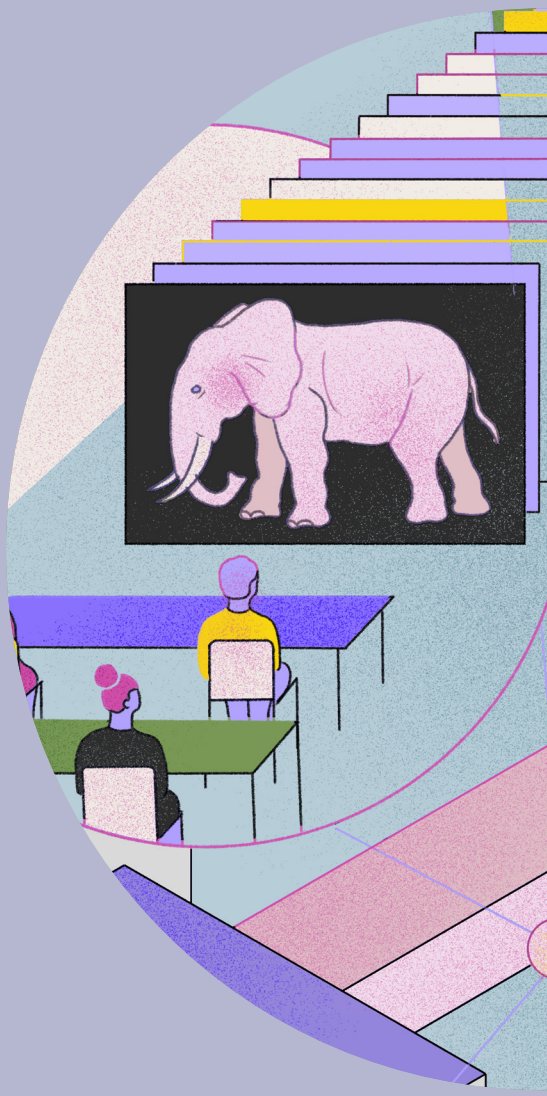
Báo Cáo Trạng Thái Zero Knowlegde 2022

Khám phá quan điểm của ngành công nghiệp tiền điện tử về zero knowledge và điều này có ý nghĩa gì cho tương lai.

Mina Foundation

Nội Dung—



—Về Báo Cáo Này

Tôi tin rằng trong tương lai, chúng ta sẽ nhìn lại quá trình công nghiệp hóa ZKPs* như một cột mốc quan trọng trong quá trình chuyển đổi quy mô lớn từ blockchain cá nhân sang công cộng.

— Paul Brody
Lãnh đạo Blockchain toàn cầu EY

***Định nghĩa ZKPs**
Viết tắt của zero knowledge proofs - Một bản gốc mật mã cho phép xác nhận và xác minh thông tin mà không tiết lộ thông tin đằng sau nó, chỉ xem tuyên bố có đúng hay không.

Theo như tôi dự đoán thì 5 hay 10 năm nữa,tôi nghĩ rằng chúng ta sẽ nói về các bằng chứng zero knowledge và ... tất cả các công nghệ và triển khai quyền riêng tư này giống như cách mà mọi người đã nói về blockchain 3 hay 5 năm trước.

— Jill Gunter
Người đứng đầu công ty Slow Ventures

Lĩnh vực bằng chứng zero knowledge cung cấp các tính năng bảo vệ quyền riêng tư cho nhiều loại tiền điện tử trong khi giữ cho các hệ thống phi tập trung hoạt động, tôi nghĩ sẽ là một trụ cột quan trọng của hầu hết các công nghệ trong thế kỷ tới.

— Tim Sweeney
Giám đốc điều hành Epic Games

Có lẽ công nghệ mật mã mạnh mẽ nhất trong thập kỷ qua là các bằng chứng zero knowledge nhỏ gọn.

— Vitalik Buterin
Đồng Sáng Lập Ethereum

Hai ứng dụng mạnh mẽ nhất của Zero Knowledge Proofs (ZKPs) là khả năng mở rộng và quyền riêng tư:

Khả năng mở rộng

ZKPs cho phép nhiều điểm dữ liệu được gói gọn trong một bằng chứng nhẹ, duy nhất, giúp tăng cường đáng kể hiệu quả và khả năng mở rộng. Bởi vì nhiều blockchain yêu cầu khả năng tính toán mạnh, công nghệ blockchain vẫn bị hạn chế đối bởi cơ sở hạ tầng, làm giảm khả năng mở rộng quy mô của nó. Bằng cách tận dụng ZKPs, các nhà phát triển có thể thiết kế các dapps rất nhẹ có thể chạy trên các phần cứng phổ biến hơn như thiết bị di động, mở ra một tương lai hứa hẹn của một Web3 có khả năng mở rộng và dễ tiếp cận hơn.

