

# WLFI Incident Investigation and Token Analysis: A Post-Mortem of the Exploit and a Deep Dive into its Market Dynamics

Subscribe to my channel: @CryptoWithCedric  
<https://www.youtube.com/@CryptoWithCedric>

**Disclaimer:** This report was generated with AI assistance. Neither this report nor the video constitutes investment advice. All investments carry risk; please invest with caution.

## Section 1: Executive Summary

This report provides a comprehensive investigation into two distinct but interconnected aspects of the World Liberty Financial (WLFI) project: a targeted security breach resulting in the theft of WLFI tokens and a detailed analysis of the token's economic structure and market debut. The analysis reveals a project characterized by sophisticated financial engineering, significant structural risks, and a security incident that underscores the critical importance of user-level operational security.

The security breach was not a protocol-level vulnerability but a sophisticated, two-stage attack targeting individual users. The foundational precondition for the attack was the compromise of users' private keys through off-chain methods. This initial breach granted attackers full control of the victim wallets, enabling the second stage: the on-chain execution of a malicious delegatecall contract. This technique allowed the attackers to run arbitrary code with the authority of the victim's wallet, leading to the complete draining of all ETH and WLFI tokens. The incident serves as a critical reminder that even in the presence of secure smart contracts, the end-user remains a primary vector for exploitation.

The analysis of the WLFI token itself uncovers a profound disconnect between its public positioning and its underlying economic reality. Marketed as a "governance-only" token with no direct financial rights, its structure appears designed to navigate a complex regulatory environment. However, a private revenue-sharing agreement directs 75% of all protocol revenues to a Trump-affiliated entity and 25% to

other insiders, entirely bypassing the token holders who bear the market risk. This "governance paradox" creates a fundamental misalignment of incentives.

Furthermore, the token's market launch was engineered through a classic "low float, high Fully Diluted Valuation (FDV)" dynamic. With a massive total supply of 100 billion tokens but a relatively small initial circulating supply, the token's valuation was highly susceptible to speculative pressure. This structure, combined with enormous unrealized gains for presale investors, created predictable and extreme volatility upon its debut on major exchanges. The project's entanglement with public markets through the ALT5 Sigma corporate treasury strategy further complicates its risk profile, blurring the lines between regulated financial markets and the crypto ecosystem.

Ultimately, the WLFI project emerges as a critical case study in the multifaceted risks of the contemporary digital asset landscape. It highlights the dangers inherent in celebrity-endorsed ventures, the necessity of deep due diligence beyond surface-level narratives, and the complex interplay between protocol design, market dynamics, and user security.

## **Section 2: Technical Post-Mortem of the WLFI Security Incident**

### **2.1 Incident Overview and Impact**

The security incident involved a series of targeted thefts of World Liberty Financial (WLFI) tokens and other high-value assets, including ETH, from multiple user addresses.<sup>1</sup> The attack vector was not a systemic flaw within the core WLFI protocol but rather a sophisticated method deployed against individual wallets that had been previously compromised. The operational impact on affected users was severe and total; attackers successfully drained the entire balance of the targeted wallets, leaving no assets behind.<sup>1</sup>

It is critical to disambiguate this specific, verifiable security breach from unrelated and misleading information found in the public domain. Several online articles use phrases

such as "wlfi accidents west lafayette" and "wlfi body found".<sup>2</sup> Investigation reveals that these are search engine optimization (SEO) driven articles that conflate the WLFI token ticker with the call sign for a local news station in West Lafayette, Indiana (WLFI-TV). While these articles provide generic advice on crypto security, they contain no specific information pertaining to the World Liberty Financial token or the security incident analyzed herein and should be disregarded as data noise.

## **2.2 Attack Vector Deconstruction: The Malicious delegatecall Contract**

The execution of the theft was facilitated by a "malicious 7702 delegate contract".<sup>1</sup> To understand this vector, a foundational knowledge of the

delegatecall function in the Solidity programming language is necessary.

