ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

Môn học : **An Toàn Kiến Trúc Hệ Thống**

BÁO CÁO CUỐI KỲ

Đề tài: DeXTT - Deterministic Cross-Blockchain Token Transfers

Lớp : **NT133.N21.ATCL**

Giảng viên hướng dẫn : **Trần Tuấn Dũng**

Nhóm 11

Nguyễn Mạnh Cường 20520421

Nguyễn Thái Dương 20520463

Thành phố Hồ Chí Minh
Ngày 09 tháng 06 năm 2023

MỤC LỤC

Phần 1: BÁO CÁO BÀI BÁO

I. Tổng quan (Abtract)

- Công nghệ blockchain hiện nay gặp phải một số giới hạn trong việc chuyển đổi dữ liệu và vận chuyển tài sản giữa các blockchain khác nhau. Điều đó làm hạn chế sự phát triển và khả năng ứng dụng của blockchain vào những lĩnh vực kinh tế, xã hội khác nhau.
- Tác giả đề xuất một giao thức mang tên DeXTT, giao thức chuyển đổi các token giữa những blockchain khác nhau. Với DeXTT, giao thức có thể hỗ trợ việc đồng thời chuyển đổi token bất kể số lượng blockchain, một cách phi tập trung.
- Phương pháp triển khai bởi ngôn ngữ Solidity và được đánh giá thông qua khả năng mở rộng các nodes, chi phí chuyển đổi.

II. Giới thiệu (Introduction)

- Công nghệ blockchain **[1]** trở thành một hướng tiếp cập hấp dẫn trong những nghiên cứu học thuật, cũng như các triển khai thực tế trong lĩnh vực tiền điện tử **[2]** (cryptocurrency). Sau khi Bitcoin **[3]** chứng minh được khả năng thực hiện lưu trữ phi tập trung, việc đầu tư vào nghiên cứu, phát triển liên quan đến blockchain và tiền điện tử đã tăng đáng kể. Công nghệ blockchain có thể đưa ra những cải tiến bằng cách thêm các lớp **[4]** (layers) mới lên các phiên bản blockchain hiện có, cải tiến Bitcoin hoặc tạo ra các blockchain hoàn toàn mới với các khái niệm mới, như hợp đồng thông minh **[5]** (smart contract).
- Mức đầu tư vào blockchain là biểu hiện cho tầm ảnh hưởng về công nghệ và khả năng ứng dụng rộng rãi trên nhiều lĩnh vực của blockchain. Mặc dù vậy, nó vẫn tồn tại những vấn đề về cấu trúc trong lĩnh vực blockchain. Những nghiên cứu phát triển cho đến nay chỉ tập trung vào việc tạo ra các blockchain và tiền tệ mới hoặc thay đổi các blockchain phổ biến như Bitcoin. Ngoài ra, có nhiều nghiên cứu về các trường hợp ứng dụng tiềm năng của blockchain trong các lĩnh vực kinh tế, xã hội, chính trị và kỹ thuật. Tuy nhiên, cách mà các blockchain có thể tương tác với nhau vẫn chưa được khám phá rộng rãi.
- Sự gia tăng không ngừng về số lượng các công nghệ blockchain độc lập, không kết nối gây ra sự phân mảnh đáng kể trong lĩnh vực nghiên cứu và phát triển, đặt ra thách thức cho cả người dùng và nhà phát triển công nghệ blockchain.
  - Một mặt, người dùng phải chọn loại tiền tệ và blockchain để sử dụng.
    - Chọn các blockchain mới lạ và sáng tạo cho phép người dùng tận dụng các tính năng mới và sử dụng công nghệ tiên tiến. Tuy nhiên, người dùng cũng có nguy cơ mất tiền nếu tính bảo mật của blockchain mới lạ bị xâm phạm, có thể dẫn đến mất toàn bộ tài sản.
    - Chọn các blockchain phổ biến và đã được phát triển lâu dài giảm thiểu rủi ro, nhưng lại không có các tính năng mới.
  - Mặt khác, khi thiết kế ứng dụng dựa trên blockchain phi tập trung, nhà phát triển (developers) phải quyết định dựa trên blockchain nào. Điều này có thể làm trở ngại đáng kể đối với nghiên cứu và tiến bộ kỹ thuật, vì các công nghệ bởi những cá nhân tạo ra các giải pháp cô lập và khả năng tương tác giữa các blockchain chủ yếu không được đảm bảo.

- Với mục tiêu cố gắng cung cấp các phương thức để tương tác giữa các blockchain, bao gồm truyền dữ liệu giữa các blockchain, tương tác hợp đồng thông minh giữa các blockchain hoặc chuyển đổi tiền tệ giữa các blockchain. Như một bước đầu để khả thi hóa khả năng tương tác giữa các blockchain như vậy, tác giả đề xuất một giao thức cho việc chuyển đổi token (mã thông báo) giữa các blockchain.
  - Trong đó token được chuyển không bị khóa trong một blockchain cụ thể, thay vào đó, nó có thể được ứng dụng trên bất kỳ số lượng blockchain nào, và các giao dịch của nó được đồng bộ tự động trên các blockchain bởi hệ thống theo một cách phi tập trung.
  - Giải pháp cũng ngăn chặn việc double spending **[6]** (tiêu tiền kép), có khả năng chống lại các vấn đề chứng minh giữa các blockchain (XPP **[7]** – một nghiên cứu trước đó của tác giả về các vấn đề trong tương tác giữa các blockchain), và không cần bên đối chiếu bên ngoài hoặc các phương tiện giao tiếp giữa các blockchain **[8]** khác để hoạt động.
  - Tác giả cung cấp một phiên bản tham khảo cho việc triển khai sử dụng ngôn ngữ Solidity **[9]** và đánh giá hiệu suất của nó về thời gian và chi phí thực hiện chuyển đổi.
- Tóm lại, tổng quan về các đề xuất từ bài báo bao gồm:
  - Cách ứng dụng tính nhất quán cuối cùng **[10]** (eventual consistency) cho giao thức chuyển đổi token qua các blockchain, bao gồm các khái niệm về claim-first transactions **[11]** (giao dịch nhận trước) và deterministic witnesses **[12]** (nhân chứng xác định).
  - Deterministic Cross-Blockchain Token Transfers (DeXTT), giao thức được phát triển dựa trên các ứng dụng nói trên. Triển khai một phiên bản của giao thức bằng ngôn ngữ Solidity và đánh giá.

III. Kiến thức nền tảng (Background)

- Phần này trình bày một số quy ước, giả định và các khái niệm được ứng dụng trong phương pháp chính.
- Về các tài sản trong blockchain, ngoài tiền tệ (ví dụ Ether thuộc Ethereum blockchain, Bitcoin thuộc Bitcoin blockchain,…) block chain có rất nhiều loại tài sản khác, thường được gọi là Token **[13]**. Loại token được sử dụng trong bài báo, tác giả sử dụng loại token có thể tồn tại được trên nhiều các blockchain gọi là pan-blockchain token (PBT) **[14]**. PBT có thể được chuyển đổi bởi giao thức DeXTT.
- Các blockchain tham gia vào giao thức được giả định là một hệ sinh thái blockchain (ecosystem of blockchains). Tác giả giả định rằng tất cả các ví tiền **[15]** (W), đại diện cho một cá nhân hay một bên sử dụng blockchain (bao gồm một cặp khóa công khai và riêng tư), khi tham gia vào hệ sinh thái sẽ quan tâm đến tất cả các blockchain trong đó. Tức là W sẽ có số dư PBT được đồng bộ trên tất cả các blockchain trong hệ sinh thái và cũng sẽ đồng bộ khi thực hiện giao dịch chuyển đổi giữa các W với nhau.

A. Tính nhất quán của số dư trên các blockchain

- Như đã đề cập ở **II** tác giả ứng dụng tính nhất quán cuối cùng cho giao thức chuyển đổi của mình. Vì một số lý do về hạn chế ở thực tế trong việc xác thực giữa các blockchain khác nhau, số dư khi giao dịch chuyển đổi giữa các W sẽ không được đồng bộ trên toàn

bộ hệ sinh thái một cách tức thời **[16]** (tính nhất quán nghiêm ngặt - strict consistency), mà sẽ chấp nhận một khoản thời gian đồng bộ cho phép để đạt được tính nhất quán cuối cùng về số dư ở tất cả các blockchain.

- Để có thể thực hiện điều đó tác giả áp dụng khái niệm claim-first transactions. Tức là khi giao dịch, sẽ có một khoảng thời gian số dư trên W của bên gửi và bên nhận chưa được xử lý (đồng bộ) trên một vài blockchain, và ở các blockchain đã được đồng bộ, bên nhận đã nhận được token trong ví tiền.
- Đồng thời, quá trình đồng bộ giao dịch trên tất cả các blockchain trong hệ sinh thái sẽ được thực hiện bởi một khái niệm khác, gọi là các nhân chứng (witnesses). Những nhân chứng này chính là những ví tiền (W) được giao thức chọn ra để giám sát, quảng bá cho quá trình đồng bộ các giao dịch trên toàn hệ sinh thái. Sau đó, những nhân chứng sẽ nhận được tiền thù lao của mình bằng một phần số PBT trong giao dịch.
  - Việc lựa chọn nhân chứng không thể thực hiện bằng quy tắc first-come-first-serve, vì các blockchain khác nhau có thể chọn ra các nhân chứng khác nhau, dẫn đến việc trao tiền thì lao không đồng bộ trong hệ sinh thái.
  - Vì thế, một khái niệm gọi lại cuộc thi nhân chứng (witness contest) được áp dụng để chọn ra duy nhất một nhân chứng nhận phần thưởng (tiền thù lao). Với phương thức này, các blockchain khác nhau trong hệ sinh thái sẽ luôn chọn ra một nhân chứng giống nhau cho một giao dịch nhất định, đảm bảo được tính đồng bộ số dư đối với các W của các nhân chứng. Trong cuộc thi nhân chứng, phần thưởng (tiền thì lao) mang ý nghĩ như một động lực thúc đẩy các ví tiền tham gia (cuộc thi) hỗ trợ quá trình đồng bộ giao dịch của giao thức.

B. Chữ ký số và hàm băm

- Trong nghiên cứu và triển khai của bài báo, tác giả áp dụng thuật toán ECDSA **[17]** (bởi Ethereum) cho các chữ ký số.
- Thuật toán Keccak256 bởi Ethereum và SHA-256 bởi Bitcoin **[18]** được sử dụng cho các hàm băm (hash) và được phân bố đồng đều.