Sự riêng tư

ZKPs cho phép người dùng chia sẻ những thông tin cần thiết một cách an toàn để có quyền truy cập vào hàng hóa hoặc dịch vụ mà không tiết lộ chi tiết thông tin cá nhân có thể khiến người dùng dễ bị tấn công, khai thác hoặc đánh cắp danh tính. Khả năng bảo mật dữ liệu của ZKPs đặc biệt quan trọng đối với sự an toàn và bảo mật của Web3, bao gồm DeFi, DAO và metaverse. Khi lĩnh vực kỹ thuật số và vật lý ngày càng trở nên gắn bó với nhau, ZKPs sẽ trở nên cần thiết hơn nhiều cho một Web3 riêng tư, do người dùng kiểm soát.

Do mối quan tâm ngày càng tăng đối với ZKPs để cho phép một Web3 riêng tư, an toàn, do người dùng kiểm soát, Mina Foundation đã tiến hành một cuộc khảo sát để hiểu rõ hơn các quan điểm xung quanh ZKPs vào năm 2022.

Phương Pháp Luận

Báo cáo này dựa trên một cuộc khảo sát được tạo nên, phân phối và phân tích bởi các thành viên của Mina Foundation. Mina Foundation đã tạo ra các câu hỏi được thiết kế nhằm mục đích tóm tắt nhận thức chung của các ngành liên quan đến zero knowledge (ZK).

Cuộc khảo sát được phổ biến trên các phương tiện truyền thông xã hội và các kênh cộng đồng do các thành viên của Hệ sinh thái Mina điều hành cũng như các nhà lãnh đạo quan điểm chính trong ngành đã thể hiện sự quan tâm trong việc khám phá ZK với khán giả của họ. Tổng cộng có 1978 người tham gia cuộc khảo sát kéo dài 3 tuần*.

**Mina Foundation ước tính rằng mẫu khảo sát này đã thu thập quan điểm và ý kiến của hơn 1% tổng số nhà phát triển Web3 trong lĩnh vực này. Theo báo cáo năm 2021 của Electric Capital, có tổng số 18.416 nhà phát triển Web3 trêntoàn thế giới và báo cáo này thu hút khoảng 218 nhà phát triển.*

Người Tham Gia Khảo Sát

Những người tham gia được hỏi ba câu hỏi để đánh giá tính đa dạng trong mẫu.

Danh tính của những người tham gia khảo sát?

Những người tham gia khảo sát được yêu cầu chọn trong số các thành viên của cộng đồng tiền điện tử, các nhà giao dịch và nhà phát triển tiền điện tử. Kết quả cho thấy 67% người được hỏi được xác định là nhà giao dịch tiền điện tử, 22% được xác định là thành viên của cộng đồng tiền điện tử và 11% được xác định là nhà phát triển.

Độ tuổi của những người tham gia khảo sát?

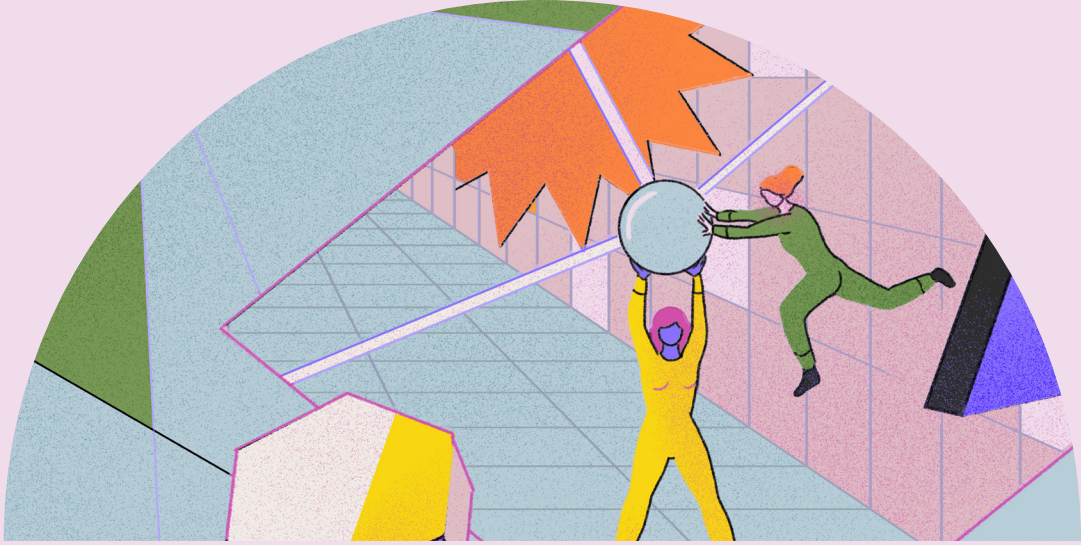
86% người được hỏi ở độ tuổi từ 19 đến 45.

Bạn có quen thuộc với Zero Knowledge Proofs (ZKPs)?

75,8% người được hỏi đã ít nhất nghe nói về ZKPs và biết ý nghĩa của nó, và 24,2% người được hỏi không biết ý nghĩa của nó.

Ngoài ra, 80% các nhà phát triển cho biết rằng họ đã quen thuộc với công nghệ ZKPs, cho thấy động lực để các nhà phát triển sử dụng ZKPs để phát triển.

