Data Theft Risk Identification and Governance in the Metaverse Economy: Based on the Bybit Cold Wallet Theft Incident

Hang Xu

Accounting Institute, Zhejiang University of Finance and Economics, Hangzhou, 310000, China
230110920236@zufe.edu.cn

Abstract. With the rapid development of the meta-universe economy, new types of risks such as data theft are becoming more and more prominent, seriously threatening economic security and user trust. This paper takes the Bybit cold wallet theft incident as a case study to analyse the causes, impacts and governance strategies of data theft risks in the meta-universe economy. It is found that technical defects such as smart contract loopholes, weak authentication mechanisms and unencrypted cross-platform data interfaces are the main sources of risk, leading to huge asset losses, market panic and economic ecological imbalance. At the same time, the lack of legal regulation and users' lack of security awareness aggravate the risk proliferation. To address the above issues, this paper proposes to introduce Threshold Signature Scheme (TSS) to optimise key management at the technical level, improve cross-border data governance and asset insurance system at the legal level, and strengthen self-regulation, collaboration and security education at the industry and user levels. The conclusions of this study can provide a basis or reference for multi-dimensional collaborative governance to build a secure and trustworthy meta-universe economic ecology.

Keywords: Metaverse Economy, Bybit Cold Wallet, Threshold Signature Scheme (TSS).

1 Introduction

Meta-universe is a combination of "transcendence" and "universe", which refers to the virtual world constructed by integrating multiple digital technologies to interact with reality. Its concept originated from the "meta world" in Neal Stephenson's novel "Snow Crash" in 1992, and Facebook's acquisition of Oculus in 2014 promoted the development of VR, and the progress of blockchain and AI technology provided the foundation for the birth of meta universe. 2021 has become the "Year of Meta-universe", and NVIDIA, Meta and other giants have accelerated the meta universe development. The year 2021 has become the "Year of Meta-universe", and NVIDIA, Meta and other giants have accelerated the layout of meta-universe development. In recent years, with the continuous development of information technology, meta universe has gradually

M. M. Husin (ed.), *Proceedings of the 2025 International Conference on Financial Innovation and Marketing Management (FIMM 2025)*, Advances in Economics, Business and Management Research 353,
https://doi.org/10.2991/978-94-6463-874-5_82

become a popular concept. Meta-universe is driven by technological advances such as the Internet, artificial intelligence, and virtual and augmented reality, and with this potential to revolutionise the Internet, meta-universe is gaining a lot of attention and investment from technology giants around the world [1]. The economic system is an important part of the metaverse as a virtual world [2]. The metaverse economic system covers virtual asset trading, decentralised finance (DeFi) and smart contracts, Play-to-Earn model, etc. In 2023, China's Ministry of Industry and Information Technology (MIIT) and other five departments released the "Three-year Action Plan for the Innovative Development of the Metaverse Industry (2023-2025)", which proposes to achieve a breakthrough of the metaverse technology and industry by 2025. in 2023, the metaverse global market size reached 924.7 million. universe global market size reached $92.46 billion (dominated by North America, with the fastest growth rate in Asia-Pacific) [3]. However, as the meta-universe economy booms, it faces new types of risks, and Maedeh Mosharraf in "Data Governance in the Meta-Universe" points out that the convergence of these technologies (IoT, digital twins, AI, augmented reality, and blockchain), while making a significant contribution to meta-universe realisation, also poses significant challenges. but also poses significant challenges. The metaverse may inherit security and privacy vulnerabilities caused by these technologies. The metaverse faces a variety of security vulnerabilities stemming from the processing of extensive data streams, extensive user profile activity, biased results from AI algorithms, and concerns about physical infrastructure and human safety. Convergence of these technologies creates new emerging risks such as potential hijacking of wearables or cloud storage, cryptocurrency theft, and malicious use of AI to generate fake news [4].

