Unravelling Token Ecosystem of EOSIO Blockchain

Zigui Jiang, *Member, IEEE*, Weilin Zheng, Bo Liu, Hong-Ning Dai, *Senior Member, IEEE*, Haoran Xie, *Senior Member, IEEE*, Xiapu Luo, *Senior Member, IEEE*, Zibin Zheng, *Fellow, IEEE*, and Qing Li, *Fellow, IEEE*

Abstract—Being the largest Initial Coin Offering project, EOSIO has attracted great interest in cryptocurrency markets. Despite its popularity and prosperity (e.g., 26,311,585,008 token transactions occurred from June 8, 2018 to Aug. 5, 2020), there is almost no work investigating the EOSIO token ecosystem. To fill this gap, we are the first to conduct a systematic investigation of the EOSIO token ecosystem by conducting a comprehensive graph analysis of the entire on-chain EOSIO data (nearly 135 million blocks). We construct token-creator graphs, token-contract creator graphs, token-holder graphs, and token-transfer graphs to characterize token creators, holders, and transfer activities. Through graph analysis, we have obtained many insightful findings and observed some abnormal trading patterns. Moreover, we propose a fake-token detection algorithm to identify tokens generated by fake users or fake transactions and analyze their corresponding manipulation behaviors. Evaluation results also demonstrate the effectiveness of our algorithm.

Index Terms—Blockchain, EOSIO, Token, Fake-Token Detection, Graph Analysis

1 Introduction

Cryptocurrencies such as Bitcoin [1] and Ethereum [2] have received great interest from investors and researchers [3]–[5]. As an underlying technology, blockchain has essentially established a distributed database with characteristics like traceability, security, and immutability [6]. Meanwhile, smart contracts running on top of blockchains can automate business processes, simplify trading actions, and reduce administrative costs [7]–[10]. However, blockchains like Bitcoin and Ethereum suffer from a low transaction throughput due to inefficient consensus protocols [11], [12], like Proof-of-Work (PoW). Thus, they are incapable of supporting real-time trading services.

Similar to Ethereum, EOSIO[1] is an open-source platform for blockchain innovation and performance. In contrast to PoW-based blockchain systems [13], [14], EOSIO adopts a more efficient consensus protocol – Delegated Proof-of-Stake (DPoS) [15], [16]. It allows EOSIO to achieve much higher transaction throughput (up to 8,000 transactions per second) and much lower confirmation latency (within one second) than Bitcoin and Ethereum [17]. Consequently, EOSIO has become an attractive option for many decentralized applications (DApps), especially for applications having a stringent requirement on trading time. According to *Crowdfundinsider* [18], EOSIO has become one of the largest Initial Coin Offering (ICO) projects (over $4 billion). A recent report indicates that the average transaction volume of EOSIO within 24 hours has reached 57 million (80 million at peak) [19]. By comparison, Ethereum has an average volume of only 717,000 transactions (1.3 million at peak) within 24 hours.

ICO has become a new approach for many startups to raise funds. Different from traditional angel finance or venture capital, an ICO issuer raises cryptocurrencies by selling blockchain-based digital assets to users. In this way, cryptocurrencies can be interchanged with fiat money, consequently boosting the cryptocurrency economy. During this process, digital assets, also called *tokens*, act as the programmable assets or access rights of participants in the blockchain. Tokens are essentially managed by smart contracts and underlying blockchains. Owing to the high liquidity brought by the high transaction throughput and low confirmation latency, EOSIO tokens have become one of the most ideal choices for ICOs. Meanwhile, the waiver of trading fees in EOSIO is another attractive feature to stakeholders (e.g., token issuers and holders).

1.1 Motivation

Surprisingly, there are few studies on the cryptocurrencies of EOSIO, considering its huge token transaction volume (i.e., more than 26.3 billion). An in-depth investigation of the EOSIO token ecosystem can help to reveal its internal

- *Zigui Jiang and Zibin Zheng are with the School of Software Engineering, Sun Yat-sen University, Zhuhai 519082, China. Email: {jiangzg3, zhzibin}@mail.sysu.edu.cn.*
- *Weilin Zheng and Bo Liu are with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510006, China. Email: {zhengwlin, liub76}@mail2.sysu.edu.cn.*
- *Hong-Ning Dai is with the Department of Computer Science, Hong Kong Baptist University, Hong Kong. Email: hndai@ieee.org.*
- *Haoran Xie is with the Department of Computing and Decision Sciences, Lingnan University, Hong Kong. Email: hrxie@ln.edu.hk.*
- *Xiapu Luo and Qing Li are with the Department of Computing, Hong Kong Polytechnic University, Hong Kong. Email: {csxluo, csqli}@comp.polyu.edu.hk.*

This work was supported by the Guangdong Basic and Applied Basic Research Foundation (2023A1515011336), the Faculty Research Grants (DB22B7, DB23B2, and DB24A4) of Lingnan University, Hong Kong, and the Hong Kong RGC Project (No. PolyU15224121). (Corresponding author: Hong-Ning Dai.)
Digital Object Identifier

1. https://eos.io/

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381

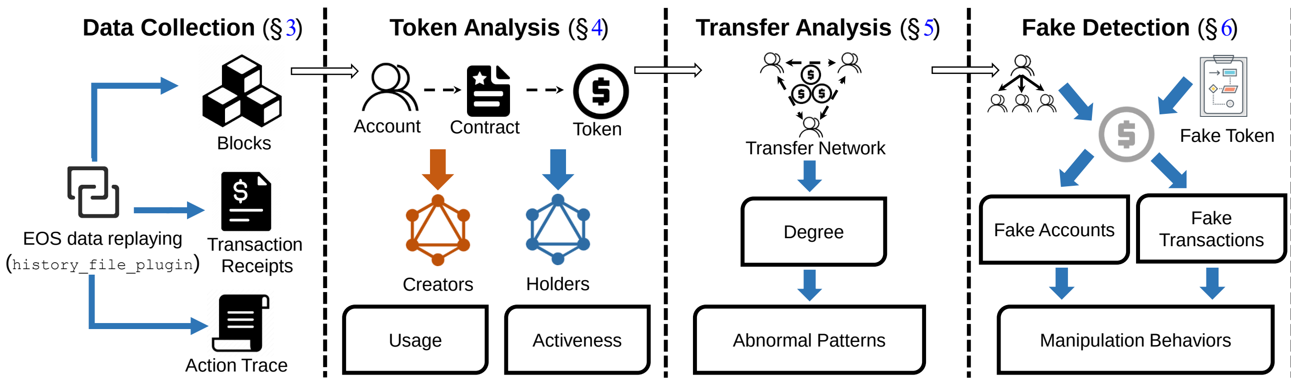


Fig. 1. An overview of the proposed framework to analyze EOSIO token data

mechanism and understand economic activities in EOSIO so as to demystify the token ecosystem. To the best of our knowledge, there is *no work to comprehensively investigate the EOSIO token ecosystem*, despite a myriad of studies on EOSIO smart contracts [20], [21], EOSIO vulnerabilities [22], and the Ethereum tokens [23]–[28] (a more comprehensive literature survey to be given in Section 8).

To fill this gap, we conduct a systematic study on the EOSIO token ecosystem by performing extensive graph analysis on the entire on-chain EOSIO data. As shown in Fig. 1, our study consists of four phases: (1) we collect the data of EOSIO and parse the token-related datasets; (2) we investigate the token ecosystem by constructing token creator graphs (TCGs), token contract creator graphs (TCCGs), and token holder graphs (THGs); (3) we analyze abnormal trading patterns by constructing token transfer graphs; and (4) we propose an algorithm to detect suspicious tokens generated by fake users or fake transactions and analyze their corresponding manipulation behaviors.

1.2 Contributions

In summary, we make the following contributions.

1) To the best of our knowledge, we are the first to conduct a holistic measurement study on the whole EOSIO token ecosystem via graph analysis. After synchronizing the entire EOSIO data and gathering a large-scale dataset of all token-related transactions, we construct multiple graphs to characterize token creators, token contract creators, and token holders. The graph analysis offers an in-depth exploration of the entire EOSIO token ecosystem. We also compare EOSIO with Ethereum in token ecosystems.
2) After conducting the exploratory graph analysis, we analyze the tokens-transfer flows and observe some anomalous behaviors done by the accounts having large indegree or outdegree. These findings help us to identify abnormal trading patterns in EOSIO.
3) We propose a fake-token detection algorithm to detect "*fake*" tokens and identify manipulation behaviors. We extract several abnormal tokens and reveal their abnormal behaviors. Evaluation results further demonstrate the effectiveness of the algorithm.

The rest of the paper is organized as follows. After reviewing EOSIO and its internal mechanism in Section 2, we detail our study design and data collection in Section 3. Section 4 then provides an overview of the EOSIO token ecosystem based on graph analysis. Section 5 next investigates the token transfer flows and identifies some abnormal trading patterns. For further analysis of the characteristics of the EOSIO token ecosystem, we compare the analysis results of EOSIO with those of Bitcoin, Ethereum, and even EOSIO itself in Section 6. Section 7 depicts the fake-token detection algorithm to identify the "*fake*" tokens. After reviewing related work in Section 8, we conclude the paper and outline future directions in Section 9.

2 EOSIO IN A NUTSHELL

2.1 Blockchain and EOSIO

In general, a typical blockchain [29], [30] is a globally shared and distributed database, which is composed of a series of blocks containing transactions. A transaction refers to the interactive operation between users. Meanwhile, a block is constructed by transactions. Each block is confirmed by the entire network through a consensus protocol, such as PoW, PoS, and DPoS [11], [12], [31]. Participants in a blockchain system can read and write transactions in the blockchain database. There is no central authority in the blockchain. All the transactions are determined by the consensus protocol in a decentralized manner. As the core of blockchain technologies, the consensus protocol plays an important role in the development of the blockchain ecosystem.

As two main blockchain platforms, both Bitcoin and Ethereum are limited by PoW consensus protocols [13], [32]. For example, Bitcoin only supports seven transactions per second while Ethereum supports 15 transactions per second. Different from Bitcoin and Ethereum, EOSIO adopts a more efficient consensus - DPOS - to scale the throughput to millions of transactions per second. Owing to its high scalability, EOSIO has gained huge popularity among users and developers. Another attraction of EOSIO to investors is the waiver of trading fees for any transactions, thereby greatly reducing the expenditure of high-frequency trading (such as arbitrage) for investors.

The working flow of EOSIO is summarized as follows. 1) A *user* first registers an EOSIO account, which can uniquely determine its identity. 2) The user interacts with the EOSIO blockchain through the invocation of smart contracts. The interaction is called an *action* in EOSIO [33]. 3) An EOSIO *smart contract* written in C++ consists of contractual clauses, which can be invoked to be executed in EOSIO virtual machine (EOSVM) [34], consequently generating a number of transactions to be stored in the EOSIO blockchain. 4) An EOSIO *transaction* contains specific information about one or multiple users' actions, e.g., transferring tokens from one user to another.

2.2 Transaction, Action, and Account

An EOSIO transaction consists of several actions, each representing an *atomic* operation [33]. Like traditional distributed database systems, the atomicity of a transaction means an indivisible set of actions in one transaction, i.e., either all of them are successful or none of them are successful. For example, a user namely Alice initiates an action consisting of (a) creating a new token named "TEST" and (b) transferring 10.0000 EOS[2] to Bob. Both *actions* (a) and (b) should occur either at the same time or none of them occurs. Both two actions are packaged into one transaction to be submitted to the EOSIO blockchain. As long as one of the actions fails, the entire transaction fails.

In EOSIO, a transaction is submitted by an account represented by a string with a length of up to 12 characters. Creating a new account in EOSIO requires an existing account to pay a certain amount of EOS for RAM resources to store the account information. The existing account can be considered as the creator of the new account. Different from EOSIO, a new account (address) creation in Ethereum does not require the help of other accounts. This account-creation mechanism implies stronger relationships of EOSIO accounts than Ethereum. Therefore, it is worth investigating the relationships between EOSIO accounts while previous studies on Ethereum often ignore the relationship analysis. In Section 7, we propose an algorithm to detect "*fake*" tokens and analyze the relationships of EOSIO accounts.