Dựa trên nhân khẩu học của những người tham gia khảo sát, kết quả báo cáo phản ánh tâm lý chung đối với ZKPs từ quan điểm của các nhà giao dịch tiền điện tử nói chung và cộng đồng tiền điện tử trong quý 1 năm 2022.



Các Phát Hiện Chính

ZKPs rất quan trọng trong các lĩnh vực sau:

metaverse và Web3

42,2% người được hỏi tin rằng ZKPs là rất quan trọng đối với tương lai của metaverse và Web3.

sự lựa chọn tiền điện tử

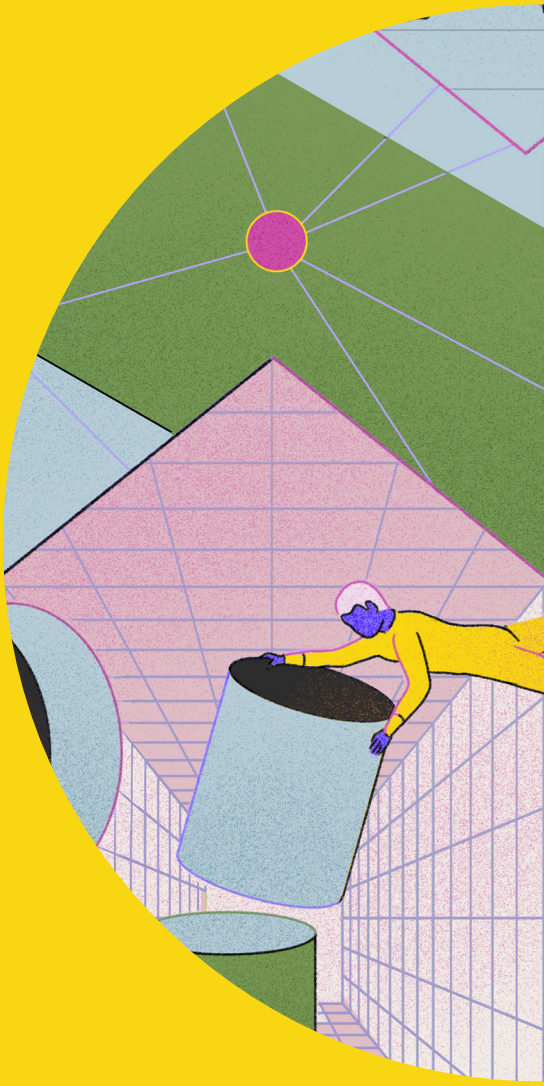
90,1% người được hỏi tin rằng tiền điện tử sử dụng ZKPs sẽ hấp dẫn hơn.

lĩnh vực tài chính

40,6% số người được hỏi tin rằng ngành tài chính là ngành cần ZKPs nhất.

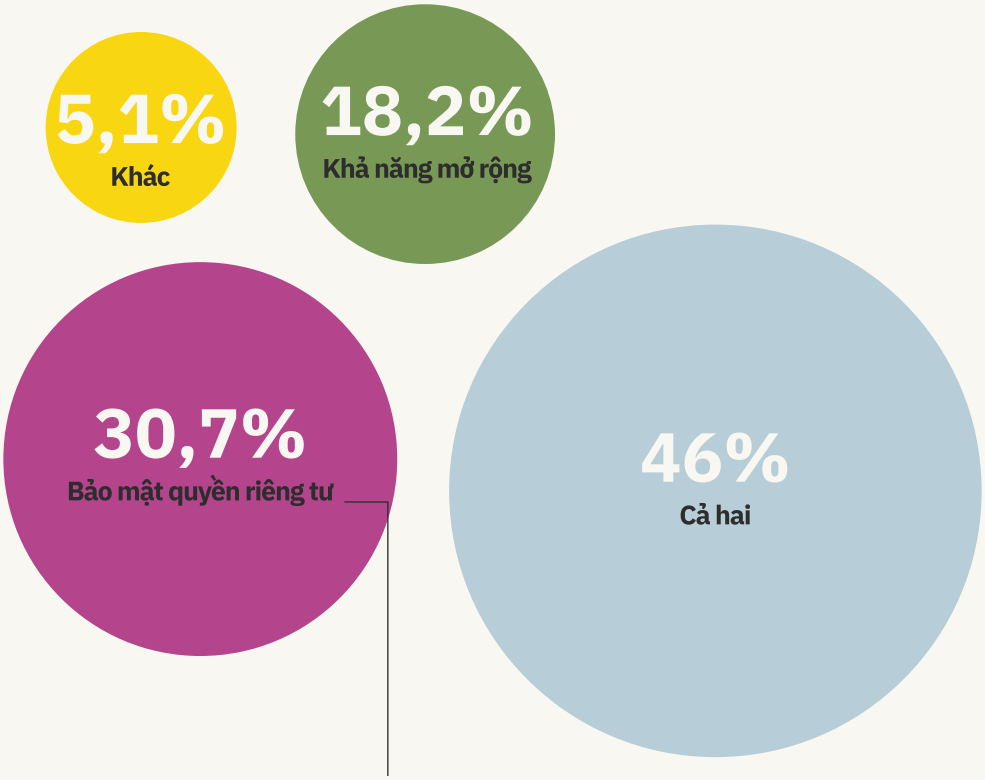
bảo vệ quyền riêng tư

30,7% người được hỏi tin rằng bảo mật quyền riêng tư là lợi thế chính của ZKPs.



