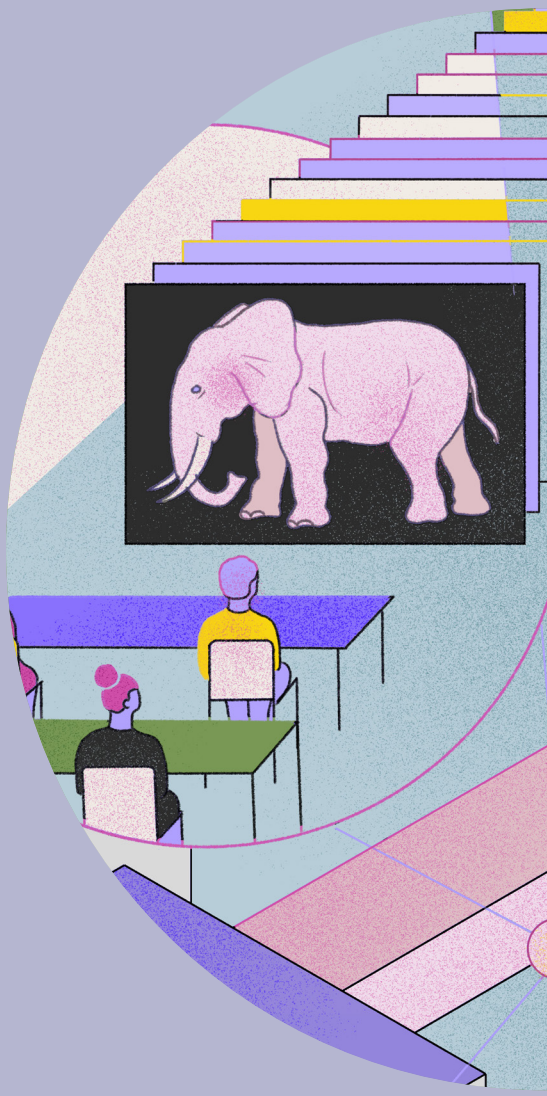
2022
零知识调查报告

解析加密业界对零知识的见解
及其未来的意义。

Mina Foundation

内容——



——关于这份报告

未来当我们回首ZKP*工业化，
它会是私有链向公有链大规模
转变的关键里程碑。

— Paul Brody
安永区块链
技术负责人

***ZKP 的定义**
zero knowledge proof
(零知识证明) 的缩写。
一种密码学原语，对信息进行证明和验证，但不暴露其背后的信息，只显示声明是否真实。

如果让我预测五年或十年后，我想那时
的话题将离不开零知识证明.....
以及隐私功能的技术和实现，就像三五
年前大家谈论区块链那样。

— Jill Gunter
Slow Ventures
负责人

零知识证明这个领域，在保持运行去中心化
系统的同时，为许多加密货币提供隐私保护
功能，我认为它将成为下世纪大部分技术的
重要支柱。

— Tim Sweeney
Epic Games
首席执行官

过去十年里，最强大的密码技术也许是通用
简洁的零知识证明。

— Vitalik Buterin
以太坊
联合创始人

零知识证明 (ZKP) 最强大的两个应用是:
可扩展性和隐私安全性

可扩展性

通过零知识证明，可以将许多数据点封装在一个轻量级的证明中，从而大大提高效率和可扩展性。由于大部分区块链需要大量算力，区块链技术仍受限于此类基础设施，因此限制了其扩展能力。通过利用零知识证明，开发者可以设计能够在更常见的硬件（如移动设备）上运行的轻量级dapp，从而开创更易于访问和可扩展的Web3未来。

隐私安全性

通过零知识证明， 用户可以安全地共享对商品或服务的必要信息，从而获得的访问权，但不会泄露可能使用户受到黑客攻击、剥夺或盗用身份的个人详细信息。零知识证明的数据隐私功能对Web3的安全和保障尤为重要，其中包括DeFi、DAO和元宇宙。对于隐私安全、用户主权的Web3而言，随着数字领域和现实世界的关联越来越紧密，零知识证明技术将变得更加重要。

鉴于人们对零知识证明的兴趣日益增长，并希望实现隐私安全、用户主权的Web3，Mina Foundation于2022年实施了一项调以更好地了解ZKP的发展前景。

理论方法

本报告内容基于由 Mina Foundation 成员创建、分发和分析的调查结果。Mina Foundation 设计提出了若干个问题，旨在归纳业界对零知识 (ZK) 的总体看法。