This study focuses on the risk of data theft in the meta-universe economy. Data leakage is the intentional or unintentional exposure of confidential information to unauthorised parties [5]. Data theft in the meta-universe seriously jeopardises the economic interests and reputation of organisations and investors. Therefore, identifying and governing against this new type of risk of data theft is of great importance in maintaining the economic security and sustainability of the meta-universe. Bybit is the second largest cryptocurrency derivatives trading platform in the world, with an average daily trading volume of $25 billion. This study aims to use a case study based on the Bybit theft incident to analyse how to identify and govern the risk of data theft in the metaverse. Thus, it provides some feasible governance strategies for relevant government departments, meta-universe economic developers, enterprises and users.

2 Bybit Cold Wallet Theft Case Study

Bybit is a leading global cryptocurrency derivatives trading platform, founded in March 2018, which focuses on providing secure and efficient cryptocurrency trading services, with a business scope covering a diverse range of products such as perpetual contracts, options contracts, spot trading, leveraged trading, non-homogeneous pass-through (NFT) market and financial products, and supports Bitcoin (BTC), Ether (ETH) USDT and other major currencies, and allows users to use up to 100 times leverage. According

to Kailko data, Bybit's market share soared from 8% to 16% from October 2023 to March 2024, overtaking Coinbase (a U.S.-based cryptocurrency exchange founded in 2012 and one of the world's most popular cryptocurrency trading platforms) to become the world's second-largest cryptocurrency exchange, with an average daily trading excess of $36 billion and $16.2 billion in assets. billion and assets of $16.2 billion [6]. Cold wallets and hot wallets are important tools in cryptocurrency trading. Cold wallets function to store and generate private key addresses for secure transaction confirmation and hot wallets are used to send bitcoins to the network. Hot wallet applications provide users with the ability to view the history of executed transactions, send and compose new bitcoin transactions, receive bitcoins, sign bitcoins and send them to the network. Users are secured by identifying, verifying, and authenticating them through a cross QR code scanning process using hot and cold wallets [7]. On 21 February 2025, Bybit detected anomalous activity during the transfer of ETH from a cold wallet to a hot wallet. As shown in Fig.1, which illustrates the complete story of the cold wallet theft. Hackers induced signers to authorise malicious transactions through the interface of the signing wallet provider Safe, tampering with the smart contract logic and ultimately taking control of the cold wallet and transferring assets. The stolen assets in this incident included 401,346 ETH, 90,375stETH (a derivative asset linked to ETH) and other tokens, with a total value of approximately $1.46 billion, making it the largest single cryptocurrency theft in history. The hackers' tactic in this attack was to deploy malicious contracts in advance and phish into signers' devices to tamper with transaction data. The attackers used a "delegatecall" mechanism to modify the "masterCopy" address of the multi-signatory cold wallet to point to the malicious contract, thereby bypassing security verification and transferring funds. Rob Behnke, co-founder and executive chairman of blockchain security firm Halborn, went so far as to say that this could be "the biggest thing ever, and not just in cryptocurrency"[8]. This latest and largest theft case fully demonstrates the seriousness of data theft in the current metaverse, and reflects the fact that there are still a number of loopholes in the current technical protection and regulatory mechanisms for data. The meta-universe economy is a huge economy composed entirely of virtual currencies, which further highlights the importance of data security in it.

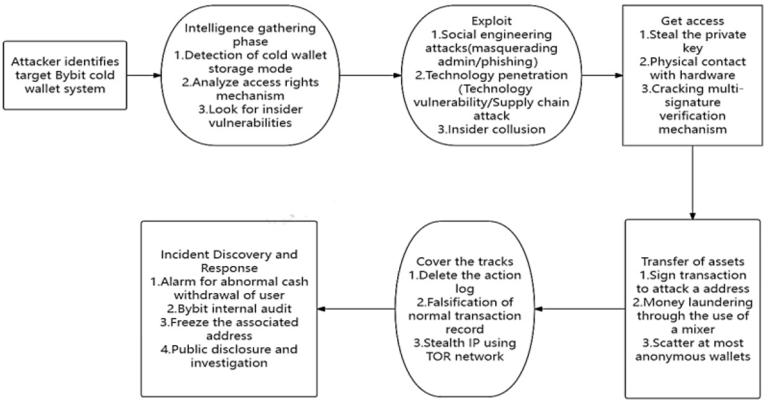

Fig. 1. Bybit cold wallet theft incident process through.

