IEEE Open Journal of the
Computer Society

Received 4 January 2023; accepted 9 February 2023. Date of publication 16 February 2023;
date of current version 2 March 2023. The review of this paper was arranged by Associate Editor Deze Zeng.

Digital Object Identifier 10.1109/OJCS.2023.3245801

Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities

JIAJING WU [1] **(Senior Member, IEEE), KAIXIN LIN** [1]**, DAN LIN** [2] **(Graduate Student Member, IEEE), ZIYE ZHENG** [1,3]**, HUAWEI HUANG** [2] **(Senior Member, IEEE), AND ZIBIN ZHENG** [2] **(Fellow, IEEE)**

[1] School of Computer Science and Engineering, Sun Yat-Sen University, Guangzhou 510275, China
[2] School of Software Engineering, Sun Yat-Sen University, 510275 Guangzhou, China
[3] School of Software Engineering, South China Normal University, Foshan 510275, China

CORRESPONDING AUTHOR: ZIBIN ZHENG (e-mail: zhzibin@mail.sysu.edu.cn).

This work was supported in part by the National Natural Science Foundation of China under Grants 61973325 and 62032025, in part by the Natural Science Foundations of Guangdong Province under Grant 2021A1515011661, and in part by the Guangzhou Basic and Applied Basic Research Project under Grant 202102020616.

This article has supplementary downloadable material available at https://doi.org/10.1109/OJCS.2023.3245801, provided by the authors.

ABSTRACT At present, the concept of metaverse has sparked widespread attention from the public to major industries. With the rapid development of blockchain and Web3 technologies, the decentralized metaverse ecology has attracted a large influx of users and capital. Due to the lack of industry standards and regulatory rules, the Web3-empowered metaverse ecosystem has witnessed a variety of financial crimes, such as scams, code exploit, wash trading, money laundering, and illegal services and shops. To this end, it is especially urgent and critical to summarize and classify the financial security threats on the Web3-empowered metaverse in order to maintain the long-term healthy development of its ecology. In this paper, we first outline the background, foundation, and applications of the Web3 metaverse. Then, we provide a comprehensive overview and taxonomy of the security risks and financial crimes that have emerged since the development of the decentralized metaverse. For each financial crime, we focus on three issues: a) existing definitions, b) relevant cases and analysis, and c) existing academic research on this type of crime. Next, from the perspective of academic research and government policy, we summarize the current anti-crime measurements and technologies in the metaverse. Finally, we discuss the opportunities and challenges in behavioral mining and the potential regulation of financial activities in the metaverse. The overview of this paper is expected to help readers better understand the potential security threats in this emerging ecology, and to provide insights and references for financial crime fighting.

INDEX TERMS Blockchain, cybercrime, financial crime, Metaverse, Web3.

I. INTRODUCTION

Metaverse, literally a combination of the prefix “meta” (meaning beyond) and the suffix “verse” (abbreviation of “universe”), describes a world of virtuality and reality beyond the real world built by human beings using digital technology. Under the context of the *metaverse*, people can get a new Internet experience with high realism and deep immersion.

A key consideration in building the metaverse is whether it is centralized (centrally owned and controlled by large technology companies), or decentralized (jointly owned by members of the metaverse community). Typically, the former is referred to as the centralized metaverse, or “Web2 closed corporate metaverse”; the latter is referred to as the decentralized metaverse, or “Web3 open crypto metaverse,” as shown in Fig. 1. The concept of “Web3” here refers to the third iteration of the Internet that has been launched globally in recent years. Compared with the second generation of the Internet, which enables users of the metaverse to “read and write,” Web3 enables users to “read, write, and own”. In the context of “Web3,” users themselves hold the ownership of

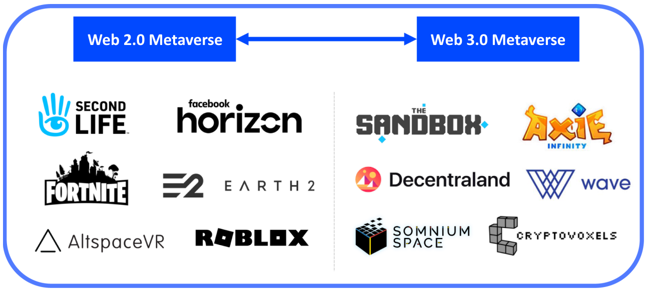


FIGURE 1. Different types of metaverses.

digital assets and their related derivative powers, which is the technical fundamental for the current decentralized Internet. The decentralized metaverse based on Web3 is referred to as the Web3-empowered metaverse (Web3 metaverse for short), and is the focus of this paper.

In the Web3-empowered metaverse, Web3 and metaverse are mutually supportive and complementary. On the one hand, the metaverse represents the future way of life and business, and provides the upper application scenarios and revolutionary front-end architectures for Web3. On the other hand, Web3 is the underlying technology foundation of the decentralized Internet, and provides revolutionary back-end support for the decentralized metaverse ecosystem. In the metaverse ecosystem, digital creation, digital asset, digital market and digital currency constitute the basic economic system [1]. The "decentralized" nature of Web3 is believed to help build a more open, autonomous, efficient, and fair metaverse ecosystem.

Motivations: According to a report of Greyscale [2], sales of items such as virtual land, goods and services in the Web3 metaverse have exceeded $200 million. However, where there is a concentration of value, there is crime, and the Web3 metaverse is no exception. The Web3 metaverse may well be a potentially attractive new vector for financial criminals. First, the Web3 metaverse will likely inherit and perpetuate the financial crimes that existed in Web3. According to Certik,[1] a blockchain security firm, more than $2 billion was stolen from Web3 projects as a result of hacking and vulnerabilities in the first half of 2022. Secondly, there are still many uncertainties in the fledgling metaverse, and there are profit–seeking inertia operations such as creating new concepts, speculating on new windfalls, and attracting new investments. Finally, the Web3 metaverse, which lacks industry standards and regulatory rules, may provides a more hidden space for financial crimes, such as fraud, malicious attacks, wash trading, terrorist financing, etc. Therefore, financial regulations needs to be expanded from the real world to the metaverse.

Up to now, there have been a number of studies that have discussed metaverse from different aspects, and we summarize these studies and discuss the current research gap in the Section I of the supplementary material.

Contributions: The contributions of this work are threefold:

- We review and summarize the various types of common financial crimes that have emerged since the development of the metaverse in five parts (i.e., scams, code exploits, wash trading, money laundering, and emerging crimes in the metaverse). This provides a reference for regulators, researchers, and practitioners to understand the possible risks of the metaverse economic system.
- We investigate the current state of financial crime prevention in the metaverse and its economic system from two perspectives: academic research and policy measurements, to inform investigators and researchers on how to prevent metaverse financial crimes, and to provide strategies and insights for deterring, detecting, and preventing metaverse financial crimes.
- We explore the possible opportunities and challenges of data-driven regulation for the metaverse at four levels: source, acquisition, query and indexing, analysis, and applications, and provide guidelines for researchers to design financial behavior mining algorithms and illegal behavior detection techniques for the metaverse.

Roadmap: This paper is organized as follows. In Section II, we describe the relationship between metaverse and Web3, and describe the core framework and technical foundation of Web3 metaverse and typical applications. In Section III, we summarize the possible financial crimes in the Web3 metaverse, giving relevant case studies to provide readers with a comprehensive understanding and key insights. Then, in Section IV, we outline the current regulatory policies and countermeasures to deal with financial crimes in the metaverse. Further, we discuss the current data-driven financial regulatory opportunities and and possible challenges in the Web3 metaverse in Section V. Finally, we conclude the paper in Section VI. Table 1 lists the abbreviations that appear frequently in this paper.