Foundational Concepts: Understanding delegatecall

delegatecall is a low-level, powerful opcode in the Ethereum Virtual Machine (EVM) that allows one contract to execute code from another contract while maintaining the context of the calling contract. This means the executed code operates on the calling contract's storage, receives its msg.sender, and uses its msg.value.<sup>5</sup> This mechanism is the cornerstone of the "proxy pattern," a widely used architecture that enables smart contracts to be upgraded. A simple proxy contract holds the state (i.e., the data in storage), while a separate logic contract contains the executable code. By using delegatecall to point to a new logic contract, developers can effectively upgrade a contract's functionality without requiring users to migrate their assets to a new address.<sup>6</sup>

The delegatecall Vulnerability

The power of delegatecall is matched by its potential for catastrophic vulnerabilities if implemented improperly. The primary risk stems from a condition known as "storage collision".<sup>6</sup> Because the logic contract's code operates on the proxy contract's storage, it is imperative that both contracts share the exact same storage layout. If the order, type, or number of state variables differs, the logic contract can inadvertently—or maliciously—overwrite critical data in the proxy's storage slots. For example, a function in the logic contract intended to modify a user balance (e.g., at storage slot 1) could instead overwrite the address of the contract owner or the logic contract implementation address (if they are located at slot 1 in the proxy contract), leading to a complete contract takeover.<sup>5</sup>

Forensic Analysis of the WLFI Attack

In the WLFI incident, the attack was executed through a malicious delegate contract. The analysis indicates that hackers "strategically placed the malicious 7702 delegate address in

the target wallet".<sup>1</sup> This phrasing implies a multi-step process. The "target wallet" in this context likely refers not to a user's Externally Owned Account (EOA) directly, but to a smart contract wallet or a related contract controlled by the user's EOA. After gaining control of the user's private key, the attacker would have forced this contract to execute a `delegatecall` to an attacker-controlled logic contract. This malicious logic contract would contain a function specifically designed to transfer all approved tokens (like WFLI) and native assets (ETH) to the attacker's address. By using `delegatecall`, this malicious transfer function was executed with the full permissions and authority of the victim's own contract, bypassing standard security checks.

## 2.3 The Critical Precondition: Private Key Compromise

A determinative factor in this incident is that the attack "requires the prior leakage of private keys".<sup>1</sup> This detail is paramount, as it reframes the event from a pure smart contract exploit into a composite attack rooted in a user-level security failure. The on-chain

`delegatecall` mechanism was the *method* of theft, but the private key compromise was the *enabling* root cause.

The logical sequence of this sophisticated, two-stage operation can be reconstructed as follows:

1. **Stage 1: Off-Chain Compromise.** The attacker first obtained the private key of a target user's wallet. This was likely achieved through traditional cybersecurity attack vectors such as phishing (tricking the user into revealing their seed phrase), malware (keyloggers or clipboard hijackers), or social engineering. This initial breach occurred entirely off-chain.
2. **Stage 2: On-Chain Exploitation.** With full control over the user's private key, the attacker could sign and broadcast any transaction on their behalf. The attacker then used this authority to set up the on-chain exploit. This involved either deploying a new malicious proxy contract funded by the victim's assets or, more likely, forcing an existing contract controlled by the victim to change its logic address to the attacker's malicious `delegatecall` contract. Finally, the attacker called the function that triggered the `delegatecall`, executing the asset drain.

This structure distinguishes the incident from common protocol-level exploits like reentrancy or integer overflows, which prey on flaws in a single, public-facing smart

contract.<sup>8</sup> Here, the vulnerability was not in the public WLF contracts but was introduced and exploited on a per-victim basis after their personal security was breached. The sophistication of the attack lies in this seamless combination of an off-chain intrusion with a highly effective on-chain exfiltration mechanism. It demonstrates that the security of a user's assets is not solely dependent on the security of the protocols they interact with, but is fundamentally anchored to the integrity of their own key management practices.

