Whitepaper v1.0

Cyborg Network: Empowering Decentralized Edge Networks

Kresna Sucandra, Barath Kanna, Megha Varshini

www.cyborgnetwork.io

Abstract. In the digital age, the demand for low-latency data processing, enhanced security, and increased data privacy have fueled the growth of decentralized edge computing. Traditional centralized cloud and edge computing solutions face inherent limitations, prompting a shift toward a more resilient and efficient paradigm. This Whitepaper introduces Cyborg Network, a groundbreaking decentralized and trusted edge computing platform that seamlessly integrates blockchain technology. It autonomously selects the most suitable server for clients, reducing latency and eliminating the reliance on traditional DNS routing. The paper delves into six central challenges: work verification, marketplace dynamics, ex-ante work estimation, privacy, parallelization, and practical low latency. These challenges serve as the backdrop for our mission to pioneer a protocol that enables trustless connectivity and cost-effective verification of off-chain tasks in the low-latency computing domain. Our dedication to this endeavor places us at the forefront of a rapidly evolving landscape. As we navigate the complexities of edge computing, Cyborg Network remains committed to delivering decentralized, secure, and efficient solutions that empower tomorrow's digital transformation.

1. Introduction

In the digital age, the demand for low-latency data processing and real-time responses has driven the necessity of edge computing across various industries. While powerful, traditional data centers and cloud computing solutions come with their own challenges, including security, data privacy, and transparency concerns. Moreover, the advent of IoT devices and 5G networks has accentuated the need for edge computing, further intensifying the issues surrounding latency and security inherent in centralized cloud computing solutions [1]. It is within this context that the Cyborg Network takes center stage.

As the demand for edge computing continues to surge, the imperative to reduce communication latency without incurring excessive costs has become increasingly evident. Nevertheless, the lack of trust and incentive among edge owners has impeded the efficient utilization of idle computing resources [2].

By seamlessly integrating blockchain technology [3] with edge computing, Cyborg Network facilitates transparent accounting and ensures the rewarding of participant contributions, thereby nurturing a trustworthy ecosystem. The platform addresses the task allocation problem by factoring in node capacity and fair reward distribution, employing a heuristic algorithm to optimize the allocation process.

Furthermore, Cyborg Connect incorporates a police patrol model to guarantee the reliability of computational results and maximize the overall system reward. We are in the process of implementing Cyborg Connect based on an open-source project [4], [5] and are actively conducting comprehensive experiments to assess its performance and effectiveness. We aim to establish Cyborg Connect as a robust and efficient edge computing solution within the blockchain domain.

In our ongoing pursuit to propel edge computing and embrace the principles of Web 3.0, Cyborg Network introduces a groundbreaking blockchain solution that promises low latency, decentralized, and trustless computing. This whitepaper provides an exhaustive overview of the challenges we are committed to overcoming and the innovative solutions we offer. Our dedication places us at the forefront of the ever-evolving landscape of edge computing.

The cloud computing arena offers scalability and load-handling capabilities, but the realm of low-latency computing remains in its early stages, with the potential to revolutionize our interaction with technology. For example, the advent of 5G technology, characterized by its significantly shorter wavelengths than its predecessor, 4G LTE, underscores the need to position servers as close as possible to users. This is because 5G's range is considerably shorter than that of 4G, emphasizing the importance of our approach in developing a blockchain solution tailored to meet the unique demands of low-latency computing in the emerging era of 5G and beyond.

2. Security Perspective

On one hand, edge computing provides a more feasible computing technology for smart city applications and beyond; on the other hand, its emergence introduces more security threats since it increases the real-world attack surface [6] from the following four angles:

Weak Computation Power - Compared to a cloud server, the computation power of an edge server is relatively weaker. Therefore, an edge server is more vulnerable to existing attacks that may no longer be effective against a cloud server. Similarly, compared to general-purpose computers, edge devices have more fragile defense systems; as a consequence, many attacks that may be ineffective against desktop computers can pose serious threats to edge devices.

Attack Unawareness - Unlike general-purpose computers, the majority of IoT devices do not have UI interfaces, regardless of the fact that some may have crude LED screens. Therefore, a user may have limited knowledge about the running status of a device, e.g., whether it has been shut down or compromised. Hence, even if an attack takes place in an edge device, most users may not be able to discern it.