TABLE 1. List of Frequently Occurring Abbreviations in the Alphabetical Order

Acronym	Explanation
3D	Three Dimensional
AML	Anti-money Laundering
AR	Augmented Reality
DAO	Decentralized Autonomous Organization
DeFi	Decentralized Finance
KYC	Know Your Customer
NFT	Non-fungible Token
P2E	Play-to-earn
VR	Virtual Reality
Web3	The Third Iteration of Internet
XR	Extended Reality

II. BACKGROUND AND FUNDAMENTALS

According to existing studies [3], metaverse and Web3 are closely related concepts. In addition, to better understand the

[1] [Online]. Available: https://certik-2.hubspotpagebuilder.com/hack3d-q1-2022-0

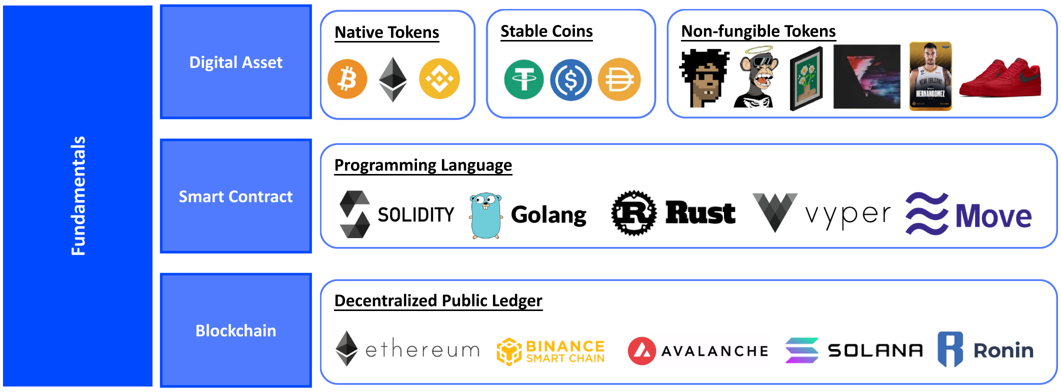


FIGURE 2. The technical fundamentals of Web3 metaverse economic system.

ecosystem of the metaverse, we will introduce some key concepts of the metaverse economy, such as blockchain, smart contracts, and crypto assets.

In addition, applications are also an important part of the metaverse economic system. We make a detailed introduction of typical metaverse applications in the Section II of the supplementary material.

A. METAVERSE AND WEB3

In 1992, when the concept of *metaverse* was first introduced, it was described as a virtual world where people who were not part of the elite could spend most of their free time. In the past decade, the industry is gradually defining the concept and main features of metaverse, and the movie “Ready Player One” is regarded as a good interpretation of the metaverse. Currently, the industry considers that blockchain and Web3 are the key technologies supporting the metaverse [4].

B. FUNDAMENTALS OF METAVERSE ECONOMY

To better understand the economic system of the metaverse, in this section, we first introduce the technologies that implement the underlying logic of the economic system, i.e., blockchain and smart contracts. In addition, the fuel for user activity in the economic system, i.e., crypto assets, also needs to be focused on. The details of the presentation are shown in Fig. 2.

Blockchain: Anu et al. [4] suggested that in Web3, application data is no longer stored in a private database but in a blockchain that can be written or read by anyone. Blockchain returns digital sovereignty to the users through a decentralized manner. There exist three main types of blockchain: public, private and consortium [5], and one of the typical applications of the public blockchain is the Bitcoin.

Smart Contract: Szabo introduced the concept of smart contracts in the mid-nineties [6], where he suggested embedding the logic of the contract into the code. With traditional contracts, a document outlines the terms of the relationship between two parties, which can be enforced by law. A smart contract [7] can be understood as an automatically executed contract with the terms of the agreement between the buyer and seller embedded within the code logic. Languages that currently support writing smart contracts include Solidity, Go, Java, and more.

Digital Assets and Tokens: Digital assets are intangible digital objects with verifiable and ownable digital values [4]. One of the main representatives of digital assets is *token*. A token is a digital asset implemented in a smart contract and is the medium for the storage and exchange of value in the metaverse [8]. The benefits of digital assets include a ubiquitous ledger, transparent updates, and payments that can be recorded and verified and do not require centralized settlement [9]. In the metaverse, the blockchain automatically records the human interactions in a tamper-proof public ledger, and the block miners obtain tokens as a reward. Tokens can be divided into two types: fungible tokens and non-fungible tokens. A fungible token is one that is interchangeable with another token while the non-fungible tokens (NFTs) are not interchangeable.

III. FINANCIAL CRIMES IN METAVERSE

Financial crimes are often defined as crimes against property and involve the unlawful transfer of money or other types of property belonging to another person. Typical financial crimes include scams, wash trading, money laundering, etc. These crimes not only bring losses to investors and users, but also pose a certain degree of threat and challenge to the current economic ecology.

Along with the recent development of Web3, financial crimes have been given a more diverse and complex meaning in the metaverse ecology. Based on the employment of blockchain in metaverse, many fraudsters have found new opportunities for illicit profits, including money laundering, identity theft, and scams [10].

The lack of effective regulation on blockchain or Web3 may make the metaverse a hotbed of criminal activities, promoting the occurrence of financial crimes such as scams, code exploits, wash trading, money laundering, and illegal services and shops. To this end, a summative research work on metaverse financial crimes is particularly urgent and critical. In this section, we provide an overview and taxonomy of financial

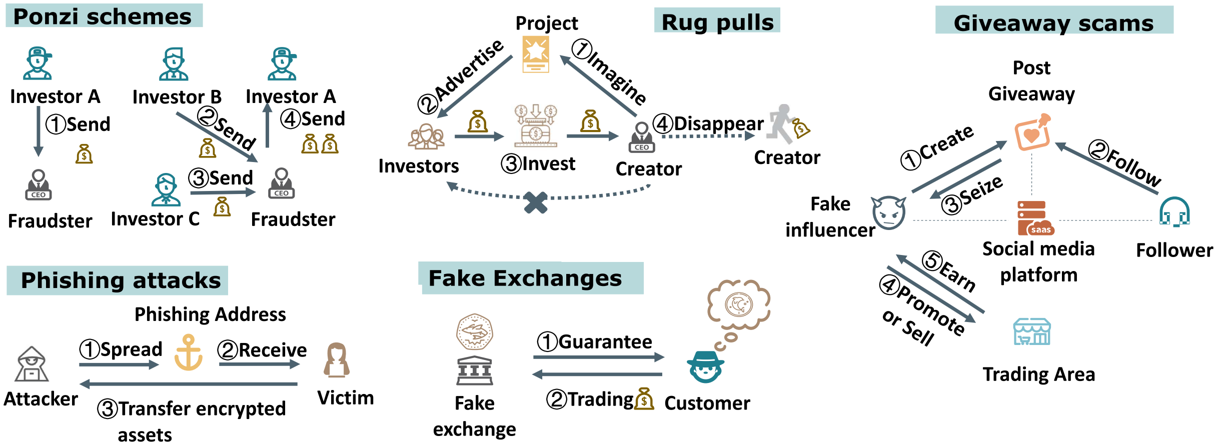


FIGURE 3. The schematic diagram of various types of scams in the metaverse.

crimes that have emerged since the development of the metaverse.

In the Section III of the supplementary material, we detailed describe the cases of scams and emerging crimes in the metaverse.

A. SCAMS

The concept of scam has been around for a long time, with the so-called Golden Age of the Great Scam having been documented in the relevant academic literature in the late 19th and early 20th centuries [11], [12]. Subsequently, Market Business News defined scam as a dishonest or fraudulent scheme. Such a scheme attempts to obtain money or something of value from people and is a confidence trick perpetrated by a dishonest group, individual or company. Whereas scams used to occur frequently in offline social interactions, with the growth of the Internet in the past decades, scams have successfully infiltrated online networks. More specifically, in the cryptocurrency market, scammers use the pseudonymous characteristics of cryptocurrencies to perpetrate untraceable crypto-asset scams and attempt to defraud investors for ill-gotten gains [13]. Scams on meterverse can be categorized into the following types [13], [14], [15]: (i) Ponzi schemes; (ii) Rug pulls; (iii) Phishing attacks; (iv) Fake exchanges; and (v) Giveaway scams. The basic workflows of various types of scams in the metaverse are shown in Fig. 3.

