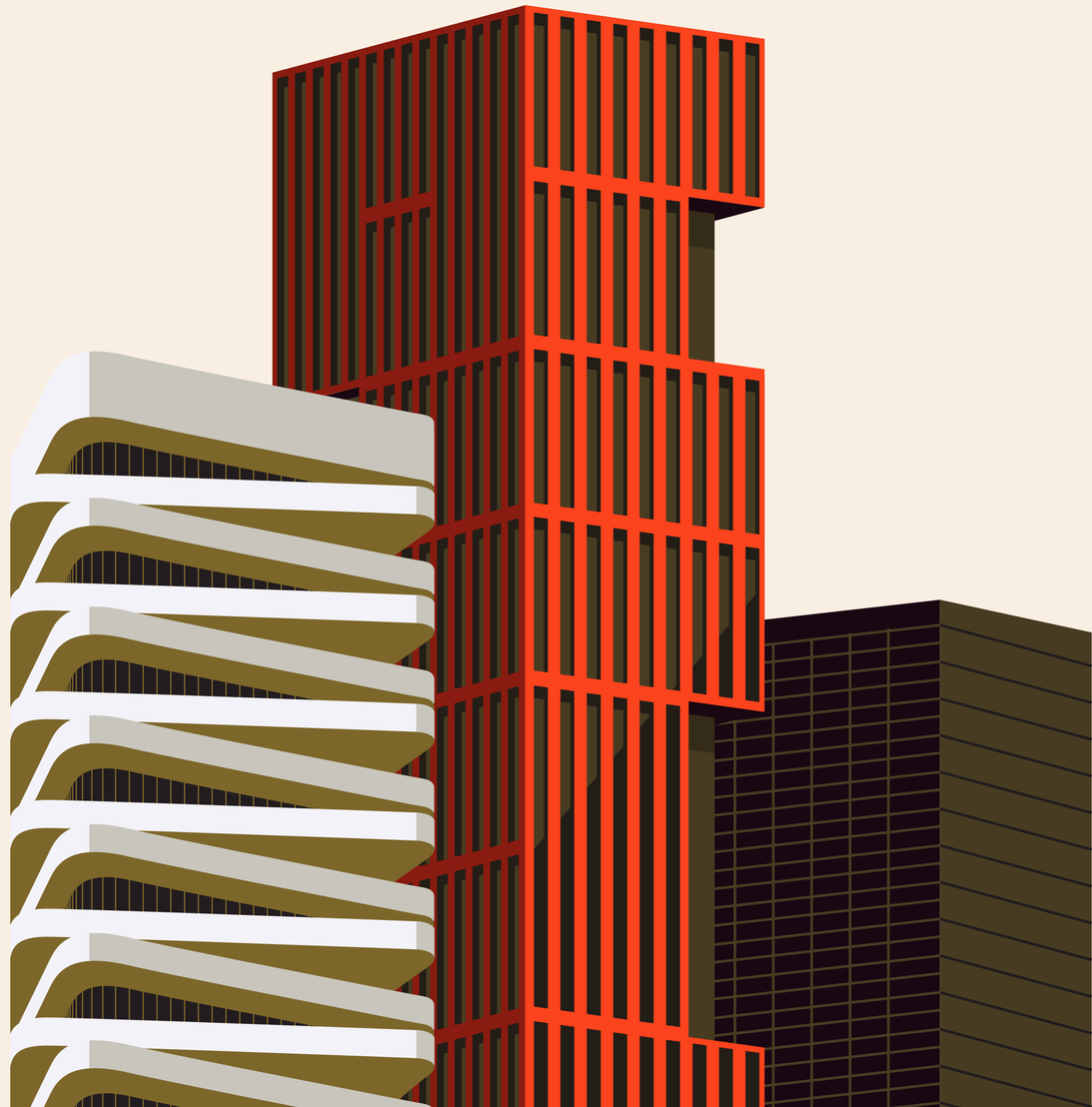
Founder Shield

De-Risking Web3

How to Mitigate Risk and Thrive in the Web3 Ecosystem



Web3 represents the next phase in the progression of the internet, moving beyond the centralized platforms of Web2 to a decentralized framework where users have true ownership and control over their data. Within this realm, Decentralized Finance (DeFi) has emerged as a notable subset, focusing on blockchain-based financial services without intermediaries.