—Kết Quả

BẠN NGHĨ ƯU ĐIỂM CHÍNH CỦA
BẰNG CHỨNG ZERO KNOWLEDGE LÀ GÌ?



Các Vấn Đề Riêng Tư

Khi được hỏi về những ưu điểm chính của ZKPs về mặt ứng dụng, 46% người được hỏi trả lời về cả quyền riêng tư và khả năng mở rộng; tuy nhiên, giữa quyền riêng tư và khả năng mở rộng, quyền riêng tư nhận được nhiều phản hồi hơn một chút, là 30,7%, trong khi khả năng mở rộng là 18,2%. **Sự ưu tiên nhỏ này đối với quyền riêng tư hơn khả năng mở rộng có thể phản ánh sự tập trung ngày càng tăng của ngành công nghiệp tiền điện tử vào quyền riêng tư, có thể được thúc đẩy bởi sự tập trung ngày càng tăng vào tập trung và sự tham gia của công ty trong metaverse.** Trên thực tế, một cuộc khảo sát gần đây của NordVPN[1] cho thấy 87% người được hỏi bày tỏ lo ngại về quyền riêng tư của họ trong metaverse. Điều thú vị là hầu hết các giải pháp dựa trên ZK khác cho đến nay đều tập trung vào khả năng mở rộng hơn là bảo mật quyền riêng tư.

[1] *https://nordvpn.com/blog/metaverse-survey/*

TIỀN ĐIỆN TỬ SỬ DỤNG ZKPS CÓ HẤP DẪN HƠN KHÔNG?

CÓ

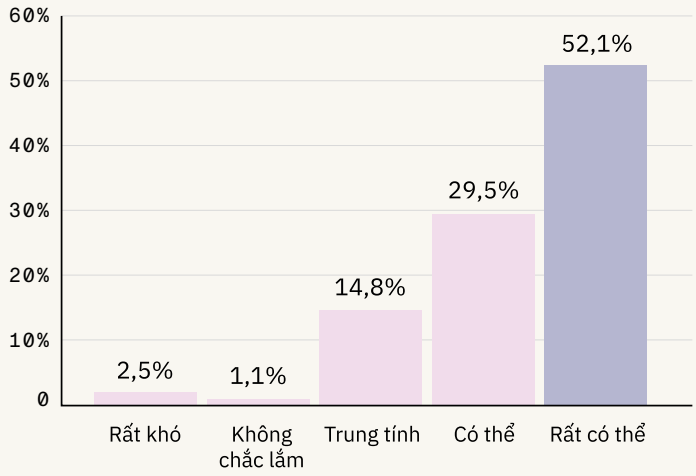
90,1%

KHÔNG

9,9%

90% người tham gia khảo sát hoàn toàn tin rằng tiền điện tử sử dụng ZKPs hấp dẫn hơn tiền điện tử không sử dụng ZKPs. Điều này có thể phản ánh mối quan tâm ngày càng tăng về quyền riêng tư, đặc biệt là xung quanh sự gia tăng của metaverse (như được mô tả trên trang 12 và 13). Tương tự như vậy, **Báo cáo[2] về tiền điện tử Messari năm 2022 dự đoán rằng "trong tương lai, tất cả các loại tiền điện tử sẽ sử dụng zero knowledge".**

NẾU BẠN BIẾT MỘT DAPP CÓ CÁC TÍNH NĂNG ZKPS ĐỂ BẢO MẬT QUYỀN RIÊNG TƯ HOẶC KHẢ NĂNG MỞ RỘNG, BẠN CÓ SẴN SÀNG MUỐN SỬ DỤNG NÓ HƠN KHÔNG?