3 Risk Analysis of Data Theft in the Meta-universe Economy

In the digital age, the risk of data theft is increasingly the focus of new types of risk identification and governance facing businesses and governments. According to IBM's 2016 Cost of a Data Breach Study, the average combined cost of a data breach has reached $4 million. predictions from Juniper Research suggest that the annual cost of data breaches globally will exceed $2.1 trillion by 2019, due to the rapid digitisation of consumer lives and business records [9]. The risk of data theft manifests itself in a variety of ways. As shown in Fig.2, it mainly includes theft and illegal transfer of digital assets, leakage of users' personal information and private data, and theft of virtual identities and permissions. Data leakage can be caused by both internal and external information leakage, which may be intentional, such as data theft by an intruder or sabotage by an internal attacker. It can also be unintentional, such as accidental disclosure of sensitive information by employees and partners. A study by Intel Security5 showed that internal employees accounted for 43 percent of corporate data breaches, half of which were accidental. Internal attacks are motivated by a variety of factors, including corporate espionage, dissatisfaction with an employer, or financial incentives. Accidental leaks are primarily the result of unintentional activities due to poor business processes, such as failure to apply proper prevention techniques and security policies, or failure to engage in employee negligence [10].

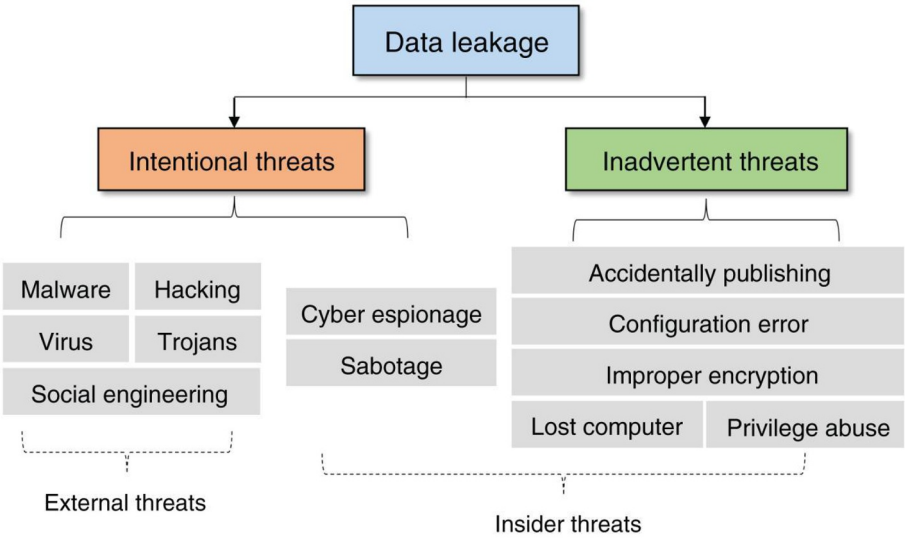

Fig. 2. Types and sources of data breaches [11].

In an information age of data explosion, the causes of data theft in the meta-universe economy are complex and multidimensional. Table1 shows us several major cases of meta-universe economy theft and their attack methods in recent years. From the system itself the meta-universe relies on blockchain (a blockchain is a distributed ledger that combines blocks of data in chronological order in a sequentially linked fashion into a

chained data structure that is cryptographically guaranteed to be tamper-proof and unforgeable) and smart contracts (i.e., low-level code scripts that run on the blockchain) and other decentralised technologies, but these are not absolutely secure [12]. Barber et al. (2012) highlight several weaknesses of Bitcoin (which can be indirectly referred to here as weaknesses that exist in blockchain technology), such as theft or loss of Bitcoin (malware attacks, accidental loss), scalability issues (e.g., delayed transaction confirmations, data retention, and communication failures), and structural issues (e.g., deflationary spirals) [13]. For example, code vulnerabilities in smart contracts were exploited by hackers in the Bybit incident. In addition, there are risks of forgery and hijacking due to weak authentication mechanisms, such as the risk of private key leakage and smart contract privilege leakage. The meta-universe needs to be integrated with multiple platforms, and data interfaces that are not encrypted or loosely managed in terms of permissions may become entry points for attacks, e.g., the risk of data theft caused by unencrypted API interfaces.

