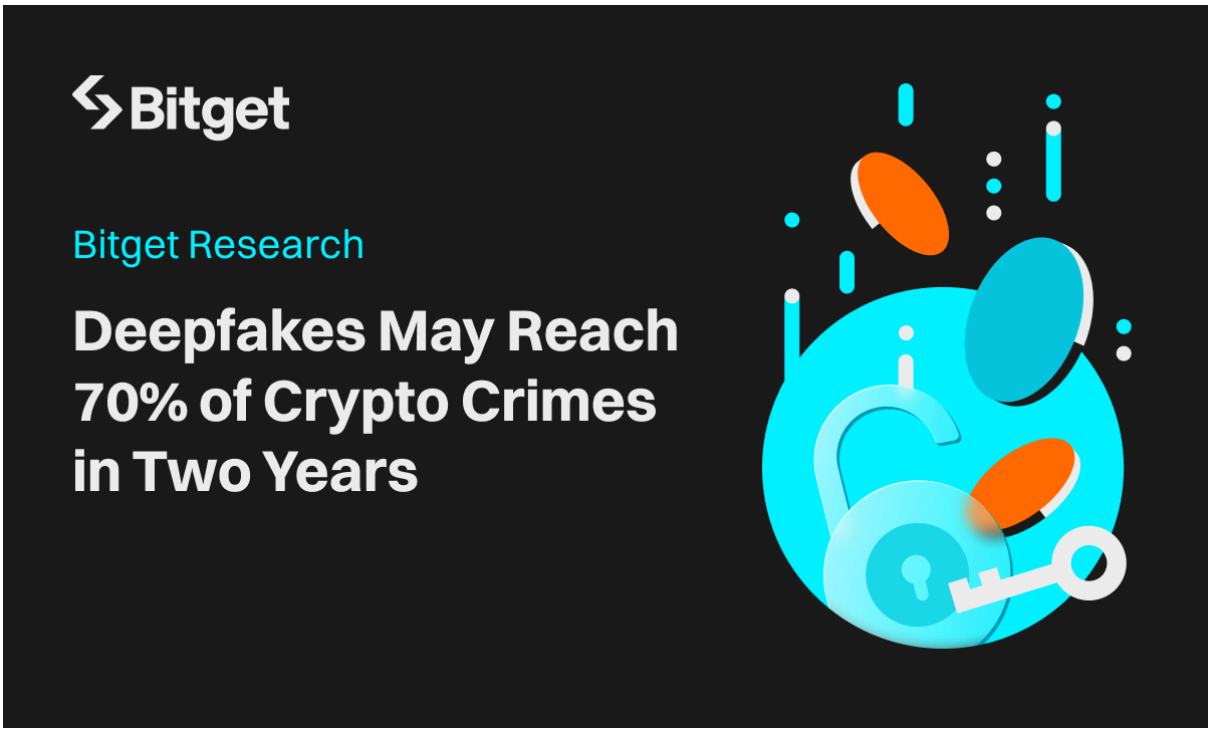
Publishing time: 10 AM UTC, 27th June 2024

REPORT

Bitget Research: Deepfakes May Reach 70% of Crypto Crimes in Two Years



Deepfakes, generated by artificial intelligence (AI), have legitimate applications in scientific research and entertainment. However, this technology is increasingly being weaponized by criminals. The growing spread of highly realistic fabricated content can influence the financial decisions of ordinary people, increasing the risk of fraud globally.

The threat extends beyond imitations of influencers' speeches. Deepfake attacks can be tailored to target specific individuals, aligning with their values, interests, and psychological profiles. Today, the market lacks adequate measures to prevent and address these modern threats and counteract the severe impact of social engineering techniques that leverage the latest technological advancements. These advancements include deep learning, face alignment and landmark detection, generative adversarial networks (GANs), autoencoders, recurrent neural networks (RNNs), facial recognition and feature extraction, and sophisticated image and video processing techniques.

Data sources and methodology

Quantitative indicators of fraud involving deepfakes are inadequate for fully capturing the technological impact on the economic landscape. Consequently, this study examines the issue through absolute figures representing the losses suffered by victims. The cryptocurrency sector has historically underestimated the risks posed by deepfakes, resulting in incomplete data from 2017 to 2021. To provide a comprehensive analysis, this study includes data from 2022 and forecasts trends for 24 months, from Q1 2022 to Q1 2024.

The research integrates data from publicly accessible sources and the findings of Bitget's investigations under the broader Anti-scam Month campaign launched by Bitget in June 2024. The platform employed a comprehensive, multi-source approach to detect and analyze deepfake-related activities. This approach was rooted in user reports and suspicions of illicit transactions involving deepfakes. Information was collected from partners and specialists in fake detection, and experiences were shared with other cryptocurrency companies. Special emphasis was placed on identifying fraudulent activities that exploited marketing content, atypical influencer speeches, and pseudo-educational videos.

The platform also monitored social media mentions using specific hashtags and keywords to build a more comprehensive picture of the situation. Requests were made to law enforcement agencies, and publicly available data on deepfake-related frauds were collected. Collaboration with fact-checking services further ensured the accuracy of the information.

The gathered reports were systematically compiled into a standardized template, categorizing data by content type, platform, reporting time, and crime detection period. Efforts were made to check for data duplication during the database population and upon completion, to avoid the multiple counting of identical cases. Bitget remained committed to maintaining user privacy and adhering to the principle of least privilege. Anonymized information was used to analyze trends and identify patterns.

Analysis

The impact of deepfakes on the crypto space

Since the beginning of 2022, losses from fraudulent operations involving cryptocurrencies have reached $79.1 billion. Analyzing the yearly dynamics from 2022 to 2023 reveals a general downward trend in these losses (see Fig. 1). These data are consistent with the study of total cryptocurrency value received by illicit addresses for 2018-2023 conducted earlier [1]. The preliminary conclusion about the decline in 2022-2023 comes from a small number of periods when considered by year. If we look at the quarterly cut (Fig. 2), the average losses for the period do not tend to be zero.

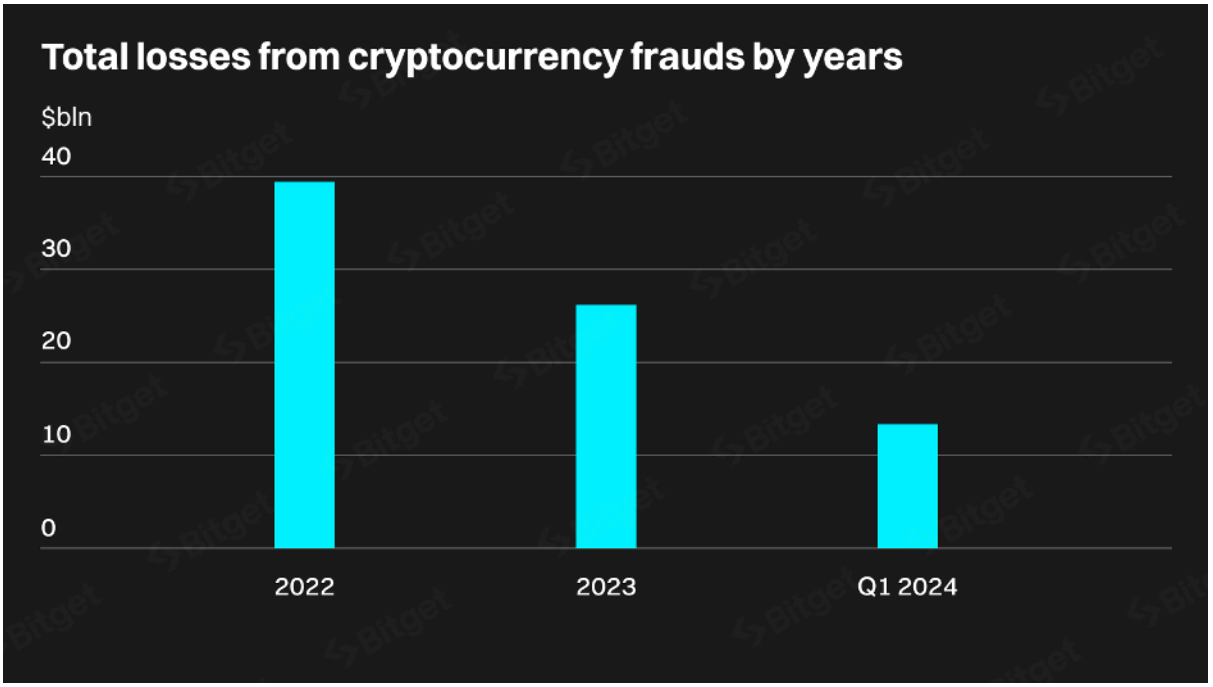


Fig. 1: Total losses from cryptocurrency frauds by years ($ billion)

