COIN98

ZERO-KNOWLEDGE PROOF ERA

Quá trình phát triển và ứng dụng trong thị trường Crypto

Mục lục

1 Ý chính

- Zero-knowledge proof (ZKP) cho phép prover chứng minh bằng mật mã cho verifier rằng một tuyên bố cụ thể là đúng hay sai mà không tiết lộ bất kỳ thông tin bổ sung nào không cần thiết.
- Mô hình hoạt động của một hệ thống ZKP có thể được phân chia thành 3 giai đoạn chính. **Giai đoạn thiết lập** (setup phase) bổ sung các tham số (gọi là RS - Reference String) và cấu hình ban đầu cho hệ thống ZKP. **Giai đoạn tạo bằng chứng** (proof generation/proving) và **giai đoạn xác minh bằng chứng**.
- Trong thị trường crypto, đa phần các hệ thống ZKP đời đầu có hạn chế lớn là cần trusted setup. Hai hướng tiếp cận để loại bỏ nhu cầu của một trusted setup là transparent setup & universal setup.
- ZKP có nhiều ứng dụng trong crypto nhưng nhóm ứng dụng quan trọng và đạt được nhiều sự chú ý nhất là nhóm các dự án cung cấp các hệ thống có khả năng lập trình như Ethereum.
- Một trong những hạn chế lớn nhất cản trở việc áp dụng ZKP vào crypto là hiệu suất. Các nhà phát triển đang xem xét nhiều cách khác nhau để cải thiện hiệu suất tổng thể của hệ thống ở cả khía cạnh phần cứng và phần mềm.

2 Tổng quan về Zero-knowledge proof trong Crypto

2.1 Định nghĩa Zero-knowledge proof (ZKP)

Zero-knowledge proof (ZKP) có thể hiểu là quá trình để một bên (gọi là người chứng minh - **Prover**), chứng minh một tuyên bố **(Statement)** với một bên khác (gọi là người xác minh - **Verifier**), rằng họ biết tuyên bố là đúng hoặc sai mà không tiết lộ những thông tin khác.

Dưới đây là một ví dụ đơn giản để hiểu cách Zero-knowledge proof (ZKP) được áp dụng trong thực tế:

*Để vào được bar, bạn cần chứng minh bản thân với bảo vệ quán bar rằng **"bạn từ 18 tuổi trở lên"**.*

Cách thức thông thường, bạn sẽ xác minh danh tính thông qua việc tiết lộ căn cước công dân (CCCD). Tuy nhiên, ngoài thông tin "bạn trên 18 tuổi", thông qua CCCD, bảo vệ quán bar sẽ biết nhiều thông tin về bạn, bao gồm: tên, tuổi, quê quán, năm sinh, số CCCD...

ZKP có thể áp dụng trong trường hợp này để bạn chứng minh mình từ 18 tuổi trở lên mà không cần tiết lộ những thông tin không cần thiết khác. Cách thức như sau:

- *Bạn và bảo vệ quán bar đồng ý về một con số bí mật là con số 18, chỉ bạn và bảo vệ quán bar biết về con số này.*
- *Bạn sẽ lấy số tuổi của mình chia cho 18 và gửi phần nguyên cho người bảo vệ quán bar để làm bằng chứng.*

Nếu ban 15 tuổi:

15 / 18 = 0.8333 - phần nguyên là 0 và phần thập phân là 0.8333

Nếu bạn 18 tuổi:

18 / 18 = 1.0 - phần nguyên là 1 và phần thập phân là 0

Nếu bạn 25 tuổi:

25 / 18 = 1.3889 - phần nguyên là 1 và phần thập phân là 0.3889

- *Dựa vào con số bí mật được thiết lập ở giai đoạn thiết lập ban đầu giữa bạn và bảo vệ, nếu kết quả >= 1 thì bảo vệ quán bar dễ dàng biết được tuổi của bạn >= 18 tuổi. Nếu kết quả = 0 thì bảo vệ quán bar biết bạn nhỏ hơn 18 tuổi.*

Trong trường hợp trên, bạn có thể chứng minh bản thân trên 18 tuổi với bảo vệ quán bar bằng toán học mà không tiết lộ những thông tin không cần thiết cho bảo vệ.

4.2 Mô hình hoạt động của một hệ thống ZKP

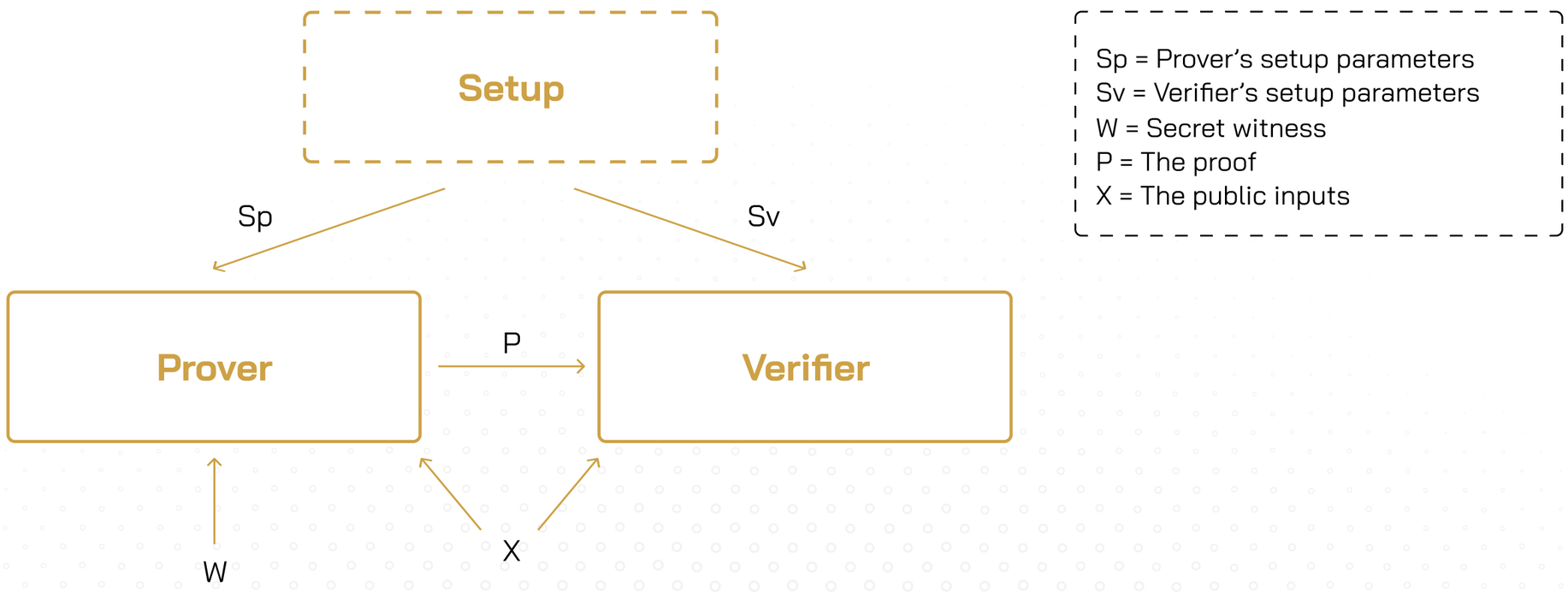
Trước khi tìm hiểu về cách hoạt động của một hệ thống ZKP, chúng tôi sẽ giới thiệu một số thuật ngữ liên quan thường được sử dụng trong các hệ thống ZKP bao gồm: proving system, statement, witness, prover và verifier.

- **Proving system (Hệ thống ZKP)**: đề cập đến một khuôn khổ hoặc phương pháp cụ thể để thiết lập hệ thống, tạo và xác thực các bằng chứng. Thị trường có rất nhiều proving system khác nhau, chúng có sự đánh đổi nhất định và phù hợp với một số trường hợp sử dụng riêng biệt.
- **Statement (Tuyên bố)**: mệnh đề mà prover muốn thuyết phục verifier là đúng mà không tiết lộ witness.
- **Witness (Nhân chứng hay thông tin đầu vào riêng tư)**: một mẩu thông tin đóng vai trò là thông tin đầu vào được cung cấp cho prover để tạo bằng chứng.
- **Prover (Bên chứng minh):** bên cố gắng chứng minh statement là đúng. Prover sử dụng witness để xây dựng bằng chứng chứng minh tính đúng đắn của statement mà không tiết lộ bất kỳ thông tin nào về witness.
- **Verifier (Bên xác minh)**: bên xác minh tính đúng đắn của statement thông qua việc xác minh bằng chứng được cung cấp bởi prover mà không cần tìm hiểu nội dung của witness.