With the development of the metaverse, scams have gradually become a major concern for the security of the decentralized financial system in the metaverse.

B. CODE EXPLOIT

Since the success of Bitcoin, the applications of blockchain technology gradually emerging in many fields and services, such as financial markets, Internet of Things, supply chain, healthcare and storage. Since these systems usually store rich information, blockchain has also become a high-value target for cybercriminals or hackers [16]. Such attacks on the blockchain are usually manifested in various ways of "hacking" into the blockchain system. For example, some blockchain attacks focus on the poor protection of private keys by blockchain account owners or cryptocurrency exchanges to steal cryptocurrencies or personal assets of others. Other cyber attackers exploit vulnerabilities in blockchain protocols or their smart contract implementations to compromise blockchain systems [17], [18]. On the one hand, protocol design vulnerabilities occur when blockchain architects fail to adequately consider the impact of features built into their technology. On the other hand, many hackers have exploited the vulnerabilities in smart contracts to steal crypto assets.

Similar to DeFi, there exist a large number of smart contracts in the metaverse. Therefore, cybercriminals can likewise take advantage of poorly structured smart contracts or vulnerabilities in smart contracts to steal cryptocurrencies and NFTs in the metaverse. There are already examples of code being maliciously exploited in metaverse projects. In September 2020, a developer of Yearn Finance developed an NFT game called Eminence Finance, which has its own token called EMN. Without much understanding of this project, some investors discovered the token and minted $15 million worth of EMN in a few hours. They used a smart contract designed to allow players to exchange DAI (a stable coin) for EMN to fund in-game purchases. However, a hacker discovered a way to deplete the funds in the contract using a flash loan, which caused the price of the token to drop dramatically. The whole process of the flash loan case on Eminence is shown in Fig. 4. Additionally, while NFTs are blockchain-based, exchanges and marketplaces such as OpenSea and Rarible operate in a centralized manner, making them unable to take advantage of peer review systems that can identify and fix errors. As a result, they are vulnerable to code exploit attacks. In September 2021, 42 NFTs worth over $100,000 disappeared into thin air due to a vulnerability in the OpenSea token marketplace [19].

At this stage, research on code exploit attack has mainly focused on the exploration of smart contract vulnerabilities in Ethereum. However, with the development of the metaverse, research on smart contract vulnerabilities in the metaverse is

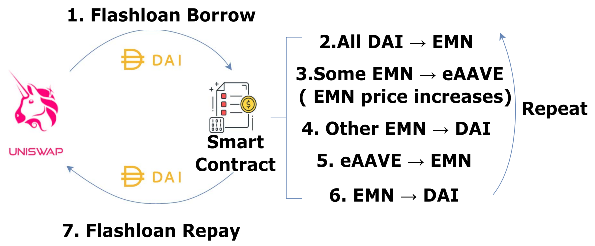


FIGURE 4. Flowchart of a hacker attack on Eminence (EMN) by flash loan.

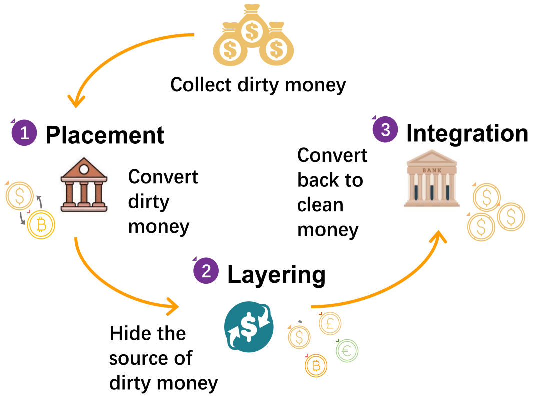


FIGURE 5. The three specific steps of money laundering.

gradually emerging. Ndiaye et al. [20] summarized cryptocurrency crimes by assessing the cost of attacks and losses caused by smart contracts. Moreover, they provide an in-depth analysis of the root causes and consequences behind the attacks and the defense strategies that exist. Kshetri et al. [21] discussed malicious attacks and disruptions on cryptocurrencies and NFTs in the metaverse, and provided an in-depth analysis of cyber attacks on crypto assets.

C. WASH TRADING

Wash trading is a market manipulation behavior that has appeared in traditional financial scenarios [22] and is recognized as a financial crime in most countries. Generally speaking, it refers to the repeated trading of assets in order to provide misleading information to the market. Wash trading activities inevitably lead to an increase in (fake) trading volume and create a false sense of prosperity.

Wash trading in the metaverse economic system exists mainly in the native cryptocurrency, ERC20 token market and NFT market. In fact, many exchanges have been accused of inflating trading volumes through wash trading. In August 2020, Coinbit, third largest cryptocurrency exchange of South Korea, was charged by the police with allegedly faking more than 99% of its trading volume [23]. In the NFT market of the metaverse, wash trading is also quite rampant. According to Elliptic [14], 95% of all activities on the decentralized NFT trading platform LooksRare is associated with wash trading. There are two main scenarios of NFT wash trading observed so far. One is the fictitious trading volume in order to get on the new NFT collection, which is similar to ICOs' conducting token washing in order to go public. One of the requirements for the centralized NFT trading platform OpenSea to validate an NFT collection is at least 100 ETH transaction volume, which may be difficult to meet for newly launched collections. This requirement appears to encourage fraudulent transactions, where fictitious transactions are executed between multiple accounts under the control of the attackers to artificially inflate transaction volumes. The other main scenario of NFT wash trading is to obtain other token rewards by wash trading through NFT transactions. Chainalysis [24] reported blatant double trading of three identical NFTs between two wallets, trading approximately 650,000 ETH and costing $114 million in transaction fees. They ended up with approximately $185.5 million worth of tokens from the NFT trading platform, bringing in nearly $71 million in profits. Therefore, wash traders influence the valuation of metaverse assets and even manipulate the metaverse market.

It is extremely challenging to detect and count wash trading. The current main methods of wash trading are based on transaction data. Some work constructs a transaction network by abstracting the transfer relationship between users and employs the network topology theory to analyze and detect the wash trading activities. For example, Victoret al. [25] proposed a wash trading detection method for decentralized exchanges based on the identification of network loops and cycles. This method found various wash trading structures and manipulated volumes of IDEX and EtherDelta with a total value of $159 million. Serneels et al. [26] proposed three methods to flag suspicious NFT wash trading activities, including closed loop token trades, closed loop value trades, and high transaction volumes. Inspired by Victor et al. [25], [27] detected suspicious wash trading in NFT and counts the proportion of suspicious wash trading in the NFT set to the total transaction volume, as well as the proportion of wash trading in the mainstream NFT trading market. Existing work also proposes to design washing behavior indicators through empirical analysis. For example, Chen et al. [23] designed several metrics to analyze wash trading on centralized exchanges based on off-chain transaction data and on-chain transaction data.

D. MONEY LAUNDERING

Money laundering, which is a serious financial crime that fuels crimes such as drug trafficking and terrorism, has a negative impact on the global economy. The Association of Internationally Recognised Anti-Money Launderers defines money laundering as acquiring the proceeds of crime and disguising their illicit origin in order to use those funds for legal or illegal activities [28]. Intuitively, money laundering is the process of making dirty money look clean. The process of money laundering can be subdivided into three specific steps, as illustrated in Fig. 5, namely, placement, layering, and integration [29]. First, illicit funds are surreptitiously channeled into the legitimate financial system. Then, complex financial transactions are used to hide the source of illicit funds, sometimes by wire transfer or by transferring money through numerous accounts to create confusion. Finally, the funds are integrated into the financial system through additional transactions until the “dirty money” looks “clean”. Due to the huge negative financial impacts of money laundering crimes on society, most financial organizations now have anti-money laundering (AML) policies in place to detect and prevent such activities [30].

In a metaverse ecosystem where crypto assets such as NFTs are widely used but legal regulation of metaverse transactions is still immature [31], the potential for money laundering is considered high. In particular, with the growing trend of total sales of land assets and wearables (also known as “skins,” which are clothing and accessories for avatars) in the metaverse, it is highly likely that criminals will use these new assets for illegal money laundering operations.