2.3 Smart Contract and Token

Nowadays, most blockchain systems support smart contracts that run on virtual machines. Like other blockchain systems such as Ethereum, EOSIO smart contracts are also executed on top of EOSVM. In EOSIO, a smart contract written in C++ is first compiled into WebAssembly machine code (aka bytecode), which is then executed in EOSVM. Unlike Ethereum equipped with a *gas* mechanism, EOSIO adopts a different resource-management mechanism, which limits the *RAM*, *CPU* and *Bandwidth* resources for transaction execution to solve the *halting problem* [33], [35]. In EOSIO, an account can act as both a common user and a contract at the same time. When created, an account first acts as a common user. Authorized by its private key, it can interact with the blockchain on behalf of the user, such as sending tokens to other accounts. When this account is used to deploy a contract, the bytecode is stored in the account, which also serves as a contract. When a user invokes the contract, he/she initiates actions to the account. Consequently, the corresponding bytecode is executed in EOSVM to change the states of the blockchain. It is worth noting that the bytecode of an account can be updated (as long as owning its private key) in EOSIO, which is nevertheless not allowed in Ethereum.

2. EOS is the token of EOSIO, similar to ether in Ethereum and BTC in Bitcoin.

TABLE 1
Several important mathematical notations

Notations	Description
TCG	Token Creator Graph
$V_{\mathtt{at}}$	The set of accounts and tokens for TCG
$E_{\mathtt{at}}$	The set of edges for TCG
(v_i, v_j, d)	An edge that indicates the creation relationship between an account v_i and a token v_j with a timestamp d
TCCG	Token Contract Creator Graph
THG	Token Holder Graph
$V_{\mathtt{th}}$	The set of tokens and holders for THG
$E_{\mathtt{th}}$	The set of edges for THG
(v_i, v_j, w)	An edge that indicates the holding relationship between a holder v_i and a token v_j with a weight w
TTG	Token Transfer Graph
$V_{\mathtt{tt}}$	The set of the token holders for TTG
$E_{\mathtt{tt}}$	The set of edges for TTG
CTTG	Center Token Transfer Graph
$V_{\mathtt{ct}}$	The set of the top-14 accounts for CTTG
$E_{\mathtt{ct}}$	The set of edges for CTTG
ACG	Account-creation Graph
ACF	The Account Control Factor for a token
ANF	Action Number Factor to further model `transfer` actions.
TANF	Total Action Number Factor for a token T_k
ATTNF	An indicator to measure whether a token is "*fake*"
TTQF	Token Transfer Quantity Factor
MTTQF	An indicator considering both the account-creation relationship and transfer amount

In EOSIO, developers can easily use smart contracts to build their projects or DApps. Due to the waiver of trading fees and the simple development process of EOSIO DApps, many startups and ICOs raise funds by creating and issuing new tokens on the EOSIO platform. Any user can buy certain tokens of ICO DApps with EOS[2], which is the native token of EOSIO. A token that acts like a digital currency becomes a profitable asset for those shareholders of DApps. When the EOSIO *mainnet* went live, a standard token protocol was introduced. As a result, the EOSIO token ecosystem has prospered rapidly and has soon become one of the largest token-selling platforms. Required by the EOSIO token standard, a token contract should consist of three functions: `create`, `issue`, and `transfer`. Using this condition, we can filter all standard token contracts on the EOSIO *mainnet*. If we parse the token-related transactions, we then can know how the tokens are transferred, where they go, and by whom they are held. It is worth mentioning that a token contract in EOSIO can create multiple tokens with different symbols and different contracts can create tokens with the same symbol. By contrast, this feature is also not allowed in Ethereum. Therefore, we uniquely mark a token with "*contract@symbol*" in EOSIO.

3 Study Design & Data Collection

This section gives a brief introduction to the research questions, study methods, and how the data are collected. Moreover, several important mathematical notations of study methods are summarized in Table 1.

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381

TABLE 2
EOSIO Token Data: Block #1 to #134,999,999

Category	Approximate size of Dataset	Row Count
token create actions	944 KB	5,598
token issue actions	40.42 GB	253,711,757
token transfer actions	4.23 TB	26,311,585,008
account creation actions	244.62 MB	1,332,669

3.1 Research Questions & Study Methods

In this paper, we aim to answer the following three research questions (RQs) when investigating the EOSIO token ecosystem.

RQ1) **What are the market characteristics of the EOSIO token ecosystem?** The EOSIO token ecosystem has huge market value due to its popularity and massive transactions. However, as far as we know, there is no study investigating market characteristics by exploratory analysis of the EOSIO token data. To this end, we conduct a comprehensive graph analysis on tokens, holders, and creators by constructing token creator graphs (TCGs), token holder graphs (THGs), and token contract creator graphs (TCCGs), respectively, accompanied by the relationship analysis.

RQ2) **Are there anomalous trading activities in the EOSIO token ecosystem?** Tokens transferred in EOSIO reveal the trading flows, which can be used to identify trading activities, especially for those anomalous trading activities that may be a detriment to the EOSIO ecosystem. After analyzing token transfer graphs (TTGs) and characterizing the features, we find that some "*center*" accounts have many `transfer` actions. We then analyze mutual trading activities and detect abnormal trading patterns.

RQ3) **Can we identify the tokens with fake users and transactions?** Although millions of token-related transactions occur in EOSIO, fake users or transactions commonly appear in EOSIO. Due to the waiver of trading fees of EOSIO, many token issuers intentionally increase both trading and user volumes of tokens with nearly no extra cost, thereby boosting the token popularity and gaining extravagant profits. To address this problem, we design an algorithm to detect these "*fake*" tokens. We find that some identified cases can effectively reveal the manipulation behaviors of tokens.

3.2 Data Collection

The collection of all the token-related actions requires replaying all transactions and gathering a large-scale dataset of all actions. However, the large transaction volume of EOSIO poses challenges in replaying transactions and efficiently obtaining the entire on-chain data. Although the EOSIO development team offers the client `Nodeos` and several plugins, like `state_history_plugin` and `mongo_db_plugin`, the official plugins severely slow down the replay procedure due to parsing and insertion operations of raw data to databases. These plugins collect the raw data when replaying transactions, and then parse them into the well-formatted data for some database engines (i.e., PostgreSQL and MongoDB). Finally, the formatted data are inserted into the database according to certain indexes (with the purpose of the fast query). Data insertion operations take extra time during the replaying procedure. Meanwhile, data parsing and insertion operations are conducted serially and may affect each other, thereby further slowing down the replaying procedure.

To address these challenges, we develop a new data-replaying plugin - `history_file_plugin` to collect raw data and write them into *Memory Buffer* during the replaying procedure. Then, another thread asynchronously reads the data from *Memory Buffer*, serializes, and finally saves them directly as JSON files. Since the subsequent data preprocessing is conducted on these files without affecting the replaying procedure, `history_file_plugin` allows data collection and data processing to be carried out simultaneously, consequently speeding up data collection. Our plugin greatly saves time in collecting the entire on-chain data in contrast to the official plugins of EOSIO. For example, our plugin takes only 1/7 time to synchronize the first 20 million blocks, compared with the official plugins of EOSIO[3].

EOSIO Token Data Summary: We have launched *Nodeos* and our own *history_file_plugin* to run an EOSIO full node and replay all the transactions (up to 134,999,999 blocks) to get the entire on-chain data (including blocks, transaction receipts, action traces) from June 8, 2018 to Aug. 5, 2020. According to the token standard defined by EOSIO, we filter out all standard tokens and extract the token-related actions covering creation, issuance, and transfer. Table 2 summarizes the EOSIO token data, which obviously has much larger volumes than Ethereum [36]. More details about the dataset are shown below.

Token Information: In EOSIO, a contract that contains three standard functions of `create`, `issue`, and `transfer` can be regarded as a standard token contract. According to this feature, we filter out 2,047 contracts to be considered as

3. Our plugin is expected to obtain even better results than the official plugins for the entire EOSIO dataset because of no insertion operations to databases.

TABLE 3
Token Transfer Format

Category	Description	Data
txid	transaction id	07fc627668a471c3d...
block_time	block timestamp	2018-06-10T14:23:39.000
contract@symbol	the token contract and token symbol	eosnowbanker@EOSNOW
from	token sender	eosnowbanker
to	token receiver	gqztamzsg4ge
quantity	the amount of token	10000.0000 EOSNOW
memo	transfer memo	Now is now Now

TABLE 4
Account Creation Format

Category	Description	Data
txid	transaction id	245786e9d77657a5e...
block_time	block timestamp	2018-06-12T17:05:16.500
creator	the name of the creator	hezdqmbygyge
name	the new account name	iloveuzi3344

standard token contracts, which have created and issued 5,598 types of tokens. For these 5,598 tokens, we collect the data including `create` actions, `issue` actions, and `transfer` actions for each token. A `create` action represents that a user creates a token through a token contract. An `issue` action represents that an issuer issues some tokens to a user directly (also known as Token `Airdrop`), while a `transfer` action represents that a user sends some tokens to another user. There are 253,711,757 token `issue` actions that were submitted by 2,140 issuers and 26,311,585,008 token `transfer` actions that occurred in 1,332,669 holding accounts. Table 3 illustrates an example of a `transfer` action for helping readers further understand the format of the dataset. And the format of the other two actions is simple and similar to that of the `transfer` action.

Account Information: In EOSIO, creating a new account requires an existing creator to pay a certain amount of EOS. There are 2,096,840 distinct accounts, which were created by only 48,691 account creators. We filter out all account creation actions and extract their relationship as the format shown in Table 4.

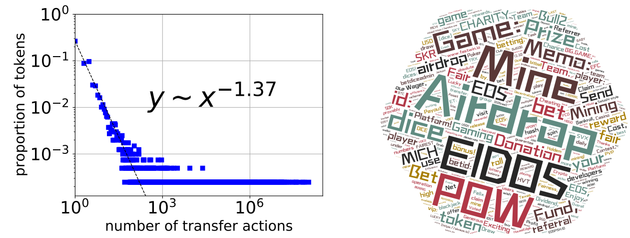
4 Token Analysis

In this section, we provide an overview of the EOSIO token ecosystem. We concentrate our study on the tokens and explore the characteristics of the token ecosystem. Based on the analysis, we obtained the following findings.

- **Finding 1**: Despite a huge volume of token `transfer` actions (exceeding 26.3 billion), most of the tokens are "*silent*". Specifically, nearly 80% of the tokens are traded less than 100 times and only 1% of the tokens cover more than 90% of the total token volume.
- **Finding 2**: Tokens can be created by an account through one or multiple contracts. Some accounts create a large number of tokens through one contract possibly because of testing or "just for fun". On the contrary, few creators create multiple tokens through multiple contracts.
- **Finding 3**: A small number of accounts (might be some exchanges) hold a large number of tokens while most accounts hold a small number of tokens. Similarly, most tokens are held by a small number of holders while only a small number of holders have a large number of tokens.

4.1 Token Activeness and Token Usage

As an important measure of the health of the token ecosystem, the degree of the *token activeness* reveals the network status and the availability of the ecosystem. We first define the *token activeness* of a token as the number of its `transfer` actions. This metric has been used as an important indicator for ranking in many DApp websites (e.g., DappReview). We then plot the distribution of the token activeness in Fig. 2(a),



(a) Distribution of token activeness (b) Word cloud of memos

Fig. 2. Token activeness and usage

from which the *Matthew effect* [37] can be observed. Nearly 27.9% of the tokens have never been transferred, and 78.9% of the tokens are transferred less than 100 times. Meanwhile, 1% of the tokens cover more than 90% of the total volume, thereby further confirming the existing Matthew effect. This result indicates that most tokens do not succeed from the perspective of users' activity. In other words, there are only a few *active* tokens while most of them are *silent*. To further analyze the token activeness, we plot the fitted line for the distribution through $y{\sim}x^{-\beta}$ as shown in Fig. 2(a). The larger β leads to a smaller degree of token activeness.