OS and Protocol Heterogeneities - Unlike general-purpose computers that tend to use standard OSes and communication protocols such as POSIX, most edge devices have different OSes and protocols without a standardized regulation. This problem directly leads to the difficulties of designing a unified protective mechanism for edge computing.

Coarse-Grained Access Control - The access control models designed for general-purpose computers and cloud computing mainly consist of four types of permissions: No Read & Write, Read Only, Write Only, Read & Write. Such a model would never be satisfiable in edge computing due to the more complicated systems and their enabled applications, which call for fine-grained access control that should handle questions such as "who can access which sensors by doing what at when and how". Unfortunately, current access control models are mostly coarse-grained.

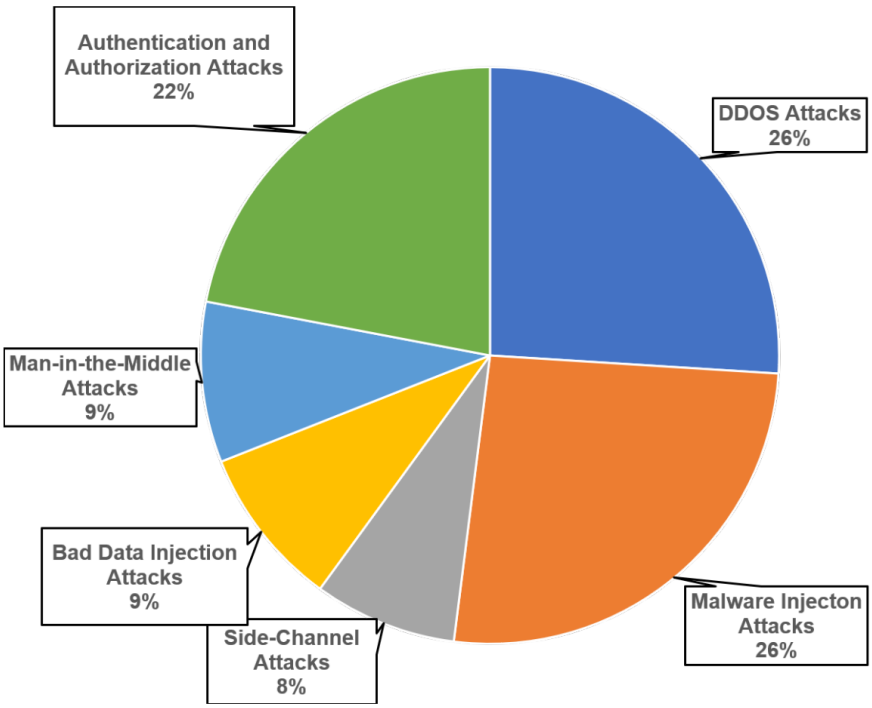


Fig. 1. Types of Attacks Targeting Edge Computing Infrastructures Happened in Real World

3. The Need for Decentralized Edge Computing

Centralized cloud and edge computing solutions have inherent data privacy, security, and latency limitations. In contrast, decentralized edge computing presents a compelling alternative that addresses these challenges while introducing several key advantages:

Reduced Latency - Decentralized edge computing processes data closer to the source, resulting in faster response times for applications and devices that require real-time processing. This is a fundamental improvement that can revolutionize our interaction with technology [7].

Enhanced Security - A decentralized architecture significantly reduces the risk of single points of failure, leading to improved security and resilience. The trustless nature of decentralized systems contributes to the overall robustness and security [8].

Increased Data Privacy - Decentralized solutions allow data to be processed and stored locally, reducing the risk of data breaches and ensuring data sovereignty. This emphasis on data privacy is of paramount importance in today's digital landscape, where safeguarding sensitive information is a top priority [9].

However, in the pursuit of implementing a protocol that enables trustless connectivity and cost-effective verification of off-chain tasks in the low-latency computing domain, we encounter six central challenges:

Work Verification - Validating off-chain computing tasks poses a considerable challenge, demanding assurance that promised computational work is executed as specified in a decentralized environment. The trustless nature of the system amplifies the complexity of this verification process.

