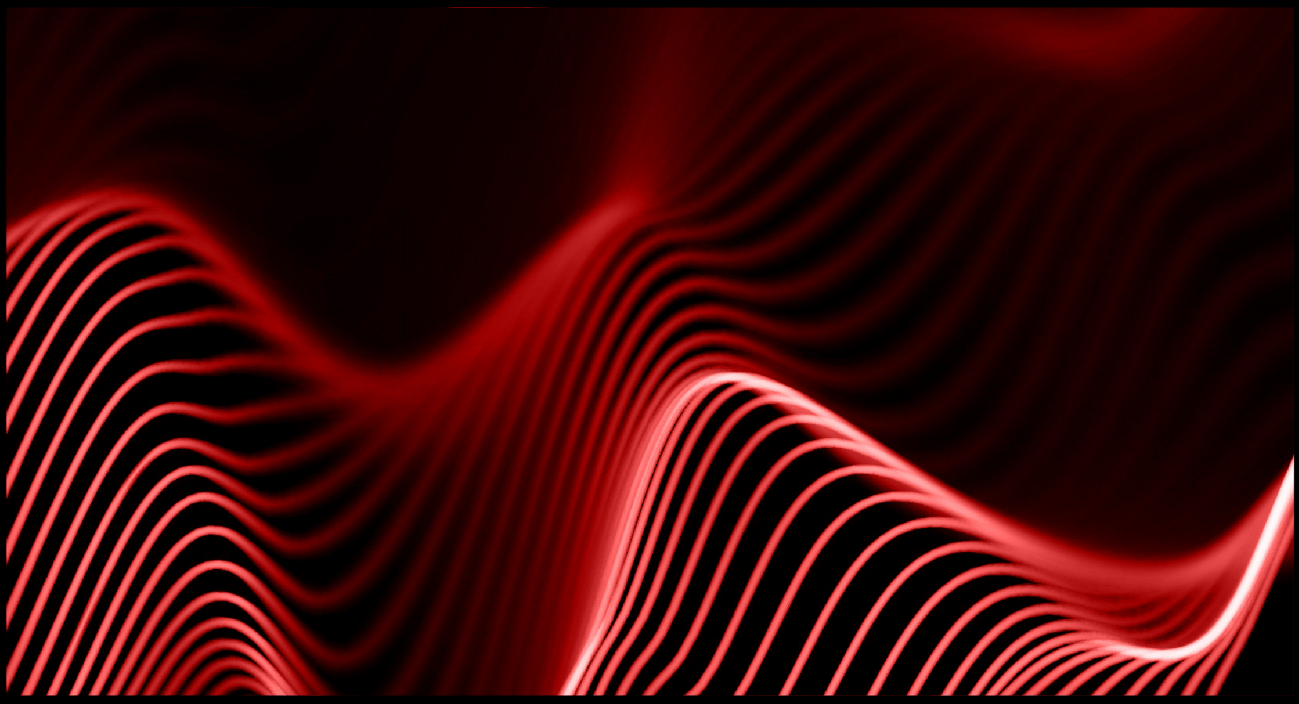
CERTIK
SKYNET

2025 SKYNET KOREA WEB3 SECURITY & ECOSYSTEM REPORT

CertiK's 2025 Skynet Korea Web3 Security & Ecosystem Report profiles South Korea's market landscape and leading platforms.



Executive Summary

South Korea's Web3 market is at a unique inflection point. Regulatory tailwinds are lowering institutional barriers while raising security baselines, and super-app distribution led by leading Web2 corporations is turning once-experimental use cases into real consumer products.

This shift introduces a uniquely demanding threat model for security. Concentrated retail assets on a handful of platforms, complex vendor and supply-chain dependencies, and persistent state-linked adversaries create a higher bar for security. In Korea, security is not just smart contract security; it's key management and upgrade safety, custody and monitoring discipline, workforce and insider controls, and operational readiness when things go wrong.

CertiK's 2025 Skynet Korea Web3 Security & Ecosystem Report profiles South Korea's market landscape and leading platforms, analyzes security incident patterns and loss drivers, decomposes the attack surface into actionable controls, and illustrates the growing segments within the market.

Key Takeaways

The outsized role of Web2 companies sets enterprise-grade security expectations.

South Korea is unique in the active role that major corporations play in their Web3 ecosystem, onboarding Web2 users at scale. **Kaia (Kakao/LINE)** and **WEMIX** exemplify top-down, super-app distribution with heavy upfront security and compliance. Kaia and WEMIX are rated among the top of Korean companies according to Skynet's security ratings due to their high security standards.

Regulatory reforms enable institutions while raising the security floor.

South Korea continues to lead the charge in Web3 regulation. VAUPA mandates **80% cold storage**, segregated client fiat, 1:1 reserve matching, insurance/reserve funds, and real-time surveillance. The FSC's February 2025 pilot allowing listed companies and professional firms to hold/trade crypto opens the door to corporate balance sheets.

Recurring vulnerabilities and a persistent state-backed adversary define the security landscape.

A detailed analysis of major security incidents reveals that access control compromises, where attackers target administrative or multisig keys, are the leading cause of direct financial losses, accounting for **over $108 million** in major heists like **Orbit Bridge** and **PlayDapp**. This threat is magnified by the constant pressure from North Korea-linked actors, who employ sophisticated social engineering and custom malware, representing the most severe threat to the entire South Korean Web3 ecosystem.

Blockchain gaming remains uniquely positioned in South Korea.

The traditional gaming market provides a massive foundation for Web3 integrations. In 2024, South Korea was the fourth-largest games market globally, with **39 million players** generating **$9.5 billion** in revenue. This highly engaged user base continues to give Korean developers a significant advantage in launching and scaling GameFi projects, currently the largest category within the South Korean market.

Adoption is already mass-market.

Top Korean exchanges surpassed 16.2M unique users (**~32% of population**) holding ₩102.6T (~$70.3B) in crypto by early 2025; KRW was the most-traded fiat against crypto in 2024.

Stablecoins and RWA applications are emerging with Web2 enterprises leading the charge.

Kakao is positioning its Kaia blockchain to become a major stablecoin hub by not only recently onboarding **USDT** but also planning to launch its own **Korean won-pegged stablecoin**. This strategy aims to leverage Kakao's massive **49 million user base** to boost Kaia's utility for payments and other services, with emerging and supportive South Korea's stablecoin regulations.

Top Korean Web3 Projects

Name	Skynet Score	Project Type
WEMIX	95.34 AAA	Layer 1, Infrastructure
Kaia	93.23 AAA	Layer 1, Infrastructure
CROSS	91.01 AA	GameFi, Gaming
League of Traders	89.27 AA	SocialFi, Trading Platform
MARBLEX	89.27 AA	Gaming, Infrastructure
Upbit	86.96 AA	Exchange
MiL.k	86.21 A	Web3 Loyalty & Rewards Platform
Bithumb	83.46 A	Exchange
Metadium	82.13 A	DID
MediBloc	81.96 A	Decentralized Healthcare Platform
Paycoin	74.16 BBB	DeFi, Payment
Olympian Games	In Progress	Gaming

Figure 1 - Featured Korean Projects on CertiK's Skynet Ratings

South Korea’s Web3 Market Overview

The Evolution of Web3 in South Korea

South Korea's Web3 market is transitioning from a speculative, retail-driven environment to a structured industrial ecosystem. This shift is driven by the re-engagement of large conglomerates, a government policy change from restriction to promotion, and strategic investment from global blockchain protocols in the local developer community.

Since 2024, the South Korean Web3 market has undergone a significant transformation. The market's role as a retail liquidity hub for global projects is diminishing as it evolves into a builder-led industrial ecosystem that creates and retains value domestically.

Two key trends are driving this transformation. First, major global blockchain projects like **Avalanche, TON, Ripple**, and **Solana** are investing heavily in the local developer community through hackathons and support programs, cultivating a domestic talent base.

Second, recent regulatory changes are creating a more favorable environment for corporate participation. A February 2025 decision to allow listed companies to trade cryptocurrencies on a pilot basis has begun to remove barriers to corporate engagement. These developments are propelling the market from an investor-driven model to one focused on growth and value.