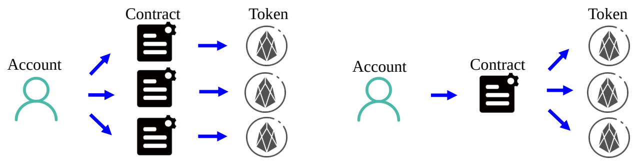
TABLE 5
Top-5 Tokens according to Token Activeness

Tokens	No. of `transfer` actions	Identities
eidosonecoin@EIDOS	23,484,345,961	Airdrop for DDoS attack
eosiopowcoin@POW	1,793,696,754	CPU Mining
betdicetoken@DICE	103,865,132	BetDice, Gambling Game
bgbgbgbgbgbg@BG	74,043,095	BigGame, Gambling Game
mine4charity@MICH	67,464,460	CPU Mining

Table 5 lists the Top-5 most active tokens. We find that `EIDOS` is the most active token with up to 23 billion `transfer` actions. According to "Blocking.net", `EIDOS` leads to a token `airdrop` feast aimed at exposing the defects of EOSIO's resource management and even "*killing*" EOSIO [38]. Anyone who transfers 0.0001 EOS to contract `eidosonecoin` can then receive 0.0001 EOS as well as some EIDOS tokens from `eidosonecoin`. To gain more EIDOS tokens, many users submitted a large number of `transfer` actions to `eidosonecoin`, thereby consuming substantial CPU resources. At the peak, the CPU resources consumed by `eidosonecoin` occupy 60% of the entire network according to DAppTotal [39], consequently causing users to be unable to transfer money normally and leading to the dysfunction of other DApps. This abnormal behavior can be regarded as a DDoS attack on the EOSIO `mainnet`. `POW` and `MICH` have a similar operating model (commonly known as CPU Mining) to `EIDOS`. All these projects caused some harm to EOSIO's resource management. Acting as tokens for gambling games, both `DICE` and `BG` have been operating gambling markets since September 2018. From the popularity of these two tokens, we speculate the popularity of *gambling and gaming* in EOSIO owing to the waiver of trading fees of EOSIO in contrast to other blockchain platforms.

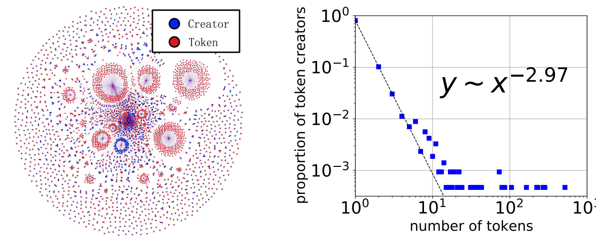
It is difficult to verify the functionality of each token since most tokens do not have any relevant information except for some well-known ones. Thus, we go through all the `transfer` actions of each token and collect the *memo*

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381



(a) One contract creates one token (b) One contracts creates multiple tokens

Fig. 3. Relationship between accounts and tokens



(a) TCG (b) Outdegree distribution of TCG

Fig. 4. Visualization of Token Creators (TCG)

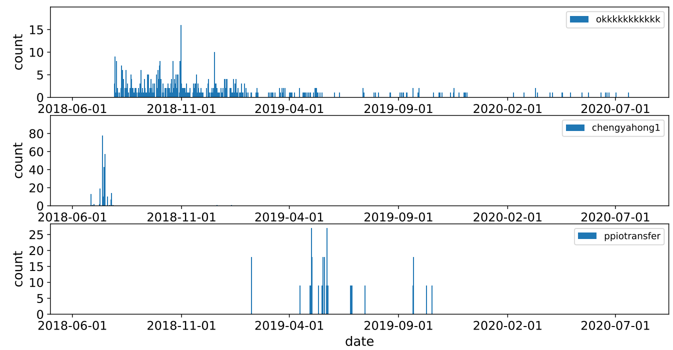


Fig. 5. Distribution of token creation over time

of each action. These memos usually imply the purposes of the actions (e.g., betting) and the potential identities of the *senders*. Fig. 2(b) depicts the word cloud of the memos of EOSIO tokens. The most common word is "`Airdrop`", indicating that the token `airdrop` occurs the most frequently in EOSIO. Meanwhile, the words "`EIDOS`", "`POW`", "`Mine`" indicate the prevalence of CPU Mining. Other frequent words include "`Bet`", "`Game`", "`Prize`" (related to gambling and game actions), further confirming the huge popularity of both gambling apps and games in EOSIO.

4.2 Token Creators

Different from Ethereum, in which one token contract can create only one token, a contract in EOSIO can create one or multiple tokens, as shown in Fig. 3. In the first case, an account is able to deploy one token contract, which can be invoked to create multiple tokens, as shown in Fig. 3(a). Thus, a contract in EOSIO can be reused for token creation. In the second case, an account can create multiple tokens through multiple contracts, as shown in Fig. 3(b). EOSIO allows different contracts to create tokens with the same name (symbol) while Ethereum disallows this feature.

To investigate the relationships between tokens and accounts, we focus on the number of tokens created by each account. We introduce TCG to investigate token creators as follows:

$$\mathsf{TCG} = (V_{\text{at}}, E_{\text{at}}, D), E_{\text{at}} = \{(v_i, v_j, d) | v_i, v_j \in V_{\text{at}}, d \in D\},$$

where V_{at} is a set of accounts and tokens, and E_{at} is a set of edges. Each edge (v_i, v_j, d) indicates the creation relationship between an account v_i and a token v_j with a timestamp d (between June 10, 2018 and Aug. 5, 2020, the same as below). To explore whether there are tokens with the same symbol, we use "*symbol*" instead of "*contract@symbol*" to mark a token node in TCG.

Fig. 4(a) illustrates the TCG constructed from our collected dataset, where creators are marked in blue and tokens are marked in red. We observe from Fig. 4(a) that a small number of accounts create a large number of tokens (i.e., one blue node is circled by many red nodes) while most of the accounts only create one or two tokens. Meanwhile, we also find an abnormal phenomenon, in which one red node is circled by many blue nodes. It can be explained by the fact that the tokens with the same symbol are created by multiple creators. For example, we find that there are 158 tokens named `EOS` being created by 158 accounts through different contracts. One reason why creators prefer the symbol `EOS` may lie in `EOS` being the native token of EOSIO so as to attract more attention. Moreover, some attackers also create the token named `EOS` to initiate the "*fake EOS*" attacks to some vulnerable contracts and steal tokens [22].

To further analyze the characteristics of the TCG, we plot the *outdegree distribution* of creators in Fig. 4(b). The *outdegree distribution* essentially indicates the number of tokens created by the creators. Fig. 4(b) reveals a strong power-law distribution reflecting a small number of nodes with a large outdegree. Moreover, nodes with smaller outdegrees in the token ecosystem account for the majority. For example, nearly 80.6% of the creators only created one token, and 95.7% of the creators created no more than 5 tokens. In addition, the account that created the most number of tokens monopolized 517 tokens, leading to a severe polarization of distribution.

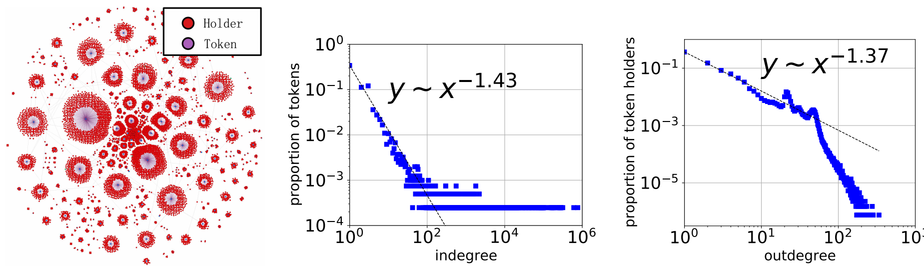
Besides the relationship between tokens and creators (as analyzed in TCG), we next analyze the relationship between tokens and token contracts. We define TCCG as follows:

$$\mathsf{TCCG} = (V_{\text{tc}}, E_{\text{tc}}, D), E_{\text{tc}} = \{(v_i, v_j, d) | v_i, v_j \in V, d \in D\},$$

where V_{tc} is a set of the token contracts and tokens and E_{tc} is a set of edges. An edge (v_i, v_j, d) represents that a token v_i is created by a token contract v_j on timestamp d. TCCG has a similar distribution to TCG, implying that both TCG and TCCG have homologous relationships. A token often has the same account for its creator and its contract (as mentioned in Section 2, an account can act as both a user and a contract). Meanwhile, we also find that creators prefer using the same contract rather than using multiple contracts to create multiple tokens. The reusability of token contracts brings convenience and saves costs since creators do not need to deploy another contract.

Who Creates the Most Types of Tokens? We then concentrate on the accounts that created the most types of tokens and summarize the relevant characteristics of top-3 creators. Account `okkkkkkkkkkk` is the creator with the

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381



(a) THG (b) THG indegree distribution (c) THG outdegree distribution

Fig. 6. Visualization of Token Holders

most number of tokens (517 tokens). By carefully analyzing all actions related to account `okkkkkkkkkkk`, we find that account `okkkkkkkkkkk` usually receives `eosbtextoken@BT` tokens from many accounts and then sends different tokens (e.g., `USDS`, `DNA`, `LOVEYOU`) to these accounts. It implies that `okkkkkkkkkkk` is probably an intermediary between `BT` token and other tokens, thereby providing a decentralized service for token exchange. The second-rank creator `chengyahong1` creates 284 tokens while the third-rank creator `ppiotransfer` creates 270 tokens. Our further analysis shows that both these two creators often issue or send the tokens created by themselves to the same account, implying that they may create tokens for testing or just for fun. To reveal the differences between these creators, we study the distribution of token creation over time after counting the number of tokens created by these three creators every day. As shown in Fig. 5, `okkkkkkkkkkk` has been continuously creating tokens. Account `okkkkkkkkkkk` has tracked the newly initiated projects as well as their tokens and created new tokens and token pairs to meet the needs for the token exchange of ICOs. This further confirms the identity of `okkkkkkkkkkk`, who is a token intermediary. On the contrary, both accounts `chengyahong1` and `ppiotransfer` only sporadically create tokens.

4.3 Token Holders

We further investigate the holders of the tokens and identify their characteristics. To this end, we define and construct THG as follows:

$$\text{THG} = (V_{\text{th}}, E_{\text{th}}, w), E = \{(v_i, v_j, w) | v_i, v_j \in V, w \in (0, 1]\},$$

where V_{th} is a set of tokens and holders, and E_{th} is a set of edges, in which each edge indicates the holding relationship between a holder v_i and a token v_j. Note that each edge is also associated with a weight w, indicating that v_i holds w shares of token v_j.

Fig. 6 presents an exploratory analysis of THG. Fig. 6(a) first gives the visualization of THG, in which the purple nodes denote the tokens and the red nodes denote the holders. Fig. 6(a) reveals that several popular tokens are owned by many holders while most of the tokens are still possessed by very few holders. Figs. 6(b) and 6(c) show the *indegree* and *outdegree distribution* of THG, respectively. The in-degree of a token in THG means the number of its holders while the outdegree of a holder is the number of tokens that he/she holds. We observe an approximate power-law distribution, i.e., there are lots of small-degree nodes while few large-degree nodes.

Who Holds the Most Types of Tokens? Analyzing the *outdegree distribution* of the holders, we find that there are 1,332,669 holders and 35.63% of them hold only one token in the token ecosystem. Moreover, 84.88% of the holders possess fewer than 20 tokens. Table 6 lists the top-3 holders possessing the most number of tokens, and **Invocation** in Table 6 represents the number of `transfer` actions involving a holder, who is either the *sender* or the *receiver*.

TABLE 6
Top-3 Accounts of THG Using Degree Centrality

Accounts	Outdegree	Invocation	Identities
newdexiofees	338	3,873,999	decentralized exchange
5lisqkvt1n2q	284	3,430	token speculator, arbitrageur
iplayeosgame	279	15,803	token speculator, arbitrageur

Account `newdexiofees` that holds the most number of tokens (i.e., 338 tokens) can be considered as the "*king*" of tokens. `newdexiofees` is essentially an exchange initiating a large number of `transfer` actions (3,873,999); this is confirmed by its banner "the first globally decentralized exchange based on EOS"[4]. As for the second-rank account `5lisqkvt1n2q` and third-rank account `iplayeosgame`, they have 284 tokens and 279 tokens, respectively. Interestingly, they also have similar **outdegree** and **invocation**. Moreover, we find that both these two accounts have frequently traded with the exchanges. Thus, we speculate that they may be token speculators who invest in EOSIO tokens to make profits. Different from `5lisqkvt1n2q`, account `iplayeosgame` is also a gambler who frequently interacts with other gambling and gaming DApps.

