Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats

Mochammad Tanzil Multazam[*], Rifqi Ridlo Phahlevi[**], Melati Indah Purnomo[***], Sri Budi Purwaningsih[****], Bobur Sobirov[*****]

DOI: https://doi.org/10.22304/pjih.v11n1.a2

Submitted: March 25, 2023 | Accepted: December 14, 2023

Abstract

This study aims to understand the vulnerabilities faced by enterprises operating on token-based blockchain businesses and the role of legal, due diligence procedures in mitigating such risks. It employed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses method and sourced data from DeFillama, a platform tracking decentralized finance developments, to categorize hacking incidents into five major groups: Ecosystem, Infrastructure, Protocol Logic, Rugpull, and Smart Contract Language. The findings highlight that Infrastructure attacks, mainly through Private Key Compromise, are the most damaging. They cause losses of over 800 million dollars between 2020 and 2023. It necessitates comprehensive and adaptable legal, due diligence strategies focusing on jurisdictional legal frameworks, platform usage terms, regulatory compliance, and potential legal issues. The study underscores the importance of further research to evaluate and enhance the effectiveness of these measures in addressing the unique challenges of blockchain technology, which are crucial for enhancing the resilience and sustainability of blockchain enterprises, thereby promoting global trust in this emerging field.

Keywords: blockchain technology, decentralized finance, legal due diligence.

A. Introduction

Since the birth of Ethereum in 2015, the use of blockchain as a media for storing transaction information in the cybersecurity world has increased.[1] Ethereum

PADJADJARAN Journal of Law Volume 11 Number 1 Year 2024 [ISSN 2460-1543] [e-ISSN 2442-9325]

[*] Senior Lecturer at the Departement of Law, Muhammadiyah Sidoarjo University, Majapahit St, 666 B, Sidoarjo-Indonesia, S.H. (Muhammadiyah Malang University), M.Kn. (Airlangga University), tanzilmultazam@umsida.ac.id.

[**] Senior Lecturer at the Departement of Law, Muhammadiyah Sidoarjo University, Majapahit St, 666 B, Sidoarjo-Indonesia, S.H. (Muhammadiyah Surakarta University), M.H. (Airlangga University), qq_levy@umsida.ac.id.

[***] Student at the Departement of Law, Muhammadiyah Sidoarjo University, Majapahit St, 666 B, Sidoarjo-Indonesia, melatiaping@gmail.com.

[****] Lecturer at the Departement of Law, Muhammadiyah Sidoarjo University, Majapahit St, 666 B, Sidoarjo-Indonesia, S.H. (Muhammadiyah Surakarta University), M.Kn. (Airlangga University), sribudi@umsida.ac.id.

[*****] Professor at the Department of Economics, Samarkand Branch of Tashkent State University of Economics, 51 Professorlar Street, Samarqand, Uzbekistan, B.A. (Samarkand Institute of Economics and Service), M.Sc. (Universidad de Las Palmas de Gran Canaria), Ph.D. (Samarkand Institute of Economics and Service), mrbobursobirov@gmail.com.

[1] Robert Donald Leonhard, "Decentralized Finance on the Ethereum Blockchain," *SSRN Electronic Journal* (2019): 1-2, https://doi.org/10.2139/ssrn.3359732.

augments smart contract technology with blockchain technology. This has led to the birth of many possibilities for the massive use of blockchain.[2] Blockchain technology was initially only functioned as a peer-to-peer payment process without involving third parties, usually banks or financial institutions.[3]

The development of blockchain technology must of course be balanced with other study related to its impact, not only in terms of economic and social,[4] but also in terms of legal aspects, especially legal protection for its users. The current total funds circulating in the blockchain ecosystem exceed $2 trillion, with daily transactions approaching $100 billion (Figure 1). These funds are distributed among numerous blockchain ecosystems, comprising decentralized applications and platforms.[5]

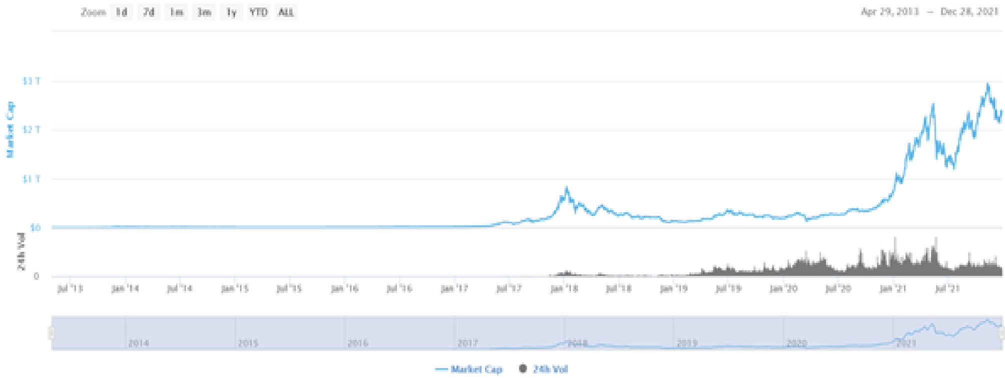


Figure 1. Total Funds in Circulation in the Blockchain Ecosystem (As of December 28, 2021)[6]

In an environment where legitimate enterprises coexist with fraudulent operations, the blockchain ecosystem has witnessed significant losses due to cybercrime. For instance, YFDEX.Finance, a fraudulent venture caused $20 million in investor losses, highlighting the prevalence of scams and Ponzi schemes.[7] Recent targeted attacks on platforms like Mango Markets, Stax, and Rabby Swap led to a

[2] Harsh Singh Chauhan and Jagjeet Jena, "Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets," *International Journal of Trend in Scientific Research and Development* (2021): 44-54.

[3] Satoshi Nakamoto, "Bitcoin: Sebuah Sistem Uang Tunai Elektronik Peer-to-Peer," accessed on July 14, 2022, https://bitcoin.org/bitcoin.pdf.

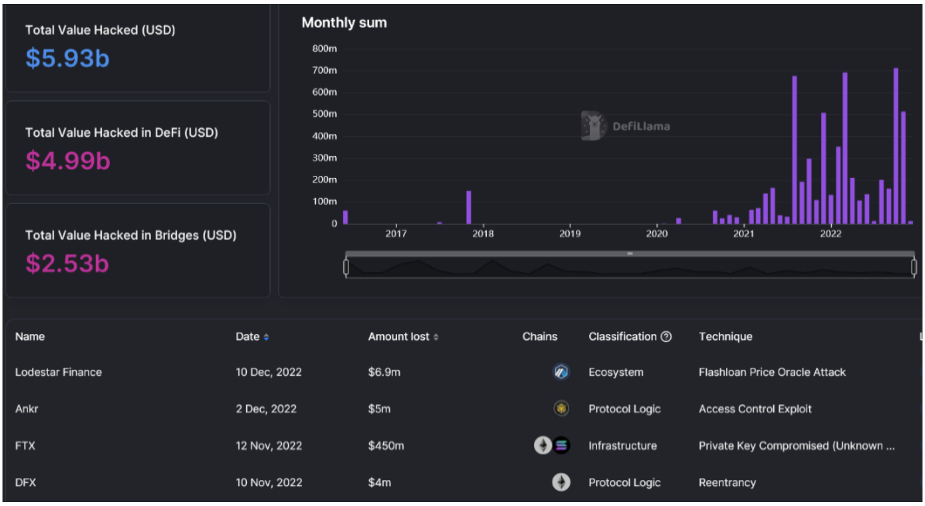
[4] Constantin Anghelache (et.al.), "Perspectives of the Development of World Economy in the Blockchain Conditions and Big Data," *Proceedings of the International Conference on Applied Statistics* 1, no. 1 (2019): 44–59, https://doi.org/10.2478/icas-2019-0005.

[5] Paolo Tasca and Claudio J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," *Ledger* 4 (2019): 1–39, https://doi.org/10.5195/ledger.2019.140.

[6] Chart Coinmarketcap, "Total Cryptocurrency Market Cap," accessed on December 28, 2021, https://coinmarketcap.com/charts/.

[7] Bedil Karimov and Piotr Wójcik, "Identification of Scams in Initial Coin Offerings with Machine Learning," *Frontiers in Artificial Intelligence* 4 (2021): 718450, https://doi.org/10.3389/frai.2021.718450.

combined loss of $114.56 million. Data from DeFiLama reveals that cumulative financial losses from criminal activities in the blockchain industry have reached $5.93 billion.[8] These incidents involve cybercrime tactics unique to the blockchain, such as RugPulls, private key compromises, and flash loans, resulting in significant user losses (Figure 2).[9]



Total Value Hacked (USD)
$5.93b

Total Value Hacked in DeFi (USD)
$4.99b

Total Value Hacked in Bridges (USD)
$2.53b

Name	Date	Amount lost	Chains	Classification	Technique
Lodestar Finance	10 Dec, 2022	$6.9m	●	Ecosystem	Flashloan Price Oracle Attack
Ankr	2 Dec, 2022	$5m	●	Protocol Logic	Access Control Exploit
FTX	12 Nov, 2022	$450m	● ●	Infrastructure	Private Key Compromised (Unknown ...
DFX	10 Nov, 2022	$4m	●	Protocol Logic	Reentrancy

Figure 2. Total Funds Stolen from the Blockchain Ecosystem (As of December 13, 2022)

The range of attack methods targeting DeFi protocols underscores the importance of robust security measures in their development and maintenance. Given the multitude of tactics available to hackers, proactive security measures are essential. This entails comprehensive vulnerability assessments, rigorous code auditing, and the implementation of multi-layered security protocols.