Nhìn chung, chúng ta có thể khái quát mô hình hoạt động của một hệ thống ZKP thành 3 giai đoạn chính:

- **Giai đoạn thiết lập (setup phase)**: Giai đoạn thiết lập, bổ sung các tham số (gọi là RS - Reference String) và cấu hình ban đầu cho hệ thống ZKP.
- **Giai đoạn tạo bằng chứng (proof generation/proving)**: Giá trị đầu vào công khai **(X)** được cung cấp cho prover và verifier để thực hiện tính toán. Giá trị đầu vào riêng tư (secret witness) chỉ được cung cấp cho prover. Prover mã hóa **secret witness** một cách độc lập bằng cách sử dụng một commitment scheme cụ thể để tạo bằng chứng. Bằng chứng được prover tạo và gửi cho verifier xác minh.
- **Giai đoạn xác minh bằng chứng (proof verification)**: Dựa vào giá trị đầu vào công khai được cung cấp ban đầu, verifier dễ dàng xác minh tính đúng đắn của bằng chứng.

Hình 1: Các EIP đang được xem xét để đưa vào Dencun



Nguồn: Figmemt Capital

3 Sự phát triển của ZKP trong Crypto

ZKP có một lịch sử phát triển phong phú, cả trong và ngoài lĩnh vực crypto. Trong phần này, chúng tôi chỉ tập trung vào những sự phát triển chính của ZKP trong lĩnh vực crypto.

3.1 Hạn chế của các SNARK-based proving system đời đầu

SNARK (Succinct Non-interactive Argument of Knowledge) được giới thiệu chính thức vào tháng 1/2012 bởi Giáo sư Alessandro Chiesa của UC Berkeley và nhóm của ông (Co-inventor Zerocash, Co-founder Zcash, Co-founder StarkWare Industries).

SNARK không đề cập đến một proving system đơn lẻ, mà là một nhóm các proving system có chung các tính năng cụ thể.

Ngay sau khi được giới thiệu, nhiều SNARK-based proving system đã phát triển dựa trên các nguyên tắc này. Các hệ thống này cung cấp **hai lợi thế** đáng kể:

1/ Non-interactive: cho phép prover tạo ra bằng chứng mà không cần tương tác với verifier.

2/ Succinct: proving system tạo ra bằng chứng có kích thước nhỏ có thể được xác minh nhanh chóng và dễ dàng.

Trong bối cảnh blockchain, đặc biệt là Ethereum, các vấn đề về tài nguyên tính toán và không gian lưu trữ on-chain là những vấn đề quan trọng. SNARK nổi trội hơn hẳn với hai đặc điểm **Non-interactive** và **Succinct** khiến cho nó phù hợp hơn với các mạng lưới blockchain nói chung và Ethereum nói riêng. Đây có thể xem là bước phát triển thay đổi về chất từ 0 lên 1 (from zero to one).

Tuy nhiên, các hệ thống này cũng có **hai khuyết điểm** lớn:

1/ Non quantum resistance: Các hệ thống này sử dụng các phương pháp mật mã dựa trên các cặp đường cong elip, mặc dù hiện tại an toàn nhưng có thể bị máy tính lượng tử tấn công trong tương lai.

2/ Trusted setup:

- Trong giai đoạn thiết lập, một RS được tạo bởi một thực thể đáng tin cậy hoặc một nhóm nhỏ người tham gia. Tuy nhiên, nếu RS bị xâm phạm hoặc rò rỉ, nó có thể cho phép kẻ gian tạo bằng chứng gian lận => Gây ra rủi ro bảo mật đáng kể cho hệ thống.
- RS chỉ có thể được sử dụng trong một chương trình - program (specific circuit). Do đó, không thể tính toán chung với một RS duy nhất => Hạn chế tiềm năng ứng dụng của ZKP trong crypto.
- Khi nâng cấp hệ thống, bắt buộc phải thực hiện lại giai đoạn thiết lập để tạo lại RS => Gây khó khăn trong việc xây dựng các ứng dụng cần cập nhật hoặc nâng cấp thường xuyên.

Cộng đồng ZKP đã nghiên cứu các cách để giải quyết những hạn chế này, chủ yếu tập trung vào hai lĩnh vực chính:

- Phương hướng nghiên cứu thứ nhất: **loại bỏ nhu cầu trusted setup** trong khi **vẫn đảm bảo tính hiệu quả của proving system.**
- Phương hướng nghiên cứu thứ hai: **tập trung vào khả năng kháng lượng tử.**

Nhiều proving system phổ biến ngày nay đã xuất hiện từ những nỗ lực nghiên cứu theo phương hướng đầu tiên. Do đó, chúng tôi sẽ đi sâu vào các điểm chính trong nhánh này để khám phá những tiến bộ và đổi mới của chúng.

3.2 Transparent Setup & Universal Setup

Để giải quyết vấn đề về trusted setup, các nhà phát triển ZKP có hai cách tiếp cận chính:

- Transparent setup.
- Universal setup.

Transparent Setup

Giai đoạn thiết lập tạo **CRS (Common Reference String)** có thể được công khai hoặc được tạo thông qua một giao thức liên quan đến nhiều người tham gia, cho phép xác minh độc lập và giảm sự phụ thuộc vào bên thứ ba.

Dù CRS có bị lộ thì proving system cũng không bị ảnh hưởng. Một số proving system nổi bật sử dụng transparent setup bao gồm: Halo, STARK-based proving system.

Hầu hết, các hệ thống ZKP sử dụng transparent setup khắc phục được ba khuyết điểm chính của trusted setup nhưng chúng thường có hạn chế là kích thước bằng chứng khá lớn (tính bằng kb). Điều này hạn chế rất nhiều ứng dụng của chúng trong blockchain.

Universal Setup

Giai đoạn setup tạo ra **SRS (Structured Reference String)**. Nó thường được tổ chức dưới dạng một Ceremony với nhiều bên tham gia. Mỗi người tham gia tạo một secret, kết quả được trộn lẫn với những đóng góp trước đó. Sau đó, đầu ra được công khai và chuyển cho người đóng góp tiếp theo.

SRS được bảo mật miễn là có ít nhất một người tham gia che giấu thành công secret của họ. Một số hệ thống ZKP nổi bật sử dụng universal setup bao gồm: Marlin, PLONK-based proving system.

Đây là cách tiếp cận khắc phục được các khuyết điểm của trusted setup proving system, kích thước bằng chứng cũng nhỏ, thích hợp với ứng dụng trong blockchain. Nhưng chúng lại có hạn chế là ở khía cạnh kháng lượng tử, thời gian tạo và xác minh bằng chứng tuyến tính với độ phức tạp tính toán. Nhìn chung, chúng tôi khái quát chúng thành bảng sau:

Hình 2: Phân loại các hệ thống theo CRS & SRS

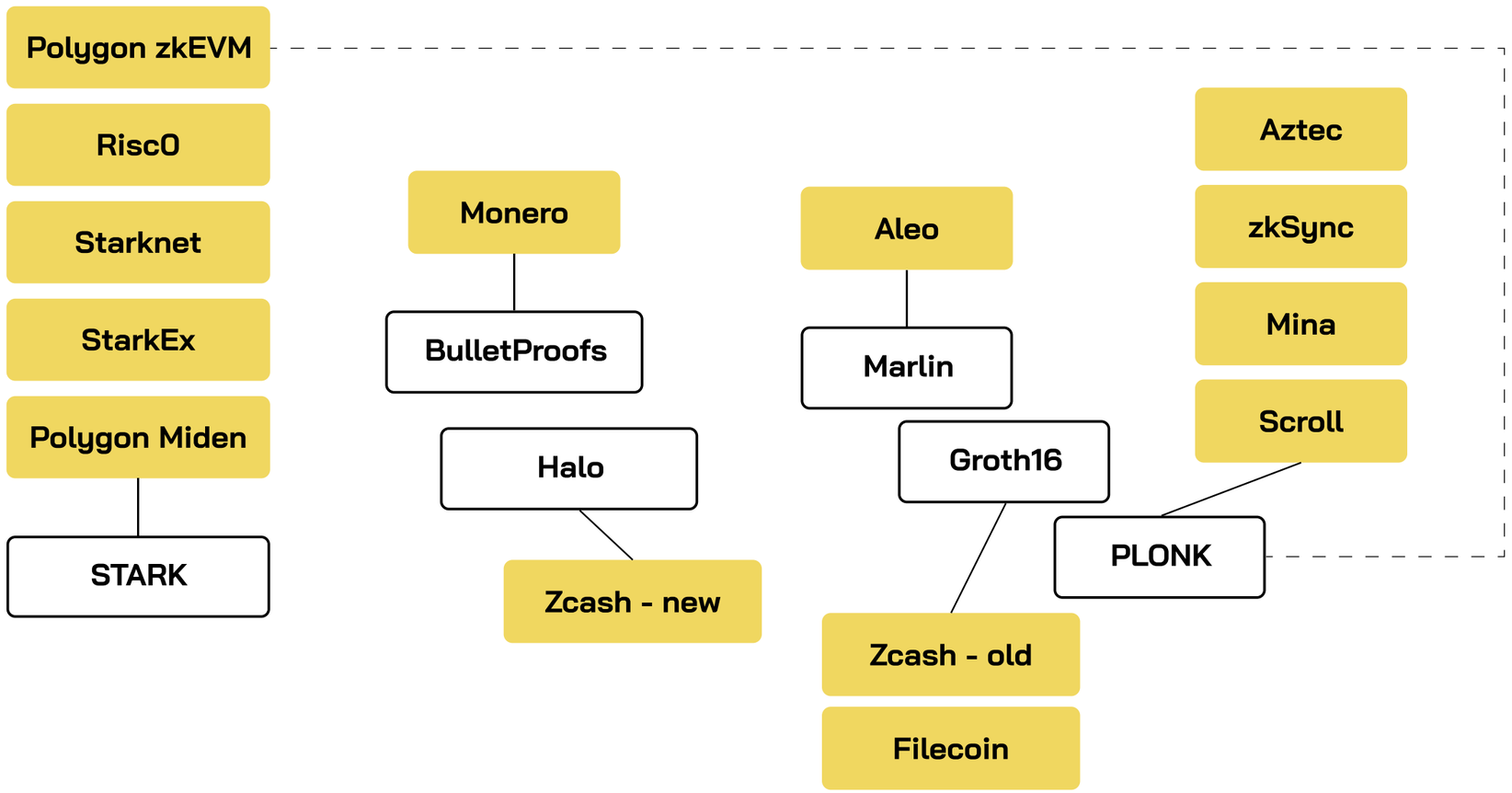
CRS (Common Reference String)	SRS (Structured Reference String)
Ligero	AuroraLight
Aurora	Sonic
Bulletproofs	Marlin
Halo	SuperSonic-RSA
Fractal	Plonk
Spartan	Groth16
SuperSonic-GG	BTCV14
ZK STARK	Libra
Hyrax	