However, our primary focus for this guide will be on the broader Web3 space, particularly blockchain companies. As this sector experiences rapid growth, understanding and mitigating associated risks is paramount.

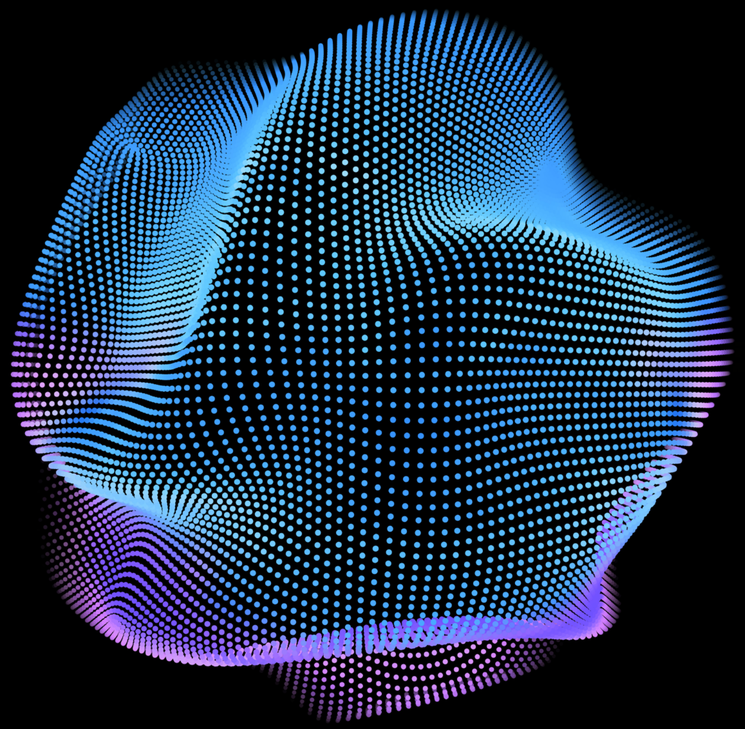
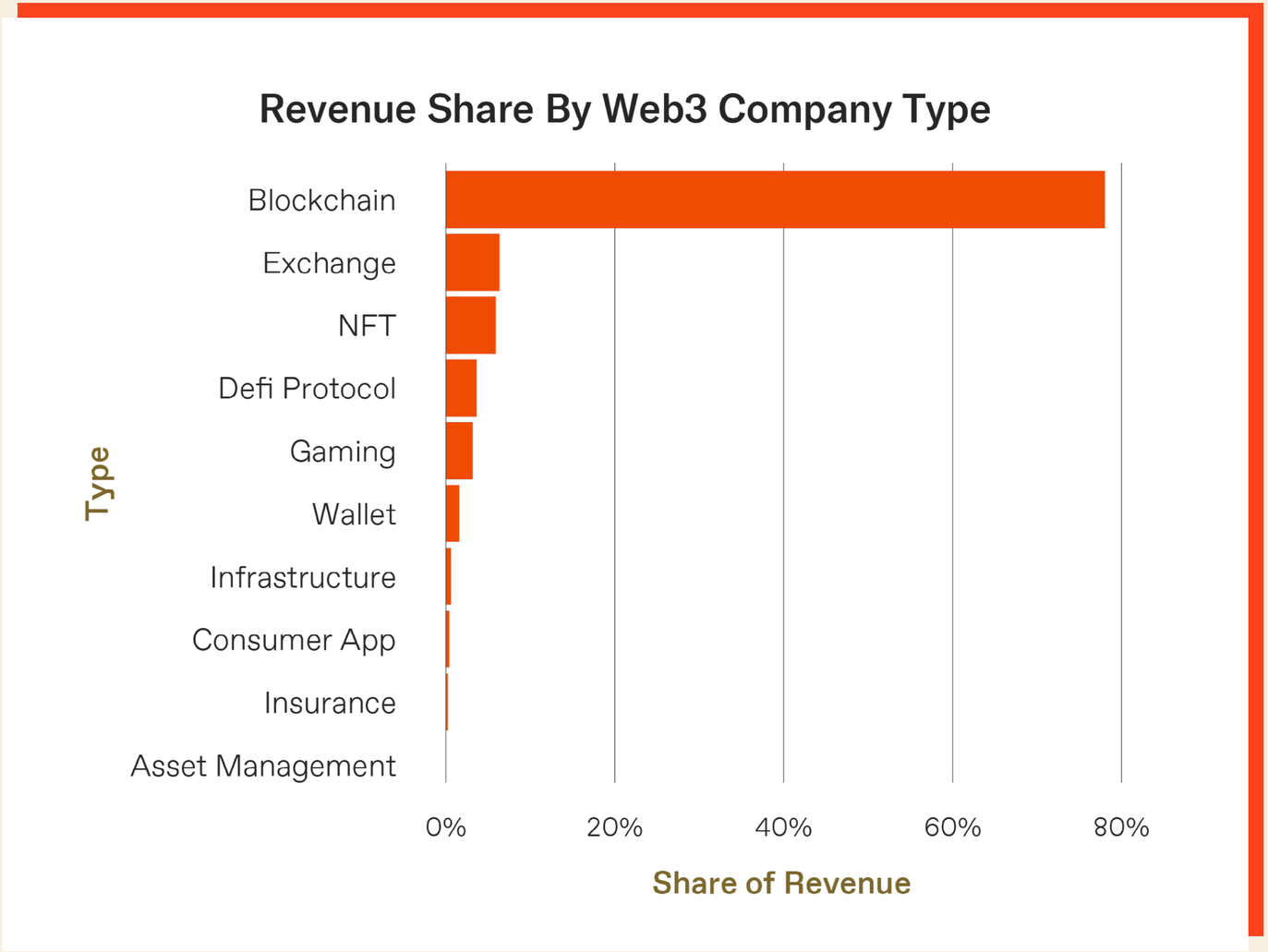


