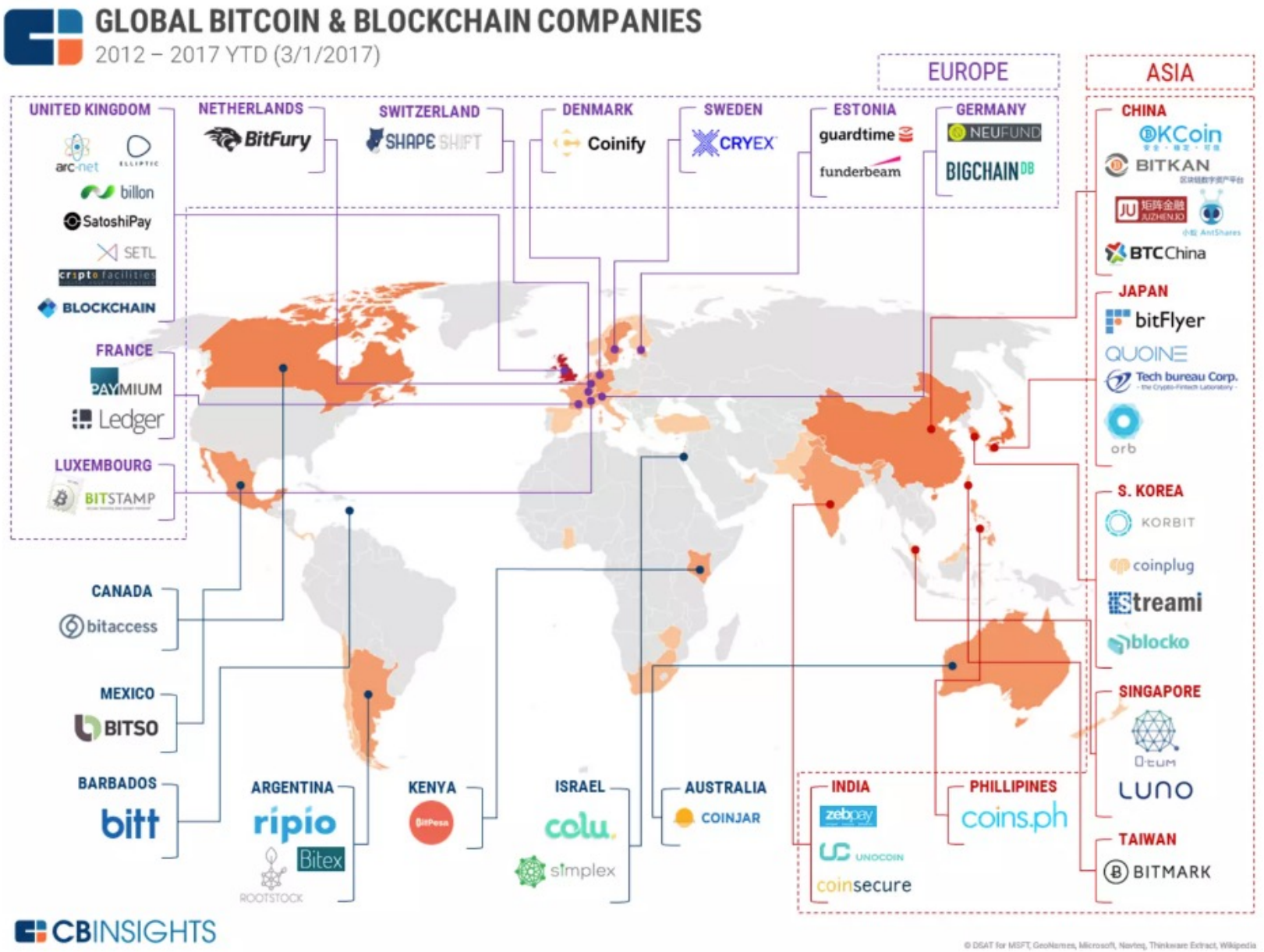
Ứng dụng Blockchain trong giáo dục