1. Trends and Techniques of Blockchain Hacking: A Comprehensive Review

The analysis conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method furnishes a comprehensive understanding of trends and techniques prevalent in cryptocurrency hacking events. Primary data sourced from DeFillama, a platform tracking Decentralized Finance (DeFi) development in the blockchain ecosystem, constitutes the dataset.[10]

1. Name represents the name of the hacked platform.

[8] Defillama Defillama, "Total Hacks Value," accessed on December 13, 2022, https://defillama.com/hacks.

[9] Yusra Fadhillah (et.al.), *Teknologi Blockchain dan Implementasinya* (Medan: Yayasan Kita Menulis, 2022), 95-106.

[10] Mochammad Tanzil Multazam, "Protocol Hack in Cryptoworld," accessed on July 26, 2023, https://doi.org/10.5281/zenodo.8185509.

2. Date represents the date when the hack took place.
3. Classification categorizes the type of hack.
4. Technique describes the specific hacking technique that was employed.
5. Amount lost represents the financial loss from the hack, given in a string format with a dollar sign and a "m" at the end, indicating millions.

The data were used to answer the following questions.

1. What are the five most used types to hack?
2. What are the five most used techniques to hack?
3. How much loss has each of the five most used techniques caused?
4. How much loss has each of the five most used types caused?
5. How much was lost in total in 2020, 2021, 2022, and 2023?
6. What was the most used technique in 2023, 2022, 2021, and 2020?
7. What was the most used classification in 2023, 2022, 2021, and 2020?
8. What are the most used techniques which result in the most total loss, and their classification, for each of 2023, 2022, 2021, and 2020?

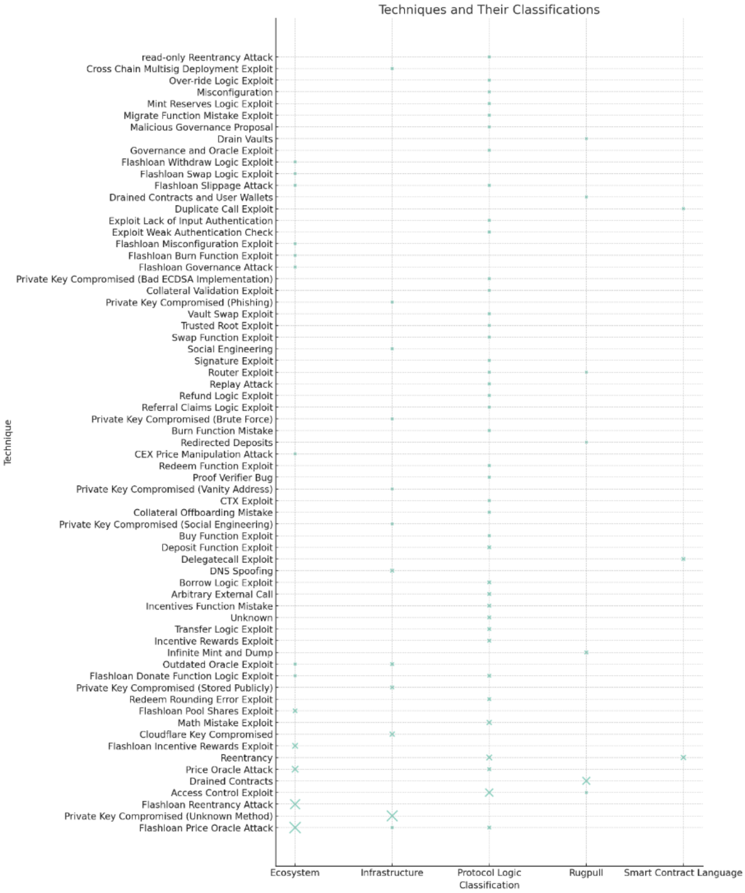


Figure 3. Hacking Technique and Their Classification in TBBB

DeFillama were employed to track hacking or exploit events in blockchain that involve platform, have a loss in value, use kind of technique. The dates is from 2020 to July 26, 2023. From the data we identified 189 events. The analysis led to the categorization of these attacks into five unique types and 67 unique techniques (Figure 3).

The scatter plot illustrates the correlation between various hacking techniques and their corresponding classifications, with each data point representing a unique pairing of a specific technique and classification. The magnitude of each data point reflects the frequency of the associated combination, emphasizing the prevalence of diverse hacking techniques within each classification. Notably, the 'Ecosystem' and 'Infrastructure' classifications demonstrate a wide array of utilized techniques, highlighting the importance of understanding both overarching categories of cyber-attacks and the specific approaches employed within each category.

a. What are the Five Most Used Classification and Technique to Hack?

The data reveals a hierarchical structure of hacking incidents characterized by distinct classifications and associated techniques. The most frequent classification, occurring 68 times, is 'Protocol Logic'. The term encapsulates hacks that exploit logical flaws in a protocol's design or implementation. It is followed by the 'Ecosystem', which pertains to attacks that take advantage of vulnerabilities within the broader network or system of interconnected entities, which appeared 61 times. The 'Infrastructure' signifies attacks that target the underlying hardware, software, networks, or other foundational components of a system, found in 36 instances. Lesser frequent yet notable classifications include 'Rugpull' and 'Smart Contract Language', occurring 17 and 7 times, respectively.

Within these classifications, specific hacking techniques have been recurrently employed. 'Flashloan Price Oracle Attack', a method that manipulates price oracles in decentralized finance through flash loans, topped the list with 24 instances. It was followed by the 'Private Key Compromised (Unknown Method)' technique, a term denoting unauthorized access to private cryptographic keys, which was identified for 19 times. The 'Flashloan Reentrancy Attack,' characterized by reentrant function calls within flash loan exploits, occurred 16 times. Furthermore, the techniques of 'Access Control Exploit' and 'Drained Contracts,' which entail breaches of access control measures and depletion of contract funds were identified in 12 and 10 instances, respectively.

b. How Much Loss Has Each of the Five Most-Used Classification and Techniques Caused?

Analyzing the financial implications of various hacking techniques provides valuable insights into the extent of damage caused by illicit activities. Among the top five utilized techniques, the 'Access Control Exploit' stands out as a significant contributor to financial losses, amounting to approximately $658.965 million.

'Drained Contracts' also resulted in substantial losses, totaling around $140.820 million. Additionally, the 'Flashloan Price Oracle Attack,' 'Flashloan Reentrancy Attack,' and 'Private Key Compromised (Unknown Method)' techniques further intensified the financial impact, leading to losses of $386.890 million, $177.990 million, and a significant $1332.890 million, respectively. These findings highlight the severe economic ramifications of these hacking techniques and underscore the critical importance of implementing robust security measures.

A comprehensive analysis of the total losses attributed to the five most prevalent types of hacks reveals the significant economic impact of these incidents. Hacks categorized under the 'Ecosystem' type resulted in losses totaling $1057.57 million, while 'Infrastructure' hacks, targeting foundational system components, incurred even higher losses of $2365.10 million. Notably, 'Protocol Logic' hacks, exploiting logical flaws in protocol design or implementation, emerged as the most financially damaging, with losses amounting to $2539.46 million. Additionally, 'Rugpull' and 'Smart Contract Language' hacks contributed to financial losses, totaling $203.496 million and $123.61 million, respectively. These financial repercussions underscore the urgent need for comprehensive audits and proactive security measures.

c. How Much Loss Compared to Technique and Classification by Year?

An examination of the total financial losses incurred due to blockchain hacks from 2020 to 2023 reveals a concerning upward trend. In 2020, the total loss amounted to a substantial $183.75 million, highlighting the financial vulnerability of blockchain ecosystems. This figure escalated drastically in 2021, reaching an alarming $2290.16 million. The losses peaked in 2022, totaling $3280.77 million, emphasizing the escalating threat posed by these illicit activities. However, there was a notable decline in losses in 2023, totaling $534.56 million, suggesting potential advancements in security measures and mitigation strategies.

A systematic examination of the predominant hacking techniques employed annually provides valuable insights into the changing landscape of security breaches. The 'Flashloan Price Oracle Attack' was the most commonly used technique in both 2020 and 2021. However, in 2022 and 2023, the 'Private Key Compromised (Unknown Method)' and 'Flashloan Reentrancy Attack' techniques, respectively, became more prevalent. These findings underscore the dynamic and evolving nature of threats in the blockchain ecosystem, necessitating proactive and adaptable security solutions.

Furthermore, a scrutiny of the most frequent classifications of hacks each year unveils shifts in the types of attacks that are most common. The 'Ecosystem' classification was the most prevalent in 2020 and 2021, indicating that attackers frequently exploited vulnerabilities within the broader network or system of interconnected entities during these years. However, in 2022 and 2023, the 'Protocol Logic' classification, which pertains to logical flaws in a protocol's design or implementation, became the most common. This transition underscores the necessity for thorough protocol logic audits and the implementation of resilient security protocols.

d. What are the Most Used Techniques Which Result in the Most Total Loss and Their Classification From 2020-2023?