C. Quy ước và kỳ hiệu

- Phần này trình bày một số quy ước và ký hiệu được sử dụng trong **IV**.
- Như đã nhắc đến ở trên, ký hiện W đại diện cho các ví tiền, cụ thể hơn:
  - W_s đại diện cho ví tiền của bên gửi.
  - W_d đại diện cho ví tiền của bên nhận.
  - W_w đại diện cho ví tiền của nhân chứng được chọn.
  - Một số ký hiệu W_u, W_v đại diện cho các thí sinh khác trong cuộc thi nhân chứng.
- Ký hiệu C đại diện cho các blockchain (trong bài báo chỉ giả định 3 blockchain được đề cập là C_a, C_b, C_c). Ký hiệu t đại diện cho thời gian. Ký hiệu x đại diện cho số PBT được giao dịch.
- Ký hiệu trains đại diện cho một giao dịch (transaction) nhỏ trong giao dịch chuyển đổi DeXTT lớn. Bao gồm các trans: CLAIM, CONTENT, FINALIZE, VETO, FINALIZE-VETO.

- Ngoài ra còn một số ký hiệu cho chữ ký số của các W sẽ được đề cập sau ở **IV.**

IV. Phương pháp (DeXTT)

- Để mô tả từng bước của giao thức DeXTT đã đề xuất, tác giả giả định một trường hợp cụ thể cho một giao dịch. Cụ thể, giao dịch giữa 2 ví tiền (W) thực hiện trên hệ sinh thái gồm 3 blockchain (C), số PBT giao dịch là 20 PBT, trong đó 1 PBT lấy làm phần thưởng cho nhân chứng. Về cuộc thi nhân chứng, sẽ có sự tham gia của 3 W. **Bảng 1** thể hiện trạng thái trước khi bắt đầu quá trình chuyển đổi (t=0).

Blockchain $\mathcal{C}_a$		Blockchain $\mathcal{C}_b$		Blockchain $\mathcal{C}_c$	
$\mathcal{W}_s$ balance:	80	$\mathcal{W}_s$ balance:	80	$\mathcal{W}_s$ balance:	80
$\mathcal{W}_d$ balance:	0	$\mathcal{W}_d$ balance:	0	$\mathcal{W}_d$ balance:	0
$\mathcal{W}_w$ balance:	0	$\mathcal{W}_w$ balance:	0	$\mathcal{W}_w$ balance:	0

Bảng 1: *Trạng thái t=0 ($t<t_0$)*

A. Khởi tạo giao dịch chuyển đổi

- Ví gửi (W_s) đang có 80 PBT, dự định sẽ gửi 20 PBT (trong đó 1 BPT là phần thưởng nhân chứng) cho ví nhận (W_d). Ví gửi dùng chữ ký số của mình (α) để ký vào dữ liệu dự định cho giao dịch chuyển đổi của mình. Đồng thời, khoảng thời gian thực hiện giao dịch cũng được xác định ($[t_0, t_1]$) và bao gồm trong dữ liệu trên (giả định thời gian từ t_0=1 đến t_1=61).

$$\left[\mathcal{W}_s \xrightarrow{x} \mathcal{W}_d, t_0, t_1 \right]_\alpha$$

- Dữ liệu trên sau đó được truyền đến ví nhận (có thể được truyền qua bất kì kênh nào, bất kể vấn đề bảo mật, vì cuối cùng cũng sẽ công khai trên toàn hệ sinh thái).
- Ví nhận tiếp nhận dữ liệu trên và tiếp tục sử dụng chữ kỳ số của mình (β) để ký thêm vào. Mục đích là có được sự xác nhận của hai bên để làm bằng chứng giao dịch trên tất cả các blockchain. Sau bước này, dữ liệu trên đã hoàn thiện để được gọi là một Proof of Intent (PoI) **[28]**.

$$\left[\mathcal{W}_s \xrightarrow{x} \mathcal{W}_d, t_0, t_1, \alpha \right]_\beta$$

- Sau đó, ví nhận đăng PoI trên với trans CLAIM, có thể và chỉ cần đăng ở bất kỳ một trong những blockchain trong hệ sinh thái (giả định là C_a). Trans CLAIM thể hiện rằng việc ví nhận sẽ nhận được số tiền giao dịch trong tương lai (khi kết thúc giao dịch, $t>t_1$).

$$\mathcal{W}_d : \text{CLAIM} \left[\mathcal{W}_s \xrightarrow{x} \mathcal{W}_d,\ t_0,\ t_1,\ \alpha \right]_\beta$$

$$\mathcal{W}_d : \text{CLAIM} \left[\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d,\ 1,\ 61,\ \texttt{0xAA} \right]_{\texttt{0xBB}}$$

- **Bảng 2** mô tả trạng thái sau khi ví nhận đăng PoI (t=1). Chỉ số 0xAA giả định cho chữ ký số của ví gửi (α), và cũng đại diện cho PoI khi được đăng trên một blockchain (giải thích ở **IV-D**).

Blockchain $\mathcal{C}_a$	Blockchain $\mathcal{C}_b$	Blockchain $\mathcal{C}_c$
$\mathcal{W}_s$ balance: 80 $\mathcal{W}_d$ balance: 0 $\mathcal{W}_w$ balance: 0 PoI 0xAA: $\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d$ $t_1 = 61$	$\mathcal{W}_s$ balance: 80 $\mathcal{W}_d$ balance: 0 $\mathcal{W}_w$ balance: 0	$\mathcal{W}_s$ balance: 80 $\mathcal{W}_d$ balance: 0 $\mathcal{W}_w$ balance: 0

Bảng 2: *Trạng thái t=1 (t_0<t<t_1)*

- Điều kiện để trans CLAIM được xem là hợp lệ:
  - PoI phải hợp lệ, tức là chữ ký số của ví gửi và ví nhận (α và β) phải chính xác.
  - Số dư của ví gửi phải đủ để thực hiện giao dịch, tức là phải lớn hơn hoặc bằng số token giao dịch. ($W_s \geq$ x (20 PBT)).
  - Thời gian khi đăng CLAIM phải trước thời gian giao dịch kết thúc (t < t_1 (61)).
  - Không tồn tại cùng lúc 2 trans CLAIM có chung một chữ kỳ số đại diện, tức là không thể có hai giao dịch cùng đang trong quá trình thực hiện với chung một ví gửi. Mục đính là tránh giao dịch kép (giải thích ở **IV-D**).

B. Cuộc thi nhân chứng

- Ở thời điểm hiện tại, PoI cho giao dịch chỉ mới được đăng trên một blockchain (C_a) và nó cần được đăng trên tất cả các blockchain trong hệ sinh thái cho mục đích đồng bộ của giao dịch. Vì thế, cuộc thi nhân chứng được triển khai. Tất cả các bên giám sát (ví tiền) có thể thấy được PoI với trans CLAIM đã đăng trước đó, đều có thể tham gia vào cuộc thi để trở thành nhân chứng được chọn.
- Để có thể là thí sinh, tất cả những ví tiền muốn tham gia phải đăng các trans, gọi là CONTEST trên tất cả các blockchain trong hệ sinh thái. Mục đích là để thí sinh đăng PoI trên tất cả các blockchain nhằm đồng bộ cho giao dịch chuyển đổi, đồng thời ghi danh

mình vào việc lựa chọn nhân chứng ở tất cả các blockchain. Quá trình này sẽ diễn ra trong phần còn lại của khoảng thời gian giao dịch chuyển đổi được xác định trước đó, và được xem là quá trình của cuộc thi nhân chứng.

$$\mathcal{W}_o : \text{CONTEST} \left[\mathcal{W}_s \xrightarrow{x} \mathcal{W}_d,\ t_0,\ t_1,\ \alpha,\ \beta \right]_{\omega}$$

- Nhìn chung, CONTEST có các dữ liệu khá giống với CLAIM (dữ liệu của PoI), vì vậy, điều kiện hợp lệ của CONTEST cũng sẽ tương tự với CLAIM. Ngoài ra, CONTEST sẽ được ký bằng chữ ký số của thí sinh đăng trans này (ký hiệu ω đại diện cho chữ ký số của thí sinh). Sau đây là các thực tế cho trans CONTEST của 3 bên giám sát giả định tham gia vào cuộc thi.

$$\mathcal{W}_u : \text{CONTEST} \left[\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d,\ 1,\ 61,\ \texttt{0xAA},\ \texttt{0xBB} \right]_{\texttt{0xC2}}$$

$$\mathcal{W}_v : \text{CONTEST} \left[\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d,\ 1,\ 61,\ \texttt{0xAA},\ \texttt{0xBB} \right]_{\texttt{0xC3}}$$

$$\mathcal{W}_w : \text{CONTEST} \left[\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d,\ 1,\ 61,\ \texttt{0xAA},\ \texttt{0xBB} \right]_{\texttt{0xC1}}$$

- **Bảng 3** thể hiện trạng thái sau khi tất cả các thí sinh của cuộc thi nhân chứng đã đăng trans CONTEST trên tất cả các blockchain. Hiện tại dữ liệu PoI về giao dịch đã tồn tại trên cả hệ sinh thái, mỗi PoI trên từng blockchain sẽ kèm theo thông tin về chữ ký số của tất cả các thi sinh tham gia.