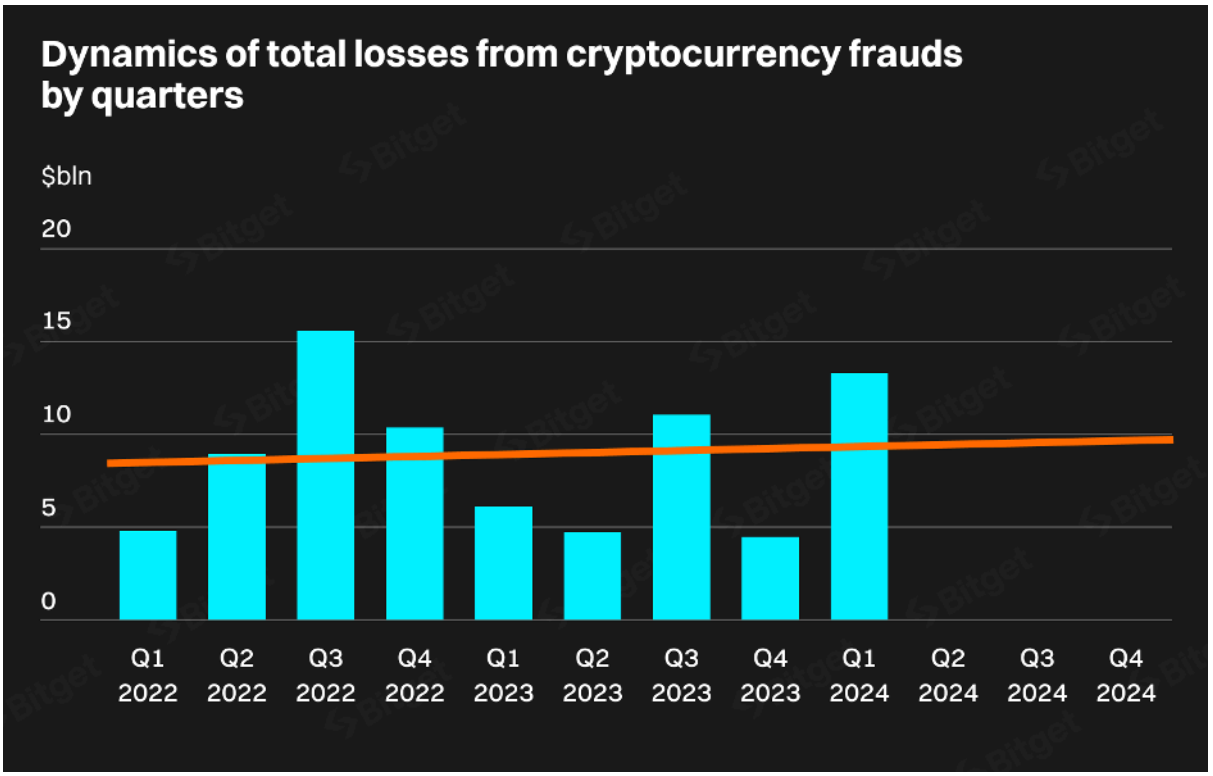


Fig. 2: Total losses from cryptocurrency frauds by quarters ($ billion)

A closer look at the data reveals a volatile trend with significant peaks in Q3 2022, Q3 2023, and Q1 2024. Several factors contribute to this volatility:

- inconsistency among fraud groups;
- coincidence of several major attacks;
- volatility of the crypto market;
- technological breakthroughs that create new tools for fraudsters;
- changes in public attitudes;
- emergence of new protective measures;
- changes in public awareness;
- legislative changes aimed at protecting cryptocurrency users.

Despite the efforts of government agencies and blockchain platforms, there has been a rise in monetary losses attributed to crypto fraudsters (Fig. 3).

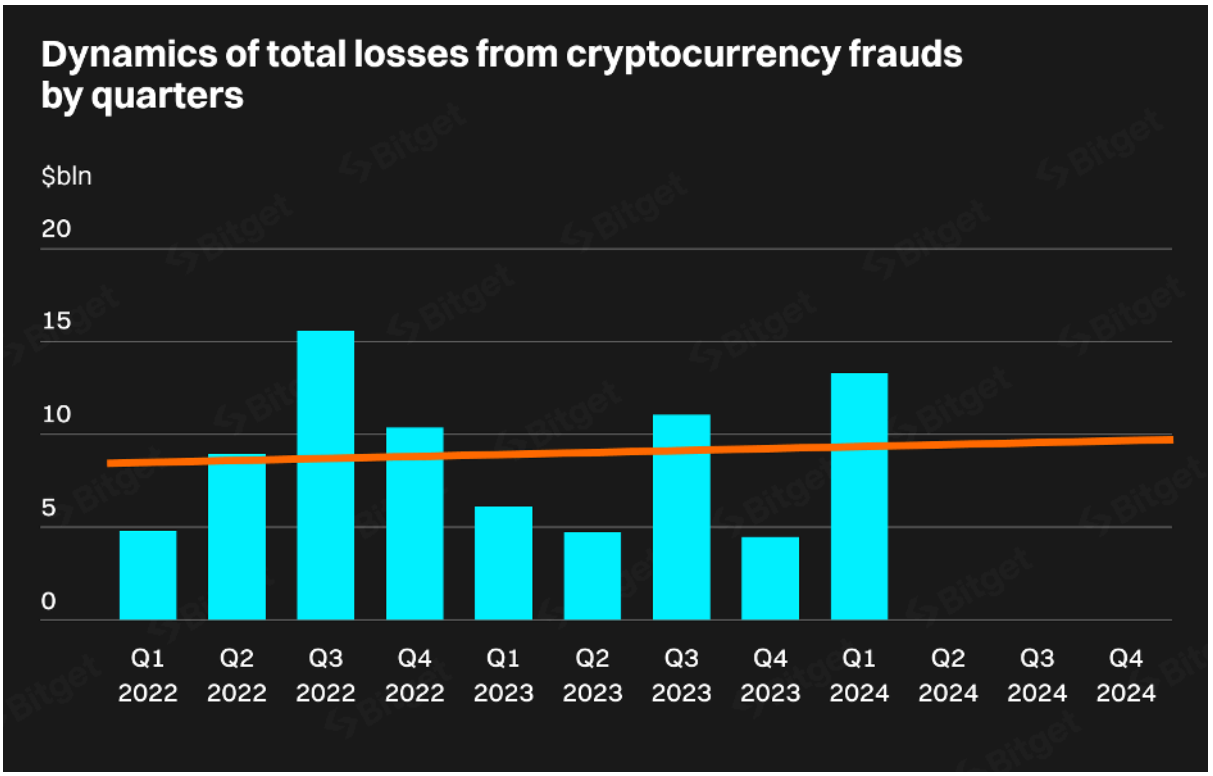


Fig. 3: Dynamics of total losses from cryptocurrency frauds by quarters ($ billion)

The global trend of a 245% increase in the number of deepfakes compared to 2023 has also significantly impacted the cryptocurrency sector, affecting the security of victims' accounts [2].

The surge in fraudulent transactions and financial losses suggests that quarterly losses could increase to an average of $10 billion by early 2025. A similar pattern emerges in losses attributed to deepfake-related illegal transactions: following a decline in 2023, Q1 2024 signals a potential resurgence in fraudulent activity (Fig. 4). Assuming this trend persists over the next three quarters, it could lead to an annual total of $25.13 billion in 2024 (Fig. 5).

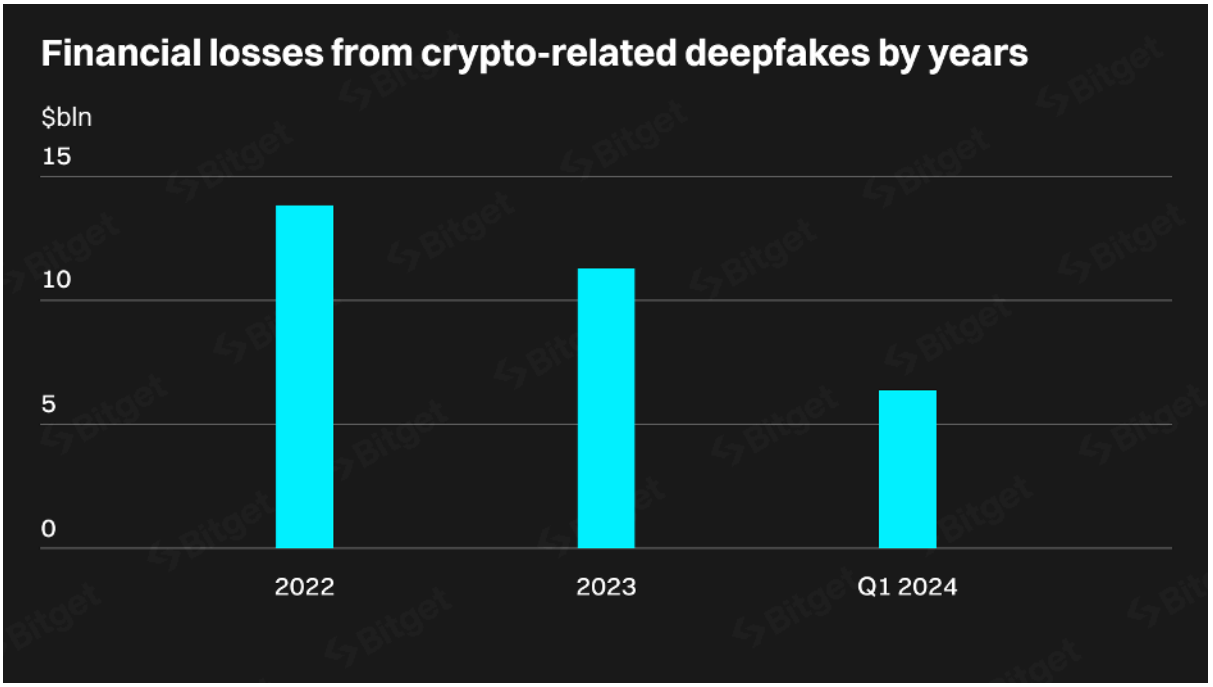


Fig. 4: Financial losses from crypto-related deepfakes by years ($ billion)

