

Thuật toán trên Blockchain

Ngày 21 tháng 7 năm 2021

1 Một số cơ chế đồng thuận

1.1 Bằng chứng công việc (Proof of Work-PoW)

Definition 1. PoW là cơ chế nhằm ngăn chặn việc sử dụng năng lực điện toán độc hại như gửi email spam hoặc phát động các cuộc tấn công từ chối dịch vụ (DoS - Denial Of Service) .

Bản chất Các nút đặc biệt (gọi là các thợ mỏ) cạnh tranh việc xác thực giao dịch (được đóng thành khối) để nhận phần thưởng. Họ thực hiện bằng cách sử dụng năng lực tính toán của hệ thống máy tính giải một câu đố chuyên sâu về tính toán (để xác minh) tìm ra số nonce, tìm ra được nonce tức là khai thác thành công khối đó.

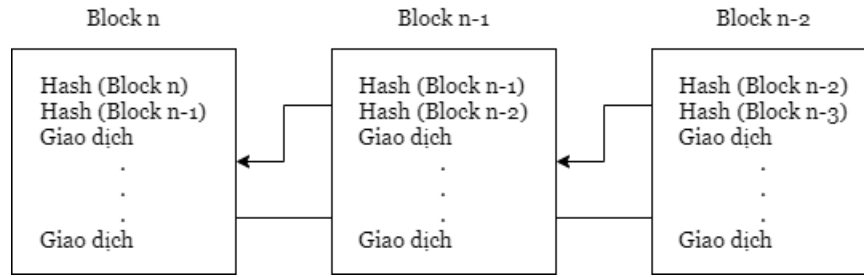
Mục đích Cơ chế PoW tạo ra nhằm mục đích kiểm soát công việc, đảm bảo rằng các khối mới không được tạo ra quá nhanh. PoW áp đặt một số giới hạn về hành động trong mạng. Nếu muốn tấn công vào mạng đòi hỏi rất nhiều sức mạnh tính toán và rất nhiều thời gian để thực hiện các tính toán. Do đó, các cuộc tấn công trên lý thuyết vẫn có thể xảy ra nhưng chi phí quá cao. Đây chính là ưu điểm lớn nhất của PoW.

PoW có khả năng ngăn chặn **chi tiêu kép** (double-spending), được hầu hết các loại tiền mã hóa sử dụng như là thuật toán đồng thuận của chúng, được dùng như một phương pháp để bảo mật cho sổ cái của tiền mã hóa. Cơ chế này phổ biến trong Bitcoin, Ethereum, và hầu hết các loại tiền mã hóa khác.

Cơ chế hoạt động

- Các thợ mỏ giải quyết các câu đố, hình thành các khối mới và xác nhận các giao dịch. Băm của mỗi khối chứa băm của khối trước đó, làm tăng bảo mật và ngăn chặn bất kỳ vi phạm khối nào. Bất kỳ khối nào bao gồm một giao dịch không hợp lệ sẽ bị mạng tự động từ chối.
- Sau khi khối mới được hình thành thì các giao dịch trong khối này được coi là đã xác nhận.

1 Một số cơ chế đồng thuận



Hình 1.1: Mô hình cơ chế hoạt động của PoW

Rào cản trong thực tiễn:

- Khả năng tiếp cận: đòi hỏi một lượng năng lượng đáng kể để duy trì, đồng thời phải mua, thiết lập và duy trì tất cả các phần cứng cần thiết để chạy hệ thống máy tính khai thác PoW.
- Tập trung: tập trung thành hai loại: các tập đoàn khai thác mỏ lớn hoạt động trong các khu vực có chi phí điện thấp và thời tiết lạnh (để giảm chi phí làm mát phần cứng khai thác) và các hồ khai thác mỏ.
- Khả năng mở rộng: khả năng mở rộng của mạng lưới bị giới hạn do phụ thuộc tốc độ khai thác khối.

1.2 Bằng chứng cổ phần (Proof of Stake - PoS)

Definition 2. PoS là cơ chế đồng thuận trong đó các nút của mạng blockchain phải cược một phần tài sản để được tham gia vào quá trình xác nhận các giao dịch trong một khối. Các nút tham gia được gọi là người xác thực (validator). Số tiền đặt cược được gọi là cổ phần (stake). Số tiền này sẽ bị hệ thống khóa lại, cho đến khi nút đó rút khỏi công việc xác thực.

Người xác thực được chọn ngẫu nhiên từ tập những người cược tiền. Nếu khối hợp lệ, nút tham gia xác thực sẽ nhận được phần thưởng là các khoản phí giao dịch, thường giao động từ 10 – 15% tiền cược. Chính vì vậy, cược càng nhiều thì phần thưởng càng lớn.

