

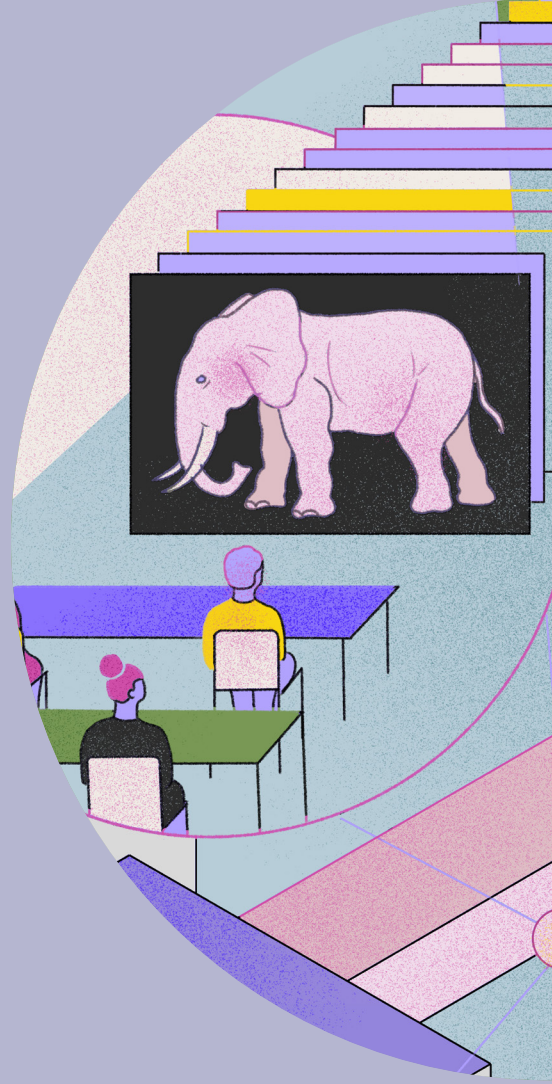
Zero Knowledge Teknolojisi Raporu - 2022

Zero Knowledge (Sıfır Bilgi) hakkında kripto endüstrisinden birçok kişinin görüşlerini ve bu teknolojinin gelecek için ne anlam ifade ettiğini keşfet!

Mina Foundation

İçerik—

Rapor Hakkında	3
Önemli Bulgular	7
Sonuç	9
Son Notlar	16



—Rapor Hakkında

İzinli blokzincirlerden açık blokzincirlere doğru gerçekleşecek kurumsal adaptasyon sürecinde ZKP* teknolojisinin endüstrileşmesine önemli bir köşetaşı olarak bakacağımıza inanıyorum.

— Paul Brody
EY Global
Blokzincir Lideri

***ZKP'lerin Tanımı**
ZKP, Zero Knowledge Proof'un kısaltmasıdır. Zero Knowledge Proof ise, bilgilerin kanıtlanabilir ve doğrulanabilir şekilde paylaşılabilmesini sağlarken, sadece talebe karşılık bilgilerin paylaşılmasına imkan veren bir kriptografi uygulamasıdır.

Eğer bundan 5, 6, 7, 8, 9, 10 yıl sonrasını tahmin edecek olsaydım, sıfır bilgi kanıtları, tüm bu gizlilik odaklı teknolojiler ve bu teknolojilerin entegrasyonu hakkında konuşuyor olurdum.... tıpkı insanların 3, 4, 5, yıl önce blokzincir hakkında konuşmaya başlamış olmaları gibi.

— Jill Gunter
Slow Ventures Yöneticisi

Merkeziyetsiz bir sistem çalıştırırken birçok kripto paraya gizlilik anlamında güç veren Sıfır Bilgi Kanıtları, gelecek yüzyılın teknolojisinin büyük bir parçası haline gelecek.

— Tim Sweeney
Epic Games / CEO

Belki de geçtiğimiz son 10 yılın bize kazandırdığı en güçlü kriptografik teknoloji Sıfır Bilgi Kanıtı teknolojisidir.

— Vitalik Buterin
Ethereum Kurucu Ortağı

Sıfır Bilgi Kanıtlarının (ZKP) en güçlü uygulamaları ölçeklenebilirlik ve gizlilik.



Ölçeklenebilirlik

ZKP'ler birçok verinin büyük ölçekte verimliliğini ve ölçeklenebilirliğini artırarak tek ve hafif bir kanıtta saklanmasına olanak sağlar. Birçok blokzincir yüksek hesaplama gücü gerektirdiğinden blokzincir teknolojisi ölçeklenebilirliği kısıtlayan altyapısı ile tartışılmaktadır. Geliştiriciler ZKP'lerden yararlanarak Web3'ün daha erişilebilir ve ölçeklenebilir olması amacıyla mobil cihazlar gibi daha yaygın donanımlarda çalışabilen küçük boyutlu dapp'ler tasarlayabilirler.