该调查通过Mina生态成员及业内主要意见领袖运营的社交媒体和社区渠道进行传播，这些意见领袖表现出了与受众一起探索ZK的浓厚兴趣。调查为期3周，共有1,978人参与*。

*据*Mina Foundation*据计，该样本收集了该领域超过1%的*Web3*开发者的看法和观点。根据*Electric Capital 2021*年报告显示，全球共有*18,416*名*Web3*开发者，本报告约对*218*名开发者进行了调查。

调查参与者

参与者被问及三个问题来评估样本的多样性。

调查参与者的身份?

调查参与者被要求从加密社区成员、加密交易者和开发者中选出最能代表他们的身份。

结果显示，67%的受访者确定为加密交易员，22%确定为加密社区成员，11%确定为开发者。

调查参与者的年龄?

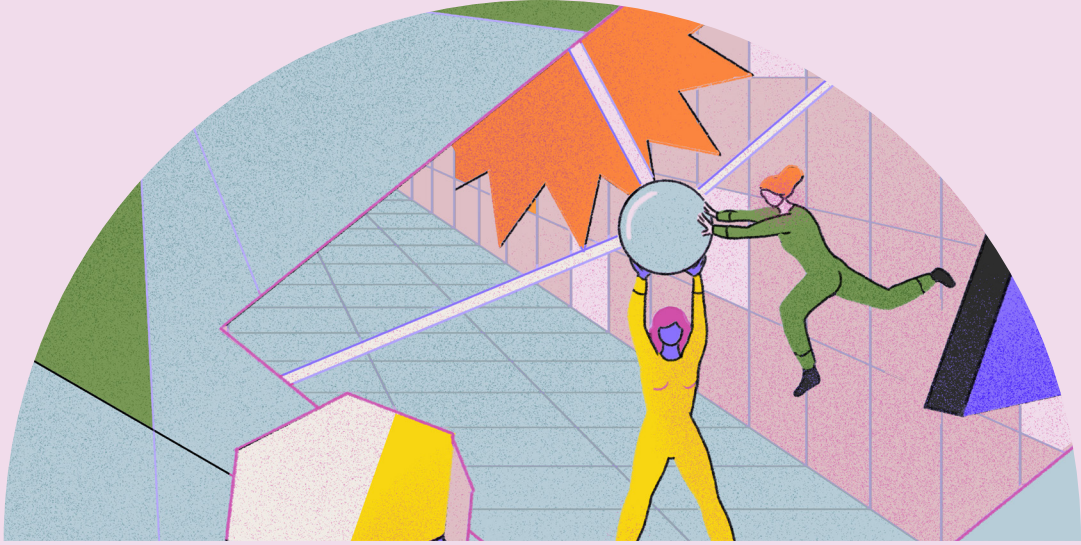
86%的受访者年龄在19至45岁之间。

你熟悉零知识证明技术 (ZKP) 吗?