Blockchain $\mathcal{C}_a$	Blockchain $\mathcal{C}_b$	Blockchain $\mathcal{C}_c$
$\mathcal{W}_s$ balance: 80 $\mathcal{W}_d$ balance: 0 $\mathcal{W}_w$ balance: 0 PoI 0xAA: $\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d$ $t_1 = 61$ Contestants: $\mathcal{W}_u$ (0xC2) $\mathcal{W}_v$ (0xC3) $\mathcal{W}_w$ (0xC1)	$\mathcal{W}_s$ balance: 80 $\mathcal{W}_d$ balance: 0 $\mathcal{W}_w$ balance: 0 PoI 0xAA: $\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d$ $t_1 = 61$ Contestants: $\mathcal{W}_u$ (0xC2) $\mathcal{W}_v$ (0xC3) $\mathcal{W}_w$ (0xC1)	$\mathcal{W}_s$ balance: 80 $\mathcal{W}_d$ balance: 0 $\mathcal{W}_w$ balance: 0 PoI 0xAA: $\mathcal{W}_s \xrightarrow{20} \mathcal{W}_d$ $t_1 = 61$ Contestants: $\mathcal{W}_u$ (0xC2) $\mathcal{W}_v$ (0xC3) $\mathcal{W}_w$ (0xC1)

Bảng 3: *Trạng thái t=? (t_0<t<t_1)*

C. Lựa chọn nhân chứng xác định

- Khi thời gian của giao dịch kết thúc (t_1<t), tức là cuộc thi nhân chứng kết thúc và quá trình đồng bộ giao dịch trên toàn bộ hệ sinh thái blockchain đã được thực hiện, cần tim ra thí sinh thắng cuộc được chọn làm nhân chứng và trao phần thưởng.
- Khi đó, trans FINALIZE được đăng trên tất cả các blockchain. Khác với 2 trans trước, FINALIZE có thể được đăng bởi nhiều cách khác nhau, có thể là ví nhận, một số bên khác hoặc áp dụng cơ chế tự động tính giờ phi tập trung nào đó. Ở trường hợp bài báo, tác giả giả định ví nhận sẽ đăng trans FINALIZE.

$$\text{FINALIZE}\left[\ \alpha\ \right]$$

- FINALIZE chỉ đơn giảm bao gồm chữ ký số đại diện cho PoI (α), vì nội dung dữ liệu của PoI đã được đồng bộ trên hệ sinh thái từ trước. Điều kiện hợp lệ của trans này là thực hiện sau khi kết thúc giao dịch (t_1<t). FINALIZE được đăng với mục đích là:
  - Thể hiện rằng cuộc thi nhân chứng đã kết thúc và chọn ra một nhân chứng xác định trên tất cả các blockchain (W_w) để trao phần thưởng (1 PBT).
  - Đồng thời, thể hiện giao dịch chuyển đổi DeXTT đã kết thúc, các số dư trên tất cả các ví tiền trong hệ sinh thái đã được đồng bộ.
- Nhân chứng thắng cuộc được lựa chọn dựa trên chữ ký số của chính nhân chứng đó, thí sinh đã tham gia và có chữ ký số với kích thước nhỏ nhất sẽ giành chiến thắng. Với việc tất cả các thí sinh đã đăng trans CONTEST trên tất cả các blockchain, việc chọn ra nhân chứng chiên thắng sẽ hoàn toàn giống nhau ở toàn hệ sinh thái. Hơn nữa, với việc lựa chọn dựa trên chữ ký số (được tạo bởi khóa bí mật và mã băm của PoI) không thể sửa đổi nội dung, việc gian lận để giành phần thắng chỉ có thể được thực hiện bằng cách tạo ra một số lượng lớn các ví tiền. Tuy nhiên, cách gian lận trên không khả thi, vì đánh đổi giữa chi phí cho việc tạo các ví tiền, tham gia cuộc thi và số phần thưởng nhận lại không tương thích (nhắc đến ở **V**).
- **Bảng 4** mô tả kết quả của giao dịch được tác giả giả định. Ví gửi bị trừ 20 PBT, ví nhận nhận được 19 PBT, vì 1 PBT được lấy làm phần thưởng được cộng vào ví của nhân chứng chiên thắng.

Blockchain $\mathcal{C}_a$		Blockchain $\mathcal{C}_b$		Blockchain $\mathcal{C}_c$	
$\mathcal{W}_s$ balance:	60	$\mathcal{W}_s$ balance:	60	$\mathcal{W}_s$ balance:	60
$\mathcal{W}_d$ balance:	19	$\mathcal{W}_d$ balance:	19	$\mathcal{W}_d$ balance:	19
$\mathcal{W}_w$ balance:	1	$\mathcal{W}_w$ balance:	1	$\mathcal{W}_w$ balance:	1

Bảng 4: *Trạng thái kết thúc giao dịch (t_1<t)*

D. Ngăn chặn giao dịch kép (double spending)

- Một số người dùng (ví tiền) độc hại có thể thực hiện 2 giao dịch với cùng một ví gửi, khác ví nhận và với khoảng thời gian giao dịch chồng chéo nhau (có khoảng thời gian được thực hiện đồng thời). Trường hợp này xảy ra vì DeXTT ứng dụng tính nhất quán cuối cùng. Điều đó là bất hợp pháp, làm rối loại số dư các ví tiền và gây ảnh hưởng đến toàn hệ thống blockchain.
- Để ngăn chặn giao dịch kép trên, phương pháp hỗ trợ trans VETO. VETO sẽ được đăng trên toàn hệ sinh thái bởi bất cứ bên nào phát hiện được sự chồng chéo giữa 2 PoI giao dịch đang được thực hiện. Ở đây, việc sử dụng chữ ký số của ví gửi làm đại diện cho một PoI như đề cập ở phần trên, là nhằm mục đích dễ phát hiện ra vi phạm. Với việc sẽ có thể có nhiều bên quan sát đăng VETO, trans sẽ được triển khai một cuộc thi tương tự như cuộc thi nhân chứng, gọi là cuộc thi phán quyết.

$$\mathcal{W}_w : \text{VETO} \left[\alpha, \mathcal{W}_s \xrightarrow{x'} \mathcal{W}_{d'}, t'_0, t'_1, \alpha' \right]_\omega$$

- Dữ liệu có trong VETO bao gồm chữ ký số đại diện cho PoI đã tồn tại trên blockchain hiện tại được đăng (α) và phần còn lại là toàn bộ dữ liệu của PoI đang được xem là chồng chéo. Điều kiện hợp lệ của VETO là 2 giao dịch đó có sự chồng chéo.
- Mục đích của cuộc thi phán quyết cũng tương tự như cuộc thi nhân chứng, đó là đăng thông tin rằng có giao dịch kép đang diễn ra và tiến hành ngăn chặn trên tất cả các blockchain trong hệ sinh thái. Sau đó, ở mỗi blockchain khi đã nhận được VETO sẽ thực hiện:
  - Dừng các PoI đang vi phạm, ngăn chặn FINALIZE của giao dịch đó diễn ra.
  - Xử phạt ví gửi bằng cách trừ toàn bộ số dư của nó (PBT = 0). Số PBT bị trừ sẽ được trích một phần làm phần thưởng cho người chiên thắng cuộc thi phán quyết (1 PBT), còn phần còn lại sẽ bị biến mất.
- Sau một khoảng thời gian được tính toán trước đó (tác giả đưa ra công thức, tuy nghiên thời gian này có thể được điều chỉnh tùy mô hình và không quan trọng để đề cập) cuộc thi phán quyết sẽ được kết thúc. Trans VETO-FINALIZE được đăng với mục đích tương tự như FINALIZE, ngoại trừ việc xác nhận giao dịch kết thúc.

$$\text{FINALIZE-VETO} \left[\alpha, \alpha' \right]$$

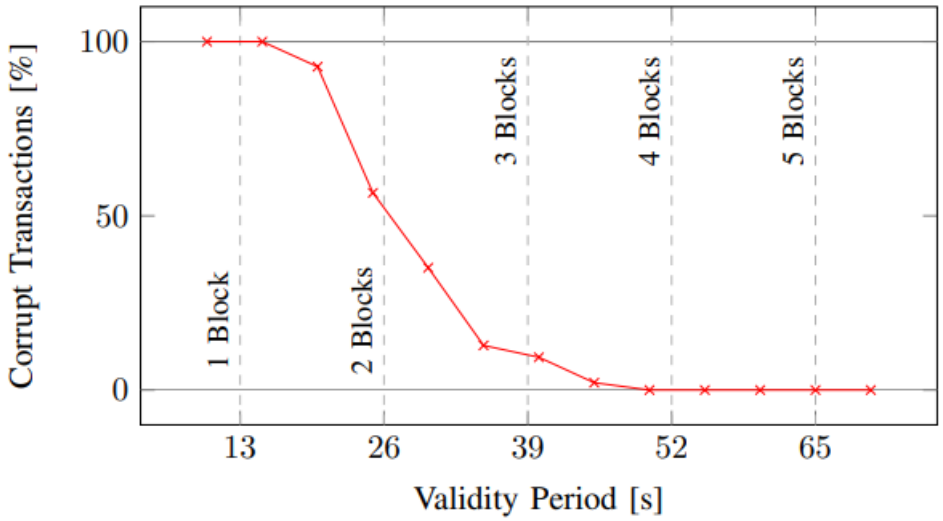
- Ở FINALIZE-VETO, sau khi thông tin về việc vi phạm của 2 PoI đã được đăng trong hệ sinh thái, 2 chữ ký số đại diện PoI sẽ là nội dung đơn giản cho trans. Cách chọn ra thí sinh chiến thắng như đã đề cập ở cuộc thi nhân chứng.

V. Đánh giá (Evaluation)

- Tác giả nhất mạnh rằng, các giả định cũng như những nền tảng được nhắc đến trong việc triển khai giao thức đề xuất chỉ là một phiên bản để thử nghiệm và đánh giá. DeXTT có thể ứng dụng được trên nhiều mô hình, ngôn ngữ hợp đồng thông minh và các thuật toán khác nhau. Đánh giá hiện tại là đủ để chứng minh chức năng tổng thể của giao thức DeXTT bằng cách sử dụng hợp đồng thông minh Solidity và khả năng ứng dụng các khái niệm.
- Để đánh giá phương pháp, tác giả nghiên cứu chức năng, hiệu suất và tác động chi phí trong một hệ sinh thái các blockchain với các bên thực hiện việc chuyển token lặp đi lặp lại. Sử dụng phiên bản tham chiếu bao gồm các hợp đồng thông minh Solidity, triển khai các hợp đồng thông minh này trên một số blockchain riêng tư (private) dựa trên Ethereum và sử dụng phần mềm thử nghiệm tương tác của khách hàng để thực hiện các giao dịch với tốc độ cho trước.
- Đảm bảo một hệ sinh thái các blockchain có thể tái sản xuất (reproducible) và đồng nhất bằng cách sử dụng ba nút geth **[21]** ở chế độ Proof of Authority **[22]** (PoA), tạo ra ba blockchain riêng tư. Tác giả chọn PoA để đạt được một nền tảng thử nghiệm và đánh giá tiết kiệm tài nguyên trong khi vẫn có thể thực hiện các thí nghiệm lặp đi lặp lại. Lưu ý rằng các thuật toán đồng thuận, tức là PoW **[23]**, Proof of Stake **[24]** (PoS) hoặc PoA, xác định hành vi của các nút blockchain lẫn nhau và duy trì tính nhất quán dữ liệu trong mạng lưới của một blockchain. Tuy nhiên, lớp hợp đồng thông minh là độc lập với thuật toán đồng thuận. Do đó, đánh giá của tác giả trên PoA có thể áp dụng trực tiếp cho các blockchain với bất kỳ thuật toán đồng thuận nào.
- Các nút geth được sử dụng trong các thí nghiệm có thể được cấu hình, ví dụ như về thời gian khối (block time) **[25]** và giới hạn Gas **[26]**. Tác giả quan sát hành vi của blockchain Ethereum thực tế (vào tháng 1 năm 2019) và cấu hình các nút của tác giả để tuân thủ hành vi này. Do đó, các nút của tác giả được cấu hình sử dụng thời gian khối trung bình là 13 giây và giới hạn Gas là 8 triệu Gas Ethereum, mô phỏng chuỗi Ethereum thực tế. Tác giả sử dụng các chuỗi riêng tư thay vì chuỗi chính Ethereum để cho phép các chỉ số lớn nhưng chi phí thấp của các thí nghiệm lặp lại một cách tự động mà không phụ thuộc vào các thành phần bên ngoài như các nút Ethereum.
- Tác giả triển khai 10 khách hàng liên tục và đồng thời khởi tạo các giao dịch trong hệ sinh thái blockchain. Con số này được chọn để cân bằng giữa các thí nghiệm khả thi, có thể lặp lại và điều kiện thực tế dự kiến. Mặc dù nhỏ hơn so với các đánh giá của các lớp hệ thống phân tán khác, lưu ý rằng tính mở rộng của các công nghệ blockchain là một vấn đề quan trọng nói chung và được coi là một trong những thách thức chính đối với các công nghệ blockchain hiện có. Tác giả tham khảo các tài liệu hiện có để nghiên cứu cách cải thiện tính mở rộng của các blockchain.
- Trong hệ sinh thái thử nghiệm của tác giả, mỗi khách hàng liên tục chuyển các số lượng ngẫu nhiên các PBT đến các ví ngẫu nhiên. Nếu một khách hàng sở hữu quá ít PBT cho một giao dịch, thì không có giao dịch nào được thực hiện với khách hàng đó cho đến khi có đủ PBT. Sau mỗi giao dịch thành công, khách hàng đợi một khoảng thời gian ngẫu

