2023

Enabling DApps Data Exchange with Hardware-Assisted Secure Oracle Network

Yue Li
University of Kentucky, yli291@uky.edu
Digital Object Identifier: https://doi.org/10.13023/etd.2023.157

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Yue Li, Student

Dr. Yang Xiao, Major Professor

Dr. Simone Silvestri, Director of Graduate Studies

Enabling DApps Data Exchange with Hardware-Assisted Secure Oracle Network

THESIS

A thesis submitted in partial
fulfillment of the requirements for
the degree of Master of Science in
the College of Engineering at the
University of Kentucky

By
Yue Li
Lexington, Kentucky

Director: Dr. Yang Xiao
Lexington, Kentucky 2023

ABSTRACT OF THESIS

Enabling DApps Data Exchange with Hardware-Assisted Secure Oracle Network

Decentralized applications (dApps), enabled by the blockchain and smart contract technology, are known for allowing distrustful parties to execute business logic without relying on a central authority. Compared to regular applications, dApps offer a wide range of benefits, including security by design, trustless transactions, and resistance to censorship. However, dApps need to access real-world data to achieve their full potential, relying on the data *oracles*. Oracles act as bridges between blockchains and the outside world, providing essential data to the smart contracts that power dApps. A significant challenge in integrating oracles into the dApp ecosystem is the *Oracle Problem*, which arises from the difficulty of securely and reliably providing off-chain data to smart contracts. Trust issues, centralization risks, and data manipulation are some concerns of the Oracle Problem. Addressing these challenges is vital for the continued growth and success of dApps.

In this paper, we propose DEXO, a novel decentralized oracle mechanism designed to tackle the oracle problem by leveraging the power of Trusted Execution Environments (TEEs) and secure attestation mechanisms. DEXO aims to provide a more transparent, decentralized, and trustworthy solution for incorporating external data into dApps, ensuring that the data originates from regular, trustworthy dApp users. By empowering dApp users and developers to contribute diverse data types, DEXO fosters a more dynamic and enriched ecosystem. The proposed DEXO network not only addresses the challenges posed by the Oracle Problem but also encourages greater trust and confidence in the data provided to dApps, ultimately enhancing the overall user experience and promoting further growth in the decentralized application space.

KEYWORDS: Trusted Execution Environment (TEE), Attestation, Oracle Problem

Enabling DApps Data Exchange with Hardware-Assisted Secure Oracle Network

By
Yue Li

Director of Thesis: Yang Xiao

Director of Graduate Studies: Simone Silvestri

Date: May 3, 2023

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

In recent years, the rise of dApps has captured the attention of both the technology and financial sectors. These innovative applications, built on top of blockchain technology, offer a wide range of benefits, including enhanced security, trustless transactions, and resistance to censorship. As dApps continue to gain popularity, they are transforming various industries, such as finance, gaming, and supply chain management.

For dApps to fully realize their potential, they must be able to access and interact with real-world data. This needs for external information introduces the critical role of *oracles* in the dApp ecosystem. In a nutshell, oracles bridge the blockchain and the outside world, providing essential data to smart contracts that power dApps. For example, a financial dApp may need to consume the exchange rate data on certain securities; a dApp providing crop insurance may need an oracle mechanism to fetch local weather data on a daily basis.

The Oracle Problem

Despite the importance of oracles, their integration into the blockchain ecosystem presents unique challenges with respect to how to securely and reliably provide off-chain data to dApps, and vice versa. These challenges, collectively known as the *Oracle Problem*, come in three aspects. First, since dApps and the off-chain data sources belong to two independent trust domains, the oracle needs to provide a secure data transport that ensures authenticity (i.e., coming from legitimate sources) and integrity (untampered in the transportation) of off-chain data [4]. Second, the oracle itself resembles a centralized service, imposing a central point of risk and data manipulation concerns. It is challenging to convince dApps to trust a centralized service while the whole purpose of a dApp is to be decentralized. Third, the external sources, from which an oracle fetches data, need to be trusted individually. This is due to the fact that all external data is beyond the verification capability of the blockchain's native consensus. Very often, an oracle service advertises its "premium sources" for proving quality data, while showing little details on how they are selected and according to what standards. Addressing these challenges is vital for the continued growth and success of dApps.

One promising solution to the oracle problem is establishing a decentralized oracle network (DON). Among the current DON services, Chainlink [5], aims to provide secure and reliable access to real-world data for dApps. By leveraging decentralization, reputation systems, and on-chain data aggregation, Chainlink offers a transparent and trustworthy means of incorporating external data into the blockchain. As dApps evolve and gain adoption, technologies like Chainlink will play an increasingly important role in bridging the gap between the blockchain and the real world.

Chainlink, as a decentralized oracle network, aims to provide a transparent and secure process for handling data. However, it is essential to note that the data sources used by Chainlink's oracle nodes might not always be transparent. The data providers may have varying levels of openness and transparency, depending on the specific data

source or API. As a result, it is worth considering the data sources used by the oracle nodes and the transparency provided by Chainlink's decentralized oracle network.

Our Approach

In the ever-evolving world of dApps and blockchain technology, the need for secure and reliable data sources is becoming increasingly crucial. While existing solutions like Chainlink have significantly addressed the oracle problem, there is always room for innovation and improvement. We design **DEXO** (Decentralized Data Exchange Oracle), an oracle network designed to provide a more transparent and decentralized alternative to current oracle solutions.

DEXO's innovative approach to data sourcing leverages the power of hardware-based TEEs to generate and sign data from programs running within a dApp's user end. Crucially, the attestation mechanism of TEE ensures that the data originates from regular, trustworthy dApp users instead of being mass-generated by bots or unknown sources. This approach enhances the transparency and decentralization of the data and guarantees that it reflects the genuine voices and needs of everyday dApp users. DEXO offers a unique opportunity to address the challenges posed by the oracle problem while fostering greater trust and confidence in the data provided to dApps.

DEXO can also potentially open up new possibilities for user and developer engagement in the decentralized community. By empowering dApp users and developers to contribute locally generated data of diverse types, DEXO fosters a more dynamic and enriched ecosystem.

2 Background and Related Work

dApps Basics

Decentralized applications, or dApps, represent a transformative approach to application development that leverages blockchain technology to create distributed, self-governing, and transparent platforms. Unlike traditional applications that rely on centralized databases as the back end, a dApp's back end is a smart contract that resides on decentralized networks, such as Ethereum or other blockchain-based infrastructures, providing higher security, immutability, and data integrity. By removing the need for intermediaries and fostering direct interactions between users, dApps empower individuals to take greater control of their digital interactions, creating a more open and equitable digital ecosystem.

DApps do not depend on centralized servers. Instead, they use Web3 technologies, such as blockchains and oracles, to contain their logic and backend functions.

Since their decentralization, the decentralized services provided by dApp are more fair, open, and transparent than centralized services. Although a fair, open, and transparent centralized service with perfect rules can gain users' trust. However, such centralized services are scarce due to the company's interests. People doubt the

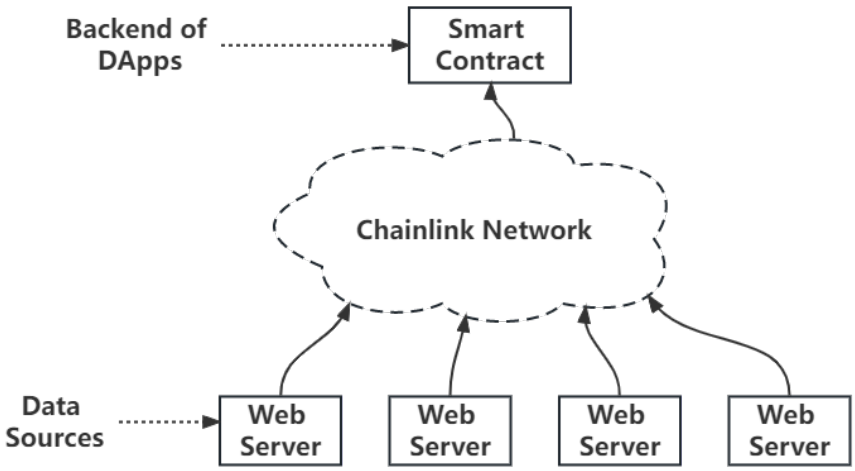

Figure 1: Chainlink's oracle network model

recommendation algorithms and blocking rules of YouTube and Twitter. Therefore, to meet the new privacy and security needs, dApps have been introduced.

