MetaOracle: A High-Throughput Decentralized Oracle for Web 3.0-Empowered Metaverse

CHEN Rui[1], LI Hui[1], LI Wuyang[1], BAI He[1], WANG Han[1], WU Naixing[2], FAN Ping[2], KANG Jian[2], Selwyn DENG[2], ZHU Xiang[2]

(1. School of Electronic and Computer Engineering, Peking University, Shenzhen 518055, China;
2. China United Network Communications Co., Ltd., Shenzhen Branch, Shenzhen 518031, China)

DOI: 10.12142/ZTECOM.202402003

https://kns.cnki.net/kcms/detail/34.1294.TN.20240529.1356.002.html, published online May 30, 2024

Manuscript received: 2024-04-19

Abstract: Recent rapid advancements in communication technology have brought forth the era of Web 3.0, representing a substantial transformation in the Internet landscape. This shift has led to the emergence of various decentralized metaverse applications that leverage blockchain as their underlying technology to enable users to exchange value directly from point to point. However, blockchains are blind to the real world, and smart contracts cannot directly access data from the external world. To address this limitation, the technology of oracles has been introduced to provide real-world data for smart contracts and other blockchain applications. In this paper, we focus on mitigating the risks associated with oracles providing corrupt or incorrect data. We propose a novel Web 3.0 architecture for the Metaverse based on the multi-identifier network (MIN), and its decentralized blockchain oracle model called MetaOracle. The experimental results show that the proposed scheme can achieve minor time investment in return for significantly more reliable data and increased throughput.

Keywords: Web 3.0; metaverse; blockchain; smart contract; oracle

Citation (Format 1): CHEN R, LI H, LI W Y, et al. MetaOracle: a high-throughput decentralized oracle for Web3.0-empowered Metaverse [J]. ZTE Communications, 2024, 22(2): 11 – 18. DOI: 10.12142/ZTECOM.202402003

Citation (Format 2): R. Chen, H. Li, W. Y. Li, et al., "MetaOracle: a high-throughput decentralized oracle for Web3.0-empowered Metaverse," *ZTE Communications*, vol. 22, no. 2, pp. 11 – 18, Jun. 2024. doi: 10.12142/ZTECOM.202402003.

1 Introduction

Web 3.0 is currently one of the most trending topics, symbolizing the Internet revolution from a mere information exchange platform into a more open, decentralized, and secure ecosystem based on blockchain. In April 2014, WOOD[1] first introduced the concept of Web 3.0, and he believed that in the aftermath of Snowden's revelations, Internet users could no longer trust corporations, as these entities tend to exploit and manipulate user data for their financial gains. Subsequently, Web 3.0 has gained significant popularity since 2021 and is widely recognized as the future direction of Internet development.

Web 3.0 encompasses the seamless integration of the state-of-the-art technologies with the ultimate aim of creating a decentralized metaverse ecosystem. For instance, the digital twin technology creates a mirror image of the real world, while virtual reality (VR) and augmented reality (AR) provide immersive 3D experiences. The advancement in 5G and beyond offers ultra-high reliable and ultra-low latency connections for various metaverse devices. Wearable sensors and brain-computer interfaces (BCI) enable user-avatar interactions within the metaverse. Artificial intelligence (AI) facilitates the creation and rendering of large-scale metaverse environments. In addition, blockchain and smart contracts are vital in ensuring authentic rights for metaverse assets[2]. As a result, the metaverse holds the potential to revolutionize various industries and redefine the way we interact with digital content and each other.

To achieve direct and secure peer-to-peer value exchange within the metaverse, without the reliance on third-party trusted service intermediaries[3], the blockchain technology is leveraged. In essence, blockchain could be regarded as a public ledger where all committed transactions are stored in blocks with a chain-like structure[4]. Asymmetric cryptography and decentralized consensus algorithms are implemented for

This work is supported by Shenzhen Fundamental Research Programs under Grant Nos. JCYJ20220531093206015, GXWD20201231165807007-20200807164903001, JCYJ20210324122013036, and JCYJ20190808155607340, GuangDong Prov. R&D Key Programs under Grant Nos. 2019B010137001 and 2018B010124001, Basic Research Enhancement Program of China under Grant No. 2021-JCJQ-JJ-0483, National Key-stone R&D Program of China under Grant No. 2017YFB0803204, Natural Science Foundation of China under Grant No. 61671001, ZTE Industry-University-Institute Fund Project under Grant No. 2019ZTE03-01, and HuaWei Funding under Grant No. TC20201222002.

nodes to reach consensus and ensure transaction immutability. The transaction rules can be encoded in smart contracts. These contracts are executed automatically within the blockchain network when predefined conditions are satisfied[5]. Therefore, it is imperative to base on objective and trustworthy data to verify the execution conditions for smart contracts.