Table of Contents

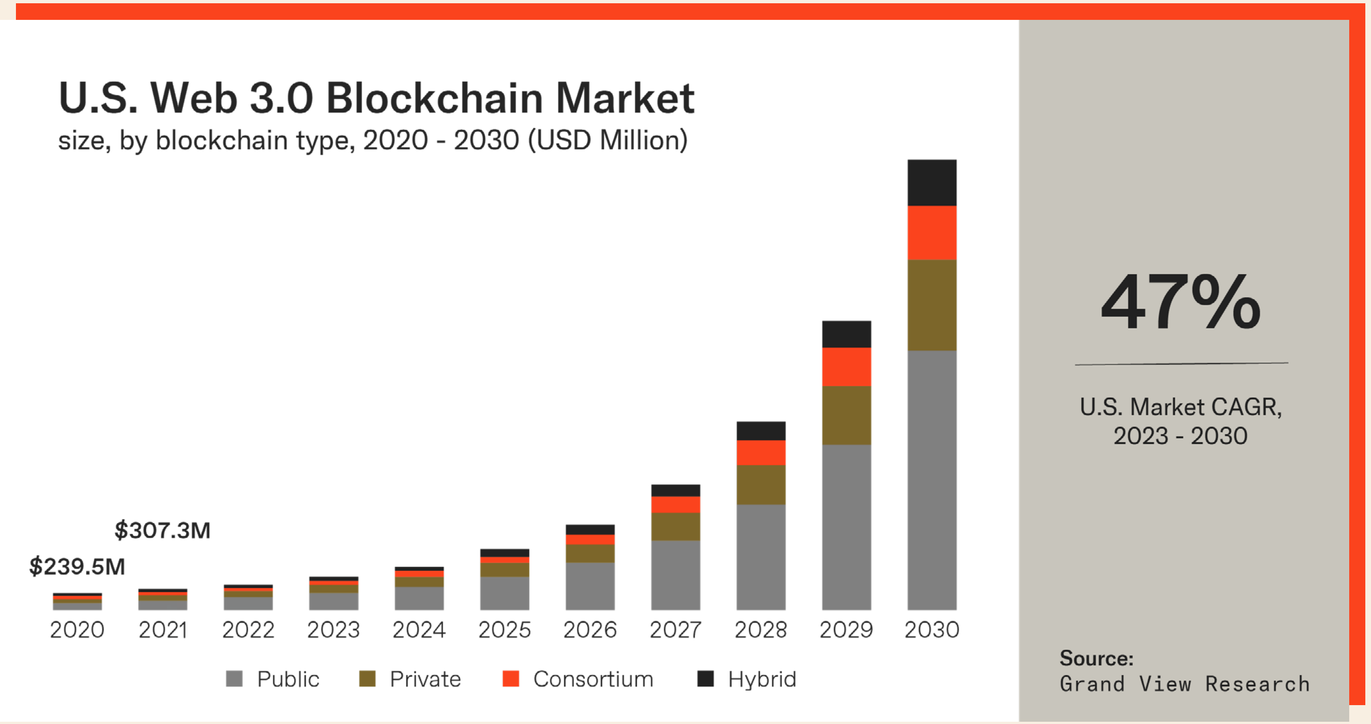
Web3 Industry Overview

Over the past few years, the landscape of internet technology has shifted with the rise of both DeFi and broader Web3 companies. Originating from the vision of a decentralized internet, Web3 aims to give individuals control over their data and interactions without the need for centralized entities. This decentralization is apparent in DeFi, which