Existing Oracle Solutions

DApps and blockchains are known to be decentralized, geographically independent, immutable, transparent, and secure. These features limit their full potential because they cannot be connected to real-life data.

To fetch external data, blockchain oracles are introduced. Oracles provide a way for dApp to access external data sources. Oracles provide data from the physical world to smart contracts on a blockchain. They act as a bridge, passing information about real-world events. Popular oracle services in the market include Chainlink [5], Band Protocol [6], etc.

In more detail, oracles play a crucial role in the decentralized application ecosystem by bridging blockchain-based platforms and the real-world data required to function effectively. Due to blockchains' deterministic and isolated nature, dApps cannot directly access external data sources, creating a demand for reliable and secure off-chain information. Oracles address this challenge by retrieving, validating, and transmitting external data to smart contracts, enabling dApps to interact with real-world events and information. In doing so, oracles expand the potential use cases for dApps, allowing them to harness the power of blockchain technology while leveraging the vast array of data available beyond the confines of the blockchain itself.

Chainlink [5] is a major decentralized oracle network designed to bridge the gap between blockchain-based dApps and real-world data. Its basic workflow is shown in Figure 1. By providing secure and reliable access to off-chain information, Chainlink enables smart contracts to execute based on external events and data points. Chainlink's decentralized architecture consists of a network of independent, incentivized nodes that fetch and process data from various sources, ensuring data reliability and resistance to manipulation. Chainlink nodes connect to various data sources, such

as APIs, websites, or other data feeds, to fetch information required by the dApps. These data sources can be run by centralized entities, like companies or organizations, or they can be decentralized, with multiple independent parties providing data. The network's flexibility allows it to accommodate different data types, from financial market data and sports scores to IoT sensor data.

On the other hand, Chainlink oracles also bear the responsibility of choosing the most reliable data sources. They sometimes promote their data as "premium data". This however introduces individualized trust on the data sources.

The Oracle Problem in Details

Data obtained through oracles becomes immutable only when recorded on a decentralized ledger. This begs the question: who authenticates the data provided to the blockchain? It is a dilemma between data authenticity from oracles and traditional trust assumptions about blockchains. This paradox is often referred to as the Oracle Problem.

The Oracle Problem [7] refers to the conflict between the security, authenticity, and trust of third-party oracles for the trustless execution of smart contracts. Oracles maintain a high degree of authority over how smart contracts are executed because their data determines how they are executed. Thus, data feeds from third-party sources have significant influence over the execution of smart contracts, removing their trustless nature as part of a decentralized network.

It is important to note that the term "Oracle problem" in the blockchain technology should not be confused with the Oracle Corporation. This multinational computer technology corporation specializes in database management systems, cloud engineering systems, and enterprise software products. The oracle problem refers to a specific challenge within the blockchain ecosystem, where dApps need a trustworthy and reliable way to access external data. This problem is unrelated to the Oracle Corporation and its products or services. In this study, we aim to explore solutions to the Oracle problem within the blockchain domain, not to analyze or discuss the offerings of the Oracle Corporation.

Many studies [8, 9, 10] have discussed the Oracle Problem. Specifically, when binding physical assets to the blockchain, oracles cannot provide trustless verification. Smart contracts need to rely on third parties to verify in the physical world. There is a level of trust in third parties for verification. This is the fundamental problem with the current third-party oracle services. Moreover, as dApps find their application in wider domains, such as in the mobile and Internet of Things (IoT) schemes, the third-party oracle model would fail to cope with the heterogeneous data requirements from a diverse range of dApp users.

Related Works

While there is not an exact match for DEXO in terms of design and functionality, several projects and research papers share some similarities or explore related concepts.

- Ocean Protocol [11]: The primary difference between Ocean Protocol and DEXO lies in their objectives. While Ocean Protocol focuses on creating a decentralized data exchange protocol to unlock data for AI and facilitate data sharing and monetization, DEXO's main goal is to provide a more transparent and decentralized oracle network. DEXO leverages TEEs to generate and sign data from programs running within dApps, whereas Ocean Protocol relies on its tokenized service layer to mediate data exchange.

- DataBroker DAO [12]: DataBroker DAO specifically targets IoT sensor data, providing a decentralized marketplace for users to buy and sell data generated by IoT devices. In contrast, DEXO aims to create a decentralized oracle network that provides a transparent and secure process for handling various data types within dApps. DEXO leverages TEEs and attestation mechanisms for data verification, while DataBroker DAO employs smart contracts to facilitate IoT data transactions.

- Streamr [13]: Streamr is a decentralized, peer-to-peer platform for real-time data sharing and monetization, primarily concentrating on creating and operating data streams. DEXO, on the other hand, aims to build a decentralized oracle network that addresses the oracle problem and provides secure and reliable access to real-world data for dApps. Streamr primarily focuses on real-time data exchange, while DEXO emphasizes data sourcing and verification through TEEs and attestation mechanisms.

While all these projects share some similarities with DEXO regarding decentralized data exchange and user-generated data, each has its unique focus and approach to tackling different challenges in the decentralized data ecosystem. DEXO's primary differentiation lies in its emphasis on creating a transparent and decentralized oracle network by leveraging TEEs and attestation mechanisms.

We compare three data marketplace platforms: Ocean Protocol, DataBroker DAO, and Streamr. Each platform has its unique characteristics and target markets, as shown in the table 1.

- Data Validation: Ocean Protocol supports third-party validation services to ensure data accuracy and reliability, while DataBroker DAO and Streamr do not have built-in data validation mechanisms.

- Rating & Reputation System: Ocean Protocol features a token-curated reputation system that allows users to evaluate data providers. DataBroker DAO and Streamr do not have a rating or reputation system in place.

- Data Preview & Samples: All three platforms, Ocean Protocol, DataBroker DAO, and Streamr, allow data previews and samples depending on the provider's settings. This feature helps users assess the quality and relevance of the data before purchasing it.

- Community Governance & Reporting: Ocean Protocol and Streamr both have community governance mechanisms in place, with Ocean Protocol offering dispute resolution and Streamr providing a reporting mechanism. DataBroker DAO does not have a community governance feature.
- Target Market: Each platform caters to a specific market. Ocean Protocol targets AI data, DataBroker DAO focuses on IoT data, and Streamr specializes in real-time data.

Table 1: Comparison of Ocean Protocol, DataBroker DAO, and Streamr

Aspect	Ocean Protocol [11]	DataBroker DAO	Streamr
Data Validation	Supports third-party validation services	None	None
Rating & Reputation System	Token-curated reputation system	None	None
Data Preview & Samples	Allows data preview and samples (depending on provider)	Allows data preview and samples (depending on provider)	Allows data preview and samples (depending on provider)
Community Governance & Reporting	Community governance with dispute resolution	None	Community governance with reporting mechanism
Target Market	AI Data	IoT Data	Real-time Data

3 Preliminary—Trusted Execution Environments

TEE are secure areas within a processor that provide an isolated and protected environment for executing sensitive code and handling confidential data. They are designed to ensure the confidentiality, integrity, and authenticity of the data and code running within them, even in the presence of potentially malicious software or hardware attacks on the rest of the system.

TEEs utilize hardware-based security mechanisms, such as encryption and access control, to protect the memory and execution of the code inside them. By doing

so, they create a secure enclave isolated from the rest of the system, including the operating system and other applications.