For security reasons, smart contracts are commonly executed within a secure sandbox environment, like the Ethereum Virtual Machine (EVM). They always depend on "oracles" to access external data[6]. Oracles can be centralized trusted third parties or decentralized entities that provide trustworthy off-chain data for verifying the conditions required to trigger smart contract execution. The centralized oracle relies on data from a single source, which may benefit high efficiency. Provable, also referred to as oraclize[7], is the leading oracle service built on Amazon Web Services (AWS). It is specifically designed to provide data feedback for smart contracts and it continues to maintain a large user base[8]. However, the utilization of centralized oracles may not only undermine the decentralization principle of the blockchain but also carry the risk of incorporating corrupt and inaccurate data into the blockchain[9]. On the other hand, by using consensus mechanisms to aggregate data from various independent sources, decentralized oracles resolve the singular data source problem. A few works have attempted to enhance the decentralized oracle models, and the details are presented in Section 2.

In the coming years, the metaverse is expected to undergo significant growth and expansion. In order to facilitate reliable and secure communication in the metaverse ecosystem, both individual and organizational users, as well as network devices, have a shared demand for trustworthy and privacy-enhancing identifiers. With the growing complexity and scale of the metaverse ecosystem, the co-governed multi-identifier network (MIN) can be a vital solution. MIN supports multiple identifiers such as identity, content, services, geographic information, and IP address in the network layer. The entire network is divided into hierarchical domains from top to bottom, with the top-level domain being multilaterally co-governed by countries that maintain a decentralized consortium blockchain. Regional organizations independently govern the other domains under the root domain[10]. This hierarchical multi-identifier network architecture allows for seamless integration and interoperability across diverse metaverse platforms, virtual worlds, and applications. Furthermore, MIN's large resolution capability enables the smooth handling of numerous identifiers and facilitates reliable and efficient communication among a wide range of metaverse entities. These features make MIN an indispensable component for supporting the evolving metaverse and its complex communication needs.

In this paper, we first propose a novel Web 3.0 architecture based on MIN for Web 3.0-empowered Metaverse, i.e., MIN-Web 3.0. It aims to enhance the connectivity and functionality of the metaverse by leveraging the capabilities of MIN and Web 3.0 technologies, providing a robust and scalable framework for metaverse entities to engage in secure and trusted communication. On the other hand, the risk of untrustworthy data input in the blockchain has gained significant attention. To address this issue, within the proposed MIN-Web 3.0 architecture, we further design a decentralized blockchain oracle model. With its decentralized design and consensus mechanism, MetaOracle ensures the availability of reliable data sources and enables high throughput for data processing. The performance of the proposed MetaOracle is compared with one of the most representative decentralized oracles, Chainlink, in terms of time overhead and throughput performance. The results demonstrate that MetaOracle outperforms Chainlink when a larger number of data request transactions need to be handled in the oracle. The main contributions of this paper are summarized as follows.

- We propose a novel Web 3.0 architecture based on MIN, MIN-Web 3.0, which provides a solid foundation for building the infrastructure and standards required for Web 3.0-empowered metaverse applications.
- Within the proposed MIN-Web 3.0 architecture, we further design a decentralized blockchain oracle model, MetaOracle, to enhance the reliability of the data from the outside world.
- To evaluate the functionality and performance of the proposed scheme, we compare MetaOracle with one of the most representative decentralized oracles, Chainlink. The experimental results demonstrate the advantages of MetaOracle, as it allows for a relatively low time overhead in return for remarkably higher throughput when handling a larger volume of requests for reliable data.

The rest of this paper is organized as follows. In Section 2, we introduce related works of the decentralized oracle models. Then, the design details of MIN-Web 3.0 architecture are formally described in Section 3. We present the core mechanism of our MetaOracle in Section 4. Section 5 demonstrates experimental results compared with another representative work in terms of time investment and throughput. Lastly, we conclude our work and the future outlook in Section 6.

2 Related Works

This section outlines the work related to decentralized oracle networks. Given the critical importance of trustworthy decentralized oracles for future blockchain applications, some studies have been conducted to enhance the trust and reliability of oracles. For example, LO et al.[11] developed a comprehensive framework to evaluate the reliability of diverse blockchain oracles based on trust. Their research provided valuable insights into the dependability of these oracles. Expanding on this topic, MA et al.[12] introduced an innovative decentralized oracle system that prioritizes reliability. Their proposal included specialized mechanisms designed to effectively verify and resolve disputes arising between blockchain smart contracts and oracles. By incorporating these mechanisms, they aimed to enhance the overall credibility of the decentralized oracle system. In a related study, HEISS et al.[13] delved into the concept of trust within decentralized oracles, specifically examining its significance in on-chain data interactions.