3.3 Khung xem xét và đánh giá các proving system

Chúng tôi cung cấp cho bạn một khung (framework) để đánh giá các hệ thống ZKP khác nhau trong thị trường Crypto (một cách tương đối):

- **Standard proof generation time:** Thời gian cần thiết để tạo bằng chứng cho một giao dịch bằng hệ thống ZKP.
- **Standard proof verification time:** Thời gian cần thiết để xác minh bằng chứng cho một giao dịch bằng hệ thống ZKP.
- **Standard proof size:** Kích thước của bằng chứng được tạo cho một giao dịch sử dụng hệ thống ZKP.
- **Computation complexity:** Kích thước, thời gian tạo và xác minh bằng chứng sẽ thay đổi như thế nào khi độ phức tạp của tính toán tăng lên (ví dụ: đối với 10 tx, 100 tx, 1000 tx).
- **Hardware:** Xem xét hệ thống ZKP yêu cầu phần cứng chuyên dụng như thế nào để tối ưu hiệu suất. Điều này có thể ảnh hưởng đến chi phí của việc triển khai hệ thống trong thực tế.
- **Universal Circuit hay Specific Circuit:** Đề cập đến tính linh hoạt và khả năng ứng dụng của một hệ thống ZKP. Hệ thống ZKP hỗ trợ universal circuit có khả năng xử lý nhiều circuit khác nhau và có thể được áp dụng cho các nhiệm vụ tính toán khác nhau. Nó cung cấp mức độ linh hoạt cao, cho phép xây dựng và xác minh bằng chứng cho các ứng dụng đa dạng.
- **Upgradeable:** Đề cập đến khả năng nâng cấp của hệ thống mà không phải chạy lại giai đoạn thiết lập để tạo RS.
- **Recursive:** Hệ thống ZKP tạo và xác minh bằng chứng chứa các bằng chứng khác (sub-proof). Bằng cách hỗ trợ đệ quy (recursive), các proving system có thể đạt được khả năng giảm kích thước và chi phí tính toán của bằng chứng.
- **Post-quantum secure:** Khả năng kháng lượng tử.

Hình 3: Một số proving system phổ biến trên thị trường



Nguồn: Eli Ben-Sasson (Co-Founder Starkware)

- **Groth16:** Một proving system ra đời vào năm 2016, sử dụng một universal setup, kích thước bằng chứng nhỏ thuận lợi cho việc xác minh on-chain, nó có thể hoạt động trên các máy tính xách tay. Hạn chế là Groth16 chỉ hỗ trợ specific circuit, không hỗ trợ nâng cấp, không hỗ trợ đệ quy và không kháng lượng tử.
- **STARK-based proving system (Còn gọi là STARK):** Một hệ thống ZKP được giới thiệu chính thức vào 2018, sử dụng transparent setup, hỗ trợ universal circuit, hỗ trợ upgradeable, hỗ trợ đệ quy và kháng lượng tử. Hạn chế là kích thước bằng chứng lớn, cần phần cứng chuyên dụng để vận hành.
- **PLONK:** Một proving system ra đời vào năm 2018, sử dụng universal setup, kích thước bằng chứng nhỏ hơn STARK nhưng lớn hơn Groth16, hỗ trợ universal circuit, hỗ trợ nâng cấp, yêu cầu phần cứng chuyên dụng để đạt được hiệu suất tối ưu. Hạn chế là không hỗ trợ đệ quy và không kháng lượng tử.

Theo quan điểm của chúng tôi, không có proving system tốt nhất cho mọi trường hợp sử dụng trong blockchain, chỉ có proving system phù hợp nhất.

Thay vào đó, việc lựa chọn proving system phụ thuộc vào các yêu cầu cụ thể của ứng dụng. Ngay cả các proving system đã ra mắt lâu đời như Groth16 vẫn tiếp tục được sử dụng rộng rãi trong crypto.

4 Một số ứng dụng ZKP trong Crypto

ZKP có nhiều ứng dụng trong lĩnh vực crypto, chúng có thể là một hệ thống phức tạp như Rollup hay một ứng dụng được xây dựng trên Ethereum, vì thế sẽ rất khó để trình bày chi tiết hết tất cả.

Mục tiêu của phần này là cung cấp cho người đọc cái nhìn tổng quan và thực tế về 4 nhóm ứng dụng phổ biến trên thị trường. Một số trường hợp không được đề cập nhưng cũng tiềm năng bao gồm trò chơi (gaming), machine learning.

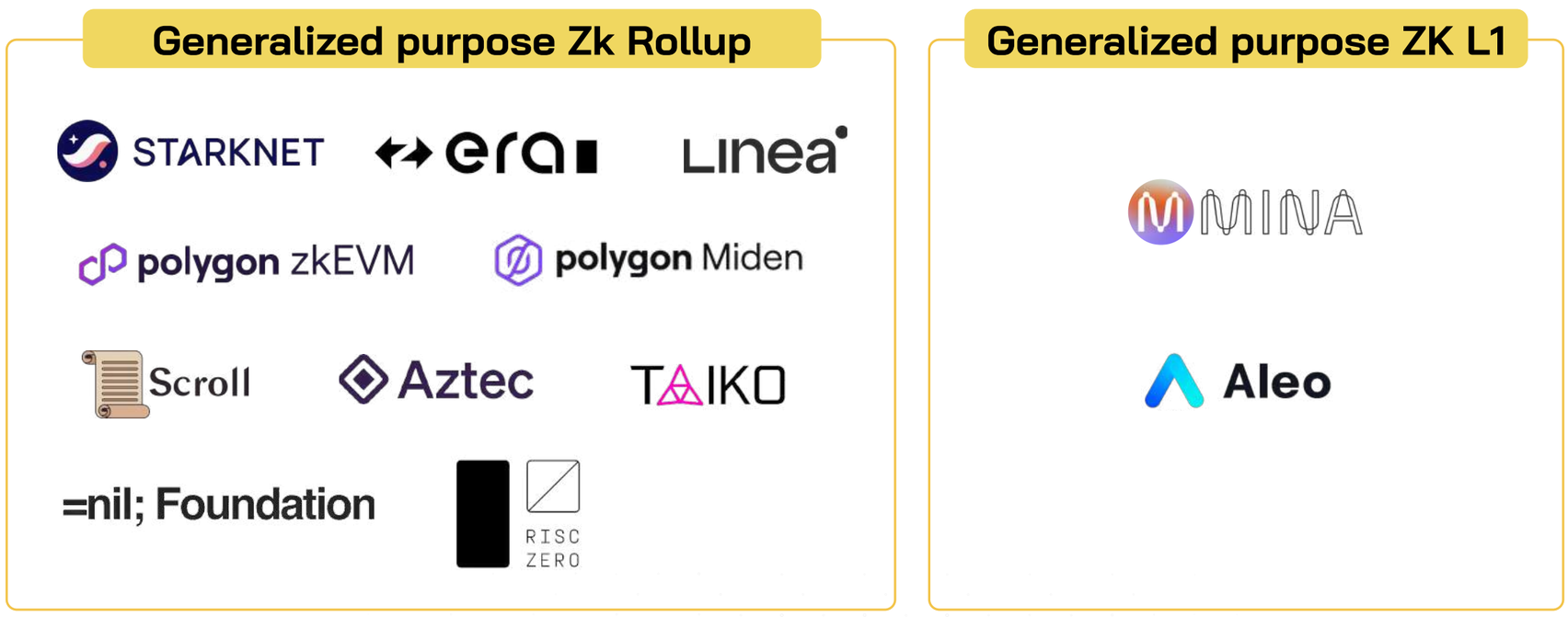
4.1 Generalized purpose ZK L1/Rollup

ZKP có nhiều ứng dụng trong crypto nhưng nhóm ứng dụng quan trọng và đạt được nhiều sự chú ý nhất là nhóm các dự án cung cấp các hệ thống có khả năng lập trình như Ethereum. Chúng tôi nhận thấy có hai cách tiếp cận chính với hướng suy nghĩ trên, tương ứng với hai nhóm dự án riêng biệt trên thị trường.

