

Crypto Asset Cybersecurity

Takaya Sugino

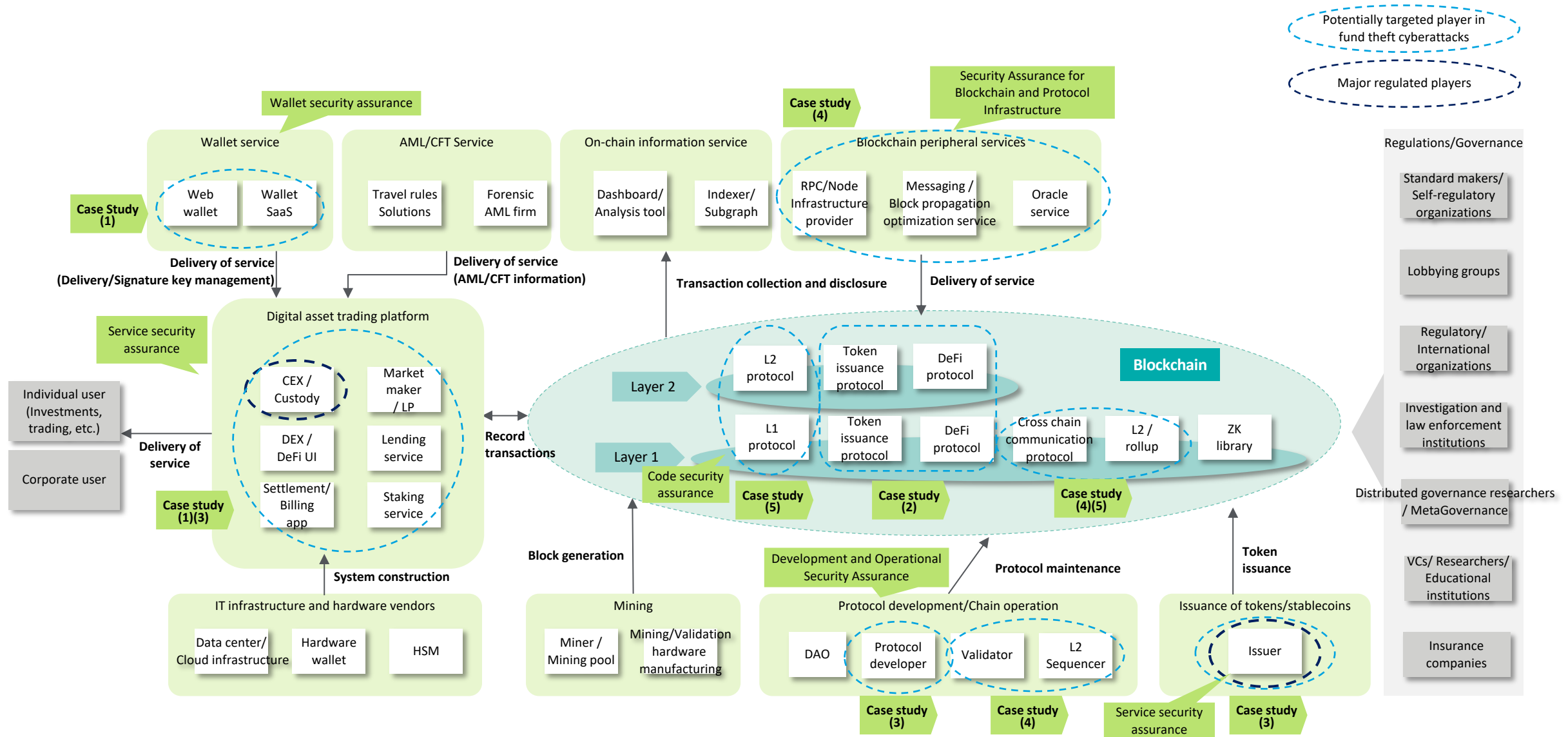
Crypto Assets & Stablecoin Division, JFSA