## 2.4 On-Chain Analysis of Fund Movement (Methodology)

While specific transaction hashes from the incident are not publicly available in the provided materials, a standard on-chain forensic analysis would be conducted to trace the stolen funds. This process leverages the public and immutable nature of the blockchain ledger and utilizes specialized analytics platforms.<sup>9</sup> The methodology would involve the following steps:

1. **Identification:** The initial theft transactions would be identified on a blockchain explorer. This involves pinpointing the exact transactions where assets were transferred from the victim addresses to the first layer of attacker-controlled wallets.
2. **Tracing:** Using on-chain analysis tools, investigators would map the flow of the stolen WLF and ETH. Attackers typically use a series of intermediary wallets to obfuscate the trail, moving funds rapidly through newly created addresses.
3. **Monitoring:** The attacker's wallets would be flagged for continuous monitoring using platforms like Glassnode, Nansen, or Arkham.<sup>9</sup> Alerts would be set to track any outbound transactions.
4. **Destination Analysis:** The ultimate goal of the tracing is to follow the funds to an exit point. This is often a centralized exchange (CEX), where the attacker might attempt to cash out into fiat currency. Transactions to CEX deposit addresses are critical, as exchanges are regulated entities that often have Know Your Customer (KYC) information on their users. Alternatively, attackers may move funds to privacy-enhancing protocols or coin mixers to break the on-chain link to the stolen funds.

## 2.5 Security Recommendations and Mitigation Strategies

A post-mortem analysis of this incident yields critical, actionable recommendations for both users and developers to prevent similar attacks, structured to address the root causes identified.<sup>12</sup>

#### **For Users:**

- **Private Key Security:** The absolute priority must be the safeguarding of private keys and seed phrases. Use hardware wallets to store significant assets, as they keep private keys in a secure, offline environment, immune to online threats like malware.
- **Phishing Awareness:** Be hyper-vigilant of phishing attempts. Never enter a seed phrase into a website, and never click on unsolicited links or connect a wallet to an untrusted decentralized application (dApp).
- **Permission Management:** Regularly review and revoke token approvals and smart contract permissions for dApps that are no longer in use. This limits the potential damage if a previously trusted application is exploited.

#### **For Developers:**

- **Avoid Low-Level Calls:** Exercise extreme caution when using low-level functions like `delegatecall`, `call`, or `callcode`.<sup>7</sup> These functions bypass many of the built-in safety checks of Solidity. If their use is unavoidable (e.g., for proxy patterns), ensure the implementation is based on thoroughly audited, open-source standards like the OpenZeppelin libraries.
- **Adhere to Secure Development Patterns:** Strictly follow best practices such as the "checks-effects-interactions" pattern to mitigate reentrancy risks. Ensure all state changes are completed before making external calls.<sup>7</sup>
- **Comprehensive Audits:** Subject all smart contract code to multiple, independent security audits from reputable firms. This is especially critical for contracts that handle user funds, manage permissions, or utilize complex and potentially dangerous architectural patterns like `delegatecall`.

### **Section 3: World Liberty Financial: A Tokenomic and Market Analysis**

### 3.1 Project Framework and the Governance Paradox

World Liberty Financial (WLFI) emerged as a high-profile decentralized finance (DeFi) platform, distinguished primarily by its prominent backing from the Trump family.<sup>15</sup> The project's stated mission is to advance U.S. leadership in the digital asset space by offering a regulated, U.S.-compliant frontend for DeFi services, built upon established protocols like Aave V3.<sup>19</sup>

#### The "Governance-Only" Claim

Central to the project's positioning is the explicit characterization of the WLFI token as a "governance-only" instrument.<sup>20</sup> The project's official terms and conditions state that the token confers no economic rights, no claim on revenue or distributions, and no equity in the underlying entity.<sup>21</sup> Furthermore, the terms explicitly caution that WLFI should not be acquired as a speculative investment or with an expectation of profit from resale.<sup>22</sup> This framing appears to be a deliberate attempt to classify the token as a utility token rather than a security under U.S. law.

