Framework macht seine bisher größte Einzelwette auf Immunefi

Zuletzt hat Immunefi eine 400-ETH-Transaktion von Arbitrum an einen weißen Hacker ermöglicht Zu den an der Runde beteiligten Investoren gehören Electric Capital, Polygon Ventures und Samsung Next Immunefi, eine Web3-Bug-Bounty-Plattform, die von prominenten Projekten wie MakerDAO, Compound und Chainlinkhat sich eine Serie A im Wert von 24 Millionen US-Dollar unter der Leitung von Framework Ventures gesichert. Framework Ventures leitete zuvor die Seed-Runde von Immunefi im Mai letzten Jahres, aber die letzte Runde wird der größte Scheck sein, den die prominente Risikokapitalgesellschaft jemals öffentlich geschrieben hat, sagte Roy Learner, Direktor bei Framework Ventures, in einer Erklärung. ȣSo wie es aussieht, ist …

- Zuletzt hat Immunefi eine 400-ETH-Transaktion von Arbitrum an einen weißen Hacker ermöglicht
- Zu den an der Runde beteiligten Investoren gehören Electric Capital, Polygon Ventures und Samsung Next

Immunefi, eine Web3-Bug-Bounty-Plattform, die von prominenten Projekten wie MakerDAO, Compound und Chainlinkhat sich eine Serie A im Wert von 24 Millionen US-Dollar unter der Leitung von Framework Ventures gesichert.

Framework Ventures leitete zuvor die Seed-Runde von Immunefi im Mai letzten Jahres, aber die letzte Runde wird der größte Scheck sein, den die prominente Risikokapitalgesellschaft jemals öffentlich geschrieben hat, sagte Roy Learner, Direktor bei Framework Ventures, in einer Erklärung.

ȝSo wie es aussieht, ist Immunefi bei weitem die am weitesten verbreitete Lösung im Bereich Krypto-Sicherheit und Bug-Bountiesȝ, sagte Learner. ȝWir freuen uns, das Unternehmen wachsen zu sehen und Talente anzuhäufen, da immer mehr Schlüsselprojekte in ihr Ökosystem aufgenommen werden.ȝ

Andere Investoren, die an der Runde teilgenommen haben, sind Electric Capital, Polygon Ventures und Samsung Next.

Mitchell Amador, Mitbegründer von Immunefi, hatte die Idee für das Unternehmen, nachdem er einen erheblichen Geldbetrag durch Smart-Contract-Hacks verloren hatte.

ȝEs gibt eine ganze Welt, die durch ermöglicht wird [blockchain] Technologie und sie kann nicht ohne Sicherheit existieren ر wir haben den gesamten Stack kartiert und sind zu dem Schluss

gekommen, dass das kritischste Teil, das der Raum nicht alleine lösen kann, die Offenlegungsebene ist ج der 911 ذ, sagte Amador.

Das Sicherheitsunternehmen belohnt White-Hat-Hacker für die Überprüfung von Blockchain-Projekten und die Offenlegung von Schwachstellen ج wodurch finanzielle Anreize für Experten geschaffen werden, um Dapps sicherer zu machen. Es verfügt derzeit über eine Community von über 11.000 Entwicklern, Prüfern, CTOs und Hackern.

Laut Amador können Belohnungen von ein paar tausend Dollar bis hin zu Millionen von Dollar für einen einzigen Fehlerbericht reichen.

> ڈWenn du Gutes für die Gemeinschaft tust, wirst du nicht nur reich, sondern auch ein Heldډ, sagte Amador.

Immunefi hat zuvor eine Bug-Bounty-Zahlung in Höhe von 10 Millionen US-Dollar für eine Schwachstelle ermöglicht, die in der Cross-Chain-Messaging-Lösung Wormhole entdeckt wurde, und eine Gefährdung in Höhe von 6 Millionen US-Dollar, die in einer Brücken- und Skalierungslösung Aurora entdeckt wurde.

Zuletzt zahlte Arbitrum, eine Layer-2-Ethereum-Skalierungslösung, 400 ETH (fast 550.000 USD) über Immunefi an einen White-Hat-Hacker als Belohnung für die Aufdeckung einer Schwachstelle.

Die jüngste Spendenaktion wird dem Ausbau des Immunefi-Teams dienen, sagte Amador.

ڈWir brauchen besseres technisches Know-how ج wir können mit dem Aktivitätsniveau nicht Schritt haltenډ, sagte Amador. ڈWir

brauchen einfach mehr Leute

. .

Der Beitrag Framework macht seine bisher größte Einzelwette auf Immunefi ist keine finanzielle Beratung.

Details