- Cung cấp khả năng mở rộng cho các hệ sinh thái đã trưởng thành như Ethereum => Generalized purpose ZK Rollup
- Tạo ra một hệ thống hoàn toàn mới => Generalized purpose ZK L1

Điểm chung của hai nhóm dự án này nhằm cung cấp một tầm nhìn chung là hỗ trợ các nhà phát triển xây dựng dApp có logic tùy ý. Hiểu cách khác, các dự án này đóng vai trò như một lớp cơ sở như Ethereum và cho phép các nhà phát triển xây dựng dApp trên đó.

Hình 4: Một số dự án Generalized purpose ZK L1/Rollup nổi bật



Nhóm dự án generalized purpose ZK Rollup có độ nhận thức cao hơn generalized purpose ZK L1 do có sự liên kết với hệ sinh thái Ethereum và đặt ra lời giải "hợp lý" cho bài toán về khả năng mở rộng của Ethereum.

Generalized purpose Zk Rollup

ZK Rollup di chuyển quá trình tính toán, chuyển đổi trạng thái (computing & state transition) và thực hiện ngoài chain chính (off-chain). ZKP được ứng dụng để tạo ra bằng chứng và xác minh trên lớp cơ sở. Quy trình này nhằm đạt được đồng thuận về tính toàn vẹn của quá trình được thực hiện off-chain.

Zk Rollup thesis chủ yếu dựa vào hai đặc điểm của ZKP là succinct và recursion. Thay vì chạy lại toàn bộ chương trình on-chain thì chỉ cần xác minh một bằng chứng nhỏ on-chain. Điều này giúp tiết kiệm nhiều sức mạnh tính toán và không gian lưu trữ trên base layer.

Tổ hợp ba tính năng "Rollup + ZKP + tính toán chung" khiến cho việc xây dựng generalized purpose ZK Rollup trở nên rất phức tạp và khó khăn. Tính đến thời điểm bài viết hoàn thành, chúng tôi ghi nhận chỉ có 5 dự án hoạt động trên mainnet bao gồm: Starknet, zkSync Era, Polygon zkEVM, Scroll và Linea.

Mặc dù tất cả nhóm dự án generalized purpose ZK Rollup đều cung cấp cho các nhà phát triển khả năng xây dựng dApp với logic tùy ý nhưng các dự án thường lựa chọn các hệ thống ZKP khác nhau và có các tùy chỉnh riêng để phù hợp với tầm nhìn của họ. Hệ quả của việc này là tạo ra các ngôn ngữ lập trình (DSL - domain specific language), dev tools/compiler mới.

Ngoài khía cạnh ngôn ngữ phát triển, lựa chọn các hệ thống ZKP khác nhau và các tùy chỉnh còn ảnh hưởng trực tiếp tới các thuộc tính của Rollup như phí giao dịch, thời gian rút tiền, tính cuối cùng của giao dịch (transaction finality), phần cứng chuyên dụng...

Hình 5: Tham số ZKP và tác động đối với Rollup

ZKP Parameter	Rollup Impact
Proving time	Affects L1 transaction confirmation & withdrawal time
Prover complexity	Affects hardware requirements for the prover and the prover decentralization
Proof size	L1& L2 transaction cost

Generalized purpose ZKP L1

Độ khó để xây dựng nên những hệ thống generalized purpose ZKP L1 cũng không kém các dự án generalized purpose Zk Rollup. Hai dự án nổi bật thường được đề cập trên thị trường là Mina Protocol và Aleo.

Mina Protocol sử dụng recursive SNARK cho phép một bằng chứng duy nhất xác minh toàn bộ lịch sử blockchain Mina. Mina giải quyết được bài toán về xác thực lightweight client nhưng lại rất khó khăn để đem việc "tính toán chung" lên mạng. Vì thế, mặc dù Mina Protocol đã mainnet vào năm 2021 nhưng mạng vẫn chưa hỗ trợ xây dựng dApp trên đó.

So về tính năng cung cấp, **Aleo** phần nào giống Aztec. Aleo có thể được miêu tả ngắn gọn là "L1 + ZKP + tính toán chung + native privacy". Hiện tại, dự án vẫn đang trong giai đoạn testnet.

4.2 Tương tác Cross-chain: ZK Cross-chain messaging/ZK Bridge

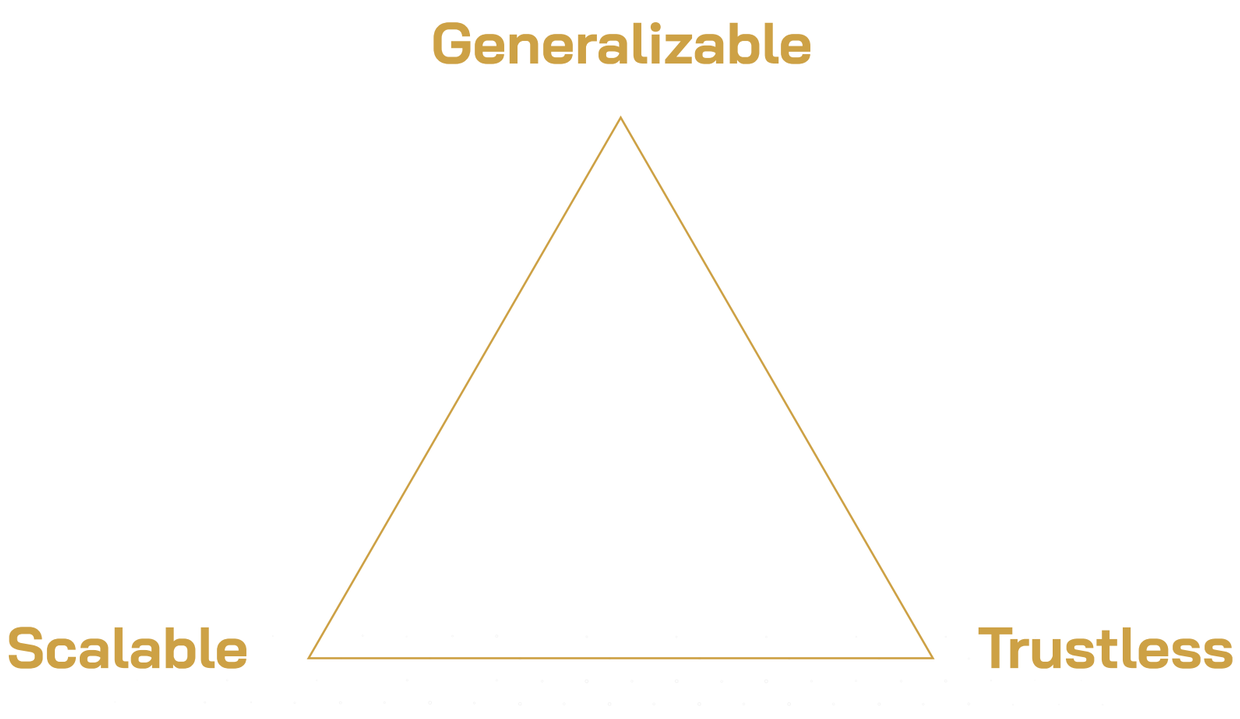
Khả năng tương tác cross-chain đã là một chủ đề thảo luận hot trong thị trường crypto. Liên quan tới chủ đề này, bridge là trường hợp sử dụng cụ thể và phổ biến nhất hiện nay. Cross-chain messaging là trường hợp sử dụng được khái quát hóa từ bridge.

Cụ thể, trên các cross-chain messaging có thể xây dựng được các bridge và nhiều loại ứng dụng khác đòi hỏi sự giao tiếp cross-chain (Layer Zero với Stargate Finance, Axelar với Squid...).

Hiện nay, các kiến trúc tương tác cross-chain luôn có những đánh đổi nhất định giữa 3 khía cạnh:

- Trustless: có bảo mật tương đương chain đích.
- Scalable: có thể được hỗ trợ trên bất cứ domain nào (L1, L2, L3).
- Generalizable: có khả năng xử lý dữ liệu cross-chain tùy ý.

Hình 6: The Interoperability Trilemma



Theo L2beat, hiện nay, hầu hết các bridge và cross-chain messaging trên thị trường sử dụng hưởng tiếp cận là "third party" cung cấp hai ưu điểm chính là khả năng mở rộng và xử lý dữ liệu cross-chain tùy ý. Về khía cạnh bảo mật, các dự án này thường bổ sung các giả thuyết bảo mật vào giao thức, khiến chúng trở thành mắt xích yếu nhất trong hệ thống.