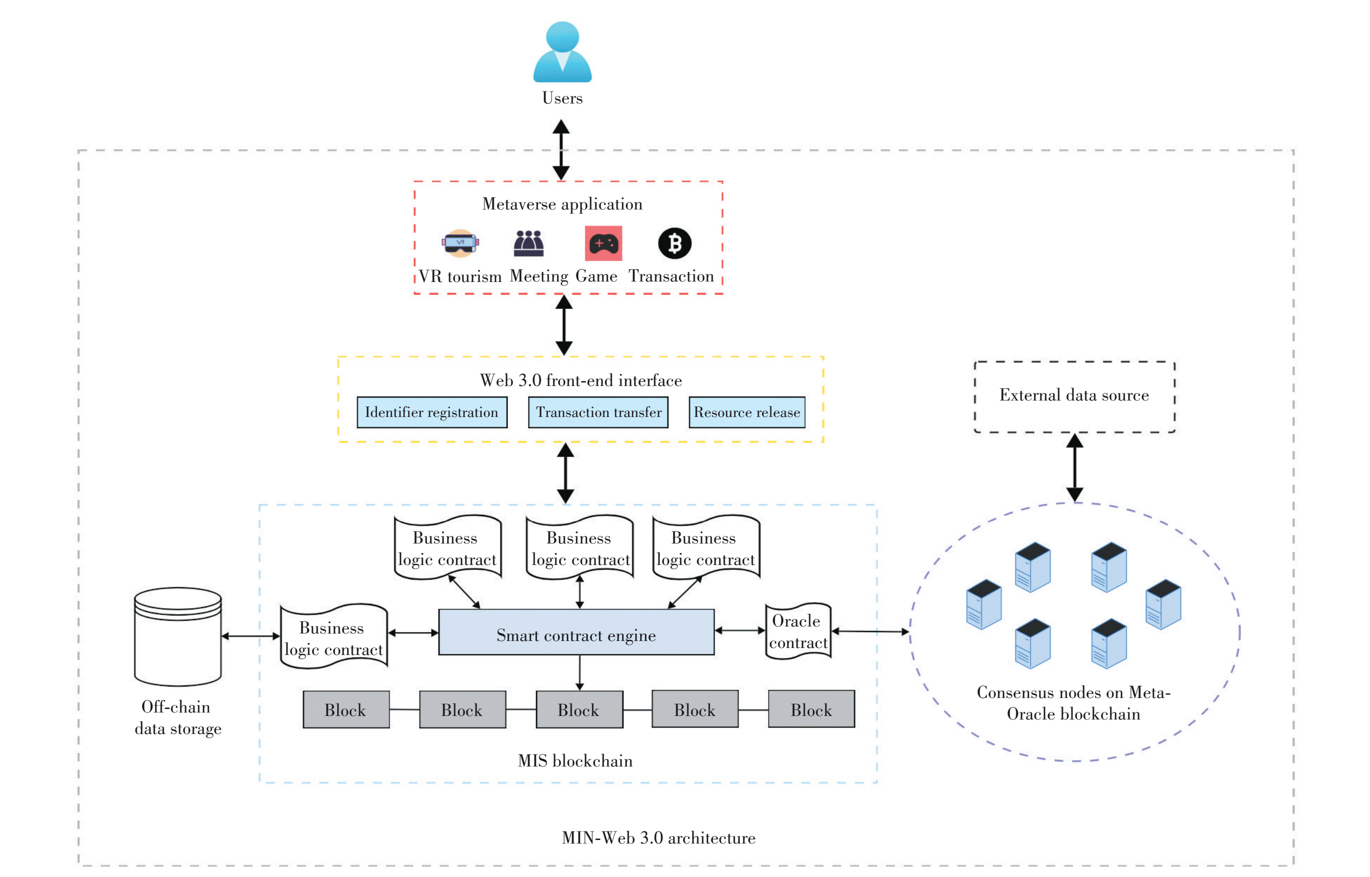
Moreover, a few oracle solutions implemented in the industry can effectively address the issue of data reliability. For instance, Chainlink serves as a decentralized oracle network which has a large market share in the decentralized oracle industry. In Chainlink, off-chain reporting (OCR) is adopted as the underlying mechanism for oracle nodes to collectively aggregate their observations into a single report of the blockchain[14]. Within the Chainlink network, a leader node is selected periodically. The leader node is responsible for regularly requesting follower nodes to provide their recently signed observations. These observations are then aggregated by the leader node to form a comprehensive report. To achieve consensus, a quorum of follower nodes must approve the report's validity by sending their own signed copies back to the leader node. Once the leader node receives the signed copies from a quorum of followers, it assembles a final report that includes the signatures of the approved quorum. This final report is then broadcast to all followers and reported to the smart contract on the blockchain. Notably, Chainlink completes the data aggregation off-chain and generates only one aggregated block in each round. As a result, individual node spends far less on gas costs.

In application, Chainlink emerges as one of the most representative oracles for connecting smart contracts with real-world data in the Web 3.0 ecosystem. For example, Chainlink provides Enjin, a virtual goods and gaming platform, with real-time game item prices and market data[15], thereby enabling fair and secure transactions within the Web 3.0 gaming ecosystem. However, challenges such as high aggregation time costs have been identified.

3 MIN-Web 3.0 Architecture for Web 3.0-Empowered Metaverse

This section provides a comprehensive overview of the MIN-Web 3.0 architecture, where the technologies of Web 3.0 are integrated into MIN. As shown in Fig. 1, the improved MIN architecture consists of five modules: metaverse application, front-end, blockchain, off-chain data storage, and the oracle. These modules work collaboratively to establish a robust and high-performing system for decentralized applications.