Some of the critical features of TEEs include the following:

- Isolation: TEEs separate sensitive code and data from the rest of the system, preventing unauthorized access or tampering.
- Integrity: Hardware-based mechanisms ensure the integrity of the code and data running within the TEE, detecting and preventing unauthorized modifications.
- Confidentiality: Sensitive data stored and processed within the TEE is encrypted and protected from unauthorized access or eavesdropping.
- Attestation: TEEs can provide cryptographic proof of the code's authenticity and integrity and the security of the environment in which it runs. This allows external parties to verify that the code runs within a genuine and secure TEE.

TEEs are employed in various applications that require enhanced security, such as secure boot processes, digital rights management (DRM), secure storage of cryptographic keys, and secure processing of sensitive data. They can be found on various devices, including smartphones, IoT devices, and servers. In the context of blockchain and dApps, TEEs are increasingly being used to enhance the security and privacy of off-chain computations and data processing, ensuring that sensitive operations are performed in a secure and verifiable manner [14, 15]. More TEE applications can be found at [16, 17, 18].

Architecture of TEE

The TEE represents the secure world within the system, while the Rich Execution Environment (REE) signifies the non-secure world, as illustrated in the figure 2 [1]. The program running in REE is called client application (CA). The program running in TEE is called trusted application (TA). The shift between the TEE and the REE is managed through a process known as context switching. When a secure function or operation needs to be executed within the TEE, the system performs a secure monitor call (SMC) to initiate the switch. The SMC is a privileged operation that securely transfers control from the REE to the TEE.

During this process, the system saves the current state of the REE, including register values and processor state, before transitioning to the TEE. The TEE then executes the secure function, and once completed, another context switch occurs, transferring control back to the REE. The system restores the REE's saved state, ensuring its execution can continue seamlessly. This mechanism enables secure and isolated execution of sensitive operations within the TEE while maintaining the overall functionality of the REE.

The REE and TEE operate on the same processor cores. TrustZone technology enables each core to execute in a secure or non-secure state, depending on the requirements. The SMC function ID and the execution sequence determine the CPU

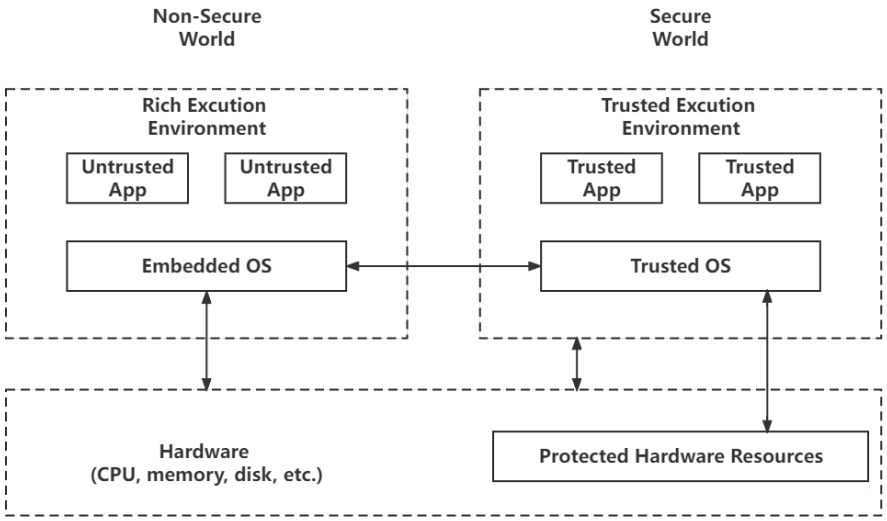

Figure 2: Architecture of TEE [1]

core responsible for executing a secure sequence. For instance, when a TA is invoked from the REE, the secure world is entered on the executing CPU core. At some point, the OP-TEE Core, acting as an execution environment, permits REE timer interrupts to pause the active OP-TEE thread and return to the REE to execute the REE scheduler. The suspended TEE thread can then be scheduled for resumption on any CPU core by the REE scheduler.

Arm TrustZone

Arm TrustZone [19] is a hardware-based security technology developed by Arm Limited, serving as a practical implementation of a TEE specifically for ARM-based devices. This technology aims to enhance the security of embedded systems, including smartphones, tablets, and IoT devices, which commonly employ ARM processors.

The foundation of TrustZone lies in partitioning the processor's resources into two distinct domains: the Secure World and the Normal World. The Secure World is a protected execution environment dedicated to handling sensitive data and operations, while the Normal World is responsible for running general-purpose applications and the operating system. This separation is facilitated by a new processor mode called "Monitor Mode," which acts as a gatekeeper between the two worlds, ensuring only authorized transitions occur.

TrustZone enables various security features such as secure boot, secure storage, and cryptographic operations. Secure boot ensures that only authenticated and authorized firmware is executed, while secure storage provides a safeguarded area to store sensitive data like encryption keys. Cryptographic operations can be offloaded to the Secure World, preventing potential leaks or tampering from malicious software running in the Normal World.

This paper's experiments focus on the Arm TrustZone technology within the Raspberry Pi 3.

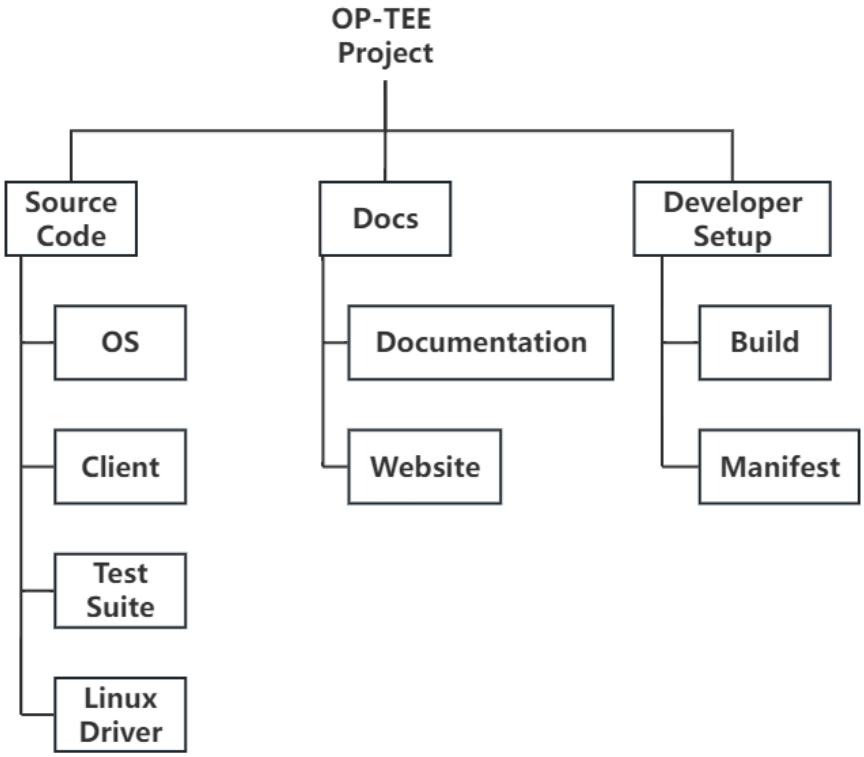

Figure 3: A pictorial representation of the OP-TEE project [2, 3].

OP-TEE

OP-TEE (Open Portable Trusted Execution Environment) is an open-source implementation of the TEE concept, designed to provide a secure and isolated environment for running sensitive code and processing confidential data. OP-TEE primarily targets ARM-based devices and is built on the GlobalPlatform TEE specifications, which define a standardized API for developing secure applications. Using OP-TEE, developers can create secure applications that benefit from enhanced privacy and protection against unauthorized access or tampering, making it particularly suitable for blockchain and dApps, where trust and security are paramount. As is shown later, our DEXO design employs OP-TEE to bootstrap the oracle participating credentials and data quality control mechanisms as a secure application at each participating dApp end user.

The OP-TEE project [2, 3] consists of several components, each serving a specific purpose in the overall TEE architecture. Shown as Figure 3, here is an overview of the main components:

- OP-TEE OS: The OP-TEE OS is the core component of the project, providing a secure operating environment that runs in the secure world of the ARM TrustZone. It manages secure services, handles secure system calls, and enforces isolation between TAs.