offers financial services built on blockchain without traditional intermediaries.



Source: Tom Tunguz

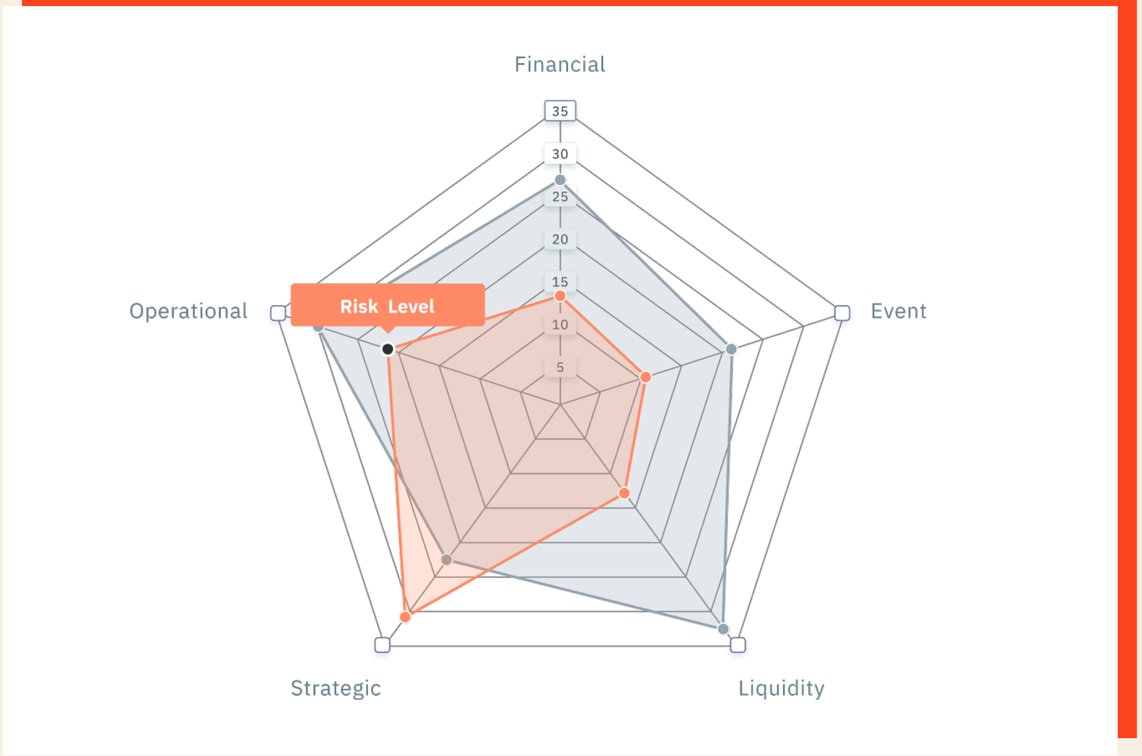
As of March 2023, according to DeFi Pulse, the total value locked in DeFi platforms has surpassed $75 billion despite the recent market downturn. Goldman Sachs reports that projections suggest that the DeFi market could reach $800 billion by 2025 and $1.5 trillion by 2030.



