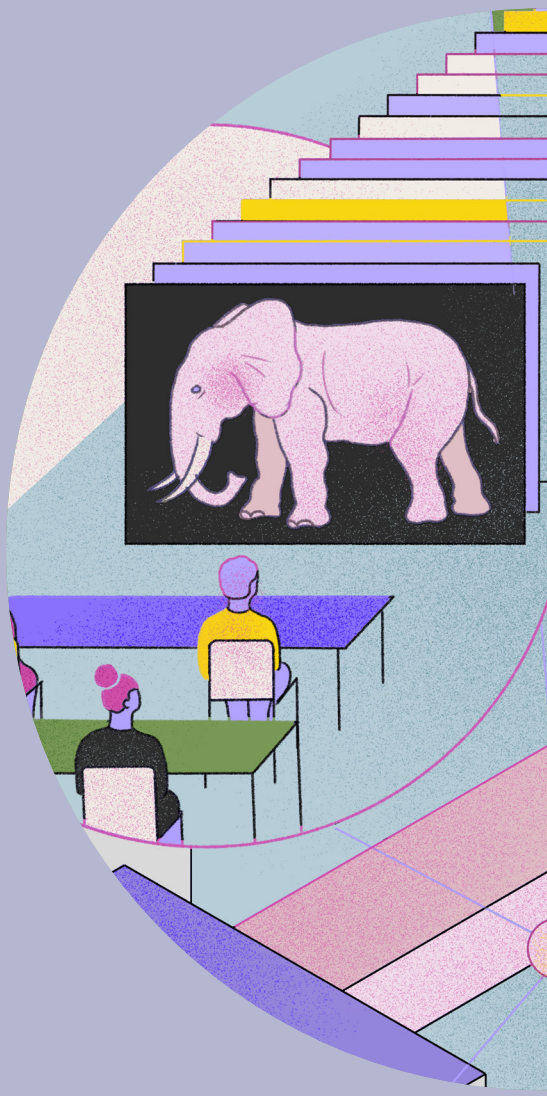
Состояние Zero Knowledge Отчет 2022

Узнайте мнения в крипто индустрии на нулевое разглашение и что это принесет в будущем.

Mina Foundation

Содержание—



Об этом отчете

“Я верю, что мы будем вспоминать индустриализацию ZKPs* как ключевую веху в широкой миграции предприятий от частных к публичным блокчейнам”.

— Пол Броуди
Лидер EY по глобальному блокчейну

“Если бы я мог прогнозировать на 5, 6, 7, 8, 9, 10 лет вперед. я думаю, что мы будем говорить о технологии нулевого разглашения и ... всех технологиях конфиденциальности о технологиях и их реализациях точно так же, как люди говорили о блокчейн 3, 4, 5 лет назад”

— Джилл Гюнтер
Директор Slow Ventures

“Область доказательств нулевого разглашения, которая обеспечивает работу ряда криптовалют в защите конфиденциальности при работе децентрализованной системы, я думаю, что это будет основой значительной части следующего века технологий”.

— Тим Суини
Генеральный директор Epic Games”

“Возможно, самая мощная криптографическая технология, появившаяся в последнее десятилетие - это лаконичные доказательства общего назначения нулевых оказательств с нулевым разглашением”.

— Виталик Бутерин
Сооснователь Ethereum

*ZKPs **Определение**
zero knowledge proof
Аббревиатура для доказательства с нулевым разглашением. Криптографический примитив, который позволяет доказать и подтвердить информацию без её раскрытия, не раскрывая сведений, лежащих в ее основе, только показывая, истинно ли утверждение или нет.

Два самых мощных применения Доказательств с нулевым разглашением (ZKPs) - это масштабируемость и конфиденциальность:

Масштабируемость
ZKPs позволяют инкапсулировать множество данных в одном, легком доказательстве, что значительно повышает эффективность и масштабируемость. Поскольку многие блокчейны требуют больших вычислений, технология блокчейн остается ограниченной в такой инфраструктуре, “что” так-же ограничивает способность её масштабирования. “Используя” ZKPs, разработчики могут создавать легковесные dapps, которые могут работать на более простом оборудовании например, на мобильных устройствах, открывая тем самым будущее, более доступного и масштабируемого Web3.