- OP-TEE Client: This component is responsible for communication between the non-secure world (REE) and the secure world (TEE). It provides an API for the client applications running in the REE to interact with the TAs running in the OP-TEE OS. The OP-TEE Client helps to initiate, manage, and terminate sessions with the TAs.
- OP-TEE Test Suite: Also known as xtest, the OP-TEE Test Suite is a collection of test cases designed to validate the functionality, security, and robustness of the OP-TEE OS, the TAs, and the overall TEE system. It is a valuable resource for developers to test their TEE implementations and identify potential issues or vulnerabilities.
- OP-TEE Linux Kernel Driver: This component is a kernel module that enables communication between the OP-TEE Client and the OP-TEE OS. It provides the necessary infrastructure to handle secure system calls and manage shared memory between the REE and the TEE.

These components work together to create a complete TEE solution, ensuring a secure, isolated environment for running sensitive applications and protecting critical data on ARM TrustZone-based systems.

Intel SGX

Intel SGX (Software Guard Extensions) is a set of security-related instruction codes built into Intel processors, designed to provide a secure and isolated execution environment for sensitive code and data. By creating protected memory regions called enclaves, Intel SGX ensures the confidentiality and integrity of sensitive operations, even in the presence of potentially compromised system software or hardware. This technology has gained significant attention in the blockchain and dApp space due to its ability to safeguard off-chain computations, enhance data privacy, and enable secure and verifiable processing, thus contributing to the overall trustworthiness of decentralized systems.

4 System Overview

Problem Description

The current oracle services, such as Chainlink, can only provide a minimal selection of external data. The vast majority of decentralized information, represented by those directly gathered by individual DApps, is not shared. The leading cause is that an intelligent contract—backend of a DApp—has minimal capacity to store or process data. This creates an issue of **information silo** among dApps.

DEXO aims to overcome the oracle problem for dApps, explicitly targeting mobile application scenes where there is a need to curate and share mobile sensory data among different dApp domains. The following challenges need to be addressed:

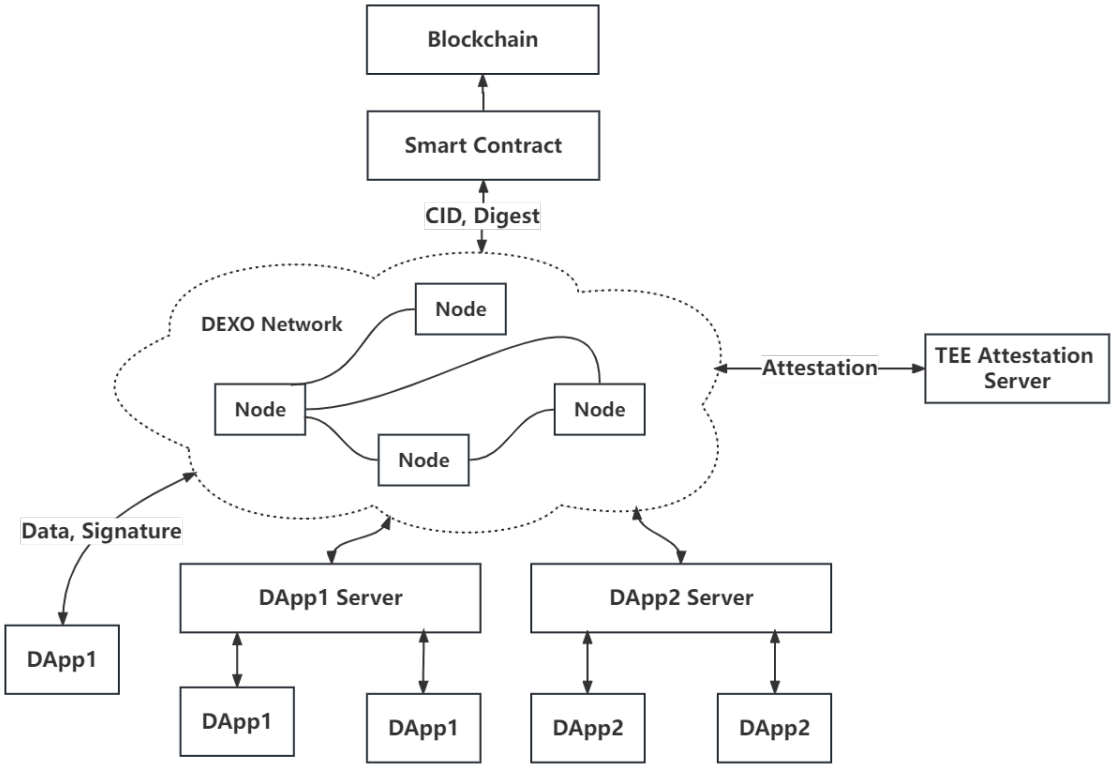

Figure 4: DEXO in DApp Ecosystem

- **Decentralization**: An ideal oracle solution should minimize the reliance on centralized authorities, mitigating the risk of single points of failure. This can be achieved by leveraging decentralized trusted data sources from dApp users, leading to the design of a new Oracle and decentralized data-providing system.
- **Data Integrity**: Ensuring the accuracy and trustworthiness of off-chain information is paramount for a successful Oracle system. This can be achieved by incorporating mechanisms to verify and validate the data sourced from dApp users while mitigating the risks of Byzantine influence and Sybil attacks.
- **Data Type Diversity**: Adapting to a wide range of data types and sources is essential for accommodating various use cases within the dApp ecosystem. Designing an Oracle solution that is flexible and adaptable to diverse data types can better serve the needs of the ever-growing and evolving decentralized application space.

In summary, an effective Oracle solution must prioritize decentralization, data integrity, and data type diversity to successfully facilitate the exchange of information between dApps and the real world. By addressing these essential requirements, an Oracle system can overcome the challenges associated with the Oracle problem and ultimately enhance decentralized applications' functionality, security, and usability.

System Goal

In this subsection, we present the system goals of DEXO, a novel decentralized oracle solution designed to harness the collective knowledge of dApp users and make it accessible to the broader decentralized community. DEXO aims to provide a reliable, transparent, and user-centric alternative to existing oracle networks, promoting greater inclusivity and diversity in the data that powers decentralized applications and services.

DECO aims to achieve the following objectives:

- **O1: User-centric data sourcing:** DEXO leverages the insights of dApp users as the primary data source for its oracle network. By engaging everyday users and dApp developers in the data collection process, DEXO aims to foster a more democratic and inclusive ecosystem that reflects the true diversity of the decentralized community.

- **O2: Trustworthy data validation:** To ensure the integrity and reliability of the data collected from dApp users, DEXO employs a robust attestation mechanism based on TEEs. Using TEEs for data signing and attestation, DEXO can guarantee that the data originates from genuine users and has not been tampered with during transmission or is mass-generated by bots or unknown sources.

- Decentralized data aggregation: DEXO's oracle network is designed to be highly decentralized, with multiple nodes working in concert to aggregate and process user-generated data. This distributed architecture helps to eliminate single points of failure and reduce the risk of data manipulation or censorship by malicious actors.

- Diversity: By fostering a user-centric ecosystem, DEXO enables the inclusion of a wide range of data sources and perspectives. This diversity of data inputs enriches the overall data pool but also helps to minimize biases and blind spots that may arise from relying on a limited set of data sources. As a result, decentralized applications and services' data-driven insights and decisions become more accurate, well-rounded, and reflective of the broader decentralized community.

- Reliability: Using TEE-based attestation mechanisms in DEXO ensures that user data is genuine and trustworthy. This enhanced reliability not only bolsters the confidence of dApp developers and other stakeholders in the data provided by the Oracle network but also reduces the risks associated with data tampering, manipulation, or corruption. By ensuring that the data that powers decentralized applications and services are diverse and reliable, DEXO contributes to the decentralized ecosystem's overall stability, security, and resilience.