Gizlilik

ZKP'ler ile kullanıcılar, kişisel bilgilerini hacklenme, silinme veya çalınma gibi risklere açık kapı bırakmadan paylaşabilirler. Ve birçok hizmete ve ürüne erişim sağlamak için sadece gerekli bilgileri güvenli bir şekilde paylaşabilirler. ZKP teknolojisinin sahip olduğu veri gizliliğini koruma yetkinlikleri, DeFi, DAO'lar ve metaverse'nin de dahil olduğu Web3 dünyasının güvenliğini sağlamak için oldukça önem arz etmektedir.



Sıfır Bilgi Kanıtlarının (ZKP) en güçlü uygulamaları ölçeklenebilirlik ve gizlilik: ZKP teknolojisine olan ve giderek büyüyen bu ilgi ışığında gizli, güvenli ve kullanıcı kontrollü Web3'ü mümkün kılmak için Mina Foundation, 2022 yılı itibarıyla ZKP teknolojisine olan bakış açısını daha iyi anlamlandırmak için bir anket gerçekleştirdi.

Metodoloji

Bu rapor, Mina Foundation üyeleri tarafından oluşturulmuş, paylaşılmış ve analiz edilmiştir. Mina Foundation, sektörün sıfır bilgi (ZK) teknolojisine ilişkin görüşlerini yansıtmak amacıyla birçok soru oluşturmuştur.

Bu anket, Mina ekosistemi üyeleri ve kendi çevrelerinde ZK teknolojisini keşfetmeye ilgi gösteren sektördeki birçok lider tarafından topluluk ve sosyal medya kanalları aracılığıyla paylaşılmıştır. Anket 3 hafta boyunca cevaplanması için açık kalmıştır ve bu sürede 1,978 kişi ankete katılım göstermiştir*.

*Mina Foundation olarak, bu örnekte sektördeki Web3 geliştiricilerinin %1'inden fazlasının görüşlerinin kapsandığını tahmin ediyoruz. *Electric Capital's 2021* raporuna göre dünya çapında toplam 18,416 Web3 geliştiricisi vardır. Hesaplama bu araştırma temel alınarak yapılmıştır. Bu rapor yaklaşık 218 geliştiriciyi kapsamaktadır.

Anket Katılımcıları

Anket üzerindeki çeşitliliği değerlendirmek amacıyla katılımcılara üç soru soruldu.

Kendinizi nasıl tanımlarsınız?

Anket katılımcılarına, Kripto Topluluğu Üyesi, Kripto Trader'ı ve Geliştirici seçenekleri arasından kendilerini en iyi neyin tanımladığı soruldu.

Anket katılımcılarının %67'si Kripto Trader'ı, %22'si Kripto Topluluk Üyesi ve %11'i ise geliştirici olarak kendilerini tanımladılar.

Kaç yaşındasınız?

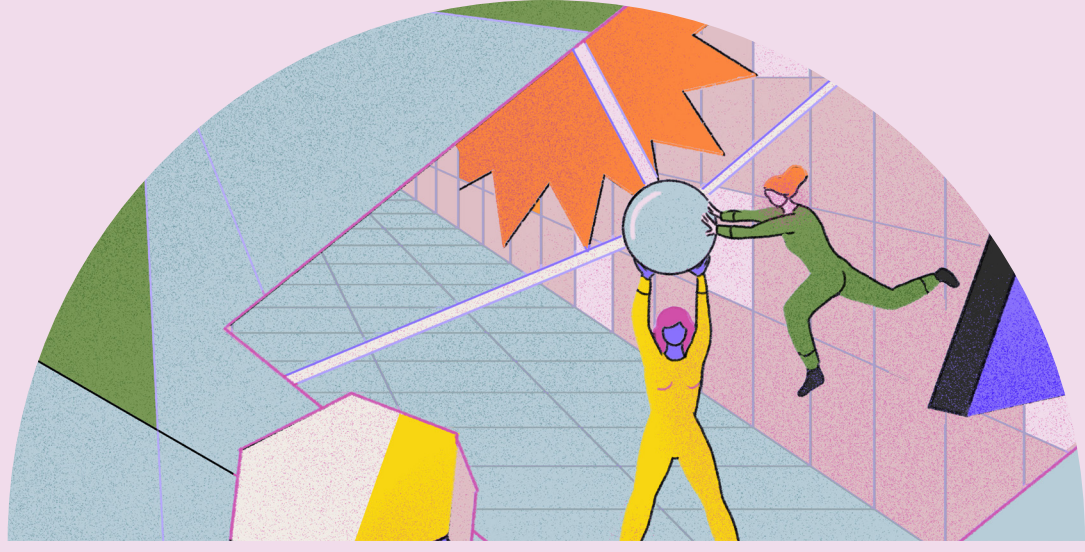
Anket katılımcılarının %86'sının yaş aralığının 19 - 45 olduğu öğrenildi.