Table 1. A few important cases of meta-universe economic data theft in recent years.

Organisation/Platform	Amount of theft	Year	Source (of information etc)	Style of attack (physics)
Decentraland (metaverse virtual world)	Over $1.5 million		externally	Dummy website cloning, social platform diversion scams
Axie Infinity (blockchain gaming platform)	Approximately $625 million in ETH and USDC (known as USD Coin, a stablecoin pegged to the U.S. dollar at a 1:1 ratio and designed to provide a means of holding, trading and settling the value of U.S. dollars in the crypto world)	2022	externally	Social Engineering Attacks (Phishing), Private Key Disclosure, Smart Contract Privilege Vulnerabilities
OpenSea (the world's largest NFT trading platform)	Over 300 users have had their NFTs (cryptocurrencies) stolen, losing over $2 million	2022	externally	Phishing site forgery, malicious contract authorisation
The Sandbox (Metaverse Virtual Land Platform)	Email, wallet addresses and transaction records of 500,000 users stolen and sold on the dark web	2023	externally	Unencrypted API interface, database injection attacks
Bored Ape Yacht Club	Jay's holdings of BAYC (an expensive form of NFT) worth over $3.2 million in human money	2022	externally	Phishing attacks, private key compromise

From the user's point of view, due to the ambiguity of the virtual-real boundary of the meta-universe, the user's vigilance or security awareness drops, and it is easy to click on the phishing links (the unscrupulous elements use all kinds of means to imitate the URL address and page content of the real website, or use the loopholes on the real website server programme to insert dangerous HTML codes into certain web pages of the site, so as to cheat the user's bank or line card account number, passwords and other private information), shared virtual device permissions, etc., leading to account or private key leakage. In addition, social interactions are frequent in the meta-universe, and attackers can disguise themselves as trusted characters (e.g., virtual customer service, friends) to induce users to disclose sensitive information. In addition, users may store their private keys on unsecured local devices or in the cloud due to lack of expertise, or use weak passwords to protect their digital wallets, increasing the risk of theft.

In terms of legal regulation and government governance, the meta-universe economy involves transnational transactions and decentralised organisations, and it is difficult for traditional laws to specify the subject of recourse for data theft. Most countries lack detailed planning for property rights protection and theft conviction of assets such as NFT and cryptocurrencies, making it difficult to defend rights. Meta-universe crimes often involve multinational participants, but international data sharing and judicial collaboration mechanisms are not yet mature, making tracing difficult.

The risk of data theft in the metaverse has far-reaching and multidimensional implications for the metaverse economy. Theft of virtual assets not only damages users' property rights, but also directly erodes their trust in virtual assets. While the Bybit incident caused economic losses, Ether plummeted by 6.7% in 24 hours, Bitcoin fell by 3%, and 170,000 people blew up their positions by more than US$570 million. the Bybit token BYB plummeted by 12.3% in one hour, and the futures market liquidated by more than US$200 million [14]. Reflecting the market panic generated by users about asset theft, it reduces user engagement and weakens the liquidity of the economic system. Data misuse indirectly resulting from data theft can have an impact on the market order. Metaverse optimises its services by tracking user behavioural data (e.g., virtual space activity paths, consumption preferences), but this data may be used for unfair competition or market manipulation. A team of professors from Fudan University found through more than 800 taxi experiments that the probability of an Apple phone user being picked up by a more expensive model at the same time when posting the same order is three times higher than that of a non-Apple phone [15]. Data misuse exacerbates information asymmetry, harms consumer rights and interests, leads to imbalance in the allocation of market resources, and threatens the long-term stability of the economic ecology. The globalised nature of the meta-universe makes cross-border transmission of data face regulatory conflicts. For example, the EU General Data Protection Regulation (GDPR) contradicts the lax policies of some countries, and enterprises may take advantage of regulatory loopholes to transfer data and evade responsibility. This weakens user trust and hinders cross-border economic co-operation.