Major corporations and financial institutions continue to adopt DeFi platforms and services, such as PayPal, which announced in 2022 that it would allow users to buy, sell, and hold cryptocurrencies. The growth of DeFi is being driven by several factors, including the increasing popularity of cryptocurrencies, the growing demand for decentralized financial services, and the development of new DeFi applications.

The expansion and recognition of DeFi and Web3 are not just trends but indicators of a shifting paradigm in how online services are offered and consumed. For stakeholders, it's crucial to understand the landscape and prepare for its potential risks and opportunities.

Risks Web3 Companies Face



The following are some of the most common vulnerabilities Web3 companies face:

Smart Contract Failures	Vulnerabilities leading to potential losses or breaches.
Regulatory Changes	The evolving landscape of cryptocurrency regulations.
Price Volatility	The notorious volatility of digital assets and its implications.
Operational Risks	Possible disruptions in day-to-day business operations.
Fraud and Malicious Attacks	Including phishing, Sybil attacks, and other potential threats.
Custodial and Non-custodial Risks	The challenges of holding and securing digital assets.

Aside from standard exposures most Web3 companies must navigate, let's explore some of the most popular sectors within this industry and the specific risks they face.

Sector	Description	Examples	Risks
Web3 infrastructure	These companies provide the underlying infrastructure for Web3, such as blockchain platforms, cryptocurrencies, and decentralized applications (dApps).	Ethereum, Bitcoin, and Solana	The web3 infrastructure is still in its early stages of development, and there is a risk of outages and security breaches.
Decentralized finance (DeFi)	These companies are building financial applications that are based on blockchain technology. DeFi applications can be used for lending, borrowing, trading, and other financial activities.	Aave, Compound, and Uniswap	The DeFi ecosystem is still largely unregulated, and there have been cases of fraud and theft.
Non-fungible tokens (NFTs)	These companies are creating and trading NFTs, which are unique digital assets that can be used to represent anything from art to music to in-game items.	OpenSea, Rarible, and Foundation	The NFT market is volatile, and there is a risk of prices crashing. Additionally, there are concerns about the environmental impact of NFTs.
Web3 applications (gaming & social media)	These companies are developing games that are based on blockchain technology. Web3 games can provide players with more control over their in-game assets and experiences.	Axie Infinity, The Sandbox, and Decentraland (Gaming). Steemit, Minds, and Mastodon (Social media)	There is a risk that blockchain-based games will not be as popular as traditional games. The current web3 infrastructure is not yet scalable enough to support large-scale social media platforms. The decentralized nature of web3 makes it more difficult to secure data and prevent attacks.
Metaverse	Companies that develop and operate virtual worlds that are powered by blockchain technology. The metaverse is seen as the next generation of the internet, and it has the potential to revolutionize the way we interact with the digital world.	AltspaceVR (Microsoft), Horizon Worlds (Meta), Nvidia	The metaverse is still in its early stages of development, and it is unclear how it will be regulated. Additionally, there are concerns about the privacy and security risks of the metaverse.

How to Manage Risks in the Web3 Industry

The Web3 industry, while offering transformative solutions, has its vulnerabilities. Managing risks in this dynamic domain necessitates combining tech-savviness and proactive planning.

> In the rapidly evolving realm of Web3, effective risk management isn't just about securing assets—it's about anticipating the unpredictable, understanding the intricate web of regulations, and safeguarding the trust of every stakeholder involved.