Policy Approaches to Strengthen Cybersecurity for Crypto-asset Exchange Service

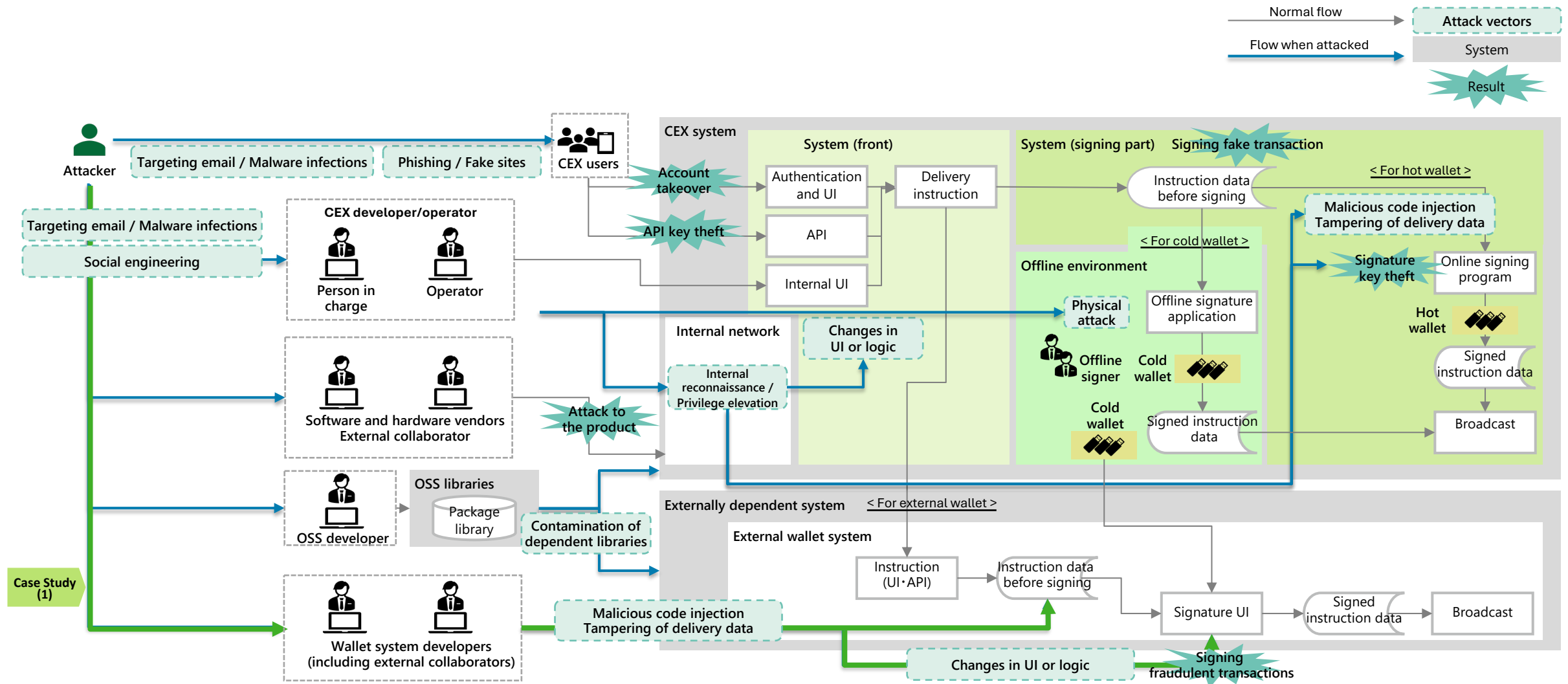
- **Crypto-assets are now widely seen as investment products**, but major cyberattacks resulting in asset losses continue to occur worldwide since the birth of Bitcoin.
- **Recent incidents often involve sophisticated methods, such as social engineering or attacks through third-party vendors**, and some are even suspected of involving state actors seeking to obtain foreign currency.
- **Given these risks, the ‘Working Group on Crypto-Asset Systems of the Financial System Council’ has called for stronger cybersecurity across the industry.** In response, the JFSA will encourage efforts by individual firms, promote cooperation within the industry, and provide public support.

Firm-level efforts	Mutual Support	Government Support
<p>Encourage crypto-asset exchange service operators to implement cybersecurity measures appropriately by</p> <ul style="list-style-type: none">• Closely monitoring each operator’s cybersecurity framework and carrying out industry-wide assessments and analysis• Considering higher cybersecurity standards in the JFSA supervisory guidelines, including staffing, external audits, and oversight of outsourcing	<p>Promote industry-wide mutual support to address cybersecurity challenges that individual firms cannot tackle alone by</p> <ul style="list-style-type: none">• Encouraging the self-regulatory organization (SRO) to strengthen its cybersecurity rules and enhance its audit capabilities• Encouraging operators to enhancing industry-wide knowledge sharing through participation in information sharing bodies (e.g., JPCrypto-ISAC)	<p>Provide public support to strengthen cybersecurity by</p> <ul style="list-style-type: none">• Analyzing past domestic/overseas cyberattacks (International Joint Research Project)• Continuously improving scenarios for crypto-asset exchanges in the JFSA-led cyber incident response exercise• Conducting threat-led penetration testing (TLPT) on some operators to demonstrate its effectiveness