4 Strategies for Managing the Risk of Data Theft in the Meta-universe Economy

At the technical level, against the risk of data theft, the Threshold Signature Scheme (TSS) deserves to be introduced. TSS is a cryptographic protocol that allows multiple participants to work together to generate a valid digital signature without the need for any single participant to be in possession of the full private key. In the meta-universe, user identity, attribution of digital assets (e.g., NFTs, virtual lands) need to be verified by trusted signatures. TSS enables distributed identity management. For example, the user's private key is stored in multiple nodes in slices, and a valid signature can be generated only when a threshold number of nodes collaborate, avoiding the risk of a single point of leakage. TSS can also be used for multi-signature control of assets, e.g., if virtual asset transactions require authorisation from multiple parties (e.g., decentralised autonomous organisations' governance in the blockchain), TSS generates a single aggregated signature, which reduces the redundancy of data on the chain compared with the traditional multi-signature scheme, and improves the efficiency. Although TSS has great potential in the metaverse, there are still some problems. For example, TSS is different between different projects, and there are difficulties in interactive operations. Meta-universe nodes join and exit frequently, and a more efficient key update mechanism is still needed. Along with the development of AI technology, combining AI technology to optimise the dynamic adjustment of threshold signatures (e.g., automatically adjusting the threshold according to the risk level) or generating distributed keys based on biometric features may become the innovative direction of TSS in the meta-universe.

At the legal and regulatory level, laws and regulations related to the metaverse should be established and improved. For example, Hong Kong's Securities and Futures Commission (SFC) will officially implement a new Virtual Asset Service Provider (VASP) licensing system on 1 June 2023 to standardise the auditing of trading platforms and cold wallets. There is also a need for a metaverse asset insurance system, as Coinbase plans to be regulated to launch a proprietary insurance company, which has even written a "crime" policy covering hot wallets (online wallets).

hacking, and insurance coverage for cryptocurrency things that are kept offline in cold storage. Dedicated insurance companies This system could solve the problem of the shortage of available insurance for cryptocurrency exchanges, in fact, even exchanges the size of Coinbase are left to set aside some of their own funds to cover their customers' losses in the event that they lose money to hackers, the problem with this solution is that the lack of a formalised structure leads to a great deal of ambiguity in the use of corporate funds, and users don't know if the exchange will set aside funds for other purposes. On the other hand, funds can be segregated through proprietary insurance and held in regulated audit vehicles, which can help companies to "go global" and get more protection from the reinsurance market.

As far as the industry and user level are concerned, it is of primary importance to improve users' data security awareness and prevention skills. Do not arbitrarily fill in personal sensitive information on untrustworthy platforms or websites, avoid clicking on suspicious links, change passwords on a regular basis, use the system's multi-identity

verification function, try to use VPN for encrypted connections to virtual private networks, and regularly check their account records, and contact the platform's customer service in a timely manner to verify and deal with any suspicious situations. All these operations can effectively avoid many risks of data theft. Industry self-regulation and collaboration are particularly important in the industry sector, where a study by Intel Security5 showed that internal employees account for 43 per cent of company data breaches, half of which are accidental. Internal attacks are motivated by a variety of factors, including corporate espionage, dissatisfaction with an employer, or financial incentives. Accidental leaks are mainly the result of unintentional activities due to poor business processes, such as failure to apply appropriate prevention techniques and security policies, or failure to perform employee negligence [16]. Improving internal auditing of companies in the field of meta-universe economy, employee training, and the establishment of meta-universe economy industry associations are all effective actions.

5 Conclusion

The coexistence of the booming meta-universe economy and new types of risks, such as data theft, poses a serious challenge to technological security, user trust, and global governance. Taking the Bybit cold wallet theft incident as the core case, this paper systematically analyses the causes, impacts and governance paths of data theft in the meta-universe economy. It is found that technical flaws such as smart contract vulnerabilities, weak authentication mechanisms, and unencrypted cross-platform interfaces are the main sources of risks, which are further amplified by the lack of user security awareness, lack of legal regulation, and lack of international collaboration mechanisms. Such risks not only lead to huge asset losses and market panic (e.g., the Bybit incident triggered sharp fluctuations in the cryptocurrency market), but also exacerbate the misuse of data and imbalance in resource allocation, threatening the long-term stability of the meta-universe economy.