Justin Kozak
EVP - Founder Shield

Regular Audits

One of the foundational pillars of risk management in Web3 is the regular audit of smart contracts and protocols. By ensuring these are thoroughly vetted, companies can preemptively identify and rectify potential security gaps. Such audits should be conducted by experts familiar with blockchain technology and its unique challenges.

Educating Users

User errors or misunderstandings can often lead to significant issues in Web3 platforms. Therefore, companies must emphasize safe practices, ensuring users are well-informed about how to use platforms securely. This approach involves transparently communicating potential risks and providing guidance on avoiding common pitfalls.

Layered Security Protocols

In the realm of Web3, relying on a single line of defense is insufficient. Multi-factor authentication ensures that only authorized users gain access. Additionally, cold storage—where assets are stored offline—protects against online hacking attempts. Companies must build multiple layers of security protocols to fortify their systems.

Regular Updates

The digital landscape is perpetually evolving, with new vulnerabilities surfacing regularly. By keeping systems and smart contracts updated, Web3 platforms can safeguard against known vulnerabilities, ensuring they're not using outdated technology that's easily exploitable.

Established Exit Strategies

While proactive measures are essential, it's equally important for companies to prepare for worst-case scenarios. A clearly outlined exit strategy guides how to act if, for instance, a critical vulnerability is exploited or a significant asset is compromised. This approach minimizes potential damages and instills confidence in stakeholders, knowing that the platform is prepared for all eventualities.

By integrating these strategies, Web3 platforms can effectively navigate the dynamic and often treacherous digital waters, ensuring their and their users' assets remain secure.

Why Web3 Insurance is No Longer “Optional”

The rapid ascent of Web3 technologies, particularly in the DeFi domain, is remarkable. Billions of dollars are now locked in various DeFi platforms, representing substantial assets and signaling a shift in the financial paradigm. Such exponential growth isn’t merely a testament to the allure of decentralized systems but also emphasizes the enormous responsibility these platforms bear.

> “Within emerging industries, a well-structured insurance program allows for several advantages. As a standard requirement amongst stakeholders, insurance acts as a bridge toward public adoption. In the case of Web3, it takes a step further, supporting leadership teams at the helm faced with navigating regulatory environments that are not yet clearly defined. This approach helps clear the path, removing the fog through the added benefits of calculated risk and a defined downside.”

Will Hamony
EVP of Sales - Founder Shield

However, this explosion of assets and trust has painted a bright target on the DeFi sector. Rising hacks, data breaches, and malicious activities in the crypto realm have become alarmingly common. These disruptions result in significant financial losses and erode the trust that users and stakeholders place in these platforms. Ensuring the security of assets and maintaining a solid reputation is pivotal to attracting and retaining users in this competitive landscape.

In this context, Web3 insurance emerges as a non-negotiable safeguard. Beyond mere protection of assets, it plays a pivotal role in instilling confidence and establishing user credibility. As more people venture into the decentralized world, they seek assurances that their investments and data are secure. Insurance provides that layer of trust and resilience against unforeseen adversities.

Furthermore, given the rapid maturation of the sector, it’s only a matter of time before regulatory bodies step in, potentially making insurance mandates a staple requirement for DeFi platforms. Proactively securing Web3 insurance positions platforms for present challenges and impending regulatory demands, ensuring they remain compliant, trustworthy, and resilient in a dynamic digital era.

Foundational Policies Web3 Companies Should Consider

> Recent tales of misplaced passwords have thrust the debate between hot and cold storage into public consciousness. At its core, it's about trusting those who safeguard digital assets. In unforeseen circumstances, a digital asset insurance can offer monetary support and peace of mind.

Will Hamony
EVP of Sales - Founder Shield

Digital Asset Insurance

This policy safeguards Web3 companies against potential losses stemming from the theft or loss of cryptocurrencies, a crucial asset in their operations.

Smart Contract Liability Coverage

As smart contracts form the backbone of many Web3 platforms, this coverage ensures that any vulnerabilities or faults within these contracts do not lead to significant financial setbacks.

Crime Insurance

Given the digital nature of Web3 companies, they are susceptible to criminal acts such as theft, fraud, and forgery; this insurance offers a protective net against such incidents.

