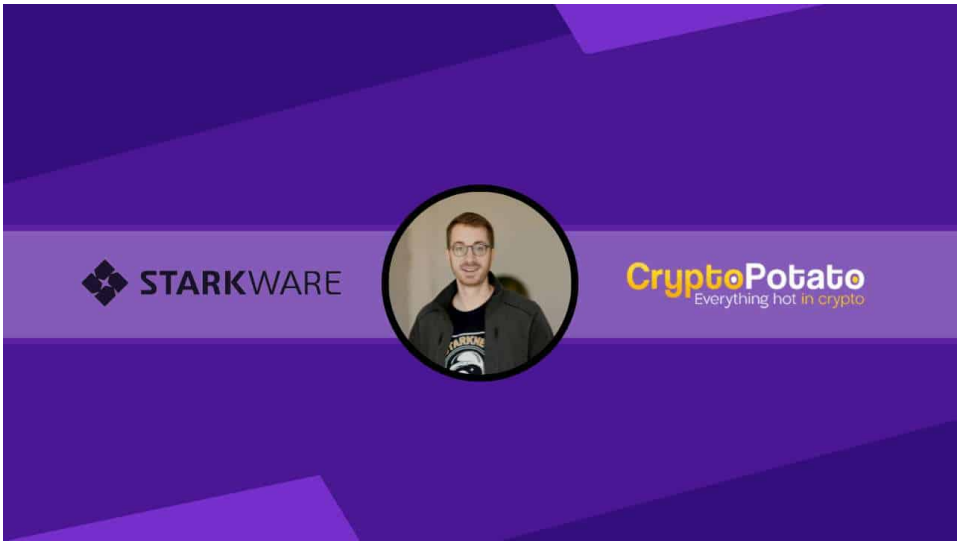
Interview mit StarkWare-PM Gal Ron

Die Skalierung von Ethereum war zweifellos eines der heißesten Themen der letzten Monate. Der Übergang des Netzwerks zu einem Proof-of-Stake-Konsensalgorithmus im September 2022 war in dieser Hinsicht ein großer Meilenstein, da er die Tür für die Implementierung vieler verschiedener Skalierungslösungen öffnete. Während Ethereum-Entwickler an Möglichkeiten arbeiten, das Netzwerk nativ zu skalieren, beginnt sich die Leistungsfähigkeit von Layer-Two-Lösungen erst zu manifestieren. Konzepte wie Zero-Knowledge-Proofs werden mittlerweile zur Arbeitsrealität, sind aber für viele noch ein Fremdwort. Um uns dabei zu helfen, mehr über die Zukunft der Ethereum-Skalierung zu verstehen, ist Gal Ron ج Produktmanager und Blockchain-Forscher bei StarkWare ج einem Unternehmen, das …



Die Skalierung von Ethereum war zweifellos eines der heißesten Themen der letzten Monate. Der Übergang des Netzwerks zu einem Proof-of-Stake-Konsensalgorithmus im September 2022 war in dieser Hinsicht ein großer Meilenstein, da er die Tür für

die Implementierung vieler verschiedener Skalierungslösungen öffnete.

Während Ethereum-Entwickler an Möglichkeiten arbeiten, das Netzwerk nativ zu skalieren, beginnt sich die Leistungsfähigkeit von Layer-Two-Lösungen erst zu manifestieren.

Konzepte wie Zero-Knowledge-Proofs werden mittlerweile zur Arbeitsrealität, sind aber für viele noch ein Fremdwort. Um uns dabei zu helfen, mehr über die Zukunft der Ethereum-Skalierung zu verstehen, ist Gal Ron ج Produktmanager und Blockchain-Forscher bei StarkWare ج einem Unternehmen, das sich hauptsächlich darauf konzentriert.

Das Problem mit Ethereum

Bevor wir uns mit einigen Einzelheiten befassen, ist es wichtig zu verstehen, was die Skalierung von Ethereum eigentlich bedeutet. Laienhaft ausgedrückt ist dies der Prozess der Erweiterung der Verarbeitungsfähigkeiten des Netzwerks, sodass jeder seiner Knoten einen höheren Transaktionsdurchsatz bewältigen kann.