Event	Year	Significance
Korbit Founded	**2013**	Establishment of South Korea's first cryptocurrency exchange, marking the formal start of the market.
Bithumb Founded	**2014**	Launch of another major exchange that became a global leader in trading volume during the 2017 bull market.
ICO Ban	**2017**	The FSC prohibits all Initial Coin Offerings, shifting the industry's focus and pushing Korean projects overseas.
Real-Name Account Mandate	**2018**	The government requires real-name bank accounts for crypto trading to combat money laundering and enhance transparency.
Act on Specific Financial Info	**2021**	Full implementation of a law requiring VASPs to register with KoFIU and adhere to strict AML/KYC standards.
Virtual Asset User Protection Act	**2024**	South Korea's first comprehensive crypto law comes into full effect, focusing heavily on investor protection.
Corporate Crypto Trading Approved	**2025**	The FSC announces a pilot program allowing listed companies to own and trade virtual assets, a major policy shift.

Figure 2 - Timeline of Key Events in South Korea's Web3 Evolution

Analyzing South Korea's World-Leading Web3 Adoption

South Korea's high level of Web3 engagement is supported by robust growth data. This deep-rooted participation is built on advanced infrastructure, a distinct investor psychology, a rich talent pool, and an increasingly supportive regulatory environment.

What Makes the Korean Ecosystem Unique?

Digital asset adoption in South Korea is extensive. As of early 2025, unique users on the top five domestic cryptocurrency exchanges surpassed **16.2 million**, representing approximately **32% of the country's population**. This figure notably exceeds the 14.1 million stock investors reported at the end of 2024. Studies suggest that more than **one in four** South Korean adults owns digital assets.

The financial scale is also significant. These 16 million users hold an estimated **102.6 trillion South Korean won (approximately $70.3 billion)** in crypto assets. In 2024, the Korean Won (KRW) briefly became the **most-traded fiat currency** against cryptocurrencies globally.

Event	Significance
Total Crypto Users	Over 16.2 million (as of Feb 2025)
Adoption Rate (% of Population)	Approx. 32%
Total Crypto Assets Held	~$70.3 billion (102.6 trillion KRW)
Global Crypto Adoption Index (2025)	15th (Overall), 18th (Population-Adjusted)
KRW Trading Volume Dominance	Most-used fiat currency for crypto trading globall (Q1 2024)

Figure 3 - Key Metrics of South Korean Web3 Adoption (as of early 2025)

The Four Pillars of Growth: An Analysis of Key Market Drivers

South Korea's high adoption rates are founded on four interconnected drivers. The market's development is notably top-down, shaped by the coordinated efforts of the government, large conglomerates, and established tech giants, which is set to accelerate mainstream adoption.

- **1. Advanced Infrastructure and Web2 Corporate Integration.**

  Korea's Web3 ecosystem is built on its world-class technological infrastructure and the involvement of its largest corporations. Over half of the nation's 82 large enterprises, including **SK, LG, and Lotte**, are actively pursuing Web3 initiatives. Tech giants like **WEMADE, Kakao and Naver** are integrating Web3 features into their "super app" ecosystems, lowering the barrier to entry for millions of users and providing a direct path for mainstream consumers.

- **2. A Risk-Tolerant and Tech-Savvy Investor Psyche.**

  The South Korean investor base is technologically literate with a high appetite for risk. **Gaming** is uniquely positioned within South Korean culture and ties well with Web3 projects. This risk tolerance is particularly strong among younger demographics, who have driven a recent **$12 billion** surge in crypto-related investments, viewing digital assets as a primary vehicle for achieving higher returns.

- **3. A Deep Talent Engine and Tech-Forward Users.**

  South Korea boasts a strong talent pool with a larger developer population. The strength of this builder community is demonstrated by high participation in major Web3 hackathons.

- **4. Strategic Regulatory Tailwinds.**

  A critical driver is the government's strategic shift from a restrictive to a promotional regulatory stance. The 2024 **Virtual Asset User Protection Act** provided much-needed regulatory clarity and increased investor confidence. It also created a "sandbox" environment for experimenting with emerging technologies like Real-World Asset (RWA) tokenization and Decentralized Finance (DeFi). The government's pro-innovation stance is creating a secure and predictable environment for long-term investment.

Evaluating Security Threats in the Korea Ecosystem

The South Korean Web3 ecosystem operates within a uniquely challenging security environment. The threats are multi-layered, ranging from state-sponsored global adversaries to localized retail-level scams. A comprehensive understanding of these risk areas is critical for any project operating in the region.

Aggregated Analysis and Analytics

The expanded case studies reveal a multi-faceted and severe threat landscape for the South Korean Web3 ecosystem, extending beyond typical code exploits.

Project	Incident Date	Estimated Loss (USD)	Attack Vector Category	Key Lesson Learned
Youbit	2017	17% of Assets + 4,000 BTC	**State-Sponsored Attack**	Persistent attacks from nation-states can be an existential threat to exchanges.
Bithumb (2017)	2017	Indirect user losses	**Customer Data Breach**	Insecure user data is a liability that enables secondary attacks like phishing.
Bithumb (2018)	June 2018	$31.5 Million	**Centralized Exchange Breach**	Hot wallets on centralized platforms remain a primary and high-value target for hackers.
Bithumb (2019)	Mar 2019	$20 Million	**Insider Threat**	The risk of malicious or negligent insiders cannot be overlooked in security planning.
KLAYswap	Feb 2022	$1.9 million	**Supply-Chain Attack**	A project's security is only as strong as its weakest third-party dependency.
Terra-Luna	May 2022	>$40 Billion	**Protocol / Economic Design Failure**	Flawed economic models can be more destructive than any traditional hack.
GDAC	Apr 2023	$13 Million	**Centralized Exchange Breach**	Confirms that CEX hot wallet security is a recurring point of failure.
Orbit Bridge	Dec 2023	$81.5 Million	**Access Control Compromise**	Protecting multisig keys is paramount; their compromise nullifies decentralized security models.
SOMESING	Jan 2024	$11.5 million	**Unknown (External Hack)**	A coordinated and transparent public response is critical in maintaining community trust.
PlayDapp	Feb 2024	$290 Million(effectively $8 million)	**Access Control Compromise**	Centralized admin roles create single points of failure that bypass smart contract logic.

Figure 4 - Aggregated Analysis of Major South Korean Security Incidents

Case Studies of Notable South Korean Security Incidents

PlayDapp (2024)

- **Incident Date**: February 9, 2024
- **Reported Loss**: Originally priced at ~$290 million (effectively ~$8m due to token freezes)
- **Attack Vector**: **Access Control Compromise** (malicious minter role added)
- **Summary of Events**: An attacker compromised a private key and used it to grant a new address the authority to mint tokens. This address then minted 200 million new PLA tokens and began depositing them into centralized exchanges.
- **Key Takeaway**: A failure of operational security, not a smart contract flaw. It highlights the severe risk of contracts with powerful, single-key administrative functions.