1.2.1 Cách thức chọn người xác nhận

Người dùng khóa một số tiền nhất định vào mạng làm cổ phần. Số lượng cổ phần càng lớn, thì cơ hội được chọn làm người xác thực khối kế tiếp càng lớn. Để tránh việc quá

1 Một số cơ chế đồng thuận

trình chỉ ưu tiên cho các nút giàu nhất trong mạng, hai phương pháp được sử dụng phổ biến nhất là:

- Lựa chọn khối ngẫu nhiên: tìm kiếm các nút có giá trị băm thấp nhất kết hợp với cổ phần lớn nhất. Vì độ lớn của cổ phần được công khai, nên có thể dự đoán người được chọn làm người xác thực kế tiếp.
- Lựa chọn độ tuổi tài sản: các nút được chọn dựa trên thời gian mà các token của họ đã được lưu giữ làm cổ phần gọi là độ tuổi tài sản. Độ tuổi của tài sản phải không dưới 30 ngày mới được xét chọn làm người xác thực.

1.2.2 Hiệu quả bảo mật:

Người xác thực có thể phê duyệt một giao dịch gian lận, tuy nhiên, người đó sẽ mất một phần trong cổ phần và không được làm người xác thực trong tương lai. Vì vậy, khi cổ phần cao hơn phần thưởng, nếu gian lận thì người xác thực sẽ mất nhiều hơn số tiền thu lại được.

PoS giải quyết ba vấn đề của chuỗi PoW được thảo luận trước đó:

- Khả năng truy cập: không cần dùng nhiều năng lực tính toán, tuy nhiên, lại yêu cầu người xác thực phải đặt cược cổ phần với một lượng khá đáng kể.
- Tập trung hoá: việc chọn người xác thực không phụ thuộc vào số nút người đó kiểm soát, mà chỉ phụ thuộc vào số cổ phần người đó đang sở hữu hay độ tuổi của tài sản.
- Khả năng mở rộng: cho phép mở rộng bằng phương pháp sharding (phân mảnh) mà không làm giảm bảo mật.

PoS phổ biến trong Decred, Peercoin, Ethereum và trong tương lai là nhiều loại tiền mã hoá khác. Phân cấp hơn, tiêu hao ít năng lượng và không dễ gì bị đe dọa.

1.3 Bằng chứng cổ phần ủy quyền (Delegated Proof of Stake - DPoS)

Definition 3. DPoS là một cơ chế đồng thuận thay thế, đòi hỏi các cổ đông phải bỏ phiếu cho các "đại biểu", những người này sau đó chịu trách nhiệm xác nhận các giao dịch và duy trì chuỗi khối.

1 Một số cơ chế đồng thuận

Những người nắm giữ tài sản sẽ bỏ phiếu cho một nhóm đại biểu được chọn để thực hiện vai trò xác nhận các giao dịch. Quyền biểu quyết nhiều hay ít phụ thuộc số lượng tài sản mà người đó nắm giữ.

Nó có thể được coi là giao thức đồng thuận ít tập trung nhất trong số các giao thức, cũng như có tính bao quát nhất. Một đại biểu thể hiện cam kết bằng cách cược tiền vào hệ thống (tài sản này sẽ bị tịch thu trong trường hợp người này thực hiện các hành vi gây hại cho hệ thống). Vai trò của các đại biểu: đảm bảo hoạt động của nút, xác thực giao dịch, chia phần thưởng cho cử tri.

Về bản chất, một mạng lưới DPoS được tự quản lí và điều chỉnh bởi tất cả những người tham gia của nó, việc đảm bảo lợi ích tốt nhất cho mạng vẫn là ưu tiên hàng đầu. DPoS được sử dụng ở nhiều đồng tiền mới sau này có thể kể đến như: Bitshares, EOS, LISH, ICON, Cybermiles,...

1.4 Bằng chứng ủy nhiệm (Proof of Authority - PoA)

Definition 4. PoA là một thuật toán đồng thuận dựa trên danh tiếng, trong đó những người xác thực khối được chọn không dựa trên số lượng tài sản mà dựa trên chính danh tiếng của mình.

Người xác thực là những người điều tiết của hệ thống được chọn dựa trên danh tiếng của họ.

Mô hình PoA có số lượng người xác thực khối giới hạn, phù hợp hơn cho các mạng blockchain riêng tư vì hiệu suất làm việc của nó cao hơn rất nhiều các hệ thống khác, đồng thời nó đề cao danh tính của người dùng thay vì số cổ phần của người dùng.

Các điều kiện cho đồng thuận PoA:

- Danh tính hợp lệ và đáng tin cậy: người xác thực cần xác nhận danh tính thực của mình.
- Khó khăn để trở thành người xác thực: ứng viên phải sẵn sàng đầu tư tiền và chấp nhận rủi ro với danh tiếng của mình.

Hạn chế của hệ thống PoA là danh tính của những người xác thực được công khai, việc này có thể tạo cơ hội cho các bên thứ ba khai thác.

Đây là mô hình tập trung thường thấy trong POA.Network, Ethereum Kovan Testnet với đặc điểm là hiệu suất cao, có khả năng mở rộng tốt.