Конфиденциальность
ZKPs позволяют пользователям безопасно обмениваться необходимой информацией для получения доступа к товарам или услугам, не раскрывая личных данных, которые могут сделать пользователя уязвимым для взлома, эксплуатации или кражи личных данных. Возможности ZKPs по обеспечению конфиденциальности данных особенно важны для безопасности и безопасности Web3, включая DeFi, DAOs, и метавселенной. Поскольку цифровая и физическая сферы все больше переплетаются, ZKP будут становиться все более важными для частного, контролируемого пользователями Web3.

В свете очевидной и растущей заинтересованности в том, чтобы ZKPs обеспечивал приватность и безопасность под контролем пользователей Web3, Mina Foundation провел опрос, чтобы лучше понять понимание перспектив, связанных с ZKP в 2022 году.

Методология

Данный отчет основан на результатах опроса, созданного, распространенном и проанализированном участниками Mina Foundation. Mina Foundation создал вопросы, разработанные для того, чтобы собрать настроения в отрасли относящиеся к нулевому разглашению (ZK).

Опрос был распространен по профильным СМИ и каналам сообществ управляемых участниками Mina Ecosystem а также ключевыми лидерами мнений в индустрии, которые продемонстрировали интерес к изучению ZK среди своей аудитории. Опрос был открыт в течение 3 недель, за это время 1 978 человек приняли участие*.

**Mina Foundation оценивает, что эта выборка отражает настроения более 1% от общего числа Web3 разработчиков в этом сегменте. Это соответствует отчету Electric Capital за 2021 год в котором указано 18 416 разработчиков Web3 по всему миру а данный отчет фиксирует ~218 разработчиков.*

Участники опроса

Участникам было задано три вопроса для оценки разнообразия в выборке.

Как вы идентифицируете себя?

Участникам опроса было предложено выбрать, что лучше всего описывает их: участник сообщества, крипто-трейдер или разработчик. 67% респондентов назвали себя крипто-трейдерами, в то время как 22% идентифицировали себя участниками криптосообщества и 11% как разработчики.

Каков ваш возраст?

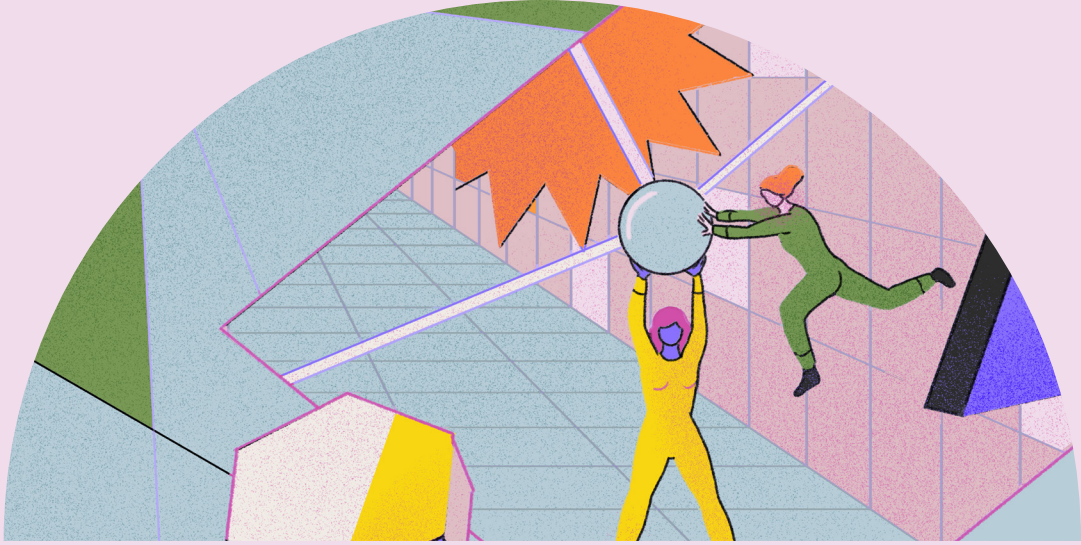
86% респондентов были в возрасте от 19 до 45 лет.

Знакомы ли вы с технологией ZKP?

75,8% респондентов по крайней мере слышали о ZKP и знают, что это такое, в то время как 24,2% не знают, что что означает ZKP.

Кроме того, 80% разработчиков заявили о своем знакомстве с технологией ZKP, что свидетельствует о желании разработчиков создавать продукты с ипользованием этой технологии

Основываясь на демографических данных участников опроса, результаты представленные в данном отчете, отражают всеобъемлющее отношение к ZKPs с точки зрения криптотрейдера в целом и с точки зрения сообщества в течение 1 квартала 2022 года.