Trong trường hợp của Wormhole & Layer Zero:

- Wormhole: Thông điệp được gửi từ chain nguồn phải được thông qua (signed) bởi ⅔ Guardians của Wormhole. Sau đó, thông điệp mới được chuyển tiếp tới chain đích.
- Layer Zero: Thông điệp được gửi từ chain nguồn phải cùng được thông qua bởi Oracle & Relayer. Hiểu theo cách khác, đây tương tự như 2-of-2 multisig.

Tuy nhiên vấn đề các bridge/cross-chain messaging tiếp cận theo hướng "third party" lại mang đến rủi ro cao. Trước đó, đã có rất nhiều giao thức liên quan bridge/cross-chain messaging bị hack/exploit.

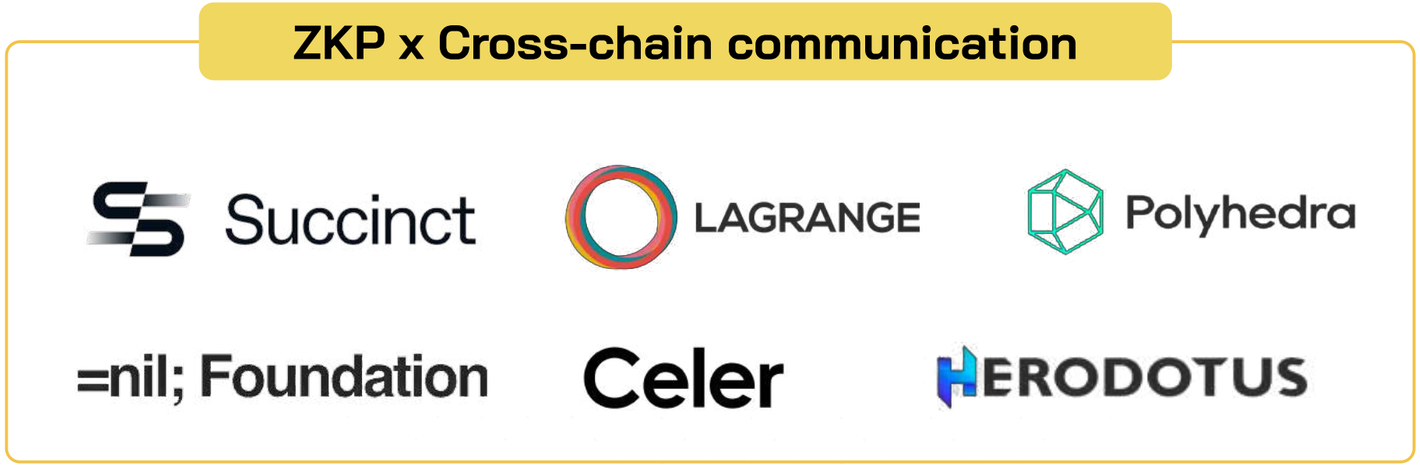
ZKP có thể được ứng dụng để cải thiện độ bảo mật của các giao tiếp cross-chain. Ý tưởng chung là bằng chứng ZKP có thể được sử dụng để chứng minh sự hợp lệ cho các thông điệp cross-chain, thông điệp từ chain nguồn sẽ được gửi kèm với một bằng chứng tới chain đích. Sau đó, bằng chứng sẽ được xác minh trên chain đích.

Tuy nhiên, có rất nhiều thách thức kỹ thuật xung quanh chủ đề ZK cross-chain messaging/ZK bridge. Một số vấn đề bao gồm:

- **Vấn đề chi phí:** Xác minh on-chain tốn nhiều gas => chi phí cho người dùng sẽ lớn.
- **Vấn đề độ trễ:** quá trình tạo bằng chứng và xác minh chúng trên chain đích sẽ tốn kha khá thời gian => người dùng chờ lâu để thông điệp/tài sản tới được chain đích.

Trong thực tế, một số dự án đã và đang bắt phát triển những nguyên bản đầu tiên dựa trên ý tưởng "sử dụng ZKP trong lĩnh vực tương tác cross-chain".

Hình 7: Một số dự án sử dụng ZKP trong lĩnh vực tương tác cross-chain



4.3 Trading: ZK Rollapp (L2/L3), ZK Appchain

Trading là một trong những ứng dụng quan trọng của crypto trong chu kỳ phát triển vừa rồi. Khi nhắc tới trading, chúng ta thường đề cập tới khía cạnh spot trading on-chain với những dự án tiêu biểu như Uniswap, Pancakeswap.

Chúng tôi muốn đề cập một khía cạnh tổng quát hơn của crypto trading, bao gồm:

- Spot trading
- NFT trading
- Derivatives trading (Perpetual, Options...)

Các ứng dụng liên quan crypto trading tồn tại dưới nhiều hình thức khác nhau, chúng có thể là một dApp trên Ethereum, Solana hoặc bất cứ một generalized purpose L1/L2 nào đó hoặc cũng có thể là một Appchain.

Trong chu kỳ vừa rồi, các khía cạnh được đề cập ở trên đều đã có những nguyên mẫu hoạt động trên thị trường và đạt được những thành công nhất định. Tiêu biểu như **Immutable X** (NFT trading), **dYdX** (Derivatives). Chúng tôi tin rằng khía cạnh này sẽ tiếp tục phát triển trong chu kỳ sắp tới của thị trường.

Khách quan, ZKP không phải lúc nào cũng phù hợp với mọi trường sử dụng liên quan trading. Chúng tồn tại như một tùy chọn trong nhiều lựa chọn khác nhau trên thị trường.

Trong một số mục đích cụ thể, chúng có thể cung cấp một ưu điểm so với các cơ sở hạ tầng khác. Hai đặc tính tiêu biểu mà ZKP mang lại cho nhóm ứng dụng trading là khả năng mở rộng **(scalable)** và sự riêng tư **(privacy)**.

Khả năng mở rộng ở lớp cơ sở hạ tầng

Etherum và EVM có những hạn chế nhất định. Việc xây dựng một order book DEX trên Ethereum là việc không khả thi vì chi phí hoạt động cho người dùng và MM quá lớn.

Các kiến trúc như ZK Rollup hoặc Validium có thể khắc phục hạn chế này. Tiêu biểu, dYdX sử dụng StarkEx để dựng một perpetual order book. dYdX duy trì matching engine off-chain và settlement on-chain. Một số lựa chọn phổ biến để xây dựng một Rollapp bao gồm:

- Orbit của Arbitrum.
- OP Stack của Optimism.
- Hyperchain của zkSync Era.
- StarkEX và L3 xây dựng trên StarkNet.
- Sovereign.

Trong các lựa chọn trên, StarkEx là dự án duy nhất có sản phẩm tồn tại trên thị trường. Các lựa chọn còn lại còn đang trong quá trình phát triển.

Tính năng Privacy trong Trading

Penumbra và Renegade là hai dự án tập trung vào Private Trading.

Renegade đang xây dựng on-chain dark pool trên Starknet, cung cấp sự riêng tư cả trước và sau khi giao dịch hoàn thành.

Trước khi giao dịch của người dùng được khớp, không ai có thể xem bất kỳ chi tiết nào về lệnh giao dịch đó. Sau khi lệnh được thực hiện, chỉ có đối tác khớp lệnh mới biết được tài sản nào đã được giao dịch.

Về mặt thiết kế, Renegade sẽ duy trì matching engine off-chain trên mạng cục bộ do dự án điều hành. Sau đó, thực thi/settlement on-chain trên Starknet.

Penumbra là một fully private Cosmos-based chain được tối ưu hóa cho trading.

Penumbra tập trung vào hệ sinh thái Cosmos. Khi các coin/token được bridge qua Penumbra, người dùng cũng có thể swap các tài sản bằng cách sử dụng native private DEX trên Penumbra. Dự án này sử dụng mô hình AMM thay vì order book.

4.4 Privacy: Privacy coin, mixer, privacy layer trên Generalized purpose L1

Privacy là một trong những ứng dụng đầu tiên của ZKP trong crypto và xuất hiện khá sớm. Tiêu biểu là **privacy coin**, chúng là các specific appchain sử dụng ZKP để cho phép chuyển coin một cách riêng tư, không tiết lộ chi tiết và dữ liệu của giao dịch trên blockchain của chúng. Một số dự án tiêu biểu như Monero, Zcash và Iron Fish.

Với mục đích tương tự, một số privacy app tồn tại trên các general purpose L1 như Ethereum hay Solana để cung khả năng chuyển token riêng tư, tiêu biểu như: **Tornado Cash, Railgun, Light Protocol...**

Một số đi xa hơn và cung cấp một số tính năng **privacy cho DeFi** trên lớp cơ sở như Aztec Connect (Dự án đã thông báo chuyển hướng phát triển). Tuy nhiên, UX-UI trên những dApp này là tương đối kém.

Nhìn chung, privacy là cần thiết nhưng chúng ta chưa bao giờ nhìn thấy nhu cầu sử dụng từ phía người dùng và nhà phát triển. Đây là vấn đề lớn nhất đối với nhóm dự án này.