At the core of the MIN-Web 3.0 architecture, MIN serves as



MIN: multi-identifier network MIS: multi-identifier system VR: virtual reality

▲Figure 1. MIN-Web 3.0 architecture for Web 3.0-empowered Metaverse the underlying network layer, enabling the parallel coexistence of multiple identifiers, including identity, content, and geographic information[16]. The MIN network facilitates the generation, management, and resolution services of these identifiers, which greatly supports the deployment of consortium blockchain technology to achieve decentralization. The combination of MIN and Web 3.0 principles creates a powerful foundation for building decentralized metaverse applications that promote user autonomy and data sovereignty.

3.1 Front-End Module

Web 3.0 front-end refers to Web applications built using a new generation of Web technologies, especially the front-end interface of decentralized applications (DApps). Compared with traditional Web 2.0 applications, the Web 3.0 front-end uses a more decentralized architecture, as well as more powerful blockchain and cryptocurrency technologies. The application of these technologies enables the front end to achieve higher security, transparency, and trustworthiness.

To facilitate interaction with distributed applications, Web 3.0 front-ends must establish connectivity with blockchain networks by employing JavaScript libraries of Web 3.0 version, mainly including Web3.js and ethers.js, for seamless communication. In general, the Web 3.0 front end represents a novel approach to metaverse application interfaces, which is based on blockchain and cryptocurrency technology, with higher security, decentralization, and transparency.

3.2 Blockchain Module

As previously stated, blockchain is a decentralized distributed ledger technology that can be used to record transactions, store data, and execute smart contracts, providing some of the foundational services for Web 3.0 applications.

3.2.1 Multiple Identifier System for Web 3.0-Empowered Metaverse

Under the MIN-Web 3.0 architecture, we adopt the multi-identifier system (MIS) blockchain as the underlying blockchain service provider. MIS consists of multiple nodes to constitute a blockchain system, and each node can be managed by an independent organization or individual. MIS records a global state of multi-identifiers, including identity, content, service, space, IP address, and domain names[17]. Only the nodes that have successfully registered an identity identifier in MIS are allowed to engage in the consensus process.

The consensus algorithm, also referred to as the consensus mechanism, is a collaborative process within a distributed system for achieving agreement among multiple nodes. Within the blockchain, the consensus algorithm plays a crucial role in ensuring the security and credibility of the blockchain network. MIS adopts the Parallel Proof of Vote (PPoV) algorithm[18], which is considered a novel Byzantine Fault Tolerance (BFT) consensus algorithm for consortium blockchains. Its underlying mechanism is that the transaction can be stored in the blockchain ledger only when the number of affirmative votes in each block exceeds two-thirds of all voters.

The PPoV consensus algorithm guarantees data consistency among various nodes and enables BFT within the system. It demonstrates the characteristics of decentralization, tamper-proof data, and reduced reliance on trust. Moreover, the system's data throughput capacity is enhanced as it permits multiple accounting nodes to generate blocks in parallel during a consensus cycle.

3.2.2 Contracts in Web 3.0 Blockchain

Within the MIN-Web 3.0 architecture, there are mainly two types of smart contracts running on the blockchain module: one is the business logic contract, and the other is the oracle contract.

At the technical level, the business logics of the metaverse application are commonly written in smart contracts and executed by the smart contract engine on the blockchain. In other words, the contracts for business logic serve as the underlying infrastructure for enforcing the predefined transaction logic within the metaverse. By leveraging the blockchain technology, the execution of business logic becomes decentralized, transparent, and secure. The design for this type of contract is driven by the specific business need. For simplification, smart contracts that retrieve off-chain data storage can be categorized as business logic contracts.

On the other hand, the oracle contracts are responsible for invoking the oracle services to bring external data onto the blockchain and make it accessible to the business logic contracts. By calling the oracle contract, the business logic contract can obtain trustworthy and up-to-date information for making informed decisions and executing transactions. The oracle contracts are categorized into three types, namely consumer contracts, proxy contracts, and aggregator contracts.

The consumer contract is exposed to the business logic contract when a user wants to request specific data from the oracle service, while the proxy contract serves as middleware between the consumer contract and the aggregator contract which will be introduced later. Proxy further points to the aggregator for a particular data feed. Using proxy enables the underlying aggregators to be upgraded without any service interruption to consumer contracts. As a result, the design of proxy provides remarkable flexibility in managing and upgrading the pre-oracle network, allowing for smooth integration of enhancements as required. The most underlying layer connecting to the oracle network is the aggregator contract. According to the pre-defined interfaces, it receives periodic aggregated data updates from oracle and stores the updated data on the MIS blockchain. It is worth noting that the aggregator contract cannot directly send a data request to oracle, while it can only periodically receive the data feed from oracle.

Regarding the frequency of the data updates from oracle, two types of thresholds are set, i.e., the value threshold and the time threshold. When a node in the oracle network identifies that the latest detected values from data providers deviate from the value on the MIS blockchain by more than the defined deviation threshold, which means when the condition of value threshold is satisfied, a new aggregation round starts. On the other hand, when a specified amount of time has elapsed since the last update, the updated data will be pushed to the MIS blockchain.