Ключевые особенности

ZKP являются ключом к:

метавселенным и Web3

42,2% респондентов рассматривают ZKP как важный компонент для будущего метавселенных и Web3.

выбору криптовалют

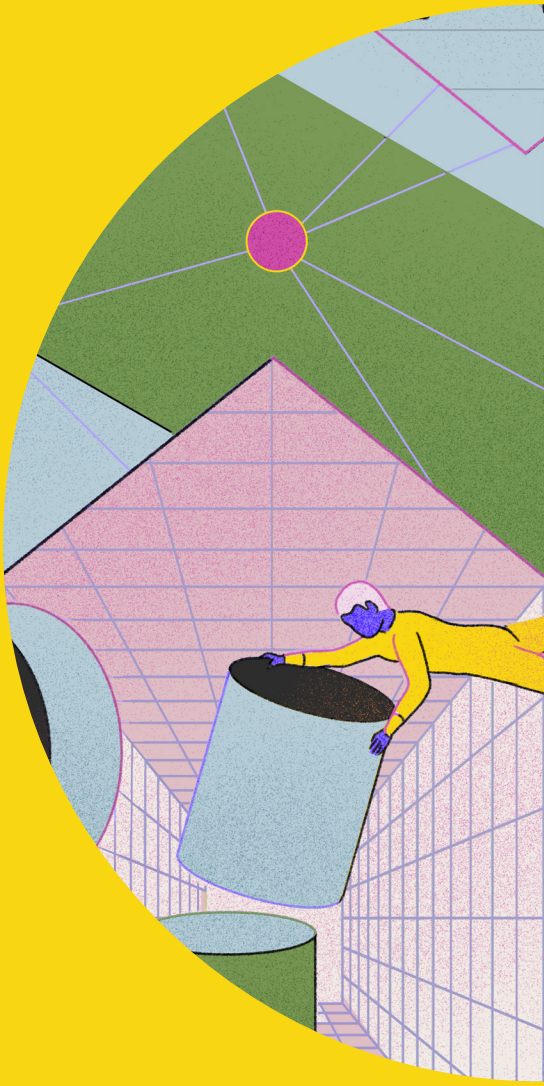
90,1% респондентов считают, что криптовалюты,использующие ZKP, являются более привлекательными.

финансовой индустрии

40,6% респондентов рассматривают финансы как отрасль, наиболее нуждающуюся в ZKP.