75.8%的受访者至少说过ZKP并知道其含义，24.2%的受访者不知道其含义。

此外，80%的开发者表示熟悉ZKP技术，显示了开发者使用ZKP进行开发的动力。

根据调查参与者的人群统计数据，报告结果体现了2022年第一季度中一般加密交易者和加密社区角度下的ZKP总体情绪。



——主要发现

零知识证明在以下领域很关键：

元宇宙和 Web3

42.2% 的受访者认为零知识证明对元宇宙和Web3的未来非常重要。

加密货币选择

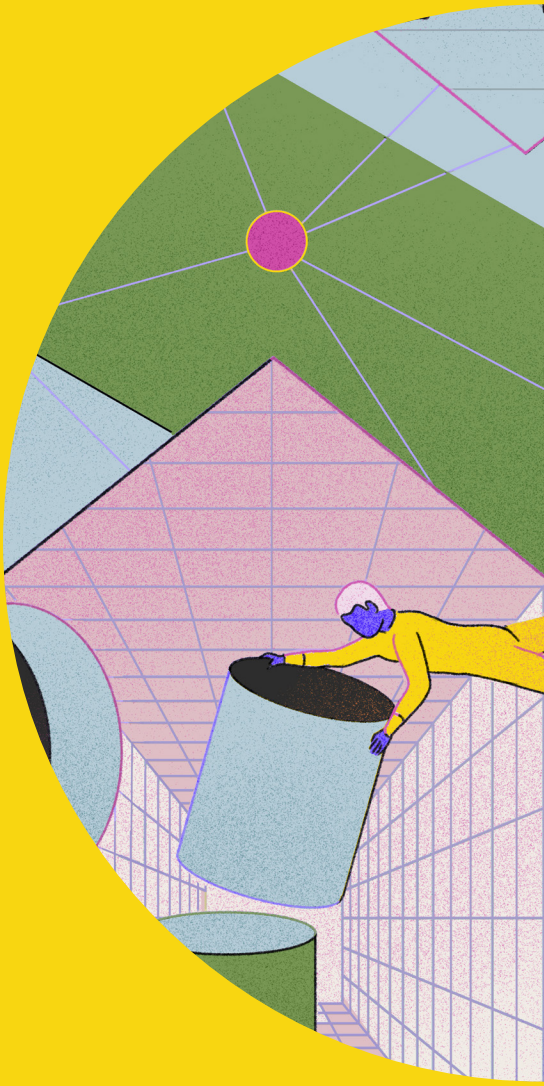
90.1% 的受访者认为利用零知识证明技术的加密货币更具吸引力。

金融行业

40.6% 的受访者认为金融业是最需要零知识证明的行业。

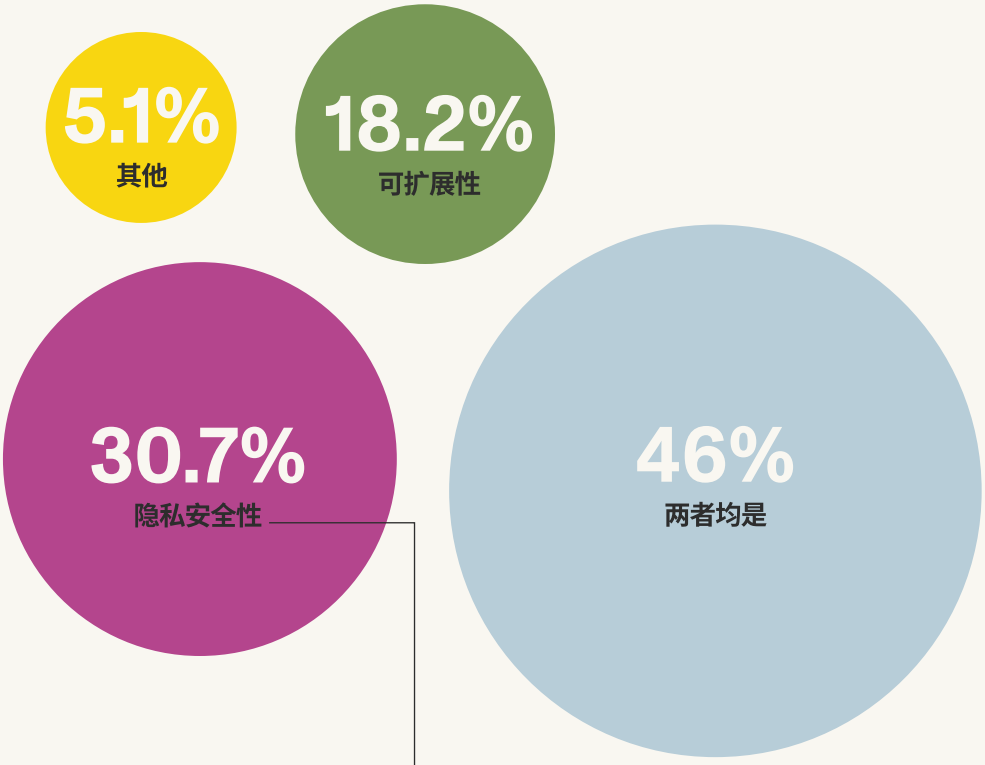
隐私保护

30.7% 的受访者认为隐私安全是零知识证明的主要优势。



——调查结果

你认为零知识证明的主要优势是什么？



隐私问题

当被问及ZKP在应用方面的主要优势时，46%的受访者回答了隐私和可扩展性两个方面；然而，在隐私性和可扩展性之间，隐私性获得的回应略多，为30.7%，而可扩展性为18.2%。**这种对隐私而非可扩展性的轻微偏好可能反映了加密货币行业对隐私的日益关注，这可能是由于人们越来越关注元宇宙中的中心化和企业参与。**