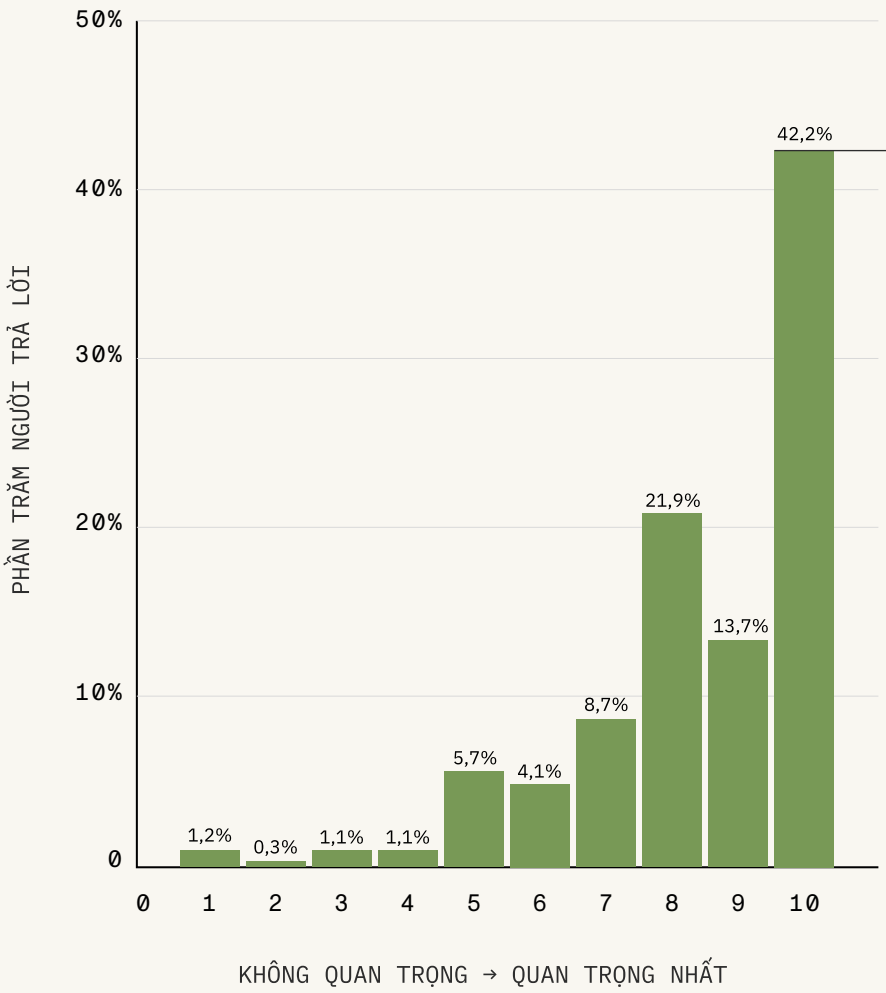


Khi được hỏi liệu họ có sẵn sàng sử dụng dapp với các ưu điểm của ZKPs hay không, **52,1% người được hỏi cho biết họ thích sử dụng dapp với các ưu điểm của ZKPs hơn. Điều này có thể cho thấy rằng các thành viên của cộng đồng tiền điện tử tin tưởng vào các lợi thế về quyền riêng tư và bảo mật của ZKPs,** đặc biệt là gần đây có các vi phạm bảo mật blockchain, với 1,2 tỷ đô la bị đánh cắp chỉ trong quý đầu tiên của năm 2022[3].

[2] *https://messari.io/pdf/messari-report-crypto-theses-for-2022.pdf* (Trang 145)

[3] *https://dappradar.com/blog/dapp-industry-report-q1-2022-overview*

ZKPS QUAN TRỌNG NHƯ THẾ NÀO TRONG WEB 3.0 VÀ METAVERSE?