Sıfır Bilgi Kanıtları (ZKP) Teknolojisini daha önce duydunuz mu?

Anket katılımcılarının %75.8'i en az bir kez ZKP'leri duymuştur ve ne olduğu hakkında bir düşüncesi vardır, %24.2'sinin ise ne anlam ifade ettiği hakkında bir fikri yoktur.

Buna ek olarak, geliştiricilerin %80'i ZKP teknolojisine aşina olduklarını ifade etmiştir. Bu bilgi, geliştiricilerin bu teknoloji ile geliştirme yapma isteğine sahip olduğunu göstermektedir.

Anket katılımcılarının demografik göstergelerine dayanarak bu raporda elde edilen sonuçlar 2022 yılının ilk çeyreğinde kripto para trader'lığı ve topluluk perspektifinden ZKP'lere yönelik kapsayıcı bilgiler aktarmaktadır.



— Önemli Bulgular

ZKP'lerin kritik önem taşıyacağı alanlar:

metaverse
ve Web3

anket katılımcılarının %42.2'si ZKP'yi metaverse ve Web3'ün geleceği için önemli olarak gördüğünü belirtti.

kripto paraların
tercih edilmesi

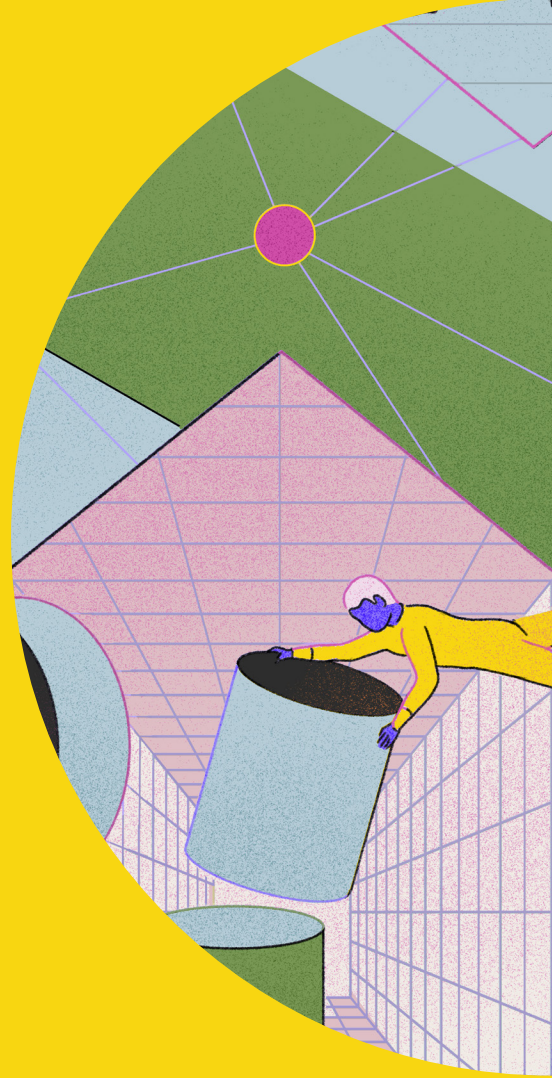
anket katılımcılarının %90.1'i ZKP teknolojisine sahip kripto paraları daha ilgi çekici bulduğunu belirtti.

finans
endüstrisi

anket katılımcılarının %40.6'sı ZKP'lere en çok Finans endüstrisinde ihtiyaç duyulduğunu belirtti.