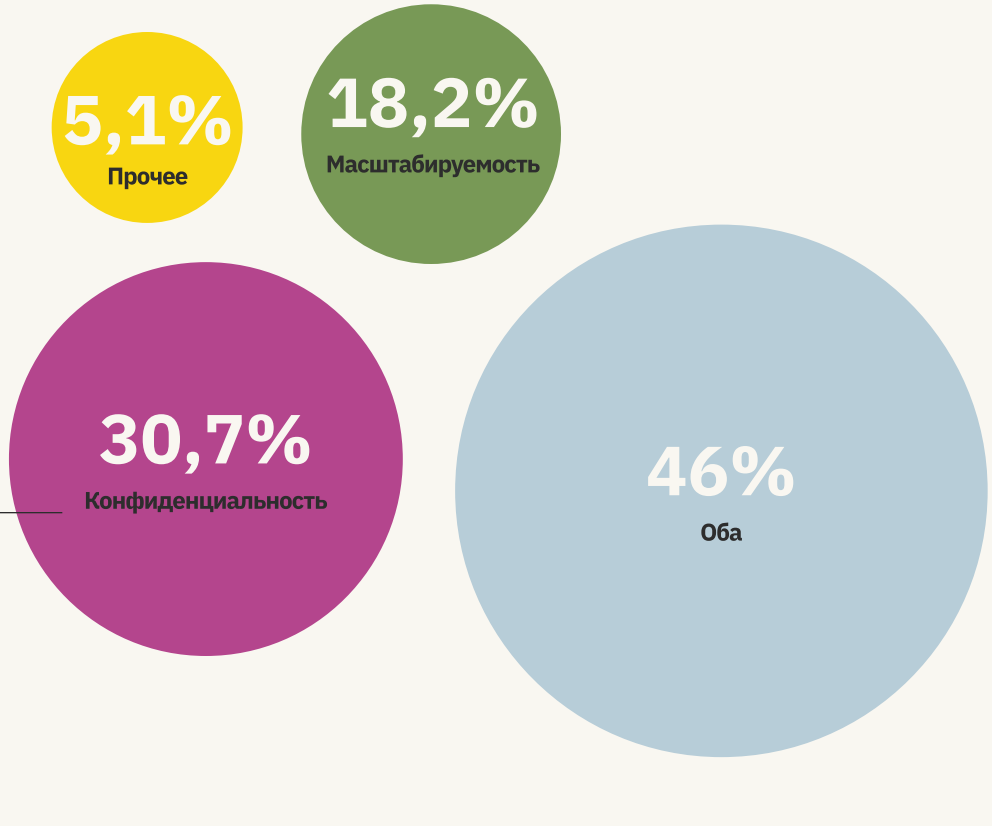
конфиденциальности и защите

30,7% респондентов считают конфиденциальность главным преимуществом ZKP.



—Результаты

В ЧЕМ ГЛАВНОЕ ПРЕИМУЩЕСТВО ДОКАЗАТЕЛЬСТВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ ПО ВАШЕМУ МНЕНИЮ?



Вопросы конфиденциальности
На вопрос о том, что является основным преимуществом ZKP для приложений, 46% респондентов ответили, что и конфиденциальность и масштабируемость; однако между конфиденциальностью и масштабируемостью, конфиденциальность получила немного больше ответов - 30,7% по сравнению с 18,2% ответов на вопрос о масштабируемости. **Такое незначительное предпочтение конфиденциальности перед масштабируемостью может быть отражением того, что криптовалютная индустрия испытывает повышенное внимание, уделяемое конфиденциальности, что, возможно, вызвано растущим беспокойством по поводу централизованного, корпоративного вмешательства в метавселенную.** Действительно, недавнее исследование, проведенное NordVPN[1], показало, что 87% респондентов были обеспокоены по поводу своей конфиденциальности в метавселенной. Интересен тот факт, что большинство других решений на базе ZK на сегодняшний день сосредоточены на масштабируемости, а не на конфиденциальности.

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

ЯВЛЯЮТСЯ ЛИ КРИПТОВАЛЮТЫ, ИСПОЛЬЗУЮЩИЕ ZKP БОЛЕЕ ПРИВЛЕКАТЕЛЬНЫМИ?

ДА

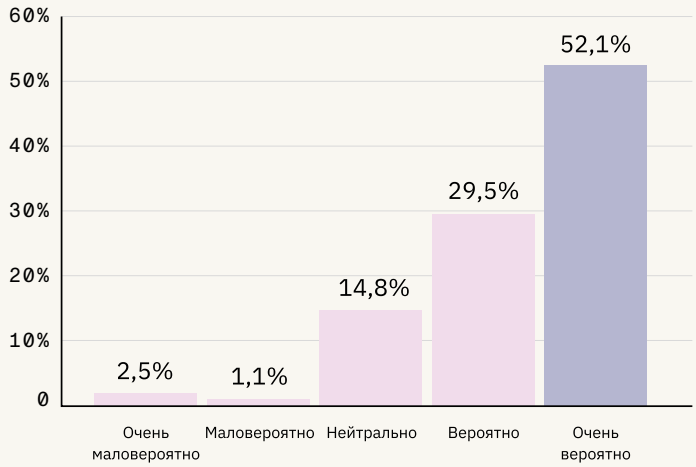
90,1%

НЕТ

9,9%

Подавляющее большинство 90% участников опроса считают, что криптовалюты, использующие ZKP, являются более привлекательными, чем те, которые не используют её. Это может быть отражением растущей обеспокоенности по поводу конфиденциальности, особенно в связи с ростом метавселенных (как упоминалось на страницах 12 и 13). Аналогично, **в отчете Messari от 2022 года предсказывают, что “В долгосрочной перспективе, все цифровые валюты придут к криптовалюте с нулевым разглашением”.**

БУДЕТЕ ЛИ ВЫ ОХОТНЕЕ ИСПОЛЬЗОВАТЬ DAPP, ЕСЛИ БЫ ВЫ ЗНАЛИ, ЧТО ОН ПРЕДЛАГАЕТ ZKP ПРЕИМУЩЕСТВА, ТАКИЕ КАК КОНФИДЕНЦИАЛЬНОСТЬ ИЛИ МАСШТАБИРУЕМОСТЬ?