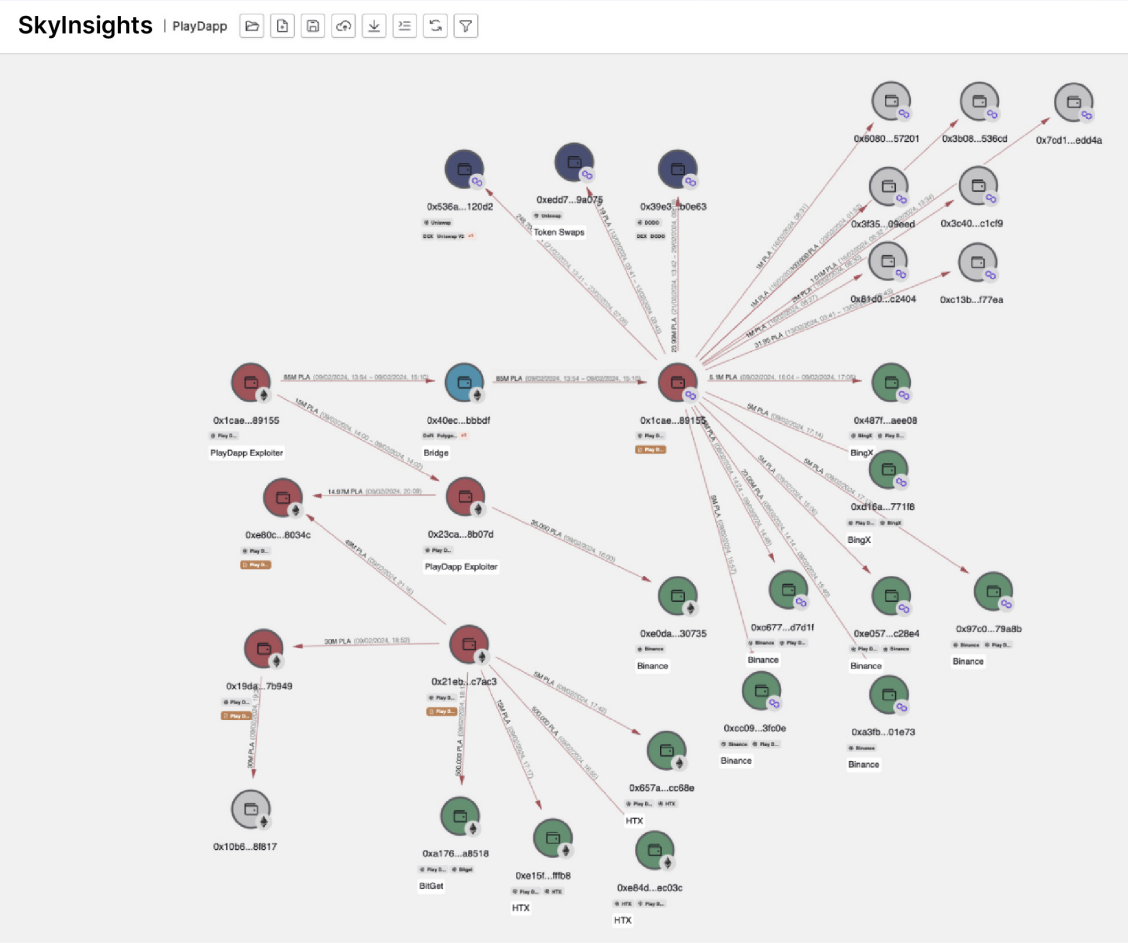


Figure 5 - CertiK SkyInsights Analysis of Fund Movement in the PlayDapp Incident

SOMESING (2024)

- **Incident Date**: January 27, 2024
- **Reported Loss**: $11.5 million
- **Attack Vector**: Unknown External Hack
- **Summary of Events**: An attacker stole 730 million SSX tokens. The SOMESING team stated the incident was conducted by professional hackers and was not an inside job, and they engaged with law enforcement and security firms to trace the assets.
- **Key Takeaway**: This case underscores the importance of a swift incident response plan, including coordination with law enforcement, to manage the fallout from a major breach.

Orbit Chain (2023)

- **Incident Date**: December 31, 2023
- **Reported Loss**: $81.5 million
- **Attack Vector**: Access Control Compromise (suspected compromised multisig keys)
- **Summary of Events**: An attacker drained approximately $81.5 million from the Orbit Chain cross-chain bridge. While the exact cause was not confirmed, analysis suggested the attacker gained control of a majority of the private keys for the bridge's multisig validator set, allowing them to approve fraudulent withdrawals.
- **Key Takeaway**: The exploit shows the critical importance of protecting administrative access. If enough private keys in a multisig scheme are compromised, the system's security model fails entirely.

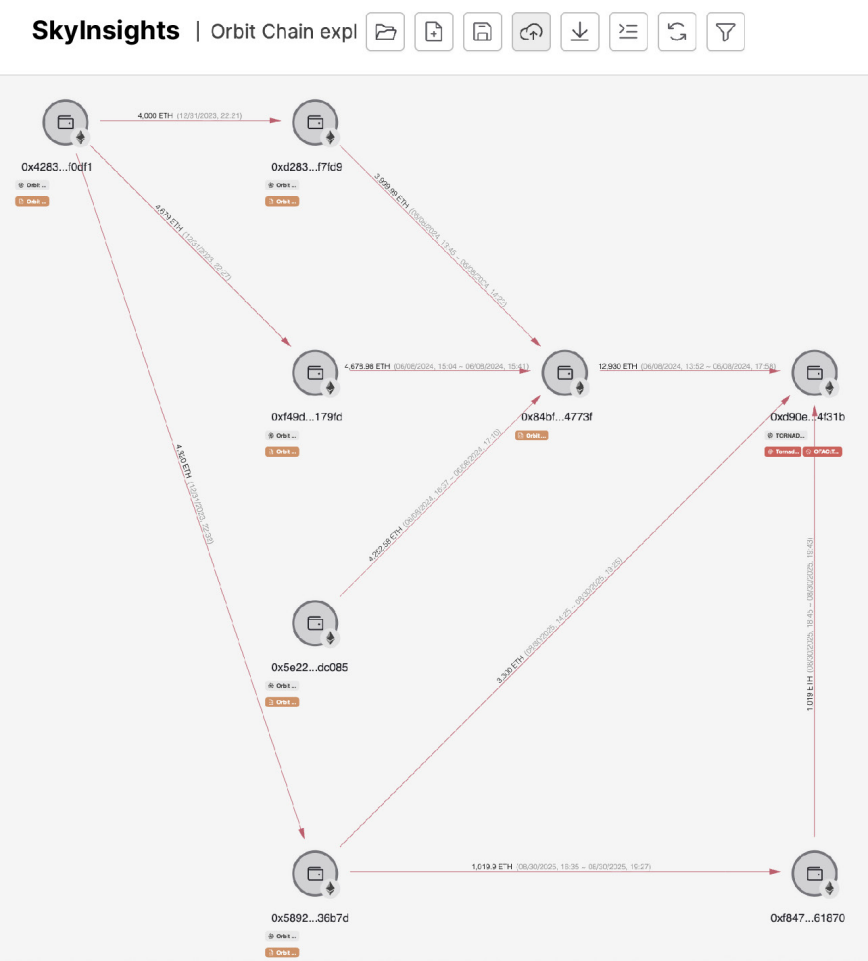


Figure 6 - CertiK SkyInsights Analysis of Fund Movement in the Orbit Chain Exploit

GDAC (2023)

- **Incident Date**: December 31, 2023
- **Reported Loss**: $81.5 million
- **Attack Vector**: Access Control Compromise (suspected compromised multisig keys)
- **Summary of Events**: An attacker drained approximately $81.5 million from the Orbit Chain cross-chain bridge. While the exact cause was not confirmed, analysis suggested the attacker gained control of a majority of the private keys for the bridge's multisig validator set, allowing them to approve fraudulent withdrawals.
- **Key Takeaway**: The exploit shows the critical importance of protecting administrative access. If enough private keys in a multisig scheme are compromised, the system's security model fails entirely.

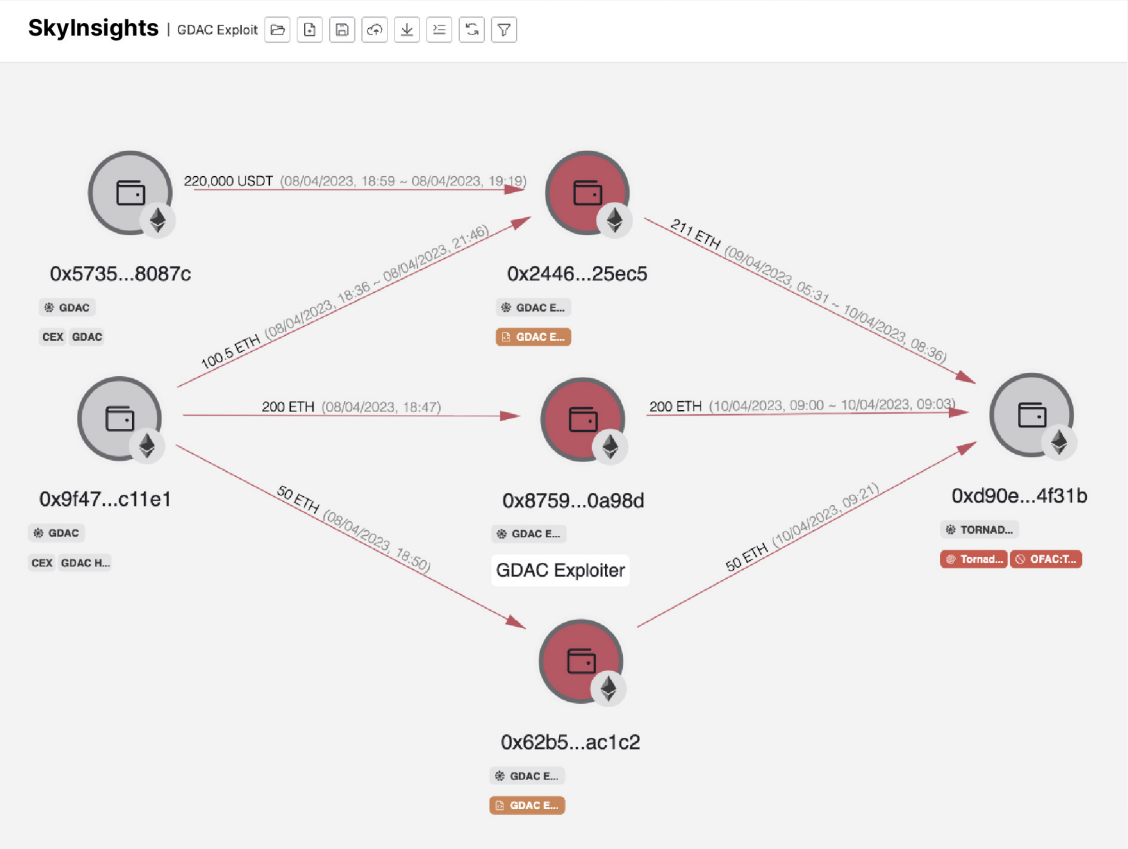


Figure 7 - CertiK SkyInsights Analysis of Fund Movement in the GDAC Exploit

Terra-Luna (2022)