#### The Economic Reality

This "governance-only" narrative is starkly contradicted by the project's foundational economic architecture. A revenue-sharing agreement, disclosed in the project's terms, dictates that 75% of the net protocol revenues are routed directly to DT Marks DeFi, LLC, an entity affiliated with Donald J. Trump, while the remaining 25% is allocated to other insiders.<sup>19</sup> Crucially, this entire economic flow occurs outside the tokenholder base.

This structure creates a profound "governance paradox." Token holders are granted the right to vote on the direction of a protocol, yet the financial success generated by that protocol exclusively benefits a separate, private group of insiders. This represents a fundamental misalignment of interests: those who govern the protocol have no direct economic stake in its revenues, and those who capture the revenues are not directly accountable to the governors. The deliberate separation of governance rights from economic rights can be interpreted as a form of regulatory arbitrage. By stripping the token of any explicit claim on cash flows, the project can argue for its utility status, while its market value is implicitly and inextricably tied to the hype and perceived success of the revenue-generating protocol. This structure effectively allows insiders to capitalize on the value generated by a community-governed network, undermining the core ethos of decentralized governance and raising significant concerns about investor protection and fairness.<sup>18</sup>

### 3.2 Deconstructing WLFI Tokenomics

The quantitative framework of the WLFI token was designed on a massive scale, with specific mechanisms governing its distribution and transition to a tradable asset.

- **Supply and Distribution:** The total supply of WLFI is fixed at 100 billion ERC-20 tokens on the Ethereum mainnet.<sup>20</sup> The initial distribution plan allocated 35% to the public token sale, 32.5% to community growth and ecosystem incentives, 30% to initial supporters, and 2.5% to the team and advisors.<sup>20</sup>
- **Initial State and Transition:** From its inception, the WLFI token was non-transferable and non-tradable, positioning it purely as a tool for participation in governance.<sup>19</sup> This changed following a community governance proposal in July, which passed with 99.94% approval, to make the token tradable. This vote set the stage for the token's public market launch on September 1st.<sup>15</sup>
- **Unlock Mechanism:** The initial liquidity event was structured to release only a fraction of the total supply. Early investors who participated in the presale rounds were allowed to unlock and trade 20% of their holdings at launch. The remaining 80% of their tokens remained locked, with future unlock schedules to be determined by subsequent governance votes.<sup>15</sup>
- **Presale Tranches:** The project conducted at least two presale rounds at significant discounts to the eventual public price. The first tranche was sold at \$0.015 per token, and the second at \$0.05 per token.<sup>21</sup> With the token debuting at a price above \$0.30, these early investors were positioned with unrealized gains exceeding 20x and 6x, respectively, creating immense latent sell pressure.

The following table consolidates the key tokenomic data for the WLFI token.

**Table 1: WLFI Tokenomic Profile**

| Metric                     | Value                           | Source(s) |
|----------------------------|---------------------------------|-----------|
| Total Supply               | 100,000,000,000                 | 20        |
| Token Standard             | ERC-20                          | 20        |
| Initial Circulating Supply | 24,600,000,000 (revised figure) | 15        |

|                                   |                           |    |
|-----------------------------------|---------------------------|----|
| Presale Tranche 1 Price           | \$0.015                   | 21 |
| Presale Tranche 2 Price           | \$0.05                    | 21 |
| Initial Unlock                    | 20% of Presale Allocation | 15 |
| Allocation - Token Sale           | 35%                       | 20 |
| Allocation - Community/Incentives | 32.5%                     | 20 |
| Allocation - Initial Supporters   | 30%                       | 20 |
| Allocation - Team/Advisors        | 2.5%                      | 20 |

### 3.3 Valuation Deep Dive: The Low Float, High FDV Dynamic

The valuation of the WLFI token at its launch was a direct product of its engineered tokenomics, specifically the dynamic between its market capitalization and its Fully Diluted Valuation (FDV).

