



QUARTERLY RISK REPORT

Q3 2026

CONTENTS

Inside this report

INTRO	Executive Summary	03
	The quarter at a glance: timeline, key figures and the three themes	
01	The key is no longer the perimeter	04
	Digital asset security: losses move from keys to governance, vendors and approvals	
02	When authority itself is counterfeit	05
	Fraud and impersonation: authentic channels, fraudulent instructions	
03	Tokenisation goes live	06
	Tokenisation and stablecoins: from pilots to operating infrastructure	
OUTLOOK	What to watch in Q4 2026	07
	Outlook and the Continuum View	
NOTES	About this report	08
	Methodology, sources and contact details	

Legal Disclaimer

The information, opinions, and materials provided on this platform are for general informational purposes only and do not constitute legal, financial, or professional advice. While every effort is made to ensure accuracy and timeliness, no guarantee is given that the content is free from errors or omissions. The publisher assumes no liability for any loss, damage, or inconvenience arising from reliance on this content. All content is provided "as is" without warranties of any kind.

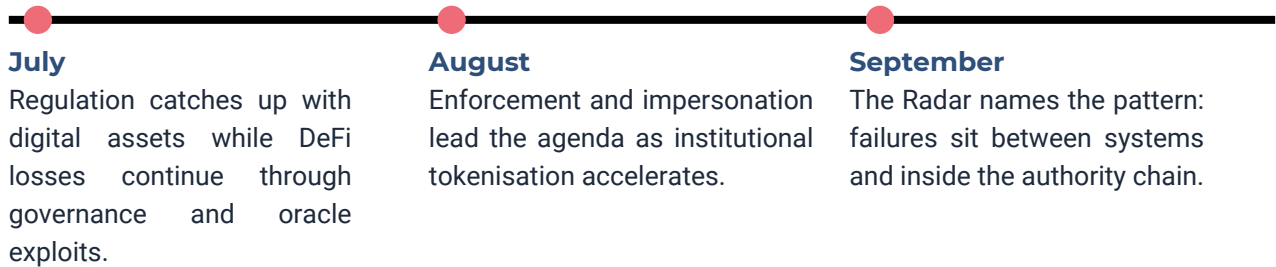
Where third-party materials, references, or links are included, they are provided for convenience and do not imply endorsement. All intellectual property rights remain with their respective owners. Unauthorized reproduction, distribution, or modification of this content is prohibited.

AI Disclosure: This article was created with the assistance of AI tools for research and drafting. It was reviewed, edited, and fact-checked by our human editorial team before publication.

EXECUTIVE SUMMARY

Risk moved from who holds the key to what is allowed to act

Across thirteen publications and roughly eighty-five developments this quarter, one pattern stood out: the largest losses began not with a stolen credential, but with a system, person or model that was permitted to act.



US \$ 387.5m

Revised Bitget loss, the largest incident of the quarter

65

Fake websites impersonating HashKey flagged by Hong Kong's SFC

28

Banks in the BIS tokenised cross-border settlement pilot

2,500+

Investigators in South Korea's new virtual asset crime unit

The Three Themes

01

Digital asset security

Losses migrated from keys to governance, vendors and approval workflows.

02

Fraud and impersonation

Authentic channels carried fraudulent instructions, and AI worked inside compromised inboxes.

03

Tokenisation goes live

Settlement and stablecoins moved from pilots into operating infrastructure.

For most of the past decade, digital asset security has meant one thing: protecting the key. This quarter showed that the key is no longer the weakest point. The Liquid Network federation lost about 4,000 BTC without its authorisation key being compromised, BonkDAO's treasury was drained through a governance proposal that passed as designed, and Revolut released data to a request that came from a genuine government domain. Each system did what it was permitted to do.

For boards, risk committees and underwriters, the question has changed. It is no longer "who can access this?" but "who, or what, is allowed to act, and who checks that the action is legitimate?" The three themes that follow trace this shift across custody, fraud and market infrastructure.

01 DIGITAL ASSET SECURITY

The key is no longer the perimeter

In almost every material loss this quarter, the private key either stayed secure or was made irrelevant by a

weakness elsewhere. Bonk DAO lost US\$20 million to a malicious governance proposal, a derivatives platform lost US\$18 million to oracle manipulation, and a randomness flaw in older Coldcard wallets let attackers drain US\$38 million in under 25 minutes.

Bitget made the pattern unmistakable. Attackers exploited a zero-day in a third-party security product and pushed spoofed transactions through the exchange's own approval workflow, taking an estimated US\$387.5 million from hot and warm wallets. Cold wallets were unaffected.

Where the failure occurred

DA	INCIDE	FAILURE	EXPOSURE
10 Jul	BonkDAO treasury drained	Governance logic	US\$20m
17 Jul	Derivatives platform exploited	Oracle price feed	US\$18m
31 Jul	Coldcard seed phrases predictable	Hardware design defect	US\$38m
14 Aug	Trezor shipping data exposed	Logistics vendor	14,000 users
11 Sep	Liquid withdrawal, key not compromised	System interface	c.4,000 BTC
25 Sep	Bitget spoofed transactions approved	Vendor zero-day	US\$387.5m

NEWS → RISK → CONTROL → INSURANCE

NEWS

Samsung Fire & Marine entered custody insurance with US\$20m of cover.

RISK

Every system that can initiate or approve a transfer is now part of the perimeter.

CONTROL

Independent transaction checks, withdrawal limits and vendor security review.

INSURANCE

Check hot wallet treatment in crime and specie cover, and vendor-originated breaches.

02 FRAUD AND IMPERSONATION When authority itself is counterfeit

The quarter's most damaging frauds relied on a victim's reasonable belief that a request, platform or executive was genuine. Hong Kong's SFC flagged 65 sites impersonating a licensed exchange, and the chief executive of Korean lender Delio was sentenced to 15 years for embezzling US\$50 million from customers.