事实上，NordVPN[1]最近的一项调查表明，87%的受访者对自己在元宇宙中的隐私安全表示担心。有趣的是，迄今为止，大多数其他基于ZK的解决方案都将重点放在了可扩展性而非隐私安全性上。

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

使用零知识证明技术的加密货币
是否更有吸引力？

是

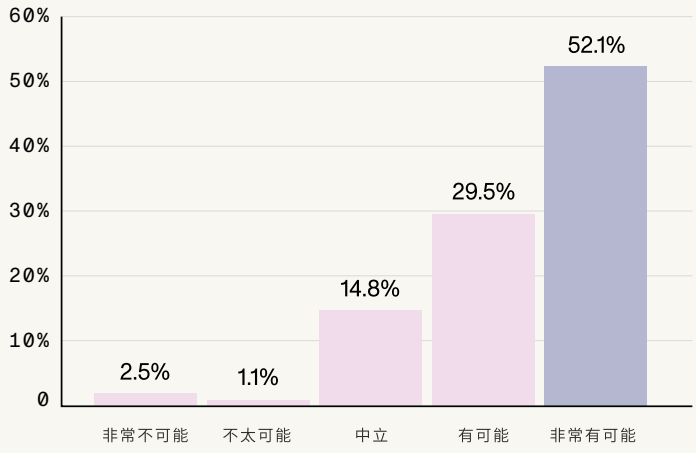
90.1%

否

9.9%

90%的调查参与者压倒性地认为，使用ZKP的加密货币比不使用ZKP的加密货币更具吸引力。这可能反映出人们对隐私问题的日益关注，尤其是在元宇宙的兴起前后（如第12和13页所述）。 同样， **2022年Messari Crypto论文报告[2]预测，“在将来，所有加密货币都将走向零知识加密”。**