3.3 Off-Chain Data Storage Module

The off-chain data storage module in blockchain enables the storage of data outside the blockchain while leveraging the smart contract capabilities of the blockchain for data access and management. The module plays a crucial role in addressing the challenges of limited storage capacity and high storage costs in blockchain. With the inherent limitations of blockchain's storage capacity, storing an extensive number of data can result in a significant increase in storage expenses. Furthermore, the public nature of blockchain data raises concerns regarding privacy and security, as it allows unrestricted access.

The inter planetary file system (IPFS) is a peer-to-peer distributed file system that utilizes content addressing to identify and retrieve files[19]. When a file needs to be stored off-chain, its content is hashed using the SHA-256 cryptographic hash function to obtain a unique content identifier (CID). The smart contract can later retrieve the data using this CID.

Considering the advantages of greater storage capacity and improved privacy protection offered by IPFS, we integrate an IPFS-based off-chain data storage scheme into our MIN-Web 3.0 architecture. Through the invocation of smart contracts, developers can conveniently access and manage data stored in off-chain data storage modules, thereby facilitating more efficient data management and interaction within the system.

3.4 Metaverse Application Module

Based on the blockchain technology, Metaverse applications are virtual world applications that transform real-world people, objects, scenes, and other elements into digital forms through digital identity, digital assets, smart contracts, etc. These applications facilitate interaction within the virtual world. With the emergence of the blockchain technology, metaverse applications have evolved towards decentralization and openness, becoming a significant component of the digital economy. Under the MIN-Web 3.0 architecture, the properties of MIN's security protection and performance optimization capabilities, along with virtual reality and the blockchain technology, enable the creation of a more real and immersive metaverse experience. Moreover, it offers a secure, transparent, and efficient solution to asset trading and management in financial scenarios.

3.5 Oracle Module

Our MetaOracle is deployed on the blockchain to conduct the data consensus, which means there are two blockchains involved in the MIN-Web3.0 architecture: MIS blockchain and MetaOracle blockchain. Further details regarding the MetaOracle blockchain are provided in Section 4.

4 Core Mechanisms of MetaOracle

In this section, we present a decentralized blockchain oracle combined with the PPoV consensus mechanism, MetaOracle, which serves as a decentralized oracle for trustworthy data feeds in Web 3.0-empowered metaverse applications.

4.1 Roles of Participants

MetaOracle includes three types of roles: the aggregator, the bookkeeper, and the voter. They collaborate to acquire the ultimate trustworthy data from external data sources.

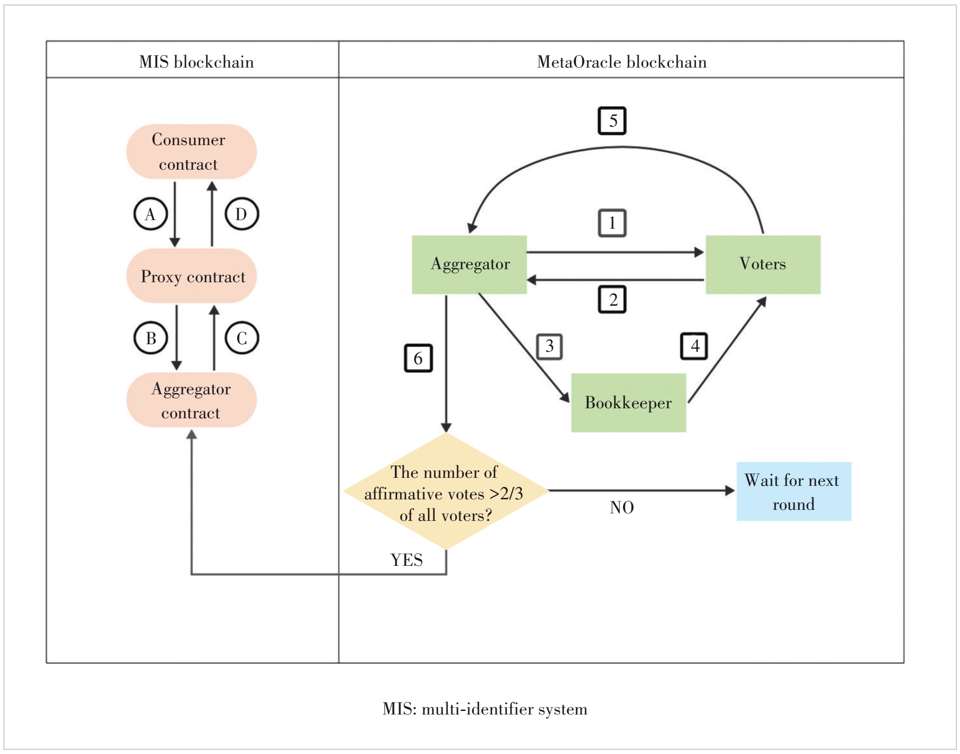
- Aggregator: An aggregator is responsible for aggregating the data collected by voter nodes on the MetaOracle blockchain. Each voter node can access various external data sources to retrieve specific data based on the predefined interfaces between the MIS blockchain and the MetaOracle blockchain. When a new round of data aggregation is triggered by meeting the threshold condition, the aggregator will request voter nodes to provide recently signed observations. These observations are then aggregated to the proper results by the aggregator according to a median or average principle. The aggregator then sends this result to the bookkeeper for generating a block.
- Bookkeeper: A bookkeeper is responsible for generating the blocks for transactions. After packaging a block for an aggregated result, the bookkeeper releases it to the network for votes.
- Voter: A voter node is responsible for two tasks within a round of data feed. One task is to fetch the information from the external world, and the other is to validate and vote on the block carrying aggregated results. The voting rule aligns with the aforementioned value threshold. In this rule, a positive vote is cast when the aggregated value deviates from the value that voters hold in this round by a margin smaller than the specified deviation threshold. The voting message contains the hash value of each block, an opinion indicating agreement or disagreement (−1, 0, 1), and the voter's signature information. By monitoring both the signature of the voter and their behavior, it is possible to detect and identify any malicious nodes within the network. Only when the number of affirmative votes in each block surpasses 2/3 of all voters, the block can be committed to the blockchain.