2 Staking

2.1 Staking là gì?

- Staking là khóa (hay đặt cược) các đồng tiền mã hóa để nhận các phần thưởng.
- Cũng giống như việc đào là điều cần thiết đối với các hệ sinh thái blockchain sử dụng bằng chứng công việc (PoW), việc đặt cược là cần thiết đối với các hệ sinh thái dựa trên bằng chứng cổ phần (PoS) và các biến thể của nó.
- Giúp mạng lưới tạo sự đồng thuận tính hợp lệ của các giao dịch trong mạng bằng cách yêu cầu người xác thực (validator) sở hữu và duy trì một số lượng nhất định đồng nội tệ được khóa trong hợp đồng thông minh.
- Phí giao dịch từ block mới trả cho validator. Một số nền tảng khác, khi có thêm cơ chế tạo ra đồng tiền mới sau những lần block được validate, sẽ trả cho validator chính khoản tiền ảo mới được sinh ra.

2.2 Quy trình Staking

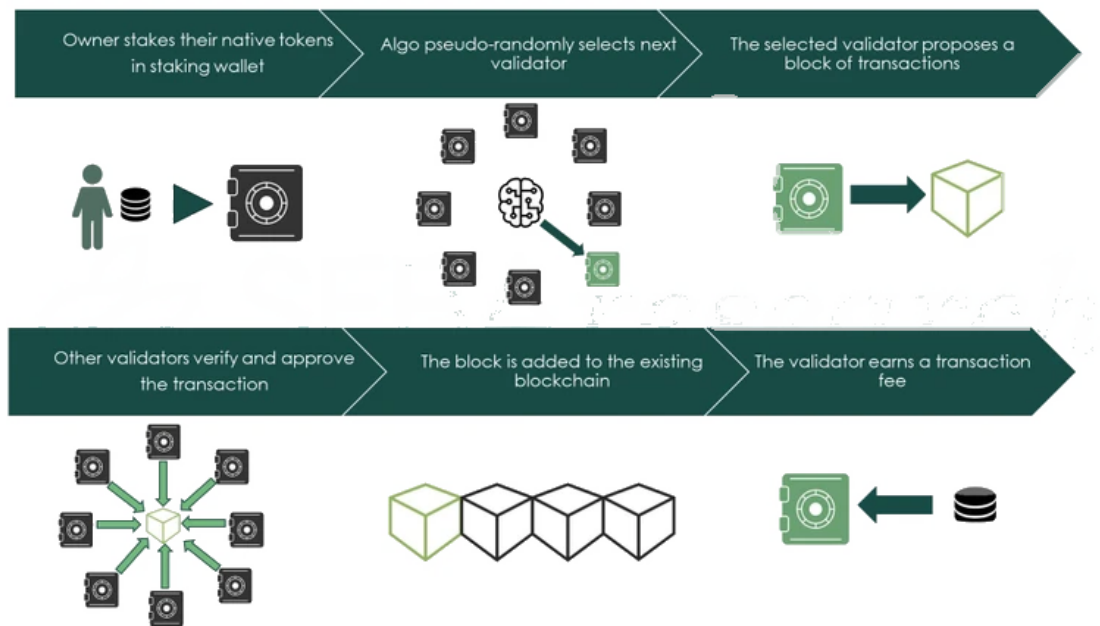
1. Trở thành người xác thực

Cần phải sở hữu một số lượng tiền điện tử (token gốc) nhất định được khóa tại một địa chỉ gửi tiền được chỉ định để trở thành người xác thực trong một giao thức staking-based.

Có hai loại giao thức staking-based phổ biến:

- PoS: không có giới hạn về số lượng người xác thực có thể tham gia vào mạng lưới, với điều kiện là họ đặt cược số lượng tiền cần thiết. Cho phép mạng lưới phi tập trung hơn bằng cách tối thiểu nhất rào cản đối với nút mạng để trở thành người xác thực. Những dự án có cơ chế staking này như: Decred, Peercoin, Ethereum2.0, IOST, TRX, WAX, TomoChain,...
- DPoS: Chỉ ủy quyền trách nhiệm xác thực cho một số nút được giới hạn. Các nút khác thường có một số quyền biểu quyết để chọn các người xác thực này

2 Staking



Hình 2.1: Quy trình Staking

(khá giống với bỏ phiếu dân chủ hiện nay). Tuy nhiên, hệ sinh thái sử dụng DPoS ít phi tập trung hơn. Dự án sử dụng cơ chế này: Bitshares, EOS, LISH, ICON, Cybermiles,...

2. Lựa chọn người xác thực

Khi tiền đã được đặt cọc, một thuật toán sẽ chọn ra người xác thực, để tạo ra một khối giao dịch mới. Thuật toán lựa chọn người xác thực thường dựa trên các tiêu chí:

- **Số lượng stake:** mạng chọn người xác thực dựa trên số lượng tiền được đặt cọc. Số lượng tiền càng nhiều thì khả năng được chọn càng lớn. Cách tiếp cận này không được khuyến nghị, vì nó dẫn đến việc phân phối tiền bị lệch trong mạng, do đó các nhà đầu tư giàu có có xác suất nhận được phần thưởng khối cao hơn.
- **Tuổi staking:** chọn người xác thực dựa trên thời gian tiền đã được đặt cọc trong thời gian bao lâu. Người xác thực đã đặt cọc trong thời gian dài hơn sẽ có cơ hội được chọn cao hơn. Khi đã được chọn, tuổi của số tiền đã đặt cọc sẽ được điều chỉnh lại thành 0.
- **Ngẫu nhiên:** người xác thực được chọn bằng cách sử dụng công thức tìm kiếm

giá trị băm thấp nhất. Khi các cổ phần được biết đến công khai, có thể dự đoán với độ chính xác hợp lý ai sẽ được chọn để đề xuất khối tiếp theo.