#### Defining the Metrics

- **Market Capitalization** is a measure of a project's current market value. It is calculated by multiplying the *circulating supply* (the number of tokens available for trading on the market) by the current price per token.<sup>24</sup>
- **Fully Diluted Valuation (FDV)** represents a project's theoretical market value if its *total supply* of tokens were in circulation. It is calculated by multiplying the total supply (including all locked and unreleased tokens) by the current token price.<sup>26</sup>

A significant gap between a project's market cap and its FDV is a critical indicator for investors. It signals that a large portion of the token supply is held off-market, representing a potential "overhang" that could exert significant inflationary pressure on the price as those tokens are unlocked and sold in the future.<sup>25</sup>

WLFI's Valuation at Launch

WLFI exemplified the "low float, high FDV" model. Premarket derivatives trading suggested a staggering FDV ranging from \$20 billion to \$42 billion.<sup>21</sup> Upon its trading debut, the token achieved a market capitalization of just under \$7 billion, ranking it as the 31st largest cryptocurrency at the time.<sup>16</sup> However, with a total supply of 100 billion tokens, its FDV was vastly higher. The initial circulating supply was itself a point of contention, having been quietly revised upward from an expected 5% of total supply to 24.6 billion tokens, or 24.6%.<sup>15</sup> This structure appears to have been deliberately engineered to generate a speculative frenzy. The low initial float creates artificial scarcity, allowing for dramatic price movements with relatively less capital inflow. Simultaneously, the massive FDV creates a powerful marketing narrative, positioning the project among the largest in the crypto space and attracting speculative retail interest. This dynamic was explicitly compared to the type of low float, high FDV assets that trading firm Alameda Research historically favored for their immense volatility and trading potential.<sup>21</sup> The tokenomics were not optimized for price stability or sustainable value accrual but rather for maximizing launch hype and creating a highly volatile trading instrument. The enormous overhang of locked tokens represents a persistent threat of dilution, placing any investor purchasing tokens on the open market at a structural disadvantage to insiders and presale participants.

The table below illustrates the dramatic relationship between WLFI's market capitalization and its FDV at various price points around its launch.

**Table 2: WLFI Valuation Scenarios at Launch**

| Token Price | Circulating Supply | Market Capitalization | Total Supply | Fully Diluted Valuation (FDV) |
|-------------|--------------------|-----------------------|--------------|-------------------------------|
| \$0.20      | 24.6 Billion       | \$4.92 Billion        | 100 Billion  | \$20 Billion                  |
| \$0.30      | 24.6 Billion       | \$7.38 Billion        | 100 Billion  | \$30 Billion                  |
| \$0.42      | 24.6 Billion       | \$10.33 Billion       | 100 Billion  | \$42 Billion                  |

**3.4 Market Debut and Investor Behavior**

The launch of WLFI on September 1st was met with intense market activity, followed by the predictable volatility its tokenomics were designed to produce.

- **Launch Performance:** The token was listed on several of the world's largest cryptocurrency exchanges, including Binance, OKX, and Bybit, ensuring massive initial visibility and liquidity.<sup>16</sup> The market interest was substantial, with derivatives open interest approaching \$1 billion before the spot launch and trading volume exceeding \$1 billion within the first few hours of trading.<sup>15</sup>
- **Price Action:** The token's price initially surged above \$0.30 in its debut before succumbing to heavy selling pressure. It ended its first day of trading down approximately 12%, at a price of \$0.246.<sup>16</sup>
- **Sell Pressure Analysis:** This price decline was a direct and foreseeable consequence of the project's tokenomics. Presale investors, holding tokens acquired for as little as \$0.015, were sitting on unrealized gains of over 20x. The initial 20% unlock provided them with a powerful incentive to immediately sell a portion of their holdings to de-risk their position and recoup their entire principal investment, if not more.<sup>21</sup> This created a massive and immediate wave of sell-side liquidity that the market had to absorb, inevitably driving the price down from its initial peak.