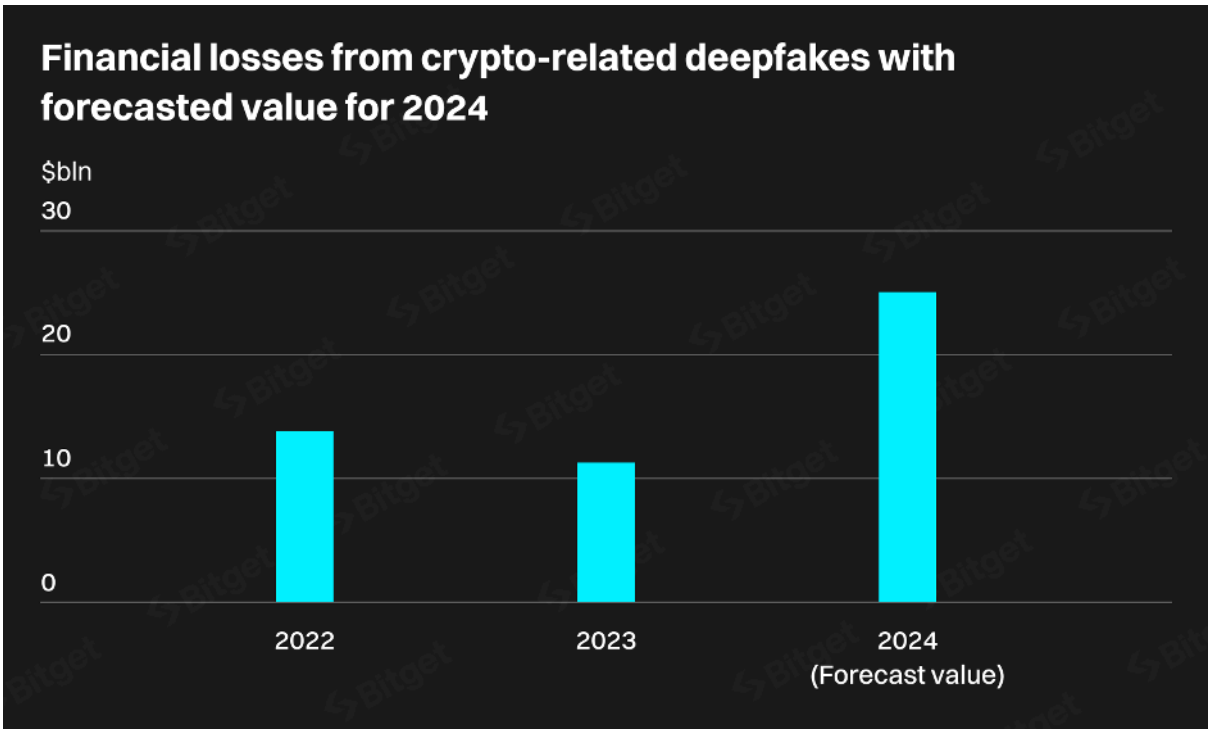


Fig. 5: Financial losses from crypto-related deepfakes with forecasted value for 2024 ($ billion)

Without regulatory intervention, losses from this type of fraud are likely to continue increasing (see Fig. 6 and Fig. 7). In such circumstances, both the cryptocurrency sector and the broader financial industry could face user distrust and financial losses.

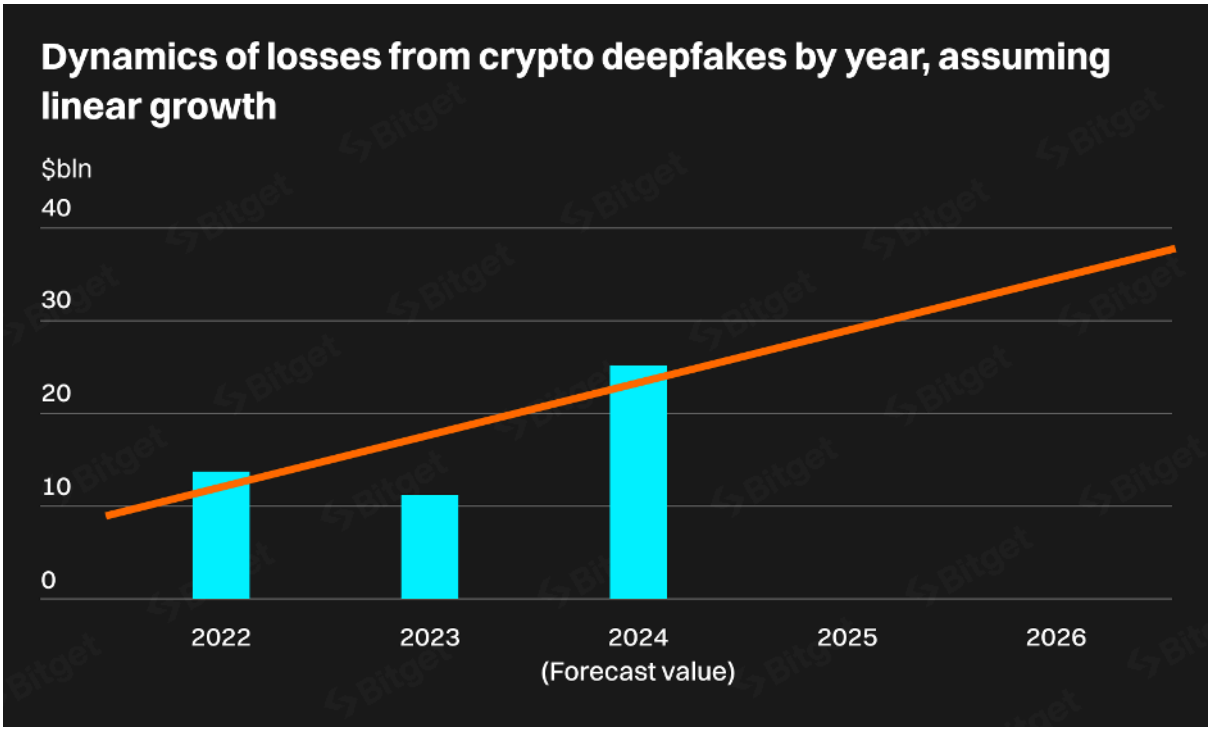


Fig. 6: Dynamics of losses from crypto deepfakes by year, assuming linear growth ($ billion)

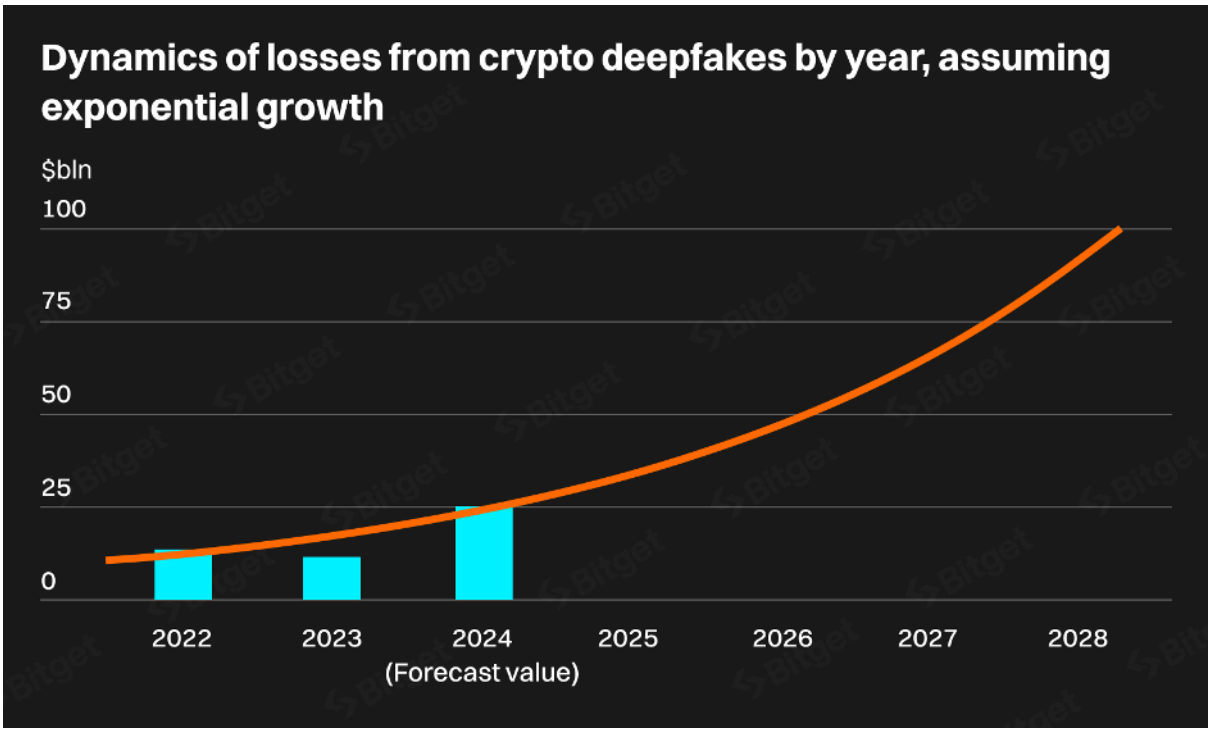


Fig. 7: Dynamics of losses from crypto deepfakes by year, assuming exponential growth ($ billion)

The proportion of crimes involving digital fakes does not exhibit significant quarter-to-quarter variation (Fig. 8) compared to the dynamics of financial losses from these crimes (Fig. 10). While the proportion of such crimes is less volatile, it continues to show a steady growth trend. The moving average line indicates a notable increase in illegal transaction activity in mid-2023 (Fig. 9), which was followed by a brief decline before the proportion of cases resumed its upward trajectory. The apparent link to market sentiment suggests a potential correlation between the use of deepfakes for illicit activities and fluctuations in the Fear and Greed Index [4].

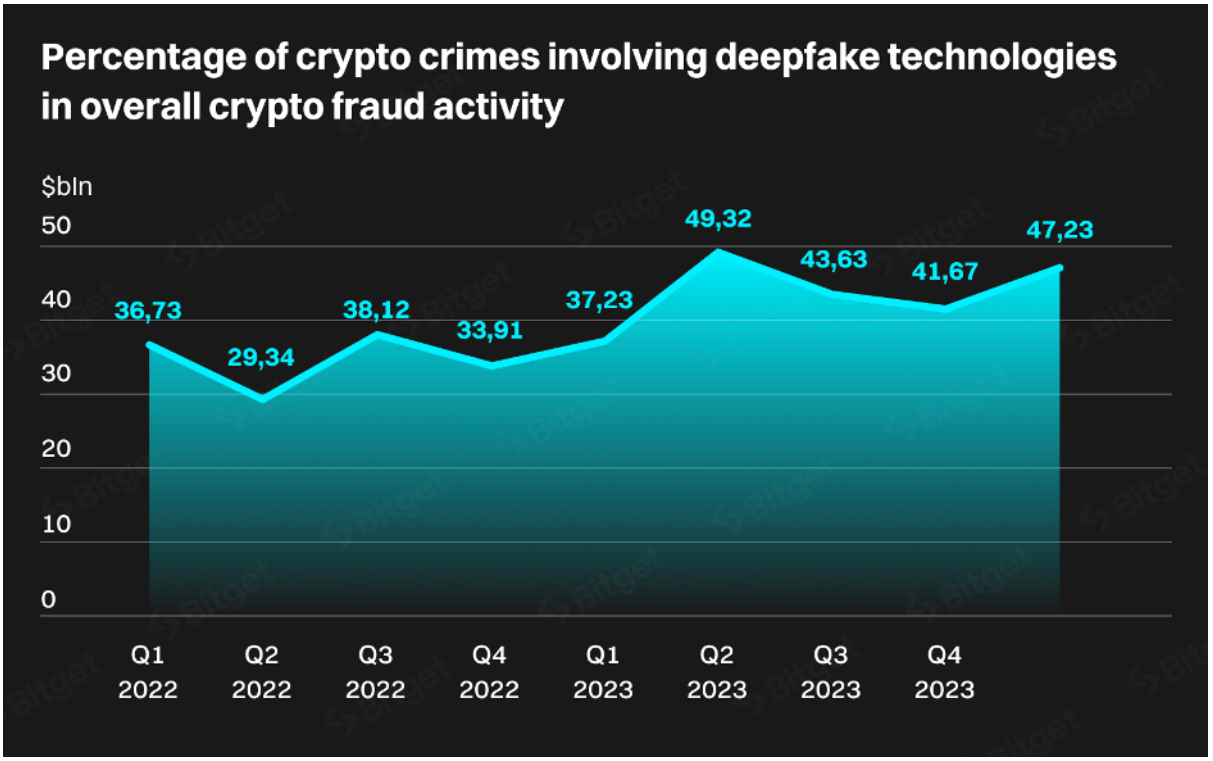


Fig. 8: Percentage of crypto crimes involving deepfake technologies in overall crypto fraud activity