- Transparent data access: Once the data is made publicly accessible, DEXO is committed to providing open and transparent access to the data it collects, enabling the wider decentralized community to benefit from the insights

and knowledge of dApp users. Through a user-friendly interface and well-documented APIs, DEXO makes it easy for developers, researchers, and other stakeholders to tap into its vast repository of user-generated data.

By pursuing these system goals, DEXO aims to revolutionize the way data is sourced, validated, and shared within the decentralized community, empowering users to take a more active role in shaping the ecosystem's future while being rewarded for their contributions.

DEXO in DApp Ecosystem

Figure 4 illustrates the position of DEXO within the dApp ecosystem. Both dApps and dApp servers can interact with DEXO, contributing data and data signatures. To ensure the data's reliability, integrity, and authenticity, DEXO utilizes third-party TEE attestation servers for verification. The specific attestation process will be elaborated upon in the subsequent attestation subsection.

Upon verification, DEXO consolidates the data and generates a digest, which is then uploaded to the Ethereum blockchain through a dedicated DEXO smart contract. These digests encompass evaluations of the data, information regarding the data type, and a general description of the data's purpose. This information lets others determine whether the data is relevant to their needs. If deemed necessary, the dApps can acquire the data through DEXO, fostering an efficient and collaborative data-sharing environment within the decentralized ecosystem. This approach facilitates secure and efficient data digests storage while maintaining the essential attributes of decentralization and transparency within the system.

5 DEXO Detailed Design

Architecture

Figure 5 depicts the working steps of DEXO. Steps 1 through 4 outline the workflow following DEXO's receipt of data, while Steps 5 to 7 describe how data consumers obtain data from the DEXO Network.

Step 1 involves legitimate dApps providing data to the DEXO network. The data must be generated and signed within TAs. This process will be further explained in the upcoming two subsections. Step 2 consists of the attestation phase, during which a third-party verifier validates the legitimacy of the data. A detailed explanation of this process will be provided in the subsequent attestation subsection.

In Step 3, the verified data is transmitted to the evaluation module. Upon assessment, the evaluation module generates a digest that is transmitted to the smart contract and uploaded to the blockchain, making the digest publicly available. Simultaneously, the evaluated data is distributed and stored within the DEXO Network.

When other dApps discover valuable data through the public blockchain, they can request and obtain the relevant data from the DEXO Network through Steps 5, 6, and 7. This collaborative approach facilitates efficient data sharing and utilization within the decentralized ecosystem.

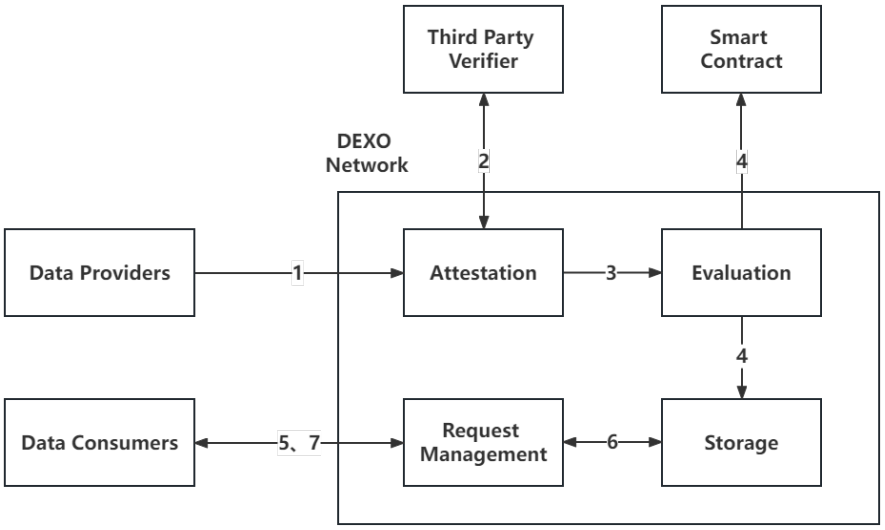

Figure 5: DEXO System Architecture and Workflow

DApps Joining DEXO Network

If a dApp wishes to transmit data to DEXO, it must employ a TA recognized and trusted by DEXO. To ensure the reliability of the data and its generation within the TA, DEXO must verify the data through a third-party verifier and confirm the legitimacy of the TEE environment. Failing to establish trust in the data could lead to various risks, such as:

- Data tampering: Malicious actors may attempt to manipulate or alter the data before it is transmitted, which could result in incorrect or misleading information being processed by DEXO or other dApps.
- Sybil attacks: An attacker might create multiple fake identities to flood the network with false data, causing DEXO to treat the fraudulent information as legitimate and skew the overall results.

Consequently, the TA must be auditable by DEXO.

Comparing DEXO's data source mechanisms to those of Chainlink, there are similarities and differences. Both systems rely on decentralized data sources to mitigate the risk of relying on a single point of failure. However, DEXO primarily focuses on obtaining data from dApp users in a TEE, while Chainlink acquires data from a network of independent node operators. A crucial distinction between DEXO and Chainlink is trust within their respective systems. Chainlink places its trust in the nodes that are responsible for retrieving and transmitting data to smart contracts. Trusted parties usually operate these nodes and are subject to security measures, such as staking and reputation systems, to ensure their reliability and accuracy in providing data.

On the other hand, DEXO shifts the focus of trust towards the everyday dApp users. Doing so aims to create a more decentralized and transparent system where

regular users generate and sign data within a TEE. This approach reduces the reliance on centralized data providers and fosters a more inclusive and diverse data landscape that reflects the actual interests and needs of the dApp community.

While Chainlink primarily relies on trusted nodes for data provision, DEXO places its trust in the hands of individual dApp users, fostering a more decentralized and representative data ecosystem.

Data Send to DEXO

Some well-known dApps that upload data to the blockchain include decentralized finance (DeFi) platforms like Uniswap [20], Aave [21], and Compound [22] and non-fungible token (NFT) marketplaces like OpenSea [23] and Rarible [24]. The data uploaded to the blockchain by these dApps typically includes transaction details, ownership records, and smart contract interactions.

These data's characteristics are immutable, transparent, and secure, which ensures the integrity of the dApps and builds trust among their users. Additionally, anyone can audit and analyze the data stored on the blockchain.

There may be other valuable data generated during the operation of these dApps that is not necessarily uploaded to the blockchain. For example, user behavior patterns, transaction volumes, and liquidity provision trends could provide valuable insights for other projects and developers.

Historically, seemingly unimportant data generated during engineering processes have sometimes been precious for other projects. For instance, the data collected by weather satellites, initially considered supplementary, later became crucial in understanding and predicting weather patterns and climate change [25, 26].

A similar situation could occur with dApps, where data generated during their operation might not be considered valuable initially. However, it could later prove to be of great significance for other projects or even entire industries. By sharing and analyzing such data, new insights and opportunities could be discovered, ultimately leading to the growth and innovation of the decentralized ecosystem. Dapps developers can decide which data to share or observe the community's needs.

Attestation

DEXO incorporates attestation mechanisms within its architecture to create a secure and trustworthy data exchange ecosystem. By leveraging these attestation techniques, DEXO can establish high confidence in the data being transmitted between DApps users, DApps servers, and the DEXO network itself. This ensures that the data being processed and shared within the system is genuine and reliable, fostering a sense of trust and security among all parties involved. Integrating attestation within DEXO's framework enhances the platform's overall data protection capabilities and solidifies its position as a dependable and secure solution for data exchange in the decentralized application landscape.

DEXO requires the attestation techniques for several reasons:

- Data Confidentiality: TEE technology provides a secure environment for processing sensitive data, ensuring that data is protected from unauthorized access, tampering, or leakage. In DEXO's case, it is crucial to maintain the confidentiality of the data being transmitted from DApps users to the DEXO network.
- Data Integrity: TEE technology ensures that the data being processed within the secure environment remains unaltered, guaranteeing that the data received and processed by DEXO has not been tampered with.
- Data Authenticity: Attestation techniques are used to verify the authenticity of the data being provided by DApps users. Using attestation, DEXO can confirm that the data originates from a trusted source (i.e., a genuine TEE) and is generated by a legitimate DApp user.