The data also provides valuable insights into the most financially damaging hacking techniques and their corresponding classifications for each year from 2020 to 2023. In 2020, the 'Flashloan Price Oracle Attack', classified under 'Ecosystem', incurred the highest loss, totaling $58.10 million. This underscores the significant financial impact of this technique, which manipulates price oracles in decentralized finance through flash loans. In 2021, the 'Access Control Exploit' emerged as the most economically detrimental technique, classified under 'Protocol Logic', resulting in losses of $635.20 million. This technique involves breaching access control measures, indicating the significant cost of such security vulnerabilities.

Significantly, in both 2022 and 2023, the 'Private Key Compromised (Unknown Method)' technique, categorized under 'Infrastructure', resulted in the greatest financial losses, totaling $641.54 million and $231.00 million, respectively. This method involves unauthorized access to private cryptographic keys, underscoring the significant financial consequences of such security breaches (Table 1). The data underscores the necessity of legal oversight in safeguarding blockchain-based enterprises. The absence of clear legal frameworks for identifying and auditing these firms is worrisome. Without such regulations, ensuring user protection and preventing fraud becomes challenging.

Considering the complexities arising from blockchain technology's distinctive characteristics and obstacles, determining the components of a legal audit process for blockchain-based enterprises becomes imperative. Effective legal audits must encompass several critical factors, including validation of smart contracts, compliance with data protection regulations, examination of risk management protocols, and evaluation of operational transparency.

This analysis corroborates previous research findings and illustrates the evolving nature of threats within the blockchain ecosystem. The most financially destructive methods and their categorization demonstrate yearly variations. To effectively counter these attacks, persistent awareness, learning, and adaptive security solutions are essential. The substantial financial losses underscore the importance of thorough legal audits and proactive due diligence to prevent costly incidents and safeguard blockchain ecosystems.

Table 1. The Most Utilized Techniques Leading to the Highest Cumulative Losses, Along with Their Respective Classifications Spanning From 2020 to 2023.

Year	Technique	Classification	Total Loss (in million
2020	Flashloan Price Oracle Attack	Ecosystem	58.10
2021	Access Control Exploit	Protocol	635.20
2022	Private Key Compromised (Unknown Method)	Infrastructure	641.54
2023	Private Key Compromised (Unknown Method)	Infrastructure	231.00

B. Innovations in Blockchain Technology and Business Applications

1. Blockchain and Crypto-Assets

Before delving further, it is essential to comprehend the concept of crypto assets. The term crypto asset stems from the incentive that blockchain validators get after they validate a transaction on the blockchain network.[11] The incentive at that time was a fraction of the coins transacted. Coins represent the native assets of a blockchain and include examples such as Bitcoin, Ethereum, Fantom, Solana, Vexanium, etc. These coins serve as the intrinsic assets or driving forces of their respective blockchains. Permissionless blockchains require such coins to incentivize validators, irrespective of the specific mechanism employed. Conversely, permissioned blockchains, which do not fully adopt blockchain technology, do not necessarily require native assets as they can manage their transaction validation internally.[12]

In blockchain technology, alongside coins, the concept of "tokens" exists. Unlike coins, tokens are not native assets of any blockchain. Their inception followed the recognition of smart contracts within blockchain technology, introduced by the Ethereum blockchain in 2015. Smart contracts enable parties interacting within the blockchain to perform functions beyond simple coin transactions, such as including clauses in each transaction. Consequently, ownership clauses in contracts give rise to tokens, which represent the owned object or right. Both coins and tokens are

[11] Satoshi Nakamoto, “Bitcoin: Sebuah Sistem Uang Tunai Elektronik Peer-to-Peer.”

[12] Rebecca Yang (et.al.), “Public and Private Blockchain in Construction Business Process and Information Integration,” *Automation in Construction* 118 (2020): 103276, https://doi.org/10.1016/j.autcon.2020.103276.

considered crypto assets, as they are derived from blockchain technology, which utilizes cryptographic technology as its foundation. Crypto assets encompass various categories, including the following.

a. Cryptocurrency:[13]
1) Stable coin: USDT, BUSD, FRAX, TUSD, USDC, etc. (It has an underlying asset of a particular national currency).
2) Gold or Silver Backed Tokens: PAX Gold (PAXG), Tether Gold (XAUT) etc. (It has an underlying asset of gold or silver and is treated the same as a stable coin).
3) Unstable coin: Bitcoin, Litecoin, Dogecoin, XRP (It has unstable value and no specific backed asset. The value is determined by acceptance of the currency).

b. Utility token:[14]
1) Profit sharing token: BNB, Kucoin Share (KCS), CRO.
2) New project pre-sale or launchpad or auction participation marks: Cake, BNB, BSW, DOT, SHEESHA, KSM, etc.

c. Security token:
1) Equity based token: APPL https://ftx.com/tokenized-stocks-kyc.
2) Commodity backed token: PTR https://www.petro.gob.ve/en/.
3) Real estate backed token: RealT Token: https://realt.co/marketplace/.

d. Governance token:

As voting rights markers in a project, the more tokens, the stronger the voting rights: CAKE, MDX, MKR, AAVE, dst. https://pancakeswap.finance/voting.

e. Non-Fungible token [15]

It is utilized to uniquely identify digital assets by leveraging Oracle's technology. It can be a "marker" for digital assets such as music, paintings, films, even houses or land:[16]

https://www.moviebloc.com/: MBL Token.
https://audius.co/: AUDIO Token.
https://opensea.io/: World's Largest NFT Market.
https://kolektibel.com/: The first NFT market in Indonesia.
https://realt.co/marketplace/: Token-based real estate ownership.

f. Hybrid Asset:

It spans all types from currency, governance, utility token: Ethereum, Matic, Fantom, Solana, BNB, etc.

[13] Farrukh Habib and Salami Saheed Adekunle, “Case Study of Bitcoin and Its Halal Dimension,” in *Halal Cryptocurrency Management* (ed.) Mohd Ma’Sum Billah (Cham: Springer International Publishing, 2019), 235–55, https://doi.org/10.1007/978-3-030-10749-9_15.

[14] Fernando García-Monleón, Ignacio Danvila-del-Valle, and Francisco J. Lara, “Intrinsic Value in Crypto Currencies,” *Technological Forecasting and Social Change* 162 (2021): 120393, https://doi.org/10.1016/j.techfore.2020.120393.

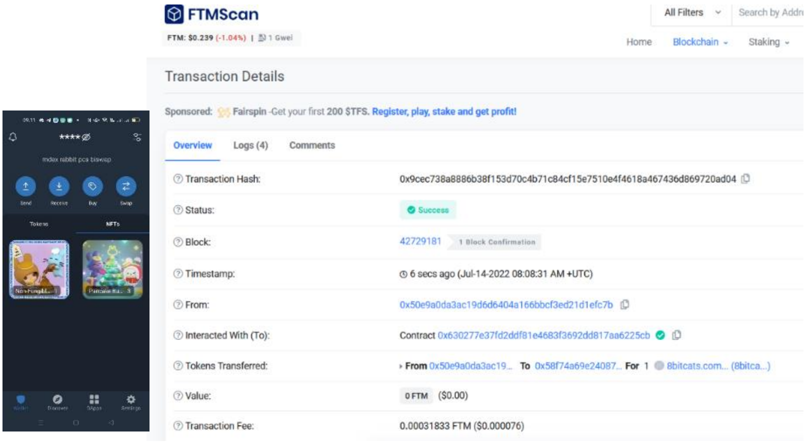
[15] Andrew Guadamuz, “What Do You Actually Own When You Buy an NFT?”accessed on July 14, 2022 https://www.weforum.org/agenda/2022/02/non-fungible-tokens-nfts-and-copyright/.

[16] Mochammad Tanzil Multazam, “Exploring the Legal and Policy Implications of Non-Fungible Tokens,” *Jurnal Politik dan Pemerintahan Daerah* 4, no. 2 (2022): 293–303, https://doi.org/10.36355/jppd.v4i2.58.

Various methods exist for acquiring crypto assets, as outlined in Table 2. Once obtained, these assets are stored in a crypto wallet, which serves as the user's public identifier. Operated by either a provider company or community, the wallet merely facilitates the visualization of blockchain data. The interface of the crypto wallet and the depiction of blockchain data are illustrated in Figure 4.