### 3.5 The ALT5 Sigma Corporate Treasury Strategy

A particularly novel and complex element of the WLFI project was its strategic integration with a publicly traded company, ALT5 Sigma (ALTS), effectively transforming it into a corporate treasury vehicle for WLFI tokens.<sup>18</sup>

- **The Mechanism:** ALT5 Sigma, a micro-cap company that had evolved from a health-tech firm, raised \$1.5 billion through a share sale. A significant portion of these funds was then used to purchase WLFI tokens directly from World Liberty Financial. This transaction resulted in ALT5 holding approximately 7.5% of WLFI's total supply.<sup>23</sup> The deal involved a circular flow of capital, as World Liberty Financial was simultaneously the lead investor in ALT5's share sale, exchanging \$750 million worth of WLFI tokens for shares in ALT5.<sup>18</sup>
- **Strategic Implications:** This maneuver represents a sophisticated form of financial engineering designed to bridge the gap between traditional financial markets and the crypto ecosystem. It created a publicly traded proxy (ALTS stock) through which traditional investors could gain exposure to WLFI without directly engaging with crypto infrastructure. The large, publicly reported transaction also served to anchor and legitimize WLFI's multi-billion-dollar valuation. However, this strategy has drawn sharp criticism from former SEC officials, who warned that it

"brings the worst practices of the crypto ecosystem into regulated public markets" and places regulators in "strange and uncharted territory" due to the complex related-party transactions and valuation methods.<sup>18</sup> This blurring of lines introduces novel risks related to transparency and regulatory oversight and could serve as a template for other crypto projects seeking access to public market capital.

## **Section 4: Synthesis and Strategic Outlook**

### **4.1 A Nexus of Risk: Connecting Governance, Tokenomics, and Security**

The disparate elements of the WLF1 project—its governance structure, its economic model, and the security incident affecting its holders—are not isolated phenomena. They are deeply interconnected, creating a nexus of risk. The project's high-profile, celebrity-driven marketing, combined with tokenomics engineered for extreme speculation, cultivated an environment of intense market hype.

This environment is highly effective at attracting a broad spectrum of market participants, including a significant number of less-experienced retail users. These users, often drawn in by the promise of outsized returns, may be more susceptible to the social engineering and phishing campaigns that lead to private key compromises. In an atmosphere where the fear of missing out is palpable, diligence in personal security practices can wane. This creates a fertile ground for the type of targeted, two-stage attacks detailed in Section 2. The project's fundamental design, therefore, inadvertently increased the attack surface at the user level, demonstrating that security risks in a crypto project extend far beyond its smart contract code.

### **4.2 Broader Implications for the Digital Asset Ecosystem**

The WLF1 saga offers several critical lessons and portends future challenges for the

broader digital asset industry.

- **Celebrity-Backed Ventures:** WLFI stands as a potent case study on the inherent risks of celebrity-endorsed crypto projects. In such ventures, the power of the brand and the associated hype can easily overshadow fundamental flaws in governance, economic alignment, and investor protection.<sup>19</sup>
- **Investor Due Diligence:** The project underscores the imperative for investors to conduct deep, critical due diligence that penetrates surface-level narratives. It is no longer sufficient to accept labels like "governance token" at face value. A thorough analysis must include a forensic examination of the actual on-chain and off-chain economic flows, the structure of revenue-sharing agreements, and the true concentration of power and control within the project.
- **Regulatory Scrutiny:** The project's unconventional governance structure and its novel entanglement with public capital markets via the ALT5 Sigma deal are almost certain to attract significant and sustained attention from regulatory bodies like the U.S. Securities and Exchange Commission (SEC). The methods used by WLFI could become a focal point for future rulemaking concerning token classification, disclosure requirements for crypto-related public companies, and the regulation of related-party transactions.<sup>18</sup>

### 4.3 Concluding Assessment

World Liberty Financial is a project of profound dualities. On one hand, it represents a masterful execution of brand marketing and sophisticated financial engineering, successfully capturing global market attention and attracting substantial capital. Its ability to create a multi-billion-dollar valuation and integrate with public markets is a testament to its strategic ambition.