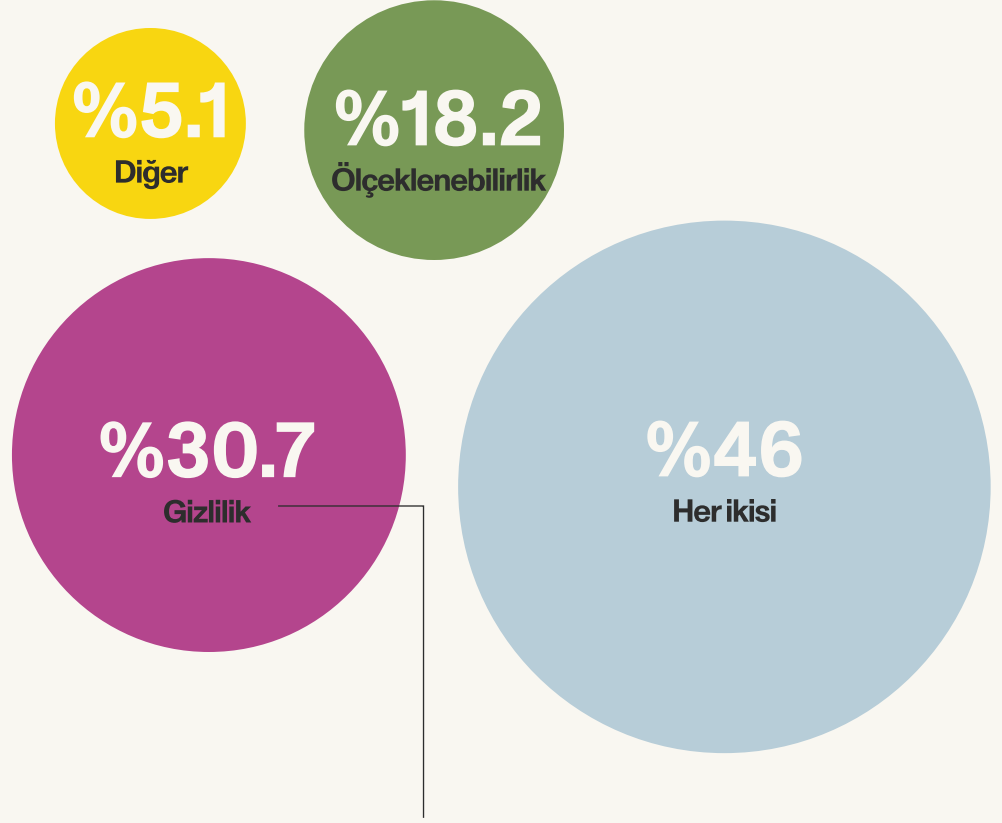
gizlilik
korunumu

anket katılımcılarının %30.7'si ZKP'leri gizlilik için bir avantaj olarak gördüğünü belirtti.



—Sonuç

SİZCE SIFIR BİLGİ KANITLARININ
EN BÜYÜK AVANTAJI NEDİR?



Gizlilik Endişeleri

Uygulamalar için ZKP teknolojisinin en büyük avantajının ne olduğu sorulduğunda anket katılımcılarının %46'sı gizlilik ve ölçeklenebilirlik olarak cevap verdi. Fakat gizlilik ve ölçeklenebilirlik arasındaki kıyaslamada ölçeklenebilirlik %18,2 iken gizlilik %30,7 şeklinde daha fazla yanıt aldı. **Gizliliğin ölçeklenebilirliğe göre daha fazla tercih edilmesi, kripto para endüstrisinin gizliliğe olan ve giderek artan ilgisini yansıtmaktadır.** NordVPN¹ tarafından yakın zamanda düzenlenen bir ankete katılanların %87'i metaverse dünyasındaki gizlilikleri konusunda endişe duyduklarını belirtmiştir. Fakat şu ana kadarki ZK tabanlı çözümlerin çoğu gizlilik yerine ölçeklenebilirliğe odaklanmıştır.

¹<https://nordvpn.com/blog/metaverse-survey/>

ZKP TEKNOLOJİSİNİ KULLANAN
KRIPTO PARALAR SİZİN İÇİN
DAHA İLĞİ ÇEKİCİ Mİ?