Table 2. Methods for Acquiring Crypto Assets

1	Mining	1. For cryptocurrencies utilizing Proof of Work (PoW) consensus mechanisms such as Ethereum (ETH), Dogecoin (DOGE), and Bitcoin (BTC), acquisition typically involves either pool mining or solo mining using dedicated hardware. 2. Cryptocurrencies employing Proof of Stake (PoS) mechanisms like Cardano, Solana, and Vexanium, which are evolving as Delegated Proof of Stake (DPoS) systems, are acquired based on the number of coins owned. 3. Cloud mining, an alternative method, entails purchasing hash rate through a platform, eliminating the need for physical hardware.
2	Purchase	1. Cryptocurrencies can also be acquired through Central Exchanges like Tokocrypto, Indodax, and Binance. 2. Cryptocurrencies can also be acquired through Decentralized Exchanges such as SpookySwap, PancakeSwap, and UniSwap. 3. Purchases can occur on a peer-to-peer basis or during Initial Coin Offerings (ICO) or Initial Farm Offerings (IFO), exemplified by PancakeSwap and ParaChain.
3	Free gift	Other methods include airdrops and loyalty bonuses for holders, represented by tokens like KCS, BNB, and CRO.
4	Liquidity Provider	users can engage in providing liquidity for crypto assets through specific pairings on centralized or decentralized exchanges like SpookySwap, UniSwap, and PancakeSwap.
5	Leasing out assets	leasing crypto assets with stable coin rewards is possible through platforms such as https://makerdao.com/en/.
6	Lending assets	Lending crypto assets with the same crypto asset reward is possible through platforms https://geist.finance/, https://app.aave.com/, or https://venus.io/.



Transaction Details

Transaction Hash: 0x9cec738a8886b38f153d70c4b71c84cf15e7510e4f4618a467436d869720ad04

Status: Success

Block: 42729181 1 Block Confirmation

Timestamp: 6 secs ago (Jul-14-2022 08:08:31 AM +UTC)

From: 0x50e9a0da3ac19d6d6404a166bbcf3ed21d1efc7b

Interacted With (To): Contract 0x630277e37fd2ddf81e4683f3692dd817aa6225cb

Tokens Transferred: From 0x50e9a0da3ac19... To 0x58f74a69e24087... For 1 8bitcats.com... (8bitca...)

Value: 0 FTM ($0.00)

Transaction Fee: 0.00031833 FTM ($0.000076)

Figure 4. Crypto Wallet View (Left), Data View on Blockchain (Right)

2. Blockchain-Based Business Patterns

Blockchain technology is anticipated to revolutionize numerous industries, including supply chains, data storage, financial institutions, and capital markets.[17] Current blockchain-based businesses can be divided into several categories as follows:

1. Businesses utilizing Token-Based Blockchain (TBBB).[18] [19]
2. Businesses utilizing blockchain without being token-based.[20]

The majority of blockchain business models that do not utilize tokens operate on a permissioned basis, wherein a single entity or group maintains control over transactions within the blockchain. Consequently, obtaining permission from this entity is necessary to access or view transactions on the blockchain. However, such models may not be particularly beneficial in a consortium setting. The primary objective of the crypto token business model is to digitize real-world assets and transfer them to the digital realm, akin to the operations of numerous contemporary digital companies. Nonetheless, the distinction lies in the database storing the digital assets, with tokens representing the value of tangible assets. These assets may encompass the asset itself or various ownership, voting, service, or profit-sharing rights, as illustrated in Figure 5.

[17] Witold Nowiński and Miklós Kozma, “How Can Blockchain Technology Disrupt the Existing Business Models?” *Entrepreneurial Business and Economics Review* 5, no. 3 (2017): 173–188, https://doi.org/10.15678/EBER.2017.050309.

[18] Hazik Mohamed, “Decentralizing Finance via Cryptocurrencies and Tokenization of Assets and Peer-to-Peer Platforms,” *International Journal of Islamic Economics* 3, no. 1 (2021): 1, https://doi.org/10.32332/ijie.v3i1.3128.

[19] Theo Lynn (et.al.) (ed.), *Disrupting Finance: FinTech and Strategy in the 21st Century* (Cham: Springer International Publishing, 2019), 135, https://doi.org/10.1007/978-3-030-02330-0.

[20] Alain Chong (et.al.), “Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models,” *Journal of the Association for Information Systems* 20, no. 9 (2019): 1310-1328, https://doi.org/10.17705/1jais.00568.

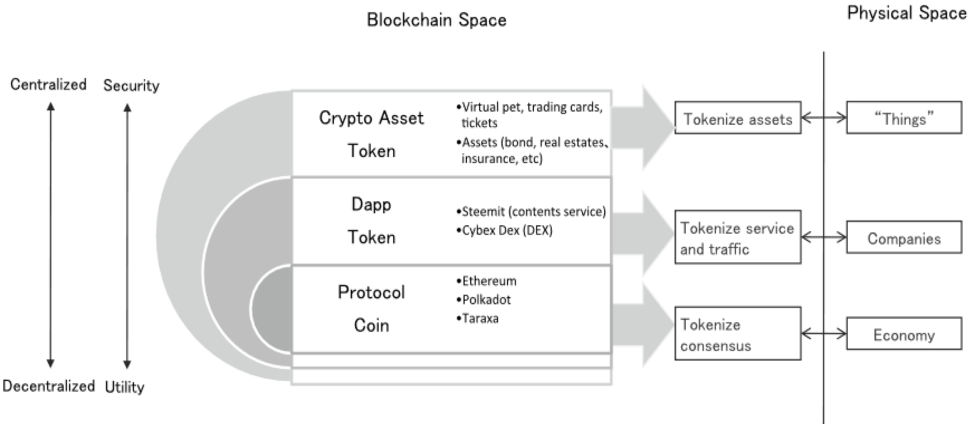


Figure 5. Variety of Current Businesses Utilizing Token-Based Blockchain (TBBB) [21]

The current phase of blockchain-based businesses is regarded as a manifestation of digital business evolution. These businesses emphasize attributes such as autonomy, decentralization, automation, security, and community engagement, reflective of the inherent characteristics of blockchain technology, including decentralization, consensus, transparency, security, and immutability, as depicted in Figure 6.[22]

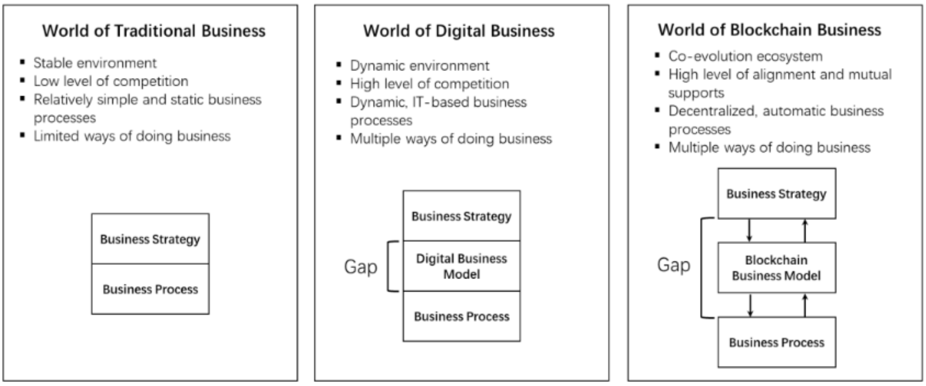

World of Traditional Business
Stable environment
Low level of competition
Relatively simple and static business processes
Limited ways of doing business
Business Strategy
Business Process
World of Digital Business
Dynamic environment
High level of competition
Dynamic, IT-based business processes
Multiple ways of doing business
Business Strategy
Gap
Digital Business Model
Business Process
World of Blockchain Business
Co-evolution ecosystem
High level of alignment and mutual supports
Decentralized, automatic business processes
Multiple ways of doing business
Business Strategy
Gap
Blockchain Business Model
Business Process

Figure 6. Comparison of Blockchain Business Schemes With Others [23] [24]

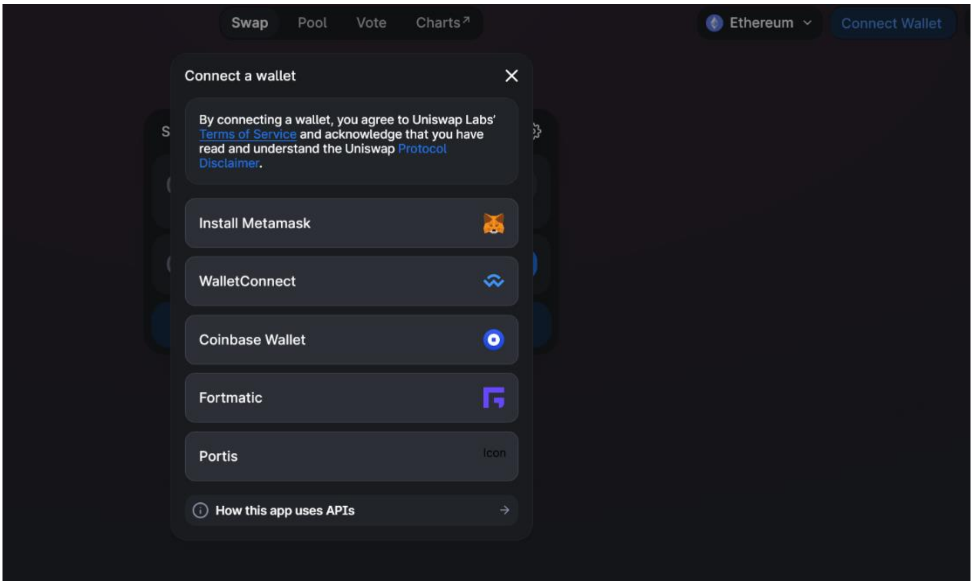
[21] Chris Dai, "DEX: A Dapp for the Decentralized Marketplace," in *Blockchain and Crypto Currency: Building a High Quality Marketplace for Crypto Data*, (ed.) Makoto Yano (et.al.), *Economics, Law, and Institutions in Asia Pacific* (Singapore: Springer, 2020), 95–106, https://doi.org/10.1007/978-981-15-3376-1_6.