In terms of metaverse land assets, the total sales of all crypto assets (including land assets in virtual platforms) in the blockchain-powered virtual reality platforms like Decentraland, Cryptovoxels, the Sandbox, and Somnium Space have exceeded $500 million in 2021 [14]. Of those, with millions of dollars of plots sold, the average land value in Decentraland reaches tens of thousands of dollars by 2021 [14], indicating a potential way for a large amount of illicit money to be transferred. In addition, unlike real world purchases of property or land, purchasing metaverse land often requires only a crypto asset address and some funds without KYC checks, which also makes it extremely convenient for money laundering and other criminal activities.

In terms of wearable device assets, the wearable market is expected to reach $3 trillion by the end of 2023. Criminals can buy a wearable device in one metaverse and then move it to another, cashing out through secondary sales, thus making the money flow harder to track as it spans multiple blockchains. These data suggest that as metaverse financial assets continue to evolve, it is likely that illicit actors will use them as a primary conduit for laundering illicit assets that may come from real-world activities or other crypto-based crimes, and that criminals can hide their origin by exchanging them for metaverse-based assets (e.g. land in a metaverse, wearables, etc.) [14].

With the booming growth of the metaverse and the expansion of crypto assets therein, it is urgent to conduct the investigation and prevention of money laundering crimes on the metaverse economic ecosystem. Recently, Qin et al. [32] discussed money laundering crimes in the crypto market and analyse the legal level measures proposed by countries or regions such as the EU, Japan, and the US on the prevention of cryptocurrency money laundering crimes in the context of the metaverse.

E. EMERGING CRIMES IN METAVERSE

Financial crimes have existed for centuries, but in the metaverse, crimes have taken on a more multifaceted meaning, with multiple types of crime closely related to metaverse crypto assets. Fig. 6 shows the trap that users may fall into. In this section, six emerging and noteworthy forms of crime, namely, illegal services and shops, fake metaverses, fake land expansions, technical support scams, 3D social engineering, and sanctions and terrorism funding, will be discussed in turn.

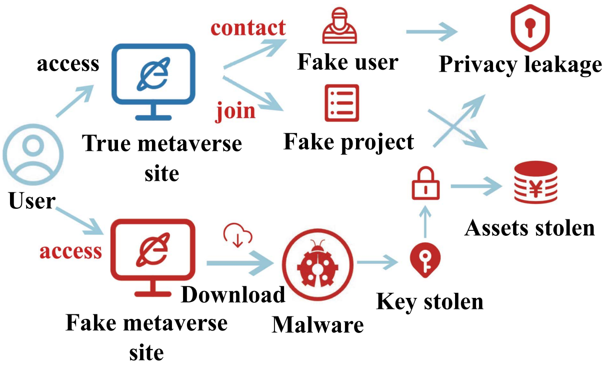


FIGURE 6. Common fraud pitfalls in metaverse.

IV. ANTI-CRIMES IN METAVERSE

No matter how much emphasis is placed on the “decentralisation” and “data freedom” of the Web3 metaverse, the issue of regulation is always an key part of the metaverse architecture. In this section, we discuss the current research on the regulation of the Web3 metaverse and its basic components from the perspectives of academic research and related policies and measures.

A. ACADEMIC RESEARCHES

With the rise of the metaverse and the widespread occurrence of related financial crimes, some efforts have been devoted to combating these crimes. The following is a brief overview of existing research on anti-crimes in metaverse from the perspectives of three academic disciplines.

1) COMPUTER SCIENCE FIELD

In the past decade, a series of studies from computer science or software engineering fields focused on blockchain smart contract security, behavioural mining, and anomaly detection.

In terms of smart contract security, Atzei et al. [33] analysed the security vulnerabilities of smart contracts on Ether, revealing the financial security issues they can cause. In 2022, Kushwaha et al. [34] conducted a systematic review of research on smart contract security issues up to 2022. In addition, security tools [35] and analytical frameworks [36] have been put forward to address security concerns in smart contract.

In terms of behavioral mining and anomaly detection, according to an overview given in [37], existing work can be divided into four parts: entity identification, transaction pattern recognition, illegal activity detection, and transaction tracking. For instance, Victor et al. [38] proposed a clustering heuristic for entity identification based on the Ethernet account model, Huang et al. [39] modeled the Ethereum transaction records as a large-scale transaction network and proposed a GCN-based model to classify account in Ethereum, and Liu et al. [40] proposed a method called FA-GNN to deal with the heterophily issue for account classification in Ethereum. In [41], Wu et al. proposed temporal attribute heterogeneous modalities, and implemented transactional pattern recognition using modal detection. In an environment where the anonymity of cryptocurrencies has led to their widespread use in financial crimes, Akcora et al. [42] propose a cryptocurrency-based ransomware detection framework that can be used to automatically detect ransomware. In addition, a series of data modeling and transaction tracking methods have been proposed [43], [44], [45], [46], [47], [48], [49], [50].

Recently, some work started to analyze metaverse security. For example, Kshetri et al. [21] discussed the impact of possible attacks and various types of frauds on NFT. However, anti-crime research on the metaverse is still at a more preliminary stage compared to related research in the blockchain and cryptocurrency.

2) INDUSTRY FIELD

Outside of academia, the industry has also paid much attention to security issues in blockchain, Web3, and the metaverse. Several cryptocurrency and Web3 services companies have released reports on security and anti-crime issues. For example, Certik published HACK3D: The Web3 Security Quarterly Report [51], in the second quarter of 2022. This report states that the security of individual projects in Web3 is dependent on the security of the entire ecosystem; Elliptic analysed potential metaverse financial crime types and proposes corresponding measures to prevent them in a report entitled The Future of Financial Crime in the Metaverse [14] published in 2022; SlowMist analysed some typical security incidents and published an advanced analysis method for the tracking of coin blender funds in its Blockchain Security and Anti-Money Laundering Analysis Report for the first half of 2022 [52].

3) FINANCIAL FIELD

The virtual economic system is a crucial part of the metaverse and the financial community has long studied financial issues in the virtual economy. Smaili et al. [53] flagged the different kinds of fraud risks that can be posed by the metaverse. Wronka et al. [54] analysed the impact of DeFi on efforts to combat financial crime. Back in 2018, the National Bureau of Economic Research released a study on the Bitcoin economic system [55]. The Financial Action Task Force on Money Laundering, one of the world's foremost international organisations combating money laundering, updated its guidance on virtual assets and virtual asset service providers [56] in 2021, further requiring countries to assess and mitigate the risks of their virtual asset financial activities. There are corresponding studies in academia, such as Barone et al. [57] comparing usury in traditional economic systems with cryptocurrency as a means of money laundering.

4) LEGAL FIELD

In the face of the fertile ground that the ecology of the metaverse presents for financial crime, we need norms to reduce the risks to which participants are exposed, and work has been done by researchers on this. Murray et al. [58] considered the legal problems that people need to face in a metaverse. Bokovnya et al. [59] discussed how realistic laws can be changed to combat cryptocurrency crime. Teichmann et al. [60] later proposed a more effective international regulatory standard using the Liechtenstein Blockchain Act [61] as a benchmark.

Summary: In addition to these four disciplines, there are many fields such as sociology, political science, international relations, etc. that are concerned with the changes that the metaverse may bring about, especially whether new financial crimes may evolve in such a "beautiful new world" as the metaverse. Since the day the financial markets were created, researchers and practitioners have been actively seeking strategies to combat financial crimes in various emerging areas in order to safeguard the smooth functioning of the system. Research into the financial aspects of the metaverse is still at an early stage and further exploration is needed in the future.

B. REGULATORY POLICIES AND MEASURES

As mentioned above, the new fertile soil of the metaverse has given birth to many new opportunities but is also coveted by many unscrupulous elements. Many criminals have expanded their scams to the area of the metaverse. They take advantage of various loopholes in the still incomplete emerging technology to carry out attacks, causing many participating investors to lose their property. Such financial crimes have largely undermined investors' confidence in the future of the metaverse, which is obviously not conducive to its long-term development. Therefore, government organizations around the world have started to introduce policies to regulate various digital assets and related services. In the Section IV of the supplementary material, we introduce the regulatory policies and measures of different countries in detail.