EVET

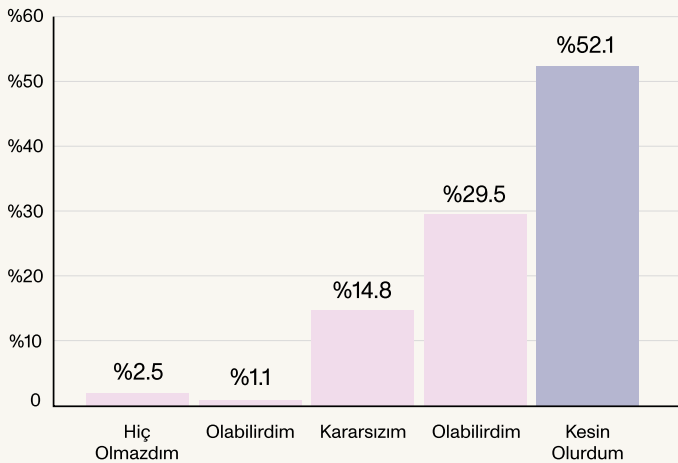
%90.1

HAYIR

%9.9

Anket katılımcılarının %90'ı ZKP teknolojisine sahip kripto paraların, bu teknolojiye sahip olmayanlara göre daha ilgi çekici olduklarını belirttiler. Bunun özellikle metaverse dünyasında giderek artan gizlilik endişelerinin bir göstergesi olduğunu söyleyebiliriz (sayfa 12 ve 13'te bahsedildiği gibi). Benzer şekilde **2022 Messari Crypto Thesis Raporu²** ise “Yeterince uzun bir zamanda tüm kripto sektörünün ZKP teknolojisi kullanan kripto varlıklara yaklaşacağını öngörmektedir”.

“BİR DAPP'İN ZKP TEKNOLOJİSİNİN GİZLİLİK VEYA ÖLÇEKLENEBİLİRLİK GİBİ AVANTAJLARINI SUNDUĞUNU BİLİYOR OLSAYDINIZ, O DAPP'İ KULLANMAK İÇİN DAHA İSTEKLİ OLUR MUYDUNUZ?”

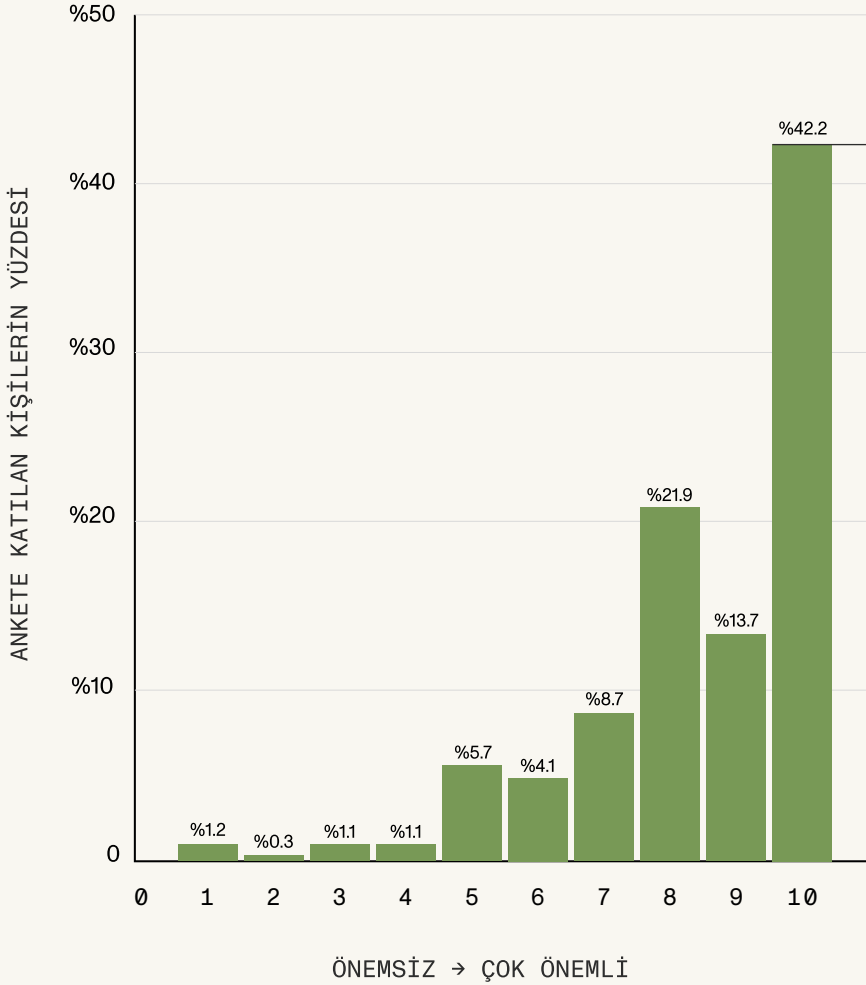


Ankete katılanlara ZKP teknolojisine sahip dapp'leri kullanmada ne kadar istekli olduklarını sordüğümüzda ise katılımcıların **%52,1'i ZKP teknolojisine sahip bir dapp'i kullanmaya daha istekli olacaklarını belirtti**. Bu sadece 2022'nin ilk çeyreğinde 1,2 milyar dolar çalınması³ gibi blokzinciri güvenlik ihlalleri ışığında kripto topluluğu üyelerinin ZKP teknolojisinin gizlilik ve güvenlik avantajlarına güvendiğinin bir göstergesi olabilir.