Hầu hết các phương pháp này về bản chất đều là pseudo-random.

3. Thêm khối mới

Có hai cơ chế thêm khối mới vào blockchain:

- Chain-based proof-of-stake: người xác thực được chọn theo tần suất xác định trước (ví dụ: cứ sau 60 giây) và được chỉ định quyền tạo một khối duy nhất.
- Byzantine-fault-tolerant proof-of-stake: người xác thực được quyền đề xuất một khối giao dịch mới, những người xác nhận khác sẽ bỏ phiếu về tính hợp lệ của khối được đề xuất.

Cách tiếp cận thứ hai chủ yếu được sử dụng trong PoS.

4. Nhận phần thưởng

- Khi khối được thêm vào chuỗi, người xác thực sẽ nhận được phần thưởng khối của họ. Phần thưởng khối này có thể là phí giao dịch, tiền mới hoặc cả hai. Tuy vậy, việc thưởng cho những người đặt cược bằng tiền mới dẫn đến sự phân phối tiền không đều.
- Để khắc phục, các mạng PoS có xu hướng khai thác trước tất cả tiền của họ hoặc sử dụng đồng thuận hỗn hợp PoS và PoW trong đó PoW được sử dụng để tạo tiền mới và PoS được sử dụng để xác thực các giao dịch.

2.3 Hình thức staking: 2 loại

2.3.1 Những người có số lượng coin nhỏ

- Không đáp ứng yêu cầu trở thành node hoặc masternode
- Tham gia voting hoặc staking vào những node có sẵn. Khi node đó trở thành validator thì sẽ nhận được phần thưởng.
- Bao gồm: staking trên ví hoặc trên sàn.

2.3.2 Những người có lượng coin lớn

- Tham gia ứng cử trở thành node hoặc masternode để trực tiếp tham gia xử lý giao dịch và tạo khối.
- Nhận được nhiều phần thưởng hơn nhưng trách nhiệm và rủi ro sẽ cao hơn.

2.4 Phương pháp staking

2.4.1 Sử dụng ví nóng

- Người dùng nạp tiền vào ví, sau đó sử dụng ví để staking.
- Tiền thu được sẽ được chuyển vào ví.
- Sử dụng cho người dùng có số lượng coin nhỏ do mức độ bảo mật không cao.




2.4.2 Cold staking

- Quá trình staking trên ví mà không được kết nối với mạng internet, được thực hiện bằng cách sử dụng phần cứng hoặc ví phần mềm air-gapped.
- Dựa trên một hợp đồng thông minh ủy quyền quyền đặt cược cho một nút đặt cược. Nút đặt cược luôn trực tuyến nhưng không chứa khóa riêng.
- Cho phép người dùng giữ tiền an toàn. Tuy nhiên, người đặt cược phải giữ các đồng tiền đã đặt cược ở cùng một địa chỉ, vì việc di chuyển chúng sẽ phá vỡ thời gian khóa, do đó khiến họ mất phần thưởng đặt cược. Hình thức này đặc biệt có ưu điểm đối với những người tham gia đặt cược lớn và muốn bảo vệ tối đa số tiền của mình trong khi vẫn được hỗ trợ mạng.
- Ví dụ: Ledger, Trust Wallet, CoolWallet S, Trezor,...

2.5 Những yếu tố ảnh hưởng đến staking

- Số lượng coin tối thiểu: để 1 user khi tham gia vào staking khác nhau tùy từng dự án.
- Độ tuổi coin: khoảng thời gian coin bắt đầu sinh lời tính từ lúc đưa coin vào stake đến lúc tham gia staking chính thức.
- Lãi suất: tùy thuộc các hệ sinh thái, lãi càng lớn thì lượng coin nhận được sau khi Stake càng lớn.
- Tỷ lệ lạm phát
- Thời gian lock, unlock

2 Staking

CRITERIA	 TOMOCHAIN	 ETHEREUM	 EOS	 TRON
TPS	2000	15	4000	2000
CONSENSUS	PoSV	PoW	DPoS	PoS
CIRCULATING SUPPLY/ TOTAL SUPPLY	59,817,850 / 100,000,000	106,058,776 / Infinity	911,510,888 / 1,011,510,892	66,682,072,191 / 99,281,283,754
MAINNET LAUNCH	Dec 2018	July 2015	Jun 2018	May 2018
BLOCKTIME	2s	15s	0.5s	3s
BLOCK PRODUCERS	150	8807	21	27
SMART CONTRACT LANGUAGE SUPPORT	Solidity, Vyper	Solidity, Vyper	C++	Solidity, Vyper
DEX ECOSYSTEM	Layer 1 TomoX, TomoDEX (To be released Q3-Q4/2019)	Layer 2 DEXs (IDEX, 0x..)	Layer 2 DEXs	Layer 2 DEXs
STAKING REWARD	Around 7% annual interest	-	1.83% annual interest	4.21% annual interest