Using attestation techniques is essential for DEXO to maintain the security, confidentiality, and integrity of the data being exchanged within its network and to establish trust among the components in the dApp ecosystem.

Next, we will introduce the attestation of two well-known TEE. They are Intel SGX and OP-TEE. Intel SGX is tailored for Intel x86-based processors, while OP-TEE is designed for ARM-based processors.

Intel SGX Attestation

By summarizing Intel's documentation and paper [27, 28, 29, 30], we present a detailed explanation of the remote attestation process using Intel SGX and the Intel Attestation Service (IAS):

1. Enclave creation: The remote device, equipped with Intel SGX, creates a secure enclave. A key pair (public and private keys) is generated within the enclave.
2. Attestation report generation: The enclave then creates an attestation report containing information about the enclave, such as measuring the code running inside it and the public key generated in step 1.
3. Report signing: The enclave signs the attestation report using a device-specific key provided by the Intel SGX hardware. This key, unique to the device, is provisioned by Intel during manufacturing.
4. Sending the attestation report: The remote device sends the signed attestation report to the Intel Attestation Service (IAS).
5. Verification by IAS: Upon receiving the attestation report, IAS verifies the signature and checks whether the report's contents match the expected values. This process involves comparing the measurements against known good values and verifying that the device-specific key is genuine.
6. Attestation Verification Report (AVR) generation: If IAS successfully validates the attestation report, it generates a signed AVR containing the results of the attestation process.

7. AVR delivery: The AVR is sent back to the remote device, which can then be shared with other parties (such as DEXO) as proof of the enclave's authenticity and the integrity of the inside code.

8. Validation by the relying party: The application or service that requested the attestation (the relying party) can now verify the AVR signature and its results. If the AVR is valid and the results are satisfactory, the relying party can trust the remote enclave and proceed with any desired interactions.

The remote attestation process using Intel SGX and IAS involves the generation of an attestation report, its signing and verification, and sharing a signed AVR as proof of the enclave's authenticity. This process allows relying parties to trust the remote enclave and the integrity of the code running inside it.

OP-TEE Attestation

The attestation function of OP-TEE was released in version 3.17, released on the 15th of April, 2022 [31]. An open-source program contributor provided OP-TEE with the proof of concept (POC) of attestation, and the code was merged into the OP-TEE core code after being audited by the OP-TEE team [32].

Figure 6 [33, 34] shows the conceptual flow of OP-TEE attestation. Like Intel SGX, OP-TEE relies on a third party to complete attestation.

However, as open-source software, OP-TEE has not fully completed all deployments of attestation but only completed a conceptual design and proof of concept. In the latest version of OP-TEE, attestation is turned off by default. If applying it, more details need to be designed.

Its attestation code [35, 36] implements four functions:

- PTA_ATTESTATION_GET_PUBKEY: Get the RSA public key that should be used to verify the values returned by other commands.
- PTA_ATTESTATION_GET_TA_SHDR_DIGEST: Return the digest found in the header of a Trusted Application binary or a Trusted Shared library
- PTA_ATTESTATION_HASH_TA_MEMORY: Return a signed hash for a running user space TA, which must be the caller of this PTA. It is a runtime measurement of the memory pages that contain immutable data (code and read-only data).
- PTA_ATTESTATION_HASH_TEE_MEMORY: Return a signed hash of the TEE OS (kernel) memory. It is a runtime measurement of the memory pages that contain immutable data (code and read-only data).

These implemented functions help developers in future programming.

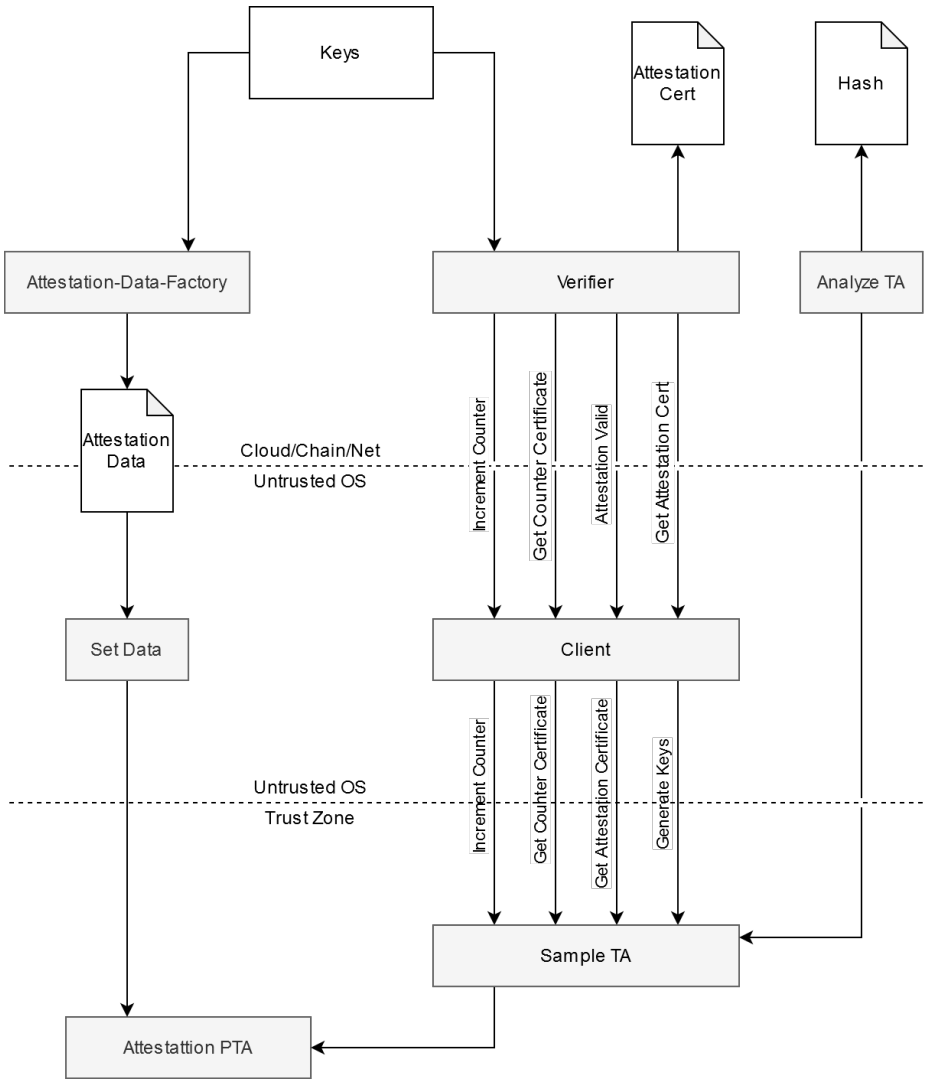

Figure 6: OP-TEE Attestation Process

Data Evaluation

In DEXO, the oracle network is designed to accept various data types from diverse sources, primarily focusing on serving as a platform for dApp users to voice their inputs. To achieve this goal while ensuring the credibility and quality of the data, DEXO employs an evaluation process that does not overly interfere with the data but assesses its trustworthiness.

The data ingested into the DEXO oracle network undergoes an initial evaluation process specific to its type. For instance, weather data might be assessed using basic statistical analysis and data comparison techniques to determine its credibility [37, 38]. This preliminary evaluation allows DEXO to assign an initial confidence score or ranking to the data without excessively scrutinizing or manipulating it.

Recognizing that some seemingly improbable data might be genuine, DEXO incorporates a mechanism to re-evaluate and adjust the confidence scores for such data

points. Additional corroborating information, user feedback, or expert review can trigger this re-evaluation process. For example, if the initially low-ranked weather data from Kentucky, which recorded an unusual temperature of -20°C, were to be supported by additional user inputs, satellite imagery, or expert analysis, DEXO would adjust the confidence score accordingly to reflect the data's authenticity.