4.2 Whole Process of Retrieving Trustworthy Data

The overall process of retrieving trustworthy data from the MetaOracle blockchain to the MIS blockchain is described in Fig. 2.

4.2.1 MIS Blockchain Phase

A user initiates a request for external data through the con-



▲**Figure 2. Overflow of data feed**

sumer contract, and the request is first forwarded to the proxy contract before being sent to the aggregator contract. When the request reaches the aggregator contract, the aggregator responds with the up-to-date data stored on the MIS blockchain to the consumer contract through proxy. The request and response process is illustrated in Fig. 2 as Steps A to D.

4.2.2 MetaOracle Blockchain Phase

The MetaOracle blockchain is a crucial component for retrieving data from real-world data sources and reaching consensus on that data. If either the value threshold or the time threshold condition is met, a new round of data feed will be initiated. During a data feed round, requests for different data feeds may occur simultaneously. The aggregated result for each request can be regarded as a transaction. A substantial number of transactions can be packaged into a single block during a consensus round within the MetaOracle blockchain. MetaOracle can process these transactions together, thus reducing the overall processing time. On the other hand, the PPoV consensus algorithm is adopted to enable multiple bookkeepers to generate blocks concurrently, thereby enhancing the throughput of the MetaOracle blockchain.

Step 1: When conditions for different data feeds are met, the aggregator initially asks voters to retrieve the data from the external world.

Step 2: At certain intervals, the aggregator waits for and receives the data feeds from voters.

Step 3: The aggregator aggregates the data collected, and obtains proper results according to a median or average principle. Notably, the results may include the responses corresponding to different data feed requests. The aggregator then sends the results to bookkeepers for block generation.

Step 4: Each bookkeeper independently generates a block with a specific transaction allocation rule. The transaction allocation rule ensures that transaction pools of bookkeepers are distinct, resulting in unique blocks generated by each bookkeeper. The bookkeeper packages the aggregated results into a block and further broadcasts the block to the network for votes.

Step 5: After collecting the blocks from the bookkeepers, a voter casts individual votes for each block and creates a comprehensive voting message to send to the aggregator.

Step 6: The aggregator consistently waits for voting messages and counts the results. When the number of affirmative votes in each block surpasses 2/3 of all voters, the block can be confirmed, and the results will be pushed to the aggregator contract on the MIS blockchain. Otherwise, the consensus cannot be reached. The data feed can be carried over to the next round of aggregation until the threshold condition is met.

5 Experimental Analysis

In this section, we evaluate the performance of our proposed scheme. Our experiment uses 4 Linux physical machines and their operating systems are Ubuntu20.04. Each of them has a memory of 8G and 4 physical CPUs, and is interconnected through fiber optic Ethernet. The CPU is Inter(R) Core (TM) i5-8500 CPU@ 3.00 GHz. To adhere to the BFT mechanism, the total number of network nodes N must satisfy $N \geqslant 3f + 1$ where f refers to the number of faulty nodes. In our MetaOracle blockchain setup, we have established 28 nodes, consisting of three different roles: the aggregator, the bookkeeper, and the voter. In the experiment, we conducted tests on MetaOracle to measure its transaction processing capacity, represented as the number of transactions it can handle transactions per second (TPS), as well as the time required for the consensus process. We conducted these tests under three different conditions, specifically when executing 5 000, 10 000, and 15 000 transactions in a consensus round within our MetaOracle. For comparative analysis, we also collected corresponding data from Chainlink[14], a well-known decentralized oracle, as a reference point.