On the other hand, its core structure raises fundamental questions about transparency, fairness, and the principles of decentralization. The governance model creates a permanent schism between the token holders who vote and the insiders who profit, while the tokenomics were optimized for speculative volatility rather than long-term stability. The security incident, while proximately caused by user error, serves as a stark reminder that in a high-stakes, high-hype ecosystem, vulnerabilities are multifaceted and can cascade from the protocol layer to the end-user.

Therefore, the WLFI story is not merely an account of a token launch or a security

breach. It is a comprehensive and cautionary case study on the evolving complexities and systemic risks of the modern digital asset landscape, offering invaluable lessons for investors, developers, and regulators alike.

## 引用的著作

1. Security Breach Involving WLFI Tokens Linked to Malicious Contract ..., 访问时间为 九月 3, 2025, <https://www.binance.com/en/square/post/09-01-2025-security-breach-involving-wlfi-tokens-linked-to-malicious-contract-29106701764490>
2. wlfi Accidents West Lafayette: Web3 Security Insights - Bitget, 访问时间为 九月 3, 2025, <https://www.bitget.com/wiki/wlfi-accidents-west-lafayette>
3. Woman Identified in Jasper County Hit and Run WLFI - Bitget, 访问时间为 九月 3, 2025, <https://www.bitgetapp.com/wiki/woman-identified-in-jasper-county-hit-and-run-wlfi>
4. wlfi Body Found: What It Means in Crypto - Bitget, 访问时间为 九月 3, 2025, <https://www.bitget.com/wiki/wlfi-body-found>
5. Delegatecall Hack in Solidity - Cyfrin Code Glossary, 访问时间为 九月 3, 2025, <https://www.cyfrin.io/glossary/delegatecall-hack-solidity-code-example>
6. Not your Type! Detecting Storage Collision Vulnerabilities in Ethereum Smart Contracts - Network and Distributed System Security (NDSS) Symposium, 访问时间为 九月 3, 2025, <https://www.ndss-symposium.org/wp-content/uploads/2024-713-paper.pdf>
7. Taxonomic insights into ethereum smart contracts by linking application categories to security vulnerabilities - PubMed Central, 访问时间为 九月 3, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC11461646/>
8. A typical example of delegatecall vulnerability. - ResearchGate, 访问时间为 九月 3, 2025, [https://www.researchgate.net/figure/A-typical-example-of-delegatecall-vulnerability\\_fig5\\_367538276](https://www.researchgate.net/figure/A-typical-example-of-delegatecall-vulnerability_fig5_367538276)
9. On-Chain Analysis Explained: How to Read Blockchain Like a Pro - CCN.com, 访问时间为 九月 3, 2025, <https://www.ccn.com/education/understanding-on-chain-analysis-a-comprehensive-guide/>
10. A Complete Guide to On-Chain Analysis - Arkham Intelligence, 访问时间为 九月 3, 2025, <https://info.arkm.com/research/on-chain-analysis-guide>
11. Glassnode - On-chain market intelligence, 访问时间为 九月 3, 2025, <https://glassnode.com/>
12. Top Post-mortem Templates for Software Developers - Notion, 访问时间为 九月 3, 2025, <https://www.notion.com/templates/collections/top-post-mortem-templates-for-software-developers>
13. Incident postmortem template | Confluence - Atlassian, 访问时间为 九月 3, 2025, <https://www.atlassian.com/software/confluence/templates/incident-postmortem>