nhiên từ 15 giây đến 30 giây trước khi tiếp tục quá trình này vô thời hạn trong suốt thời gian thử nghiệm.

- Tác giả thực hiện hai loạt thí nghiệm:
  - Loạt thí nghiệm đầu tiên được sử dụng để đánh giá tính mở rộng của DeXTT và sự ảnh hưởng của khoảng thời gian thực hiện chuyển đổi ($[t_0, t_1]$). Bao gồm một loạt các thí nghiệm trong 30 phút, mỗi thí nghiệm sử dụng một khoảng thời gian chuyển đổi tăng lên dần.
  - Loạt thí nghiệm thứ hai bao gồm 20 thí nghiệm giống nhau, mỗi thí nghiệm có thời lượng 30 phút, được sử dụng để đo chi phí trung bình của một giao dịch DeXTT.
- Kết quả từ hai loạt thí nghiệm trên:
  - Loạt thí nghiệm 1:
    - **Hình 1** thể hiện kết quả của các thí nghiệm này. Sau khi trôi qua 52 giây, quan sát được không còn giao dịch thất bại. Cho thấy rằng việc sử dụng phiên bản triển khai và chờ đợi 4 khối (4 block time - 52 giây) là đủ để đảm bảo tính nhất quán. Trong khoảng từ 1 đến 3 khối (tương ứng với 13 giây và 39 giây), số lượng giao dịch thất bại giảm đi với tốc độ khác nhau.
    - Từ thí nghiệm này, tác giả kết luận rằng việc sử dụng một khoảng thời gian hợp lệ có độ dài ít nhất là 4 khối (52 giây) là đủ để duy trì tính nhất quán bằng cách sử dụng phiên bản triển khai của tác giả. Có thể cần thời gian bổ sung tùy thuộc điều kiện kết nối mạng.



Hình 1: *Kết quả từ loạt thí nghiệm 1 về ảnh hưởng của khoảng thời gian chuyển đổi bằng DeXTT*

  - Loạt thí nghiệm 2:
    - Dựa trên loạt thí nghiệm trước đó, tác giả chọn thời gian 65 giây (5 khối, lớn hơn giới hạn đã xác định là 52 giây) làm thời gian hiệu lực của chu kỳ xác thực PoI trong mỗi giao dịch. Ghi lại chi phí trung bình của mỗi giao dịch, **Bảng 5** cho thấy tổng quan về chi phí của các trans liên quan đến một giao dịch chuyển đổi DeXTT. Đối với mỗi trans, hiển thị chi phí trung bình (mean) và độ lệch chuẩn, cả hai đều được tính bằng nghìn Gas Ethereum (kGas) và USD. Tác giả giả định một giá Gas là 10 Gwei **[27]** (1

Ether = 10^9 Gwei = 10^{18} wei) và giá Ether là 115.71 USD. Các giá trị này được lấy từ chuỗi Ethereum trực tiếp vào tháng 1 năm 2019.

	Cost (kGas)		Cost (USD)	
Transaction	Mean	σ	Mean	σ
CLAIM	57.7	11.1	0.0668	0.0128
CONTEST	81.5	64.2	0.0943	0.0743
FINALIZE	45.5	0.1	0.0527	< 0.0001
VETO	131.3	91.9	0.1520	0.1063
FINALIZE-VETO	48.6	1.7	0.0563	0.0020

Bảng 5: *Kết quả từ loạt thí nghiệm 2 về chi phí chuyển đổi bằng DeXTT*

- Chi phí tính bằng kGas cho một giao dịch DeXTT như sau (với m là số blockchain trong hệ sinh thái):
  - Người nhận chịu chi phí cho một trans CLAIM (57.7 kGas) và m giao dịch FINALIZE (mỗi trans 45.5 kGas). Tổng cộng, ít nhất 103.2 kGas cho giao dịch.
  - Mỗi bên quan sát (nhân chứng) đăng các trans, chịu chi phí cho m trans CONTEST (mỗi trans 81.5 kGas).
  - Người gửi không chịu bất kỳ chi phí nào.
  - Giả định một hệ sinh thái blockchain gồm 10 chuỗi, tổng chi phí giao dịch cho người nhận là 0.59 USD. Mỗi bên quan sát dự kiến đăng các giao dịch chịu chi phí là 0.94 USD.
- Ngoài ra, từ những con số này cho phép tác giả suy luận về tác động kinh tế của một đơn vị tiền tệ điện tử sử dụng các giao dịch DeXTT. Những bên quan sát trả chi phí giao dịch 0.94 USD và có thể nhận được phần thưởng, hiện được giả định là 1 PBT.
  - Qua một số tính toán, kết luận được giá của PBT tính bằng USD chia cho số lượng bên quan sát phải cao hơn 0.94. Giả định n=10 bên quan sát, giá PBT phải lớn hơn 2.83 USD. Giả định n=100, giá PBT phải lớn hơn 14.15 USD. Với n=1000, giá PBT phải lớn hơn 94.32 USD.

VI. Công việc liên quan (Related work)

- Trong phần này, tác giả đề cập đến một số nghiên cứu liên quan trong đề tài nghiên cứu về các vấn đề tương tác giữa các blockchain khác nhau. Tác giả nên ra một số hạn chế của những nghiên cứu đó, cũng như dẫn chứng cho phương pháp của mình.
- Phương pháp đề xuất hiện tại được phát triển dựa trên một vài nghiên cứu trước đây của tác giả, bao gồm các nghiên cứu về token tồn tại được trên nhiều blockchain, cách triển khai cuộc thi nhân chứng và những vấn đề khi tương tác giữa các block chain (XPP).

VII. Tổng kết (Conclusion)

- Tác giả nhất mạnh lại những đề xuất về phương pháp của mình trong bài báo (tương tự **II**). Sau đó là một số tổng kết rút ra được từ triển khai của tác giả ở **V**.
- Trong công việc tương lai, tác giả sẽ giải quyết những hạn chế chính qua đánh giá hiện tại. Bằng cách triển khai DeXTT bằng các công nghệ bổ sung như OmniLayer hoặc CounterParty **[19]**, từ đó đánh giá hiệu suất của DeXTT trong một hệ sinh thái blockchain bao gồm các loại blockchain kết hợp. Hơn nữa, triển khai DeXTT trên các nền tảng hợp đồng thông minh nguyên bản khác như EOS.IO **[20]**. Ngoài ra, khám phá một số hướng tiếp cận khác cho cuộc thi veto.

Phần 2: THỰC NGHIỆM PHƯƠNG PHÁP

- Nhóm đã triển khai lại thực nghiệm của tác giả dựa trên mã nguồn mở tác giả đã công bố. (https://github.com/pantos-io/dextt-prototype)
- Triển khai thực hiện trên máy tính cá nhân của nhóm. Chi tiết ở phần thuyết trình báo cáo.

Phần 3: PHỤ LỤC

I. Phân công công việc

Thời gian	Đảm nhận	Nội dung
06/03/2023 – 02/04/2023	Tất cả các thành viên	Tự đọc bài báo
03/04/2023 – 09/04/2023	Cường	Làm slides báo cáo giữa kì
	Dương	Thuyết trình giữa kì
10/04/2023 – 07/05/2023	Tất cả các thành viên	Thời gian thực hiện các bài thực hành
08/05/2023 – 09/06/2023	Cường	Viết báo cáo, làm slides thuyết trình, thuyết trình cuối kì
	Dương	Triển khai demo bài báo, thuyết trình demo cuối kì

II. Chú thích và trích dẫn

[1] Blockchain là một công nghệ phân tán và đáng tin cậy được sử dụng để lưu trữ và quản lý thông tin mà không cần sự tín nhiệm vào một bên thứ ba trung gian. Nó được phát triển từ việc kết hợp một số công nghệ đã có từ trước đó như mật mã hóa, hệ thống ngang hàng (peer-to-peer network) và hợp đồng thông minh (smart contract).

Blockchain hoạt động dựa trên một mạng lưới phân tán của các máy tính, được gọi là các nút (nodes), trong đó mỗi nút chứa một bản sao của toàn bộ dữ liệu blockchain. Mỗi giao dịch mới được xác nhận và thêm vào blockchain thông qua quá trình xác minh của các

nút trong mạng lưới. Một khi một khối giao dịch mới được thêm vào blockchain, nó không thể bị thay đổi hoặc xóa bỏ mà chỉ có thể được mở rộng với các khối mới.

Đặc điểm chính của blockchain bao gồm tính toàn vẹn dữ liệu, tính minh bạch, tính phi tập trung và tính khả năng chống thay đổi. Tính toàn vẹn dữ liệu đảm bảo rằng mọi giao dịch và thông tin trong blockchain không thể bị sửa đổi một khi đã được xác nhận. Tính minh bạch cho phép mọi người trong mạng lưới xem xét và xác minh các giao dịch. Tính phi tập trung đảm bảo rằng không có một bên duy nhất nắm giữ quyền kiểm soát toàn bộ hệ thống, mà quyền lực được phân tán đến tất cả các nút trong mạng lưới. Tính khả năng chống thay đổi đảm bảo rằng một khi dữ liệu đã được xác nhận và thêm vào blockchain, nó không thể bị thay đổi một cách bất hợp pháp.