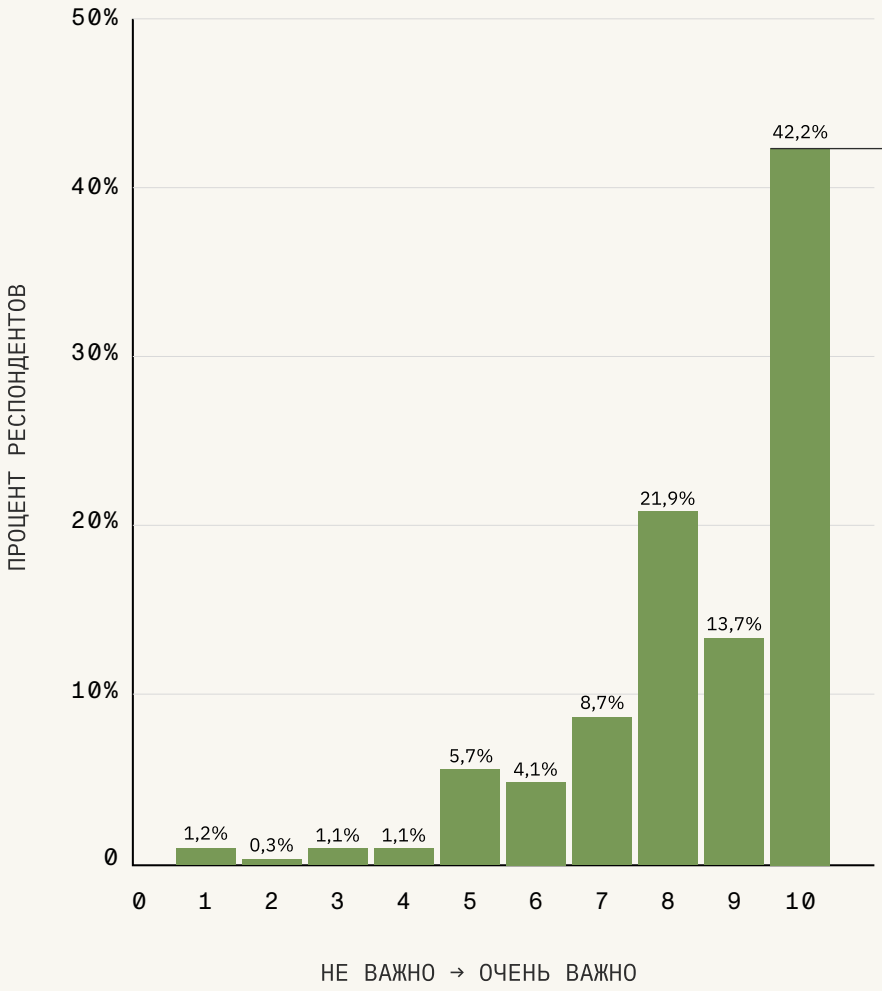


Когда респондентов спрашивали об их готовности использовать dapps с ZKP преимуществами, **52,1% респондентов заявили, что они охотнее использовали бы dapp, если бы у него были преимущества ZKP.** Это может свидетельствовать о том, что участники криптосообщества доверяют преимуществам ZKP в области приватности и конфиденциальности, особенно в связи с недавними взломами, когда только в 1 квартале 2022 года было похищено 1,2 млрд. долл.

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

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

НАСКОЛЬКО ВАЖНЫМ БУДЕТ ZKP В WEB 3.0 И METAVERSE?.