Which Has the Most Number of Holders? We then analyze the *indegree distribution* of THG. Among 5,598 tokens, 52.47% of them only have one holder, and even 78.62% of tokens have less than 10 holders. We consider some well-known tokens that have many holders and analyze the distribution of daily participants of tokens over time. According to the number of holders, `MPT` is the most popular token possessed by 766,793 holders. As disclosed in DappRadar, `MPT` is essentially a token for the supply chain of the metal packaging industry [40]. The second-rank token is `ZOS` (604,884 holders), which is a new token for the discount e-payment system provided by AirDropsDAC [41]. The third-rank token is `DICE` that has 314,278 holders for *BetDice*, i.e., one of the most famous gambling DApps (aforementioned in Table 5). To explore the popularity of these tokens, we

4. https://newdex.io/

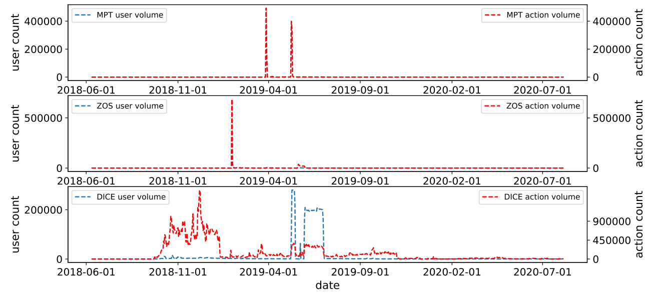


Fig. 7. Daily user and `transfer` action volume

present the daily volume of users and `transfer` actions of top-3 tokens according to time, as shown in Fig. 7.

Although `MPT` and `ZOS` are the top-2 tokens, their user volume and action volume have only sporadically increased (sharply). This phenomenon can be explained by the fact that these tokens (or DApps) have only received sudden attention from the public for a short time. Meanwhile, some ICO projects inject lots of fake users or fake transactions so as to arouse public attention. Section 7 will conduct an in-depth study of this phenomenon. By contrast, there have been many participants continuously interacting with `DICE`, implying that gambling DApps have kept prospering in EOSIO. More interestingly, the user volume of `DICE` does not have the same trend as the action volume. In the early days of `DICE` launch, its user volume was small despite the surged action volume. This implies the importance of evaluating the token popularity from multiple perspectives.

5 Token Transfer Analysis

The exploratory analysis of token creators, holders, and token usage presents an exploration of the EOSIO token ecosystem. We next investigate the token transferring network and identify some abnormal trading patterns. Based on the investigation, we obtained the following findings.

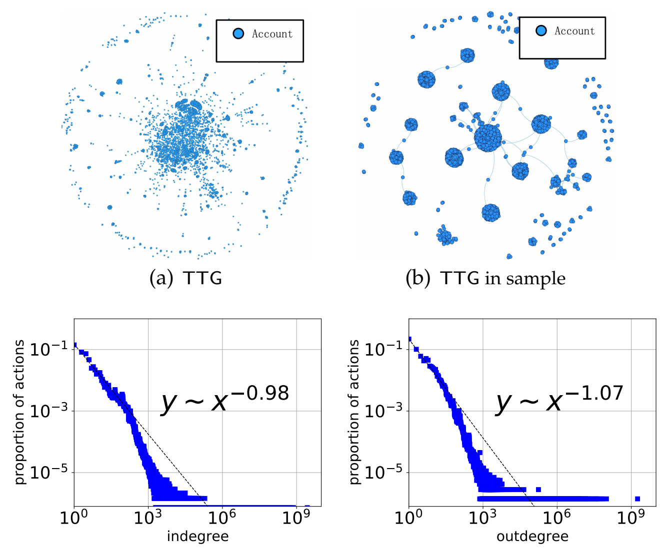
- **Finding 4**: The overall transaction network is relatively sparse while many accounts are clustered together to form multiple sub-networks. The accounts with a large degree are often the center of the closely-connected groups, such as the gambling DApp *BetDice* and the wallet DApp *MykeyPocket*.
- **Finding 5**: Three types of abnormal trading patterns can be found: 1) the "binary" pattern refers to the abnormal users (or investors) trading with each other too many times, 2) the "tree" pattern refers to the abnormal users to trade with several accounts so frequently, and 3) the "grid" pattern refers to the abnormal activities that a DApp involves with so many accounts, which trade with each other so frequently.

5.1 Token Transfer

To study the behavior characteristics of users participating in token transferring, we define the TTG as follows:

$$\mathsf{TTG} = (V_{\text{tt}}, E_{\text{tt}}, w), E_{\text{tt}} = \{(v_i, v_j, w) | v_i, v_j \in V_{\text{tt}}, w \in (0, \infty)\},$$

where V_{tt} is a set of the token holders and E_{tt} is a set of edges. Each edge (v_i, v_j, w) indicates that a holder v_i transfers some tokens to a holder v_j, where w is the total number of `transfer` actions. Hence, TTG is essentially a weighted directed graph. Note that we ignore the type and the amount of the transferred tokens and only count the number of `transfer` actions since different tokens are not comparable. As shown in Fig. 8(a), the overall transaction network is relatively sparse while it contains some closely-connected components (i.e., trading groups). After randomly sampling 10,000 edges from Fig. 8(a), we then reconstruct a sampled TTG as shown in Fig. 8(b). We further observe that many accounts are clustered together to form multiple sub-networks. To have an in-depth understanding of TTG, we further analyze the distribution of *receivers* and *senders*, as depicted in Fig. 8(c) and Fig. 8(d), respectively. In particular, the outdegree of TTG denotes the number of `transfer` actions initiated by a *sender*. The in-degree denotes the number of `transfer` actions ceased at a *receiver*. The approximate degree distributions show that a large number of users keep "silent" in the transferring network. In addition, we find that the accounts with a large degree are often the center of the closely-connected groups as shown in both Fig. 8(a) and Fig. 8(b). We will further study these accounts and find the relationship between them.



(a) TTG (b) TTG in sample (c) Indegree distribution of TTG (d) Outdegree distribution of TTG

Fig. 8. Visualization of Token Transfer

TABLE 7
Top-5 Accounts of TTG Using Degree Centrality

Accounts	Indegree	Outdegree	Identities
eidosonecoin	34,137	23,480,436,814	Token Airdrop
betdicegroup	15,582,144	98,538,083	BetDice, Gambling DApp
betdicehouse	58,671,515	39,645,381	BetDice, Gambling DApp
betdicetoken	78	60,557,132	BetDice, Gambling DApp
mykeypostman	247,895,918	28	MykeyPocket, Wallet DApp

Who is the Most Active in Token Transfer? Table 7 shows the top-5 accounts with the largest degree. Account `eidosonecoin` is the issuer of token `EIDOS` (as mentioned in Table 5), which always sends `EIDOS` to other accounts for `airdrop`. Thus, account `eidosonecoin` has the largest outdegree of 23,480,436,814 but has a smaller indegree of 34,137. All three accounts with a prefix "`betdice-`" belong to a gambling DApp called *BetDice* though some of them have a larger indegree and some of them have a

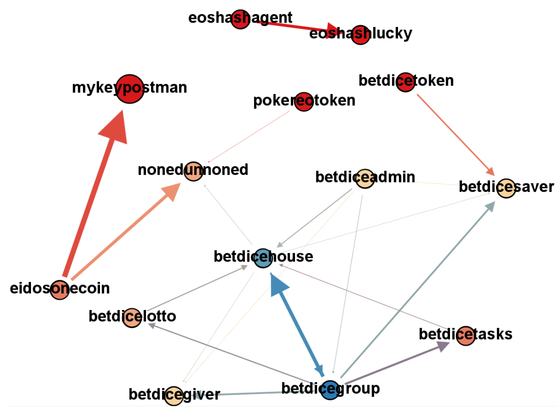


Fig. 9. CTTG

smaller in-degree. This implies that they provide different functions while all working together to constitute the gambling DApp. For example, the account with a larger indegree takes stakes from gamblers while the account with a larger outdegree runs a lottery for gamblers and pays the bonus. Compared with `eidosonecoin`, `mykeypostman` has a larger indegree (247,895,918) and a smaller outdegree. We find that `mykeypostman` is a popular wallet DApp called *MykeyPocket*, which provides users with account-creation services. Since it requires purchasing RAM resources to create accounts in EOSIO, `mykeypostman` also requires payment from users.

5.2 Abnormal Trading Patterns

In blockchain-based platforms and the cryptocurrency market, cryptocurrencies can be used to perpetrate untraceable crypto-asset scams and attempt to defraud investors for ill-gotten gains [42]. Many types of scams, such as Ponzi schemes, Rug pulls, Phishing attacks, fake exchanges, and Giveaway scams, are found and studied [43]. For cryptocurrency scams, the characteristics of their transactions are usually applied to identify abnormal trading behaviors, fake transactions, and fake tokens [44]–[46]. Thus, we attempt to identify some abnormal trading activities and typical patterns based on the token transfer graphs.

We mainly concentrate on the *"center"* accounts in Fig. 8(b) to find abnormal trading patterns. The main reason for focusing on "central" accounts lies in the *relative importance* of "central" accounts than other "peripheral" accounts, where the relative importance of an account can be measured by the Page-Rank algorithm [47]. We first get the top-14 accounts having lots of `transfer` actions and define a *"center"* token `transfer` graph (CTTG) as follows:

$$\mathsf{CTTG} = (V_{\text{ct}}, E_{\text{ct}}, w),$$
$$E = \{(v_i, v_j, w) | v_i, v_j \in V_{\text{ct}}, w \in (0, \infty)\},$$

where V_{ct} is a set of the top-14 accounts and E_{ct} is a set of edges. The definition of each edge is similar to that of TTG. The weight w of each edge represents the number of `transfer` actions, being represented by the thickness of the edge. We can easily find some thick edges in Fig. 9, which can be used to explore abnormal patterns.

According to the connection types of the nodes, we consider several abnormal patterns: 1) "binary" pattern, 2) "tree" pattern, and 3) "grid" pattern. As shown in Fig. 9, `eoshashagent` frequently trades with `eoshashlucky` using many different types of tokens, consequently forming the "binary" pattern. It is abnormal for users (or investors) to trade with each other so many times, especially in a traditional financial market. Meanwhile, `eidosonecoin` in Fig. 9 often sends `EIDOS` to `mykeypostman` and `nonedunnoned`, which also often trades with `pokeneotoken`, thereby forming the "tree" pattern. As discussed in Section 4.1, the `EIDOS` airdrop action can be considered as a DDoS attack. Therefore, both `mykeypostman` and `nonedunnoned` are likely to be accomplices in this attack. Moreover, all the accounts with the prefix "`betdice-`" form the "grid" pattern; all of them belong to a gambling DApp. It is worth mentioning that there is a thick bidirectional link between `betdicegroup` and `betdicehouse`, both of which may serve as the leaders of this gambling DApp. It is abnormal that a DApp involves so many accounts which trade with each other so frequently. We will further investigate whether there are malicious activities like money laundering in such a trading network. In addition, it is also doubtful that all the accounts within the same DApp deliberately increase the transaction volume of tokens to attract huge public attention (like a scam). Further exploration of these abnormal patterns and related arguments will be carried out in future work.

TABLE 8
Row Count Comparison with updated EOSIO Token Data

Category	EOSIO Token Data	Updated Data
token create actions	5,598	4,876
token issue actions	253,711,757	316,886,956
token transfer actions	26,311,585,008	38,794,534,661
account creation actions	1,332,669	3,335,874

6 Comparison

This section compares the analysis results of EOSIO with those of Bitcoin, Ethereum, and even EOSIO itself for a further understanding of the EOSIO token ecosystem. Based on the comparison, we obtain the following findings.

- **Finding 6**: The overall picture of the EOSIO token ecosystem does not show distinct changes in the following two years after Aug. 2020.
- **Finding 7**: There are more differences than similarities between Bitcoin, EOSIO, and Ethereum when comparing their token ecosystems.