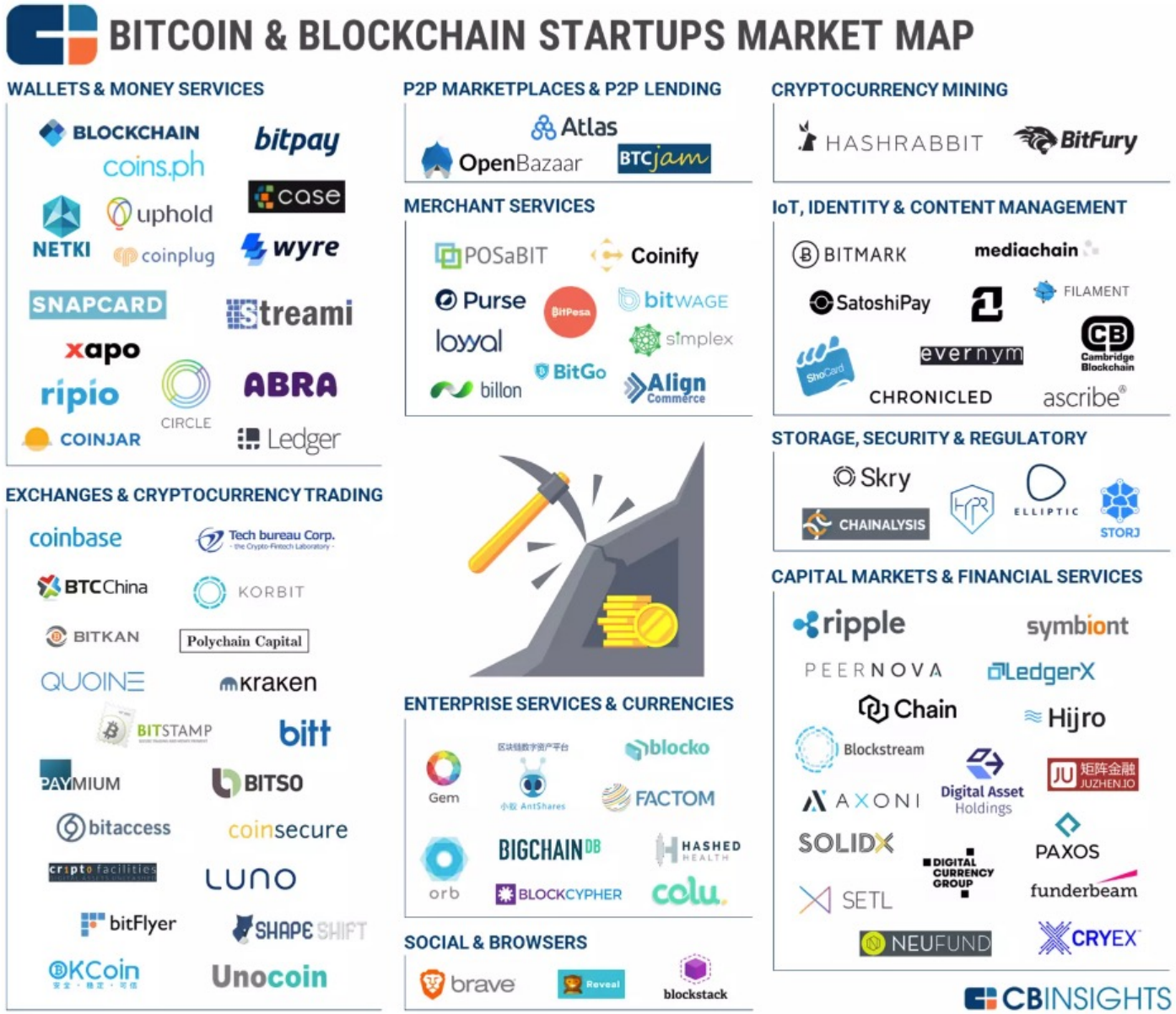
Ứng dụng Blockchain trong ngân hàng thanh toán