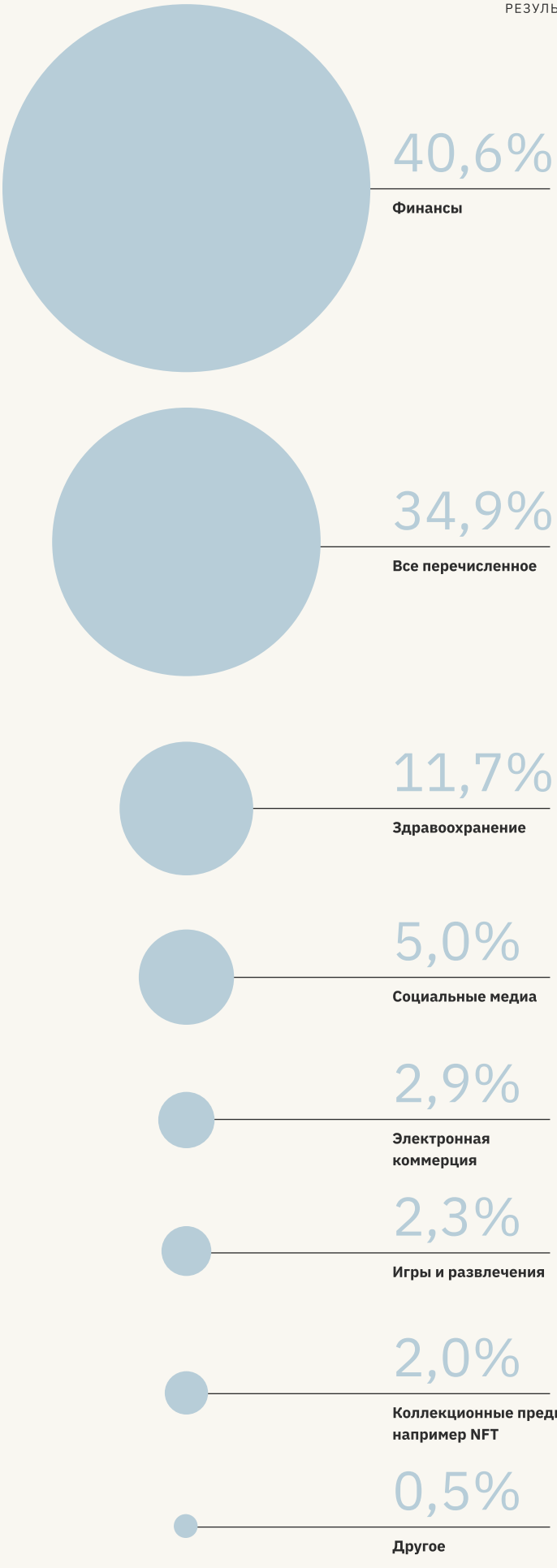
42,2% респондентов отметили, что ZKP будут иметь наибольшее значение в metaverse и Web3, при этом **77,7%** респондентов оценили его на 8 баллов или выше по важности. В свете того внимания, которое уделяется metaverse крупными компании, такие как Epic, Roblox, Microsoft, и Meta (бывший Facebook), **эти данные подтверждают растущие опасения которые испытывает криптосообщество по поводу корпоративного контроля над metaverse.** Недавнее исследование, проведенное NordVPN[4] показало, что 47% интернет-пользователей пользователей не верят, что их личные данные будут будут защищены. Без возможности пользователей контролировать свои личные данные и данными в metaverse, пользовательские данные будут уязвимы для эксплуатации –что еще больше указывает на нерешительность в принятии metaverse большого количества пользователей.

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

“Я думаю, что ZKP–это то, чего не хватает большинству блокчейнов сегодня”

— участник опроса

КАКАЯ ОТРАСЛЬ МОЖЕТ ЛУЧШЕ РАБОТАТЬ ПРИ ВКЛЮЧЕНИИ В НЕЕ ДОКАЗАТЕЛЬСТВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ?



“В конечном счете, участники опроса считают, что все отрасли, включая финансы, здравоохранение, социальные сети, электронная коммерция, гейминг и развлечения, а также коллекционные предметы могут извлечь выгоду из ZKP, но респонденты были наиболее заинтересованы в использовании ZKP в качестве решения для финансов.

Поскольку число случаев использования децентрализованных финансов (DeFi) постоянно растет, **приложения с нулевым разглашением и масштабируемостью могут быть полезны в сфере финансов. Приложения с нулевым разглашением, обладающие преимуществами масштабируемости и конфиденциальности, имеют возможность помочь повысить более широкое внедрение в отрасль.**

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

В КАКОМ ТИПЕ ДАННЫХ ВЫ БОЛЬШЕ ВСЕГО ХОТИТЕ СОХРАНИТЬ КОНФИДЕНЦИАЛЬНОСТЬ?