Errors & Omissions Insurance

Even the most meticulous companies can make mistakes. This policy covers Web3 businesses against losses from any unintentional errors, omissions, or breaches by the company or its personnel.

Operational Disruption Insurance

Downtime can severely affect a Web3 company's operations and reputation. Partnering with firms like Parametrix, this insurance offers a safety net against losses from system failures or prolonged downtimes.

Cybersecurity Insurance

As cyber threats become increasingly sophisticated, this insurance becomes vital for Web3 companies, covering losses from digital fraud and theft.

Directors and Officers Insurance

Leadership decisions shape a company's trajectory. This policy ensures that company leaders are shielded from personal liabilities arising from their roles.

Specie insurance

Traditionally covers physical assets like precious metals or cash in transit, but in the Web3 context, it could be tailored to suit specific tangible assets crucial to a company's operations.

Web3 Insurance Costs

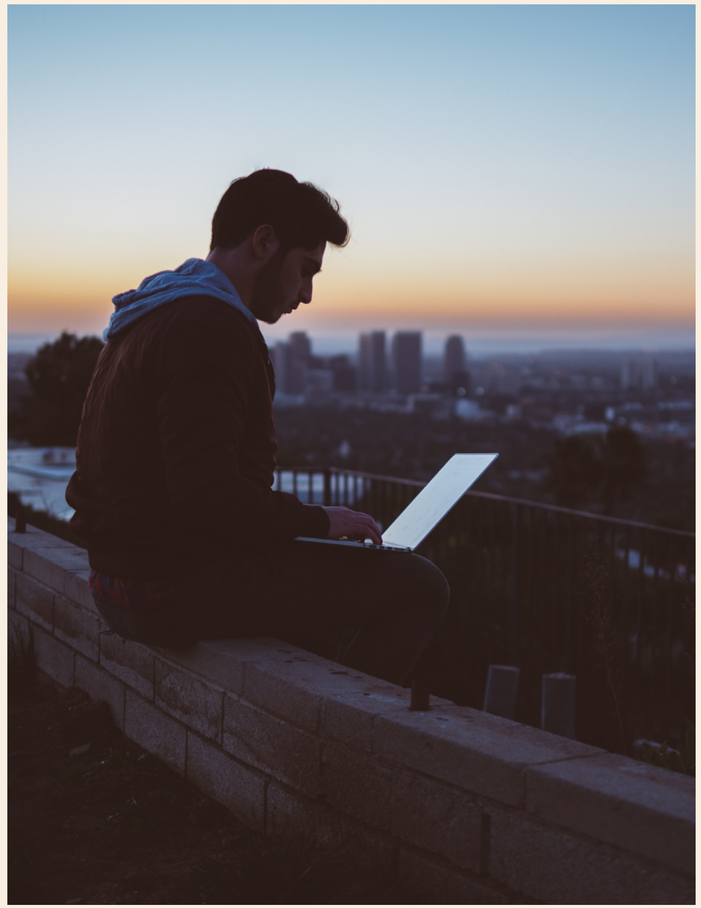
The baseline costs for digital asset insurance are typically higher than traditional insurance markets due to the inherent risks associated with digital assets, such as the volatility of the market, the lack of regulation, and the risk of hacks and theft.

The cost of digital asset insurance can vary depending on a number of factors, such as the type of asset being insured, the amount of coverage being sought, and the risk profile of the insured entity. However, in general, digital asset insurance is more expensive than traditional insurance markets.

Some of the factors that can affect the pricing of digital asset insurance include:

- The value and volume of assets under management.
- The track record of the company (history of breaches, claims).
- The complexity of the smart contracts in use.
- The risk profile of the insured entity.
- The underlying protocols and their security measures.
- The presence of third-party custodial solutions.
- The type of coverage being sought.
- The geographical location of the insured entity.
- The deductible.
- Discounts and incentives.

It is important to note that these are just some of the factors that can affect the pricing of digital asset insurance. The actual cost of insurance will vary depending on the specific circumstances of the insured entity.