V. OPPORTUNITIES AND CHALLENGES

As mentioned earlier, the underlying technical foundation of the Web3 metaverse is blockchain technology, and thus the data of the Web3 metaverse also has the good nature of blockchain data: open and transparent, forgery-proof, tamper-proof, and traceable, which provides unprecedented opportunities for researchers to understand and solve related problems by analyzing blockchain data. The value of analyzing and mining Web3 metaverse financial data is twofold. 1) Researchers can broadly explore the evolution of user behavior, transaction networks, wealth distribution, asset values, and organizational decisions in the metaverse economic system, as a reference for other financial activities. 2) In recent

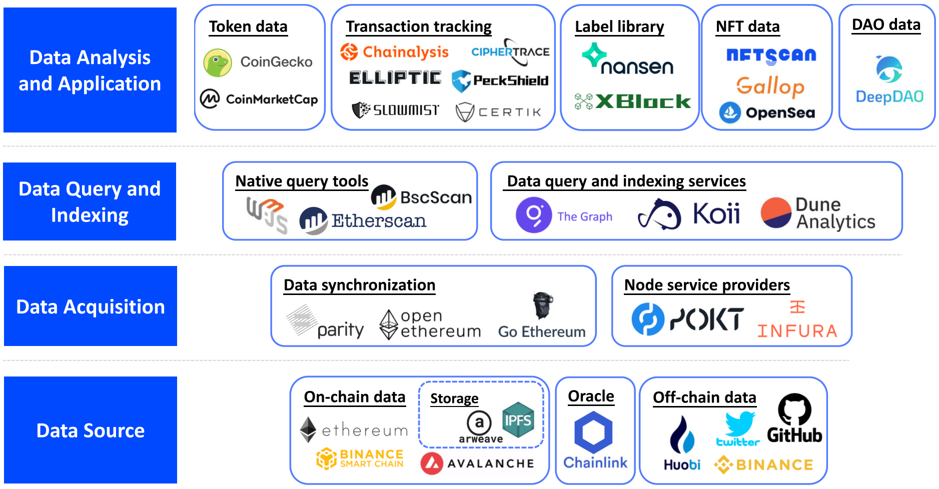


FIGURE 7. **Web3 metaverse data track structure.**

years, various types of financial crimes have started to appear in the metaverse. Metaverse financial data analysis can help identify illegal behaviors among them and provide effective regulatory solutions for building a healthier metaverse ecology, and the related technology can also be a reference for metaverse transaction regulation in political affairs and other scenarios. Therefore, this section focuses on several opportunities and challenges of financial regulation in the metaverse from a data-driven perspective.

In addition, more examples of opportunities and challenges can be found in the Section V of the supplementary material.

A. OPPORTUNITIES

Next, we discuss the opportunities of data-driven financial governance in Web3 metaverse at four levels: the bottom level is data sources, the second level is data acquisition, the third level is data query and indexing, and the top level is data analysis and application, as shown in Fig. 7.

1) DATA SOURCE

The data of blockchain and Web3 metaverse can be categorized into on-chain data and off-chain data. On-chain data mainly includes blocks, transfer transactions, wallet addresses, smart contract bytecodes, smart contract events, digital asset information, and other data. In addition, decentralized storage is also the main source of on-chain data; for example, NFT can be saved in the Inter Planetary File System (IPFS) [62], a peer-to-peer hypermedia transfer protocol. The off-chain data, on the other hand, mainly includes data from centralized exchanges (e.g., Cryptocurrency Exchange), as well as some typical Web2 data, such as social media data, GitHub website data, etc.

2) DATA ACQUISITION

There are more diverse ways to obtain Web3 metaverse data, but since off-chain data is often the data of centralized institutions (e.g. centralized trading platforms) or Web2 type data, the ways to obtain it vary greatly, so this paper mainly discuss the acquisition of on-chain data.

The underlying blockchain data of metaverse contains a large amount of heterogeneous data, and there are various methods to obtain Web3 metaverse on-chain data. Taking the Ethereum-based metaverse project as an example, the main ways to obtain Ethereum on-chain data include: 1) downloading and directly parsing block files. This method is simple and fast to implement, but it cannot collect complete data. This is because internal transactions are not stored in the blockchain and therefore cannot be obtained by parsing blocks; 2) deploying an Ethereum client, such as the Parity client's API allowing users to directly access internal transactions and external transactions in Ethereum. Some of the more well-known decentralized data service providers are Pocket Network (https://www.pokt.network/), whose core business is to provide decentralized data relay services (or RPC services) for developers on various public chains.

3) DATA QUERY AND INDEXING

As mentioned earlier, almost all blockchain transactions in the metaverse are publicly available on the blockchain. However, it is usually a daunting work to query and index the raw transaction data, which is often large and diverse in data type. The earliest tools for querying and indexing Web3 metaverse data were the APIs of the underlying public chain and blockchain browsers, such as the Web3 API and the Ethereum browser provided by Etherscan. Web3 API uses a remote procedure call (RPC) to communicate with Etherscan nodes.

In addition to the blockchain browsers of the underlying public chains of the metaverse, there are also service providers that offer data query and indexing services. They make raw data more accessible and usable by parsing and structuring it on top of node service providers that interact directly with various public chains. In what follows, we give two representative examples: (1) Dune Analytics (https://dune.com/) is a comprehensive Web3 data platform that adds raw data to SQL tables and parses them based on APIs provided by node service providers to enable users to query, analyze, and visualize through dashboards in real-time in their well-built databases using SQL. (2) The Graph (https://thegraph.com) is a decentralized on-chain data indexing protocol for querying networks like Ether and IPFS. The Graph is a cloud service like API composed of decentralized indexing nodes. This side-by-side demonstrates the necessity and feasibility of regulation in the decentralized financial ecosystem of the Web3 meta-universe.

4) DATA ANALYSIS AND APPLICATIONS

One layer up from the data query and indexing is the encapsulated, deliverable data products that can provide metaverse data value directly to users. The players in this layer can be broadly classified according to the type of data as token data analysis, on-chain transaction tracking, label library applications, NFT data analysis, DAO data analysis, etc.