54,5%

Финансовый

48,6%

Любая персонально идентифицируемая информация

46,7%

Я хочу быть настолько анонимным, насколько это возможно

26,7%

Местонахождение

25,8%

Здравоохранение

13,3%

Имя

10,9%

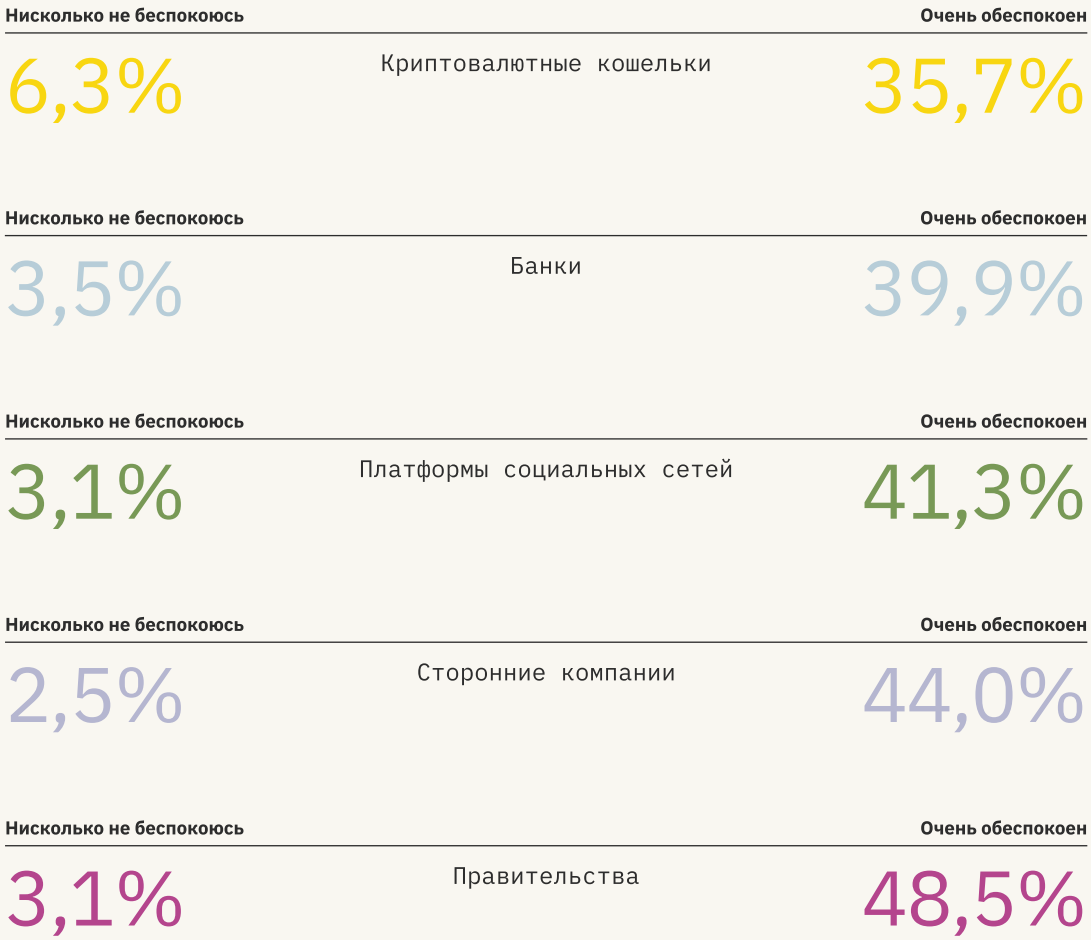
Кредитный рейтинг

Примечание: Респондентов попросили выбрать до 3 вариантов из этого вопроса.

Финансовая конфиденциальность
Многие участники также отметили что важно хранить всю личную информацию в тайне, но больший акцент был сделан на финансовых данных, которые могут включать в себя номер социального страхования, баланс криптовалюты, сумму чистой прибыли, кредитный рейтинг и т.д.

В качестве примера, ZKP можно использовать для создания dapp, который позволяет пользователям просто поделиться доказательством того, что их кредитный рейтинг выше 700, чтобы получить кредит, вместо предоставления всей своей частной информации. **Важность сохранения конфиденциальности финансовых данных подразумевает, что ZKPs будут играть ключевую роль в будущем Web3 и DeFi".**

НАСКОЛЬКО ВЫ ОБЕСПОКОЕНЫ ТЕМ,
КТО ИМЕЕТ ДОСТУП К ВАШИМ ДАННЫМ?



Респонденты больше всего обеспокоены по поводу доступа к данным от правительств, чем от любой другой организации. Интересно, что респонденты выразили довольно сильное беспокойство по всем типам организаций, хотя крипто-кошельки вызывают наименьшую озабоченность по сравнению с банками, платформами социальных сетей и сторонними компаниями.

Это показательно в свете различных взломов и утечек данных, которые произошли со стороны DeFi, финансовых учреждений, платформ социальных сетей, и правительств.

[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/

—Итоги

Настроения, отраженные в этом отчете, показывают, что глобальное криптосообщество смотрит в сторону решений с нулевым разглашением для решения самых больших дилемм: конфиденциальности и масштабируемости.