A bird's-eye view of the players involved in the crypto ecosystem



Typical attack vectors and methods to CEX's fund outflow process

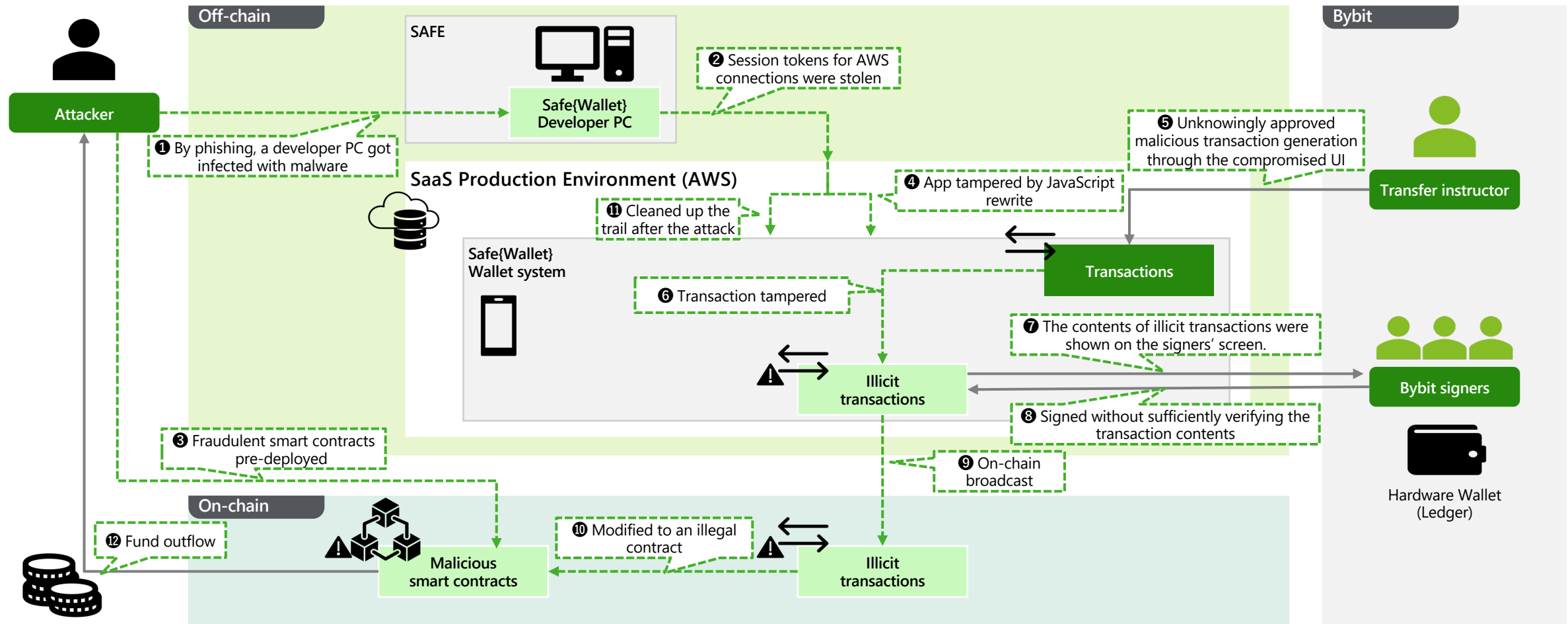


Attack Overview

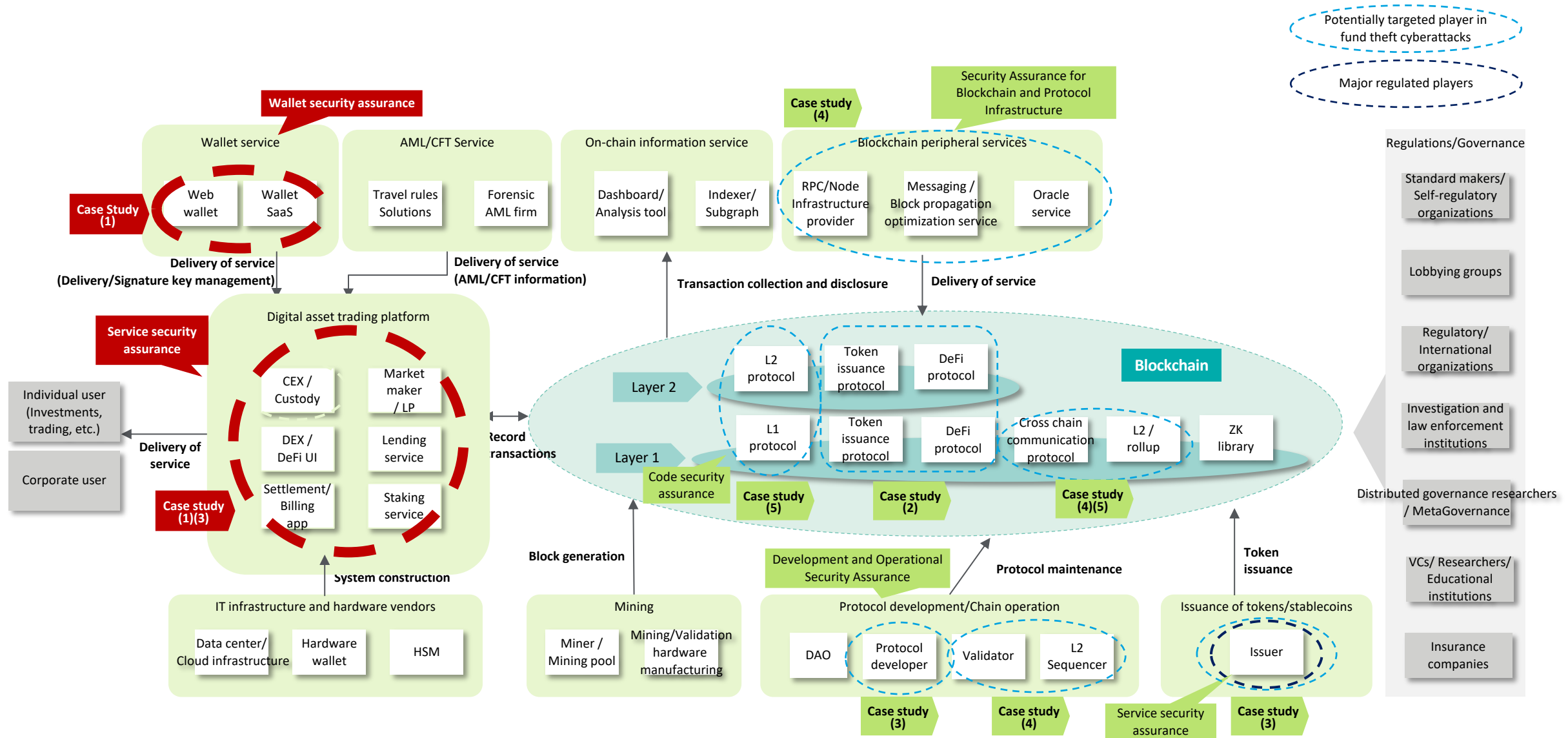
- Attackers compromised Safe's transaction interface through **social engineering**.
- Bybit personnel then approved and signed a malicious transaction without fully verifying its details, resulting in the asset theft.