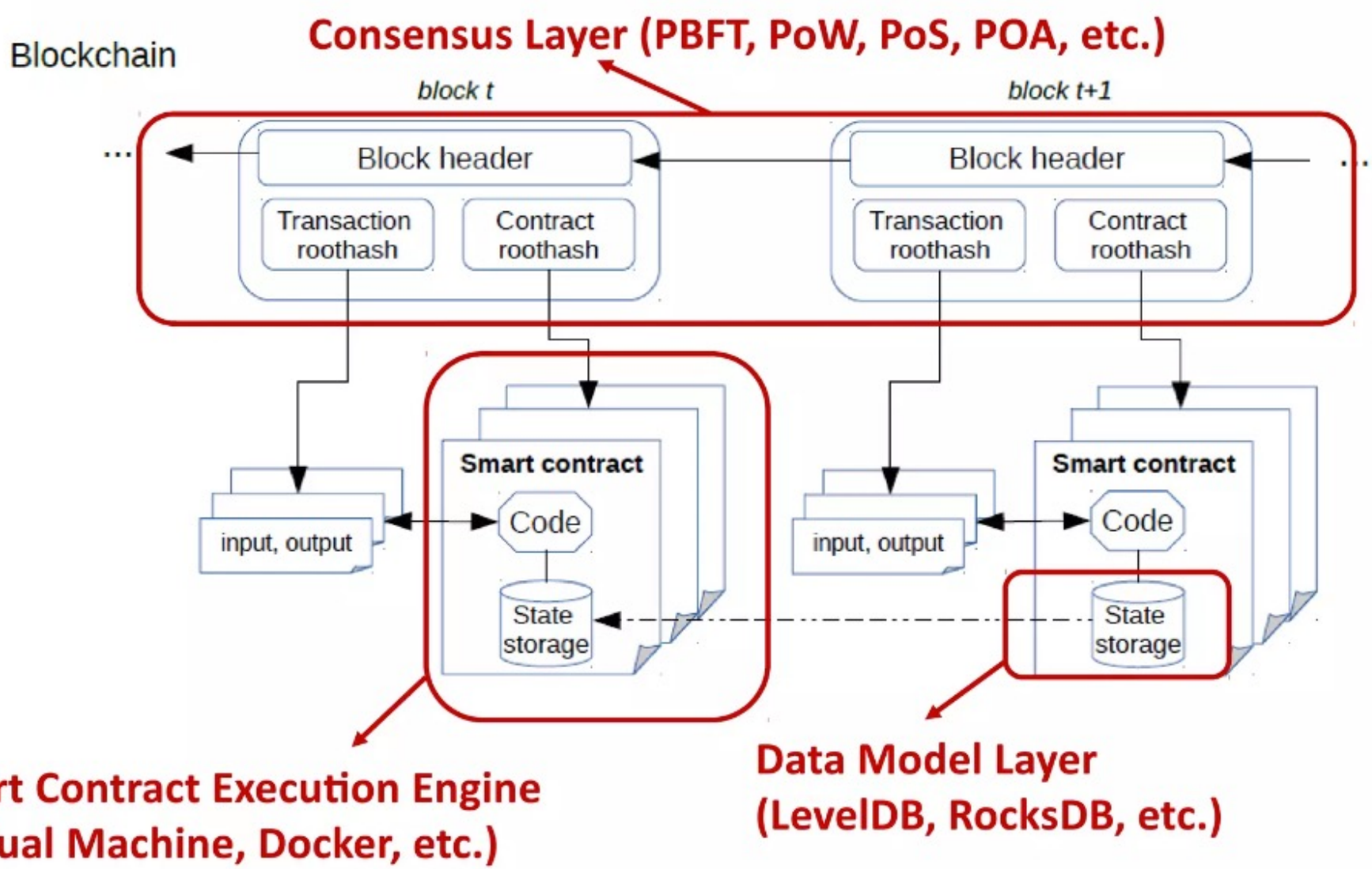
Global Blockchain Company



Global Blockchain Company (tt)



Blockchain 2.0 stack



Anh Dinh et al., SIGMOD 2017