- **Incident Date**: May 2022
- **Reported Loss**: Approximately $40 billion in market value wiped out
- **Attack Vector**: **Protocol / Economic Design Failure**
- **Summary of Events**: This was not a hack, but a catastrophic protocol failure. The algorithmic stablecoin TerraUSD (UST), which was designed to maintain a $1.00 peg via a mint-and-burn mechanism with its sister token LUNA, lost its peg during a period of extreme market pressure. This triggered a hyperinflationary "death spiral." As UST holders rushed to redeem it for $1 worth of LUNA, the LUNA supply swelled exponentially, causing its price to crash toward zero. The mechanism failed, and the value of both tokens was effectively erased, leading to massive systemic losses across the crypto industry.
- **Key Takeaway**: This event highlights the immense systemic risk of flawed economic design in protocols. It proved that, even without a code exploit or key compromise, a poorly designed mechanism can lead to a complete and irreversible ecosystem collapse.

KLAYswap (2022)

- **Incident Date**: February 3, 2022
- **Reported Loss**: $1.9 million
- **Attack Vector**: **Supply-Chain Attack** via a compromised third-party Software Development Kit (SDK))
- **Summary of Events**: Attackers compromised a legitimate JavaScript SDK file hosted by Kakao. When users visited the KLAYswap site, a malicious version of this trusted file was loaded, which rerouted their assets to attacker-controlled wallets. The attack did not exploit a vulnerability in KLAYswap's own smart contracts, but rather in its external dependencies.
- **Key Takeaway**:This incident is a classic example of a supply-chain attack, proving that a project's security depends on the integrity of all its dependencies. On-chain security alone is insufficient.

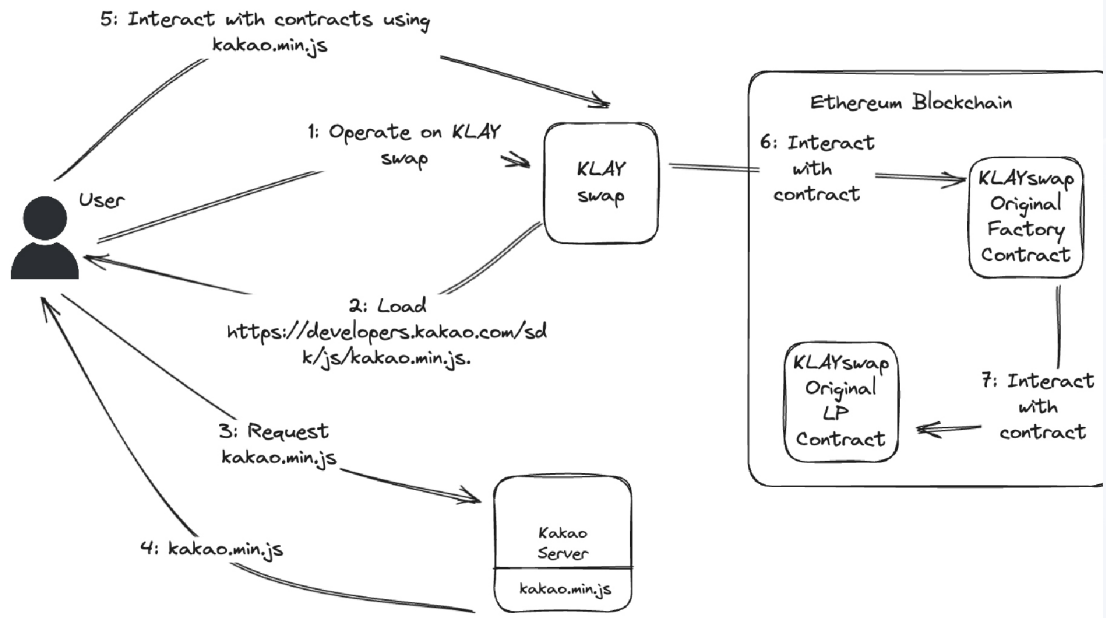


Figure 8 - Attack Flow Diagram of the KLAYswap BGP Hijack Incident

Bithumb (2017, 2018, 2019)

- **Incident Date**: 2017, June 2018, and March 2019
- **Reported Loss**: User funds lost to phishing (2017); $31.5 million (2018); ~$20 million (2019)
- **Attack Vector**: Customer Data Breach (2017); Centralized Exchange Breach (2018); **Insider Threat** (2019)
- **Summary of Events**: Bithumb has suffered at least three major, distinct security incidents.
    - **2017**: A customer data breach enabled attackers to conduct successful phishing campaigns against users.
    - **2018**: Hackers directly breached the exchange's hot wallets, stealing approximately $31.5 million.
    - **2019**: The exchange lost another $20 million from its corporate funds. Bithumb stated this incident was not a hack of its cold storage but was an "accident involving insiders" and was being investigated as a likely inside job.
- **Key Takeaway**:This incident is a classic example of a supply-chain attack, proving that a project's security depends on the integrity of all its dependencies. On-chain security alone is insufficient.

Youbit (2017)

- **Incident Date**: April and December 2017
- **Reported Loss**: 4,000 BTC in April - an additional 17% of total assets in December
- **Attack Vector**: **State-Sponsored Attack** (suspected North Korea)
- **Summary of Events**: The South Korean exchange Youbit (formerly Yapizon) was hacked twice in less than eight months. The first attack in April 2017 resulted in the theft of 4,000 bitcoins. A second attack in December 2017 caused the loss of 17% of the exchange's remaining assets, which forced the company to halt trading, file for bankruptcy, and shut down permanently. South Korea's Internet and Security Agency (KISA) investigated the incidents, having previously blamed cyber-spies working for North Korea for the April attack.
- **Key Takeaway**:This case demonstrates the existential threat posed by persistent, state-sponsored cyberattacks, which can target a single entity repeatedly until it is forced out of business.

Attack Vector Analysis

The expanded analysis reveals four distinct categories of risk responsible for major losses:

- **Protocol & Economic Risk**: The **Terra-Luna** collapse stands in a category of its own, causing approximately **$40 billion** in market value destruction. This was not a hack, but a failure of the system's core economic design, demonstrating a fundamental risk layer beyond cybersecurity.

- **Access Control Compromise**: Responsible for the largest direct thefts, this category includes **Orbit Chain** and **PlayDapp**. These attacks targeted administrative keys to bypass normal protocol rules, accounting for over **$108 million** in stolen funds.

- **External & Internal Threats to Centralized Entities**: This broad category covers a range of incidents.
  - **Direct Hacks:** Breaches at **Bithumb (2018)** and **GDAC** resulted in over **$44 million** in losses.
  - **State-Sponsored Attacks:** The **Youbit** case shows the unique geopolitical risk faced by South Korean exchanges, leading to the platform's complete failure.
  - **Insider Threats:** The **Bithumb (2019)** incident, attributed to insiders, resulted in a **$20 million** loss, highlighting that threats can come from within an organization.

- **Supply-Chain & Data Integrity Risks**: The **KLAYswap** incident (supply-chain) and the **Bithumb (2017)** incident (data breach) represent attacks on the wider technological and data infrastructure surrounding a project, proving that security must extend beyond the blockchain itself.