Key Lesson

- Because smart contract transactions are difficult to interpret, they are prone to **blind signing**.
- Exchanges should implement controls to mitigate this risk, particularly **when using staking services or interacting with smart contracts**.



A bird's-eye view of the players involved in the crypto ecosystem



How Euler Finance works

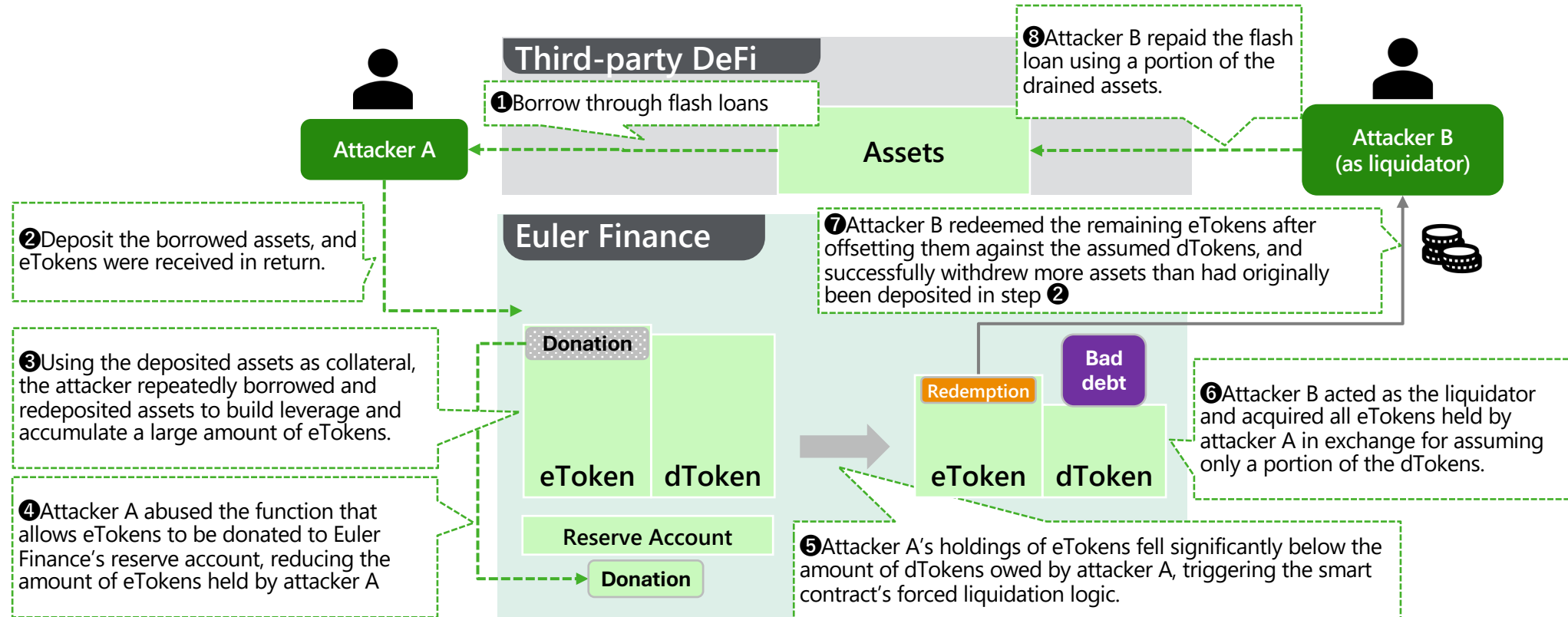
- Euler is a DeFi lending protocol that issues **eTokens** for deposits and **dTokens** for debt. Users can create leverage by repeatedly borrowing and redepositing assets. Undercollateralized positions are liquidated.