[22] Paolo Tasca and Claudio J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification."

[23] Alain Chong (et.al.), "Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models."

[24] Horst Treiblmaier and Roman Beck, (ed.), *Business Transformation through Blockchain: Volume I* (Cham: Springer International Publishing, 2019) 77-120, https://doi.org/10.1007/978-3-319-98911-2.

This attribute has led to the rise of a widespread global peer-to-peer business model. What makes this model intriguing is its departure from conventional localized and nationalized peer-to-peer concepts.[25] Notably, transactions in this model do not necessitate the provision of personal identity information; users merely need to connect their public ID to the designated platform for transactions. This simplicity facilitates usage across diverse demographic groups and geographical regions, as exemplified in Figure 7.



By connecting a wallet, you agree to Uniswap Labs' Terms of Service and acknowledge that you have read and understand the Uniswap Protocol Disclaimer.

Figure 7. The Process of Pooling Public Ids (Crypto Wallets) on Uniswap's DEX Platform[26]

This business model employs tokens as a means of exchange for its services or products. Therefore, high value to tokens is associated with useful or profitable offerings. Since the key to the value of tokens lies in the dynamics of the service and product, the key considerations include the following questions.[27]

1. What is the track record of the team that runs the service or produces the product? Is this the first product or service they have managed? (people)
2. What uniqueness is offered? What is the latest technology created (because this is a tech industry, it is natural that the technology point also needs to be questioned)? (tech)

[25] Steven Kane Curtis, "Business Model Patterns in the Sharing Economy," *Sustainable Production and Consumption* 27 (2021): 1650–1671, https://doi.org/10.1016/j.spc.2021.04.009.

[26] Uniswap, "Uniswap Interface," accessed on July 14, 2022, https://app.uniswap.org/#/swap?chain=mainnet.

[27] Mochammad Tanzil Multazam (et.al.), "Is It Legal to Provide Liquidity on the Vexanium Decentralized Exchange in Indonesia?" *Yustisia Jurnal Hukum* 12, no. 1 (2023): 29, https://doi.org/10.20961/yustisia.v12i1.69007.

3. Does this business have a clear roadmap? Has the roadmap been implemented on time? Have the products and services been developed over the years and in the future? (development)
4. Do these products and services have competitors? What is the advantage of this product and service over competitors? (market)

These factors are crucial as they influence supply and demand dynamics, with utility directly impacting demand, as outlined in Table 3.

Table 3. Usefulness of Tokens as an Asset and as a Powerful Tool

Token as an Asset	Tokens as an Empowering Tool
3. Used as a marker of asset ownership in the real world. Example: a. The purchase of a RealT Token is proof of partial ownership of a whole house in the United States. The house is then rented out, and we get a share of the rent according to our token ownership.[28]	1. Used to vote on the DAO (decentralized autonomous Org) token or coin. 2. Used as a legitimized identity following an ICO or IFO release of a new product.[31] 3. Used to upgrade in-game abilities.
b. Purchasing APPL tokens is proof of ownership of apple shares.[29]	4. Used to raise funds for project development, funders get a share if the project is already running.
4. Used as a marker of ownership for digital assets recorded on the Blockchain (NFT).[30]	5. Used to get a share of the platform's profits. Example: a. Geist tokens: Geist token holders can share in the profits of a digital savings and loan platform running on the Fantom blockchain.[32] b. KCS tokens: KCS token holders get a revenue share of all total income of the trade-based KuCoin Exchanger platform.[33] c. BNB tokens get an airdrop only every time a new token or coin is listed on Binance via launchpad.

[28] RealIT. Inc, “RealT, Inc.,” accessed on April 27, 2019, https://realt.co/.

[29] Trust Wallet, “How to Invest in Tokenized Stocks Using Trust Wallet,” accessed on July 17, 2022, https://trustwallet.com/blog/how-to-invest-in-tokenized-stocks.

[30] Moringiello, Juliet M. and Odinet, Christopher K., “The Property Law of Tokens,” *Florida Law Review* 607 (2022): 74, http://dx.doi.org/10.2139/ssrn.3928901.

[31] Parachains.info, “Polkadot & Kusama Ecosystem Projects Directory,” accessed on July 14, 2022, https://parachains.info/; “Initial Farm Offering | PancakeSwap,” accessed on July 17, 2022, https://pancakeswap.finance/ifo.

[32] GEIST, “GEIST Token,” accessed on July 17, 2022, https://docs.geist.finance/.

[33] KuCoin, “Earn Crypto with High APY | KuCoin,” accessed on July 17, 2022, https://www.kucoin.com/earn.

	6. Used to obtain services or goods Example: a. Purchases of in platform items on the Decentraland platform can only be made using MANA tokens. b. Use of document file storage services on the filecoin platform using FIL tokens only.

These types of businesses can be categorized into four types as follows:[34]

a. DEFI stands for decentralized finance. It is a business with services similar to banking, but run on a community basis rather than a centralized system that include the following.

1) Exchanger: A business that exchanges crypto assets, earning administrative fees in the form of crypto assets for each transaction.
2) Providing liquidity for exchangers, known as farming, results in administrative fee revenue shares for each transaction made in a specific pair (e.g., BTC-ETH pair).
3) Loan provider. This business's crypto asset loan provider will receive an interest profit share from the borrower's loan. The borrower must pledge crypto assets on the platform to get a loan. Borrowers must also lend. Platform bonuses are sometimes given to borrowers for borrowing. Many name this service lend-and-borrow.
4) Yield aggregator. This automates farming so liquidity suppliers do not have to claim the yield share every time to invest (compounding). A performance or withdrawal charge of a percentage of yield share or total liquidity benefits the platform.

The four are the most popular services in DEFI's business. Other services are collateralized debt, reserve currency, payment, insurance, algo-stables, synthetics, bridge, liquid stacking, etc.

b. NFT Marketplace: NFT purchases on this platform use tokens from businesses. Thus, the token functions as a medium of exchange. Revenue from administrative fees every time a trade transaction is made.

c. Protocol: this business focuses on developing new technology that can later be used by other business platforms. The source of income for business actors depends on the protocol usage agreement.

d. Games: online games that are integrated with blockchain. Tokens from businesses are used as the main medium of exchange for playing or as prizes. Profits are obtained from fees for playing the game or administrative fees for each transaction to purchase tools to play games.

[34] Mochammad Tanzil Multazam, "Unleashing the Potential of DeFi: A Comprehensive Guide to Maximizing Rewards While Mitigating Risks," *Ganaya: Jurnal Ilmu Sosial dan Humaniora* 4, no. 2 (2021): 906–918.

Based on this, this study tries to map the current TBBB competition map. The Data collection from the five highest-volume ventures on the Ethereum blockchain,[35] Binance Smart Chain,[36] and Fantom.[37] The collected data will be presented in Table 4.

Table 4 illustrates that the predominant focus of the platform's business lies within the DEFI sector. DEFI regulations differ from traditional finance, primarily because there is no intermediary involved; instead, a technology provider facilitates the protocols necessary for the service to function.[38] DEXs (Decentralized Exchanges) operate without stringent KYC/AML (Know Your Customer/Anti-Money Laundering) regulations, although they remain susceptible to regulatory oversights and inadequate record-keeping practices.

Table 4. TBBB's Current Competition Map

Business Name	Product/Service						
	Blockchain						
	Ethereum	BSC	Fantom	DEFI	NFT Marketplace	Protocols	Games
Uniswap	x			x			
Curve	x		x	x			
CowSwap	x			x			
OxProtocol	x					x	
Compound	x		x	x			
PancakeSwap		x		x	x		x
BiSwap		x		x	x		x
Venus		x		x			
Alpaca		x	x	x			
Celer Network	x		x			x	
Geist			x	x			
SpookySwap			x	x			
BeethovenX			x	x			
1Inch Network	x	x	x	x			
Total	7	5	9	12	2	2	2

[35] DappRadar, "Top Ethereum Dapps," accessed on July 17, 2022, https://dappradar.com/rankings/protocol/ethereum.

[36] DappRadar, "Top BNB Chain Dapps," accessed on July 17, 2022, https://dappradar.com/rankings/protocol/binance-smart-chain.

[37] DappRadar, "Top Fantom Dapps," accessed on July 17, 2022, https://dappradar.com/rankings/protocol/fantom.

[38] Caroline A. Crenshaw, "Statement on DeFi Risks, Regulations, and Opportunities," accessed on July 17, 2022, https://www.sec.gov/news/statement/crenshaw-defi-20211109.