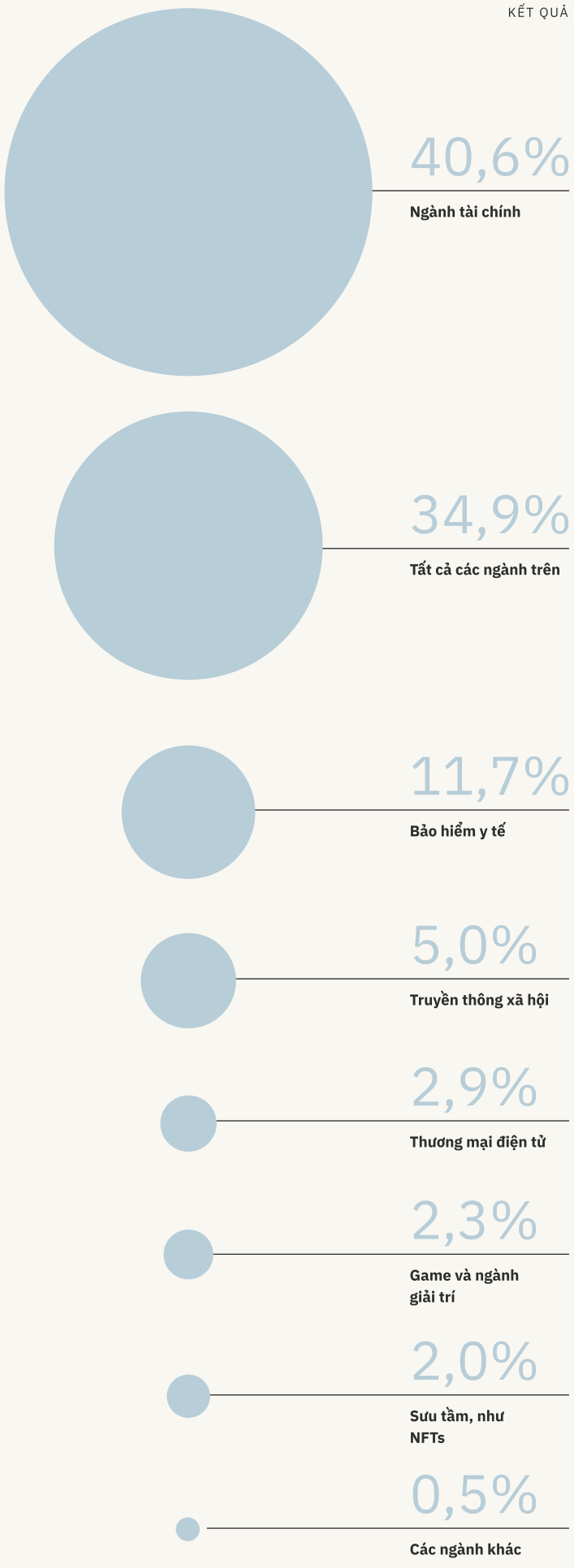


42,2% số người được hỏi chỉ ra rằng ZKPs có tầm quan trọng cao nhất trong metaverse và Web3, với **77,7%** cho điểm quan trọng từ 8 trở lên. Do sự chú ý của các công ty lớn như Epic, Roblox, Microsoft và Meta (trước đây là Facebook), **những con số này chứng minh mối quan tâm ngày càng tăng của cộng đồng tiền điện tử đối với sự kiểm soát của các tập đoàn metaverse.** Một nghiên cứu gần đây của NordVPN[4] cho thấy 47% người dùng internet không tin rằng danh tính của họ được bảo vệ. dữ liệu trong metaverse, dữ liệu người dùng có thể sẽ được sử dụng, điều này càng phản ánh mối quan tâm của nhiều người dùng hơn khi tham gia metaverse.

[4] *https://nordvpn.com/blog/metaverse-survey/*

> "Tôi nghĩ ZKPs chính xác là thứ mà hầu hết các blockchain đang thiếu ngày nay"
>
> —Người tham gia khảo sát

NHỮNG NGÀNH NÀO CÓ THỂ TÍCH HỢP TỐT NHẤT BẰNG CHỨNG ZERO KNOWLEDGE?



Kết quả cuối cùng cho thấy những người tham gia khảo sát tin rằng tất cả các ngành, bao gồm tài chính, chăm sóc sức khỏe, truyền thông xã hội, thương mại điện tử, trò chơi & giải trí và sưu tầm, sẽ được hưởng lợi từ ZKPs như một giải pháp cho ngành tài chính.

Khi việc sử dụng tài chính phi tập trung (DeFi) ngày càng tăng[5], **zsẽ có nhiều cơ hội hơn cho các ZKPs với khả năng mở rộng và các lợi ích bảo mật quyền riêng tư để tăng mức độ áp dụng rộng rãi trong ngành.**

[5] *https://www.statista.com/statistics/1272181/defi-tvl-in-multiple-blockchains/*

BẠN MUỐN GIỮ BÍ MẬT LOẠI DỮ LIỆU NÀO NHẤT?

54,5%

Dữ liệu tài chính

48,6%

Các loại thông tin nhận dạng cá nhân

46,7%

Tôi muốn ẩn danh nhất có thể

26,7%

Địa Điểm

25,8%

Sức khoẻ

13,3%

Tên

10,9%

Điểm tín dụng

Lưu ý: Câu hỏi này yêu cầu người trả lời chọn 3 tùy chọn.

Quyền riêng tư về tài chính

Những người tham gia cho biết điều quan trọng là phải giữ bí mật tất cả thông tin nhận dạng cá nhân, nhưng nhấn mạnh hơn vào tính bảo mật của dữ liệu tài chính, có thể bao gồm số An sinh xã hội của người dùng, số dư tiền điện tử, giá trị ròng, điểm tín dụng, v.v.

Ví dụ: sử dụng ZKPs để tạo dapp, người dùng chỉ cần chia sẻ bằng chứng về điểm tín dụng cá nhân của họ trên 700 để được vay mà không cần tiết lộ thông tin cá nhân khác. **Tầm quan trọng của việc bảo mật dữ liệu tài chính có nghĩa là ZKPs sẽ đóng một vai trò quan trọng trong tương lai của Web3 và DeFi.**

MỨC ĐỘ LO LẮNG CỦA BẠN VỀ CÁC ĐỐI TƯỢNG SAU ĐÂY TRUY CẬP VÀO DỮ LIỆU CÁ NHÂN CỦA BẠN LÀ GÌ?

Không lo lắng gì cả		Rất lo lắng
6,3%	Ví tiền điện tử	35,7%
3,5%	Các ngân hàng	39,9%
3,1%	Các nền tảng truyền thông xã hội	41,3%
2,5%	Công ty bên thứ ba	44,0%
3,1%	Chính quyền	48,5%

Những người được hỏi lo ngại nhất về việc chính quyền truy cập dữ liệu cá nhân của họ thông qua bất kỳ tổ chức nào khác. Điều thú vị là những người được hỏi bày tỏ mối quan tâm khá cao đối với tất cả các loại tổ chức. Với ngân hàng[6], nền tảng truyền thông xã hội[7] và các công ty bên thứ ba[8], ví tiền là thứ ít được quan tâm nhất.

Điều này thể hiện rõ ràng trong các vụ tấn công và vi phạm dữ liệu khác nhau đã xảy ra trong DeFi[9], các tổ chức tài chính, nền tảng truyền thông xã hội[10] và các chính phủ[11].