6.1 Comparison with EOSIO after 2020

Section 4 and Section 5 analyze the EOSIO token ecosystem based on around two-year EOSIO on-chain data from June 8, 2018 to Aug. 5, 2020. In order to observe whether the EOSIO token transactions change or not, we update the next two-year EOSIO token data[5] from Aug. 2020 to Aug. 2022 (denoted by **Updated Data**) and compare their analytical results. Table 8 compares the row count of the first EOSIO token dataset and the updated dataset. It can be observed that more actions of token issue, token transfer, and account creation occur even though fewer tokens have been created

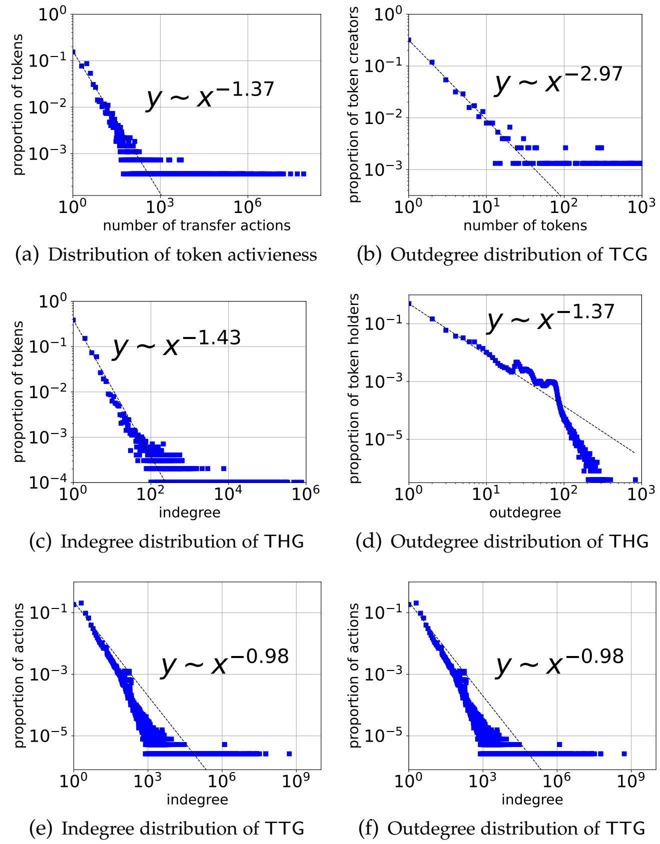
5. The dataset is available viahttps://xblock.pro/#/dataset/43

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381

TABLE 9
Comparison on Top-10 Menos of EOSIO Tokens

June 2018 - Aug. 2020 (meno:count)	Aug. 2020 - Aug. 2022 (meno:count)
Airdrop EIDOS:23,456,588,708	Airdrop EIDOS:33,666,335,356
Mine POW:1,792,980,705	Mine POW:3,115,140,670
Mining airdrop.[1]:65,834,502	'':637,484,993
'':64,983,727	Refund EOS:540,781,878
Prize Fund:55,888,012	n31:47,509,136]
Cost:29,034,211	push.sx:41,380,908
Send to EIDOS Team.:23,848,109	...Gravy Train![3]:33,802,489
for developers:23,398,157	Woot! Woot!:33,757,833
type:cancel-order:22,394,352	Issue GRV:30,314,539
...BG reward..betting.[2]:18,718,683	swap protocol fee:23,461,638

[1] Mining airdrop MICH for CHARITY Donation mining
[2] This is the BG reward for your betting. BIG.GAME
[3] All Aboard the Gravy Train!



(a) Distribution of token activieness (b) Outdegree distribution of TCG (c) Indegree distribution of THG (d) Outdegree distribution of THG (e) Indegree distribution of TTG (f) Outdegree distribution of TTG

Fig. 10. Distribution of Token activeness, Token Creators (TCG), Token Holders (THG) and Token Transfer (TTG) based on EOSIO Token Data after 2020

in the latter two years. In the previous analysis shown in Fig. 2(b), we adopt a word cloud to display the *memo* of EOSIO tokens. Here, we adopt Table 9 to present and compare the frequencies of Top-10 menos in two periods. The left part of Table 9 depicts the same results as Fig. 2(b), and the right part depicts the results after 2020. Comparing two lists of Top-10 menos, we can find that the Top-2 menos are still "`Airdrop EIDOS`" and "`Mine POW`" until two years later.

To further compare the EOSIO token ecosystem in the two-year periods before and after Aug. 2020, we also plot the fitted lines $y{\sim}x^{-\beta}$ for the distributions of Token activeness, Token Creators (TCG), Token Holders (THG) and Token Transfer (TTG) based on the updated dataset, shown in Fig. 10. Comparing Fig. 2(a) with Fig. 10(a), Fig. 4(b) with Fig. 10(b), Fig. 6(b) with 10(c), Fig. 6(c) with Fig. 10(d), Fig. 8(c) with Fig. 10(e), and Fig. 8(d) with Fig. 10(f), we find that the fitted lines shown in every comparison group have similar distributions, i.e., the same $y{\sim}x^{-\beta}$. Therefore, we conclude that the token transactions after 2020 still show the same characteristics as the ones before 2020.

6.2 Comparison with Bitcoin and Ethereum

Although Bitcoin, Ethereum, and EOSIO all provide token creation and transfer, the implementation architectures that support their token ecosystems are completely different. Token actions are external services in Bitcoin since Bitcoin does not natively support tokens. Developers in Ethereum need to write smart contracts to create tokens, while EOSIO provides its token contract called `eosio.token` to achieve token-related actions such as token creation, issuance, and transfer. Considering that both Ethereum and EOSIO are representatives of Blockchain 2.0 while Bitcoin is usually regarded as the symbol of Blockchain 1.0, here we mainly compare the token ecosystem in EOSIO with the one in Ethereum. Further exploration of Bitcoin tokens will be carried out in future work.

Despite several studies [24], [25], [27], [28] on the Ethereum token ecosystem, there are few studies on the EOSIO token system. Through the above analysis, we summarize key similarities and differences between the EOSIO and Ethereum token ecosystems.

Similarities: (1) *The Matthew effect has been observed in both EOSIO and Ethereum* in multiple aspects like token activity, token holders, and token creators. Many tokens and holders keep "silent" in the ecosystem. (2) *Decentralized exchanges (DEX) play an important role in the token ecosystem* [48]. Examples include `newdexiofees` in EOSIO, `Augur` and `EtherDelta` in Ethereum [24]. Token exchange is the most active activity in the ecosystem. Many investors seek arbitrage opportunities in token exchange.

Differences: (1) *The number of tokens in EOSIO is much smaller than that in Ethereum*, because the cost of deploying and maintaining a token contract in EOSIO is high (in terms of substantial resources such as CPU, RAM being staked for users). (2) *One smart contact can create multiple tokens in EOSIO* although this is not allowed in Ethereum. Project parties in EOSIO are in favor of creating multiple tokens using the same contract, possibly saving the cost of token issuance. (3) *Gambling and gaming are the most active activities in the EOSIO token ecosystem*. The reasons lie in the waiver of trading fees and a lower confirmation latency than Ethereum. (4) *The resource-management mechanism in EOSIO is not better than the gas mechanism in Ethereum in terms of security*, and it still has many security flaws, which can be exploited by attackers to attack the ecosystem as mentioned by [49]. For example, the DDoS attack launched by `eidosonecoin@EIDOS` almost exhausted the CPU resources of the EOSIO *mainnet*, resulting in the exceptions of other DApps or tokens. (5) *EOSIO has a much larger transaction volume than Ethereum* despite a smaller number of tokens. The major reason lies in the DPoS consensus protocol and the waiver of trading fees, which also reduces the cost of

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381

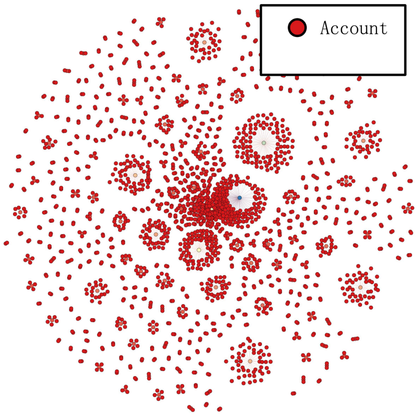


Fig. 11. ACG

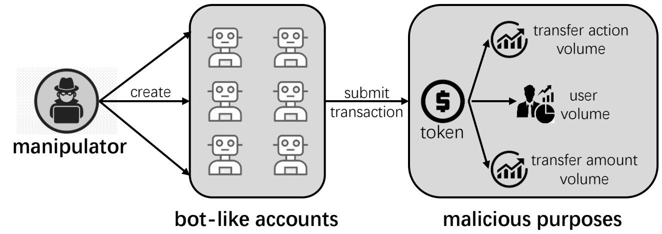


Fig. 12. Malicious Behavior of Token Manipulators

injecting fake transactions/users into DApps or tokens.

7 Fake Token Detection

The exploration of abnormal activities in the token ecosystem implies that some ICO projects and DApps may be rife with fake tokens owned by fake users to either attract sudden popularity or make exorbitant profits. This section aims to detect the "*fake*" tokens and find out how malicious ICO projects and DApps conduct manipulation activities to make their tokens "popular".

7.1 Relationship Between Accounts

We first investigate the account-creation relationship between accounts. Considering that an account *Alice* in EOSIO is created by an existing account *Bob*, we then regard *Bob* as the parent of *Alice*. To describe such a relationship, we define the account-creation graph (ACG) as below:

$$\text{ACG} = (V_{\text{ac}}, E_{\text{ac}}, D), E_{\text{ac}} = \{(v_i, v_j, d) | v_i, v_j \in V_{\text{ac}}, d \in D\},$$

where V_{ac} is a set of the accounts, E_{ac} is a set of edges indicating the creation relationship between these accounts, and an edge (v_i, v_j) represents that a parent account v_i creates a child account v_j on timestamp d. As shown in Fig. 11, the result of ACG shows that there are a few parent accounts that have nevertheless created a large number of children accounts. When further exploring the names of these children accounts, we find a certain similarity and regularity among them. For example, many account names have the same prefix (e.g., "`bnr`", "`gg`") followed by several digits indicating their sequence number (i.e., created sequentially). These results imply that the ICO projects and DApps may adopt similar methods to create and control many fake accounts to frequently interact with their tokens, consequently flourishing their tokens.

7.2 Algorithm

We then propose an algorithm to identify the "*fake*" tokens in the ecosystem. Fig. 12 shows how a manipulator maliciously injects fake users and fake transactions into a token. The manipulator typically creates a large number of bot-like children accounts. He/she then submits transactions through these accounts to interact with the token, with the purpose of rapidly increasing the user volume. At the same time, the manipulator will also try to increase the number of `transfer` actions and the `transfer` amount of tokens to attract public attention. Thus, we model the tokens and their users mainly from two dimensions. One dimension is **Average Token Transfer Number Factor (ATTNF)**, which models the number of `transfer` actions of users of a token. Another dimension is **Max Token Transfer Quantity Factor (MTTQF)**, which models the normalized `transfer` amount of users of a token. Both these two factors consider the account-creation relationship between users, which plays an important role in our algorithm. Our evaluation results also reveal a strong relationship between the token manipulator and its controlled children accounts.

Average Token Transfer Number Factor. Considering that a token manipulator usually controls many accounts, we define the Account Control Factor (ACF) for a token as below:

$$\text{ACF} = \frac{\left|\{\text{holder}_i | i = 1, 2, ..., n\}\right|}{\left|\{\text{parent}_j | j = 1, 2, ..., m\}\right|} \text{ and } m \leq n, \quad (1)$$

where holder_i represents a unique account i who transfers the token and parent_j represents a parent account of holders in the set $\{\text{holder}_i | i = 1, 2, ..., n\}$. For convenience, $\{\text{parent}_j | j = 1, 2, ..., m\}$ and $\{\text{holder}_i | i = 1, 2, ..., n\}$ are abbreviated to $\mathbb{P}$ and $\mathbb{H}$, respectively. ACF is the ratio of the size of $\mathbb{H}$ to that of $\mathbb{P}$. If a token is only transferred by the accounts that have the same parent, it is quite possible that the parent creates a large number of fake children accounts to manipulate transactions, leading to a large ACF.