5 Hạn chế của việc áp dụng ZKP vào Crypto

Mặc dù việc áp dụng ZKP trong lĩnh vực crypto đang được mở rộng nhanh chóng, nhưng sự chú ý và nhận thức không được phân bổ đồng đều giữa các nhóm và dự án khác nhau.

Hiện tại, trọng tâm và nguồn lực đang tập trung vào nhóm các giải pháp như Zk Rollup hoặc ZK L1, ZK Bridge... Các nhóm dự án này đang chi phối đáng kể phương hướng R&D của ZKP trong crypto.

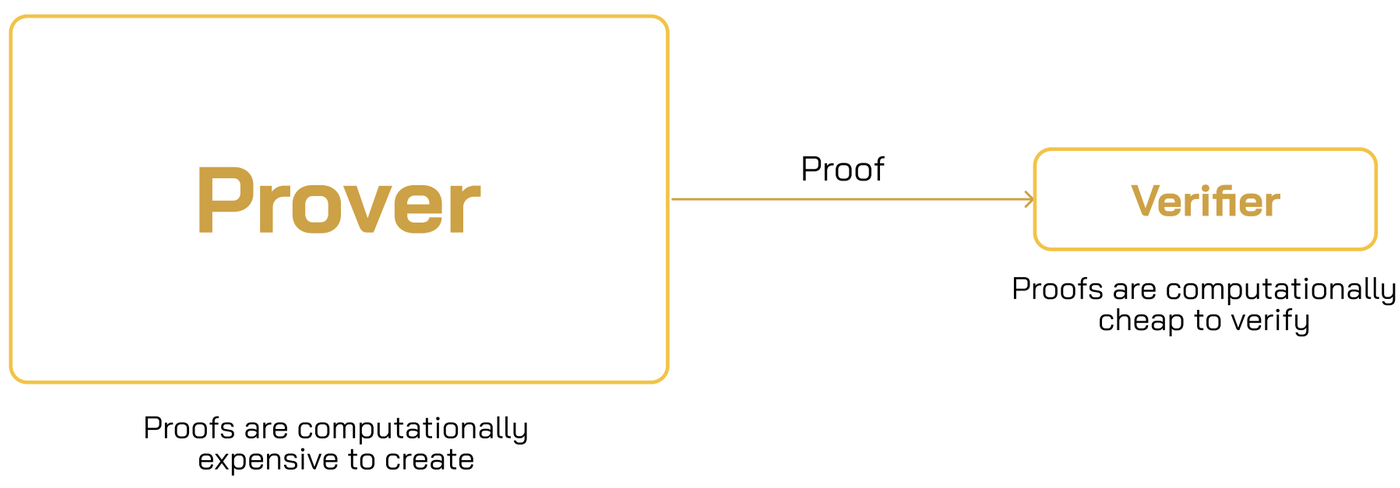
Theo quan điểm của chúng tôi, yếu tố ảnh hưởng lớn nhất tới việc áp dụng của chúng chính là **hiệu suất** tổng thể của hệ thống. Chúng có thể được đo lường bằng 3 thuộc tính chính:

- Thời gian tạo bằng chứng.
- Thời gian xác minh bằng chứng.
- Kích thước bằng chứng.

Tuy nhiên, ba thuộc tính trên biến thiên phụ thuộc vào độ phức tạp của ứng dụng. Ứng dụng càng phức tạp sẽ yêu cầu prover chứng minh các tuyên bố phức tạp hơn, chẳng hạn như tính toán liên quan đến cấu trúc dữ liệu nâng cao, điều kiện logic phức tạp, tương tác với các hệ thống bên ngoài.

Điều này sẽ làm tăng ràng buộc giữa các biến đầu vào trong circuit. Càng nhiều ràng buộc thì prover cần phải tính toán nhiều hơn để tạo bằng chứng. Với các ứng dụng phức tạp, quá trình tạo bằng chứng có thể mất vài phút, thậm chí vài giờ phụ thuộc nhiều vào phần cứng máy tính mà prover sử dụng.

Hình 8: Prover và Verifier



Thời gian xác minh và kích thước bằng chứng phụ thuộc nhiều vào proving system mà dự án lựa chọn. Mặc dù đã có nhiều proving system xuất sắc được phát triển như STARK, PLONK, Halo, Marlin... Nhưng nhìn chung, các proving system khác nhau có sự đánh đổi khác nhau giữa kích thước bằng chứng, thời gian xác minh, sự cần thiết của một trusted setup.

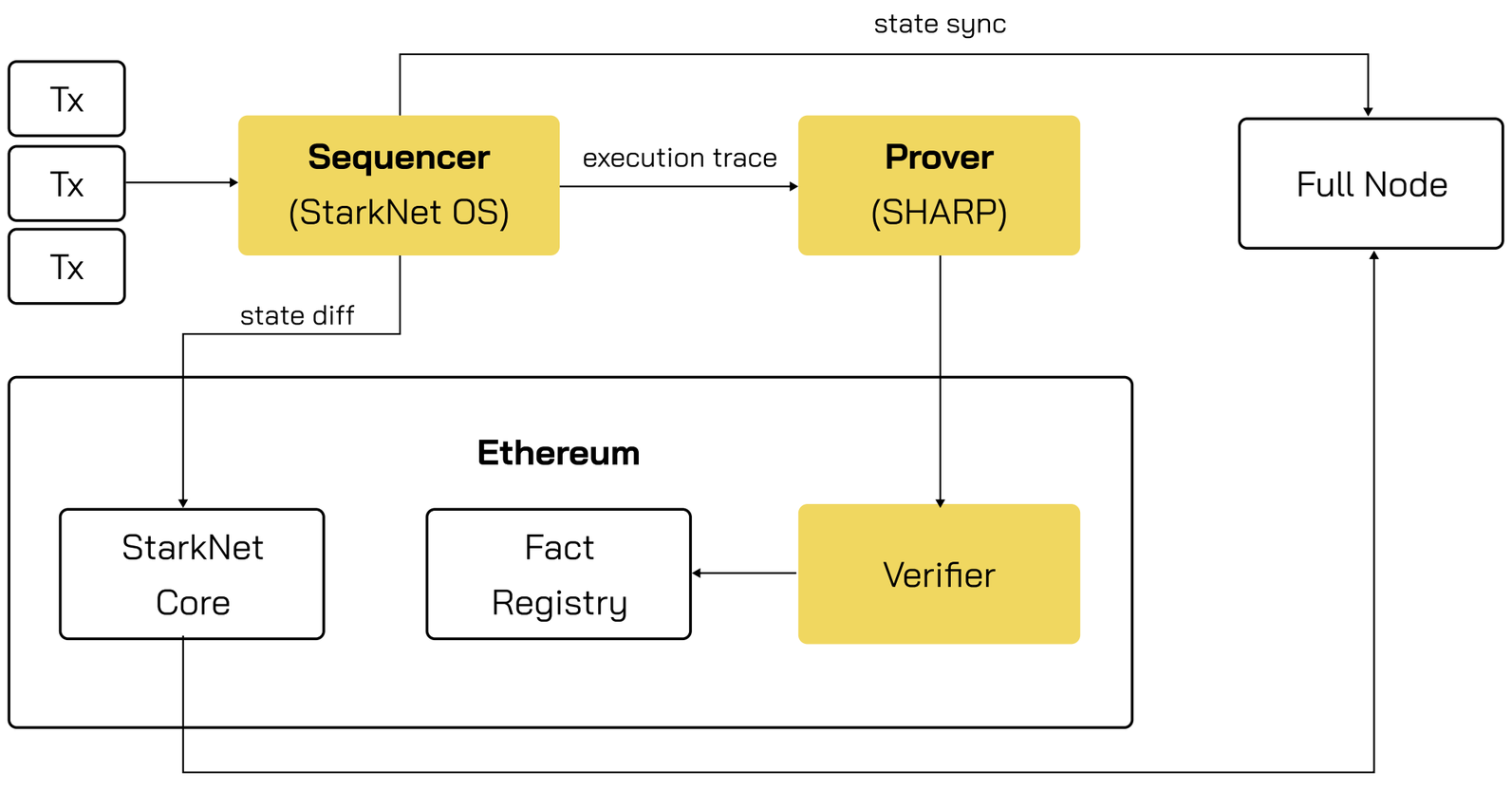
Hãy xem xét Starknet:

Starknet là generalized purpose ZK Rollup, sử dụng STARK-based proving system. Starknet là một hệ thống cực kỳ phức tạp. Vì thế, quá trình tạo ra một bằng chứng trên Starknet cực kỳ tốn tài nguyên tính toán.

Do đó, Starknet đang phải sử dụng centralized prover, tức là họ tự vận hành hoặc ủy quyền cho các công ty chuyên ngành (proving-as-a-service company) để tạo bằng chứng cho Starknet. Lựa chọn này giúp Starknet cải thiện đáng kể thời gian tạo bằng chứng (mặc dù vẫn rất chậm, tốn vài giờ) nhưng cũng khiến mạng tập trung hơn.

Ngoài ra, kích thước bằng chứng của Starknet cũng rất lớn nên họ không thể xác minh on-chain thường xuyên vì điều này sẽ gia tăng đáng kể chi phí cho người dùng trên Starknet, thường vài giờ Starknet mới xác minh một lần.