Hình 2.2: Một số hệ sinh thái

2.6 Ưu, nhược điểm

2.6.1 Ưu điểm khi staking




















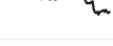





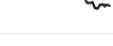




- Dễ dàng khai thác: Với staking, không cần chuẩn bị dàn máy đào cầu kỳ như mining. Người dùng hoàn toàn có thể mua coin dễ dàng rồi trữ chúng trong ví điện tử. Tiếp theo là trở thành “người xác thực” và chờ nhận thưởng.
- Giảm chi phí đầu tư: quá trình khai thác coin của bạn không cần thông qua thiết bị máy móc đắt tiền và tốn kém như GPU hay ASIC. Việc này giúp các trader dễ dàng tham gia mà không bỏ ra nhiều chi phí ban đầu hay phí bảo quản trong quá trình đào.
- Không tốn nhiều điện
- An toàn, bảo mật hệ thống: Nếu tấn công hệ thống, hacker cần nắm giữ ít nhất 51% toàn bộ số coin trong mạng lưới. Đó là điều rất khó xảy ra, hơn nữa chi phí để nắm giữ 51% lượng coin thậm chí còn vượt quá số lượng coin hack được.
- Lãi suất ổn định: những người xác thực chắc chắn sẽ nhận được phần thưởng

2 Staking

(chính là phí giao dịch).

2.6.2 Rủi ro khi staking

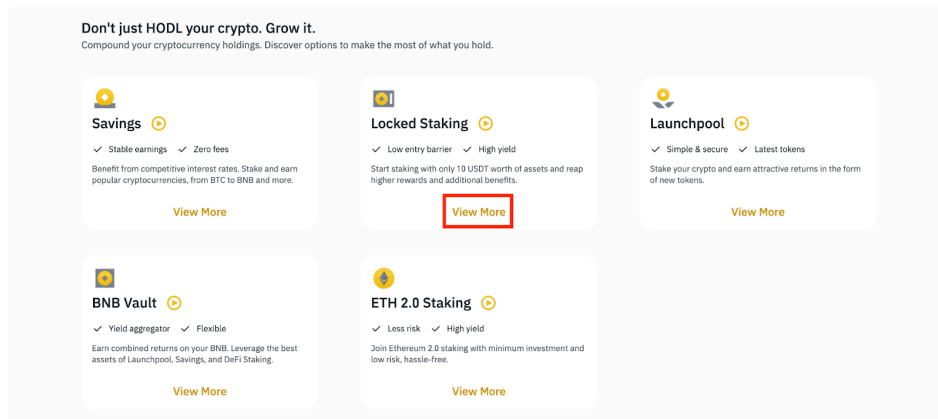
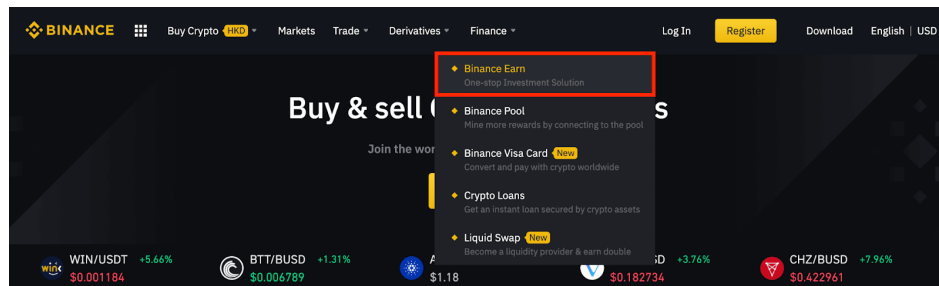
- Không thể dùng tiền trong khi bị khóa: không thể thực hiện bất kỳ giao dịch nào với số coin này.
- Chịu rủi ro nếu coin mất giá: khi tiền điện tử bị khóa trong ví bị mất giá, người xác thực không kịp thời bán chúng đi nếu còn nằm trong thời hạn khóa.
- Bảo mật ví cá nhân còn kém: Sử dụng ví nóng bạn cần phải công khai thông tin cá nhân. Những tin tặc rất dễ xâm nhập vào ví điện tử để đánh cắp tài sản và thông tin.

# ¹	Asset	Price ¹	24h ¹	Reward ¹	Staked Value ¹	Market Cap ¹	Total Staked ¹	7d Price Change ¹	Add ¹
1	 Cardano ADA	\$1.06	-2.75%	9.3%	\$24,328,221,791	\$33,978,764,568	70.54%		
2	 Ethereum 2.0 ETH	\$1,786.07	+1.56%	5.9%	\$11,190,191,115	\$208,059,493,678	5.4%		
3	 USD Coin USDC	\$1	+0.48%	5.13%	\$10,983,103,717	\$26,806,919,333	N/A		
4	 Solana SOL	\$23.35	-0.26%	6.03%	\$8,475,723,809	\$6,380,394,248	73.52%		
5	 Polkadot DOT	\$11.12	+1.94%	13.27%	\$7,484,623,285	\$11,230,024,892	62.89%		
6	 Dai DAI	\$1	+0%	3.74%	\$5,601,357,491	\$5,226,085,775	N/A		
7	 Algorand ALGO	\$0.71	-1.78%	5.6%	\$3,883,206,726	\$2,217,000,343	51.76%		
8	 Binance Smart Ch BNB	\$266.35	-0.54%	9.74%	\$3,519,436,629	\$41,178,820,112	60.2%		
9	 Terra LUNA	\$5.84	-0.51%	9.85%	\$2,196,073,333	\$2,445,048,126	38.07%		
10	 Avalanche AVAX	\$9.77	-1.31%	9.8%	\$2,073,747,802	\$1,675,186,715	55.63%		