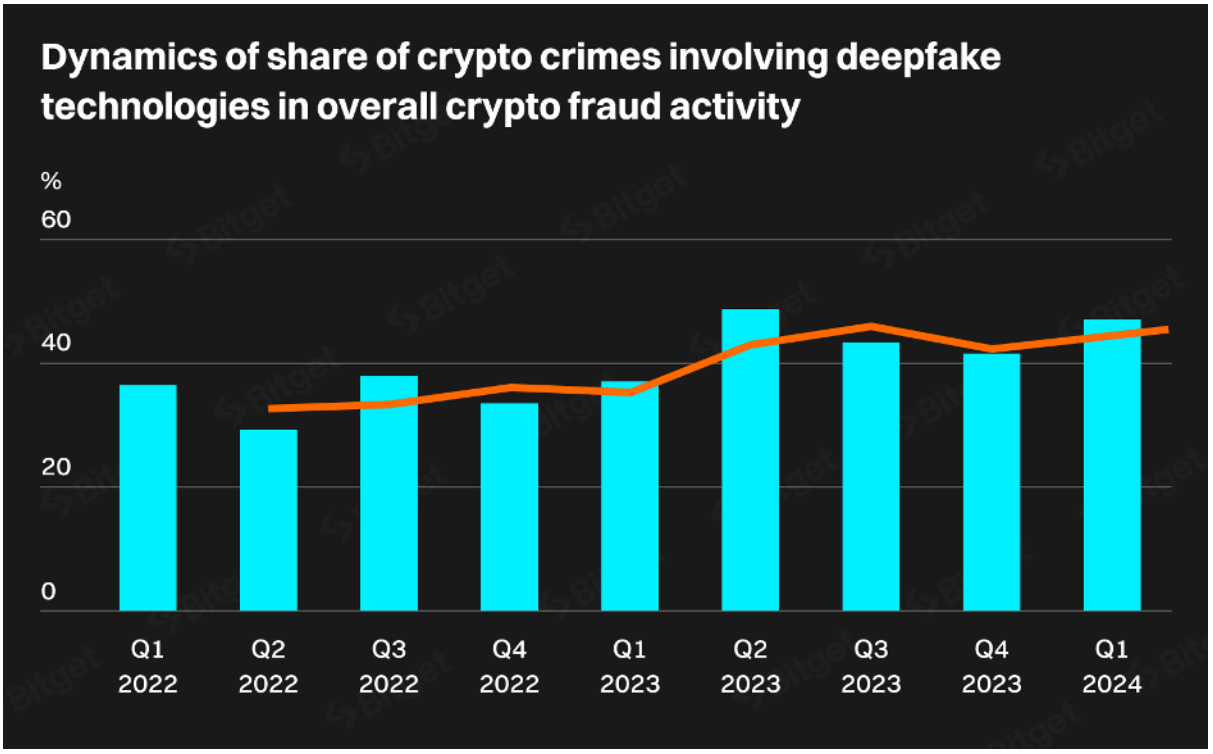


Fig. 9: Dynamics of share of crypto crimes involving deepfake technologies in overall crypto fraud activity

Correlation with the Fear and Greed Index

The surge in losses observed during the bullish market periods in Q3 2023 and Q1 2024 (Fig. 10) underscores a direct correlation with market sentiment during its growth and the hype surrounding related developments. During times of increased profitability, cryptocurrency users tend to take risks to leverage the prevailing market conditions. A study by the National Bureau of Economic Research (NBER) confirmed this view and showed that overconfident investors are more likely to trade and own riskier assets, potentially making them more vulnerable to fraud during periods of greed [3].

Following the crypto winter period, 2023 witnessed growth across most crypto assets. To contextualize this phenomenon, the study compares it with Bitcoin's Fear and Greed Index (Fig. 11), given the dominant influence of this coin [4][5].

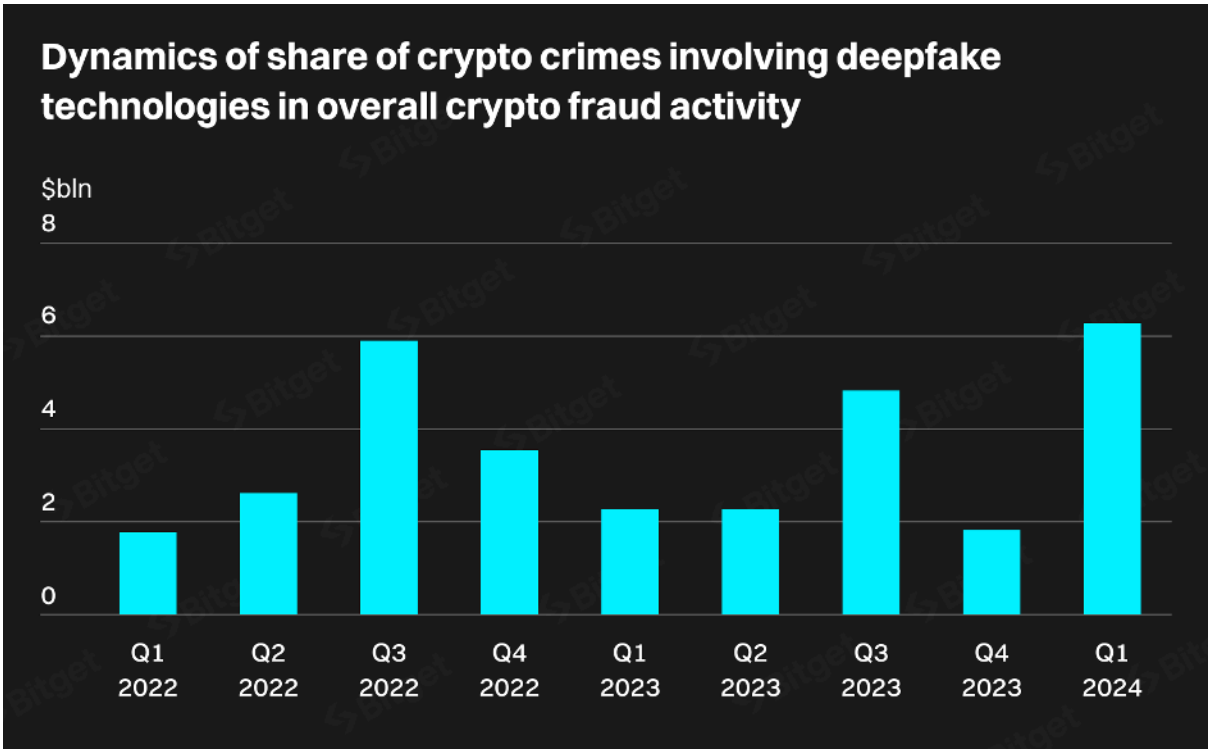


Fig. 10: Amount of losses from cryptocurrency frauds involving deepfakes ($ billion)

Fig. 11: Historical Movement of the Crypto Fear and Greed Index against BTC

Overlaying the graphs from Figure 10 and Figure 11 reveals a subtle correlation in the past six months. Following the surge in interest in Bitcoin in Q3 2023, there was a notable uptick in the losses incurred by fraud victims. A similar pattern emerged after the downturn in early 2024, indicating a strong correlation. However, the asynchronous behavior in 2022 and early 2023 does not allow to confirm that these indicators are fully connected. This discrepancy

can be attributed to the indirect relationship and the multifaceted nature of the drivers of technology-related crimes. The frequency of losses resulting from criminal operations involving digital fakes constitutes a segment of the overall losses from crypto fraud, which tend to escalate during periods of recklessness among cryptocurrency holders.

Connection with the technology development

Deepfake technologies continue to advance, leveraging scientific breakthroughs from the past decade. The groundwork laid by research on deep learning-based face recognition systems in 2014 sparked a technological revolution [6]. Face2Face (face and voice replacement technology) gave rise to the first fake video that became widespread, which created a public outcry and drew the attention of regulators to the danger of deep fakes [7]. Since then, deepfakes have found widespread application in various spheres, including politics, marketing, and entertainment.

The emergence of DeepFaceLab further deepened people's understanding of algorithms and popularized automatic face replacement techniques [8]. By 2018, efforts were underway to find and introduce methods for verifying video authenticity, prompting media entities to combat the dissemination of fake content. While corporate solutions for deepfake detection became available in 2022, average users lacking the necessary knowledge and skills remained vulnerable [9]. The ongoing competition in sophistication between fraudsters and security solution providers persists to this day.

As attackers exploit vulnerabilities in detection software, a cat-and-mouse game ensues, with fraudsters capitalizing on loopholes to reap rewards before the next update. This dynamic explains the irregular pattern of losses observed quarterly (Fig. 10).