Es gibt dieses Sprichwort, das besagt, dass eine Kette nur so stark und leistungsfähig ist wie ihr schwächstes Glied. Dies liegt daran, dass nur eines der Glieder brechen muss, damit die gesamte Kette versagt. Das schränkt auch die Festigkeit der Kette ein, weil sie nur so viel Last aufnehmen kann wie ihr schwächstes Glied ج egal wie stark alle anderen Glieder sind.

Dasselbe gilt für Ethereum in seinem aktuellen Zustand. Die Notwendigkeit dafür ergibt sich aus der Tatsache, dass Ethereum die ȝVertrauensȝ-Anforderung erfüllen muss.

Zu diesem Thema erklärt Ron:

Um alle Vertrauensannahmen und Vertrauensanforderungen zu

erfüllen, müssen alle Knoten (auf Ethereum) dasselbe tun. Per Definition begrenzt dies den Durchsatz des Systems, denn wenn wir die TPS oder die Blockgröße über einen bestimmten Schwellenwert erhöhen, würden wir anfangen, die kleineren (sprich: mit weniger Rechenleistung) Knoten daran zu hindern, teilzunehmen.

Im Wesentlichen macht dies Ethereum per Definition in seiner Kapazität eingeschränkt.

Ansatz von StarkWare: Was ist ein ZK-Proof?

Ron erklärt, dass es ein paar Optionen gibt, um die Beschränkungsprobleme von Ethereum zu lösen. Eine davon ist, etwas anderes zu erfinden.

StarkWare hat jedoch einen anderen Ansatz gewählt, nämlich ȝEthereum von Ethereum zu skalieren und keine weitere Kette zu erstellenȝ. Sie tun dies über StarkNet und StarkEx, also lasst uns einen Blick darauf werfen.

StarkNet wird als ȝerlaubnisloses dezentrales Gültigkeits-Rollup, auch bekannt als ZK-Rollupȝ beschrieben. Es funktioniert als L2-Netzwerk (Layer-Two) über Ethereum und zielt darauf ab, es jeder dezentralisierten Anwendung (dApp) zu ermöglichen, eine unbegrenzte Skalierung für ihre Berechnung zu erreichen. Dies geschieht, ohne die Sicherheit und Zusammensetzbarkeit der Hauptschicht ȼ Ethereum ȼ zu opfern, da StarkNet auf das als STARK bekannte kryptografische Beweissystem angewiesen ist.

Hier gibt es viel zu entpacken, also fangen wir mit dem Konzept der Zero-Knowledge-Beweise an.

ȝBei Ethereum müssen alle Knoten alle Transaktionen erneut ausführen. Vor ZK (Zero-Knowledge) gab es keine andere Möglichkeit, darauf zu vertrauen, dass jemand anderes die Berechnungen mit Integrität durchführte. Wenn ich ein Knoten

auf Ethereum bin, sehe ich, was andere Knoten mir in Bezug auf den Zustand des Systems melden. Es gibt keine Möglichkeit für mich, ihnen zu vertrauen, außer einfach dieselben Berechnungen erneut auszuführen, die sie gerade ausgeführt haben.

Das Wunderbare an ZK ist, dass es ein neues Paradigma schafft, anderen Entitäten zu vertrauen, ohne die Berechnungen, die sie gerade durchgeführt haben, erneut ausführen zu müssen.ڊ ج Sagte Ron.

Im Wesentlichen reduzieren ZK-Rollups wie StarkNet die Menge an Rechenarbeit, die Knoten auf Ethereum leisten müssen, erheblich und erhöhen somit den Durchsatz des Netzwerks.

All dies geschieht, ohne die Sicherheit der Hauptschicht zu opfern. Zu diesem Zweck erfand StarkWare ZK-STARKs, die es Blockchains ermöglichen, Berechnungen auf einen einzelnen Off-Chain-STARK-Prover zu verschieben und dann die Integrität dieser Berechnungen mit einem On-Chain-STARK-Verifier zu überprüfen.

Gal Ron erklärte, wie sowohl der Prover als auch der Sequencer funktionieren, also schauen Sie sich für weitere Details bitte das obige Video an.

Wir werfen auch einen genaueren Blick darauf, was genau Rollups sind, was StarkEx ist und welche Pläne StarkWare für die Zukunft hat.

.

Details