However, it is not enough to only consider the relationship between the parent and its children accounts, because token manipulators who have created lots of children accounts often have the aim to conduct `transfer` actions including many fake transactions. Hence, we define another factor, Action Number Factor (ANF) to further model `transfer` actions. ANF is defined as follows:

$$\text{ANF}_{\text{holder}_i}^{T_k} = \frac{\text{NUMBER}(\text{holder}_i, T_k)}{\text{NUMBER}(\text{holder}_i, \{T_k | k = 1, 2, ..., z\})}, \quad (2)$$

where $\text{NUMBER}(\text{holder}_i, T_k)$ represents the number of the `transfer` actions on the token T_k initiated by the account holder_i. Set $\{T_k | k = 1, 2, ..., z\}$ represents all tokens held by holder_i and $\text{NUMBER}(\text{holder}_i, \{T_k | k=1,2,...,z\})$ denotes the number of all the `transfer` actions of holder_i on all tokens he/she holds. In other words, if $\text{ANF}_{\text{holder}_i}^{T_k} = 1$, it implies that holder_i is created only for interacting with token T_k. For a token T_k, we get its Total Action Number Factor (TANF) across all its holders as follows:

$$\text{TANF} = \text{ANF}_{\text{holder}_1}^{T_k} + \text{ANF}_{\text{holder}_2}^{T_k} + ... + \text{ANF}_{\text{holder}_n}^{T_k}. \quad (3)$$

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381

To a certain extent, TANF reflects the "loyalty" of users to a token. If TANF is very large, it means that almost all holders of a token only hold and transfer this token forever. It is possible that these accounts are manipulated to increase the transaction volume of the token. TANF that is only evaluated from the behaviors of token holders do not consider account-creation relationships like ACF. Thus, we should consider both ACF and TANF together for each token. One naive method is dividing TANF by $|\mathbb{P}|(|\mathbb{P}|=|\{\text{parent}_j|j=1,2,...,m\}|)$, i.e., TANF/$|\mathbb{P}|$. The smaller $|\mathbb{P}|$ leads to the larger TANF/$|\mathbb{P}|$, implying that this token may be controlled by a few parent accounts. However, this naive method is not optimal due to the following reasons. In EOSIO, there are several wallet DApps that help common users create a large number of accounts. When a token is really popular, many (but not all) accounts whose parent is a wallet DApp will follow to participate ($|\mathbb{P}|$ may be small). This may mistakenly cause a large value of TANF/$|\mathbb{P}|$, consequently leading to some false positives.

To address this issue, we model the behaviors of each parent (using M_{parent_j}) instead of simply counting the number. We finally define the ATTNF for a token as follows:

$$\mathsf{ATTNF} = \frac{\mathsf{TANF}}{\sum_{j=1}^{m} M_{\text{parent}_j}}, \tag{4}$$

where $M_{\text{parent}_j} = \frac{|\{\text{child}_i|i=1,2,...,N\}|}{|\{\text{holder}_i|i=1,2,...,n\}|}$ for each parent account. The set $\{\text{child}_i|i=1,2,...,N\}$ (abbreviated as $\mathbb{C}$) is the total accounts created by parent_j and $\{\text{holder}_i|i=1,2,...,n\}$ denotes the accounts who are created by parent_j and hold the token. Thus, we have the set $\mathbb{C} \subseteq \mathbb{H}$ and $n \leq N$. For a token, we calculate all its M_{parent_j} by dividing $|\mathbb{C}|$ by $|\mathbb{H}|$ and add them up to get $\sum_{j=1}^{m} M_{\text{parent}_j}$. To create a fake token, the manipulator generally exploits almost all of its children accounts to initiate lots of `transfer` actions in a short time. So its M_{parent_j} is nearly equal to 1. On the contrary, the behavior of children accounts of a wallet DApp is more scattered and only partial children accounts interact with the token. Thus, its M_{parent_j} is greater than 1. The sum $\sum_{j=1}^{m} M_{\text{parent}_j}$ is still large when many children accounts of a wallet DApp (whose M_{parent_j} is relatively large) participate in a real popular token, leading to a relatively small ATTNF and alleviating the problem of false positives. Meanwhile, if a token is "*fake*", almost each M_{parent_j} is nearly equal to 1 and $\sum_{j=1}^{m} M_{\text{parent}_j}$ is relatively small, leading to a large ATTNF. To this end, ATTNF is an important indicator to measure whether a token is "*fake*". The larger the ATTNF is, the more likely the token is "*fake*".

Max Token Transfer Quantity Factor. In addition to the number of transactions and the number of holders, the total amount of a token being transferred has also attracted public attention. Thus, we also consider the `transfer` quantity (i.e., the amount of `transfer` actions in EOSIO). To measure it, we first divide holders of a token into multiple account groups, each of which has the same parent. We denote such an account group by $\{\text{holder}_i|i=x,x+1,...,y\}$. We then define the Token Transfer Quantity Factor (TTQF) as follows:

$$\mathsf{TTQF} = \sum_{x}^{y} \mathsf{Qua}_i = \sum_{x}^{y} \frac{\mathsf{Qua}(\text{holder}_i, T_k)}{\mathsf{Qua}(\text{holder}_i, \{T_k|k=1,2,...,z\})}, \tag{5}$$

where $i \in [x,y]$,

$$\begin{aligned}&\mathsf{Qua}(\text{holder}_i, T_k)\\ &= \frac{\text{total transfer quantity of holder}_i \text{ on token } T_k}{\text{issue quantity of token } T_k},\end{aligned} \tag{6}$$

and

$$\mathsf{Qua}(\text{holder}_i, \{T_k|k=1,2,...,z\}) = \sum_{k=1}^{z} \mathsf{Qua}(\text{holder}_i, T_k). \tag{7}$$

In Eq. (6), $\mathsf{Qua}(\text{holder}_i, T_k)$ denotes the ratio of the transferring quantity of an account (in an account group) to the total issuance quantity of a token. Since the total issuance of different tokens is not the same, it is necessary to normalize $\mathsf{Qua}(\text{holder}_i, T_k)$. Similar to the definition of ANF in Eq. (2), the set $\{T_k|k=1,2,...,z\}$ in Eq. (5) and Eq. (7) represents all tokens held by holder_i. If $\mathsf{Qua}_i = \frac{\mathsf{Qua}(\text{holder}_i, T_k)}{\mathsf{Qua}(\text{holder}_i, \{T_k|k=1,2,...,z\})} = 1$, it means that holder_i only holds one token and transfers this token. We finally add up all Qua_i of each holder_i to get the TTQF for an account group. If $\mathsf{TTQF} = |x-y|+1$ for a token, it means that this account group only holds and transfers this token. Thus, it may be a suspicious group of the token controlled by the manipulator. A large value of TTQF means that this group that has a large scale almost only interacts with this token. Regarding a token, there are generally multiple account groups. We define the MTTQF for a token as:

$$\mathsf{MTTQF} = \max(\mathsf{TTQF}_1, \mathsf{TTQF}_2, ..., \mathsf{TTQF}_q). \tag{8}$$

A token that has a larger MTTQF also has a higher possibility of being manipulated. As another important indicator considering both the account-creation relationship and transfer amount, MTTQF is helpful for finding fake accounts and the manipulator behind them.

Search For Maximum ATTNF **And** MTTQF. Most token manipulators always deluge their tokens with fake users and fake transactions. There is often a surge of

Algorithm 1 Search maximum ATTNF or MTTQF

Input: `Actions[<sender,token,quantity,sender_parent>]`, Window Size W, Pieces P, Flag F
Output: maximum ATTNF or MTTQF

arr ← [], $\text{piece}_{\text{size}} \leftarrow \frac{W}{P}$, $\text{piece}_{\text{count}} \leftarrow \frac{|\texttt{Actions}|}{\text{piece}_{\text{size}}}$
for $i = 0 \rightarrow (\text{piece}_{\text{count}} - 1)$ **do**
  $\text{piece}_{\text{start}} \leftarrow i \times \text{piece}_{\text{size}}$, $\text{piece}_{\text{end}} \leftarrow (i+1) \times \text{piece}_{\text{size}}$
  res ← ATTNF_OR_MTTQF(Actions[$\text{piece}_{\text{start}} : \text{piece}_{\text{end}}$], F)
  push res into arr
end for
$\text{sum}_{\max} \leftarrow 0$
for $i = 0 \rightarrow (P-1)$ **do**
  $\text{sum}_{\max} \leftarrow \text{sum}_{\max} + \text{arr}[i]$
end for
$\text{temp} \leftarrow \text{sum}_{\max}$, $\text{index}_{\max} \leftarrow 0$
for $i = P \rightarrow (|\text{arr}| - 1)$ **do**
  $\text{temp} \leftarrow \text{temp} + \text{arr}[i] - \text{arr}[i-P]$
  if $\text{temp} > \text{sum}_{\max}$ **then** ▷ calculate the maximum of continuous P pieces
    $\text{sum}_{\max} \leftarrow \text{temp}, \text{index}_{\max} \leftarrow i - P + 1$
  end if
end for
$\text{window}_{\text{start}} \leftarrow \text{index}_{\max} \times \text{piece}_{\text{size}}$, $\text{window}_{\text{end}} \leftarrow \text{window}_{\text{start}} + W$ ▷ $\text{index}_{\max}$ to calculate window range
return ATTNF_OR_MTTQF(Actions[$\text{window}_{\text{start}} : \text{window}_{\text{end}}$], F)

transactions within a short time. Once enough popularity (or investments) has been received, the volume of transactions quickly slumps. It is challenging to capture this phenomenon if we only calculate ATTNF and MTTQF using all historical records, thereby missing many *"fake"* tokens. Addressing this issue requires selecting an appropriate window to include the maximum value of ATTNF or MTTQF. To this end, we propose Algorithm 1, where the input includes `Actions`, Window Size W, Pieces P, and Flag F. `Actions` contain all the `transfer` actions of a token and also the parent information of *senders*. W is the number of actions in a window and F indicates whether looking for ATTNF or MTTQF. We first divide each window into P pieces, each of which is a small window with size $\text{piece}_{\text{size}}$. `Actions` are divided into $\text{piece}_{\text{count}}$ pieces. We then calculate ATTNF or MTTQF of each small window by sliding one piece and saving them into array arr (lines 2 to 6). We next adopt the greedy strategy to obtain the maximum sum of the continuous P pieces as well as the corresponding index $\text{index}_{\max}$ (lines 11 to 17). Thus, we regard $\text{index}_{\max}$ as the target to seek for a window and calculate its ATTNF or MTTQF (lines **18** to **19**). The sliding mode based on the small window can find a larger ATTNF or MTTQF, improving the accuracy of Algorithm 1. Note that ATTNF_OR_MTTQF($\texttt{Actions}[x:y], F$) is given in both Eq. (4) and Eq. (8).

7.3 Evaluation Results

We implement Algorithm 1 with Python. In our experiment, we set $W = 100,000$ and $P = 10$. After calculating the maximum ATTNF and MTTQF for each token, we finally visualize the distribution of these two factors, as shown in Fig. 13, where we adopt the logarithmic form of MTTQF because of its large variance.