14. Incident Postmortem Templates: Improve Response Process | Atlassian, 访问时间为 九月 3, 2025,  
<https://www.atlassian.com/incident-management/postmortem/templates>
15. Trump-backed WLFI to unlock 24.6B tokens at launch - Cointelegraph, 访问时间为 九月 3, 2025,  
<https://cointelegraph.com/news/trump-backed-wlfi-unlock-27-billion-tokens-coinmarketcap>
16. Trump's World Liberty token falls in first day of trading - The Indian Express, 访问时间为 九月 3, 2025,  
<https://indianexpress.com/article/technology/tech-news-technology/trumps-world-liberty-token-falls-in-first-day-of-trading-10225565/>
17. Trump fortune balloons by billions after family firm's crypto token starts trading, 访问时间为 九月 3, 2025,  
<https://www.theguardian.com/technology/2025/sep/02/trump-world-liberty-financial-cryptocurrency>
18. Trumps' \$750 million crypto deal sparks scrutiny: Family firm sells to itself, cashes in big; why watchdogs see red flags, 访问时间为 九月 3, 2025,  
<https://timesofindia.indiatimes.com/business/international-business/donald-trumps-750-million-crypto-deal-sparks-scrutiny-family-firm-sells-to-itself-cashes-in-big-why-watchdogs-see-red-flags/articleshow/123616920.cms>
19. The Risks of the Trump-Backed WLFI Governance Token | Oxford Law Blogs, 访问时间为 九月 3, 2025,  
<https://blogs.law.ox.ac.uk/oblb/blog-post/2024/12/risks-trump-backed-wlfi-governance-token>
20. World Liberty Financial and \$WLFI Tokenomics Explained - Datawallet, 访问时间为 九月 3, 2025,  
<https://www.datawallet.com/crypto/world-liberty-financial-and-wlfi-explained>
21. WLFI Unlocks, Google's Blockchain, Dev Protections in Focus | Galaxy, 访问时间为 九月 3, 2025,  
<https://www.galaxy.com/insights/research/weekly-top-stories-8-29-25>
22. New crypto token boosts Trump family's wealth by \$5 billion - CBS News, 访问时间为 九月 3, 2025,  
<https://www.cbsnews.com/news/trump-wlfi-world-liberty-financial-crypto-wealth/>
23. Trump-Backed Crypto Token WLFI Has a Treasury Company. Here's What That Means., 访问时间为 九月 3, 2025,  
<https://www.investopedia.com/trump-backed-crypto-token-wlfi-has-a-treasury-company-here-s-what-that-means-11790255>
24. What Is Fully Diluted Valuation (FDV) In Crypto? | Tangem Blog, 访问时间为 九月 3, 2025,  
<https://tangem.com/en/blog/post/fdv-in-crypto/>
25. Fully Diluted Valuation (FDV) - Binance Academy, 访问时间为 九月 3, 2025,  
<https://academy.binance.com/en/glossary/fully-diluted-valuation-fdv>
26. Fully Diluted Value (FDV) Definition - CoinMarketCap, 访问时间为 九月 3, 2025,  
<https://coinmarketcap.com/academy/glossary/fully-diluted-value-fdv>
27. What Is Fully Diluted Valuation (FDV)? - Crypto.com, 访问时间为 九月 3, 2025,

<https://crypto.com/en/university/what-is-fully-diluted-valuation-fdv-in-the-crypto-currency-market>

28. What is FDV in Crypto? (Beginner's Guide 2025) - CoinLedger, 访问时间为 九月 3, 2025, <https://coinledger.io/learn/what-is-fdv-crypto>
29. Crypto Crashing: Altseason CANCELLED? World Liberty WLF Goes Live! - YouTube, 访问时间为 九月 3, 2025, <https://www.youtube.com/watch?v=OA5eDsYt7io>
30. Solana News: '100x Quicker' AlpenGlow Is a Go! WLF and Jupiter Lend Go Live, 访问时间为 九月 3, 2025, <https://coinmarketcap.com/academy/article/solana-news-100x-quicker-alpenglow-is-a-go-wlfi-and-jupiter-lend-go-live>
31. Trump family's cryptocurrency is now available for public buying and selling, 访问时间为 九月 3, 2025, <https://timesofindia.indiatimes.com/technology/tech-news/trump-familys-cryptocurrency-is-now-available-for-public-buying-and-selling/articleshow/123639319.cms>