Attack Overview

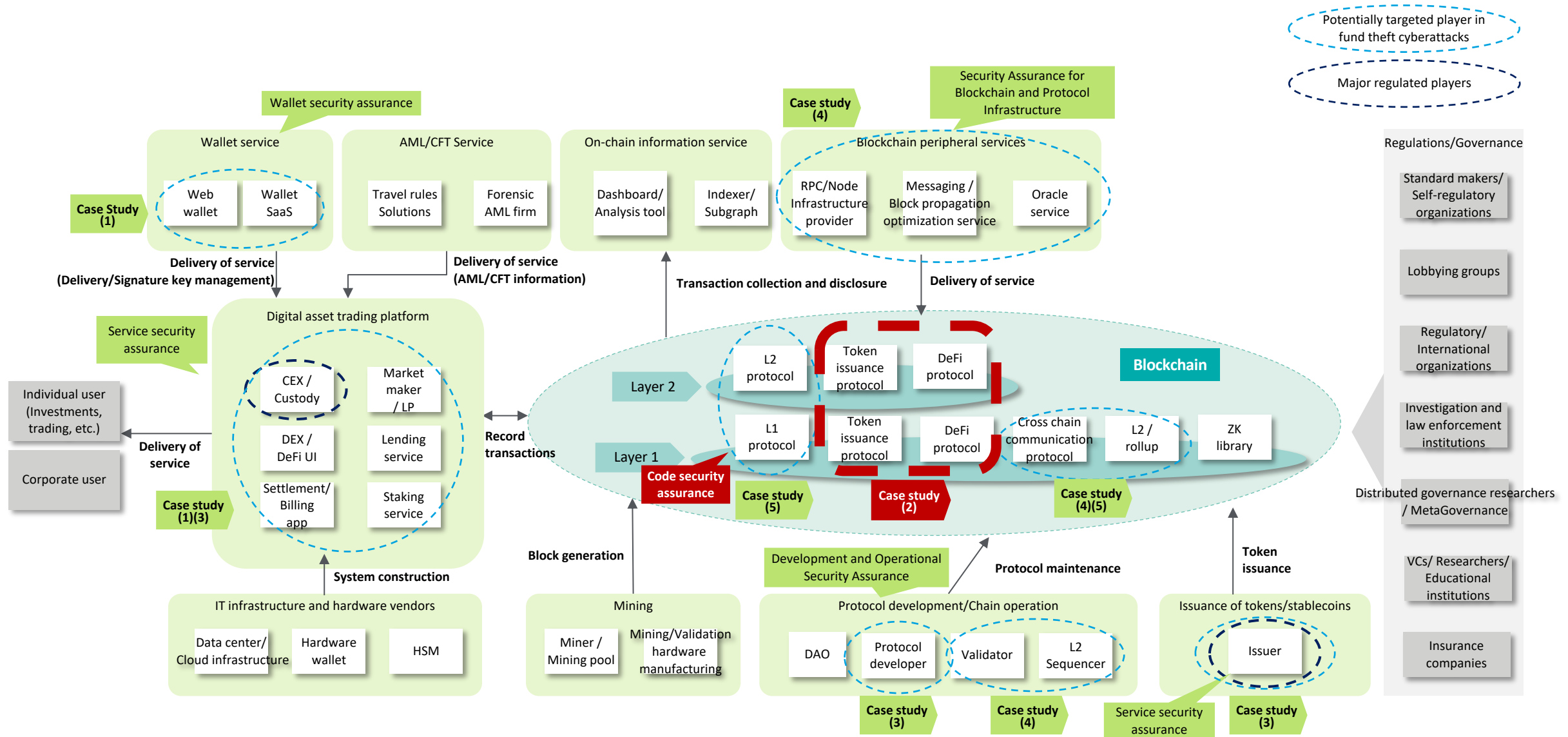
- The attacker used a **flash loan** to build a leveraged position and exploited the donation function to reduce collateral. A coordinating account then acquired the remaining eTokens while assuming only part of the debt, leaving Euler with bad debt. The attackers redeemed the eTokens and withdrew excess assets.

Key Lesson

- Smart contract vulnerabilities** can directly cause asset loss. Exchanges that rely on DeFi protocols may also face **supply chain risk**.