Structure of crimes involving deepfakes

When analyzing crypto crimes in the context of the use of deepfakes, we can identify the following types:

- Identity theft and impersonation;
- Deepfake-generated fake IDs for bot networks;
- Scams and fraudulent schemes;
- Market manipulation;
- Investment fraud;
- Ransom and extortion;
- Regulatory evasion and compliance violations;
- Social engineering attacks;
- Technology exploitation;
- Public deception and misinformation;

- Automated trading manipulation;
- Credential stuffing and account takeover;
- Cryptojacking;
- Fake legal or regulatory announcements;
- Crowdsourced attacks;
- Illicit fundraising;
- Impersonation in virtual reality and metaverse;
- Fake arbitration;
- Black market transactions.

A more generalized structure with consolidation of parts includes:

- Identity and impersonation fraud;
- Scams, fraud, and deception;
- Market manipulation and exploitation;
- Cyber extortion and regulatory violations.

The share of each category fluctuated during the study period (Fig. 12), but some dominant trends are evident. Similar to 2022, losses from scams, fraud, and deception continue to dominate, although their share has decreased from 57.91% to 53.32% by Q1 2024. These illicit activities encompass the creation of fake projects, phishing attacks, and Ponzi schemes. The prominence of this category is not due to the sheer number of schemes but rather their global reach and their capacity to target thousands of victims simultaneously. In such schemes, deepfake technologies are employed to gain the trust of cryptocurrency investors. By impersonating influential figures, these schemes create the illusion of credibility and substantial project capitalization, thereby receiving large investments from victims without thorough due diligence.

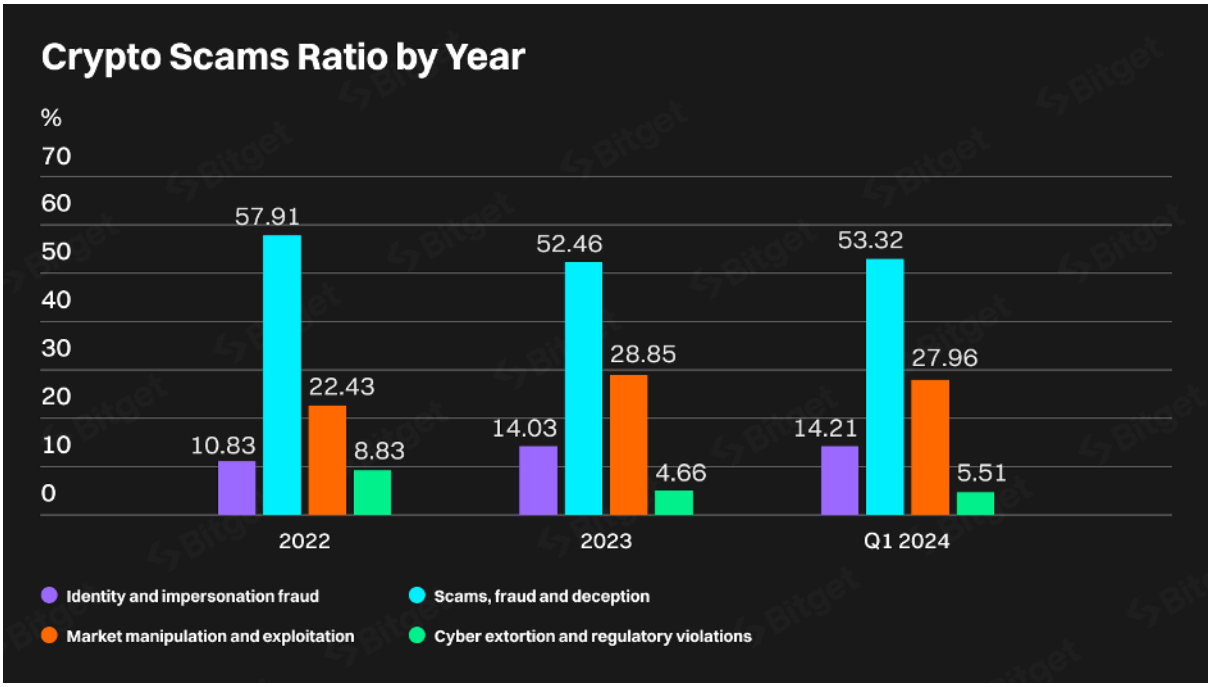


Fig. 12: Breakdown of losses from cryptocurrency deepfakes across four categories

In the cryptocurrency market, swift responses to news are essential, with the most adaptable investors often reaping the greatest rewards. A statement from an influencer, a comment from a news anchor, or an update on a project's financial status can serve as catalysts for asset value fluctuations. For instance, leveraging deepfakes to simulate inflated trading volumes can immediately increase the appeal of a token, thereby benefiting fraudsters.

As the market expands, the incidence of losses from such crimes has surged, accounting for 28.85% of total losses in 2023 (Fig. 13). The emergence of new protection methods has not stopped attackers from continuing to create new fraud schemes, such as 'stream-jacking'. Studies point to evidence of a combination of hacking events on YouTube accounts, operations with artificial intelligence, and deepfakes [10].

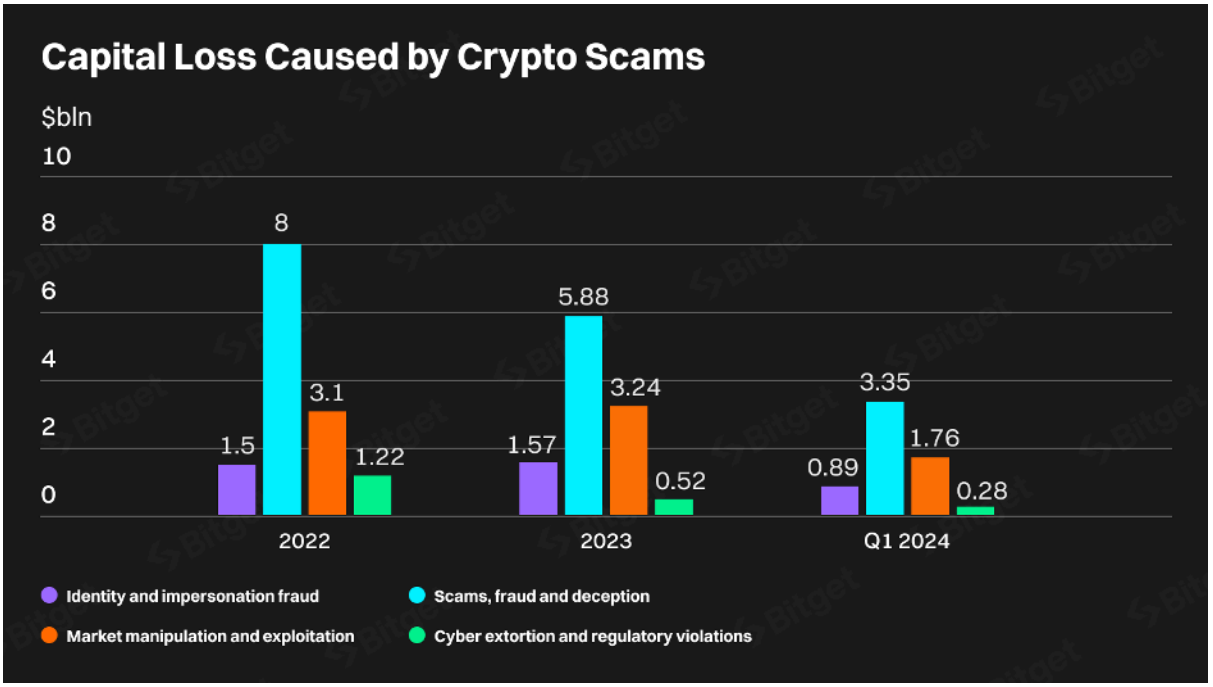


Fig. 13: Amount of losses from cryptocurrency frauds involving deepfakes in 2022, 2023 and Q1 2024

Identity fraud ranks third in terms of losses, representing the most extensive application of deepfake technology (Fig. 13). The widespread practice involves the creation of artificial identities to establish fictitious accounts and gain unauthorized access to other accounts. Although prevalent, it did not claim the top spot in the rankings primarily due to the smaller sums of stolen funds associated with each incident. These crimes also leverage social engineering techniques and bot technologies, enabling scalable criminal operations. The share of these frauds increased by 3.2% in 2023, reaching 14.21% by Q1 2024.

Extortion can be time-consuming, and victims do not always report to law enforcement and trading platforms. This explains the downward trend in 2022-2023, as it can take several years to detect a crime. Research on the detection of deepfakes highlights the complexity of the task, as these forgeries are nearly indistinguishable to untrained viewers [9]. A study by blockchain analysis firm Chainanalysis suggests that, depending on the complexity of the case and the level of international law enforcement involvement, investigations can span from several weeks to several years [11]. During the study period, losses attributable to this type of fraud were estimated at $2.03 billion, representing the smallest share across each examined period (Fig. 14, Fig. 15, Fig. 16).

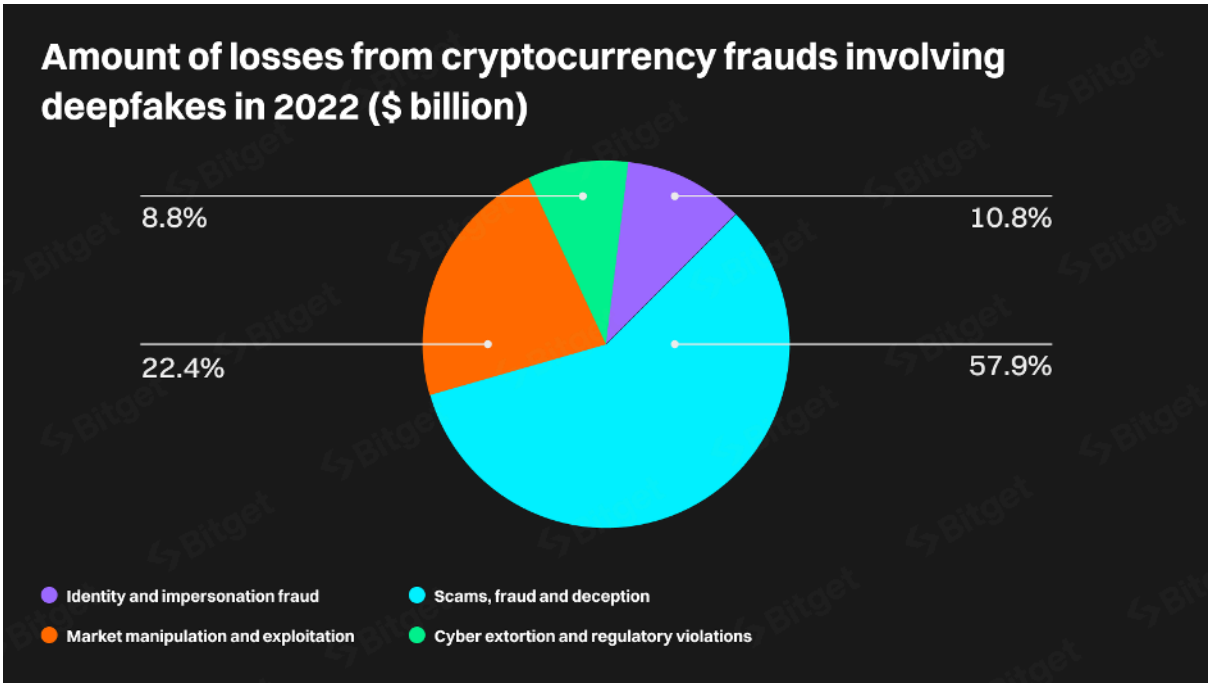


Fig. 14: Amount of losses from cryptocurrency frauds involving deepfakes in 2022 ($ billion)