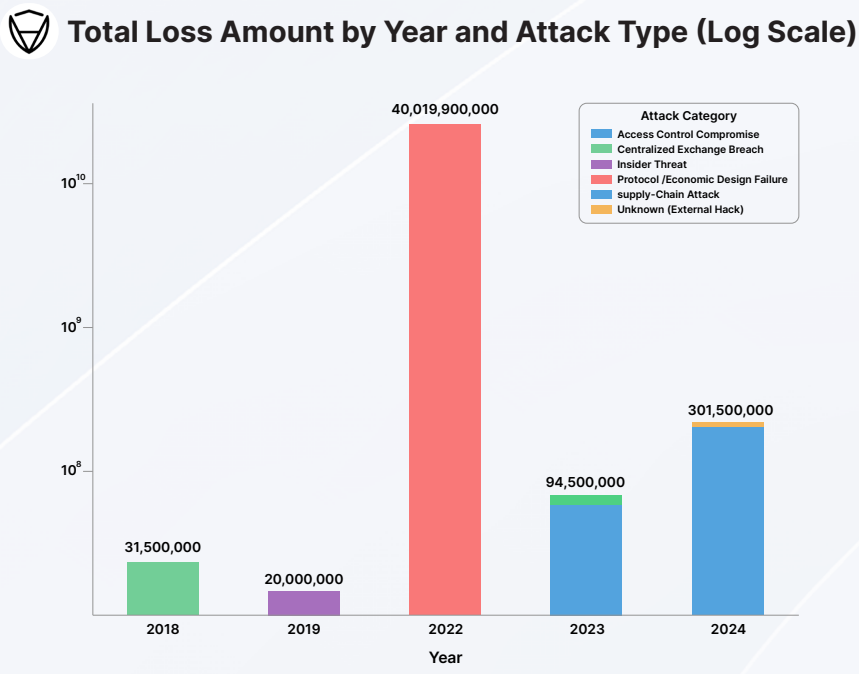


Figure 9 - Total Loss Amount by Year and Attack Vector Category (Log Scale)

Key Risk: The Geopolitical Threat (State-Sponsored Actors)

The geopolitical threat is the primary and most severe risk layer. The entire ecosystem operates under the persistent threat of sophisticated cyber campaigns conducted by the Democratic People's Republic of Korea (DPRK), most notably the Lazarus Group.

Their capabilities are state-backed and extensive, having been linked to thefts totaling over $6 billion since 2017 and a significant portion of all cryptocurrency stolen globally in recent years.

Their resources are state-backed, and their methods are sophisticated and constantly evolving. They have demonstrated consistent success in executing multi-hundred-million-dollar heists, making them an existential threat to any major pool of capital in the region.

- **Tactics:** Their methods are multi-faceted, combining technical prowess with intricate social engineering.
    - **Social Engineering**: They often initiate contact with employees at Web3 companies through platforms like LinkedIn, posing as recruiters with high-paying job offers. This leads to a series of fake interviews and eventually the delivery of a malicious PDF or document that installs a backdoor.
    - **Custom Malware**: They deploy custom malware families like TraderTraitor and AppleJeus, designed specifically to target cryptocurrency users and companies.
    - **Strategic Infiltration**: There is evidence of North Korean IT workers successfully gaining remote employment at crypto firms, giving them deep insider access to internal systems and private keys.

The constant pressure from a state-backed adversary fundamentally elevates the baseline security requirements for any project operating in or connected to the Korean market. Standard threat models, which typically account for financially motivated but less-resourced cybercriminals, are insufficient.

Korean projects must operate under the assumption that they are being actively targeted by a nation-state intelligence agency, necessitating a disproportionately high investment in counter-intelligence measures, intensive background checks for all personnel (especially remote), and a zero-trust architecture that treats insider threats as an inevitability. The financial losses from a single successful attack, such as the $81.5 million Orbit Bridge heist, far exceed the cost of these proactive defenses.

Key Risk: Centralized Infrastructure Risk

The structure of the South Korean market, which is heavily reliant on a few dominant centralized exchanges (CEXs), such as Upbit and Bithumb, creates significant systemic risk.This concentration of capital turns these exchanges into "honeypots," the most valuable targets for sophisticated threat actors.

Historically, these platforms have proven to be vulnerable to single points of failure. The hacks of Bithumb in June 2018, which resulted in a $31.5 million loss, and Upbit in November 2019, with losses exceeding $50 million, had catastrophic, market-wide consequences. These incidents highlighted that a compromise of a single exchange's wallet infrastructure is a matter of national economic importance.

In response, Korean regulators have made this risk a primary focus. The **Virtual Asset User Protection Act (VAUPA)**, which came into full effect in July 2024, directly addresses this threat by mandating stringent security controls. Key requirements include that exchanges must hold at least 80% of user assets in offline cold storage and enroll in insurance programs to protect users from the fallout of a potential hack.

While these regulations establish a much-needed higher security floor, they may also inadvertently create new challenges. The focus on achieving compliance can sometimes foster a "compliance-is-security" mindset, where resources are allocated to checking regulatory boxes rather than holistically addressing the unique, evolving threat landscape. Furthermore, the operational complexity required to manage a strict 80/20 cold-to-hot wallet ratio for a high-volume exchange increases the number of human touchpoints and intricate procedures. As major incidents have repeatedly shown, the most devastating attacks often exploit these very human and procedural failures. The complexity introduced by well-intentioned regulations, if not managed with extreme diligence, could create new avenues for operational security (OpSec) failures, turning a security measure into a potential attack vector.

Key Risk: Supply-Chain Vulnerability

The high degree of integration and partnership within the ecosystem creates a broad and complex supply-chain attack surface. Modern applications are rarely built from scratch; they rely on a web of third-party software packages and services.

- **The KLAYswap Precedent**: The KLAYswap hack serves as the canonical example of this risk. The attackers did not breach KLAYswap's own code, but instead compromised a trusted, third-party software development kit (SDK) provided by the tech giant Kakao. By "poisoning" this dependency, they were able to inject malicious code into KLAYswap's front end.

- **Beyond the Smart Contract**: This incident demonstrates that a project's security is only as strong as that of its least secure partner or software dependency. It proves that even a perfectly audited and secure smart contract can be compromised if the front-end interface that users interact with is fed malicious code from a trusted source.

Key Risk: Retail Speculator Targeting

The large, highly active, and often speculative retail user base constitutes the final layer of the attack surface. This group is a prime target for a high volume of lower-sophistication but highly effective attacks.

- **Exploiting FOMO:** The market's culture of rapid, trend-driven investing—partially evidenced by the "Kimchi Premium"—makes this user segment particularly susceptible to social engineering tactics that prey on the fear of missing out (FOMO).

- **Common Scams:** These attacks include sophisticated phishing campaigns that clone popular dApp websites, social media scams with fake airdrop announcements from impersonated project accounts, and fraudulent rug pulls where anonymous developers launch a token only to drain its liquidity and disappear. For these attackers, the sheer volume of active retail traders in Korea makes it a target-rich environment.

Skynet Korean Ecosystem Project Overview

The Three Pillars of the Korean Ecosystem

The blockchain ecosystem in South Korea can be understood as three unique interlinked pillars:

Corporate Initiatives, driven by the nation's large conglomerates, **Crypto-Native Applications & DeFi**, built bottom-up by local startups and communities, and **Core Infrastructure & Enablers**, including exchanges, investors, and technical service providers.

Each pillar has distinct goals, strategies, and security postures.

- **Corporate-led projects** prioritize mass adoption by leveraging existing user bases and brand trust; they tend to invest heavily in formal security measures (for example, **Kaia**, the merged Klaytn/LINE blockchain, maintains a high CertiK Skynet Score of **93.25 (AAA)**, reflecting rigorous security measures).

- In contrast, grassroots **crypto-native dApps** focus on rapid innovation and user growth in DeFi, NFTs, and gaming. These smaller projects often face greater security challenges, sometimes learning through costly incidents: **KLAYswap**'s $1.9M hack via BGP hijacking in 2022 is a case in point.

  Meanwhile, **core infrastructure players** form the backbone, providing platforms and funding. Exchanges and custodians in Korea have gradually tightened security after early breaches (**Bithumb**, for instance, lost $31.5 million in a 2018 hack, but later improved its practices, earning a Skynet Score of **83.59 (A)** in Skynet's exchange security rankings). Another notable example is **Upbit**, South Korea's largest exchange by trading volume, which incurred a $50M+ Ethereum hack in 2019 but has since reinforced its defenses and now holds a Skynet Score of approximately **87.04 (A)**, thanks to a combination of ISO-27001/ISMS certifications, extensive cold-wallet usage (now **98%**), and active bug-bounty programs. Venture investors like Hashed aggressively foster local projects, though they accept higher risk. **Hashed** reportedly lost over $3.5 billion in the Terra collapse, underscoring that each pillar balances opportunity and security differently.

Overall, these three segments collectively drive Korea's blockchain growth: corporates bring scale and credibility, crypto-natives bring innovation and community, and infrastructure players ensure stability and support, each with a tailored approach to strategy and security.

Corporate Initiatives

Korea's Unique Top-Down, Mass-Adoption Strategy

South Korea's corporate giants have pursued a top-down strategy to bring Web3 to the masses. Internet and gaming conglomerates are launching their own blockchains, platforms, and tokens, leveraging familiar services to onboard users en masse.

