Architect Partners

Eric F. Risley Managing Partner efr@architectpartners.com

Adlee Heshmat Senior Financial Analyst adlee@architectpartners.com

Dong Yang Term Analyst dong@architectpartners.com

September 14th - September 20th (Published September 21st)

PERSPECTIVES by Eric F. Risley

Historically, our industry has demonstrated an extraordinarily high tolerance for risk. One only has to look at the losses. This is changing.

This week, S&P Global agreed to acquire OpenZeppelin, whose open-source code sits under most of the largest stablecoins and tokenized funds. As covered in our M&A Alert, S&P rates the issuer, and OpenZeppelin checks the code. Together they intend to assess both. Why would a ratings company buy a security firm? Because preventable failure has a price, and onchain it is very high.

Set fraud and scams aside. To date, roughly $20.7 billion has been lost to hacks and exploits, per DefiLlama. Nearly all of it traces to things good risk management exists to prevent: flawed code, stolen or mishandled keys, weak access controls and botched upgrades.

The good news is that progress is being made, though only partly. In the first half of 2026, smart-contract exploits were 125 of 207 incidents but only a small share of the dollars lost, per TRM Labs. Audits, bug bounties and monitoring are working. What remains is operational. Infrastructure and operational failures were 15% of incidents but 76% of dollars lost, led by KelpDAO ($292M) and Drift ($285M). The code problem is being solved. The people-and-process problem is not.

Traditional finance makes the same mistakes. Knight Capital lost $440 million in 45 minutes in 2012 when a software deployment went wrong. Citi wired $894 million to Revlon's lenders in 2020 when it meant to send $7.8 million in interest. Nine UK banks and building societies logged 158 IT failures and 800-plus hours of downtime in two years. Execution and process errors cost 38 large US banks $31 billion between 2000 and 2017.

The difference is what happens next: can it be recovered, or is the loss permanent? Knight was rescued within days. Citi got its money back on appeal. Bank outages cost downtime and compensation, not customer principal. All of it sits inside two decades of Basel operational-risk discipline: standard loss categories, shared loss databases and capital held against them. Onchain, finality turns the same error into permanent loss of capital, with limited reversal and little insurance behind it.

S&P is buying the capability to ensure the code problem is addressed as part of its risk modeling.

RECENT CRYPTO M&A TRANSACTIONS (click here for full AP M&A Tracker)

Target	Acquirer	Transaction Summary	M&A Alert
OpenZeppelin	S&P Global	**Transaction Value:** Undisclosed **Rationale:** To add smart-contract security review to S&P's issuer and asset risk assessments **Sector:** Data & Data Analytics **Target Description:** Open-source smart contract standards library and security audit firm for onchain finance	●
Nomina	IRF	**Transaction Value:** Undisclosed **Rationale:** To own the live solver network executing its planned AI-agent DeFi strategies **Sector:** Investing & Trading Infrastructure **Target Description:** Solver network executing cross-chain DeFi intents with unified perpetual-DEX trading terminal	○
LimeWire	BABYDOGE	**Transaction Value:** Undisclosed **Rationale:** To own a consumer product layer that BabyDoge's token community can distribute **Sector:** DApp: Consumer **Target Description:** File-sharing platform with AI creator studio, decentralized storage network, and LMWR token	○

OVERALL CRYPTO M&A ACTIVITY LEVELS