Полученные результаты особенно подчеркивают растущую важность конфиденциальности в свете огромного потенциала для эксплуатации пользовательских данных, если мы не сможем внедрить безопасные и надежные технологии и если мы не сможем внедрить безопасный и контролируемый пользователями Web3. Всемирный отчет о конфиденциальности в Интернете, подготовленный Joseph Johnson обнаружил, что 53% пользователей Интернета были более обеспокоены своей конфиденциальностью в сети чем год назад. Поскольку обеспокоенность продолжает расти, а Web3 продолжает развиваться, преимущества конфиденциальности, предоставляемые ZKP будут становиться все более важными для широкого круга пользователей".

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

Все больше разработчиков и пользователей криптовалют также обращают внимание на ZKP с точки зрения разработки и торговли сейчас, чем когда-либо прежде. Это внимание вероятно, воплотится в запуске большего количества dapps использующих технологию ZKP для обеспечения конфиденциальности, масштабируемости или и того, и другого в ближайшем будущем. Более того, в своей статье о прогнозах на 2022 год, Surojit Chatterjee, директор по продуктам компании Coinbase, предсказал, что "В этом году технология доказательств с нулевым разглашением получит все большее распространение" для масштабирования и использования в целях обеспечения конфиденциальности.

Все больше разработчиков и пользователей криптовалют также обращают внимание на ZKP с точки зрения разработки и торговых стратегий сейчас, чем когда-либо прежде.

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

DEFI нуждается в безопасном и приватном обмене данными осуществимый благодаря ZKP

Децентрализованные финансы (DeFi) оказываются неотъемлемой областью применения ZKP после того, как результаты этого отчета показали, что более 54% пользователей криптовалют считают наиболее важным важным иметь финансовую конфиденциальность (Страница 16). Это особенно важно, учитывая рост числа взломов DeFi, как показано в недавнем отчете Chainanalysis. Если DeFi действительно выполнит свое обещание - дать пользователям возможность контролировать свою собственную стоимость, DeFi нуждается в безопасном, приватном обмене данными обмен данными, который становится возможным благодаря ZKP. Мы также можем ожидать увеличения числа участников Традиционных Финансов в DeFi, когда внедрение ZKP станет нормой, поскольку частное финансирование, обеспечиваемое ZKP, будет более привлекательным. Также ZKP будут более привлекательным для традиционных корпоративных финансов.

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

В целом, участники криптосообщества выразили мнение, что ZKP сыграют важную роль в обеспечении будущего DeFi, Web3 и metaverse. Мы с нетерпением ждем возможности следить за общим продвижением технологии нулевого разглашения в индустрии, чтобы создать безопасный и приватный Web3, которым сможет пользоваться каждый.

Данный отчет был подготовлен при содействии Mina Foundation путем опроса отдельных участников в криптосообществе

Mina Foundation это общественно-полезная корпорация, обслуживающая Mina Protocol, самый самый легкий в мире блокчейн. Фонд поддерживает протокол и его сообщество путем выдачи грантов третьим лицам, которые вносят значительный вклад, а также путем поддержания и управления сообществом и здоровьем сети.

Об Mina

Вместо применения техноогии brute-force, Мина использует передовую криптографию и рекурсивный zk-SNARKs для создания блокчейна, размер которого составляет около 22 кб, размер пары твитов. Это первый Layer-1, позволяющий эффективно реализовывать и легко программировать смарт-контракты с нулевым разглашением (zkApps). Благодаря своим уникальным функциям конфиденциальности и способностью подключаться к любому веб-сайту, Mina создает частный шлюз между реальным миром и криптовалютами—безопасное, демократическое будущее, которого мы все заслуживаем.

Mina находится под управлением Mina Foundation, общественно-полезная корпорация со штаб-квартирой в Соединенных Штатах.

Чтобы узнать больше о Mina и быть в курсе последних успехах в области нулевых разглашений:

Веб-сайт:
https://minaprotocol.com/

Twitter:
https://twitter.com/minaprotocol

“Отказ от ответственности”: Информация, предоставленная в настоящем документе, включает в себя результат опроса, проведенного среди участников сообщества Mina Foundation

Заявления могут быть прогнозными и не предназначены для гарантии будущих результатов деятельности”.

Для получения информации от СМИ пожалуйста, обращайтесь:

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

Цитаты

перечислены по номерам страниц в порядке появления

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