A bird's-eye view of the players involved in the crypto ecosystem

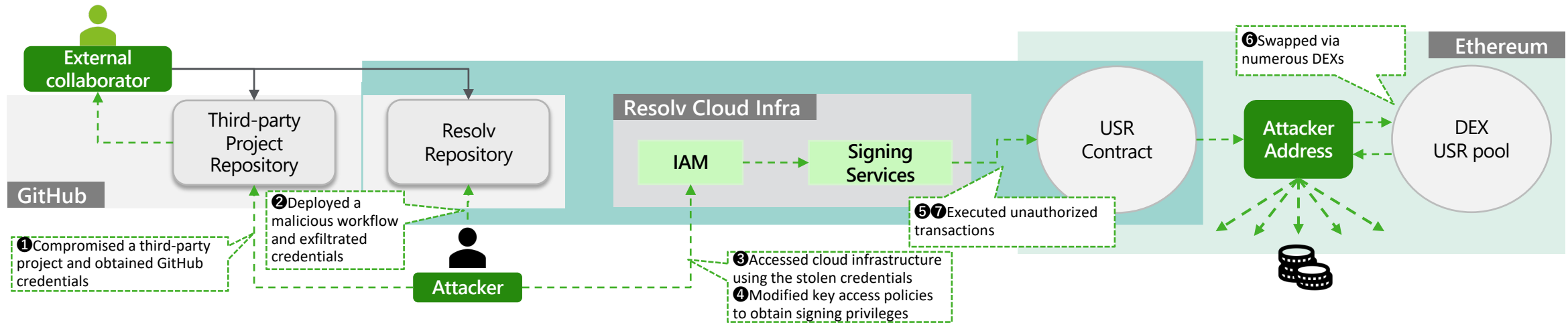


Attack Overview

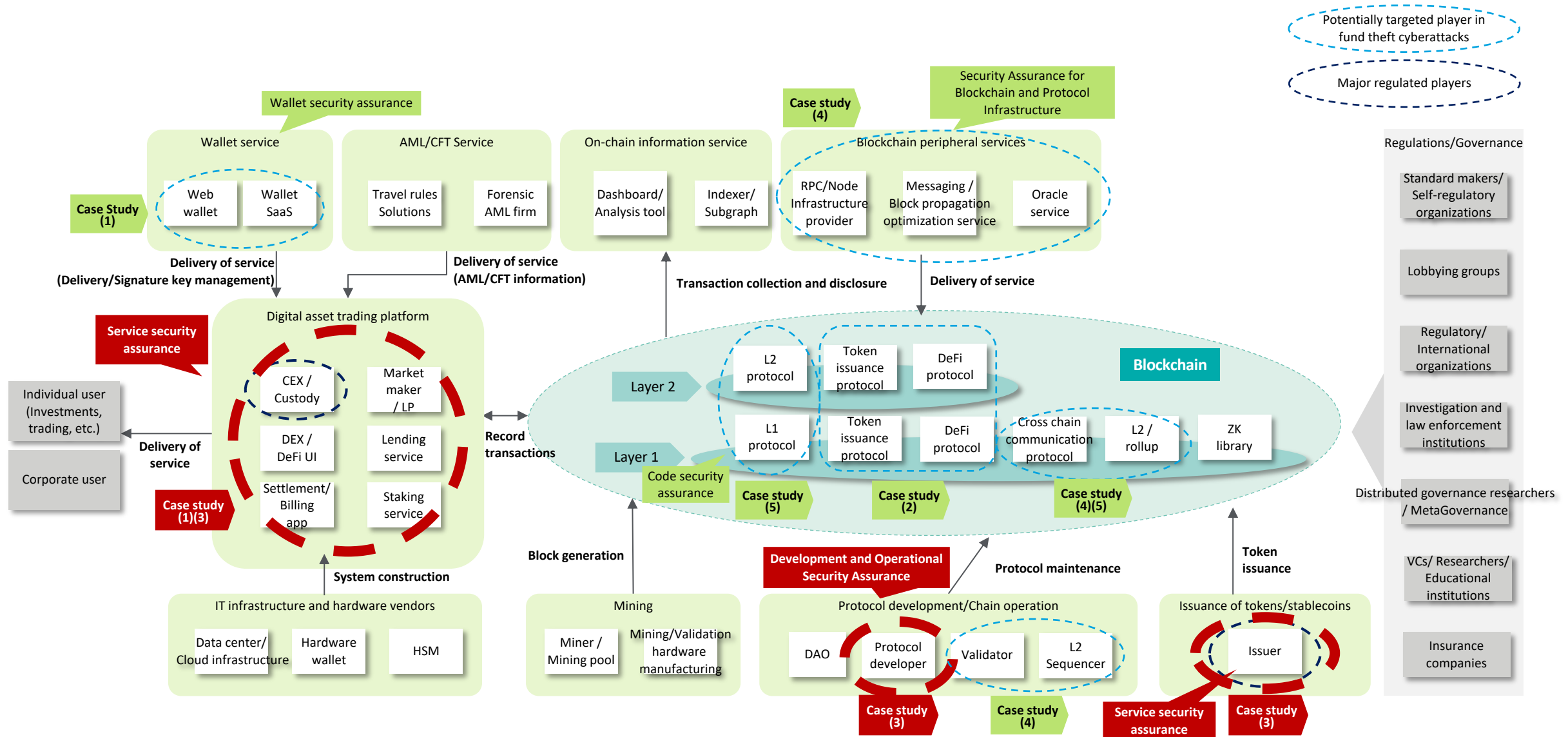
- Resolv is a DeFi protocol that issues USR, a 'stablecoin' backed by cryptoassets such as ETH, BTC, and USDC.
- Through **social engineering**, the attacker stole an external developer's credentials, accessed Resolv's cloud environment, and obtained signing authority for the USR smart contract. The attacker then fraudulently minted a large amount of unbacked USR.

Key Lesson

- Minting and signing privileges for blockchain contracts must be strictly controlled.
- Compromised signing authority may enable the **fraudulent minting of unbacked stablecoins**.
- Such tokens entering circulation may cause **losses to cryptoasset exchanges and users**.