Hình 2.3: Một số tiền điện tử cho phép staking

2.7 Hình thái mới: DeFi Staking


- Thay vì sử dụng các đồng token gốc thì người dùng sử dụng các token dưới dạng stablecoin để ngăn chặn việc bị mất giá trong quá trình staking.
- Đặc điểm:
 - Không cần quản lý khóa cá nhân, thu thập tài nguyên
 - Không phải thực hiện giao dịch hoặc thực hiện các nhiệm vụ phức tạp khác
- Một số sàn phi tập trung cho phép staking trên sàn: Binance, Coinbase,...



2 Staking






Locked Staking

DeFi Staking



Risk Warning

Binance strives to offer its users only the best DeFi Mining projects. However, Binance only acts as a platform to showcase projects and provide users with related services, such as accessing funds on behalf of the user and distributing earnings, etc. Binance does not assume liability for any losses incurred due to project on-chain contract security issues.

Token	Est. APY	Duration (days) ⓘ	Minimum Locked Amount	
<div><div>continue</div><div> BNB</div></div>	8.49%	Flexible Lock	10BNB	<div>Stake Now</div>
<div><div>available</div><div> BUSD</div></div>	25.12%	Flexible Lock	0.00001BUSD	<div><div>Sold out</div><div>Check</div></div>
<div><div>ready</div><div> XVS</div></div>	9.10%	Flexible Lock	0.00001XVS	<div>Stake Now</div>
<div><div>available</div><div> USDC</div></div>	34.79%	Flexible Lock	0.00001USDC	<div><div>Sold out</div><div>Check</div></div>
<div><div>ready</div><div> HARD</div></div>	10.00%	Flexible Lock	0.00001HARD	<div>Stake Now</div>

Hình 2.4: Sàn Binance với cơ chế DeFi Staking

- Ưu điểm:
 - Người dùng trực tiếp tiếp cận với các dự án DeFi với tư cách là nhà cung cấp thanh khoản.
 - Lợi nhuận cao do không phải chịu nhiều khoản phí.
 - Không chịu rủi ro mất giá.
- Nhược điểm
 - Đi kèm với lợi nhuận cao là rủi ro cao từ việc các dự án lừa đảo. Các sàn chỉ có nhiệm vụ cầu nối trung gian nên không chịu trách nhiệm.

3 Bridge Blockchain

3.1 Hoàn cảnh ra đời

- Các Public BC (Ethereum, Bitcoin,...) cho phép tất cả dữ liệu trên chuỗi đều minh bạch, cơ sở hạ tầng của blockchain phục vụ một hệ sinh thái khép kín.
- Nhưng bản chất của các blockchain đang cản trở tiến trình xây dựng các ứng dụng DeFi, khóa người dùng DeFi vào một mạng duy nhất.
- **Bài toán:** các blockchain độc lập phải “giao tiếp” với một blockchain khác.

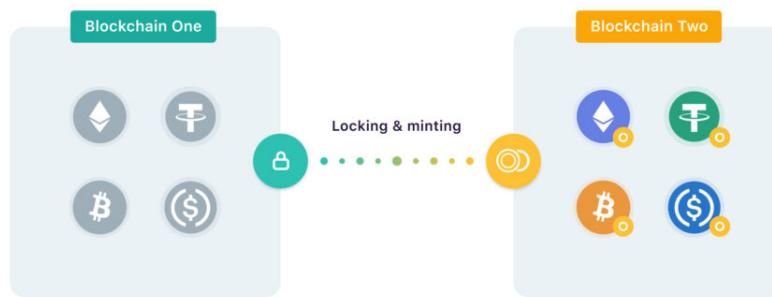
⇒ Sự ra đời của Bridge.

3.2 Bridge BC là gì?

- Các cầu nối chuỗi khối cho phép khả năng tương tác giữa các mạng rất lớn khác nhau (chẳng hạn như Bitcoin và Ethereum) hoặc giữa một chuỗi khối mẹ và chuỗi con của nó, được gọi là sidechain, cho dù chúng hoạt động theo các quy tắc đồng thuận khác nhau.
- Khả năng tương tác này có thể bao gồm việc chuyển token, dữ liệu hay thậm chí cả các hợp đồng thông minh giữa các nền tảng độc lập, cho phép người dùng:
 - Deposit các tài sản kỹ thuật số được lưu trữ trên một chuỗi khối tới các dapp trên một chuỗi khối khác
 - Thực hiện các giao dịch nhanh chóng, chi phí thấp với các token trên các chuỗi có khả năng mở rộng thấp hơn.
 - Thực thi Dapp đa nền tảng.
- Tuy nhiên, do bản chất khác nhau nên một số bridge được xây dựng theo hướng tập trung (Polkadot, Cosmos, Avalanche,...), hoặc phi tập trung (RenVM, xDAI,...).
- Báo cáo sẽ đi theo **hướng phi tập trung**.

