Introduction

What is Aura

By securely sharing transaction records on the blockchain, ensuring immutability through encryption, and leveraging smart contracts for automatic verification and payment, we transform the earnout process into a transparent, fair, and tamper-proof mechanism—eliminating trust friction in M&A.

What is M&A earn-out

In mergers and acquisitions (M&A), buyers and sellers often reach an impasse due to differing views on a company's valuation. From the buyer's perspective, the key concern is whether they may end up overpaying if the acquired company fails to perform as expected after the transaction. Meanwhile, the seller hopes that the company's future growth potential will be fully reflected in the final purchase price.

In such cases, an earnout mechanism, also known as contingent consideration, becomes a commonly adopted solution.

Earnout is a contractual arrangement in M&A transactions where part of the purchase price is tied to the future performance of the acquired company. Upon closing, the buyer pays only a portion of the agreed price (the initial consideration). If the target company meets predetermined performance metrics—such as revenue, operating profit, EBITDA, or specific KPIs—within a defined period after closing, the buyer will then pay the additional agreed amount to the seller.

Therefore, an earnout is not a one-time lump-sum payment at closing, but rather a conditional and staged payment mechanism. For companies in the growth phase or those with strong future potential, this structure allows future value creation to be reflected in the purchase consideration.

As AI-, Web3-, and emerging innovation-driven startups continue to grow, earnout-based acquisitions are expected to become increasingly common.

Pain Points of the Traditional Earnout Mechanism

Nowadays, In an Earn-out Mechanism, the core challenge stems from the lack of transparency in post-closing performance records, which leads to trust breakdown and information asymmetry.

I. When earn-out mechanism occurs
   A. The seller is concerned that the buyer may leverage their informational advantage to manipulate or passively manage the company's performance afterwards, thereby preventing the earn-out targets from being met. To hedge against this moral hazard and information asymmetry, the seller tends to demand a higher initial consideration.
   B. Conversely, the buyer faces significant valuation difficulty as they cannot be fully confident in the true future performance of the target company, especially when pressured by a high initial price. The ultimate outcome is that both parties face the risk of potential overpaying or underpaying, highlighting the difficulty of effective pricing under the earn-out structure when information is opaque.

II. Post-Closing Manipulation and Data Integrity Issues
   leading to disputes where no single source of truth exists, making evidence difficult to present.
   A. Both parties have incentives to manipulate the M&A agreement, including:
      1. Accounting methods (e.g., depreciation estimates, inventory cost estimation, allocation method of headquarter expenses)
      2. Target revenue metrics
   B. When control shifts to the acquirer after closing, giving the buyer the incentive and ability to alter post-acquisition records or financial statements to intentionally lower the acquired company's performance and therefore reduce earnout payments.
      1. Example: The revenue for the current year is confirmed as 40M by both parties, but the buyer later modifies the prior-year revenue to 30M,

artificially reducing performance growth.

C. Alter performance achievement

1. Example: KPI achievement is acknowledged at 40% this year, yet next year the buyer unilaterally reinterprets last year’s achievement as only 30%, intentionally weakening the performance calculation.

III. Seller Meets Earnout Requirements, but Buyer Refuses to Pay

IV. Seller Cannot Verify Buyer’s Post-Acquisition Decisions

Aura Brings Precision and Trust to M&A Earn-Out Pricing and Payments

I. The core value of the Aura protocol lies in ensuring that post-acquisition transaction records are secure and tamper-proof through decentralized storage and encrypted access control. This foundation creates a single, verified source of truth for all financial evidence and supporting documents, eliminating information opacity and manipulation risks.

II. Building on this, smart contracts encode the pre-agreed performance metrics and execute automatically, triggering payments upon milestone achievement to avoid delays and disputes. This “immutable and transparent” mechanism enables both parties to establish a fair and predictable framework during negotiations:

III. For sellers: No longer worried about buyers manipulating performance or refusing payment, they are more willing to accept a lower upfront amount. Even after control shifts, sellers can continuously verify subsequent performance through immutable records.

IV. For buyers: Payments are tightly linked to actual performance, reducing valuation uncertainty and mitigating the risk of mismatched perceived versus actual company value.

V. Additionally, the audit process is transformed by complete, real-time verifiable data. Auditors can focus on anomaly detection and risk analysis rather than tedious data collection and reconciliation, significantly lowering compliance costs and improving audit quality. Ultimately, the entire M&A lifecycle shifts from a traditional manual, adversarial process to an automated, executable, and efficient mechanism—enabling faster negotiations, lower monitoring costs, and fairer value transfer.

How we work

Key terms

Participants

I. Acquirer:
   A. Uploads transaction records to Walrus and encrypted with Seal for privacy when transactions occur. These records form a single, tamper-proof source of truth, and serve as the basis for KPI calculations.
   B. Has strong incentives to disclose documents, as doing so enables an initially lower purchase price and helps avoid both overpayment and underpayment by ensuring all parties have access to shared, transparent reports.
      1. Sellers gain confidence that the buyer cannot manipulate performance to avoid milestones — making them more comfortable accepting a lower upfront payment.
      2. Even after control transfers to the buyer, the seller can continuously verify performance through authenticated records.

II. Acquiree:
   A. Seller can verify performance anytime to ensure that buyer doesn't manipulate it.
   B. Trigger KPI calculation with verified, tamper-proof records.

III. Auditor:
   A. Can instantly access records and sign off once they verify their accuracy.
   B. Can shift focus from data collection and reconciliation toward identifying anomalies and high-risk entries.

Concepts

I. Journal entry:

    A. The basic accounting record that logs a business transaction in the company's books and must be audited.

II. Tax return:

    A. The Business Tax Return is uploaded every two months to prevent the buyer from underreporting their income. Additionally, the Business Income Tax Return is uploaded once a year in May.

    B. To ensure the buyer does not fail to upload all required revenue records.

Contract documentation

Smart contract overview

I. create_deal

This function is used to create a new earn-out mechanism. It sets all the details of the agreement, such as the agreement name, the buyer, the seller, the auditor, the start date, the duration, the performance targets (KPIs) required to receive payment, the depreciation period, the allocation ratio for headquarters costs, and the maximum payable amount. It also divides the agreement into several smaller stages to facilitate document management

II. add_walrus_blob

This function uploads agreement-related documents (such as performance data) to a secure cloud storage service (Walrus) and records their reference information on the blockchain. At the same time, it creates an audit record to notify auditors that these documents require verification. The documents are categorized according to the previously defined stages for easier management.

III. audit_data

This function is designed for auditors. After the buyer uploads documents, the auditor reviews them for authenticity and accuracy. Once the verification is complete, the auditor uses this function to confirm on the blockchain that the documents have been audited.

IV. seal_approve

This is a special function that interacts with the encryption system (Seal). It is not intended for direct use by regular users but is called by the service responsible for managing encryption keys. When someone attempts to decrypt encrypted documents related to the earn-out agreement or post-acquisition transaction, this function checks whether the requester (such as the buyer, seller, or auditor) has the proper authorization. It verifies the requester’s identity and ensures they are indeed a participant in the agreement.

V. submit_kpi_and_settle

This is the final settlement stage of the earn-out agreement. After all performance milestones have been completed, the seller submits the final performance results (KPI outcomes) along with an attestation generated by a secure computing environment (Nautilus TEE) to verify the authenticity of these figures. The blockchain then validates this attestation and, based on the performance targets defined in the agreement, determines whether the seller has met the conditions. It automatically calculates and transfers the payment due to the seller.