By employing this evaluation process and a flexible mechanism for adjusting confidence scores, DEXO ensures that the data provided to dApps is accurate and reliable while respecting the diverse inputs of its user community. This approach strikes a balance between maintaining data quality and fostering an open platform for dApp users, which is vital to the success of the decentralized ecosystem.

6 Implementation

This section will explain the compilation steps of OP-TEE, how to write and compile TA and CA, call OP-TEE's attestation functions, and the algorithm and code we use for testing. We will mention the troubles we encountered while completing this testing. In the subsequent evaluation section, we will show our test results. Since we use rpi3 to build OP-TEE, the experimental results can only be used to show the characteristics of rpi3 Arm TrustZone.

As stated in the OP-TEE documentation for the rpi3 [39], it is essential to note that the implementation of OP-TEE on rpi3 lacks the necessary security features. Although the processor of the rpi3 includes ARM TrustZone exception states, the hardware and mechanisms for implementing secure boot, memory, peripherals, or other secure functions are absent. Consequently, using OP-TEE or TrustZone capabilities in this package does not guarantee a secure implementation. Implementing OP-TEE on rpi3 is intended solely for educational and prototyping purposes. In a real-world engineering scenario, different situations may arise.

OP-TEE and Testing Implementation

The OP-TEE project can be compiled into a Linux-like operating system. The easiest, trouble-free way to implement OP-TEE OS is with the help of the Repo Manifest [40]. We utilized Repo Manifest to compile and configure the various components involved. The Repo Manifest helped streamline the management of multiple source code repositories and ensured that the appropriate branches, tags, and remote server locations were synchronized correctly. This approach facilitated a smooth and efficient development process, enabling us to focus on testing OP-TEE while maintaining consistency and proper organization across the project. Other methods and troubles we used during the development process will be described in detail in the "Challenges Encountered During Testing" subsection.

Listing 1 shows the way to compile OP-TEE OS.

As shown in the listing, before compiling OP-TEE OS we get toolchains. In compiling OP-TEE for rpi3, one of the essential prerequisites is acquiring the appropriate toolchains. Toolchains, in the context of software development, refer to a collection of programming tools that work together to enable developers to build, test, and

optimize applications for specific platforms or architectures. These tools typically include compilers, linkers, debuggers, and other utilities that facilitate creating and optimizing executable binaries. By acquiring the right toolchains, we ensure that the OP-TEE environment is tailored to the rpi3 platform, allowing seamless integration and optimal performance.

```
#!/bin/bash
repo init -u https://github.com/OP-TEE/manifest.git -m
   rpi3.xml
repo sync --no-clone-bundle
cd build
make toolchains
make -j `nproc`
```

Listing 1: OP-TEE Compile Script

To conduct the tests, we modified one of the existing programs within the OP-TEE examples, ensuring compliance with the GlobalPlatform TEE Internal Core API Specification [41]. We incorporated the algorithm described in Algorithm 1 into the selected program and measured its execution time, thus enabling us to evaluate its performance effectively.

Algorithm 1 Pseudocode for generating and signing data in TA

```
Obtain TA runtime environment
Initialize avg ← random number
for i ← 1 to 10000 do
    Generate random number n_i
    avg ← avg * 0.98 + n_i * 0.02
end for
Retrieve public encryption key
Sign TA runtime environment and data using public key
Send data, public key, and signature to CA
```

Challenges Encountered During Testing

We encountered several challenges related to working with OP-TEE.

- Managing component versions: OP-TEE comprises several distinct components, such as OP-TEE OS, OP-TEE Client, and OP-TEE Test Suite. These elements can be found in both integrated repositories and individual repositories. When not using Repo Manifest and opting to compile each part separately, it is essential to verify that the versions of all components correspond correctly to ensure compatibility and prevent potential issues.
- Activating attestation in OP-TEE: By default, the attestation feature in OP-TEE is disabled. To enable the kernel's attestation functionality, one must edit

the "optee_os/mk/config.mk" file by changing the "CFG_ATTESTATION_PTA ?= n" line to "CFG_ATTESTATION_PTA = y."

- Maintaining toolchain consistency: Pre-installed toolchains may be present in some compilation environments. When compiling individual parts of the project separately, it is necessary to adjust the Makefile to guarantee consistent toolchain usage across the entire project. This step helps to avoid potential problems that could arise from toolchain discrepancies.

7 Evaluation

Attestation Performance

In our evaluation, we conducted tests to measure the time consumption of three distinct functionalities, as shown in Table 2:

- REE: In the REE, we implemented the algorithm mentioned in the implementation section and utilized OpenSSL to create an encryption key and sign the data.
- TEE: Within the TEE, we employed the algorithm mentioned in the implementation section to generate and sign data and runtime environment.
- Key Generation & Runtime Environment Hash: We assessed the duration required for generating encryption keys and computing the hash values of the runtime environment (using the TA to call PTA) in the OP-TEE's built-in attestation mechanism. This step would be executed before each signature process.

Table 2: Performance Comparison of Key Operations in TEE and REE. All values are in milliseconds (ms)

Test Group	1 Iteration	5 Iterations	10	100	1000	10000
REE	5.370	17.645	36.946	301.183	2947.845	29382.711
TEE	116.416	579.686	1160.896	11598.469	115966.846	1159568.173
KG & REH	18.973	93.576	186.811	1865.193	18654.571	186218.589

Based on the testing conducted with OP-TEE on RPI3, it has been observed that generating a data item in TEE and signing it along with the TA execution environment takes approximately 116ms. If we assume that this latency will also be present in the DApp endpoints, it is crucial to evaluate the potential impact of this delay on the DApp's performance.

Introducing a 116ms latency per data item generation and signing operation could have varying effects on different DApps, depending on their specific use cases and requirements. This added latency might lead to a noticeable slowdown in overall performance for DApps that rely heavily on real-time data processing and high-speed transactions, such as Uniswap [20] and Augur [42]. This, in turn, could affect user

experience and the DApp's efficiency in processing transactions or updating information.

On the other hand, for DApps that do not require real-time data processing or rapid transaction execution such as CryptoKitties [43] and Arweave [44], the impact of the 116ms latency may be less significant. In such cases, users might not perceive any substantial changes in the performance or responsiveness of the DApp. Moreover, the increased security and reliability provided by the TEE-based attestation mechanism might outweigh the relatively small increase in latency.

The effect of the added 116ms latency due to data generation and signing in TEE will largely depend on the specific use case and performance requirements of the DApp in question. To fully understand the implications of this latency, it is essential to evaluate its impact on a case-by-case basis, weighing the potential performance trade-offs against the benefits provided by the enhanced security and trustworthiness of the TEE-based attestation mechanism.

Discussion

Regarding computational capabilities, the RPI3 is relatively modest compared to contemporary smartphones. Although the RPI3 is a versatile and cost-effective single-board computer, it lacks the advanced processing power and sophisticated hardware features commonly found in modern smartphones. As a result, the performance of the RPI3 falls short compared to the cutting-edge devices available in today's market.

If we were to conduct tests using modern smartphones instead of the RPI3, the obtained results would likely demonstrate superior performance. The reason is that contemporary smartphones have the advanced processing power, enhanced hardware features, and optimized energy efficiency.

In evaluating the REE and TEE groups, the results indicate that modern CPUs and architectures employ specific optimization mechanisms to enhance performance when a task is executed repeatedly. This is evident from the non-linear test results observed in the REE group, where the execution speed increases with more iterations. In contrast, the TEE group demonstrates linear results, suggesting that these optimization mechanisms may be absent or are less effective within the Trusted Execution Environment.

This difference in performance could be attributed to how modern processors optimize their operations, such as through dynamic branch prediction [45], instruction prefetching, and caching [46]. These techniques help reduce the overall execution time for repetitive tasks in the REE group. However, the TEE group's focus on maintaining a secure and isolated environment for processing sensitive data might limit the application of such optimization techniques, thereby resulting in a linear performance pattern.