Blockchain đã tạo ra sự đột phá trong lĩnh vực tài chính và tiền điện tử với việc phát triển của tiền điện tử đầu tiên là Bitcoin. Ngoài ra, blockchain cũng có ứng dụng trong nhiều lĩnh vực khác như chuỗi cung ứng, quản lý tài sản kỹ thuật số, bỏ phiếu điện tử, quản lý dữ liệu y tế và nhiều hơn nữa.

[2] Cryptocurrency là một loại tiền điện tử hoạt động dựa trên công nghệ blockchain. Nó được tạo ra và quản lý bằng cách sử dụng mã hóa để bảo mật các giao dịch và kiểm soát việc tạo ra đơn vị tiền tương ứng.

Cryptocurrency không thuộc sở hữu của bất kỳ quốc gia hay tổ chức tài chính cụ thể nào. Thay vào đó, nó hoạt động trên một mạng lưới phân tán của các máy tính trên toàn thế giới. Các giao dịch được thực hiện trong cryptocurrency được ghi lại trong blockchain, một sổ cái công khai và bất biến.

Một trong những đặc điểm quan trọng của cryptocurrency là tính phi tập trung. Không có một cơ quan trung gian nào kiểm soát hay quản lý tiền điện tử này. Thay vào đó, quyền kiểm soát và xác minh các giao dịch nằm trong tay cộng đồng người dùng và các nút trong mạng lưới blockchain.

Bitcoin là cryptocurrency đầu tiên và phổ biến nhất. Tuy nhiên, còn rất nhiều loại cryptocurrency khác như Ethereum, Ripple, Litecoin, và nhiều loại khác. Mỗi loại cryptocurrency có đặc điểm riêng và có thể được sử dụng cho các mục đích khác nhau như thanh toán trực tuyến, đầu tư, hoặc xây dựng các ứng dụng phi tập trung (decentralized applications - DApps).

[3] Bitcoin là một loại tiền điện tử (cryptocurrency) đầu tiên và phổ biến nhất trên thế giới. Nó được tạo ra vào năm 2009 bởi một người hoặc một nhóm người giấu mình dưới bút danh Satoshi Nakamoto.

Bitcoin hoạt động trên mạng lưới phân tán blockchain. Blockchain của Bitcoin là một công nghệ lưu trữ dữ liệu phi tập trung, trong đó mọi giao dịch được xác minh và ghi lại

một cách công khai và bất biến. Điều này đảm bảo tính toàn vẹn và an ninh của các giao dịch Bitcoin.

Một số đặc điểm quan trọng của Bitcoin bao gồm:

Tính phi tập trung: Bitcoin không thuộc sở hữu của bất kỳ ngân hàng, tổ chức tài chính hay chính phủ nào. Quyền kiểm soát và xác minh giao dịch thuộc về cộng đồng người dùng Bitcoin.

Tính ẩn danh: Mỗi giao dịch Bitcoin được thực hiện trong blockchain được mã hóa và không liên kết trực tiếp với danh tính cá nhân. Người dùng có thể sử dụng địa chỉ Bitcoin để thực hiện giao dịch mà không cần tiết lộ thông tin cá nhân của mình.

Số lượng có hạn: Bitcoin được giới hạn số lượng tổng cung chỉ có thể tạo ra 21 triệu đồng Bitcoin. Điều này tạo ra sự khan hiếm và giúp bảo vệ giá trị của Bitcoin.

Thanh toán trực tiếp: Bitcoin cho phép người dùng thực hiện các giao dịch trực tiếp mà không cần thông qua bên thứ ba trung gian như ngân hàng. Điều này giúp giảm phí giao dịch và tăng tính tiện lợi.

Tính an toàn và bảo mật: Bitcoin sử dụng mã hóa mạnh mẽ để bảo vệ tính toàn vẹn và an ninh của các giao dịch. Người dùng có quyền kiểm soát và bảo vệ tiền của mình thông qua việc sở hữu một khoá riêng tư.

Bitcoin đã tạo ra sự thay đổi và tạo ra một nền tảng cho sự phát triển của tiền điện tử và blockchain. Nó đã trở thành một công nghệ và tài sản tài chính đáng chú ý, được sử dụng cho việc thanh toán, đầu tư và lưu trữ giá trị.

[4] Các layers trong cải tiến blockchain: Cải tiến blockchain đã đưa đến sự phát triển của nhiều lớp (layers) khác nhau để mở rộng và tăng cường khả năng của công nghệ blockchain. Dưới đây là một số layers quan trọng trong cải tiến blockchain:

Layer 1 - Blockchain Layer: Đây là lớp cơ bản của blockchain, nơi ghi lại các giao dịch và xác minh chúng. Layer 1 bao gồm các giao thức và quy tắc để xây dựng và quản lý blockchain. Ví dụ điển hình của Layer 1 là Bitcoin và Ethereum.

Layer 2 - Scaling Layer: Layer 2 tập trung vào việc mở rộng khả năng xử lý và tăng tốc độ giao dịch của blockchain. Nó giải quyết vấn đề về chi phí giao dịch và thời gian xác nhận trong blockchain cơ bản. Các giải pháp Layer 2 bao gồm Lightning Network (cho Bitcoin) và các mạng lưới Plasma và Raiden (cho Ethereum).

Layer 3 - Application Layer: Layer 3 là nơi xây dựng các ứng dụng và hệ thống dựa trên blockchain. Nó bao gồm các dApp (decentralized applications), smart contracts và các giao thức tương tác với blockchain. Ví dụ, Ethereum cung cấp một môi trường phát triển dApp và smart contracts thông qua ngôn ngữ lập trình Solidity.

Layer 4 - Governance Layer: Layer 4 tập trung vào vấn đề quản lý và điều hành hệ thống blockchain. Nó liên quan đến việc xác định các quy tắc, quyền lực và quy trình quyết định trong mạng lưới blockchain. Các giải pháp trong Layer 4 bao gồm DAO (Decentralized Autonomous Organization) và các cơ chế bỏ phiếu để định hình quyết định cộng đồng.

Layer 5 - Interoperability Layer: Layer 5 tập trung vào khả năng tương tác và giao tiếp giữa các blockchain khác nhau. Nó giúp kết nối và trao đổi thông tin, tài sản hoặc giao dịch giữa các blockchain khác nhau. Các giao thức như Polkadot, Cosmos và AION cung cấp giải pháp cho việc liên kết và tương tác giữa các blockchain.

Các lớp này cùng nhau tạo nên một hệ sinh thái blockchain phong phú và đa dạng, giúp mở rộng khả năng và ứng dụng của công nghệ blockchain trong nhiều lĩnh vực khác nhau.

[5] Smart contract (hợp đồng thông minh) là một khái niệm trong lĩnh vực blockchain và công nghệ tiền điện tử. Nó là một chương trình máy tính tự động hoạt động và thực thi các điều khoản và điều kiện của một hợp đồng.

Smart contract được xây dựng trên nền tảng blockchain, thường là trên các nền tảng như Ethereum. Nó được viết bằng các ngôn ngữ lập trình đặc biệt như Solidity, Vyper, hoặc Serpent.

Một smart contract chứa mã logic, các điều khoản và điều kiện mà tất cả các bên liên quan đồng ý tuân theo. Khi điều kiện đã được thỏa mãn, smart contract tự động thực hiện các hành động đã được định nghĩa trong mã, chẳng hạn như chuyển tiền, phân phối tài sản kỹ thuật số, ghi log dữ liệu, hoặc thực hiện một hành động cụ thể khác.

Đặc điểm quan trọng của smart contract là tính tự động, không thể thay đổi sau khi được triển khai, và không có nhiều nguy cơ xung đột hoặc gian lận. Các điều khoản và điều kiện trong smart contract được xác định trước và mã logic của nó được thực thi một cách đáng tin cậy dựa trên quy tắc của blockchain.

Smart contract có rất nhiều ứng dụng tiềm năng, bao gồm tài chính phi tập trung (Decentralized Finance - DeFi), chuỗi cung ứng, bảo hiểm, bỏ phiếu điện tử, quản lý tài sản kỹ thuật số, và nhiều lĩnh vực khác. Nó giúp tạo ra các giao dịch tự động, minh bạch, và tiết kiệm thời gian, đồng thời loại bỏ sự tín nhiệm vào bên thứ ba trong các giao dịch.

[6] Double spending (giao dịch kép) là một vấn đề tiềm ẩn trong các hệ thống tiền điện tử, bao gồm cả blockchain. Nó xảy ra khi một người dùng sử dụng một đơn vị tiền tệ (ví dụ: cryptocurrency) để thực hiện hai giao dịch tương tự nhau mà không bị hạn chế bởi tính toàn vẹn của hệ thống.

Trong hệ thống blockchain, double spending có nghĩa là một người dùng sử dụng một số tiền trong tài khoản của mình để thực hiện một giao dịch, sau đó nhanh chóng tạo ra một

giao dịch khác sử dụng cùng một số tiền đó, và cố gắng xác nhận cả hai giao dịch trước khi hệ thống kịp thực hiện quá trình xác nhận.

Để ngăn chặn double spending, hầu hết các hệ thống blockchain sử dụng một cơ chế gọi là xác nhận giao dịch. Trong quá trình xác nhận, các nút mạng trong blockchain xác minh tính hợp lệ của giao dịch và thêm nó vào khối mới của blockchain. Một khi giao dịch đã được xác nhận và được ghi vào blockchain, nó trở thành không thể thay đổi và ngăn chặn double spending.

Trong Bitcoin và các hệ thống blockchain khác, xác nhận giao dịch được thực hiện thông qua quá trình khai thác (mining). Các khối mới được tạo ra và giao dịch được xác nhận sau khi một số lượng đủ lớn các khối trước đó đã được kết nối với khối hiện tại. Việc xác nhận này làm tăng đáng kể độ tin cậy và tính toàn vẹn của giao dịch, giảm khả năng double spending.

Mặc dù các hệ thống blockchain đã áp dụng các biện pháp phòng ngừa double spending, nhưng vẫn có thể xảy ra trong các tình huống nhất định. Do đó, số lượng xác nhận cần thiết cho một giao dịch được coi là an toàn có thể khác nhau tùy thuộc vào từng blockchain cụ thể và mức độ đảm bảo an toàn mà người dùng mong muốn.