A prime example is **Kaia**, a new Layer-1 blockchain formed by the merger of Kakao's Klaytn and LINE's Finschia networks. By uniting two major tech platforms, Kaia aims to put Web3 at the fingertips of **200 million+ Monthly Active Users globally**. Kakao is positioning its Kaia blockchain to become a major stablecoin hub by not only onboarding **USDT** but also planning to launch its own **Korean won-pegged stablecoin**, evidenced by new trademarks. This strategy aims to leverage Kakao's massive **49 million user base** to boost Kaia's utility for payments and other services, though its success will depend on navigating South Korea's regulatory hurdles.

Another flagship project is **WEMIX**, launched by gaming giant WeMade. The WEMIX Network embeds blockchain into popular games (part of the play-to-earn wave) and has pursued rapid expansion through its own mainnet, DEX, and NFT platforms.

These corporate projects typically emphasize security and compliance from day one, understanding that any breach could damage their brand reputation. Accordingly, they undergo extensive audits and monitoring—for instance, **Kaia** received CertiK audits and boasts an **AAA Skynet security rating 93.25**, and **WEMIX** likewise holds an elite Skynet Score (**95.37, AAA**), ranking among the top secure projects.

The corporate entrants of blockchain in Korea are marked by big-budget projects (often backed by the likes of Samsung, Kakao, Naver, and major game companies) aiming for mainstream adoption with minimal friction. Their strategy is top-down: integrate blockchain into services people already use, and ensure security and regulatory checkpoints are met to build user trust. This approach has positioned corporate-backed platforms like Kaia and WEMIX as core pillars of Korea's Web3 landscape, bridging the gap between traditional internet services and the decentralized future.

Crypto-Native Applications & DeFi

Bottom-Up Innovation, User-Focused dApps

In parallel to corporate efforts, South Korea's homegrown crypto startups and developer communities have produced a rich array of crypto-native applications, from decentralized finance protocols to blockchain games. These projects grow bottom-up, often starting small but rapidly gaining users in the Korean market and beyond.

A hallmark example is **CROSS**, a blockchain gaming platform and "Game Token Protocol" launched in early 2025 by NEXUS. CROSS integrates Web2 user accessibility with Web3 asset ownership on an Ethereum sidechain, allowing each game to issue its own token and facilitating free, transparent player-to-player trading of in-game assets. The project's vision is to provide players with true ownership of all digital items, and it distinguishes itself with developer-friendly tools (SDKs and APIs) for building in-game economies.

These user-facing dApps prioritize community engagement and novel use-cases (gaming, collectibles, financial products) to drive adoption from the ground up. However, their agility and rapid growth can come at the expense of mature security processes. Many Korean DeFi/apps have had to contend with exploits and technical risks.

- For instance, **KLAYswap** suffered a unique exploit in February 2022: attackers hijacked internet routing (BGP hijack) to trick KLAYswap users into downloading malicious code, resulting in a **$1.9 million loss**. This incident—the first known BGP hijack attack in Korea's crypto sector—bypassed smart contract audits entirely, underscoring the diverse threat landscape such projects face.

- **CROSS**, by contrast, has not made headlines for hacks—the project underwent four CertiK audits as of September 2025 and currently boasts a high Skynet security score (~91, rated AA)—but like many young platforms, it faces challenges such as bootstrapping liquidity and sustaining user interest in a fast-moving market. According to CertiK's security assessments, community-driven apps can have varied security postures. This gap reflects how some grassroots projects still exhibit unresolved code or operational issues, while others (like CROSS) are now emphasizing security from the start through audits and community transparency.

Additionally, Korea's most ambitious crypto-native project, Terraform Labs' **Terra USD** stablecoin, demonstrated both the potential and peril of bottom-up endeavors: it achieved massive scale before collapsing disastrously in 2022, wiping out an estimated $40 billion in value and impacting thousands of Korean investors. The Terra saga (while a failure in economic design rather than security) nonetheless has made Korea's crypto community acutely aware of systemic risks in fast-growing projects.

In response, many crypto-native teams are now adopting better practices: open-source development, bug bounty programs, frequent audits, and community governance, to shore up confidence.

Core Infrastructure & Enablers

Foundational Services Driving the Ecosystem

The third pillar of Korea's blockchain arena comprises the essential infrastructure and supporting players that enable both corporate and crypto-native projects to thrive. This includes cryptocurrency exchanges, payment gateways, custodians, blockchain investors (VCs), and technical service providers (e.g. node operators, security firms).

- **Exchanges**: South Korea is home to some of the world's largest crypto exchanges by volume. Bithumb, founded in 2014, and its rivals (Upbit, Coinone, etc.) provide the on/off-ramps and liquidity that power the local market.

- **Venture Capital**: Funds like Hashed, a Seoul-based crypto VC fund, have seeded and mentored many prominent Korean projects.

- **Technical Providers**: Companies like CertiK provide security services to enhance the security of Korean ecosystem projects and users.

Notable Skynet Korean Project Standouts

Notable Korean projects featured on Skynet showcase a tremendous diversity in strategy and security ratings that reflect the ecosystem's multifaceted nature.

Top Korean Web3 Projects

Name	Skynet Score	Project Type
WEMIX	95.34 AAA	Layer 1, Infrastructure
Kaia	93.23 AAA	Layer 1, Infrastructure
CROSS	91.01 AA	GameFi, Gaming
League of Traders	89.27 AA	SocialFi, Trading Platform
MARBLEX	89.27 AA	Gaming, Infrastructure
Upbit	86.96 AA	Exchange
MiL.k	86.21 A	Web3 Loyalty & Rewards Platform
Bithumb	83.46 A	Exchange
Metadium	82.13 A	DID
MediBloc	81.96 A	Decentralized Healthcare Platform
Paycoin	74.16 BBB	DeFi, Payment
Olympian Games	In Progress	Gaming

Figure 10 - Featured Korean Projects on CertiK's Skynet

Core Infrastructure & Exchanges

Upbit: As South Korea's largest digital asset exchange, Upbit is a cornerstone of the nation's Web3 infrastructure. Launched in 2017 by fintech firm Dunamu (with Kakao's backing), it provides the primary fiat on-ramp for Korean crypto investors. Upbit regularly ranks among the global top-five exchanges by volume, processing **$2-4 billion in daily** trades and serving **8+ million verified users**. It reportedly handles about **73% of South Korea's exchange trading volume**, equivalent to roughly **$2.5 billion in daily volume as of 2025**. Upbit is known for its high liquidity, strict listing process (around 200+ listed coins), and robust security/compliance measures (e.g. >95% cold storage custody). These factors have cemented Upbit's role as the go-to exchange for KRW-based trading in Korea.

Bithumb: Founded in 2014, Bithumb is one of South Korea's oldest and most established cryptocurrency exchanges. It played a pivotal role in the market's early growth and was among the world's largest exchanges by volume during the 2017 bull market – at one point ranking #1 globally with nearly ₩1 trillion (≈$770 million) in 24h volume. Over the years, Bithumb has accumulated **over 8 million registered accounts**, and today its daily trading volumes are on the order of a few hundred million USD. The exchange has invested significantly in security upgrades (after some high-profile hacks in 2017-2018) and improved regulatory compliance. It holds an Information Security Management System (ISMS) certification and is working towards full licensing under Korea's digital asset regulations. Bithumb's longevity and large user base underscore its continued importance, even as it now faces strong competition and a reduced market share compared to Upbit.

Corporate-Led Platforms & Ecosystems

Kaia (KAIA): Kaia is a major corporate-backed Layer-1 blockchain formed by the 2024 merger of Kakao's **Klaytn** network with LINE's **Finschia** network. This unified chain aims for mass adoption by tapping into the enormous user bases of the KakaoTalk and LINE messenger apps (which together exceed **200 million+ MAU globally**). Kaia's design prioritizes scalability and speed: it sustains **over 4,000 transactions per second** with a 1-second block time and immediate finality, making it one of the fastest EVM-based L1s. The project emphasizes security and sustainability for mainstream use. Notably, Kaia engaged CertiK for comprehensive smart contract audits and ongoing security monitoring during its re-launch. It achieved a **Skynet Security Score of 93.25 (AAA)**, reflecting excellent code quality and community trust. By utilizing Skynet's real-time insights, the Kaia team can continuously track on-chain health and address any issues proactively. On the stability and payment side, Kaia recently partnered to integrate Tether's USDT natively: Crypto.com's Onchain Wallet now supports USDT deposits/swaps on Kaia, and **Tether launched USDT on Kaia's network**. Kaia is also rolling out local stablecoins: it plans to support Japanese yen, Korean won and Indonesian rupiah–pegged tokens. These features – combined with Kakao/LINE ecosystem integration – position Kaia as a backbone for bringing hundreds of millions of Asian users into Web3.