3.3 Cơ chế hoạt động

- Khi người dùng chuyển tài sản từ BC này sang BC khác bằng cách sử dụng một bridge phi tập trung, những tài sản đó không được di dời hoặc “gửi đi” ở bất kỳ đâu theo nghĩa đen.
- Cơ chế:
 1. Các tài sản bị khóa hoặc “đóng băng” trên blockchain ban đầu bằng cách sử dụng hợp đồng thông minh.
 2. Tiếp đó, các token mới với số lượng tương đương được tạo trên blockchain nhận.
 3. Khi người dùng muốn đổi về tài sản ở BC ban đầu, các token tương đương sẽ bị hủy và sau đó tài sản ban đầu sẽ được mở khóa.



3.4 Minh họa: Ren Bridge

- Là cầu nối blockchain phi tập trung. Máy ảo Ren (RenVM) được hỗ trợ bởi khá nhiều mạng phi tập trung lớn (ví dụ Ethereum,...).
- Bất kỳ ai cũng có thể sử dụng.
- Cho phép tạo chữ ký số để khóa tài sản kỹ thuật số trên một chuỗi khối và người dùng có thể tin cậy sử dụng tài sản kỹ thuật số tương đương trên chuỗi khác.

3 Bridge Blockchain

The screenshot shows a mobile application interface for the RenVM Bridge. At the top, there are two tabs: "Minting" (selected) and "Release". The main display shows "10 BTC" in large text, with a red underline, and its equivalent value, "= \$561,973.75". Below this, there are two dropdown menus: "Send" set to "BTC" with a Bitcoin icon, and "Destination" set to "Ethereum" with an Ethereum icon. At the bottom, there is a "Receiving:" section showing a Bitcoin icon and the amount "9.974 renBTC". A large blue button labeled "Next" is at the very bottom.

- Cách tiếp cận này cho phép người dùng “di chuyển” bất kỳ tài sản kỹ thuật số nào (có khả năng) từ blockchain này sang blockchain khác mà không cần sự hỗ trợ của bên thứ ba. RenVM hiện cho phép sử dụng token BTC, BCH, ZEC và DOGE trên Ethereum và Binance Smart Chain.

3.5 Lợi ích của Bridge

- Tài sản thế chấp cross-chain: cho phép người dùng chuyển tài sản kỹ thuật số từ một chuỗi khối có giá trị đáng kể nhưng ít Dapp của riêng nó (như Bitcoin) sang một chuỗi có hệ sinh thái DeFi phát triển, như Ethereum.
- Khả năng mở rộng: khối lượng giao dịch cao cho phép khả năng mở rộng lớn hơn, mà không buộc các nhà phát triển và người dùng phải từ bỏ các chuỗi ban đầu.
- Hiệu quả: có thể tạo và nhận các giao dịch vi mô một cách nhanh chóng và không phải trả phí giao dịch cao, cho phép trải nghiệm chơi game (thông qua cơ chế

3 Bridge Blockchain

chuyển token gốc vào game) và các sàn thương mại điện tử tốt hơn.

4 Swapping

- Do mỗi sàn giao dịch có một cơ chế swap khác nhau nên báo cáo sẽ nghiên cứu cụ thể sàn uniswap.
- Uniswap là một giao thức thanh khoản tự động và là một trong những sàn giao dịch phi tập trung (DEX) phổ biến nhất hiện nay.
- Các user có thể trở thành những Liquidity Provider (nhà cung cấp thanh khoản- viết tắt là LP) cho một pool trên Uniswap bằng cách gửi một giá trị tương đương của token để đổi lấy các token khác trong pool.
- Uniswap có những tính năng:
 - Swap: Hay gọi là hoán đổi, tính năng này cho phép hoán đổi Ethereum và các token ERC-20 khác nhau.
 - Pool: Tính năng này của Uniswap giúp người dùng kiếm tiền thông qua việc trở thành LP. Thực hiện bằng cách gửi token vào một smart contract và đổi lại bạn sẽ nhận được token ở pool đó.