In September, Revolut released customer data in response to fraudulent requests sent from a real government domain, and Microsoft disrupted EvilTokens, a platform using AI to map payment authority inside compromised inboxes. Validating the channel is no longer enough.

How authority was abused

DATE	EVENT	AUTHORITY EXPLOITED	SCALE
31 Jul	Seoul fake staking platform	Product credibility	Up to US\$20m
14 Aug	Delio chief executive sentenced	Executive position	US\$50m
21 Aug	Sites impersonating HashKey	Licensed brand	65 sites
18 Sep	Revolut data disclosure	Government email domain	Customer data
25 Sep	EvilTokens AI fraud platform	Compromised inboxes	Platform

NEWS → RISK → CONTROL → INSURANCE

NEWS

Japan urged exchange withdrawal delays; Korea launches a 2,500+ crime unit.

RISK

Apparent authority is the attack surface, driving customer loss and governance claims.

CONTROL

Out-of-band verification, dual authorisation and withdrawal delays.

INSURANCE

Review social engineering sublimits, D&O for executive misconduct and cyber for data disclosure.

Regulators across the region are now trying to stop fraud before funds leave the platform. Japan's FSA and NPA have asked exchanges to consider withdrawal delays, and Korea's virtual asset crime unit, with more than 2,500 investigators, begins operations in October. In Taiwan, authorities dismantled a USDT laundering network that ran through Hong Kong exchanges, which shows that licensed venues can be used as channels as well as targets. For firms, this means closer scrutiny of transfer controls and a higher expectation that suspicious activity is caught at the point of withdrawal.

TOKENISATION AND STABLECOINS

03Tokenisation goes live

Banks, central banks and regulators moved tokenisation from pilots into production this quarter. Twenty-eight banks completed a real-money tokenised settlement in a BIS pilot, Hong Kong began live testing of an HKD stablecoin, and the ECB launched Pontes for wholesale settlement in central bank money. The result is new operational risk: settlement failures and shared-infrastructure outages that can hit many institutions at once.

us \$1.79tn

Record stablecoin volume in June

72%

Crypto volume from institutions

us \$180bn

USDT reserves audited by KPMG

28

Banks in the BIS pilot

From pilot to infrastructure

DATE	DEVELOPMENT	MARKET	STAGE
31 Jul	BIS tokenised cross-border settlement	Global banks	Real-money test
14 Aug	MUFG government bond settlement test	Japan	Pilot
21 Aug	HKD stablecoin live beta	Hong Kong	Sandbox
18 Sep	SEC relief for tokenised U.S. stocks	United States	Market structure
21 Sep	ECB launches Pontes	Euro Area	Live infrastructure

NEWS → RISK → CONTROL → INSURANCE

NEWS

CPMI-IOSCO issued guidance on third-party dependence.

RISK

Smart contract defects and shared settlement outages create accumulation risk.

CONTROL

Map critical dependencies and test failover across settlement layers.

INSURANCE

Assess technology E&O, dependent business interruption and custody crime cover.

OUTLOOK

What to watch in Q4 2026

FROM OCTOBER

Korea's crime unit goes live

More than 2,500 investigators and new account freeze powers raise investigation exposure for platforms.

ONGOING

Bitget recovery

Further findings on the vendor vulnerability will shape how underwriters assess exchange vendor risk.

INTO 2027

Tax and reporting deadlines

Korea's 22 percent crypto tax and Singapore's CARF reporting both begin in 2027.

ONGOING

AI acting with authority

As AI agents gain real permissions, liability questions will follow.

CONTINUUM VIEW

The control question has moved from "who has the key?" to "what can act, on whose authority, and where can it be stopped?"
Understand the loss scenario first. Then controls. Then insurance.

NEWS → RISK → CONTROL → INSURANCE

About this report

Based on nine Weekly Risk Updates (3 July to 28 August 2026) and four Emerging Risk Radar issues (4 to 25 September 2026). Bitget figures are updated to its 30 September root-cause disclosure.

ADDITIONAL SOURCES

Bitget security notice: bitget.com/support/articles/12560603896024

Bleeping Computer, Bitget root cause: bleepingcomputer.com/news/security/bitget-hacked-via-zero-day-in-third-party-security-products

Halborn, Bitget incident analysis: halborn.com/blog/post/explained-the-bitget-hack-september-2026

Microsoft, EvilTokens disruption: blogs.microsoft.com/on-the-issues/2026/09/22/disrupting-eviltokens-the-ai-chatbot-built-for-cybercrime

ECB, Pontes launch: ecb.europa.eu/press/pr/date/2026/html/ecb.pr260921~e754847a7b.en.html

This report is provided for general information only and does not constitute legal, regulatory, financial or insurance advice. Coverage availability, terms, conditions and exclusions vary by insurer and policy, and any insurance decision should be based on a review of specific circumstances with a qualified adviser. Information is drawn from public sources believed to be reliable as at 30 September 2026 and may change as events develop.

Continuum Risk Advisory Pte Ltd ("Continuum") registered in Singapore, UEN 202316352E is an independent risk advisory consultancy and technology provider. Continuum provides general risk advice and insurance product information through our website and other online means. Continuum is not an insurance company, insurance agency or insurance brokerage company and does not provide financial advice.



Risk. Insurance. Technology.

 hello@continuuminsure.com

 www.continuuminsure.com

Continuum Risk Advisory Pte Ltd ("Continuum") registered in Singapore, UEN 202316352E is an independent risk advisory consultancy and technology provider. Continuum provides general risk advice and insurance product information through our website and other online means. Continuum is not an insurance company, insurance agency or insurance brokerage company and does not provide financial advice.