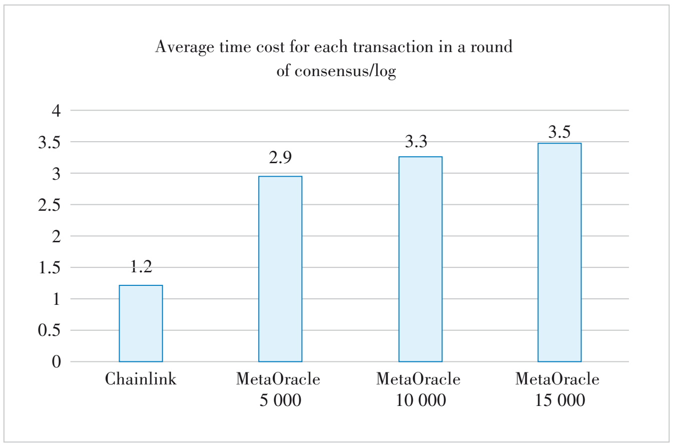
We initially compared the proposed MetaOracle with Chainlink in terms of the average time cost for each transaction in a round of consensus. Chainlink employs the Schnorr signature scheme to conduct off-chain consensus, eliminating the need for block generation during the consensus process. In other words, this approach reduces the time required for block production. To facilitate the analysis, we applied a logarithmic scale to the time cost in Fig. 3. In practice, the time cost for each transaction in a round of consensus in the Chainlink oracle is approximately 1 s lower than that of our proposed oracle.

However, the off-chain blockchain characteristic of Chainlink has a dual impact when it comes to a large number of transactions. If a large number of transactions are not packaged together in a block for transmission, the time required to transmit each transaction can be influenced by network latency. MetaOracle can package a bundle of transactions into a block and broadcast it on the blockchain to achieve consensus. This allows MetaOracle to handle a considerable number of transactions within a consensus round.

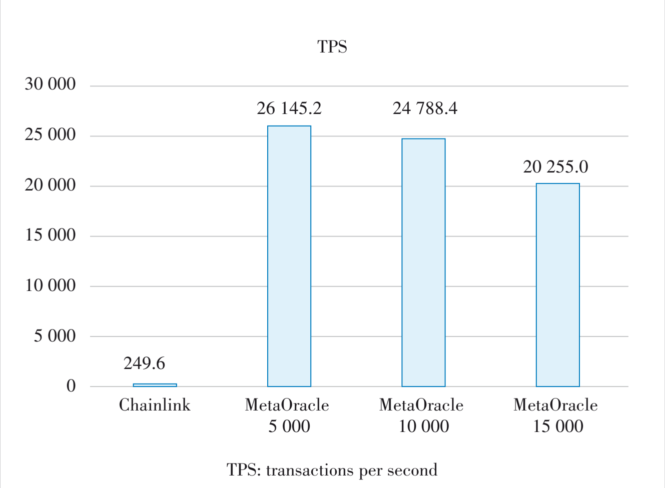
As it is depicted in Fig. 4, Chainlink's capability to handle TPS is limited to less than 250 due to the negative impact of the off-chain consensus mechanism mentioned earlier. In contrast, our MetaOracle achieves a minimum TPS of 20 000 when handling 1 5000 transactions within a round of consensus, surpassing Chainlink by a factor of at least 80. However, it is important to note that the TPS performance of MetaOracle may exhibit a peak value. Therefore, the TPS value of MetaOracle may vary when the block size changes from 5 000 to 15 000. The factors contributing to these phenomena can be considered as potential directions for future research in the field of oracles. As a result, our proposed MetaOracle achieves significantly higher throughput compared with Chainlink, albeit with a slight sacrifice of 1 s in latency.

6 Conclusions

In summary, this paper proposes a new MIN-Web 3.0 architecture for secure communications in Web 3.0-empowered metaverse applications, and a decentralized blockchain oracle called MetaOracle, which can enhance the reliability and security of data feed on the MIS blockchain while maintaining its low time overhead and high throughput. We also compare MetaOracle with Chainlink to demonstrate its effectiveness. In the future, we will undertake real-world case studies to examine the behavior and response strategies of blockchain oracles in diverse attack scenarios, such as the Sybil attack and collusion attack, to enhance the robustness of our scheme. Additionally, further research on the factors that influence the TPS performance of MetaOracle will be explored to further optimize its throughput and scalability.



▲Figure 3. A comparison of the average time cost for each transaction in a round of consensus process between Chainlink and MetaOracle. The time cost data have been logarithmically scaled for ease of observation. MetaOracle 5 000 refers to the condition when MetaOracle handles 5 000 transactions within a round of consensus, and with a block size of 5 000. In contrast, since Chainlink does not generate blocks during consensus, we only compare Chainlink when it handles a single transaction



▲Figure 4. A comparison of TPS between Chainlink and MetaOracle

References

[1] WOOD G. What is Web 3? Here's how future Polkadot founder Gavin Wood explained it in 2014 [EB/OL]. (2022-01-04) [2024-04-19]. https://cryptonews.net/news/altcoins/2974191/

[2] WANG Y T, SU Z, ZHANG N, et al. A survey on metaverse: fundamentals, security, and privacy [J]. IEEE communications surveys & tutorials, 2023, 25(1): 319 – 352. DOI: 10.1109/COMST.2022.3202047

[3] POTTS J, RENNIE E. Web3 and the creative industries: how blockchains are reshaping business models [M].A research agenda for creative industries. London: Edward Elgar Publishing, 2019. DOI: 10.4337/9781788118583.00013

[4] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends [C]//International Congress on Big Data (BigData Congress). IEEE, 2017: 557 – 564. DOI: 10.1109/BigDataCongress.2017.85