- *Token data analysis:* One representative platform is CoinMarketCap (https://coinmarketcap.com, established in 2013, which is used to observe and track token prices, trading volume, market value, etc. For example, CoinMarketCap gives a marketcap ranking of metaverse tokens (including trading tokens or governance tokens)[2] and a “Play-to-Earn” ranking of metaverse projects[3] for players’ reference. In the area of regulation, Chen et al. [23] conducted an empirical study on the analysis of cryptocurrency exchange swipes based on scores and rankings of exchanges provides by Coinmarketcap. Another data platform similar to CoinMarketCap is CoinGecko (https://www.coingecko.com/), which has been used by a number of researchers to conduct research on cryptocurrency and DeFi applications. For example, DeFiRanger [63] refers to the market capacity and the price of tokens of five vulnerable DeFi apps provided by CoinGecko, to represent the market value of these DeFi apps, and proposes a price manipulation identification technique for DeFi apps. These classifications and statistics help researchers summarize and generalize the models of different types of attacks and design more accurate and efficient methods for DeFi attack detection and DeFi attack defense [64], [65].
- *On-chain transaction tracking:* The on-chain transaction tracking platform is a platform that has been around since the birth of Bitcoin. The representative platform is Chainalysis (https://www.chainalysis.com/). Recently, Chainalysis has revealed examples of NFT wash trading in its Web3 report [66], which also provide inspiration for subsequent papers on NFT wash trading detection.
- *Label library applications:* The representative platform in industry is Nansen (https://www.nansen.ai/), founded in 2020. Nansen provides a number of wallet labels,[4] a way to tag and identify wallet addresses, classify wallets as “Fund,” “Heavy DEX trader,” “Legendary NFT collector” etc. Mapping on-chain data with a database of millions of labels, researchers can understand what is happening on the blockchain in the metaverse and the types of wallets executing transactions, and can see who is behind these transactions. The representative platform in the academic community is Xblock (http://xblock.pro/), which provides several datasets that allow for transaction data analysis and anomalous behavior detection [37], [45], [67], [68], [69].
- *NFT data analysis:* Founded in 2021, the NFTscan platform (https://www.nftscan.com/) provides NFT collectors and investors and researchers with an API[5] to access NFT asset data and historical data held at any wallet address, as well as data analysis including top mint, gas tracker, NFT marketplace, trending collection, etc. NFTscan is designed to help users better track and evaluate the value of NFT assets to help make informed investment decisions. Such NFT data platforms have been used by researchers in academic studies, e.g., Cho et al. [70] utilized data from six profile picture collections (PFP) type NFT collections provided by Gallop (https://www.higallop.com/), including transaction history, price, the associated wallet address, visual features and attachment of the NFT. The article also describes some of the challenges associated with NFT transaction data and data pre-processing recommendations. The dataset is currently open source [71].
- *DAO data analysis:* As we know, in the process of on-chain decision making of a DAO, members first vote on the proposal on chain to decide whether to execute the proposal, and then the smart contract will automatically execute the proposal after the vote is passed. As the first DAO comprehensive data platform, DeepDAO (https://deepdao.io/), founded in 2020, analyzes, explores and ranks DAO based on multiple dimensions. For example, DeepDao provides an overview of the DAO of Decentraland,[6] including information on project members’ shares, proposals, Voting Coalitions, etc.[7] Based on the data analysis of DeepDao, future researchers can explore the possible financial crimes in the metaverse DAO ecosystem, such as vote manipulation of DAOs, money laundering through DAOs, collusion or cronyism, and vote swiping of proposals.

In conclusion, these publicly available, processed, and easy-to-use data sources, access, query, and analysis platforms can not only enhance the theoretical value and application of data mining, social network analysis, quantitative trading, and

[2] [Online]. Available: https://coinmarketcap.com/view/metaverse/

[3] [Online]. Available: https://coinmarketcap.com/watchlist/6163287dad9db6359e33775b/

[4] [Online]. Available: https://www.nansen.ai/guides/wallet-labels-emojis-what-do-they-mean

[5] [Online]. Available: https://docs.nftscan.com/nftscan/APIOverview

[6] [Online]. Available: https://dao.decentraland.org/en/

[7] [Online]. Available: https://deepdao.io/organization/60c9b31c-4495-4028-aeac-eb7bb117fece/organization_data/members

other techniques in the financial system, but also help enhance the financial security and regulation of the meta-universe economic system.

B. CHALLENGES AND OPEN ISSUES

Although the publicly available data of the Web3 metaverse provides opportunities for technical research to prevent financial crimes, the "decentralized" nature of Web3 also pose a great challenge for the governance of the metaverse. On the one hand, since the Web3 metaverse economic system integrates the latest technologies and systems such as blockchain, smart contracts, and digital assets as its foundation, the metaverse is very likely to inherit the regulatory challenges of these underlying technologies. On the other hand, the financial regulation of Web3 metaverse may face new challenges in the new scenario of metaverse.

1) CHALLENGES INTRODUCED BY WEB3 FUNDAMENTALS

From a technical point of view, Web3 provides the technical basis for the current hotly debated metaverse. From the economic point of view, compared with Web2, the most significant feature of Web3 is that it is a distributed Internet infrastructure, user-centered, emphasizing the autonomy of users' digital identity, personal data, and algorithms, and equal rights for users and builders. According to the technical basis of Web3, the challenges of metaverse regulation brought by Web3 have three main levels:

- *The underlying blockchain:* Similar to blockchain, users of Web3 metaverse can conduct a large number of frequent transactions between accounts under their control. These result in the difficulty of identifying the entities of the Web3 metaverse accounts, with a large number of anonymous transactions and uncertain behavior. While de-anonymization may be possible through transaction data mining techniques, this in turn may raise other issues, such as user privacy breaches. Countless records of user activities and traces of user interactions will be retained in the Web3 metaverse. As these data are stored on the public blockchain, the accumulation of records and traces over time may cause user privacy disclosure problem.
- *Smart contracts and digital assets:* Smart contracts enable all types of digital assets, including stablecoins, fungible tokens, NFTs, etc. Smart contracts enable various types of digital assets to be exchanged on a trading platform. At the same time, Turing-complete smart contracts can represent and execute more complex application logic and functionality, leading to more complex transaction patterns. Meanwhile, as mentioned in the previous section, there are already many regulatory policies and measures for blockchain cryptocurrencies (e.g., Bitcoin, Ether, etc.) at home and abroad. The future regulation of the Web3 metaverse at home and abroad also needs to dovetail with the norms and measures for cryptocurrencies.
- *DeFi and DAO:* The goal of DeFi is to create a decentralized, open-source, permissionless and transparent economic system that operates behind a DAO [72] that operates strictly through programmed code/protocols. Although DeFi offers great opportunities for Web3 and the metaverse, DeFi and the DAOs behind it still need to be adequately regulated in order to ensure the trustworthiness of DeFi in the metaverse. However, users of current DeFi protocols or DApps are not mandated to meet anti-money laundering (AML) and know-your-customer (KYC) requirements. As described by Salami [72], if a Web3 metaverse project has achieved a high degree of decentralization, they need to be operated and managed entirely by the DAO of the programming code/protocols without any influence from a centralized authority such as software developers. Then, it will become very difficult to hold anyone accountable for crimes and errors in the operation of the DeFi protocol in the Web3 metaverse.

2) OPEN ISSUES INTRODUCED BY THE METAVERSE

The metaverse constructs a new social structure where the virtual and the real are highly intertwined. The users of the metaverse are also residents of the real world, thus also making traditional security risks and non-traditional security risks superimposed on each other, and the virtual economy of the metaverse and the real economy of the real world will inevitably interact with each other. In this part, we will discuss the open issues introduced by the metaverse to financial regulation in terms of the different paths into the metaverse.

- *Digital twins:* A digital twin is a digital mapping of the physical world, where the user enters the metaverse with their digital body. At this point, the definition of personal identity becomes problematic. In the real world, financial regulation regulates the actual person. It is then a challenge to regulate the interaction between this digital avatar and the real world person in person in a metaverse regulatory regime.
- *Digital primordial:* The digital native is a virtual universe parallel to the physical world, where multiple avatars of the self in the metaverse can multitask, collaborate and talk to each other. Therefore, a criminal in the real world can have multiple doppelgangers in the metaverse, and it will be difficult to correspond between the metaverse and the real-world "person" in fact. At the same time, the metaverse breaks through national geographical boundaries, which poses a major obstacle to effective financial regulation and enforcement in individual countries.
- *Virtual-real synthesis:* The real world interacts with the virtual world. A real-world criminal can take the assets he illegally obtained in the metaverse (e.g., stealing assets via DeFi exploits) and can exchange the stolen assets on the chain for real-world fiat currency through an exchange that does not require KYC. The laundered

fiat currency, in turn, flows into the real-world financial system and may be used to finance real-world terrorism. Thus, the interconnection of the real world and virtual world in the metaverse makes the metaverse economic system will face more severe risks than the traditional financial industry, which puts higher demands on the risk-awareness of the metaverse financial system.