How to Get Web3 Insurance

When diving into the crypto world, it's crucial to align with specialized insurance providers that grasp the intricacies of this space and offer policies tailored to its unique challenges. A seasoned broker, well-versed in cryptocurrency, can be an invaluable ally in navigating this intricate landscape. They bring knowledge of the field and insights into the nuances of different providers, making the path smoother for businesses.

Risk assessment stands as a foundational pillar in securing appropriate insurance. A company must understand its vulnerabilities thoroughly, considering every nook and cranny. Enlisting third-party audits, particularly for smart contracts, strengthens the security framework and provides a more robust footing during the insurance application process.

Establishing the company's insurance needs entails a meticulous evaluation of the types of coverage that align with its operations. The application process is more than a mere formality; it demands a comprehensive documentation phase where companies delve deep into their operations, security protocols, and past incidents. Furthermore, negotiation is vital. Engaging in active discussions with providers can yield better terms and pricing, ensuring that the insurance acquired provides optimum protection.

Maintaining insurance relevance requires a vigilant eye. As a company evolves and the risk environment transforms, regular reviews and updates to the coverage become imperative. Additionally, ensuring that the insurance aligns with regulatory mandates specific to operational areas is vital. But beyond the policies, companies must instill best practices among their team members through continuous training, minimizing risk at its source. Should an unfortunate event occur that necessitates a claim, understanding the claim process intricacies becomes indispensable, ensuring swift processing and reimbursement.

Real-life Examples of Crypto Claims

Three real world examples of insurance claims involving Web3 companies:

BINANCE	In 2021, the cryptocurrency exchange Binance filed a $200 million insurance claim after it was hacked and $40 million worth of cryptocurrency was stolen. The hack was one of the largest in the history of cryptocurrency, and it highlighted the risks that Web3 companies face from cyberattacks. Binance's insurance claim was eventually approved, and the company was able to recover some of the stolen cryptocurrency.
Badger	In 2022, the decentralized finance (DeFi) protocol BadgerDAO was hacked and $120 million worth of cryptocurrency was stolen. The hack was caused by a vulnerability in BadgerDAO's smart contract. BadgerDAO's insurance provider, Nexus Mutual, paid out $100 million to cover the losses from the hack.
OpenSea	In 2023, the NFT marketplace OpenSea was hacked and $30 million worth of NFTs were stolen. The hack was caused by a phishing attack that tricked OpenSea users into giving up their login credentials. OpenSea's insurance provider, Arbol, is still investigating the hack, and it is not yet clear if the insurance claim will be approved.

Next Steps

For Web3 companies, proactive risk management isn't merely beneficial—it's indispensable. Given the unique and often unpredictable challenges of the crypto realm, insurance emerges as an essential tool to safeguard interests and assets. To navigate this intricate landscape, Web3 companies are strongly encouraged to collaborate with insurance professionals who deeply understand the crypto industry. Furthermore, relying on trusted insurance providers specializing in crypto can significantly bolster a company's defense against potential threats.

About Founder Shield

Founder Shield is a data-driven insurance brokerage serving high-growth, innovative industries. We have a passion for creating and developing innovative risk management products across emerging industries and work hand-in-hand with clients and underwriters to ensure transparency, efficiency, and reliability.

Bespoke Insurance Solutions

Founder Shield understands the unique risks faced by Web3 companies and can often design insurance policies that specifically address those risks. This is in contrast to traditional insurance companies, which often offer one-size-fits-all policies that may not be tailored to the specific needs of Web3 companies.

Top Carrier Access

Founder Shield has access to top insurance carriers, which gives us the ability to negotiate the best possible rates for their clients. This is in contrast to traditional insurance companies, which may only have access to a limited number of carriers.

Niche Expertise

Founder Shield has a team of experts who are knowledgeable about the Web3 industry and the risks that Web3 companies face. This expertise allows them to provide their clients with the best possible advice and support.

ADDITIONAL RESOURCES

Cryptocurrency Risk Management Guide →

Insurance for Blockchain Companies →

Insurance for Cryptocurrency Companies →

(646) 854-1058
INFO@FOUNDERSHIELD.COM
114 E 25TH ST, NEW YORK, NY