[6] *https://carnegieendowment.org/specialprojects/rotectingfinancialstability/timeline*

[7] *https://human-id.org/blog/biggest_social_media_breach_history/*

[8] *https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022*

[9] *https://blog.chainalysis.com/reports/2022-defi-hacks/*

[10] *https://firewalltimes.com/facebook-data-breach-timeline/*

[11] *https://www.comparitech.com/blog/vpn-privacy/us-government-breaches/*

—Kết Luận

Ý kiến được ghi lại trong báo cáo này cho thấy ngày càng nhiều cộng đồng tiền điện tử đang tìm cách giải quyết một số vấn đề đang lo ngại nhất của blockchain: bảo mật và khả năng mở rộng.

Những phát hiện này đặc biệt nhấn mạnh tầm quan trọng của quyền riêng tư, bởi vì nếu chúng tôi không đạt được Web3 an toàn và có chủ quyền người dùng, thì dữ liệu người dùng có nguy cơ bị khai thác rất lớn. Báo cáo Bảo mật Trực tuyến Toàn cầu của Joseph Johnson[12] cho biết rằng 53% Người dùng Internet quan tâm hơn đến quyền riêng tư trực tuyến của họ so với một năm trước. Khi mối quan tâm ngày càng tăng và Web3 tiếp tục phát triển, ngày càng có nhiều người dùng chú ý hơn đến lợi ích bảo mật của ZKPs.

[12] https://www.statista.com/statistics/1272181/defi-tvl-in-multiple-blockchains/

Ngày càng có nhiều nhà phát triển và người dùng tiền điện tử chú ý đến ZKPs hơn bao giờ hết, cả từ quan điểm phát triển và giao dịch.

Từ góc độ phát triển và giao dịch, ngày càng có nhiều nhà phát triển và người dùng tiền điện tử chú ý đến ZKPs hơn bao giờ hết. Sự chú ý này có thể được phản ánh nhiều hơn trong việc giới thiệu khả năng sử dụng công nghệ ZKPs để đạt được sự bảo mật riêng tư, khả năng mở rộng trong ngắn hạn. Trên DApps, hoặc cả hai. Trên thực tế, Giám đốc sản phẩm Coinbase Surojit Chatterjee đã viết trong bài báo "Dự đoán cho năm 2022"[13] rằng trong số các trường hợp sử dụng mở rộng quy mô và tập trung vào quyền riêng tư, "công nghệ bằng chứng zero knowledge sẽ đạt được sức hút lớn hơn nữa" trong năm nay.

[13] https://blog.coinbase.com/10-predictions-for-web3-and-the-cryptoeconomy-for-2022-745a20a60cd0

ZKPs là không thể thiếu để chia sẻ dữ liệu an toàn, bảo vệ quyền riêng tư trong DeFi

Các phát hiện của báo cáo này cho thấy hơn 54% người dùng tiền điện tử coi quyền riêng tư và bảo mật tài chính là quan trọng nhất, khiến **DeFi trở thành một trường hợp sử dụng ZKPs sắp xảy ra** (trang 16). Điều này đặc biệt quan trọng, như báo cáo gần đây của Chainanalysis14 cho thấy, số lượng các vụ hack DeFi ngày càng tăng. Nếu DeFi thực hiện lời hứa trao cho người dùng quyền kiểm soát giá trị tài sản của họ, thì DeFi cần ZKPs để đạt được sự chia sẻ dữ liệu an toàn, được bảo vệ quyền riêng tư. Một khi việc triển khai ZKPs trở thành tiêu chuẩn,chúng ta cũng có thể mong đợi Tài chính truyền thống ngày càng tham gia nhiều hơn vào DeFi, làm cho tài chính tư nhân hỗ trợ ZKPs trở nên hấp dẫn hơn so với tài chính doanh nghiệp truyền thống.

[14] https://blog.chainalysis.com/reports/2022-defi-hacks/

Nhìn chung, các thành viên của cộng đồng tiền điện tử bày tỏ quan điểm rằng các ZKPs sẽ đóng một vai trò quan trọng trong việc đảm bảo tương lai của DeFi, Web3 và metaverse. Chúng tôi mong muốn được thấy rằng với sự tiến bộ chung của zero knowledge, một Web3 an toàn và được đảm bảo quyền riêng tư dành cho tất cả mọi người cuối cùng sẽ được hiện thực hóa.

Nội dung của báo cáo này được xây dựng bởi Mina Foundation thông qua cuộc khảo sát các cá nhân trong cộng đồng tiền điện tử

Mina Foundation là một công ty phi lợi nhuận cung cấp Mina Protocol, là một blockchain nhẹ nhất trên thế giới. Công ty hỗ trợ giao thức này và cộng đồng của nó bằng cách cấp các khoản tài trợ cho các bên thứ ba có đóng góp đáng kể, duy trì và quản lý cộng đồng và hệ thống mạng.

Về Mina

Mina sử dụng mật mã tiên tiến và zk-SNARKs đệ quy để thay thế rất nhiều phép tính chuyên sâu nhằm thiết kế một chuỗi khối đầy đủ khoảng 22kb, kích thước bằng một vài tweet. Mina là mạng layer 1 thực hiện các hợp đồng thông minh zero knowledge đơn giản dễ lập trình (zkApps). Với các tính năng riêng tư và bảo mật độc đáo cũng như khả năng liên kết với bất kỳ trang web nào thông qua zkApps, Mina đang xây dựng một cổng riêng giữa thế giới thực và tiền điện tử, cũng như tương lai dân chủ, an toàn mà tất cả chúng ta đều xứng đáng có được.