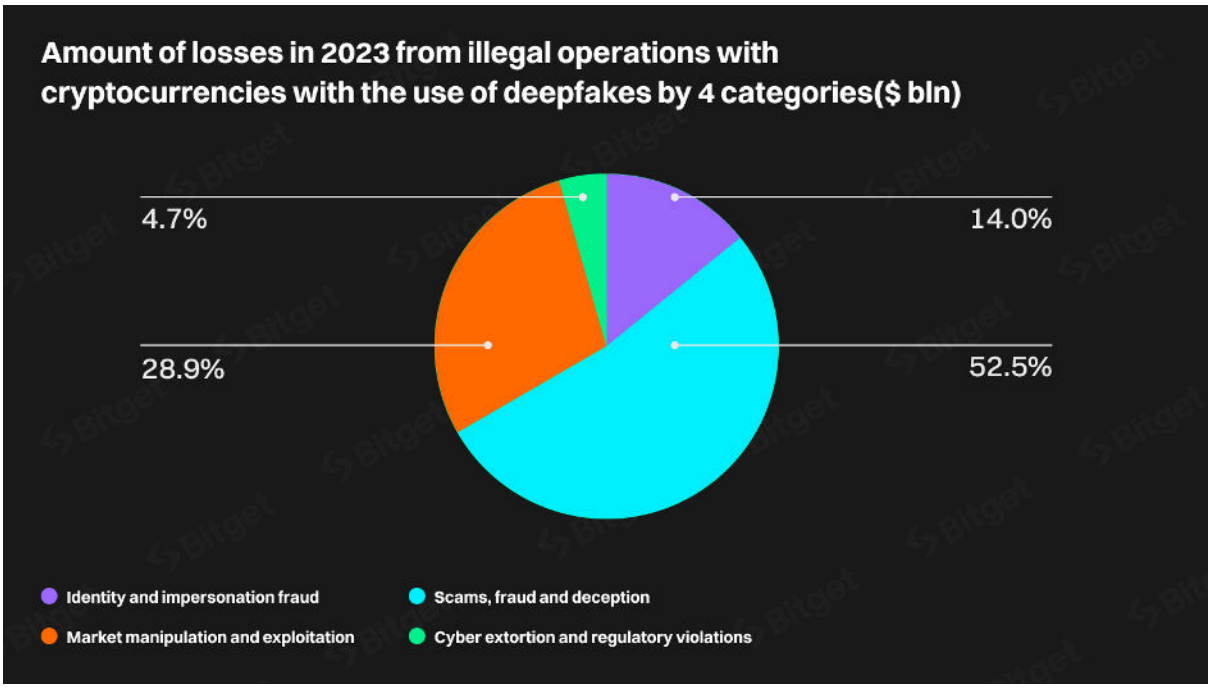


Fig. 15: Amount of losses from cryptocurrency frauds involving deepfakes in 2023 ($ bln)

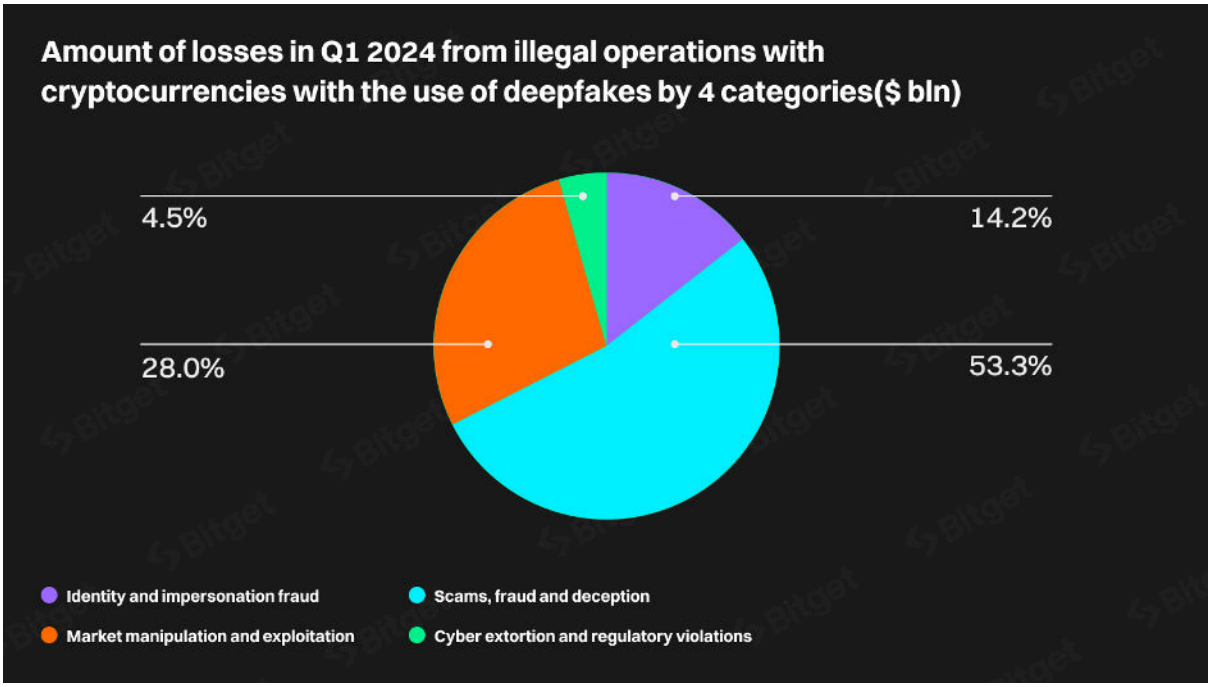


Fig. 16: Amount of losses from cryptocurrency frauds involving deepfakes in Q1 2024 ($ bln)

The lower figures for 2024 depicted in Figure 13 may suggest a decline in the losses faced by victims of fake news fraud. However, it's important to note that only the first quarter of 2024 was examined. If the losses in Q2-Q4 2024 prove to be significant, we may anticipate a pattern similar to that represented in Fig. 17. According to earlier studies, the number of deepfakes detected worldwide increased 10 times from 2022 to 2023 [12]. Crypto security measures have previously restrained the impact on the industry, but in 2024 the situation may change dramatically (Fig. 17).

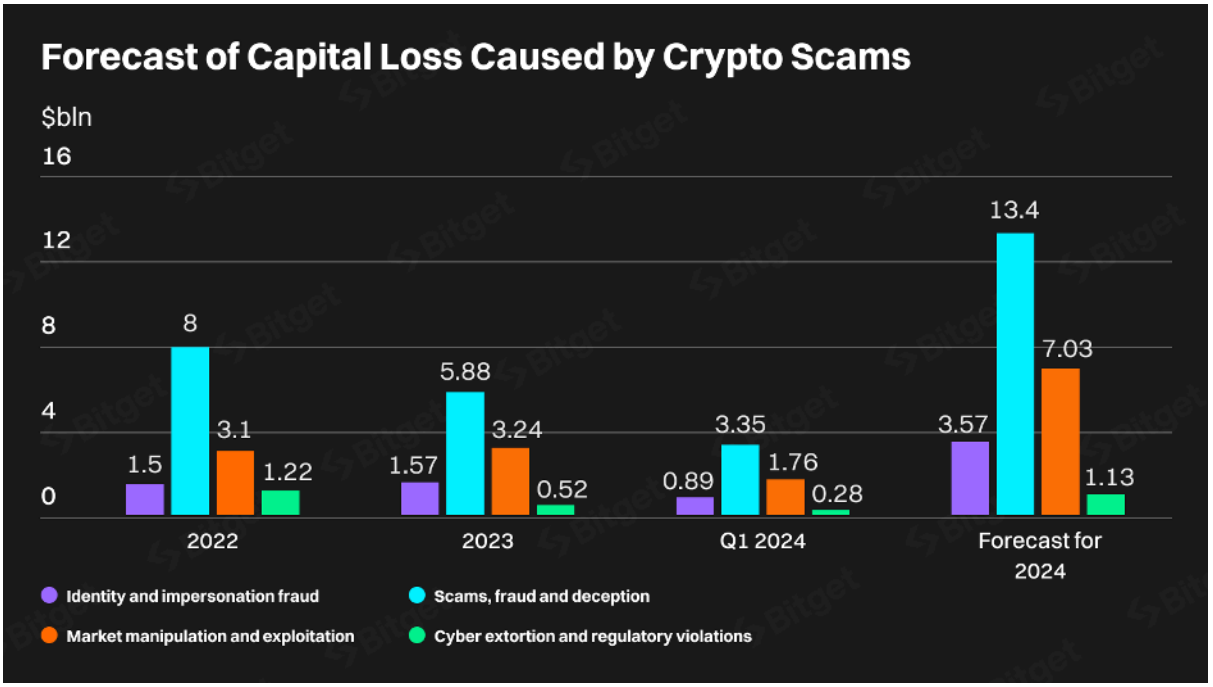


Fig. 17: Forecasted losses from cryptocurrency frauds involving deepfakes by 4 categories

This would imply that losses from the category of scams, fraud, and deception could soar to $13.40 billion, nearly equivalent to the total losses from fraudulent actions involving deepfakes in the crypto sphere in 2022 ($13.81 billion).