VI. CONCLUSION

This paper focuses on financial crimes in Web3-empowered metaverse. First, we introduce the background, foundation and diverse applications of the Web3 metaverse economic system. Then, we summarize the financial crimes and anti-crime techniques that have emerged on the metaverse from both academia, industry and government. Particularly, this paper provides a taxonomy of financial crimes on the metaverse, and a specific discussion of each crime, including existing definitions of the crime, case studies and analyses related to the metaverse, and existing academic research on the crime. Finally, the paper explores the possible opportunities and challenges of data-driven metaverse regulation. Overall, by providing an overview of this paper, we hope that readers can gain a better understanding of the financial crime issues that the metaverse may currently face and that it will help to improve metaverse regulation. Among the future research directions, researchers may be able to explore the following directions: 1) Researchers can synthesize and analyze the current case data as well as employ corresponding statistical and analytical methods to explore the prevalence and trends of financial crimes in the metaverse and the corresponding countermeasures. 2) Researchers can also utilize the latest technologies and tools, such as artificial intelligence and Big Data analysis, to support research efforts on financial crimes in the metaverse. 3) Experts and scholars from cross-disciplinary disciplines work together to conduct in-depth research and analysis of current domestic and international legal and regulatory rules, and propose policies and recommendations that are more suitable for the long-term development of the metaverse.

REFERENCES

[1] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 122–136, 2022.

[2] G. Research, "The metaverse: Web3.0 virtual cloud economies," 2021. Accessed: Nov. 1, 2021. [Online]. Available: https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf

[3] L. Cao, "Decentralized AI: Edge intelligence and smart blockchain, metaverse, web3, and DeSci," *IEEE Intell. Syst.*, vol. 37, no. 3, pp. 6–19, May/Jun. 2022.

[4] A. Banerjee, R. Byrne, I. D. Bode, and M. Higginson, "Web3 beyond the hype," 2022. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/web3-beyond-the-hype

[5] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[6] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, 1997, doi: 10.5210/FM.V2I9.548.

[7] W. Zou et al., "Smart contract development: Challenges and opportunities," *IEEE Trans. Softw. Eng.*, vol. 47, no. 10, pp. 2084–2106, Oct. 2021.

[8] T. Chen et al., "Understanding ethereum via graph analysis," *ACM Trans. Internet Technol.*, vol. 20, no. 2, pp. 1–32, 2020.

[9] R. K. Lyons and G. Viswanath-Natraj, "What keeps stablecoins stable?," *J. Int. Money Finance*, 2022, Art. no. 102777, doi: 10.2139/ssrn.3508006.

[10] T. Kadar, "The metaverse fraud question: What are the risks?," 2022. [Online]. Available: https://seon.io/resources/metaverse-fraud/

[11] A. Lindesmith, *The Big Con: The Story of the Confidence Man and the Confidence Game*. New York, NY, USA: JSTOR, 1940.

[12] J. R. Weil and W. T. Brannon, *The Con Game and "Yellow Kid" Weil*. Sydney, NSW, USA: ReadHowYouWant. com, 1948.

[13] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, "Cryptocurrency scams: Analysis and perspectives," *IEEE Access*, vol. 9, pp. 148353–148373, 2021.

[14] Elliptic, "The future of financial crime in the metaverse,", 2022. [Online]. Available: https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf

[15] APWG, The APWG Ecrime Exchange (ECX), 2021. [Online]. Available: https://apwg.org/

[16] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[17] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, 2019, Art. no. 1788.

[18] M. R. Parizi and A. Dehghantanha, "Smart contract programming languages on blockchains: An empirical evaluation of usability and security," in *Proc. Int. Conf. Blockchain*, 2018, pp. 75–91.

[19] BTC Peers Reporter. $100,000 worth of NFTs disappear forever, thanks to OpenSea bug, 2021. [Online]. Available: https://btcpeers.com/100-000-worth-of-nfts-disappear-forever-thanks-to-opensea-bug/

[20] M. Ndiaye and P. K. Konate, "Cryptocurrency crime: Behaviors of malicious smart contracts in blockchain," in *Proc. IEEE Int. Symp. Netw., Comput. Commun.*, 2021, pp. 1–8.

[21] N. Kshetri, "Scams, frauds, and crimes in the nonfungible token market," *Computer*, vol. 55, no. 4, pp. 60–64, 2022.

[22] Y. Cao, Y. Li, S. Coleman, A. Belatreche, and T. M. McGinnity, "Detecting wash trade in the financial market," in *Proc. IEEE Conf. Comput. Intell. Financial Eng. Econ.*, 2014, pp. 85–91.

[23] J. Chen, D. Lin, and J. Wu, "Do cryptocurrency exchanges fake trading volumes? An empirical analysis of wash trading based on data mining," *Physica A: Stat. Mechanics Appl.*, vol. 586, 2022, Art. no. 126405.

[24] Chainalysis, "The chainalysis 2021 NFT market report," 2022. [Online]. Available: https://go.chainalysis.com/nft-market-report.html

[25] F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in *Proc. ACM Web Conf.*, 2021, pp. 23–32.

[26] S. Serneels, "Detecting wash trading for nonfungible tokens," *Finance Res. Lett.*, to be published, doi: 10.1016/j.frl.2022.103374.

[27] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the NFT ecosystem," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2022, pp. 667–681.

[28] ACAMS, "Study guide for the CAMS," 2012. [Online]. Available: https://www.acams.org

[29] FATF, "What is money laundering," 2021. [Online]. Available: https://www.fatf-gafi.org/faq/moneylaundering/

[30] FINRA, "Anti-money laundering (AML)," 2022. [Online]. Available: https://www.fatf-gafi.org/faq/moneylaundering/

[31] E. Hartwich, P. Ollig, G. Fridgen, and A. Rieger, "Probably something: A multi-layer taxonomy of non-fungible tokens," 2022, *arXiv:2209.05456*.

[32] H. X. Qin, Y. Wang, and P. Hui, "Identity, crimes, and law enforcement in the metaverse," 2022, *arXiv:2210.06134*.

[33] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *Proc. 6th Int. Conf. Princ. Secur. Trust*, 2017, pp. 164–186.

[34] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.

[35] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, "Securify: Practical security analysis of smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 67–82.

[36] L. Brent et al., "Vandal: A scalable security analysis framework for smart contracts," 2018, *arXiv:1809.03981*.

[37] J. Wu, J. Liu, Y. Zhao, and Z. Zheng, "Analysis of cryptocurrency transactions from a network perspective: An overview," *J. Netw. Comput. Appl.*, vol. 190, pp. 103–139, 2021.

[38] F. Victor, "Address clustering heuristics for ethereum," in *Proc. 24th Int. Conf. Financial Cryptogr. Data Secur.*, 2020, pp. 617–633.

[39] T. Huang, D. Lin, and J. Wu, "Ethereum account classification based on graph convolutional network," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 69, no. 5, pp. 2528–2532, May 2022.

[40] J. Liu, J. Zheng, J. Wu, and Z. Zheng, "FA-GNN: Filter and augment graph neural networks for account classification in ethereum," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2579–2588, Jul./Aug. 2022.

[41] J. Wu, J. Liu, W. Chen, H. Huang, Z. Zheng, and Y. Zhang, "Detecting mixing services via mining bitcoin transaction network with hybrid motifs," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 52, no. 4, pp. 2237–2249, Apr. 2022.

[42] C. G. Akcora, Y. Li, Y. R. Gel, and M. Kantarcioglu, "BitcoinHeist: Topological data analysis for ransomware detection on the bitcoin blockchain," in *Proc. Joint. Conf. Arti. Intell.*, 2020, pp. 4439–4445.

[43] S. Phetsouvanh, F. Oggier, and A. Datta, "EGRET: Extortion graph exploration techniques in the bitcoin network," in *Proc. IEEE Int. Conf. Data Mining Workshops*, 2018, pp. 244–251.

[44] H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing transactions across cryptocurrency ledgers," in *Proc. 28th USENIX Secur. Symp.*, 2019, pp. 837–850.

[45] D. Lin, J. Chen, J. Wu, and Z. Zheng, "Evolution of ethereum transaction relationships: Toward understanding global driving factors from microscopic patterns," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 2, pp. 559–570, Apr. 2022.

[46] D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "T-edge: Temporal weighted multidigraph embedding for ethereum transaction network analysis," *Front. Phys.*, vol. 8, 2020, Art. no. 204.

[47] D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "Modeling and understanding ethereum transaction records via a complex network approach," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 67, no. 11, pp. 2737–2741, Nov. 2020.