Both the private and public sectors play pivotal roles in combating illicit transactions within the blockchain ecosystem. Private sector initiatives involve strengthening due diligence procedures, expanding educational outreach efforts, and promoting collaboration and information exchange. Strengthened due diligence practices enable businesses to identify and mitigate risks associated with blockchain transactions effectively. Educational campaigns empower users with essential knowledge to recognize potential threats. Additionally, collaborative efforts and information sharing among stakeholders help to stay updated on emerging hacking trends and techniques, thereby enhancing defensive strategies.[39]

Concurrently, the public sector can establish regulatory frameworks to delineate the legal ramifications of blockchain transactions, particularly those related to TBBB. Additionally, fostering effective cooperation among law enforcement agencies is essential for swiftly addressing and remedying illicit transactions. Public awareness initiatives could also play a significant role in educating the broader population about the complexities of blockchain transactions and the associated risks. However, there remains a conspicuous absence of specific regulations governing transactions within the blockchain ecosystem, particularly those involving TBBB, thereby fostering an environment perceived as lacking in regulation.[40]

To address this issue, users need to possess the capacity to conduct thorough due diligence, which includes legal due diligence. This comprehensive approach, involving collaboration between the private and public sectors, plays a pivotal role in thwarting illicit transactions, ensuring a secure environment for blockchain users, and upholding the integrity of the blockchain ecosystem.

Therefore, preventing illicit transactions in blockchain requires a collective endeavor from all stakeholders, providing a robust defense against potential vulnerabilities and promoting an environment conducive to growth and innovation. Due to its global nature and rapid evolution, the World Economic Forum has released the DEFI Policymaker Toolkit to assist policymakers and regulators in navigating the complexities of decentralized finance and formulating appropriate responses.[41]

C. Legal Due Diligence in Blockchain Transactions: Mitigating Risks and Ensuring Transparency

1. Legal Due Diligence Against Blockchain Hacks and Vulnerabilities

Legal due diligence, originating from the Anglo-Saxon legal doctrine of “caveat emptor” or “let the buyer beware,” lacks a universally acknowledged standard beyond the guidelines set forth by Capital Market Legal Consultants. This principle

[39] Mohong Liu, “Research on Legal Regulations of Blockchain,” *Advances in Social Behavior Research* ASBR 1 (2021): 33–40, https://doi.org/10.54254/asbr.2021005.

[40] Wahyu Yun Santoso (et.al.), “Governing Blockchain-Based Token in Indonesia: Legal and Technical Perspective,” *Brawijaya Law Journal* 7, no. 1 (2020): 108–128, https://doi.org/10.21776/ub.blj.2020.007.01.08.

[41] Aylin Elci, “Decentralized Finance Heats up: New Approaches Needed for Industry Transformation,” accessed on July 17, 2022, https://www.weforum.org/press/2021/06/decentralized-finance-could-improve-the-industry-but-new-approaches-to-regulation-are-needed/.

emphasizes the importance of prospective buyers conducting extensive investigations before completing a transaction.[42] The purpose of this due diligence procedure is to guarantee that buyers are well-informed and cautious, thereby protecting their interests.

Nevertheless, the principle of "caveat venditor" or "let the seller beware" is also relevant. This principle encourages the seller to perform their own due diligence when seeking qualified buyers for their assets. This dynamic establishes a mutually beneficial relationship between buyers and sellers, promoting trust through transparency. In this context, the terms "buyer" and "seller" can refer to any parties making critical decisions and underscores the importance of due diligence in their decision-making processes.[43]

Furthermore, due diligence serves a primary purpose, which is to mitigate risk.[44] The initial step in this procedure involves reviewing the legal records of the target company. These documents encompass establishment records detailing the company's structure and partners, licenses or permits obtained (such as those for labor, services, or specific business activities), assets including tangible and intangible assets, land ownership records indicating ownership proof, pledged land, or relevant agreement clauses, ongoing or current court cases, and existing agreements.[45]

In the analysis, consideration must be given to various theories of corporate law, including the *Business Judgment Rule, Corporate Governance, Piercing the Corporate Veil, Ultra Vires,* and *Fiduciary Duty*. These theories are utilized to assess the compliance of the target company with legal regulations and its absence of potential legal liabilities. Consequently, the legal due diligence process aims to evaluate the value of a business by scrutinizing data from corporate contracts, assets, and identifying any potential future issues. The characteristics of TBBB, such as being paperless, borderless, open-source, decentralized, and transparent, underscore its revolutionary nature,[46] aligning with the decentralized and transparent principles of blockchain technology.

The categorization of hacks encompasses five main types: Ecosystem, Infrastructure, Protocol Logic, Rugpull, and Smart Contract Language. Any platform may be susceptible to these categories of hacks. Legal due diligence is essential to prepare for such incidents, particularly in anticipating vulnerabilities in protocol logic and infrastructure, which have incurred the highest number of victims from 2020 to 2023.

[42] Peter Howson, *Due Diligence: The Critical Stage in Mergers and Acquisitions* (England: Taylor & Francis, 2017), 15.

[43] Melissa E. Graebner, "Caveat Venditor: Trust Asymmetries in Acquisitions of Entrepreneurial Firms," *Academy of Management Journal* 52, no. 3 (2009): 435–472, https://doi.org/10.5465/amj.2009.41330413.

[44] H. Krieger, A. Peters, and L. Kreuzer, *Due Diligence in the International Legal Order* (UK: OUP Oxford, 2020), 35.

[45] Peter Howson, *Checklists for Due Diligence* (UK: Routledge, 2017), 24.

[46] Iris H.-Y. Chiu, *Regulating the Crypto Economy: Business Transformations and Financialisation* (UK: Bloomsbury Publishing, 2021), 96.

- Ecosystem Hack: this type of hack occurs when the broader environment of a blockchain network is targeted. It can involve manipulating system interfaces, exploiting vulnerabilities in third-party integrations, or attacking the consensus mechanism.
- Infrastructure Hack: this type of hack targets the underlying hardware and software systems that support a blockchain network. Examples include server attacks, Distributed Denial of Service (DDoS) attacks, and other forms of cyber-attacks that compromise the blockchain's operational infrastructure.
- Protocol Logic Hack: this type of hack involves exploiting the rules and operations defined in the blockchain protocol itself. For instance, manipulating transaction ordering, block rewards, or consensus mechanisms to gain an unfair advantage.
- Rugpull: in the context of Decentralized Finance (DeFi), a Rugpull is a scam where developers abandon a project and run off with investors' funds. This is often facilitated by holding a significant amount of the project's tokens, which are then sold, causing the token price to crash.
- Smart Contract Language Hack: it exploits vulnerabilities in the programming languages used to write smart contracts. Examples include reentrancy attacks, where a function can be recursively called before the first function call is finished, leading to unintended behavior.

Legal due diligence plays a crucial role in preventing various types of blockchain hacks by posing pertinent questions aimed at understanding and mitigating potential vulnerabilities. These questions are rooted in a fundamental comprehension of the different categories of blockchain hacks, including Ecosystem, Infrastructure, Protocol Logic, Rugpull, and Smart Contract Language. By addressing these questions, stakeholders can proactively safeguard against potential threats to blockchain systems.

a. What Measures are Taken to Ensure the Security of the Ecosystem and Infrastructure?

Inquiring about the measures implemented to safeguard the ecosystem and infrastructure aims to ascertain the entity's strategies for defending against potential attacks targeting the broader system environment and the underlying hardware and software. Understanding these measures is essential for preventing ecosystem and infrastructure hacks.

b. How is the Protocol Logic Designed to Prevent Exploitations?

Assessing the design of the protocol logic aims to determine how effectively the entity's blockchain protocol is structured to thwart manipulations of its rules and operations. Given the severity of Protocol Logic hacks, understanding the preventive measures in place is critical.

c. What Safeguards are in Place to Prevent a Rugpull Scenario?

Examining the safeguards against Rugpull scenarios is crucial due to the significant financial losses and adverse effects on investor confidence that can arise from such incidents. Understanding the measures in place to prevent developers from absconding with funds is essential.

D. How are Smart Contracts Tested and Audited to Ensure They are Free from Vulnerabilities?

Investigating the testing and auditing procedures for smart contracts is necessary to ensure their integrity and identify vulnerabilities. Smart contracts, being fundamental to blockchain transactions and applications, require thorough evaluation to mitigate risks associated with Smart Contract Language vulnerabilities. Our questions to prevent hacks in the ecosystem, infrastructure, protocol logic, Rugpull, and smart contract language are related to legal due diligence on TBBB as follows.

1. Legal Framework of the Jurisdiction Where the Platform is Located

Despite its borderless nature, TBBB platforms are typically hosted on websites registered within a specific country. According to the principle of website jurisdiction, the country associated with the website can enforce laws related to cybercrimes occurring through that platform. Initial checks can be conducted using website verification platforms like ICANN to determine the country of registration.

2. Legal Framework That Supports the Platform

Examining the legal framework supporting the platform involves reviewing documents such as whitepapers, work plans, or operational schematics provided by TBBB. These documents, often accessible through links like https://docs.pancakeswap.finance/, offer insights into various aspects of the platform's operations. Key considerations include the regulatory compliance outlined in these documents, along with other pertinent information regarding the platform's functioning.

1. Who has access to the main smart contracts of the platform? Example: https://docs.geist.finance/useful-info/timelock.
2. How long does it take for changes to be made to the smart contract after a developer has made changes (timelock)? Example: https://docs.geist.finance/useful-info/timelock.
3. Is the liquidity of the token guaranteed?
4. Who can be the decider of policy changes on the platform, is there a DAO scheme supported by users? Example: https://pancakeswap.finance/voting.
5. Are the smart contracts used secure?