² <https://messari.io/pdf/messari-report-crypto-theses-for-2022.pdf> (Sayfa 145)

³ <https://dappradar.com/blog/dapp-industry-report-q1-2022-overview>

SİZCE WEB 3.0 VE METAVERSE DÜNYASINDA
ZKP'LER NE KADAR ÖNEMLİ OLACAK?



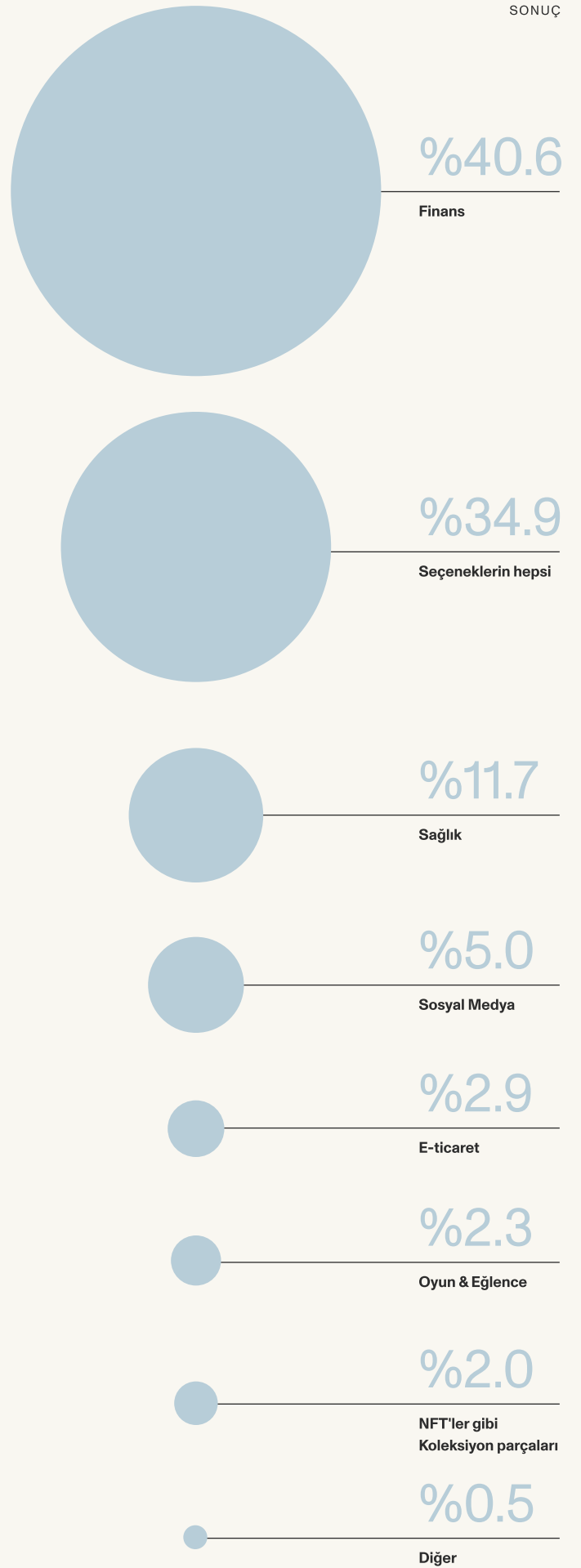
Ankete katılanların %42.2'si ZKP teknolojisinin metaverse ve Web3 dünyasında büyük öneme sahip olacağını belirtirken ankete katılanların %77.7'si önem verme puanını 8 veya üzeri verdi. Epic, Roblox, Microsoft ve Meta (eski adıyla Facebook) gibi büyük şirketler tarafından metaverse'e gösterilen ilginin ışığında bu veriler kripto topluluğunun metaverse'ün kurumsal kontrolü hakkında sahip olduğu artan endişelerini desteklemektedir. NordVPN⁴ tarafından yakın zamanda yapılan bir araştırma, internet kullanıcılarının %47'sinin kimliklerinin korunacağına güvenmediğini gösteriyor. Kullanıcıların metaverse dünyasında kimliklerini ve verilerini kontrol etme olanağı olmaması, kullanıcı verilerinin kötü niyetli kişilerin kullanımına açık hale gelmesine neden olur. Bu durum metaverse dünyasının daha fazla kullanıcı tarafından benimsenmesinin önünde engel teşkil edebilir.

⁴<https://nordvpn.com/blog/metaverse-survey/>

“ZKP'ler, bugün çoğu
blokzincirinin eksik
bir parçasıdır.”

—anket katılımcısı

SIFIR BİLGİ KANITLARININ
KULLANILMASI EN ÇOK HANGİ
ENDÜSTRİYE KATMA DEĞER
YARATACAKTIR?