To address the above issues, this paper proposes a multi-dimensional governance strategy: at the technical level, the introduction of TSS optimises key management and reduces the risk of single-point leakage; at the legal level, it improves the cross-border data governance framework and the asset insurance system, and strengthens the regulatory coordination; and at the level of the industry and the users, it is necessary to improve the protection ability through security education and self-regulation. The study also points out that the dynamic and globalised nature of the metaverse requires flexibility and foresight in the governance mechanism, and in the future, it is necessary to optimise the dynamic security strategy with AI technology, and promote international judicial collaboration and standardisation.

This study provides theoretical and practical references for the risk governance of meta-universe economy, but limited by the singularity of the case analysis and the rapid iteration of technological development, it is necessary to further combine the multi-scenario empirical research in the future, and continue to track the long-term impacts of the technological evolution and policy adjustments on the risk governance. Only

through the synergistic innovation of technology, law and society can build a safe and trustworthy meta-universe economic ecology and support its sustainable development.

References

1. Cheng, S.: Metaverse. In: Metaverse: Concept, Content and Context, pp. 1-23. Springer Nature Switzerland, Cham (2023).
2. Chen, Y., Cheng, H.: The economics of the metaverse: A comparison with the real economy. Metaverse **3**(1), 19 (2022).
3. GoerTek: AI + Metaverse Drive Growth in Consumer Electronics Demand; Over 8,000 Patents Empower Innovation. Hexun.com. https://mr.baidu.com/r/ 1Blt4oOD3Dq 2025/04/18, last accessed 2025/4/25.
4. Mosharraf, M.: Data governance in the metaverse: addressing security threats and countermeasures across the data lifecycle. Technology in society, 102910 (2025).
5. Cheng, L., Liu, F., Yao, D.: Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery **7**(5), e1211 (2017).
6. Hexun.com: Stock Market Update on July1st, 2024, last accessed 2025/4/25. https://m.hexun.com/stock/2024-07-01/213372052.html, last accessed 2025/4/25.
7. Khan, A.G., Zahid, A.H., Hussain, M., et al.: Security of cryptocurrency using hardware wallet and QR code. in: 2019 International Conference on Innovative Computing (ICIC), pp. 1-10. IEEE (2019).
8. 21st Century Business Herald: The Biggest Theft Ever! Crypto currency market hacked, 10.8 billion yuan vanished without a trace. https://www.21jingji.com/article/20250222/herald/88cc725f9c41febc73469ead5723e6a1, last accessed 2025/4/25.
9. Albshaier, L., Almarri, S., & Hafizur Rahman, M. M.: A review of blockchain's role in e-commerce transactions: open challenges, and future research directions. Computers (2073-431X) **13**(1), (2024).
10. Syed, R.: Enterprise reputation threats on social media: a case of data breach framing. North-Holland (3), (2019).
11. Ganta, S. R., & Acharya, R.: On breaching enterprise data privacy through adversarial information fusion. IEEE International Conference on Data Engineering Workshop. IEEE, (2008).
12. Zou, W., Lo, D., Kochhar, P.S., et al.: Smart contract development: challenges and opportunities. IEEE Transactions on Software Engineering **47**(10), 2084-2106 (2019).
13. Nofer, M., Gomber, P., Hinz, O., et al.: Blockchain. Business & Information Systems Engineering **59**, 183-187 (2017).
14. Recent incidents of virtual currency exchanges being stolen have mainly centred around Bybit Exchange. Baidu News. https://mr.baidu.com/r/ 1BlzCWESoBq 2025/04/18, last accessed 2025/4/25.
15. 21st Century Business Herald: Professor from Fudan University spent 50,000 yuan on taxi fares for over 800 rides! Is it true that Apple mobile phones cost more for taxi rides than Android ones? Is it true that Apple mobile phones cost more for taxi rides than Android ones? Reporter's personal test. 21st Century Business Herald. https://export.shobserver.com/baijiahao/html/347817, last accessed 2025/4/25.
16. Patil, R., Pise, G., & Bhosale, Y.: Root causes, ongoing difficulties, proactive prevention techniques, and emerging trends of enterprise data breaches, (2023).