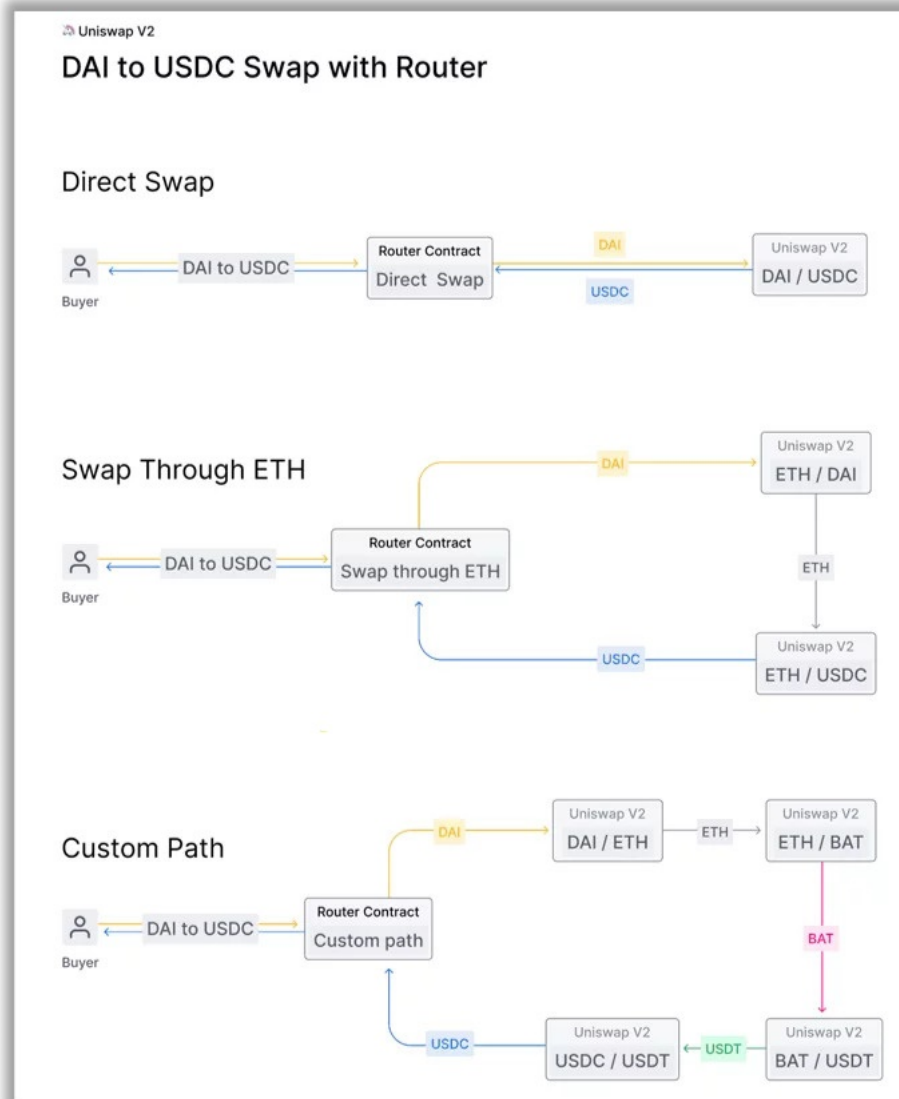


Hình 4.1: Uniswap

Uniswap V2 cung cấp cho người dùng cuối 3 tùy chọn khác nhau để swap token của họ, sử dụng “Router Contract”. Dưới đây là ba khả năng swap:

4 Swapping

- Một là swap trực tiếp giữa hai token ERC20. Ví dụ: hai stablecoin như DAI/USDC.
- Swap truyền thống thông qua ETH, nơi bạn phải trả phí 2 lần.
- Swap Custom path trong đó xây dựng một path phức tạp hơn như DAI/ETH, ETH/BAT, BAT/USDT và USDT/USDC để swap DAI của bạn sang USDC. Thông thường, điều này cung cấp cho các nhà giao dịch những cơ hội chênh lệch giá.



Hình 4.2: Uniswap Swap

Ưu điểm

- Phí giao dịch thấp: Uniswap chỉ tính phí cố định là 0.3% cho mỗi giao dịch, rẻ hơn nhiều so với hầu hết các sàn giao dịch phi tập trung.
- Không yêu cầu KYC: giúp giao dịch trên sàn nhanh hơn, và thông tin sẽ không rơi và tay kẻ xấu nếu sàn bị tấn công.
- Tự quản lý tài sản: toàn quyền quản lý tiền của mình, tránh khỏi những rủi ro liên quan đến sàn giao dịch phi tập trung chẳng hạn sàn phá sản hoặc bị hack.
- Cơ hội tiếp cận với đồng coin/token mới: Một việc bạn hay gặp phải ở các sàn giao dịch tập trung là: Các dự án tiền điện tử nào đó sẽ phải trải qua quá trình kiểm duyệt với sàn coin/token được niêm yết. Trên Uniswap, người dùng có thể nhận được những token mới này trước tiên. Và với những biến động mạnh mẽ về giá token, đặc biệt là khi chúng ra mắt lần đầu tiên.

Nhược điểm

- Smart contract giả mạo: vấn đề lớn nhất của Uniswap là bất kỳ ai cũng có thể tạo token ERC20 và thêm nó vào Uniswap. Ngay sau khi cung cấp thanh khoản lớn, người đó có thể rút thanh khoản của pool, khiến những người dùng khác bị thua lỗ. Vì vậy có những người đã lợi dụng việc này lên Uniswap với mục đích lừa mọi người gửi tiền của họ cho những tên này để đổi lấy các đồng tiền scam.
- Giao dịch không thành công: giao dịch sẽ không thành công hoàn toàn 100% trên Uniswap, các giao dịch vẫn có nguy cơ thất bại: vượt giá, trả ít fee gas,...