Sonuç olarak, anket katılımcıları Finans, Sağlık Hizmetleri, Sosyal Medya, E-Ticaret, Oyun & Eğlence ve Koleksiyonlar dahil tüm sektörlerin ZKP teknolojilerinden yararlanabileceğini belirttiler. Katılımcılar ZKP teknolojisinin en çok Finans sektörü için bir çözüm sunacağını belirttiler.

Merkeziyetsiz Finans (DeFi) kullanımının artmasıyla⁵, **ölçeklenebilirlik ve gizlilik avantajlarına sahip sıfır bilgi uygulamaları, endüstrinin daha geniş çapta benimsenmesini iyileştirmeye yardımcı olmak için artan bir fırsata sahiptir.**

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

EN ÇOK HANGİ TÜR VERİLERİNİZİ
GİZLİ TUTMAK İSTERSİNİZ?

%54.5

Finansal

%48.6

Herhangi kişisel bir bilgi

%46.7

Mümkün olduğunca anonim olarak
kalmak istiyorum

%26.7

Lokasyon

%25.8

Sağlık

%13.3

İsim

%10.9

Kredi Skoru

Not: Bu soru için
katılımcılardan en az 3
kategori seçmeleri istendi.

Finansal Gizlilik

Birçok katılımcı kişisel bilgilerinin gizli tutulmasının önemli olduğunu belirtti. Aynı zamanda kullanıcıların sosyal güvenlik numarasını, kripto para bakiyesini, net varlığını, kredi skorunu vb. içeren finansal verileri de önem sırasınca oldukça öne çıktı.

Bir örnek vermek gerekirse ZKP'ler, birçok kullanıcıya borç alma sürecinde tüm kişisel bilgilerini paylaşmaya gerek kalmadan kredi skorunun 700'ün üzerinde olduğunu gösteren bir kanıtın oluşturulmasını mümkün kılan bir dapp geliştirmek için kullanılabilir. **Finansal verilerin gizli tutulmasına verilen önem, Web3 ve DeFi alanının geleceğinde ZKP'lerin önemli bir rol oynayacağına işaret ediyor.**

AŞAĞIDAKİLERDEN HANGİSİNİN
VERİLERİNİZE ERIŞİMİ KONUSUNDA
EN ÇOK ENDİŞE DUYARSINIZ?

Endişe duymam		Endişe duyarım
%6.3	Kripto Cüzdanlar	%35.7
%3.5	Bankalar	%39.9
%3.1	Sosyal Medya Platformları	%41.3
%2.5	Üçüncü Parti Şirketler	%44.0
%3.1	Devlet	%48.5

Ankete katılanlar, seçenekler arasında en çok devletin verilerine erişiminden endişe duyacaklarını belirttiler. Genel olarak tüm varlık türlerinde oldukça yüksek düzeyde endişe dile getiren katılımcılar için bankalar⁶, sosyal medya platformları⁷ ve üçüncü parti şirketler⁸ ile karşılaştırıldığında kripto para cüzdanları en az endişe duyulandır.

Bu, DeFi⁹, finans kurumları, sosyal medya platformları¹⁰ ve devletin¹¹ kontrolünde meydana gelen çeşitli veri hacklenmeleri ve ihlallerine dikkat çekmektedir.

⁶ <https://carnegieendowment.org/specialprojects/protectingfinancialstability/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/>



—Son Notlar

Bu rapordan elde edilen sonuçlar, bazı blokzincirlerin en büyük dilemması olan gizliliği ve ölçeklenebilirliği çözmek için daha geniş kripto topluluklarının sıfır bilgi teknolojisine yöneldiğini gösteriyor.

Bulgular, güvenli ve kullanıcı kontrollü bir Web3'ün uygulanabilmesi için kullanıcı verilerinin kötü niyetli kullanılmaması konusundaki büyük potansiyel ışığında gizliliğin artan önemi özellikle pekiştiriyor. Joseph Johnson tarafından hazırlanan Online Privacy Worldwide Raporunda¹², internet kullanıcılarının %53'ünün çevrimiçi gizlilikleri konusunda bir yıl öncesine göre daha fazla endişe duyduğunu ortaya koymuştur. Endişeler artmaya devam ettikçe ve Web3 gelişmeye devam ettikçe, ZKP teknolojisinin sağladığı gizlilik avantajları daha fazla kullanıcı için her zamankinden daha önemli hale gelecektir.