Forecasted losses from identity and impersonation fraud would surge to 2.26 times higher than the previous year, reaching $3.57 billion compared to $1.57 billion (Fig. 18). Additionally, losses from market manipulation and exploitation would exceed those of 2022 and 2023 by $0.69 billion.

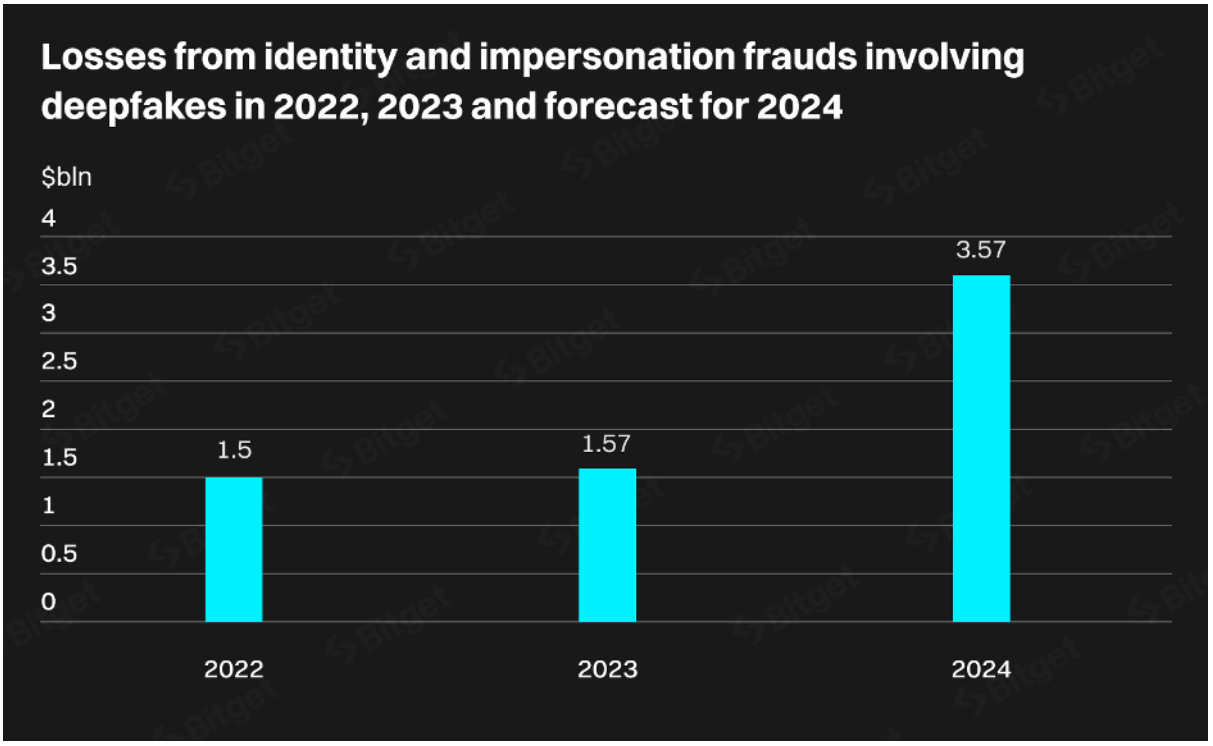


Fig. 18: Losses from identity and impersonation frauds involving deepfakes in 2022, 2023 and forecast for 2024

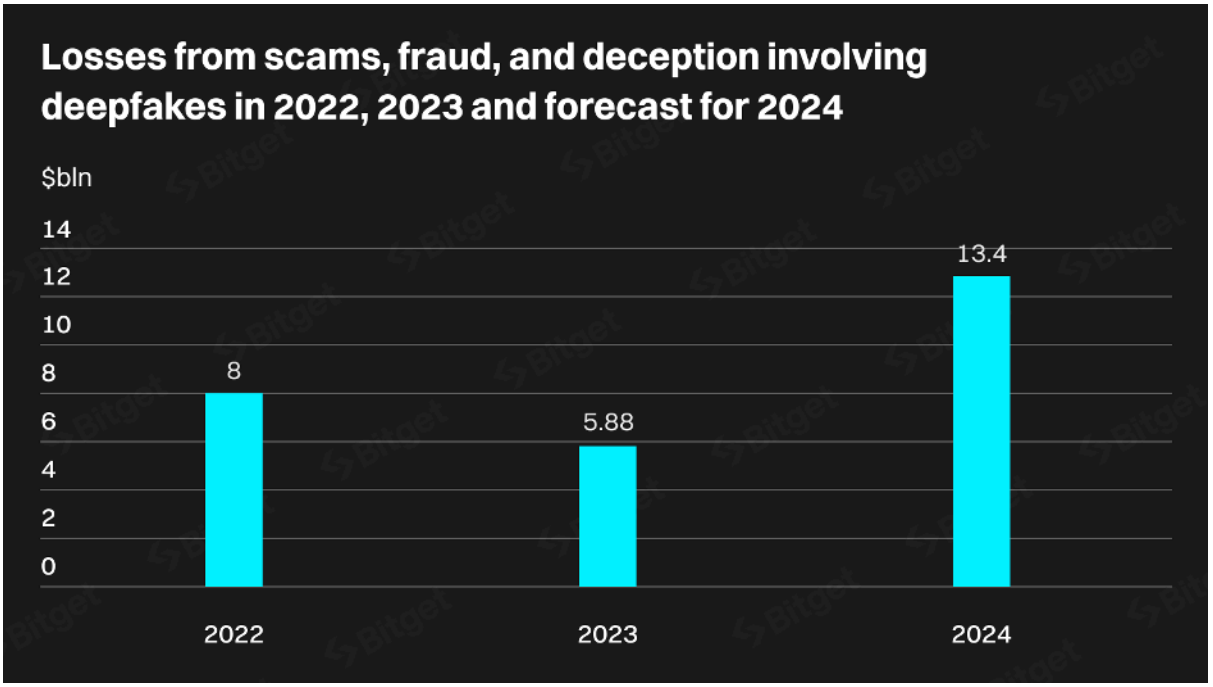


Fig. 19: Losses from scams, fraud, and deception involving deepfakes in 2022, 2023 and forecast for 2024

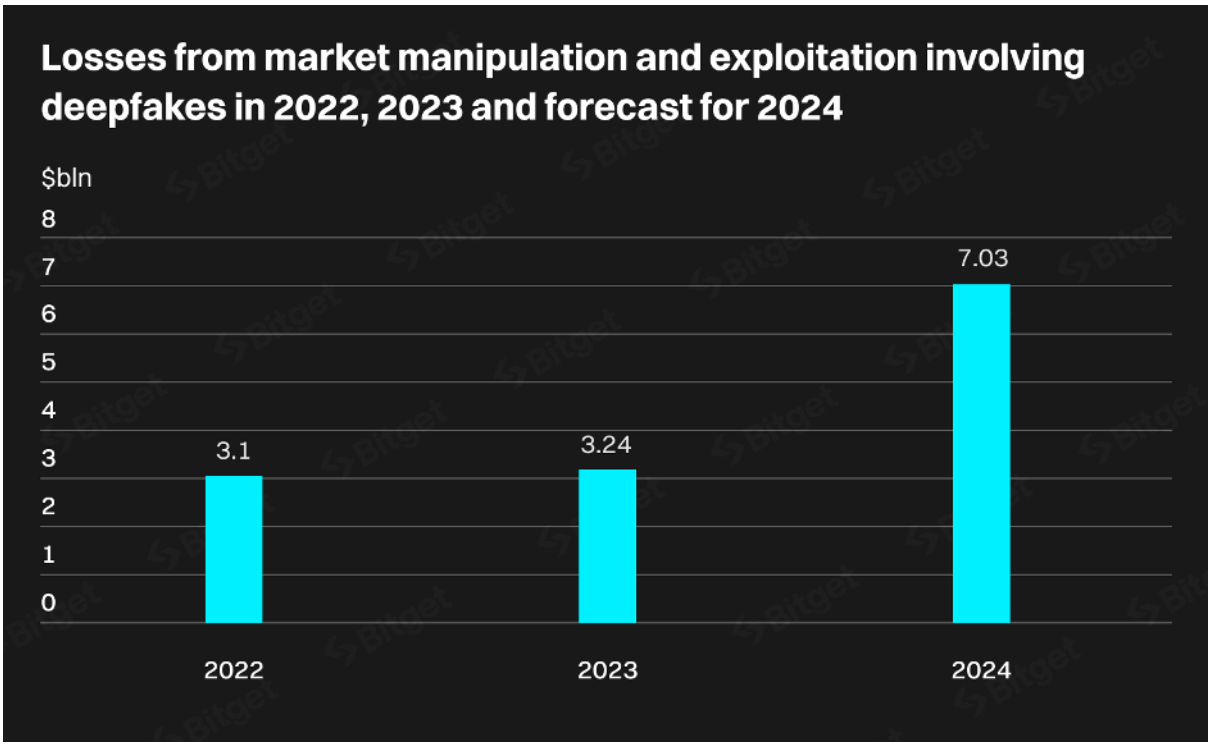


Fig. 20: Losses from market manipulation and exploitation involving deepfakes in 2022, 2023 and forecast for 2024