3. Platform's Terms and Conditions

In any typical business transaction, the contract serves as a fundamental element ensuring smooth operations and protecting the interests of all involved parties. Within TBBB, smart contracts hold a significant role. However, vulnerabilities in smart contract security, indicating weaknesses in their code.[47] They pose risks that can be exploited by hackers or malicious entities. Examples of such vulnerabilities include reentrancy vulnerabilities, where attackers can repeatedly invoke contract functions to deplete funds, and integer overflows and underflows, which enable the manipulation of variables to behave unexpectedly.

1) Reentrancy vulnerabilities permit attackers to repeatedly call contract functions, depleting their funds. Such weaknesses have facilitated token theft,[48] resulting in significant financial losses. Detection methods for reentrancy attacks include fuzz testing and a novel tool known as ReDefender.[49]
2) Integer overflows and underflows enable attackers to manipulate contract variables,[50] causing unexpected behavior. These vulnerabilities arise when values exceed maximum limits or become too small to fit into variables, leading to potential exploits. Initializing variables with the "long-long" data type can mitigate this risk.[51]
3) Unchecked return values allow attackers to manipulate contract behavior by providing malicious input, posing a significant security risk.[52]
4) Unprotected functions expose vulnerabilities that enable attackers to invoke internal contract functions, potentially accessing sensitive data or altering behavior.[53]
5) Uninitialized storage variables previously allowed attackers to access sensitive data stored within contract storage. However, Solidity version 0.5.0 addressed this issue, eliminating this vulnerability.[54]

[47] Roberto Infante, *Building Ethereum Dapps: Decentralized Applications on the Ethereum Blockchain* (New York: Simon and Schuster, 2019) 302-400.

[48] Redfox, "Reentrancy Attacks in Smart Contracts - Redfox Security," accessed on December 13, 2022, https://redfoxsec.com/blog/reentrancy-attacks-in-smart-contracts/.

[49] Bixin Li, Zhenyu Pan, and Tianyuan Hu, "ReDefender: Detecting Reentrancy Vulnerabilities in Smart Contracts Automatically," *IEEE Transactions on Reliability* 71, no. 2 (2022): 984–999, https://doi.org/10.1109/TR.2022.3161634.

[50] Infosec Resources, "What is Integer Overflow and Underflow?" accessed on December 13, 2022, https://resources.infosecinstitute.com/topic/what-is-is-integer-overflow-and-underflow/.

[51] Infosec Resources.

[52] Vijaya Bhaskar, "Unchecked Return Value in Smart Contracts as an Attack Surface," accessed on 21, 2022, https://coinsbench.com/unchecked-return-value-in-smart-contracts-providing-an-attack-surface dab2eed64251.

[53] Kadenzipfel, "Smart-Contract-Attack-Vectors/Unprotected-Callback.Md at Master · Kadenzipfel/Smart-Contract-Attack-Vectors," accessed on December 13, 2022, https://github.com/kadenzipfel/smart-contract-attack-vectors.

[54] Kadenzipfel, "Smart-Contract-Attack-Vectors/Uninitialized-Storage-Pointer.Md at Master · Kadenzipfel/Smart-Contract-Attack-Vectors," accessed on December 13, 2022, https://github.com/kadenzipfel/smart-contract-attack-vectors.

Thoroughly examining smart contract code is imperative to identify and rectify potential security vulnerabilities. Developers frequently engage auditing organizations like Hacken, CertiK, Slowmist, PeckShield, and OpenZeppelin to assess their smart contracts. Users within TBBB often refer to the audit reports provided by these organizations to evaluate smart contracts, typically available on the developer's website, such as https://docs.pancakeswap.finance/#is-pancakeswap-safe. Additionally, users can conduct self-checks using platforms like https://defillama.com.

4. Platform's Compliance with Applicable Laws and Regulations

Determining the jurisdiction of the website registration serves as the initial step in verifying the platform's compliance with legal regulations. Presently, there exists a dearth of adequate legal frameworks globally to govern TBBB operations. However, an initial precaution entails ensuring that the TBBB concept, smart contracts, content, and digital assets adhere to intellectual property rights. Frequently, TBBB concepts or smart contracts are derived from existing models, such as PancakeSwap (a UniSwap fork), Geist (a fork of Aave), Scream (a Compound fork), among others, facilitated by the open-source nature of the code. Although open-source, the usage of code is subject to licensing or usage restrictions mandated by each project. Example: https://github.com/aave.[55]

5. Any Possible Risks or Legal Issues Faced by Platform

TBBB platforms are susceptible to various legal risks and challenges due to their decentralized nature and absence of clear regulatory frameworks. Some possible risks or legal issues that the TBBB platform may face as follows.

1. The anonymity and decentralized nature of TBBB platforms can lead to disagreements with users about fund loss, fraud, or technical concerns. Platforms should provide clear and fair dispute resolution and transparent information delivery to reduce this risk.
2. Despite the lack of strong regulation, regulators worldwide are increasingly focusing on TBBB operations and may take legal action against platforms that violate the law. Platforms should follow laws and regulations, obtain licenses and permissions, and work with regulators to reduce this risk.
3. The quick and anonymous transmission of payments on TBBB may lead to criminal activities like money laundering or terrorist funding. TBBB platforms should have strong AML and KYC standards to verify users and report questionable transactions to reduce this risk.

[55] Open Source Initiative, "Licenses & Standards | Open Source Initiative," accessed on December 24, 2022, https://opensource.org/licenses.

4. TBBBs may be forks of open-source systems. Use of such code must conform with licenses and use limitations. The owners of copyrights and trademarks may sue TBBB platforms for infringement.
5. TBBB systems provide greater anonymity than centralized platforms, they may nonetheless face legal difficulties with user data privacy. Platforms should have clear privacy rules and follow local data protection regulations to reduce this danger.

In light of these possible legal risks and concerns, it becomes crucial for the TBBB platform to implement preventive measures and uphold compliance with relevant laws and regulations. Therefore, conducting comprehensive legal due diligence is paramount for the TBBB platform to proactively identify and mitigate potential legal issues before they escalate. The legal due diligence process should encompass several key components that include:

1) Consultation with legal experts who have knowledge and experience in TBBB and relevant laws to help identify and address potential legal risks;
2) Conducting a thorough review of the platform's terms and conditions of use, privacy policy and other legal documents to ensure compliance with applicable laws;
3) Ensuring that the TBBB platform has obtained the necessary licenses or permits to operate in relevant jurisdictions;
4) Working with security auditors and testing agencies to test smart contract code and identify and address security vulnerabilities; and
5) Establishing a clear and fair dispute resolution mechanism to address potential disputes with users.

By adhering to these steps, the TBBB platform can mitigate legal risks and ensure adherence to relevant laws and regulations. In addition, a robust legal due diligence process will foster trusts among users and investors that eventually facilitate the TBBB platform to develop sustainably and successfully in an increasingly regulated environment.

E. Conclusion

The proliferation of TBBB presents both opportunities and challenges for legal due diligence. Research has identified five main areas of TBBB hacks: Ecosystem, Infrastructure, Protocol Logic, Rugpull, and Smart Contract Language. Notably, Infrastructure vulnerabilities, particularly through Private Key Compromise, resulted in the highest financial losses exceeding $800 million from 2020 to July 26, 2023. These vulnerabilities underscore the critical need for comprehensive legal due diligence to mitigate risks associated with TBBB platforms. Such due diligence should encompass thorough assessments of the legal framework governing the jurisdiction where the platform operates. Understanding the regulatory environment is crucial for ensuring compliance and managing legal risks effectively. Additionally, evaluating the legal underpinnings of the platform itself is essential. This involves scrutinizing the terms and conditions of platform usage, including user agreements and privacy policies, to identify any potential legal pitfalls or liabilities. By conducting a comprehensive analysis, TBBB platforms can proactively address legal challenges and safeguard the interests of all stakeholders.

Furthermore, given the dynamic nature of blockchain technology, ongoing monitoring and adaptation are imperative. Therefore, further investigation is warranted to assess current legal due diligence practices and develop proactive strategies to address the unique challenges posed by blockchain technology. This may involve refining existing frameworks and methodologies to better align with the evolving landscape of TBBB. Integrating these procedures into the legal audit process is essential to ensure the resilience and longevity of blockchain-powered organizations. By institutionalizing robust legal due diligence practices, TBBB platforms can enhance trust and confidence among users, investors, and regulators alike. Ultimately, these efforts are crucial for fostering a regulatory-compliant and sustainable ecosystem that promotes innovation while mitigating legal risks effectively.

References

Books

Chiu, Iris H.-Y. *Regulating the Crypto Economy: Business Transformations and Financialisation*. UK: Bloomsbury Publishing, 2021.

Dai, Chris. "DEX: A Dapp for the Decentralized Marketplace." In *Blockchain and Crypto Currency: Building a High-Quality Marketplace for Crypto Data*, Makoto Yano, Chris Dai, Kenichi Masuda, and Yoshio Kishimoto (ed.) *Economics, Law, and Institutions in Asia Pacific*. Singapore: Springer, 2020.

Fadhillah, Yusra (et.al.) *Teknologi Blockchain dan Implementasinya*. Medan: Yayasan Kita Menulis, 2022.