8 Conclusion

The continued growth and success of dApps hinge on their ability to access and interact with real-world data securely and reliably while maintaining data type di-

versity and data integrity. The oracle problem, marked by trust issues, centralization risks, and data manipulation, presents a substantial challenge in incorporating oracles into the dApp ecosystem. This paper introduced DEXO, an innovative decentralized oracle network explicitly designed to address these challenges by focusing on three essential aspects. DEXO aims to minimize reliance on centralized authorities, thus mitigating the risk of single points of failure. By leveraging decentralized trusted data sources from dApp users, it fosters a new Oracle and decentralized data-providing system, promoting decentralization. Furthermore, DEXO ensures the accuracy and trustworthiness of off-chain information by incorporating mechanisms to verify and validate data sourced from dApp users, effectively reducing the risks of Byzantine influence and Sybil attacks. In addition to decentralization and data integrity, DEXO emphasizes the importance of data type diversity, adapting to a wide range of data types and sources to cater to various use cases within the dApp ecosystem. This flexibility makes DEXO a versatile solution for the ever-growing and evolving decentralized application space. In summary, DEXO offers a comprehensive and well-rounded solution to the oracle problem, addressing crucial aspects such as decentralization, data integrity, and data type diversity. By tackling these challenges, DEXO plays a vital role in ensuring the sustained growth and success of decentralized applications.

Bibliography

[1] "Introduction to trusted execution environment and arm's trustzone." https://sergioprado.blog/introduction-to-trusted-execution-environment-tee-arm-trustzone/, 2020.

[2] "Op-tee on github." https://github.com/OP-TEE, 2017.

[3] S. Kulkarni, "Op-tee part 3: Setting up op-tee on raspberry pi 3," 11 2022.

[4] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A decentralized truth discovery approach to the blockchain oracle problem," in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, IEEE, 2023.

[5] L. Breidenbach, C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, D. Moroz, *et al.*, "Chainlink 2.0: Next steps in the evolution of decentralized oracle networks," 2021.

[6] Band Protocol, "Bandchain whitepaper." https://docs.bandchain.org/whitepaper/, 2022.

[7] G. Caldarelli, "Understanding the blockchain oracle problem: A call for action," *Information*, vol. 11, no. 11, p. 509, 2020.

[8] B. Curran, "What are oracles? smart contracts chainlink & the oracle problem," 2018.

[9] A. Egberts, "The oracle problem-an analysis of how blockchain oracles undermine the advantages of decentralized ledger systems," *Available at SSRN 3382343*, 2017.

[10] A. Antonopoulos, "The killer app: Bananas on the blockchain," *Coinscrum Meetup on*, vol. 13, 2019.

[11] O. Protocol, "A decentralized data exchange protocol to unlock data for ai," 2020.

[12] "Databroker official website." https://www.databroker.global/, 2020.

[13] "Streamr: Decentralized real-time data economy. white paper.." https://www.databroker.global/, 2017.

[14] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song, "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 185–200, IEEE, 2019.

[15] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proceedings of the 2016 aCM sIGSAC conference on computer and communications security*, pp. 270–282, 2016.

[16] R. S. Mahadev, A. Seshadri, S. Rajamani, and V. Kumar, "Using trusted execution environments to enable integrity of offline test taking," *Applications of Cognitive Computing Systems and IBM Watson: 8th IBM Collaborative Academia Research Exchange*, pp. 9–18, 2017.

[17] R. Pettersen, H. D. Johansen, and D. Johansen, "Secure edge computing with arm trustzone.," in *IoTBDS*, pp. 102–109, 2017.

[18] S. Jeon and H. K. Kim, "Tzmon: Improving mobile game security with arm trustzone," *Computers & Security*, vol. 109, p. 102391, 2021.

[19] S. Pinto and N. Santos, "Demystifying arm trustzone: A comprehensive survey," *ACM computing surveys (CSUR)*, vol. 51, no. 6, pp. 1–36, 2019.

[20] "Uniswap whitepaper." `https://uniswap.org/whitepaper.pdf`, 3 2020.

[21] "Aave protocol whitepaper." `https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf`, 1 2020.

[22] "Compound: The money market protocol." `https://compound.finance/documents/Compound.Whitepaper.pdf`, 2 2019.

[23] "Opensea official website." `https://opensea.io/`, 11 2017.

[24] "Rarible official website." `https://rarible.com/`, 2020.

[25] S. S. Board, N. R. Council, *et al.*, *Issues in the Integration of Research and Operational Satellite Systems for Climate Research: Part I. Science and Design*, vol. 1. National Academies Press, 2000.

[26] S. Q. Kidder and T. H. V. Haar, *Satellite meteorology: an introduction*. Gulf Professional Publishing, 1995.

[27] "Intel® software guard extensions: Strengthen enclave trust with attestation." `https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/attestation-services.html`, 1 2023.

[28] "Attestation service for intel® software guard extensions (intel® sgx): Api documentation. revision: 6.1." `https://api.trustedservices.intel.com/documents/sgx-attestation-api-spec.pdf`.

[29] "Intel® sgx attestation technical details." `https://www.intel.com/content/www/us/en/security-center/technical-details/sgx-attestation-technical-details.html`, 2 2023.

[30] V. Costan and S. Devadas, "Intel sgx explained," *Cryptology ePrint Archive*, 2016.

[31] D. Harbin, "Trusted firmware op tee: v3.17.0 release." https://www.trustedfirmware.org/blog/Trusted-Firmware-OPTEE-Release-3-17-0/, 4 2022.

[32] "[rfc] poc remote attestation #4011 of op-tee." https://github.com/OP-TEE/optee_os/pull/4011, 7 2020.

[33] "Integritee network docs." https://docs.integritee.network/, 2021.

[34] "[rfc] poc remote attestation #76." https://github.com/linaro-swg/optee_examples/pull/76, 7 2020.

[35] "Op-tee: attestation.c." https://github.com/OP-TEE/optee_os/blob/master/core/pta/attestation.c, 3 2023.

[36] "Op-tee: pta_attestation.h." https://github.com/OP-TEE/optee_os/blob/master/lib/libutee/include/pta_attestation.h, 10 2021.

[37] D. S. Wilks, *Statistical methods in the atmospheric sciences*, vol. 100. Academic press, 2011.

[38] I. T. Jolliffe and D. B. Stephenson, *Forecast verification: a practitioner's guide in atmospheric science*. John Wiley & Sons, 2012.

[39] "Op-tee documentation: Raspberry pi 3." https://optee.readthedocs.io/en/latest/building/devices/rpi3.html, 2020.

[40] "Repo manifest for op-tee development." https://github.com/OP-TEE/manifest/, 2023.

[41] GlobalPlatform, "Globalplatform tee internal core api specification v1.1.2.50," 2018.

[42] J. Peterson, J. Krug, and M. Zoltu, "Augur: a decentralized, open-source platform for prediction markets," 2018.

[43] A. Zen, "Cryptokitties: Collectible and breedable cats on the ethereum blockchain," 2017.

[44] S. Williams, "Arweave: A protocol for economically sustainable information permanence," 2017.

[45] L. N. Vintan, "Neural branch prediction: from the first ideas, to implementations in advanced microprocessors and medical applications," *Proc Rom Acad Ser A Math Phys Tech Sci Inf Sci*, vol. 20, no. 2, pp. 200–207, 2019.

[46] P. K. Valsan, H. Yun, and F. Farshchi, "Taming non-blocking caches to improve isolation in multicore real-time systems," in *2016 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pp. 1–12, IEEE, 2016.

Vita

Name: Yue Li

Education

- 2021 - 2023: MS student in Computer Science at the University of Kentucky
- 2016 - 2020: Bachelor's degree in Software Engineering at the University of Electronic Science and Technology of China

Work Experience

- 2020 - 2021: Research Assistant at the University of Electronic Science and Technology of China
- Spring 2019: Intern at Chinese Academy of Sciences