Hình 9: Kiến trúc của Starknet



Nguồn: Starknet

Điểm mạnh của Starknet là bằng chứng STARK không tuyến tính với độ phức tạp của ứng dụng/ circuit, vì thế họ có thể tạo một bằng chứng cho hàng ngàn giao dịch và sử dụng kỹ thuật đệ quy (recursive proof) để giảm chi phí và tăng hiệu quả trong Starknet.

Thời gian xác minh là một điểm mạnh đối với Starknet nói riêng hay các ZK Rollup nói chung, có thể mất từ vài phút đến vài chục phút đối với việc rút tiền từ Starknet, điều này là chấp nhận được với các giao thức Rollup nói chung.

Ngoài yếu tố hiệu suất, còn có những yếu tố khác ảnh hưởng tới sự áp dụng của ZKP, ví dụ, trải nghiệm người dùng rườm rà, phức tạp **(UX-UI).**

Tornado Cash và Railgun là hai dự án xây dựng trên Ethereum, cung cấp một số tùy chọn chuyển token riêng tư cho người dùng trên Ethereum. Hai dự án đều sử dụng hệ thống Groth16 vì người dùng sử dụng máy tính với phần cứng phổ thông để tương tác với ứng dụng.

Khía cạnh UX-UI, Tornado Cash hoạt động liền mạch với Metamask mà không cần người dùng cài đặt phần mềm hỗ trợ. Ngược lại, Railgun yêu cầu người dùng phải tải native wallet của dự án để sử dụng được dApp. Đây có thể xem là một rào cản đáng kể cho người dùng và nhà phát triển.

Nhìn chung, có nhiều trở ngại để ngăn cản sự áp dụng hàng loạt của ZKP. Tùy vào từng lớp ứng dụng thì sẽ có các khó khăn khác nhau. Trong đó, trở ngại lớn nhất của nhóm dự án ZK Rollup, ZK L1, ZK Bridge là vấn đề về **hiệu suất.**

6 Hai cách cải thiện hiệu suất tổng thể của ZKP

Chúng ta có thể cải thiện hiệu suất tổng thể của ZKP bằng cách hai cách tối ưu hóa phần cứng và phần mềm liên quan.

- Tối ưu hóa phần mềm liên quan tới DSL, Low-level libraries & Proving system.
- Tối ưu hóa phần cứng máy tính.

6.1 Tối ưu hóa phần mềm: DSL program, Low-level libraries & Proving system

Tối ưu hóa phần mềm bao gồm:

- Tối ưu hóa Low-level libraries.
- Tạo ra các DSL thân thiện với nhà phát triển.
- Tạo ra các hệ thống proving system phù hợp với từng nhóm ứng dụng.

Low-level libraries (ví dụ: Arkworks bằng Rust) cung cấp các nguyên tắc tính toán cho các hoạt động ZKP. Bằng cách tinh chỉnh Low-level libraries, chúng có thể giúp thực hiện các tính toán ZKP hiệu quả hơn về mặt thời gian và sức mạnh tính toán, dẫn đến hiệu suất tổng thể được cải thiện.

Cải tiến các DSL program (ví dụ: Cairo của Starknet) liên quan tới việc tạo ra một ngôn ngữ lập trình thân thiện hơn với con người (high-level language), giúp các nhà phát triển dễ dàng thể hiện ý định của họ một cách chính xác.

Proving system (ví dụ: PLONK, Halo, Marlin...) có hai nhiệm vụ chính là tạo bằng chứng và xác minh bằng chứng. Một proving system lý tưởng là một hệ thống có:

- Độ phức tạp và độ trễ của quá trình tạo bằng chứng thấp: Yêu cầu phần cứng thấp và tạo bằng chứng nhanh.
- Bằng chứng nhỏ và xác minh nhanh.

Tuy nhiên, không có một proving system nào có thể được coi là tốt nhất cho tất cả các trường hợp sử dụng. Thay vào đó, các proving system khác nhau phù hợp với các ứng dụng khác nhau và mỗi lựa chọn thường liên quan đến sự đánh đổi.

6.2 Phần cứng được tối ưu cho ZKP

Nhìn chung, tất cả các proving system đều có chung chức năng cơ bản là tạo bằng chứng và xác minh bằng chứng. Tùy thuộc vào proving system, quy trình tạo bằng chứng có thể khác nhau, nhưng "bottleneck" cuối cùng lại giống nhau - phần cứng máy tính để tối ưu hóa hiệu suất hoạt động.

Hai tác vụ tính toán chính trong một proving system

Như chúng tôi trình bày ở phần trước, các ứng dụng càng phức tạp thì prover càng phải tính toán nhiều để tạo bằng chứng. Cụ thể hơn, hai tác vụ tính toán chính thường được sử dụng trong các proving system bao gồm MSMs & FFTs.

- Multi-scalar Multiplications (MSMs)
- Number Theoretic Transforms (NTTs). Nó còn được gọi với tên khác là Fast Fourier Transforms (FFTs)

Hai tác vụ tính toán trên có thể chiếm 80–95% thời gian tạo bằng chứng. Tuy nhiên, rất khó ước lượng tỷ lệ chính xác của hai tác vụ tính toán các FFT và NTT trên toàn hệ thống vì phụ thuộc nhiều vào commitment scheme và các tùy chỉnh của mỗi dự án cụ thể.

Tuy nhiên, các nhà phát triển ZKP có thể kết luận tổng quan là các STARK-based proving system sẽ có nhiều tác vụ tính toán FFT hơn. Ngược lại, các SNARK-based proving system sẽ có nhiều tác vụ tính toán MSM hơn. Sơ đồ dưới đây sẽ giúp bạn có góc nhìn tổng quan về vấn đề này.

Hình 10: Tác vụ tính toán FFT & MSM trong các proving system phổ biến

Project name	Category	PCS	Proving System
Starknet	STARK	FRI	STARK
Risc0			
Polygon Miden			
Polygon zkEVM	STARK + SNARK	FRI & KZG	STARK + SNARK / Groth16
Scroll	SNARK	KZG	Halo2
zkSync Era			PLONK
Azec			
Aleo			Marlin

More FFT

More MSM

Tổng quan về 4 loại chip máy tính chính

Có bốn loại chip máy tính chính bao gồm: CPU, GPU, FPGA và ASIC:

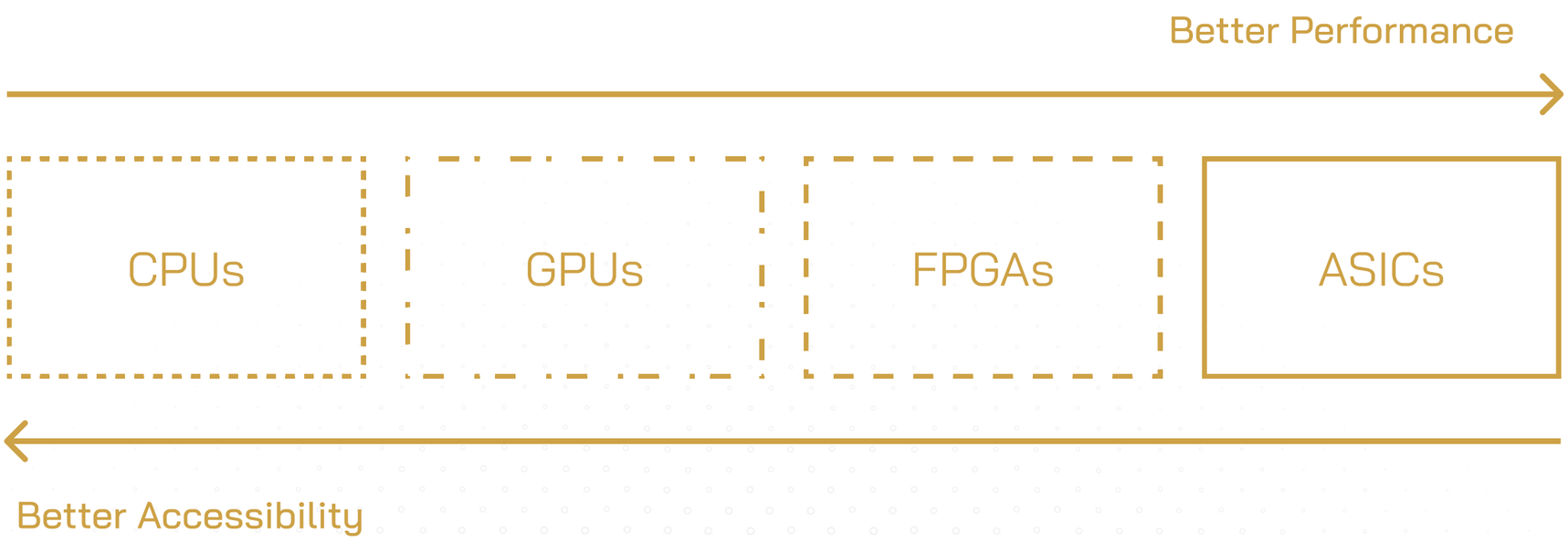
- **Central Processing Units (CPU)** là những con chip có mục đích chung (general-purpose chip) thường thấy trong thiết bị điện tử tiêu dùng. Chúng mang lại khả năng khái quát hóa cao và có thể xử lý nhiều loại nhiệm vụ. Tuy nhiên, bản chất xử lý tuần tự giới hạn hiệu suất của chúng đối với các ứng dụng yêu cầu nhiều tác vụ xử lý song song.
- **Graphics Processing Units (GPU)** là những chip chuyên dụng được thiết kế để xử lý song song. Nó vượt trội trong các nhiệm vụ như kết xuất đồ họa và machine learning. Mặc dù ít mục đích chung hơn CPU, nhưng GPU cũng khá phổ biến, dẫn đến sự phát triển của các libraries như CUDA và OpenCL giúp đơn giản hóa việc sử dụng chúng.
- **Field-Programmable Gate Arrays (FPGA)** là các chip có thể tùy chỉnh để tối ưu hóa cho các ứng dụng cụ thể. Các nhà phát triển có thể lập trình FPGA bằng ngôn ngữ mô tả phần cứng (HDL, Hardware Description Languages), cho phép hiệu suất cao hơn. FPGA cung cấp tính linh hoạt vì chúng có thể được sửa đổi mà không yêu cầu chip mới. Tuy nhiên, lập trình FPGA phức tạp về mặt kỹ thuật và đòi hỏi chuyên môn cao.
- **Application-Specific Integrated Circuits (ASIC)** là những con chip được thiết kế tùy chỉnh để siêu tối ưu hóa cho các tác vụ cụ thể. Không giống như FPGA, ASIC không thể lập trình lại vì thông số kỹ thuật của chúng được cố định trong chip. ASIC mang lại hiệu suất/USD và hiệu suất năng lượng cao nhất cho mục đích đã định trước.