Habib, Farrukh and Salami Saheed Adekunle. "Case Study of Bitcoin and Its Halal Dimension." In *Halal Cryptocurrency Management*, Mohd Ma'Sum Billah (ed.) Cham: Springer International Publishing, 2019.

Howson, Peter. *Checklists for Due Diligence*. United Kingdom: Routledge, 2017.

____________. *Due Diligence: The Critical Stage in Mergers and Acquisitions*. United Kingdom: Taylor & Francis, 2017.

Infante, Roberto. *Building Ethereum Dapps: Decentralized Applications on the Ethereum Blockchain*. New York: Simon and Schuster, 2019.

Krieger, H., A. Peters, and L. Kreuzer. *Due Diligence in the International Legal Order*. UK: OUP Oxford, 2020.

Lynn, Theo, John G. Mooney, Pierangelo Rosati, and Mark Cummins (ed.) *Disrupting Finance: FinTech and Strategy in the 21st Century*. Cham: Springer International Publishing, 2019.

Treiblmaier, Horst and Roman Beck (ed.) *Business Transformation Through Blockchain: Volume I*. Cham: Springer International Publishing, 2019.

Other Documents

A. Crenshaw, Caroline. “Statement on DeFi Risks, Regulations, and Opportunities.” Accessed on July 17, 2022**,** https://www.sec.gov/news/statement/crenshaw-defi-20211109.

Anghelache, Constantin, Mădălina-Gabriela Anghel, Gabriel Ștefan Dumbravă, and Daniel Dumitru. “Perspectives of the Development of World Economy in the Blockchain Conditions and Big Data.” *Proceedings of the International Conference on Applied Statistics* 1, no. 1 (2019): 44–59. https://doi.org/10.2478/icas-2019-0005.

Bhaskar, Vijaya. “Unchecked Return Value in Smart Contracts as an Attack Surface.” Accessed on February 21, 2022. https://coinsbench.com/unchecked-return-value-in-smart-contracts-providing-an-attack-surface-dab2eed64251.

Chauhan, Harsh Singh and Jagjeet Jena. “Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets.” *International Journal of Trend in Scientific Research and Development* (2021): 42-54.

Chong, Alain, Eric Lim, Xiuping Hua, Shuning Zheng, and Chee-Wee Tan. “Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models.” *Journal of the Association for Information Systems* 20, no. 9 (2019): 1310-1339, https://doi.org/10.17705/1jais.00568.

Coinmarketcap, Chart. “Total Cryptocurrency Market Cap.” Accessed on December 28, 2021**.** https://coinmarketcap.com/charts/.

Curtis, Steven Kane. “Business Model Patterns in the Sharing Economy.” *Sustainable Production and Consumption* 27 (2021): 1650–1671. https://doi.org/10.1016/j.spc.2021.04.009.

DappRadar. “Top BNB Chain Dapps.” Accessed on July 17, 2022. https://dappradar.com/rankings/protocol/binance-smart-chain.

_________. “Top Ethereum Dapps.” Accessed on July 17, 2022. https://dappradar.com/rankings/protocol/ethereum.

_________. “Top Fantom Dapps.” Accessed on July 17, 2022. https://dappradar.com/rankings/protocol/fantom.

Defillama Defillama, “Total Hacks Value." Accessed on December 13, 2022. https://defillama.com/hacks.

Elci, Aylin. “Decentralized Finance Heats up: New Approaches Needed for Industry Transformation.” Accessed on July 17, 2022. https://www.weforum.org/press/2021/06/decentralized-financecouldimprove-the-industry-but-new-approaches-to-regulation-are-needed/.

García-Monleón, Fernando, Ignacio Danvila-del-Valle, and Francisco J. Lara. “Intrinsic Value in Crypto Currencies.” *Technological Forecasting and Social Change* 162 (2021): 1-9. https://doi.org/10.1016/j.techfore.2020.120393.

Graebner, Melissa E. “Caveat Venditor: Trust Asymmetries in Acquisitions of Entrepreneurial Firms.” *Academy of Management Journal* 52, no. 3 (2009): 435–472. https://doi.org/10.5465/amj.2009.41330413.

Guadamuz, Andrew. “What Do You Actually Own When You Buy an NFT?” Accessed on July 14, 2022**.** https://www.weforum.org/agenda/2022/02/non-fungible-tokens-nfts-and-copyright/.

Infosec Resources. “What is Integer Overflow and Underflow?” Accessed on December 13, 2022. https://resources.infosecinstitute.com/topic/what-is-is-integer-overflow-and-underflow/.

Kadenzipfel. “Smart-Contract-Attack-Vectors/Uninitialized-Storage-Pointer.Md at Master · Kadenzipfel/Smart-Contract-Attack-Vectors.” Accessed on December 13, 2022. https://github.com/kadenzipfel/smart-contract-attack-vectors.

Karimov, Bedil and Piotr Wójcik. “Identification of Scams in Initial Coin Offerings With Machine Learning.” *Frontiers in Artificial Intelligence* 4 (2021): 1-16. https://doi.org/10.3389/frai.2021.718450.

Leonhard, Robert Donald. “Decentralized Finance on the Ethereum Blockchain.” *SSRN Electronic Journal* (2019): 1-22. https://doi.org/10.2139/ssrn.3359732.

Li, Bixin, Zhenyu Pan, and Tianyuan Hu. “ReDefender: Detecting Reentrancy Vulnerabilities in Smart Contracts Automatically.” *IEEE Transactions on Reliability* 71, no. 2 (2022): 984–999. https://doi.org/10.1109/TR.2022.3161634.

Liu, Mohong. “Research on Legal Regulations of Blockchain.” *Advances in Social Behavior Research ASBR* 1 (2021): 33–40. https://doi.org/10.54254/asbr.2021005.

Mohamed, Hazik. “Decentralizing Finance via Cryptocurrencies and Tokenization of Assets and Peer-to-Peer Platforms.” *International Journal of Islamic Economics* 3, no. 1 (2021): 1-15. https://doi.org/10.32332/ijie.v3i1.3128.

Moringiello, Juliet M. and Odinet, Christopher K. “The Property Law of Tokens.” *Florida Law Review* 607 (2022): 607-671. http://dx.doi.org/10.2139/ssrn.3928901.

Multazam, Mochammad Tanzil. “Exploring the Legal and Policy Implications of Non-Fungible Tokens.” *Jurnal Politik Dan Pemerintahan Daerah* 4, no. 2 (2022): 293–303. https://doi.org/10.36355/jppd.v4i2.58.

__________________________. “Unleashing the Potential of DeFi: A Comprehensive Guide to Maximizing Rewards While Mitigating Risks.” *Ganaya: Jurnal Ilmu Sosial Dan Humaniora* 4, no. 2 (2021): 906–918.

__________________________. “Protocol Hack in Cryptoworld.” Accessed on July 26, 2023. https://doi.org/10.5281/zenodo.8185509**.**

Multazam, Mochammad Tanzil, Regita Amanah Huzairin, Sandika Putra Pratama, and Irwansyah Irwansyah. “Is It Legal to Provide Liquidity on the Vexanium Decentralized Exchange in Indonesia?” *Yustisia Jurnal Hukum* 12, no. 1 (2023): 29–46. https://doi.org/10.20961/yustisia.v12i1.69007.

Nakamoto, Satoshi. “Bitcoin: Sebuah Sistem Uang Tunai Elektronik Peer-to-Peer.” Accessed on July 14, 2022**.** https://bitcoin.org/bitcoin.pdf.

Nowiński, Witold and Miklós Kozma. “How Can Blockchain Technology Disrupt the Existing Business Models?” *Entrepreneurial Business and Economics Review* 5, no. 3 (2017): 173–188. https://doi.org/10.15678/EBER.2017.050309.

Open Source Initiative. “Licenses & Standards | Open-Source Initiative.” Accessed on December 24, 2022. https://opensource.org/licenses.

Redfox Security. “Reentrancy Attacks in Smart Contracts - Redfox Security.” Accessed on December 13, 2022. https://redfoxsec.com/blog/reentrancy-attacks-in-smart-contracts/.

Santoso, Wahyu Yun (et.al.) “Governing Blockchain-Based Token in Indonesia: Legal and Technical Perspective.” *Brawijaya Law Journal* 7, no. 1 (2020): 108–128. https://doi.org/10.21776/ub.blj.2020.007.01.08.

Tasca, Paolo, and Claudio J. Tessone. “A Taxonomy of Blockchain Technologies: Principles of Identification and Classification.” *Ledger* 4 (2019): 1–39. https://doi.org/10.5195/ledger.2019.140.

Tauda, Gunawan A, Andy Omara, and Gioia Arnone. “Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union.” *BESTUUR* 11, no. 1 (2023): 1–25. https://doi.org/10.20961/bestuur.v11i1.67125.

Uniswap. “Uniswap Interface.” Accessed on July 14, 2022. https://app.uniswap.org/#/swap?chain=mainnet.

Yang, Rebecca (et.al.) “Public and Private Blockchain in Construction Business Process and Information Integration.” *Automation in Construction* 118 (2020): 103276. https://doi.org/10.1016/j.autcon.2020.103276.