如果你知道某个DAPP具备隐私安全性或可扩展性的ZKP特性，你会更愿意使用它吗？

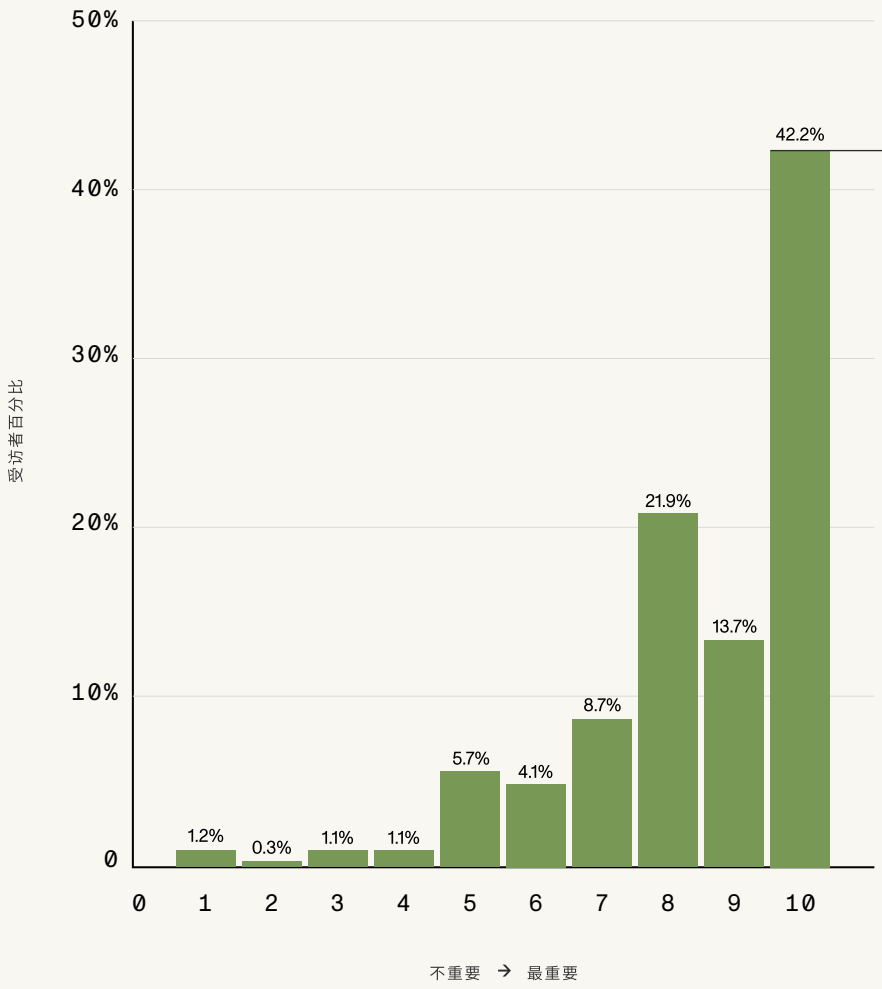


当被问及是否愿意使用具有ZKP优势的dapp时，**52.1%的受访者表示他们更愿意使用具有ZKP优势的dapp。这可能表明加密社区成员相信ZKP的隐私和安全优势，**尤其考虑到近期的区块链安全漏洞事件，仅2022年第一季度，就有12亿美元被盗[3]。

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

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

ZKP在WEB3.0和元宇宙中有多重要？



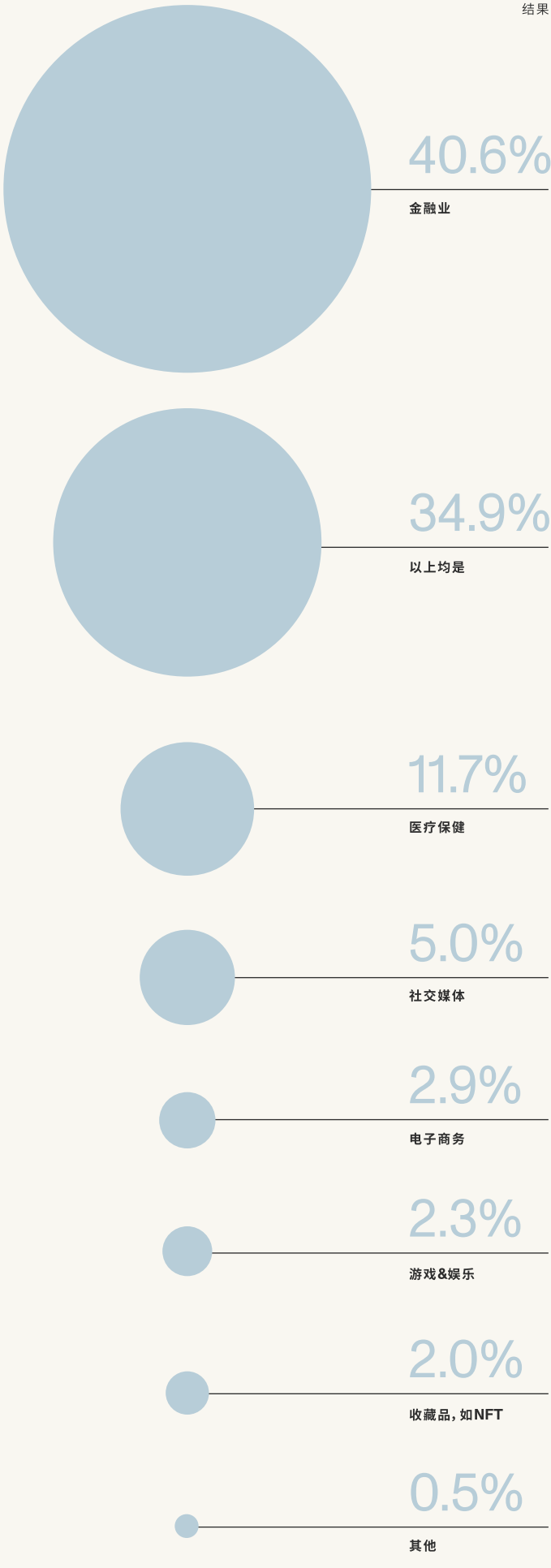
42.2%的受访者表示，ZKP在元宇宙和Web3中的重要性最高，其中**77.7%**的受访者给出的重要性得分为8分或以上。鉴于Epic、Roblox、Microsoft和Meta（前Facebook）**等大公司对元宇宙的高度关注，这些数据表明了加密社区对元宇宙公司控制权的日益担忧。**NordVPN[4]最近的一项研究表明，47%的互联网用户不相信自己的身份信息会受到保护。如果用户无法掌控自己在元宇宙中的身份和数据，用户数据将很有可能被利用，进一步体现了更多用户在进入元宇宙时的顾虑。