We mark suspicious tokens in red as their ATTNF or MTTQF is at a high level (ATTNF > 50 *or* MTTQF $> 10,000$). In particular, we select the top-3 tokens (with large ATTNF $\times$ MTTQF products): `HBGO`, `BABY`, and `HORUS`. We then focus on these three tokens and investigate the manipulation behaviors of masterminds as well as fake transactions. To achieve this goal, we select a normal token `DICE` and compare it with these three tokens. We randomly sample the `transfer` actions of these four tokens and analyze the quantity distribution of each action. As shown in Fig. 14, the distribution of `DICE` presents an irregular fluctuation while the top-3 tokens periodically have high volumes of `transfer` actions with a relatively fixed quantity. Meanwhile, these `transfer` actions have been submitted in a short time. Further, it can be observed from the green box in Fig. 14 that `HORUS` has a large number of `transfer` actions with 20.00 `HORUS`. We next explore the evidence of the existence of fake users or fake transactions of these three tokens.

hashbabycoin@HBGO: `HBGO` token that has served as a famous pornographic DApp was created by `pornhashbaby` through the contract `hashbabycoin`. The work [22] has reported that `pornhashbaby` is the controller who has created eight groups of bot-like accounts. Each group of them has hundreds to thousands of accounts. It is quite possible that `HBGO` has been controlled by `pornhashbaby`. When

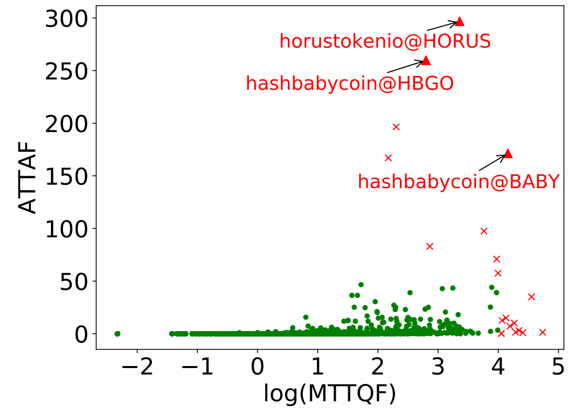


Fig. 13. Visualization of normal and suspicious tokens

scanning the `transfer` actions, we find that `pornhashbaby` usually sends 1.0000 `HBGO` to the accounts when being registered as users. Most of the names of these accounts have a common prefix like "k", "z", "gi", and "gg". Meanwhile, these names are sorted according to alphabet letters (a-z) or decimal digits (1-9). In addition, the transfer amount of most actions is fixed in a period (e.g., 11, 47). Locating the parent of the accounts, we find that a large number of accounts involved `HBGO` were created by `moneyloveyou`, `eosbank54321`, and `greedysogood`. These accounts may be accomplices who assist `pornhashbaby` to manipulate the token `HBGO`. More interestingly, all three accounts have been created by `Meetone`, another well-known DApp.

hashbabycoin@BABY: `BABY` The same as the `HBGO`, `BABY` is another token created through the token contract `hashbabycoin` by `pornhashbaby`. We observe some similar phenomena on `BABY`. For example, there are a large number of `transfer` actions done by `pornhashbaby`, which sends 11.0000 `BABY` to other accounts. Among them, 41,956 accounts that are prefixed with "bnr" have all been created by *walletbancor*. These accounts periodically interact with `BABY`. It is shown in the top two sub-figures of Fig. 14 that both `HBGO` and `BABY` have a similar quantity distribution with a periodical trend. Surprisingly, there are 7,173,443 `transfer` actions involved in the accounts with the prefix "bnr*", accounting for 43.25% of the total transaction volume of `BABY`.

horustokenio@HORUS: `HORUS` The contract `horustokenio`[6] represents an entity called *HorusPay* mainly used for companies to exchange private encrypted data. `HORUS` is one of the tokens created by `horustokenio`. After analyzing its action records, we find some abnormal `transfer` actions. For example, nearly 9,000 actions involve the accounts named "g*ge" or "h*ge" and `chainceoneos` from July 17, 2018 to Aug. 13, 2018. Meanwhile, `chainceoneos` transfers `HORUS` to `chainceout11` several times, each `transfer` action is associated with a large amount of `HORUS` tokens (from 300,000.0000 to 15,845,927.6564). More interestingly, we observe that `chainceout11` frequently interacts with the accounts named "g*ge" or "h*ge" and transfers `HORUS` to them. It seems that these accounts have formed a closed loop between `chainceoneos` and `chainceout11`. It is

6. https://horuspay.io/

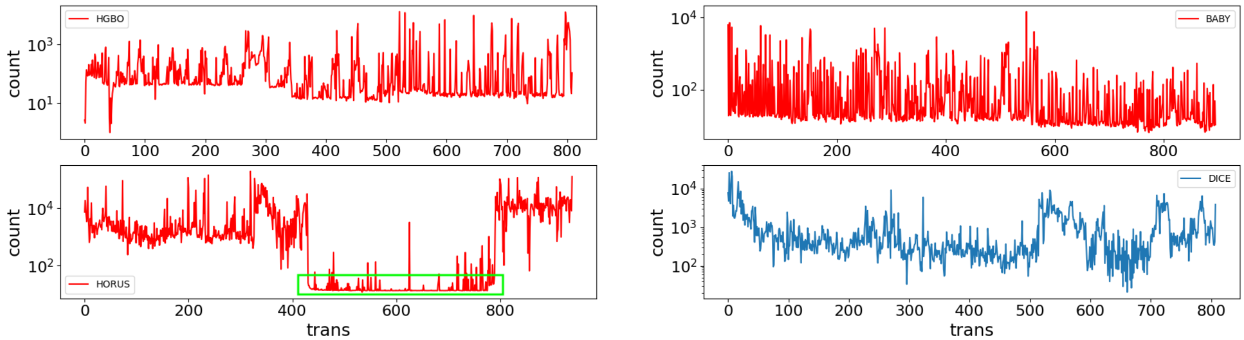


Fig. 14. Visualization of normal and suspicious tokens

reasonable to suspect that it is a manipulation of HORUS, attempting to make HORUS be "popular".

8 Related Work

8.1 EOSIO Analysis

There are a number of studies on blockchain data analytics on Ethereum and Bitcoin [50]–[58]. Most of them focus on user behaviors, cryptocurrency flows, and scams of blockchains. Despite the popularity of EOSIO, there are few systematic studies on the EOSIO ecosystem. XBlock-EOS [59] provides an efficient method of data extraction and exploration on the EOSIO blockchain data. Meanwhile, some recent studies characterize different types of activities in EOSIO (such as money transfer and contract invocation) and attempt to identify some bots and fraudulent activities [22], [60]. Moreover, other studies focus on detecting vulnerable EOSIO contracts [20], [21], [61]. Further, studies [49], [62] find design defects in the EOSIO framework, which can be exploited by attackers. However, most of the existing studies either focus on the visualization of EOSIO's various activities or identify security vulnerabilities of EOSIO. There is no work to explore EOSIO from the cryptocurrency ecosystem perspective. It is critical for EOSIO cryptocurrency stakeholders to fully understand the EOSIO token ecosystem. This paper aims to bridge this gap by conducting a comprehensive analysis of the EOSIO token ecosystem.

8.2 Token Analysis

In recent years, the prosperity of ICOs has brought immeasurable value to blockchains, such as Ethereum and EOSIO. As the crucial component in the value-transferring process of blockchains, the benign development of the token ecosystem has become an inevitable trend. Recent efforts have been conducted to analyze the token ecosystem of Ethereum across various dimensions. For example, [24], [28] analyze Ethereum-based ERC20 token networks from a graph perspective. Meanwhile, studies [25], [27], [63] attempt to detect inconsistent and abnormal behaviors in the ERC20 token ecosystem. Moreover, Fenu et al. [23] investigated the relationship between ICO and Ethereum contracts, while [64], [65] summarize the characteristics of successful tokens. However, none of these studies have explored the token ecosystem in EOSIO. The comparison study of the EOSIO token ecosystem and other blockchains (like Ethereum) can help to characterize different blockchains in terms of ICOs. Our paper is the first comprehensive work to study the EOSIO token ecosystem.

8.3 Fake Detection

The prosperity of blockchain systems and smart contracts also brings fraudulent activities. Fraudsters often make scams to defraud investors' assets. For example, some studies [66], [67] show that Ponzi schemes with forged high-yield illusions were found in Ethereum to attract huge investments from victims. Similarly, many ICO parties also counterfeit fake users and fake transactions to make unreal prosperity of their ICO projects or DApps. Several recent studies have attempted to detect fake users and illegal activities. Farrugia et al. [68] identified fake and illicit accounts over the Ethereum blockchain. Meanwhile, Huang et al. [22] found some bot-like and malicious accounts in EOSIO while their study does not consider tokens of EOSIO. Gao et al. [44] conducted a measurement study of counterfeit tokens on Ethereum and identified two types of scams related to counterfeit tokens. Xia et al. [45] detected and characterized scam tokens on Uniswap by machine learning classifiers based on four types of identified features, including time-series features, transaction features, investor features, and Unisway-specific features. Although the machine learning-based scam token detection approach achieves high performance, the authors focused on fake tokens that are from Ethereum. No previous work has identified fake tokens and fake users or transactions related to tokens for EOSIO. We propose an algorithm to detect fake tokens and recognize manipulation behaviors in EOSIO, thereby increasing investors' vigilance against fake tokens and avoiding harmful investments.

9 Conclusion and Future Work

To the best of our knowledge, we are the first to conduct a holistic measurement study on the EOSIO token ecosystem. After gathering a comprehensive dataset, we construct multiple graphs to characterize the tokens, token holders, and token creators, accompanied by a comparison study with Ethereum. We then analyze token transfer flows; this analysis also helps us to identify some abnormal trading patterns in EOSIO. Moreover, we propose an algorithm to detect tokens with fake users and fake transactions. Our study may help investors to be aware of abnormal behaviors of tokens to avoid harmful investments. This study offers many insightful findings, which help people have an in-depth understanding of the EOSIO token ecosystem and also raise many interesting open questions in this area: 1) Why have some inactive users created so many tokens with attempts to attack EOSIO? 2) What has occurred in the abnormal trading patterns? 3) What roles do the accounts play in each abnormal pattern? 4) Are there other relationships between the manipulators and fake accounts?

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[2] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[3] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[4] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, "Trust-based blockchain authorization for iot," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1646–1658, 2021.

[5] K. Nelaturu, J. Adler, M. Merlini, R. Berryhill, N. Veira, Z. Poulos, and A. Veneris, "On public crowdsource-based mechanisms for a decentralized blockchain oracle," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1444–1458, 2020.

[6] A. Braeken, M. Liyanage, S. S. Kanhere, and S. Dixit, "Blockchain and cyberphysical systems," *Computer*, vol. 53, no. 9, pp. 31–35, 2020.

[7] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19316280

[8] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "Blockchain-based business process management (bpm) framework for service composition in industry 4.0," *Journal of Intelligent Manufacturing*, pp. 1–12, 2018.

[9] E. Ganne, *Can Blockchain revolutionize international trade?* World Trade Organization Geneva, 2018.

[10] C. G. Schmidt and S. M. Wagner, "Blockchain and supply chain relations: A transaction cost theory perspective," *Journal of Purchasing and Supply Management*, vol. 25, no. 4, p. 100552, 2019.

[11] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, "A survey on blockchain consensus with a performance comparison of pow, pos and pure pos," *Mathematics*, vol. 8, no. 10, p. 1782, 2020.

[12] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digital Communications and Networks*, 2020.

[13] A. Meneghetti, M. Sala, and D. Taufer, "A survey on pow-based consensus," *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, pp. 2516–0281, 2020.

[14] A. Mizrahi and O. Rottenstreich, "Blockchain state sharding with space-aware representations," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1571–1583, 2021.

[15] D. Larimer, "Delegated proof-of-stake (dpos)," *Bitshare whitepaper*, 2014.

[16] Block.one, "EOSIO Consensus Protocol v2.0," *https://developers.eos.io/welcome/v2.0/protocol/consensus_protocol*, 2020.

[17] D. Larimer, "EOSIO Dawn 3.0 Now Available," *https://medium.com/eosio/eosio-dawn-3-0-now-available-49a3b99242d7*, 2018.

[18] Crowdfundinsider, "EOS Raised $4 Billion in Largest ICO Ever, Now they are Launching their Platform," *https://www.crowdfundinsider.com/2018/06/134320-eos-raised-4-billion-in-largest-ico-ever-now-they-are-launching-their-platform/*, 2018.

[19] Cryptonomist, "EOS: porn blowing up transaction volumes?" *https://en.cryptonomist.ch/2019/09/03/eos-porn-transaction-volumes/*, 2019.

[20] Y. Huang, B. Jiang, and W. K. Chan, "Eosfuzzer: Fuzzing eosio smart contracts for vulnerability detection," in *12th Asia-Pacific Symposium on Internetware*, 2020, p. 99–109. [Online]. Available: https://doi.org/10.1145/3457913.3457920

[21] N. He *et al.*, "EOSAFE: Security analysis of EOSIO smart contracts," in *30th USENIX Security Symposium (USENIX) Security 21)*, 2021.

[22] Y. Huang, H. Wang, L. Wu, G. Tyson, X. Luo, R. Zhang, X. Liu, G. Huang, and X. Jiang, "Understanding (mis)behavior on the EOSIO blockchain," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 2, pp. 1–28, 2020.