[7] XPP (cross-blockchain proof problem) là một khái niệm trong lĩnh vực blockchain và nó được đề cập đến trong nghiên cứu liên quan đến tích hợp và tương tác giữa các blockchain khác nhau.

Vấn đề XPP xuất hiện khi người dùng hoặc ứng dụng muốn chứng minh một sự kiện xảy ra trên một blockchain A cho một blockchain B mà không cần phụ thuộc vào bên thứ ba trung gian. Ví dụ, giả sử một người dùng muốn chứng minh rằng một giao dịch đã xảy ra thành công trên blockchain A và sau đó sử dụng thông tin này để thực hiện một hành động trên blockchain B.

Vấn đề quan trọng trong XPP là làm thế nào để chứng minh tính toàn vẹn và độ tin cậy của thông tin từ một blockchain đến một blockchain khác mà không cần tin tưởng vào bất kỳ bên trung gian nào. Điều này thường được gọi là bài toán chứng minh xuyên blockchain.

Các giải pháp cho vấn đề XPP có thể liên quan đến việc sử dụng công nghệ mã hóa và giao thức xác thực đáng tin cậy. Một số phương pháp phổ biến bao gồm sử dụng giao thức zero-knowledge proof, giao thức sử dụng tổ chức đa bên (multi-party computation), hoặc việc xây dựng một hệ thống giao tiếp đáng tin cậy giữa các blockchain.

Khái niệm trên được tác giả trích dẫn từ bài báo nghiên cứu trước đây của chính tác giả:

M. Borkowski, C. Ritzer, D. McDonald, and S. Schulte. Caught in Chains: Claim-First Transactions for CrossBlockchain Asset Transfers. 2018. URL: http://dsg.tuwien.ac.at/staff/mborkowski/pub/tast/tast-white-paper-2.pdf. White Paper, Technische Universitat Wien. Version 1.1. Accessed 2019-02-15.

[8] External oracles và các phương tiện giao tiếp giữa các blockchain đều là các công cụ và giải pháp được sử dụng để tạo kết nối và truyền thông giữa các hệ thống blockchain khác nhau. Dưới đây là mô tả ngắn về hai khái niệm này:

External Oracles (các trung gian bên ngoài) là các thành phần hoặc dịch vụ được sử dụng để mang thông tin từ bên ngoài vào blockchain. Trong một blockchain đóng, thông tin từ thế giới thực như dữ liệu từ cảm biến, thông tin thời tiết, thông tin tài chính, hoặc bất kỳ nguồn dữ liệu ngoại vi nào khác không thể trực tiếp được gửi đến và sử dụng trong smart contract hoặc blockchain. External oracles đóng vai trò như một cầu nối, thu thập thông tin từ bên ngoài và đưa nó vào blockchain, cho phép smart contract truy cập và sử dụng thông tin này để thực hiện các hành động tự động.

Các phương tiện giao tiếp giữa các blockchain là các công nghệ, giao thức hoặc tiêu chuẩn được sử dụng để kết nối và truyền thông giữa các blockchain khác nhau. Với sự phát triển của nhiều blockchain độc lập, việc tạo ra các kết nối giữa chúng để chia sẻ thông tin và tài sản trở nên quan trọng. Các phương tiện giao tiếp giữa các blockchain cho phép trao đổi tài sản kỹ thuật số, thông tin giao dịch, hoặc tài nguyên giữa các mạng lưới blockchain khác nhau. Các giao thức và tiêu chuẩn như Atomic Swap, Interledger Protocol (ILP), Polkadot, Cosmos và AION là các ví dụ về các phương tiện giao tiếp giữa các blockchain.

[9] Solidity là một ngôn ngữ lập trình dùng để viết smart contract trên nền tảng Ethereum. Được tạo ra bởi Ethereum Foundation, Solidity là ngôn ngữ chính thức và phổ biến nhất cho việc phát triển smart contract trên Ethereum và các blockchain khác sử dụng Ethereum Virtual Machine (EVM).

Solidity là một ngôn ngữ hướng đối tượng, có cú pháp tương tự với JavaScript và một số đặc điểm từ ngôn ngữ như C++, Python. Nó cung cấp các tính năng mạnh mẽ để xây dựng các smart contract phức tạp, bao gồm cả việc xác định cấu trúc dữ liệu, hàm, kiểu dữ liệu, sự kiện và modifier.

Các smart contract được viết bằng Solidity có thể triển khai và chạy trên mạng Ethereum và tương tác với các ứng dụng và người dùng khác. Solidity cho phép các lập trình viên định nghĩa quy tắc kinh doanh, hợp đồng, token, các thuật toán phức tạp và nhiều tính năng khác.

Solidity cung cấp các công cụ phát triển mạnh mẽ như trình biên dịch, bộ thư viện, trình gỡ lỗi và trình biên dịch đóng gói (compiler). Nó được tích hợp với các IDE (Integrated Development Environment) như Remix, Truffle và Visual Studio Code để hỗ trợ phát triển và kiểm thử smart contract một cách dễ dàng.

Với Solidity, người dùng có thể viết các smart contract thông minh phức tạp để thực hiện các ứng dụng phân quyền, hợp đồng tài chính, ICO (Initial Coin Offering), DeFi

(Decentralized Finance) và nhiều ứng dụng khác trên nền tảng Ethereum và các blockchain tương thích EVM.

[10] Eventual consistency trong multi-blockchain là một khái niệm liên quan đến độ nhất quán dữ liệu giữa các blockchain khác nhau trong một môi trường đa blockchain.

Khi có nhiều blockchain hoạt động song song và không có một cơ chế trung tâm duy nhất để quản lý toàn bộ mạng lưới, việc đảm bảo sự nhất quán và đồng bộ dữ liệu trở thành một thách thức. Eventual consistency đề cập đến việc các blockchain trong mạng lưới sẽ cuối cùng đạt được trạng thái nhất quán, nhưng không cần thiết phải đồng bộ ngay lập tức.

Trong một mạng lưới đa blockchain, mỗi blockchain hoạt động độc lập và có thể có thời gian trễ khi truyền thông và cập nhật dữ liệu. Điều này có nghĩa là các blockchain có thể không nhất quán về trạng thái của các giao dịch, thông tin tài sản, hoặc thông tin khác liên quan. Tuy nhiên, thông qua quá trình xác nhận và cập nhật dữ liệu, các blockchain sẽ cuối cùng đạt được sự nhất quán.

Eventual consistency chấp nhận việc tồn tại một khoảng thời gian mà các blockchain trong mạng lưới có thể không nhất quán, nhưng cam kết rằng sự nhất quán sẽ được đảm bảo sau một khoảng thời gian xác định. Thời gian này có thể phụ thuộc vào các yếu tố như giao thức liên-blockchain, cơ chế xác nhận, hoặc quy trình xử lý dữ liệu.

Với eventual consistency, các blockchain trong mạng lưới có thể hoạt động một cách độc lập và vẫn đảm bảo tính toàn vẹn và an toàn của dữ liệu. Điều này cho phép mạng lưới đa blockchain cung cấp tính mở rộng, khả năng tương tác giữa các blockchain và hỗ trợ việc triển khai các ứng dụng phức tạp và các trường hợp sử dụng đa dạng.

[11] Claim-first transactions là một cách tiếp cận trong việc xử lý giao dịch trên các blockchain đa nền tảng, trong đó người dùng có thể tạo ra một giao dịch đòi hỏi trước (claim-first transaction) trước khi gửi các tài sản hoặc thực hiện hành động khác liên quan đến giao dịch đó.

Trong một giao dịch claim-first, người dùng tạo một giao dịch và yêu cầu xác nhận từ mạng lưới. Tuy nhiên, thay vì gửi tài sản hoặc thực hiện hành động ngay lập tức, người dùng có thể giữ lại quyền kiểm soát và hoãn việc thực hiện các hành động tiếp theo cho đến khi các điều kiện hoặc sự kiện xảy ra. Điều này cung cấp cho người dùng sự linh hoạt và kiểm soát trong việc thực hiện các giao dịch phức tạp hoặc đa bước.

Đề cập chi tiết hơn ở III-A.

[12] Deterministic witnesses (còn được gọi là chứng nhân xác định) là một khái niệm trong lĩnh vực blockchain và bảo mật. Nó đề cập đến việc sử dụng một quá trình xác định và dự đoán được để tạo ra các chứng nhân hoặc bằng chứng có tính xác thực cao.

Trong blockchain, các chứng nhân được sử dụng để xác minh tính đúng đắn của một sự kiện, giao dịch hoặc trạng thái trong mạng lưới. Chúng thường được sử dụng để giải quyết các vấn đề như sự nhất quán, bảo mật và bằng chứng trong quá trình xử lý giao dịch.

Deterministic witnesses đảm bảo rằng quá trình tạo ra chứng nhân là xác định và dự đoán được. Điều này có nghĩa là cùng một sự kiện hoặc giao dịch sẽ luôn tạo ra cùng một chứng nhân, không thay đổi theo thời gian hoặc ngẫu nhiên. Việc sử dụng deterministic witnesses giúp đạt được tính công bằng, minh bạch và đáng tin cậy trong quá trình xác minh và xác thực các giao dịch và sự kiện trong mạng lưới blockchain.

Đề cập chi tiết hơn ở III-A.

[13] Token trong blockchain là một đơn vị giá trị tương đương với một loại tài sản hoặc quyền sở hữu được biểu thị bằng mã thông qua một chuỗi ký tự đặc biệt. Token có thể đại diện cho tiền tệ, quyền biểu quyết, quyền sở hữu tài sản, hoặc bất kỳ quyền lợi nào khác mà người sử dụng blockchain muốn biểu thị.

Tokens có thể được tạo, quản lý và trao đổi trên các nền tảng blockchain, chẳng hạn như Ethereum, Binance Smart Chain, hoặc các chuỗi khác. Các chuỗi này hỗ trợ việc tạo ra các token tiêu chuẩn hoặc token tùy chỉnh thông qua các giao thức thông dụng như ERC-20 trên Ethereum.

[14] Pan-blockchain token là một loại token được thiết kế để có thể sử dụng và tồn tại trên nhiều blockchain khác nhau. Điều này có nghĩa là pan-blockchain token có thể được trao đổi và chuyển đổi giữa các mạng lưới blockchain khác nhau mà không cần thông qua các cổng (gateways) trung gian hoặc các quy trình phức tạp.

Với pan-blockchain token, người dùng có khả năng chuyển đổi và sử dụng token trên nhiều mạng lưới blockchain khác nhau mà không cần mất thời gian và công sức để rút và gửi token qua các cổng kết nối blockchain. Điều này mang lại tính linh hoạt và khả năng tương tác giữa các blockchain khác nhau.