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

“我认为ZKP正是当今大多数区块链所缺少的”

— 调查参与者

零知识证明的整合最能服务于哪个行业？



最终结果显示，调查参与者认为，所有行业，包括金融、医疗保健、社交媒体、电子商务、游戏&娱乐以及收藏品都将从零知识证明中受益，但受访者最感兴趣的是利用零知识证明作为金融解决方案。

随着去中心化金融（DeFi）使用量的增长[5]，**具有可扩展性和隐私安全性优势的零知识应用将有更多的机会提高行业的广泛采用率。**

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

你最想保密的数据类型是什么？

54.5%

金融数据

48.6%

任何类型的个人身份信息

46.7%

我希望尽可能匿名

26.7%

位置

25.8%

健康

13.3%

姓名

10.9%

信用评分

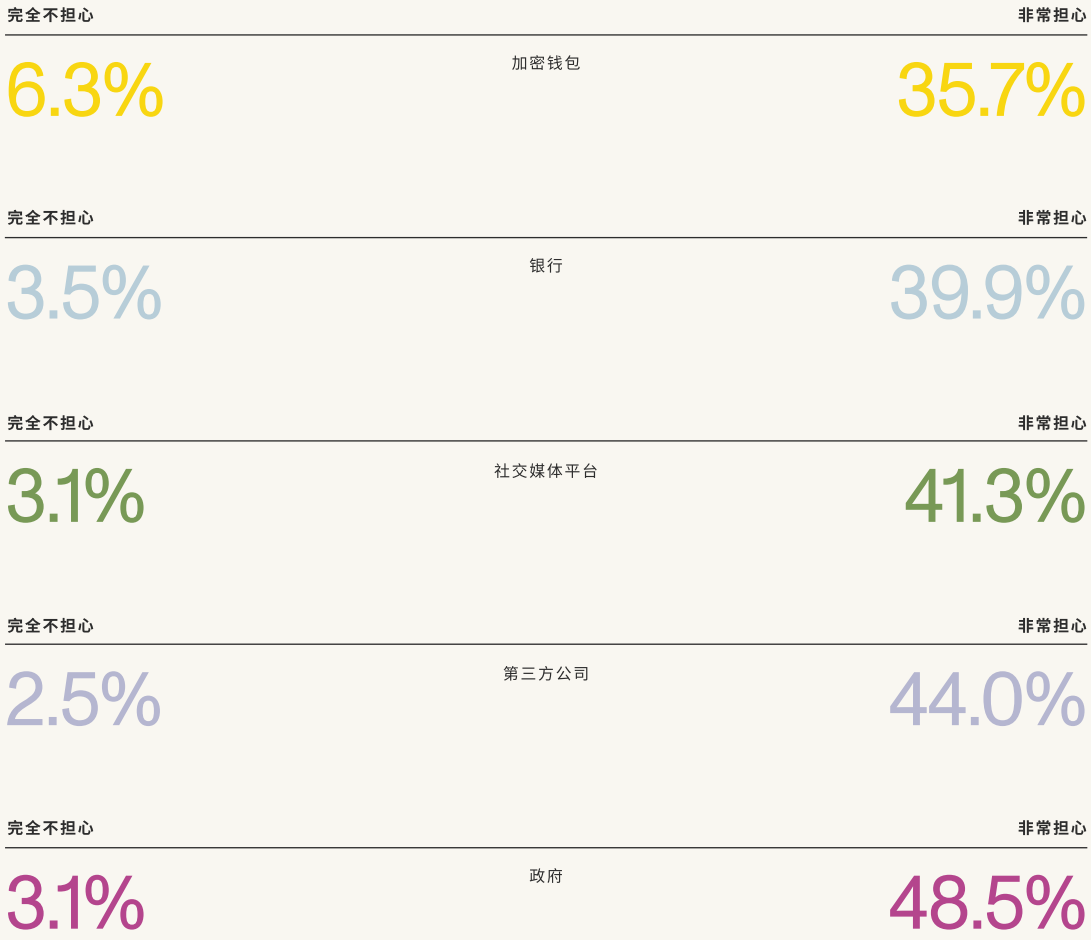
注：此问题要求受访者选出3个选项。

财务隐私

参与者纷纷表示，将所有个人身份信息保密非常重要，但更强调财务数据安全，其中可能包括用户的社会安全号码、加密货币余额、净资产、信用评分等。

比如，利用ZKP创建一个dapp，用户只需共享个人信用评分超过700的证明，即可获得贷款，无需泄漏其他隐私信息。**保持财务数据隐私的重要性意味着ZKP将在Web3和DeFi的未来发挥关键作用。**