[48] C. Jin, J. Jin, J. Zhou, J. Wu, and Q. Xuan, "Heterogeneous feature augmentation for ponzi detection in ethereum," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 69, no. 9, pp. 3919–3923, Sep. 2022.

[49] D. Lin, J. Wu, Q. Xuan, and K. T. Chi, "Ethereum transaction tracking: Inferring evolution of transaction networks via link prediction," *Physica A: Stat. Mechanics its Appl.*, vol. 600, 2022, Art. no. 127504.

[50] J. Zhou, C. Hu, J. Chi, J. Wu, M. Shen, and Q. Xuan, "Behavior-aware account de-anonymization on ethereum interaction graph," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 3433–3448, 2022, doi: 10.1109/TIFS.2022.3208471.

[51] CERTIK, "CERTIK's HACK3D: The Web3 security quarterly report," 2022. [Online]. Available: https://www.certik.com/resources/blog/7fuXtbfo4CXEXcwy5Pqijp-hack3d-the-web3-security-quarterly-report-q2-2022

[52] SLOWMIST, "Mid-year blockchain security and anti-money laundering analysis report," 2022. [Online]. Available: https:https://www.slowmist.com/report/first-half-of-the-2022-report(EN).pdf

[53] N. Smaili and A. de Rancourt-Raymond, "Metaverse: Welcome to the new fraud marketplace," *J. Financial Crime*, vol. 29, 2022, doi: 10.1108/JFC-06-2022-0124.

[54] C. Wronka, "Financial crime in the decentralized finance ecosystem: New challenges for compliance," *J. Financial Crime*, vol. 30, no. 1, pp. 97–113, 2023, doi: 10.1108/JFC-09-2021-0218.

[55] J. Abadi and M. Brunnermeier, "Blockchain economics," Nat. Bur. Econ. Res., Cambridge, MA, USA, Tech. Rep. 25407, 2018. [Online]. Available: https://www.nber.org/papers/w25407

[56] F. A. T. Force, "Guidance for a risk-based approach to virtual assets and virtual asset service providers," Jun., 2019. [Online]. Available: www.fatfgafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

[57] R. Barone and D. Masciandaro, "Cryptocurrency or usury? Crime and alternative money laundering techniques," *Eur. J. Law Econ.*, vol. 47, no. 2, pp. 233–254, 2019.

[58] M. D. Murray, "Ready lawyer one: Lawyering in the metaverse," *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.4082648.

[59] A. Y. Bokovnya, A. A. Shutova, T. G. Zhukova, and L. V. Ryabova, "Legal measures for crimes in the field of cryptocurrency billing," *Utopía y Praxis Latinoamericana*, vol. 25, no. 7, pp. 270–275, 2020.

[60] F. M. J. Teichmann and M.-C. Falker, "Cryptocurrencies and financial crime: Solutions from Liechtenstein," *J. Money Laundering Control*, vol. 24, no. 4, pp. 775–788, 2020, doi: 10.1108/JMLC-05-2020-0060.

[61] Liechtenstein, "Liechtenstein: Parliament adopts blockchain act," 2019, [Online]. Available: https://www.loc.gov/item/global-legal-monitor/2019-10-30/liechtenstein-parliament-adopts-blockchain-act/

[62] J. Benet, "IPFS-content addressed, versioned, p2p file system," 2014, *arXiv:1407.3561*.

[63] S. Wu et al., "DeFiRanger: Detecting price manipulation attacks on DeFi applications," 2021, *arXiv:2104.15068*.

[64] S.-H. Wang, C.-C. Wu, Y.-C. Liang, L.-H. Hsieh, and H.-C. Hsiao, "ProMutator: Detecting vulnerable price oracles in DeFi by mutated transactions," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, 2021, pp. 380–385.

[65] K. Qin, L. Zhou, B. Livshits, and A. Gervais, "Attacking the DeFi ecosystem with flash loans for fun and profit," in *Proc. Financial Cryptogr. Data Secur.*, 2021, pp. 3–32.

[66] Chainalysis, "The chainalysis state of web3 report," 2022. [Online]. Available: https://go.chainalysis.com/2022-web3-report.html

[67] P. Zheng, Z. Zheng, J. Wu, and H.-N. Dai, "XBlock-ETH: Extracting and exploring blockchain data from ethereum," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 95–106, 2020.

[68] Z. Wu, J. Liu, J. Wu, and Z. Zheng, "Transaction tracking on blockchain trading systems using personalized PageRank," 2022, *arXiv:2201.05757*.

[69] D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "Modeling and understanding Ethereum transaction records via a complex network approach," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 67, no. 11, pp. 2737–2741, Nov. 2020.

[70] J. B. Cho, S. Serneels, and D. S. Matteson, "Non-fungible token transactions: Data and challenges," *Data Sci. Sci.*, vol. 2, 2022, Art. no. 2151950.

[71] S. Serneels, J. B. Cho, and D. S. Matteson, "Data containing transaction history and visual traits of eight highly valued non-fungible token (NFT) collections," 2022. [Online]. Available: https://ecommons.cornell.edu/handle/1813/111404

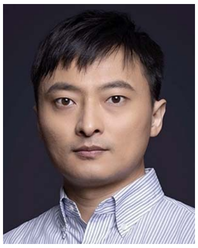
[72] I. Salami, "Challenges and approaches to regulating decentralized finance," *AJIL Unbound*, vol. 115, pp. 425–429, 2021, doi: 10.1017/aju.2021.66.

JIAJING WU (Senior Member, IEEE) received the Ph.D. degree from The Hong Kong Polytechnic University, Hong Kong, in 2014. In 2015, she joined Sun Yat-sen University, Guangzhou, China, where she is currently an Associate Professor. Her research interests include blockchain, graph mining, and network science. Dr. Wu was the recipient of the Hong Kong Ph.D. Fellowship Scheme during her Ph.D. in Hong Kong from 2010 to 2014. She is also an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II: EXPRESS BRIEFS.

KAIXIN LIN received the B.Eng. degree from the School of Computer Science, South China Normal University, Guangzhou, China, in 2022. She is currently working toward the M.Sc. degree with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China. Her research interests include blockchain, smart contracts, and graph mining.

DAN LIN (Graduate Student Member, IEEE) received the B.Eng. in software engineering from Sun Yat-sen University, Guangzhou, China, in 2019. She is currently working toward the Ph.D. degree with the School of Software Engineering, Sun Yat-sen University. Her research interests include blockchain, cryptocurrency, theories and applications of network science, and anti-money laundering.

ZIYE ZHENG is currently working toward the B.Eng. degree from the School of Software Engineering, South China Normal University, Foshan, China. He is a Research Assistant with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China. His research interests include blockchain, cryptocurrency, and graph mining.



HUAWEI HUANG (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from The University of Aizu, Aizuwakamatsu, Japan, in 2016. He is currently an Associate Professor with Sun Yat-Sen University, Guangzhou, China. He was a Research Fellow with the Japan Society for the Promotion of Science, and an Assistant Professor with Kyoto University, Kyoto, Japan. His research interests include blockchain and distributed computing. He is also the Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and IEEE OPEN JOURNAL OF THE COMPUTER SOCIETY, Operation-Committee Chair of the IEEE Symposium on Blockchain at IEEE Services 2021, and TPC Co-Chair of Globecom’2021/ICC’2022 Workshop on Scalable, Secure, and Intelligent blockchain.

ZIBIN ZHENG (Fellow, IEEE) is currently a Professor anda Deputy Dean with the School of Software Engineering, Sun Yat-sen University, Guangzhou, China. He has authored or coauthored more than 200 international journal and conference papers, including one ESI hot paper and six ESI highly cited papers. According to Google Scholar, his papers have more than 15000 citations. His research interests include blockchain, software engineering, and services computing. He was the BLOCKSYS’19 and CCOLLABORATECOM16 General Co-Chair, SC2’19, ICIOT18 and IOV14 PC CoChair. He was the recipient of several awards, including the Top 50 Influential Papers in Blockchain of 2018,ACM SIGSOFT Distinguished Paper Award at ICSE2010, Best Student Paper Award at ICWS2010.