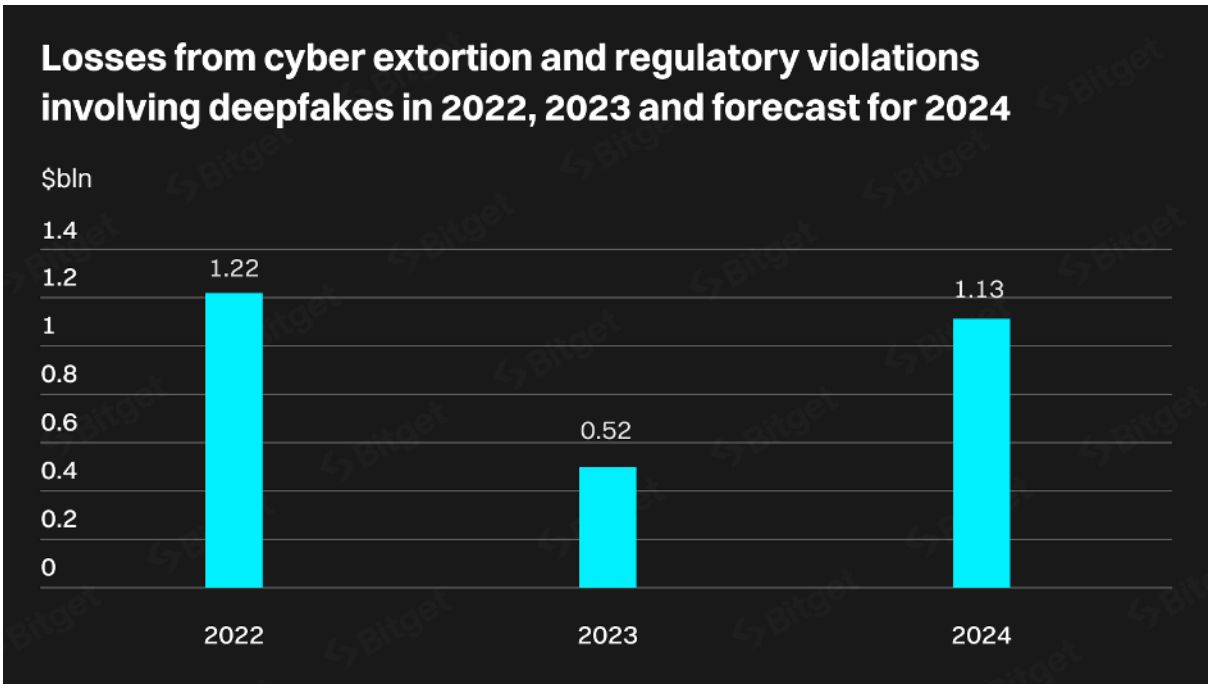


Fig. 21: Losses from cyber extortion and regulatory violations involving deepfakes in 2022, 2023 and forecast for 2024

Conclusions

During the analyzed period, we witnessed an upward trajectory in the volume of losses caused by crypto frauds, totaling $79.1 billion. Concurrently, there has been a notable increase in deepfake-related crimes, with total losses reaching $6.28 billion in Q1 2024, nearly half of the figure for the entire year of 2022 ($13.81 billion). A quarterly analysis of changes in the number of losses reveals a gradual uptick with fluctuations (Fig. 2 and Fig. 3).

To halt this trend, it's crucial to adapt regulatory frameworks and enhance the technological capabilities of industry players. However, meaningful change can only be achieved through international cooperation. Without it, we risk witnessing a geographical shift in victimization, as illegal operations may simply move from one country to another.

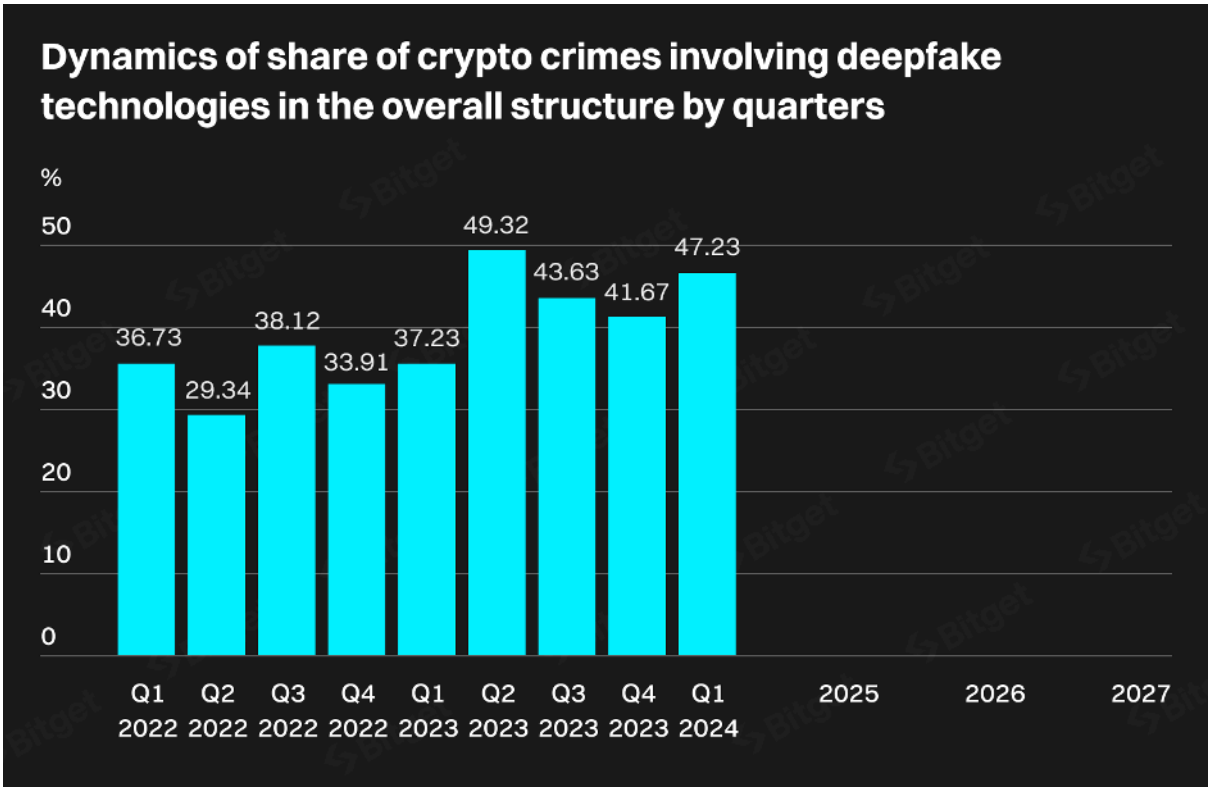


Fig. 22: Dynamics of share of crypto crimes involving deepfake technologies in the overall structure by quarters (%)

Without effective measures in place, the share of deepfake crimes within the crypto space could reach 70% by early 2026 (Figure 22). Several factors contribute to this concerning trend:

- Advancements in deepfake technologies;
- Emergence of new methods to scale crimes using fake identities;
- Market volatility, with both upswings and downturns;
- Rapid decision-making by crypto investors;
- Continued evolution of social engineering tactics;
- Increased influence of social networks.

Market sentiment, reflected in investors' risk appetite, poses a significant risk to those who consume unverified information without caution (Fig. 10 and Fig. 11). The development of new techniques for identifying fake photos, videos, and audio materials could help mitigate losses resulting from fraudulent deepfake usage during bullish market periods. Accessible identification methods will be crucial, as victims of fraud encompass not only large fintech corporations but also individuals with varying levels of wealth and awareness of blockchain technology.

The majority of crypto frauds can exploit deepfake technology to some extent, as shown by the share of losses attributed to such frauds in the overall structure (Fig. 4 and Fig. 8). The largest subset of fake news crimes in terms of losses encompasses scams, illegal fundraising,

sham arbitration, social engineering attacks, disinformation, and fake announcements (Fig. 12). Without adequate countermeasures, 2024 may witness a new record for deepfake-enabled fraud, potentially surpassing the combined losses of 2022 and 2023 (Fig. 17).

Further research

An in-depth examination of the geographic distribution of victims affected by illicit activities utilizing deepfakes within the crypto sphere can unveil legislative shortcomings in certain countries. Furthermore, it can illuminate strategies to mitigate the impact of this technology on the peace of mind and financial stability of residents in these regions. Assessing the repercussions of the proliferation of fraudulent activities involving fake photos, videos, and audio materials on investor sentiment and blockchain enterprises can unveil correlations between these metrics. Such insights can provide compelling arguments for increased funding aimed at developing countermeasures. Additionally, gathering and analyzing data on user awareness regarding methods to detect and combat fraud perpetrated through digital fakes can reveal vulnerabilities exploited by attackers and facilitate the implementation of measures to thwart fund extortion attempts.

References

1. "2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth", Chainalysis, January 2024, https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/
2. "Deepfake Cases Surge in Countries Holding 2024 Elections", Sumsub Research, May 2024 https://sumsub.com/newsroom/deepfake-cases-surge-in-countries-holding-2024-elections-sumsub-research-shows/
3. "Greed? Profits, Inflation, and Aggregate Demand", National Bureau of Economic Research, March 2018 https://www.nber.org/papers/w31618
4. "Crypto Fear and Greed Index", Mudrex, June 2024 https://mudrex.com/fear-and-greed-index
5. "Market Cap BTC Dominance", Trading View, June 2024 https://www.tradingview.com/symbols/BTC.D/
6. "Deep learning for deepfakes creation and detection: A survey", Thanh Thi Nguyen, Quoc Viet Hung Nguyen, Dung Tien Nguyen, October 2022 https://www.sciencedirect.com/science/article/abs/pii/S1077314222001114
7. "Face2Face: Real-time Face Capture and Reenactment of RGB Videos", Justus Thies, Michael Zollhofer, Marc Stamminger, June 2016

https://openaccess.thecvf.com/content_cvpr_2016/html/Thies_Face2Face_Real-Time_Face_CVPR_2016_paper.html
8. "DeepFaceLab: Integrated, flexible and extensible face-swapping framework", Ivan Perov, Daiheng Gao, Nikolay Chervoniy, May 2020 https://arxiv.org/abs/2005.05535
9. "Analysis Survey on Deepfake detection and Recognition with Convolutional Neural Networks", Saadaldeen Rashid Ahmed, Emrullah Sonuç, Mohammed Rashid Ahmed, June 2022 https://ieeexplore.ieee.org/abstract/document/9799858
10. "YouTube Deepfake and AI Crypto Scams Take $600K With "Double Your Money!" Promise", Techopedia, January 2024 https://www.techopedia.com/youtube-deepfake-crypto-scams-take-600k
11. "The Chainalysis 2024 Crypto Crime Report", Chainalysis, April 2024 https://go.chainalysis.com/crypto-crime-2024.html
12. "Identity Fraud Report", Sumsub, 2023 https://sumsub.com/fraud-report-2023/