[5] WANG S, YUAN Y, WANG X, et al. An overview of smart contract: architecture, applications, and future trends [C]//Intelligent Vehicles Sym-

posium (IV). IEEE, 2018: 108 – 113. DOI: 10.1109/IVS.2018.8500488

[6] CALDARELLI G. Understanding the blockchain Oracle problem: a call for action [J]. Information, 2020, 11(11): 509. DOI: 10.3390/info11110509

[7] Provable. Provable Documentation [EB/OL]. [2024-04-19]. https://docs.provable.xyz/

[8] SOBER M, SCAFFINO G, SPANRING C, et al. A voting-based blockchain interoperability Oracle [C]//International Conference on Blockchain (Blockchain). IEEE, 2021: 160 – 169. DOI: 10.1109/Blockchain53845.2021.00030

[9] AL-BREIKI H, REHMAN M H U, SALAH K, et al. Trustworthy blockchain Oracles: review, comparison, and open research challenges [J]. IEEE access, 2020, 8: 85675 – 85685. DOI: 10.1109/ACCESS.2020.2992698

[10] LI H, WU J X, YANG X, et al. MIN: Co-governing multi-identifier network architecture and its prototype on operator's network [J]. IEEE access, 2020, 8: 36569 – 36581. DOI: 10.1109/ACCESS.2020.2974327

[11] LO S K, XU X W, STAPLES M, et al. Reliability analysis for blockchain Oracles [J]. Computers & electrical engineering, 2020, 83: 106582. DOI: 10.1016/j.compeleceng.2020.106582

[12] MA L M, KANEKO K, SHARMA S, et al. Reliable decentralized Oracle with mechanisms for verification and disputation [C]//The 7th International Symposium on Computing and Networking Workshops (CANDARW). IEEE, 2019: 346 – 352. DOI: 10.1109/CANDARW.2019.00067

[13] HEISS J, EBERHARDT J, TAI S. From Oracles to trustworthy data onchaining systems [C]//International Conference on Blockchain. IEEE, 2019: 496 – 503. DOI: 10.1109/Blockchain.2019.00075

[14] Chainlink. Chainlink 2.0 Whitepaper [EB/OL]. [2024-03-06]. https://naorib.ir/white-paper/chinlink-whitepaper.pdf

[15] Enjin. Enjin Coin [EB/OL]. [2024-03-06]. https://enjin.io/enjin-coin

[16] WANG Y M, LI H, HUANG T, et al. Scalable identifier system for industrial Internet based on multi-identifier network architecture [J]. IEEE Internet of Things journal, 2023, 10(3): 1919 – 1932. DOI: 10.1109/JIOT.2021.3137526

[17] LYU Q, LI H, LIN X N, et al. H-MIS: A hierarchical multi-identifier system based on blockchain [C]//International Conference on Big Data. IEEE, 2023: 2326 – 2333. DOI: 10.1109/BigData59044.2023.10386505

[18] WANG Z X, LI H, WANG H, et al. A data lightweight scheme for parallel proof of vote consensus [C]//IEEE International Conference on Big Data. IEEE, 2021: 3656 – 3662. DOI: 10.1109/BigData52589.2021.9671637

[19] CHEN Y L, LI H, LI K J, et al. An improved P2P file system scheme based on IPFS and Blockchain [C]//International Conference on Big Data. IEEE, 2017: 2652 – 2657. DOI: 10.1109/BigData.2017.8258226

Biographies

CHEN Rui is currently pursuing the master degree at the School of Electronic and Computer Engineering, Peking University, China. Her research interests focus on blockchain.

LI Hui (lih64@pkusz.edu.cn) is a professor of Shenzhen Graduate School, Peking University, China. He received his BE and MS degrees from School of Information Engineering, Tsinghua University, China in 1986 and 1989, respectively, and PhD degree from the Department of Information Engineering, The Chinese University of Hong Kong, China in 2000. He is the Director of Shenzhen Key Lab of Information theory & Future Internet Architecture, and Director of PKU Lab of China Environment for Network Innovations (CENI), National Major Research Infrastructure.

LI Wuyang is currently pursuing his master degree at the School of Electronic and Computer Engineering, Peking University,China. His research interests focus on blockchain.

BAI He received her BE degree from the School of Information Engineering, Zhengzhou University, China in 2019. She is currently pursuing her PhD degree at the School of Electronic and Computer Engineering, Peking University, China. Her research interests focus on congestion control and transport protocol.

WANG Han is currently pursuing her PhD degree at the School of Electronic and Computer Engineering, Peking University, China. Her research interests focus on blockchain and metaverse.

WU Naixing works as a professor-level senior engineer in China United Network Communications Co., Ltd. He received his PhD degree from the Department of Computer Application Technology, Beijing University of Posts and Telecommunications, China in 2000.

FAN Ping works as a senior engineer in China United Network Communications Co., Ltd.

KANG Jian works as a senior engineer in China United Network Communications Co., Ltd.

Selwyn DENG works as a senior engineer in China United Network Communications Co., Ltd.

ZHU Xiang works as a senior engineer in China United Network Communications Co., Ltd.