WEMIX (WEMIX): Launched by gaming giant WeMade, WEMIX has grown into one of the leading **blockchain gaming platforms** globally. The project has successfully embedded Web3 features into popular games—most famously, WeMade's MMORPG MIR4 introduced a play-to-earn model to millions of players worldwide. The WEMIX ecosystem now includes its own **L1 mainnet**, a decentralized exchange, an NFT marketplace, and dozens of game dApps. WeMade's focus on security is evident: WEMIX operates under a continuous audit partnership with CertiK, with **78 public smart contract audits** published to date. This rigorous approach has contributed to WEMIX's outstanding **Skynet security score of 95.37 (AAA)**—placing it near the top of CertiK's global leaderboard. The platform's emphasis on safety and transparency is further bolstered by a large community (over **460k on-chain community ratings** received) and in-depth on-chain monitoring. By leveraging its gaming IP (e.g. Legend of MIR franchise with 500+ million downloads historically) and robust security, WEMIX has positioned itself as a frontrunner in GameFi. It demonstrates how a top-down corporate player can drive Web3 adoption at scale—WEMIX's continuous security investment creates user trust, which in turn attracts more gamers and developers into its ecosystem.

Marblex (MBX): Marblex is the blockchain arm of **Netmarble**, another major Korean gaming company. Focused on integrating blockchain features into Netmarble's extensive portfolio of mobile games, Marblex represents the top-down, mass-adoption strategy employed by South Korea's large corporate players. Netmarble's games have a massive global audience (one popular title, Let's Get Rich, attracted **200 million+ players** worldwide), and Marblex aims to convert a portion of this audience into Web3 users. The Marblex platform issues game tokens/NFTs for titles like Ni no Kuni: Cross Worlds and A3: Still Alive, and it recently announced a migration of its ecosystem to an ImmutableX-powered chain for greater scalability. While specific usage metrics for Marblex are not publicly disclosed, the **active player base has been growing (up 40% in 2024)** according to press releases, and Netmarble is earmarking significant resources (including a $20 million ecosystem fund) to boost Marblex's Web3 gaming adoption. Marblex's strategy underscores how Korea's gaming leaders are embracing blockchain: by leveraging huge existing IPs and user bases, and layering in crypto rewards or NFT features, they aim to onboard mainstream gamers in a seamless way.

GameFi, NFTs, and Social Platforms

Cross The Tides (CROSS): An emerging project in the competitive GameFi sector, Cross The Tides is notable for being spearheaded by industry veterans from major Korean gaming companies like Nexon and WeMade. The project is building an open blockchain gaming platform (often referred to as "CROSS") that will host a suite of interoperable games and NFTs. While still early-stage, Cross The Tides has garnered attention for its experienced team and its vision of connecting AAA game content with decentralized ownership.

League of Traders (LOT): This platform addresses the social aspect of crypto trading by allowing users to engage in copy trading and other social finance activities. It has successfully gamified the trading experience to build a strong community.

Metadium (META): Metadium is a project specializing in decentralized identity (DID). Launched in 2018, it provides blockchain-based infrastructure for managing and securing personal digital identities. Metadium's platform allows users to control their own identity data and share verified credentials without relying on centralized authorities. Over the years, the project has contributed to DID standardization efforts and formed partnerships to drive adoption in the public and enterprise sectors. For example, Metadium partnered with Coinplug in an initiative to bring its DID system to government and corporate services in Korea. It also collaborated with hospitals (like Severance Hospital in Seoul) to explore **blockchain health record management**. In summary, Metadium represents the Korean projects targeting foundational Web3 infrastructure (digital identity) rather than finance or gaming. Its journey highlights both the opportunities and challenges for DID in gaining mass adoption.

Olympian Games (SOX): Developed by United Games Corp., Olympian Games is an ambitious project aiming to create the "world's first Metagame." It connects multiple, otherwise separate games through a "tri-meta" framework consisting of: a shared mythological lore based on ancient Greece; a unified economy powered by a single token, SOX, which is usable across all titles; and a cross-game competitive layer called the "League of Games" for tournaments and events. This approach is designed to create a more cohesive and interconnected player experience than is found on typical game platforms, where each title operates as a self-contained universe.

DeFi & Payments

Paycoin (PCI): Paycoin is a project focused on bringing cryptocurrency to real-world commerce through an integrated payment system. Developed by Danal (a major Korean payments company), Paycoin launched in 2019 and rapidly built a sizable network of retail partners in South Korea. By 2022, Paycoin's payment app had **over 3 million users** and was accepted at **150,000+ merchant locations nationwide**, including major franchises like **7-Eleven, KFC, Domino's Pizza**, and dozens of others. This made PCI one of the most broadly used crypto payment tokens in the country. The system works by allowing users to top-up PCI and spend it via a mobile app or prepaid Mastercard, with merchants receiving instant conversion to fiat. Going forward, the project is also expanding globally through partnerships (e.g., with Singapore's Triple-A payment gateway) to enable PCI payments overseas. Paycoin stands as a prime example of real-world blockchain utility in Korea—successfully integrating with point-of-sale systems to let users buy coffee or meals with crypto as easily as they would with cash.

Specialized & Real-World Use Cases

MiL.k (MLK): MiL.k is a lifestyle loyalty point integration platform that has achieved notable real-world traction. The platform allows users to combine, exchange, and spend loyalty points from various major Korean companies by converting them to a single token (MLK). This effectively **unifies fragmented reward programs** into one ecosystem. MiL.k has amassed **1.5 million+ users** in its alliance and forged partnerships with many household-name brands in Korea, including airline and hotel groups, the OK Cashbag program (SK Planet), and even global partners like AirAsia Rewards.MiL.k's success in Korea demonstrates how blockchain can **seamlessly augment existing consumer reward systems**, bringing Web3 benefits to the masses without requiring them to be crypto-savvy.

MediBloc (MED): MediBloc is a long-standing project (founded 2017) aiming to create a **decentralized healthcare information ecosystem**. MediBloc built its own blockchain (Panacea, based on Cosmos SDK) to store and verify medical records and issued the MED token to incentivize participation. Over the years, MediBloc has partnered with multiple medical institutions in Korea. A notable collaboration was with **Severance Hospital** to develop a blockchain-based medical information platform for handling insurance claims, prescription records, and patient identity management. Additionally, MediBloc's tech partner WeavrCare rolled out a cloud EMR (Electronic Medical Records) solution called **Dr. Palette** that uses Panacea under the hood. As of Q1 2025, Dr. Palette has been adopted by **350 hospitals and clinics** as a trusted records system. By giving patients ownership of data and ensuring tamper-proof record sharing, MediBloc is helping to modernize Korea's medical data infrastructure in a patient-centric way.

CertiK Key Client Leader Skynet Showcase

Many of the aforementioned projects in the Korean ecosystem have partnered with CertiK to reinforce their security and transparency, showcasing a commitment to best practices. Here are the top two notable CertiK clients and analyze how they leverage security services:

Kaia (previously Klaytn & Finschia): As a major corporate-backed blockchain, Kaia engaged CertiK for smart contract audits and ongoing security monitoring. CertiK's audit of Kaia's new Layer-1 was in progress as of 2025, and the platform achieved a Skynet security score of **93.25 (AAA)**, reflecting excellent code quality and community trust. By utilizing Skynet's real-time insights, Kaia can continuously track its on-chain health and address any issues proactively.

WEMIX: WeMade's WEMIX network has made security a top priority through a deep partnership with CertiK. The project operates under a continuous audit program, completing 70+ audits accessible via CertiK's Skynet. This comprehensive audit history has contributed to WEMIX's outstanding Skynet Score of **95.37 (AAA)**.

The analysis of their options shows that Korean projects are increasingly opting for layered security, combining traditional audits with ongoing monitoring and community oversight. This approach is encouraged by regulators and expected by users. By prominently showcasing their CertiK engagement, projects like Kaia and WEMIX send a strong signal to the market that security is taken seriously. This creates a positive feedback loop where better security leads to greater user trust and adoption, further solidifying South Korea's reputation as a leader in secure blockchain development.

Navigating South Korea's Evolving Regulatory Landscape

South Korea's approach to digital asset regulation has evolved from risk containment to strategic industry promotion. The legal framework is a multi-layered system designed to protect investors while enabling institutional adoption and fostering innovation.

The Legislative Bedrock: Key Acts and Their Market Impact

Two key laws form the basis of South Korea's digital asset regulation: one focused on AML/KYC requirements and a more recent act centered on comprehensive user protection.