Nhìn chung:

- CPU cung cấp chức năng đa năng với khả năng ứng dụng rộng rãi.
- GPU cung cấp khả năng xử lý song song để kết xuất đồ họa và machine learning.
- FPGA cung cấp giải pháp phần cứng có thể tùy chỉnh với tiềm năng hiệu suất cao hơn.
- ASIC mang lại hiệu suất/USD và hiệu suất năng lượng tối đa cho các tác vụ cụ thể.

Mỗi loại chip đều có điểm mạnh và sự cân bằng riêng, khiến chúng phù hợp với các ứng dụng khác nhau trong các ngành công nghiệp. Bảng sau sẽ cho bạn thấy tổng quan về 4 loại chip trên:

Hình 11: Đánh đổi giữa khả năng tiếp cận và hiệu suất của các loại phần cứng



Nguồn: Figmemt Capital

Tối ưu hóa hiệu suất ZKP với phần cứng chuyên dụng

Sự khác nhau về tỷ lệ của các tác vụ tính toán MSM và FFT tác động trực tiếp đến phần cứng máy tính phù hợp với các proving system.

Tác vụ tính toán MSM có thể được thực hiện song song nên chip GPU có thể đạt hiệu suất tốt hơn. Ngược lại, FPGA có thể xử lý tốt FFT tốt hơn.

Khi so sánh hiệu suất trung bình trên mỗi USD, GPU thường hoạt động tốt hơn so với FPGA. Tuy nhiên, khi FPGA hoạt động trên quy mô lớn và được ghép thành cụm thì chúng mang lại hiệu suất cao hơn cụm GPU tương xứng.

Mặc dù, ASIC mang lại hiệu suất trung bình trên mỗi USD cao nhất, nhưng chúng thường không được đem ra so sánh trong bối cảnh hiện tại. Điều này chủ yếu là do:

- Chi phí nghiên cứu và phát triển cao (hàng triệu USD). Thời gian sản xuất cũng rất lâu giao động từ 12 - 14 tháng.
- Công nghệ nền tảng chưa ổn định. Nếu trong thời gian phát triển, proving system đó "out meta" thì ASIC phải được thiết kế lại, tốn thêm chi phí và thời gian.

Ngày nay, để tăng tốc cho ZKP, có hai xu hướng sử dụng phần cứng chính: GPU và FPGA.

- **GPU** cung cấp thời gian phát triển nhanh với các libraries như CUDA và OpenCL. GPU dễ tiếp cận với mọi người, chúng cũng có giá cả phải chăng. Hạn chế là chúng lại có yêu cầu cao về điện năng.
- Mặt khác, **FPGA** có chu kỳ phát triển phức tạp hơn và yêu cầu các kỹ sư chuyên ngành. Chúng cho phép tối ưu hóa ở mức độ mà GPU không thể thực hiện được, dẫn đến hiệu suất có khả năng cao hơn. FPGA cũng cung cấp độ trễ thấp hơn, đặc biệt khi xử lý các luồng dữ liệu lớn. Tuy nhiên, FPGA đắt hơn GPU và vẫn đang trong giai đoạn phát triển (chưa có sẵn trên thị trường).

Hình 12: Ưu điểm và hạn chế của 4 loại phần cứng trong bối cảnh ZKP

Chip	CPUs	GPUs	FPGAs	ASICs
Pros	- Cheap, easy to acquire - The most generalizable	- Easy parallelizable - Strong software libraries to take advantage of parallelism	- Hardware can be programmed specifically for ZK operations - Cheaper than GPUs - More energy efficient than GPUs	- Has the highest performance - More energy efficient than FPGAs
Cons	- Not parallelizable - Not powerful	- Expensive - Not designed for cryptographic operations	- Requires knowledge of low-level hardware to maximize performance - Requires R&D to optimize for ZKP	- Can't be repurposed - Requires 1- 2 years to develop & produce

Nguồn: Figmemt Capital

Trong ngắn hạn từ 1 - 2 năm tới, GPU có lợi thế về giá, đặc biệt là sau khi ETH chuyển sang PoS. GPU cũng có lợi thế về thời gian phát triển ngắn và cung cấp cho các nhà phát triển khả năng xử lý song song lớn.

Tuy nhiên, trong trung hạn từ 2 - 3 năm, FPGA sẽ bắt kịp. Các FPGA khi được nhóm lại với nhau cũng mang lại hiệu suất tốt hơn so với các nhóm GPU. FPGA cũng có mức tiêu thụ điện năng tốt hơn GPU.

7 Lời kết

Zero-knowledge proof (ZKP) có tầm quan trọng ngày càng tăng đối với các hệ thống blockchain. Nhiều trường hợp sử dụng tiềm năng của ZKP trong crypto đã và đang được thảo luận, một số trường hợp sử dụng đang ứng dụng trong thực tế, tiêu biểu như Rollup.

Mặc dù vẫn còn những trở ngại cần vượt qua và những hạn chế cần giải quyết, nhưng nhìn chung những lợi thế và tiềm năng của ZKP đã được thể hiện rõ ràng.

Chúng tôi dự đoán một điểm bùng phát vào chu kỳ sau thị trường. Đối với các nhà phát triển blockchain và nhà đầu tư, câu hỏi quan trọng là khi nào ZKP season bắt đầu, chứ không phải ZKP season có xảy ra hay không?

Nguồn tham khảo

1. https://github.com/ventali/awesome-zk
2. https://figmentcapital.medium.com/accelerating-zero-knowledge-proofs-cfc806de611b
3. https://hackmd.io/@0xMonia/SkQ6-oRz3
4. https://medium.com/coinmonks/zero-knowledge-proof-izks-nizks-snarks-starks-5bc06c96c7ee
5. https://medium.com/@lucafra92/a-guide-to-zero-knowledge-proofs-f2ff9e5959a8
6. https://medium.com/nonce-classic/throne-of-zk-snark-vs-stark-e449984d5c36
7. https://medium.com/amber-group/need-for-speed-zero-knowledge-1e29d4a82fcd
8. https://medium.com/alliancedao/how-to-leverage-zkps-as-a-web3-builder-ae504783973d
9. https://medium.com/alliancedao/zkps-in-web-3-now-and-the-future-21b459348f29
10. https://hackmd.io/@Cysic/BJQcpVbXn
11. https://www.paradigm.xyz/2022/04/zk-hardware

Xem thêm

COIN98 INSIGHTS

Đọc thêm tại đây

Google Forms

Phản hồi tại đây

Về Coin98 Insights

Coin98 Insights là kênh truyền thông chính thức của Coin98 Super App - siêu ứng dụng lưu trữ tiền mã hóa. Thành lập từ 2017 với mục tiêu chia sẻ kiến thức đầu tư Crypto tới độc giả Việt Nam. Báo cáo của Coin98 Insights hướng đến các phân tích khách quan, độc lập. Chúng tôi tập trung vào những hệ sinh thái mới trong thị trường DeFi cũng như những số liệu hữu ích về Crypto ở Việt Nam.

Đội Ngũ Thực Hiện

Chịu trách nhiệm sản xuất: Vo Dang Vinh

Tác giả: Vo Dang Vinh

Biên tập: Duy Nguyen, Trang Tran

Thiết kế: Vinh Le