对于以下访问个人数据的实体，
你的担心程度是？



受访者最担心的是政府通过任何其他实体访问其个人数据。有趣的是，受访者在所有实体类型中都表达了相当高的担忧。与银行[6]、社交媒体平台[7]和第三方公司[8]相比，钱包的担忧程度最低。

这一点从在DeFi[9]、金融机构、社交媒体平台[10]和政府[11]中发生的各种数据黑客事件和漏洞中可见一斑。

[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/

——结论

从本报告中捕捉到的情绪可以看出，越来越多的加密社区正在寻求通过零知识来解决一些区块链的最大难题：隐私安全和可扩展性问题。

这些发现尤其强调了隐私安全的重要性，因为如果我们不能实现安全且用户主权的Web3，那么用户数据就有极大风险被利用。 Joseph Johnson[12]的《全球在线隐私报告》指出， 53%的互联网用户比一年前更关心他们的线上隐私安全。随着担忧的不断加剧以及Web3的不断发展，越来越多的用户将更加重视ZKP在隐私方面的优势。

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

从开发和交易的角度来看，越来越多的开发者和加密用户也比以往更加关注ZKP。这种关注可能更多体现在推出利用ZKP技术在短期内实现隐私安全性、可扩展性或两者兼而有之的DAPP上。事实上，Coinbase首席产品官Surojit Chatterjee在其文章《2022年预测》[13]中写到，今年规模化和以隐私为中心的用例中，“零知识证明技术将获得更大的吸引力”。

从开发和交易的角度来看，越来越多的开发者和加密用户也比以往更加关注 ZKP。

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

为实现DeFi安全的、保护隐私的数据共享，零知识证明不可或缺。

本报告调查结果显示，超过54%的加密用户认为财务隐私安全是最重要的，由此可见**DeFi是一个迫在眉睫的ZKP用例**（第16页）。这一点尤其重要，正如Chainanalysis[14]的近期报告所示，这是由于DeFi黑客数量正在不断增加。如果DeFi要兑现其赋予用户资产价值控制的承诺，DeFi需要通过ZKP来实现安全、保护隐私的数据共享。一旦ZKP的实现成为常态，我们还可以期待传统金融越来越多地参与DeFi，因为由ZKP赋能的私人金融比传统公司金融更具吸引力。

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

总的来说，加密社区成员表达了一个观点，即零知识证明将对确保DeFi、Web3和元宇宙的未来发挥重要作用。我们期待看到，随着业界零知识技术的普遍进步，人人可用的安全、隐私保障的Web3终将实现。

本报告内容由Mina Foundation通过向
加密社区内的个体进行的调查构成

Mina Foundation是一家公益性公司，服务于全球最轻量区块链Mina Protocol。基金会通过向做出重大贡献的第三方发放资助金、维护和管理社区以及网络健康来支持协议及其社区的发展。

关于Mina

Mina使用先进的密码学和递归 zk-SNARK 取代大量密集计算，设计一个约为22kb的完整区块链，相当于几条推文的大小。

Mina是实现简易编程性零知识智能合约(zkApp)的一层网络。凭借其独特的隐私和安全功能及其通过zkApp 与任何网站链接的能力，Mina 正在构建现实世界和加密货币之间的私人网关，以及我们所有人都应得的安全、民主的未来。

Mina 由总部位于美国的非营利组织 *Mina Foundation* 管理。
了解有关*Mina*的更多信息及零知识的最新进展：

官网：
https://minaprotocol.com/
推特：
https://twitter.com/minaprotocol

免责声明：
本文提供的信息包括Mina Foundation社区成员的调查结果。

陈述有可能是前瞻性的，不作为未来业绩的保证。

媒体咨询请联系：

Sarah Cohen
+1 (310) 260-7901
Sarah@MelrosePR.com

引用

按出现页码顺序列出

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