[23] G. Fenu, L. Marchesi, M. Marchesi, and R. Tonelli, "The ico phenomenon and its relationships with ethereum smart contract environment," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 2018, pp. 26–32.

[24] W. Chen *et al.*, "Traveling the token world: A graph analysis of Ethereum ERC20 token ecosystem," in *Proceedings of The Web Conference 2020*, 2020, pp. 1411–1421.

[25] T. Chen *et al.*, "Tokenscope: Automatically detecting inconsistent behaviors of cryptocurrency tokens in ethereum," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1503–1520.

[26] S. Somin, G. Gordon, and Y. Altshuler, "Network analysis of ERC20 tokens trading on ethereum blockchain," in *International Conference on Complex Systems*. Springer, 2018, pp. 439–450.

[27] M. Fröwis, A. Fuchs, and R. Böhme, "Detecting token systems on ethereum," in *International conference on financial cryptography and data security*. Springer, 2019, pp. 93–112.

[28] F. Victor and B. K. Lüders, "Measuring Ethereum-based ERC20 token networks," in *International Conference on Financial Cryptography and Data Security*. Springer, 2019, pp. 113–129.

[29] N. Weerasinghe, T. Hewa, M. Liyanage, S. S. Kanhere, and M. Ylianttila, "A novel blockchain-as-a-service (baas) platform for local 5g operators," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 575–601, 2021.

[30] E. J. Scheid, B. Rodrigues, and B. Stiller, "Policy-based blockchain selection," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 48–54, 2021.

[31] B. C. Ghosh, T. Bhartia, S. K. Addya, and S. Chakraborty, "Leveraging public-private blockchain interoperability for closed consortium interfacing," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, 2021, pp. 1–10.

[32] M. H. Nasir, J. Arshad, M. M. Khan, M. Fatima, K. Salah, and R. Jayaraman, "Scalable blockchains — a systematic review," *Future Generation Computer Systems*, vol. 126, pp. 136–162, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21002971

[33] B. Xu, D. Luthra, Z. Cole, and N. Blakely, "EOS: An architectural, performance, and economic analysis," *Retrieved June*, vol. 11, p. 2019, 2018.

[34] D. Larimer, "EOS VM - A Low-Latency, High Performance and Extensible WebAssembly Engine," *https://github.com/EOSIO/eos-vm*, 2019.

[35] L. Burkholder, "The halting problem," *ACM SIGACT News*, vol. 18, no. 3, pp. 48–60, 1987.

[36] L. Zhao, S. Sen Gupta, A. Khan, and R. Luo, "Temporal analysis of the entire ethereum blockchain network," in *Proceedings of the Web Conference 2021*, ser. WWW '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 2258–2269. [Online]. Available: https://doi.org/10.1145/3442381.3449916

[37] R. K. Merton, "The matthew effect in science: The reward and communication systems of science are considered," *Science*, vol. 159, no. 3810, pp. 56–63, 1968.

[38] Blocking.net, "EOS is dead: Does EIDOS really kill EOS?" https://blocking.net/22349/eos-is-dead-does-eidos-really-kill-eos/, 2019.

[39] DAppTotal, "World leading DApp data service platform," https://dapptotal.com/.

[40] DappRadar, "Metal Packaging Token," https://dappradar.com/eos/other/metpacktoken-mpt, 2019.

[41] AirDropsDAC, "ZOS Token," https://www.airdropsdac.com/zos, 2019.

[42] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, "Cryptocurrency scams: analysis and perspectives," *Ieee Access*, vol. 9, pp. 148 353–148 373, 2021.

[43] J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang, and Z. Zheng, "Financial crimes in web3-empowered metaverse: Taxonomy, counter-

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381

measures, and opportunities," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 37–49, 2023.

[44] B. Gao, H. Wang, P. Xia, S. Wu, Y. Zhou, X. Luo, and G. Tyson, "Tracking counterfeit cryptocurrency end-to-end," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 3, pp. 1–28, 2020.

[45] P. Xia, H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, and G. Xu, "Trade or trick? detectxiing and characterizing scam tokens on uniswap decentralized exchange," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 5, no. 3, pp. 1–26, 2021.

[46] Z. Wu, J. Liu, J. Wu, Z. Zheng, X. Luo, and T. Chen, "Know your transactions: Real-time and generic transaction semantic representation on blockchain & web3 ecosystem," in *Proceedings of the ACM Web Conference 2023*, 2023, pp. 1918–1927.

[47] M. Pasquinelli, "Google's pagerank algorithm: A diagram of cognitive capitalism and the rentier of the common intellect," *Deep search: The politics of search beyond Google*, pp. 152–162, 2009.

[48] F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in *WWW '21: The Web Conference 2021*, 2021, pp. 23–32. [Online]. Available: https://doi.org/10.1145/3442381.3449824

[49] S. Lee, D. Kim, D. Kim, S. Son, and Y. Kim, "Who spent my EOS on the (in) security of resource management of eos.io," in *13th USENIX Workshop on Offensive Technologies (WOOT 19)*, 2019.

[50] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 6–24.

[51] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and privacy in social networks*. Springer, 2013, pp. 197–223.

[52] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, "Do the rich get richer? an empirical analysis of the bitcoin transaction network," *PloS one*, vol. 9, no. 2, p. e86197, 2014.

[53] T. Chen, Y. Zhu, Z. Li, J. Chen, X. Li, X. Luo, X. Lin, and X. Zhange, "Understanding ethereum via graph analysis," in *IEEE INFOCOM 2018-IEEE conference on computer communications*. IEEE, 2018, pp. 1484–1492.

[54] J. Wu *et al.*, "Who are the phishers? phishing scam detection on ethereum via network embedding," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020.

[55] C. F. Torres, M. Steichen *et al.*, "The art of the scam: Demystifying honeypots in ethereum smart contracts," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1591–1607.

[56] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, and Y. Liu, "Transaction-based classification and detection approach for ethereum smart contract," *Information Processing & Management*, vol. 58, no. 2, p. 102462, 2021.

[57] L. Liu, W.-T. Tsai, M. Z. A. Bhuiyan, H. Peng, and M. Liu, "Blockchain-enabled fraud discovery through abnormal smart contract detection on ethereum," *Future Generation Computer Systems*, vol. 128, pp. 158–166, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21003319

[58] B. Tao, H.-N. Dai, J. Wu, I. W.-H. Ho, Z. Zheng, and C. F. Cheang, "Complex network analysis of the bitcoin transaction network," *IEEE Transactions on Circuits and Systems II: Express Briefs*, pp. 1–1, 2021.

[59] W. Zheng, Z. Zheng, H.-N. Dai, X. Chen, and P. Zheng, "Xblock-eos: Extracting and exploring blockchain data from eosio," *Information Processing & Management*, vol. 58, no. 3, p. 102477, 2021.

[60] Y. Zhao, J. Liu, Q. Han, W. Zheng, and J. Wu, "Exploring EOSIO via graph characterization," in *International Conference on Blockchain and Trustworthy Systems*. Springer, 2020, pp. 475–488.

[61] L. Quan, L. Wu, and H. Wang, "Evulhunter: Detecting fake transfer vulnerabilities for eosio's smart contracts at webassembly-level," *arXiv preprint arXiv:1906.10362*, 2019.

[62] D. Lee and D. H. Lee, "Push and pull: Manipulating a production schedule and maximizing rewards on the eosio blockchain," in *Proceedings of the Third ACM Workshop on Blockchains, Cryptocurrencies and Contracts*, 2019, pp. 11–21.

[63] M. Di Angelo and G. Salzer, "Identification of token contracts on ethereum: standard compliance and beyond," *International Journal of Data Science and Analytics*, pp. 1–20, 2021.

[64] J. P. Conley *et al.*, "Blockchain and the economics of crypto-tokens and initial coin offerings," *Vanderbilt University Department of economics working papers*, no. 17-00008, 2017.

[65] S. T. Howell, M. Niessner, and D. Yermack, "Initial coin offerings: Financing growth with cryptocurrency token sales," *The Review of Financial Studies*, vol. 33, no. 9, pp. 3925–3974, 2020.

[66] W. Chen *et al.*, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proceedings of the 2018 World Wide Web Conference*, 2018, pp. 1409–1418.

[67] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting ponzi schemes on ethereum: Identification, analysis, and impact," *Future Generation Computer Systems*, vol. 102, pp. 259–277, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18301407

[68] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the ethereum blockchain," *Expert Systems with Applications*, vol. 150, p. 113318, 2020.

Zigui Jiang (Member, IEEE) received the Ph.D degree in computer science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2019. She is currently an Associate Professor with the School of Software Engineering, Sun Yat-sen University, China. Her research interests include blockchain, services computing and big data.

Weilin Zheng received the M.Eng. degree with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China. His research interests include performance monitoring and optimization, blockchain computing power utilization, blockchain data analysis, and blockchain-based decentralized applications.

Bo Liu received the M.Eng. degree with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China. His research interests include blockchain smart contract analysis, blockchain data analysis, and smart contract concurrent systems.

Hong-Ning Dai (Senior Member, IEEE) is an Associate Professor in the Department of Computer Science, Hong Kong Baptist University, Hong Kong. He obtained his Ph.D. in Computer Science and Engineering from the Department of Computer Science and Engineering at the Chinese University of Hong Kong. His research interests include blockchain, the Internet of Things, and big data analytics. He has served as associate editor of IEEE Communications Surveys & Tutorials, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Industrial Informatics, and IEEE Transactions on Industrial Cyber-Physical Systems. He is also a senior member of the Association for Computing Machinery.

This article has been accepted for publication in IEEE Transactions on Knowledge and Data Engineering. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2024.3378381

Haoran Xie (Senior Member, IEEE) received a Ph.D. degree in Computer Science from City University of Hong Kong and an Ed.D degree in Digital Learning from the University of Bristol. He is currently the Department Head and Associate Professor at the Department of Computing and Decision Sciences, Lingnan University, Hong Kong. His research interests include artificial intelligence, big data, and educational technology. He has published 400 research publications, including 226 journal articles such as IEEE TPAMI, IEEE TKDE, IEEE TAFFC, and IEEE TCVST. He is the Editor-in-Chief of Natural Language Processing Journal, Computers & Education: Artificial Intelligence and Computers & Education: X Reality. He has been listed as one of the World's Top 2% Scientists by Stanford University.

Xiapu Luo (Senior Member, IEEE) is a Professor at the Department of Computing, the Hong Kong Polytechnic University. His research focuses on Blockchain and Smart Contracts Security, Mobile and IoT Security, Network Security and Privacy, and Software Engineering with papers published in top-tier security, software engineering, and networking conferences and journals. His research led to eleven best/distinguished paper awards, including ACM SIGSOFT Distinguished Paper Awards in ICSE'24, ISSTA'22 and ICSE'21, Best Paper Award in INFOCOM'18, Best Research Paper Award in ISSRE'16, etc. and several awards from the industry, such as the BOCHK Science and Technology Innovation Prize (FinTech) for his contribution to blockchain security. He regularly serves in the program committees of top security and software engineering conferences and received Top Reviewer Award from CCS'22 and Distinguished TPC member Award from INFOCOM'23 and INFOCOM'24. He currently serves as an associate editor for IEEE/ACM Transactions on Networking (ToN), IEEE Transactions on Dependable and Secure Computing (TDSC), and ACM Transactions on Privacy and Security (TOPS).

Zibin Zheng (Fellow, IEEE) received the Ph.D. degree from the Chinese University of Hong Kong. He is currently a Professor and the Deputy Dean of the School of Software Engineering, Sun Yat-sen University, China. He authored or co-authored more than 200 international journal and conference papers. His research interests include blockchain, software engineering, and services computing.

Qing Li (Fellow, IEEE) received the B.Eng. degree in Computer Science from Hunan Univeristy, Hunan, China, in 1982, and the M.S. and Ph.D. degrees in Computer Science from the University of Southern California, LA, California, USA, in 1985 and 1988, respectively. Qing Li is a Chair Professor at the Department of Computing, The Hong Kong Polytechnic University. His research focuses on data science, web mining, and artificial intelligence.He is a Fellow of IET, a Fellow of IEEE, a member of ACM SIGMOD and IEEE Technical Committee on Data Engineering. He is the chairperson of the Hong Kong Web Society, and is a steering committee member of DASFAA, ICWL, and WISE Society.