A bird's-eye view of the players involved in the crypto ecosystem

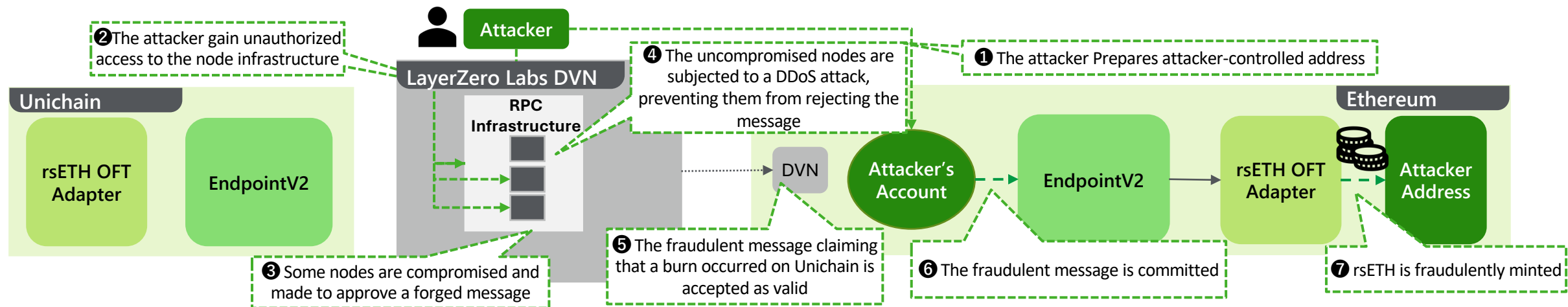


Attack Overview

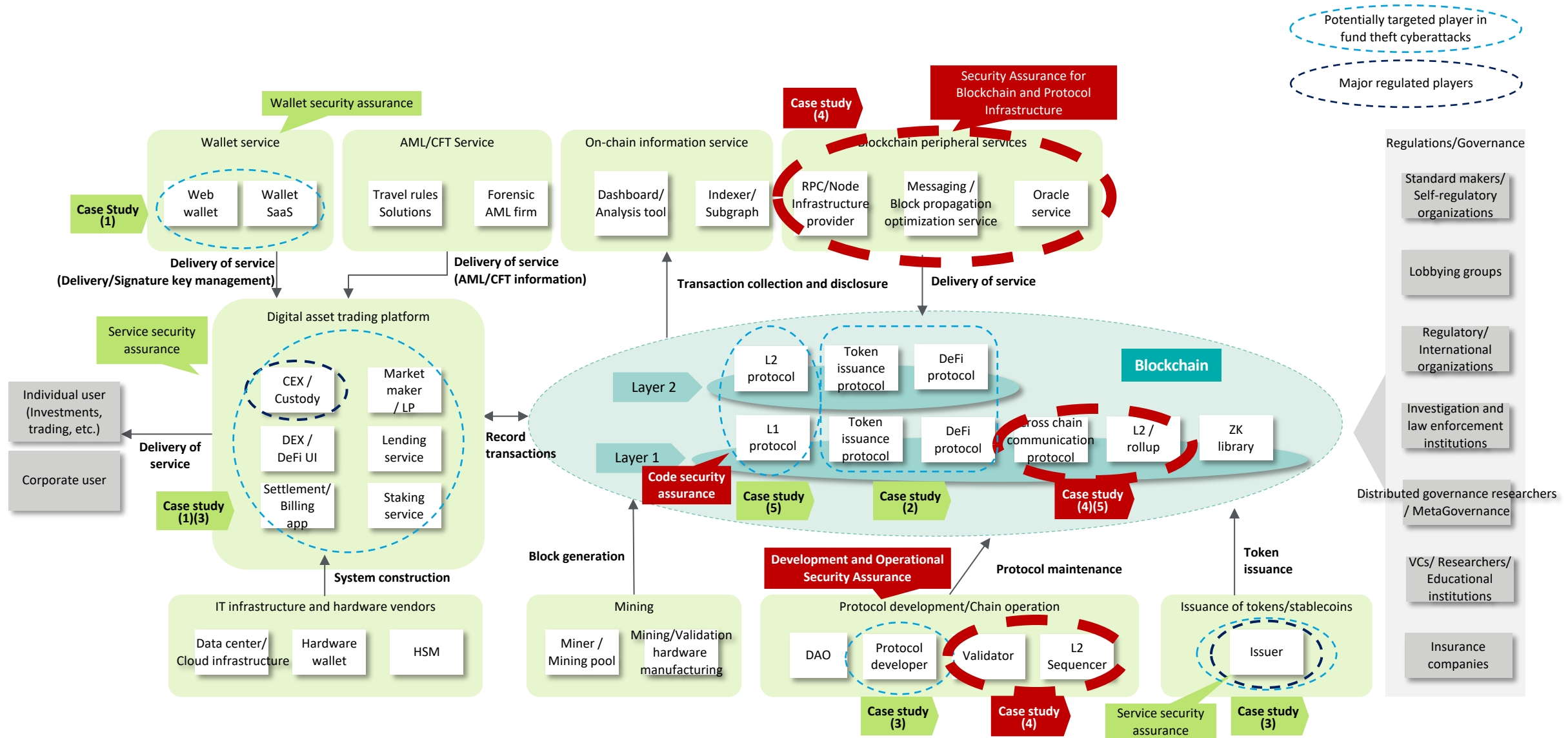
- LayerZero is a cross-chain messaging protocol that enables tokens burned on one chain to be minted on another.
- Kelp uses LayerZero to transfer its ETH-backed rsETH across multiple chains.
- The attacker fabricated a message indicating that rsETH had been burned on Unichain.
- This caused rsETH to be fraudulently minted to the attacker on Ethereum without a valid burn.

Key Lesson

- Weaknesses in cross-chain messaging may lead to **unauthorized token minting**.
- Fraudulently minted tokens may enter exchanges, causing price and loss risks.
- If unbacked tokens are used as collateral in DeFi lending, falling prices and liquidations may spread **credit risk** across the DeFi market.