Một số dự án và giao thức đã cung cấp pan-blockchain token, cho phép người dùng tạo và sử dụng token trên nhiều nền tảng blockchain. Ví dụ, Wrapped Bitcoin (WBTC) là một pan-blockchain token được tạo trên mạng Ethereum để đại diện cho Bitcoin và cho phép người dùng trao đổi và sử dụng Bitcoin trên mạng Ethereum.

Tuy nhiên, việc triển khai pan-blockchain token vẫn đòi hỏi sự phối hợp và hỗ trợ từ các mạng lưới blockchain liên quan. Điều này bao gồm việc xây dựng cổng kết nối hoặc giao

thức giao tiếp giữa các blockchain để thực hiện việc chuyển đổi và xác thực của pan-blockchain token.

Pan-blockchain token có tiềm năng mở rộng tính tương tác và tính ứng dụng của các token trên blockchain, cho phép người dùng tiếp cận và sử dụng các dịch vụ và ứng dụng trên nhiều blockchain khác nhau một cách thuận tiện và linh hoạt.

[15] Wallet trong blockchain là một ứng dụng hoặc công cụ được sử dụng để lưu trữ, quản lý và tương tác với các khóa riêng tư (private keys) và khóa công khai (public keys) của người dùng trong mạng lưới blockchain.

Một wallet cho phép người dùng tạo ra và quản lý các cặp khóa riêng tư và công khai, mà cặp này đóng vai trò quan trọng trong việc xác thực và chứng thực các giao dịch và tương tác trên blockchain. Khóa riêng tư là một chuỗi ký tự bí mật chỉ người dùng biết, trong khi khóa công khai là một chuỗi ký tự được chia sẻ công khai.

Wallet cung cấp một giao diện đơn giản và an toàn để người dùng có thể thực hiện các hoạt động như gửi và nhận token/cryptocurrency, xem số dư tài khoản, ký và xác minh các giao dịch. Wallet có thể được cài đặt trên các thiết bị di động, máy tính cá nhân hoặc thậm chí là các phần cứng riêng biệt như Ledger hoặc Trezor.

[16] Strict consistency (tính nhất quán nghiêm ngặt) đề cập đến một mô hình hoạt động trong đó tất cả các blockchain đồng thuận và thực hiện các giao dịch theo cùng một quy tắc và thứ tự. Điều này đảm bảo rằng mọi thay đổi hoặc giao dịch trên một blockchain sẽ được phản ánh và phê duyệt nhất quán trên tất cả các blockchain khác.

Khi đạt được strict consistency, các sự kiện và giao dịch trên một blockchain sẽ được sao chép hoặc đồng bộ hóa trên các blockchain khác một cách chính xác và theo thứ tự. Điều này đảm bảo rằng không có sự xung đột hoặc mâu thuẫn giữa các phiên bản của blockchain và đảm bảo tính nhất quán về dữ liệu và trạng thái trên toàn hệ thống.

Tuy nhiên, strict consistency có thể đòi hỏi một số giới hạn và độ trễ trong việc xác nhận và xử lý các giao dịch. Vì mỗi blockchain trong mạng lưới có thể có độ trễ và tốc độ xử lý khác nhau, việc đạt được strict consistency có thể đòi hỏi thời gian và nỗ lực phối hợp để đồng bộ hóa trạng thái và dữ liệu trên các blockchain.

Mô hình strict consistency có thể được sử dụng trong các trường hợp yêu cầu tính nhất quán cao và sự đồng bộ giữa các blockchain là cần thiết. Tuy nhiên, nó cũng có thể ảnh hưởng đến hiệu suất và khả năng mở rộng của hệ thống, do yêu cầu phải đảm bảo sự nhất quán trên tất cả các blockchain. Do đó, việc chọn mô hình hoạt động phù hợp trong multi-blockchain phụ thuộc vào yêu cầu và mục tiêu cụ thể của dự án.

[17] ECDSA là viết tắt của "Elliptic Curve Digital Signature Algorithm" (Thuật toán Chữ ký Số học Đường cong Elliptic). Đây là một thuật toán mã hóa chữ ký số được sử dụng trong mật mã học và các ứng dụng liên quan đến chứng thực và xác thực trong môi trường công cộng.

ECDSA sử dụng thuật toán đường cong elliptic (elliptic curve cryptography) để tạo ra các khóa và chữ ký số. Nó dựa trên việc sử dụng khóa riêng tư và khóa công khai để thực hiện chữ ký số học và xác thực thông tin.

Quá trình hoạt động của ECDSA bao gồm các bước sau:

Tạo khóa: Người dùng tạo một cặp khóa bao gồm khóa riêng tư (private key) và khóa công khai (public key) dựa trên thuật toán đường cong elliptic.

Chữ ký số: Người dùng sử dụng khóa riêng tư để tạo ra một chữ ký số học (digital signature) cho dữ liệu cần ký. Quá trình này bao gồm việc tính toán và chọn điểm trên đường cong elliptic.

Xác thực chữ ký: Người nhận sử dụng khóa công khai của người ký để xác minh tính hợp lệ của chữ ký số học. Quá trình này bao gồm việc tính toán và so sánh các giá trị để xác định xem chữ ký có được tạo bởi khóa riêng tư tương ứng hay không.

ECDSA được sử dụng rộng rãi trong các ứng dụng mật mã học, bao gồm trong các hệ thống blockchain như Bitcoin và Ethereum để xác thực các giao dịch và đảm bảo tính toàn vẹn của dữ liệu. Thuật toán này cung cấp tính bảo mật cao và khả năng xử lý hiệu quả với các khóa có kích thước nhỏ hơn so với các thuật toán mã hóa truyền thống.

[18] Keccak256 bởi Ethereum và SHA-256 bởi Bitcoin là hai thuật toán băm (hash algorithm) được sử dụng trong các hệ thống blockchain như Ethereum và Bitcoin để mã hóa thông tin và tạo ra giá trị băm (hash value).

Keccak256: Đây là thuật toán băm được sử dụng trong Ethereum, một nền tảng blockchain phổ biến cho các ứng dụng phân cấp và hợp đồng thông minh. Keccak256 được sử dụng để tạo ra định danh duy nhất cho các khối (block) và giao dịch trên Ethereum. Nó là phiên bản của thuật toán Keccak, một trong năm đề xuất ban đầu cho chuẩn băm SHA-3 của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ.

SHA-256: Đây là thuật toán băm được sử dụng trong Bitcoin, hệ thống blockchain đầu tiên và phổ biến nhất. SHA-256 (Secure Hash Algorithm 256-bit) được sử dụng để tạo ra giá trị băm duy nhất cho các khối và giao dịch trong mạng Bitcoin. Nó là một trong loạt thuật toán mã hóa SHA-2 phát triển bởi Cơ quan Bảo mật Quốc gia Hoa Kỳ (NSA) và được sử dụng rộng rãi trong các ứng dụng mật mã học và bảo mật.

Cả Keccak256 và SHA-256 đều sử dụng quy trình băm (hashing process) để chuyển đổi dữ liệu đầu vào (message) thành một giá trị băm duy nhất có độ dài cố định. Các giá trị băm này có tính chất không thể đoán trước, không thể phục hồi ngược lại dữ liệu gốc, và

thay đổi ngay cả với một sự thay đổi nhỏ trong dữ liệu đầu vào. Điều này giúp bảo mật thông tin và xác thực tính toàn vẹn trong các hệ thống blockchain.

[19] OmniLayer và CounterParty đều là các giao thức và lớp phần mềm được xây dựng trên nền tảng blockchain, đặc biệt là blockchain Bitcoin, để phát triển và quản lý các tài sản kỹ thuật số (digital assets) và hợp đồng thông minh.

OmniLayer (hay còn được gọi là Omni Protocol) là một giao thức phụ trên blockchain Bitcoin. Nó cho phép người dùng tạo ra và quản lý các token tùy chỉnh, được gọi là "Omni tokens" hoặc "Omni assets", trên blockchain Bitcoin. OmniLayer sử dụng các giao dịch đặc biệt trong blockchain Bitcoin để mã hóa thông tin về các tài sản, giao dịch và quản lý tài khoản người dùng. Các Omni tokens có thể đại diện cho bất kỳ tài sản nào như tiền tệ, chứng khoán, hàng hóa, điểm thưởng và nhiều hơn nữa.

CounterParty cũng là một giao thức và lớp phần mềm xây dựng trên blockchain Bitcoin. Nó cho phép người dùng tạo ra và quản lý các tài sản kỹ thuật số tùy chỉnh, được gọi là "CounterParty tokens" hoặc "CounterParty assets". Tương tự như OmniLayer, CounterParty sử dụng các giao dịch đặc biệt trong blockchain Bitcoin để mã hóa thông tin về các tài sản, giao dịch và quản lý tài khoản. Các CounterParty tokens có thể đại diện cho các loại tài sản khác nhau và được sử dụng trong các ứng dụng như giao dịch, chứng khoán phi tập trung (decentralized exchanges), và trò chơi trực tuyến.

Cả OmniLayer và CounterParty đều sử dụng lớp phần mềm và giao thức phụ trên blockchain Bitcoin để mở rộng khả năng của nền tảng Bitcoin và cung cấp các công cụ và tính năng để phát triển và quản lý các tài sản kỹ thuật số.

[20] EOS.IO là một nền tảng blockchain mã nguồn mở được thiết kế để xây dựng và triển khai các ứng dụng phi tập trung (decentralized applications - DApps). EOS.IO được phát triển bởi Block.one, một công ty công nghệ blockchain có trụ sở tại Cayman Islands.

EOS.IO nhằm mục tiêu cung cấp một nền tảng mạnh mẽ, linh hoạt và dễ sử dụng cho việc phát triển và triển khai ứng dụng blockchain. Nền tảng này được thiết kế để đạt được khả năng mở rộng cao và hiệu suất tốt, đồng thời giảm thiểu các phí giao dịch và thời gian xác nhận.

EOS.IO đã thu hút sự chú ý và sử dụng rộng rãi trong cộng đồng blockchain, nhất là trong lĩnh vực phát triển ứng dụng phi tập trung. Tuy nhiên, nó cũng gặp phải một số tranh cãi và thách thức liên quan đến mô hình bỏ phiếu DPoS và việc phân quyền quản lý mạng.

[21] Nút geth trong blockchain (viết tắt của Go Ethereum) là một phần mềm thực thi mã nguồn mở được sử dụng để chạy một nút đầy đủ trên nền tảng Ethereum. Geth là một trong những hiện thực Ethereum được phát triển bằng ngôn ngữ lập trình Go.