The Act on Reporting and Use of Specific Financial Transaction Information

This act, which took effect in March 2021, was the first major legislation to bring the cryptocurrency industry under regulatory oversight. The law required all VASPs to:

- Register with the Korea Financial Intelligence Unit (KoFIU).
- Obtain an Information Security Management System (ISMS) certification.
- Implement robust AML and KYC procedures.
- Partner with a domestic bank to provide real-name verified accounts.

This legislation institutionalized the industry but also created high barriers to entry, leading to market consolidation as smaller exchanges were forced to close.

The Virtual Asset User Protection Act (VAUPA) of 2024

Fast-tracked after the Terra-Luna and FTX collapses, VAUPA is South Korea's first comprehensive crypto law. It came into effect on July 19, 2024, with a strong focus on safeguarding investor assets and ensuring market integrity.

Regulatory Area	Specific Requirement under VAUPA
Asset Custody	VASPs must hold at least **80%** of users' total crypto deposits in **cold storage** (offline wallets).
User Deposits (Fiat)	Users' cash deposits must be segregated from the VASP's own funds and held in custody at a licensed local bank.
Reserve Management	VASPs must maintain cryptocurrency reserves that are equal in both amount and type to the assets deposited by customers.
Insurance & Reserves	VASPs are required to enroll in an adequate insurance plan or establish a reserve fund to compensate users.
Market Integrity	Prohibits unfair trading practices, including insider trading, market price manipulation, and other fraudulent activities.
Surveillance	Exchanges must establish real-time monitoring systems to detect and report irregular trading activities to the FSC.

Figure 11 - Key Regulatory Requirements under the Virtual Asset User Protection Act (VAUPA)

A Strategic Pivot: The Government's Pro-Web3 Agenda

Following VAUPA, the government has shifted to a pro-innovation agenda designed to foster sustainable growth. This includes two key policy developments:

1. **Legalizing Corporate Trading**: In February 2025, the FSC announced a pilot program to allow listed companies and professional investment firms to own and trade virtual assets, expected to bring significant corporate capital into the Web3 market.

2. **Institutionalizing Stablecoins**: The current administration has made the legalization of KRW-denominated stablecoins and spot crypto ETFs key parts of its financial reform agenda, with multiple bills already introduced.

Future Outlook: The General Act on Digital Assets and Regulated ICOs

The next legislative phase is expected to address gaps left by VAUPA, primarily focusing on the issuance of new digital assets. A proposed "General Act on Digital Assets" aims to create a comprehensive framework defining asset types, establishing licensing standards, and setting rules for issuance. This second phase is also expected to revisit the 2017 ICO ban, with a proposed bill seeking to replace it with a modern, disclosure-based regime.

Implications for Market Participants

The evolving regulatory landscape presents both opportunities and challenges for businesses.

- **Opportunities:** New regulatory clarity, the legalization of corporate crypto holdings, and forthcoming legal frameworks for stablecoins and STOs are creating a favorable environment for investment and new, regulated product categories. For international firms, the government's pro-innovation stance provides a more predictable and attractive market.

- **Compliance Challenges:** The new regulations impose a significant compliance burden. VAUPA's strict requirements, such as the 80% cold storage mandate and mandatory insurance, result in high operational costs. These standards favor larger, well-capitalized firms and may lead to further market consolidation.

Korean Market Landscape Analysis

The South Korean Web3 ecosystem is composed of several distinct sectors at different stages of maturity. The country's leadership in **GameFi** and its culturally-driven **NFT** market stand in contrast to a still-developing **DeFi** and **RWA** space. This disparity reflects Korea's unique economic strengths and regulatory priorities.

GameFi: South Korea's Uncontested Global Stronghold

South Korea's leadership in GameFi builds directly on its long-standing dominance in the traditional video game industry. The nation's vibrant gaming culture, advanced internet infrastructure, and crypto-savvy population create an ideal environment for GameFi innovation.

Market Dominance and Size

The traditional gaming market provides a massive foundation for Web3 integration. In 2024, South Korea was the fourth-largest games market globally, with **39 million players** generating **$9.5 billion** in revenue. The domestic video game market is projected to reach **$21.7 billion by 2030**. This highly engaged user base gives Korean developers a significant advantage in launching and scaling GameFi projects.

On the Horizon: Anticipated Titles and Emerging Trends

The Korean GameFi market is evolving beyond early Play-to-Earn models. The industry is now shifting to more sustainable models that integrate blockchain into established IPs. A key example is Nexon's MapleStory Universe, an ecosystem built on an Avalanche subnet. Its sister project, MapleStory N, has demonstrated a commitment to fair play and long-term ecosystem health by banning 20,000 bot accounts. This trend of leveraging strong IP to create sustainable Web3 experiences is expected to define the next phase of Korean GameFi.

Decentralized Finance (DeFi): A Sector Poised for Growth

South Korea's DeFi market is currently underdeveloped compared to its GameFi sector, primarily due to a historical regulatory focus on curbing speculation rather than fostering financial innovation. However, a legislative push focused on stablecoins is expected to unlock the sector's potential.

The Current State: An Underdeveloped Market

Despite high cryptocurrency trading volumes, South Korea's domestic DeFi market accounts for only 3% of the global market size. Only **15% of virtual assets** that entered the Korean market were transferred to a DeFi protocol, indicating a significant disconnect between centralized trading and on-chain financial activity. Regulatory obstacles, including the 2017 ICO ban and the lack of a clear legal framework, have created uncertainty and constrained growth.

The Stablecoin Catalyst: Unlocking Future Growth

The institutionalization of a Korean won-denominated (KRW) stablecoin is widely expected to be the catalyst for DeFi growth. The government has made creating a regulated KRW stablecoin a legislative priority.

Forthcoming legislation is expected to create a strict regime for stablecoin issuers, likely limiting issuance to licensed financial institutions. In anticipation, major tech companies like **Naver** and **Viva Republica (Toss)** are forming strategic partnerships with crypto exchanges and banks.

The first private test-launch of a won-pegged stablecoin, **KRWIN**, occurred in August 2025. A regulated KRW stablecoin will serve as the foundation for a domestic DeFi ecosystem, providing a low-risk on-ramp for users, a stable unit of account for protocols, and a bridge to the traditional financial system.

Kakao is actively developing its Kaia blockchain into a major stablecoin hub by supporting **USDT** and planning its own **Korean won-pegged stablecoin**, as confirmed by recent trademark filings.

Emerging Web3 Segments in South Korea

Beyond GameFi and NFTs, South Korea is strategically focusing on emerging sectors, particularly the tokenization of real-world assets (RWA), which is strongly supported by government initiatives.

Real-World Assets (RWA)

The convergence of traditional finance and blockchain is a key strategic priority in Korea. The government has established a regulatory framework for tokenized securities, with official guidelines released in late 2023. The domestic security token market is projected to reach $287 billion by 2030. The FSC has authorized the Korea Exchange (KRX) to establish a dedicated market for trading security tokens. Asset classes being explored for tokenization include Real Estate, Commodities, Bonds, and more.

Pioneering Initiatives: The Busan Digital Asset Exchange (BDX) and DePIN

The city of Busan is establishing the Busan Digital Asset Exchange (BDX), which will focus exclusively on trading tokenized real-world assets and will not list cryptocurrencies. In parallel, South Korea is becoming a hub for innovative models like Decentralized Physical Infrastructure Networks (DePIN). **Piggycell**, which once held a 90% share of the shared mobile charging market, is tokenizing its network of over 13,000 charging stations as NFTs, transforming a traditional business into a Web3 "Charge-to-Earn" (C2E) ecosystem.

Conclusion

The South Korean Web3 market is transitioning from a speculative phase to one of scaled production. This evolution requires a foundational approach to security, integrating it as a core operational principle rather than a final compliance check.

Korean Web3 companies and projects face a sophisticated threat environment. Leading projects are demonstrating their security posture through transparent reporting, continuous validation, and well-rehearsed incident response plans. To succeed, firms must deliver products that meet consumer application standards, provide verifiable documentation of their security controls, and align with South Korea's evolving regulatory framework. With a primary focus on security, South Korea is positioned not only as a significant growth market but also as a key driver for the secure, global adoption of Web3.

Check out the **Skynet** platform today and elevate your Web3 journey by learning more about the security insights of the projects highlighted in this report and reading more on the CertiK blog hub.

Protect your community and your organization today. Visit **CertiK.com** or get in touch at **bd@certik.com**.

CERTIK
SKYNET

Elevate Your Web3 Journey