Artık daha fazla geliştirici ve kripto para kullanıcısı, üzerinde geliştirme yapmak ve alım satım yapmak için ZKP'lere her zamankinden daha çok önem veriyor. Bu yaklaşım, yakın dönemde gizliliği, ölçeklenebilirliği veya her ikisini de mümkün kılan ZKP teknolojisini kullanan daha fazla dapp'in geliştirilmesi ile sonuçlanacaktır. Surojit Chatterjee, CPO/Coinbase, 2022 öngörülerinde "sıfır bilgi kanıtı teknolojisinin ölçeklenebilirlik ve gizlilik odaklı örnek uygulamalar için yüksek bir gelişme" göstereceğini belirtmiştir.

Bu rapordan elde edilen kripto kullanıcılarının %54'ünden fazlasının finansal gizliliğin çok önemli olduğunu belirten bulgu, Merkeziyetsiz Finans (DeFi) uygulamaları için ZKP teknolojisinin önemli katma değer üretebileceğine işaret etmektedir (Sayfa 16).

Chainanalysis¹⁴ tarafından yakın zamanda yayınlanan raporda gösterildiği üzere, DeFi hacklenmelerindeki artış göz önüne alındığında da bu bulgu önem arz etmektedir. DeFi, kullanıcıları kendi bilgileri üzerinde kontrollerini artırmak istiyorsa, DeFi'nin ZKP teknolojisi tarafından mümkün kılınan güvenli, gizli veri paylaşımına ihtiyacı olacak. ZKP teknolojisinin sağladığı özel finansman geleneksel kurumsal finansmana göre daha çekici geldiğinden ZKP entegrasyonu norm haline geldiğinde, Geleneksel Finans'ın DeFi'ye olan katılımının artmasını da bekleyebiliriz.

Artık daha fazla geliştirici ve kripto para kullanıcısı, üzerinde geliştirme yapmak ve alım satım için her zamankinden daha çok ZKP'lere önem veriyor.

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

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

¹⁴ <https://blog.chainalysis.com/reports/2022-defi-hacks/>

Kripto para topluluk üyeleri, ZKP'lerin DeFi'nin, Web3'ün ve metaverse'ün geleceğini güvence altına almada önemli bir rol oynayacağını aktardılar.

Herkesin erişebileceği güvenli ve gizli bir Web3'ü mümkün kılmak için sektördeki sıfır bilgi gelişmelerini takip etmeyi dört gözle bekliyoruz.

DeFi alanında ZKP'ler ile birlikte uygulanabilir olan güvenli ve gizli veri paylaşımına ihtiyaç duyuluyor.

Bu rapor, kripto topluluğu içindeki kişiler ile anket yapılarak Mina Foundation tarafından hazırlanmıştır.

Mina Foundation, dünyanın en hafif blokzinciri olan **Mina Protokolüne**, toplumsal fayda yaratma amacı ile hizmet eden bir kuruluştur. Mina Vakfı, protokole ve topluluğa katkıda bulunan üçüncü partilere hibe vererek ve Mina topluluğunu yöneterek, hem Mina ağının hem de Mina topluluğunun sürdürülebilirliğini destekler.

Mina Protocol Hakkında

MINA yüksek işletim gücü yerine, yenilikçi bir blokzincir erişilebilirliği başlatarak, birkaç tweet boyutunda olan ve her zaman birkaç tweet boyutunda kalacak olan, yaklaşık 22kb boyutunda bir blokzinciri tasarlamak için gelişmiş kriptografi ve yinelemeli zk-SNARK'lar kullanır. Sıfır bilgi akıllı sözleşmelerinin etkili entegrasyonunu ve kolay programlanabilirliğini sağlayan ilk L1 protokolüdür. Eşsiz gizlilik ve herhangi bir web sitesine bağlanabilme özelliği ile Mina, gerçek dünya ve kripto arasında özel bir geçit — ve hepimizin hak ettiği gibi güvenli ve demokratik bir gelecek — sunuyor.

Mina, ana merkezi Amerika Birleşik Devletleri'nde bulunan ve bir kamu yararına kuruluş olan Mina Vakfı tarafından yönetilmektedir.

Mina ve sıfır bilgi hakkındaki en güncel haberleri takip etmek için:

Website:
<https://minaprotocol.com/>

Twitter:
<https://twitter.com/minaprotocol>

Referanslar

görünüm temel alınarak sayfa numarasına göre listelenmiştir

Sorumluluk Reddi:
Burada sunulan bilgiler
Mina Foundation topluluk
üyelerinin katılımı ile
gerçekleşen anketten
elde edilmiştir.

**İfadeler ileriye dönük
öngörüler içerebilir ve
gelecekteki performans
dair taahhüd
vermemektedir.**

**Medya işbirlikleri için
lütfen iletişime geçiniz:**

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

- 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