Một nút Geth đóng vai trò là một điểm kết nối trong mạng lưới Ethereum và tham gia vào việc xác nhận và xử lý giao dịch, tạo khối mới và duy trì toàn bộ blockchain. Nút Geth hoạt động như một phần mềm đồng thuận (consensus software) và thực hiện các quy tắc và thuật toán của Ethereum để duy trì tính toàn vẹn và bảo mật của mạng lưới.

Nút Geth cung cấp các chức năng và giao diện lập trình (API) cho phép người dùng tương tác với mạng Ethereum thông qua các lệnh dòng lệnh hoặc giao diện lập trình ứng dụng (API). Các nhà phát triển và người dùng có thể sử dụng nút Geth để truy cập dữ liệu từ blockchain Ethereum, gửi và nhận giao dịch, triển khai và quản lý hợp đồng thông minh, và thực hiện các hoạt động khác liên quan đến Ethereum.

Nút Geth là một phần quan trọng trong hệ thống Ethereum, đảm bảo sự phân phối và độ tin cậy của mạng lưới, cũng như cung cấp giao diện để tương tác với các ứng dụng và dịch vụ xây dựng trên Ethereum.

[22] Proof of Authority (PoA) là một thuật toán đồng thuận trong blockchain, nơi sự xác nhận và tạo khối mới được thực hiện bởi các nhà quản trị đã được xác định trước (trusted authorities) thay vì dựa trên việc khai thác (mining) hoặc sự chứng minh công việc (proof of work).

Trong hệ thống Proof of Authority, các nhà quản trị (authority nodes) được chỉ định và có trách nhiệm xác nhận các giao dịch và tạo khối mới trên mạng blockchain. Các nhà quản trị thường được xác định dựa trên sự tin cậy và uy tín của họ trong mạng lưới hoặc thông qua quy trình lựa chọn trước.

Proof of Authority thường được sử dụng trong các mạng blockchain tư nhân (private blockchains) hoặc các mạng blockchain công cộng (public blockchains) nhằm đạt được hiệu suất cao và kiểm soát tốt hơn từ phía các nhà quản trị. Tuy nhiên, mô hình này đòi hỏi sự tin cậy vào các nhà quản trị và có thể giảm bớt tính phân quyền của một hệ thống blockchain.

[23] Proof of Work (PoW) là một thuật toán đồng thuận được sử dụng trong các mạng blockchain như Bitcoin để xác nhận giao dịch và tạo khối mới. PoW đòi hỏi các miners phải thực hiện một công việc tính toán khó khăn và tốn nhiều thời gian để chứng minh rằng họ đã đóng góp vào việc bảo vệ và duy trì tính toàn vẹn của blockchain.

Mục tiêu của PoW là đảm bảo tính toàn vẹn và an toàn của mạng blockchain. Việc thực hiện các tính toán phức tạp trong PoW yêu cầu nhiều sức mạnh tính toán và tài nguyên năng lượng. Điều này tạo ra một ngưỡng khó khăn cho việc tấn công mạng, bởi vì một kẻ tấn công sẽ cần kiểm soát một phần lớn sức mạnh tính toán để áp đặt ý muốn của mình.

Tuy nhiên, việc sử dụng PoW cũng tiêu tốn nhiều năng lượng và có thể gây ra sự cạnh tranh lớn trong việc sử dụng tài nguyên tính toán. Đó là lý do mà một số blockchain khác

đã chuyển sang các thuật toán đồng thuận khác như Proof of Stake (PoS) để giảm tốn năng lượng và tăng hiệu suất của mạng.

[24] Proof of Stake (PoS) là một thuật toán đồng thuận được sử dụng trong các mạng blockchain như Ethereum 2.0 và Cardano để xác nhận giao dịch và tạo khối mới. Khác với Proof of Work (PoW) trong đó người tham gia cạnh tranh để giải quyết một bài toán tính toán phức tạp, PoS dựa trên việc đặt cược (stake) một số lượng token của người tham gia để xác định quyền kiểm soát và quyền tạo khối.

Trong PoS, việc xác định quyền tạo khối dựa trên sự đóng góp tài chính của người tham gia. Điều này giúp giảm đi nhu cầu sử dụng tài nguyên tính toán và năng lượng so với PoW. PoS cũng thúc đẩy việc giữ token và tham gia vào việc bảo vệ mạng, vì việc đặt cược lớn hơn sẽ tăng khả năng người tham gia được chọn để tạo khối và nhận phần thưởng.

Tuy nhiên, PoS cũng đặt ra một số thách thức và tranh cãi nhất định, bao gồm việc xác định các nguồn đáng tin cậy để tham gia vào mạng và vấn đề về trạng thái "Nothing at Stake" (không có gì để đặt cược). Để giải quyết những vấn đề này, các phiên bản khác nhau của PoS đã được phát triển, bao gồm Delegated Proof of Stake (DPoS) và Byzantine Fault Tolerance (BFT).

[25] Block time là khoảng thời gian mà một mạng blockchain cần để tạo ra một khối mới trong chuỗi khối. Nó định nghĩa tần suất tạo khối và ảnh hưởng đến tốc độ xác nhận giao dịch trên mạng.

Trong các mạng blockchain, như Bitcoin và Ethereum, block time được đo bằng giây. Ví dụ, Bitcoin có block time trung bình là khoảng 10 phút, trong khi Ethereum có block time trung bình là khoảng 15 giây. Điều này có nghĩa là mỗi 10 phút (đối với Bitcoin) hoặc 15 giây (đối với Ethereum), một khối mới sẽ được tạo ra và thêm vào chuỗi khối.

Block time quyết định tốc độ xác nhận giao dịch trên mạng blockchain. Khi một giao dịch được gửi đi, nó phải được xác nhận và đưa vào một khối trước khi được coi là hợp lệ. Vì vậy, thời gian xác nhận giao dịch sẽ phụ thuộc vào block time. Ví dụ, trong mạng có block time 10 phút, một giao dịch có thể mất khoảng thời gian từ 10 phút đến vài giờ để được xác nhận và được coi là hợp lệ.

Block time cũng có ảnh hưởng đến độ khó của việc khai thác trong các thuật toán đồng thuận như Proof of Work (PoW). Độ khó được điều chỉnh để đảm bảo rằng block time trung bình duy trì ở mức ổn định. Khi sức mạnh tính toán trên mạng tăng lên, độ khó tăng để giữ cho block time ổn định. Ngược lại, nếu sức mạnh tính toán giảm, độ khó sẽ giảm để đảm bảo block time không quá lâu.

Tuy block time là một yếu tố quan trọng trong thiết kế của một mạng blockchain, nó có thể thay đổi hoặc được điều chỉnh trong các phiên bản hoặc nâng cấp của mạng để đáp ứng yêu cầu và mục tiêu của từng dự án cụ thể.

[26] Gas limit là một khái niệm trong mạng Ethereum, nó xác định số lượng gas tối đa mà một khối có thể sử dụng trong quá trình thực hiện các giao dịch và thực hiện các hợp đồng thông minh.

Trong Ethereum, gas là đơn vị tính toán và đo lường công việc được thực hiện trên mạng. Mỗi hoạt động, từ việc chuyển tiền đến việc thực hiện hợp đồng thông minh, đều tiêu tốn một lượng gas nhất định. Gas limit là giới hạn tối đa cho tổng số gas mà một khối có thể sử dụng. Nếu một giao dịch hoặc hợp đồng thông minh vượt quá gas limit của khối, nó sẽ bị từ chối hoặc không thực hiện.

Người dùng của Ethereum phải trả phí gas để thực hiện các hoạt động trên mạng. Mức phí gas được xác định bằng cách nhân gas used (số gas đã sử dụng) với giá gas (giá trị quy định từ trước). Mức phí gas cũng phụ thuộc vào độ phức tạp của hoạt động và cung cấp đủ động lực cho các thợ mỏ trong việc xác nhận giao dịch và xây dựng khối mới.

Gas limit được đặt bởi người khai thác khối (block miner) khi tạo một khối mới. Nếu gas limit quá thấp, các giao dịch phức tạp hoặc các hợp đồng thông minh có thể không thực hiện được. Ngược lại, nếu gas limit quá cao, nó có thể dẫn đến lãng phí tài nguyên và ảnh hưởng đến hiệu suất của mạng.

Qua việc điều chỉnh gas limit, người dùng và khai thác khối có thể tương tác và ứng dụng các hoạt động phức tạp trên mạng Ethereum một cách hiệu quả và công bằng.

[27] Gwei là một đơn vị đo lường được sử dụng trong mạng Ethereum để đo giá trị của Gas, một phí được sử dụng để thực hiện các giao dịch và thao tác trên mạng. Gwei là viết tắt của Gigawei, và tương đương với 1 tỷ Wei.

Wei là đơn vị nhỏ nhất trong mạng Ethereum và được sử dụng để đo lường giá trị nhỏ nhất của Ether, đơn vị tiền tệ trong mạng Ethereum. 1 Ether tương đương với 1 quintillion (10^18) Wei.

Do đó, Gwei được sử dụng để đo giá trị của Gas trong mạng Ethereum, với mỗi Gas có giá trị được xác định bằng một số Gwei. Giá trị của Gas có thể thay đổi tùy thuộc vào cấu hình mạng và tình trạng cộng đồng Ethereum.

[28] Proof of Intent (PoI) là một khái niệm trong DeXTT. PoI đề cập đến sự chứng minh ý định của người tham gia trong việc thực hiện các giao dịch.

Trong DeXTT, PoI được sử dụng để xác định rằng người gửi và người nhận trong một giao dịch đã đạt được sự đồng ý và hiểu rõ về việc chuyển tài sản. Điều này đảm bảo tính xác thực và rõ ràng của giao dịch và giúp tránh những tranh chấp hoặc lừa đảo có thể xảy ra.

Cách thức thực hiện PoI có thể khác nhau trong từng giao thức cụ thể, nhưng ý tưởng chung là yêu cầu người gửi và người nhận phải chứng minh rằng họ đã rõ ràng và tự nguyện tham gia vào giao dịch. Điều này có thể được thực hiện thông qua việc chữ ký số, gửi thông điệp hoặc đặt cọc trước, tùy thuộc vào cơ chế của giao thức.

PoI là một yếu tố quan trọng trong việc đảm bảo tính an toàn và đáng tin cậy của các giao dịch trên blockchain, và nó đóng vai trò quan trọng trong việc xác định sự tham gia tự nguyện và rõ ràng của các bên trong mạng lưới.

HẾT