A bird's-eye view of the players involved in the crypto ecosystem

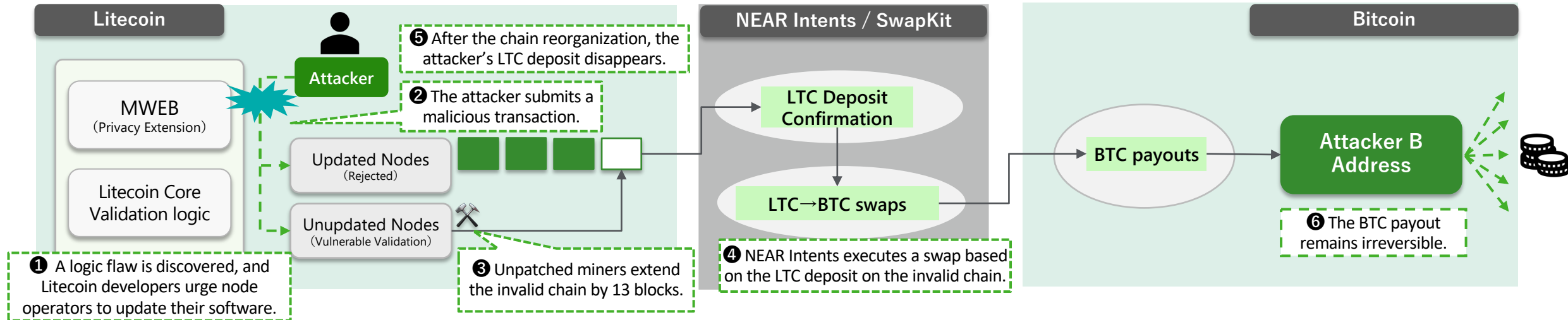


Attack Overview

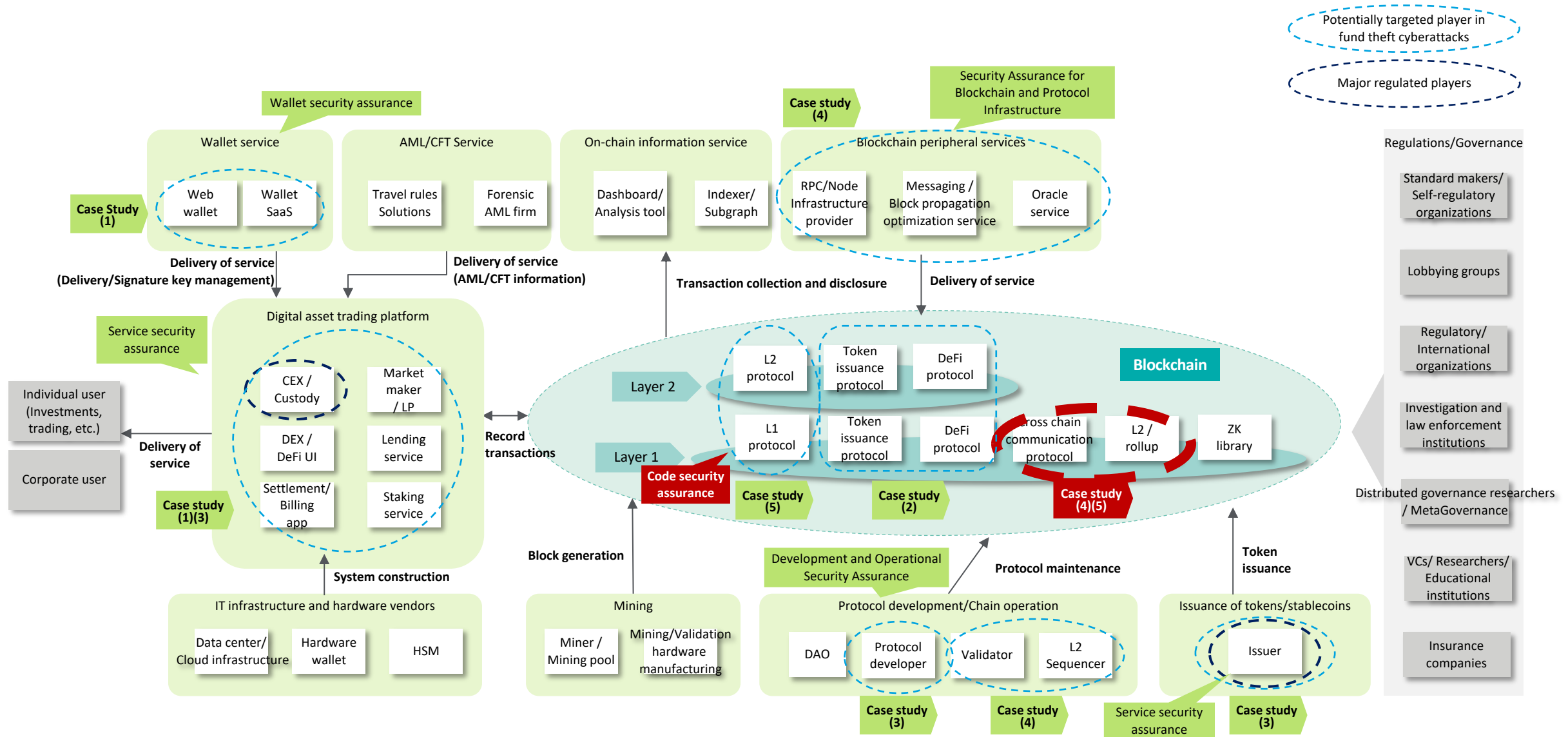
- NEAR Intents is a cross-chain protocol that enables token swaps across blockchains.
- The attacker exploited a Litecoin chain fork by depositing LTC on a branch that was later invalidated.
- NEAR Intents recognized the deposit and released BTC to the attacker.
- After the fork was resolved, the LTC deposit disappeared, allowing the attacker to obtain BTC without paying LTC.

Key Lesson

- Blockchain transactions may be reversed due to chain reorganizations.
- Attackers may exploit this to reverse deposits while retaining withdrawn assets.
- **Exchanges must assess transaction finality for deposits and withdrawals** based on each blockchain's characteristics.



A bird's-eye view of the players involved in the crypto ecosystem



Recommendations

Enhanced Third-Party Risk Management

- Identify risks arising from dependencies on third parties and subcontractors, and enforce least privilege, continuous monitoring, regular audits, and contractual controls.

Prevention of Malicious Code Injection and Tampering

- Separate development and CI/CD environments from signing and production systems, and implement strict credential management, change approval, integrity verification, and anomaly detection.

Prevention of Unauthorized Cryptoasset Transfers

- Independently verify transaction details and apply additional approvals or execution delays to high-risk transactions. Limit asset exposure and privileges, and use automated controls to contain losses.

Smart Contract and DeFi Risk Management

- Go beyond code audits by continuously managing administrative privileges, configuration changes, and external dependencies. Implement multi-party approval, timelocks, monitoring, and emergency shutdown mechanisms.

Use of Independent Assessments

- Review the scope and limitations of third-party assessments, and address uncovered risks through internal audits and continuous monitoring.