Mina được quản lý bởi Mina Foundation, một tổ chức phi lợi nhuận có trụ sở tại Hoa Kỳ.

Tìm hiểu thêm về Mina và những thành tựu mới nhất của công nghệ zero knowledge:

Trang web chính thức:
https://minaprotocol.com/

Twitter:
https://twitter.com/minaprotocol

Tuyên bố từ chối trách nhiệm: Thông tin được trình bày trong bài viết này là kết quả cuộc khảo sát từ các thành viên của cộng đồng Mina Foundation.

Các tuyên bố có thể hướng tới tương lai và không phải là đảm bảo về kết quả trong tương lai.

Mọi thắc mắc về phương tiện truyền thông vui lòng liên hệ:

Sarah Cohen
(310) 260-7901
Sarah@MelrosePR.com

Trích dẫn

được liệt kê theo thứ tự số trang xuất hiện

p4 "EY releases third-generation zero-knowledge proof blockchain technology to the public domain" *Business Insider*, 18 Dec. 2019. https://markets.businessinsider.com/news/stocks/ey-releases-third-generation-zero-knowledge-proof-blockchain-technology-to-the-public-domain-1028774016

p4 "The Future of Privacy in Tech | Illuminate: Genesis Summit" *YouTube*, Mina Protocol, 17 June 2021. https://www.youtube.com/watch?v=3Cl9pSwjoaA

p4 Sullivan, Mark. "Epic Games CEO Tim Sweeney Talks the Metaverse, Crypto, and Antitrust." *Fast Company*, 22 Apr. 2022, https://www.fastcompany.com/90741893/epic-games-ceo-tim-sweeney-talks-the-metaverse-crypto-and-antitrust

p4 Buterin, Vitalik. "An Approximate Introduction to How Zk-Snarks Are Possible." *Vitalik Buterin's Website*, 26 Jan. 2021 https://vitalik.ca/general/2021/01/26/snarks.html

p6 Shen, Maria. "Electric Capital Developer Report (2021)." *Medium,* Electric Capital, 28 Jan. 2022 https://medium.com/electric-capital/electric-capital-developer-report-2021-f37874efea6d

p10 Bareckas, Karolis. "Would You Join the Metaverse?" *NordVPN,* 7 Apr. 2022 https://nordvpn.com/blog/metaverse-survey/

p11 "Crypto Theses for 2022—Messari.io." Edited by Ryan Selkis, *Messari,* 2021 https://messari.io/pdf/messari-report-crypto-theses-for-2022.pdf

p11 "Dapp Industry Report: Q1 2022 Overview." *DappRadar Blog RSS*, 6 Apr. 2022 https://dappradar.com/blog/dapp-industry-report-q1-2022-overview

p12 Bareckas, Karolis. "Would You Join the Metaverse?" *NordVPN,* 7 Apr. 2022 https://nordvpn.com/blog/metaverse-survey/

p13 Johnson, Joseph. "Topic: Online Privacy Worldwide." *Statista*, 1 June 2021 https://www.statista.com/topics/8002/online-privacy-worldwide/#dossierKeyfigures

p15 "Timeline of Cyber Incidents Involving Financial Institutions." *Carnegie Endowment for International Peace* https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

p15 Olivo, Lorence. "7 Social Media Sites and Their Data Breaches." *HumanID*, 22 July 2021 https://human-id.org/blog/biggest_social_media_breach_history/

p15 Jennings, Mike. "Top Data Breaches and Cyber Attacks of 2022." *TechRadar*, 26 Apr. 2022 https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022

p15 "Defi Hacks Are on the Rise" *Chainalysis Blog*, 14 Apr. 2022 https://blog.chainalysis.com/reports/2022-defi-hacks/

p15 Heiligenstein, Michael X. "Facebook Data Breaches: Full Timeline through 2022." *Firewall Times*, 21 Mar. 2022 https://firewalltimes.com/facebook-data-breach-timeline/

p15 Bischoff, Paul. "Government Breaches–Can You Trust the US Government with Your Data?" *Comparitech*, 21 Jan. 2022 https://www.comparitech.com/blog/vpn-privacy/us-government-breaches/

p17 Johnson, Joseph. "Topic: Online Privacy Worldwide." *Statista*, 1 June 2021 https://www.statista.com/topics/8002/online-privacy-worldwide/#dossierKeyfigures

p17 Chatterjee, Surojit. "10 Predictions for Web3 and the Cryptoeconomy for 2022." *Coinbase Blog*, 30 Dec 2021 https://blog.coinbase.com/10-predictions-for-web3-and-the-cryptoeconomy-for-2022-745a20a60cd0

p17 "Defi Hacks Are on the Rise" *Chainalysis Blog*, 14 Apr. 2022 https://blog.chainalysis.com/reports/2022-defi-hacks/

Mina Foundation