Marketplace Dynamics - Constructing an effective marketplace for computing resources introduces intricacies in aligning supply and demand. In this ecosystem, achieving a harmonious equilibrium that encourages resource contribution while meeting resource requirements is pivotal.

Ex-ante Work Estimation - The variability in the complexity of tasks within this computing domain makes it challenging to accurately anticipate computational demands in advance. This unpredictability complicates resource allocation and planning.

Privacy - The stringent landscape of data privacy regulations necessitates robust privacy-focused design and development in this computing arena. Safeguarding sensitive data is of paramount concern in the implementation of these solutions.

Parallelization - Leveraging parallel processing is often indispensable for optimizing performance across a range of tasks within this dynamic and untrusted computing environment.

Practical Low Latency - Ensuring consistently low-latency responses is of utmost importance in real-time applications and services. In the context of this computing paradigm, where data processing occurs in close proximity to the source or user, mitigating delays becomes a critical objective. The challenge of achieving low latency involves factors like network congestion, hardware constraints, and the efficient distribution of computational resources, further underscoring the need for robust solutions in this domain.

These challenges underscore the importance of our work in developing a blockchain-based solution that not only overcomes these hurdles but also pioneers a new era of decentralized, secure, and efficient edge computing.

4. Cyborg Network

Cyborg Network is a layer-1 trustless protocol designed for low-latency computation. It rewards participants on the supply side who pledge their computing time to the network and perform tasks related to Edge AI and Edge IoT. This protocol operates without the need for centralized oversight or legal enforcement. Instead, task distribution and payments are automated through smart contracts. As highlighted, one of the fundamental challenges in constructing this network revolves around verifying completed tasks in the realm of Edge AI and Edge IoT. This intricate problem lies at the crossroads of complexity theory, game theory, cryptography, and optimization.
Addressing this challenge involves a unique approach that differs from conventional methods, such as replicating work for verification. Traditional solutions often entail doubling the operations, potentially leading to an infinite replication chain to ensure trustworthiness. Our solution interlocks three crucial concepts to tackle this issue, delivering a more efficient resolution than existing best-practice replication methods while solving the infinite-chain problem.

Homomorphically encrypted communication tooling
Building upon the research by Deepika et al. [10], we employ a homomorphically encrypted messaging pattern that harnesses Trusted Execution Environments (TEEs) within providers' machines. This approach facilitates Oblivious Transfer (OT) of information and commands, guaranteeing the utmost privacy and security in transmitting sensitive data within our decentralized edge computing ecosystem**.**

Graph-based pinpoint protocol
Following the work of Zheng et al. [11], our project embraces a multi-granular, graph-based pinpoint protocol coupled with cross-evaluator consistent execution. This combination of techniques enables efficient verification processes, allowing us to rerun and cross-compare verification work for consistency. Ultimately, these

verifications are confirmed by the chain itself, enhancing trust and reliability in the decentralized edge computing network.

Truebit-style incentive game:
Drawing inspiration from the research of Teutsch and Reitwießner [12], we implement staking and slashing mechanisms to construct a Truebit-style incentive game. This unique game design incentivizes every financially rational participant to act honestly and diligently to perform their intended tasks within our decentralized edge computing platform. By incorporating these incentives, we ensure that participants act in a manner that benefits themselves and strengthens the integrity of the network and task execution.

5. Core Components and Architecture

5.1. Participants

These concepts are employed to establish a system with four primary participants: *Customers*, *Providers*, and *Evaluators*.

a. **Customers** - Customers represent the end-users of the system, submitting tasks for computation and remunerating units of work accomplished.
b. **Providers** - Providers act as the primary workforce within the system, executing various computational tasks and creating verifiable proofs to be assessed by Evaluators.

c. **Evaluators** - Evaluators play a pivotal role in connecting the non-deterministic computation process to a deterministic linear computation. They achieve this by reproducing segments of the Providers' proofs and comparing distances against predefined thresholds.

5.2. Functional Components

The core of the system comprises three key components that ensure its robust functionality.

Cyborg Smart Client (CSC) - The Cyborg Smart Client is a lightweight WebSocket client software built in Rust. It empowers Linux-based devices to serve as network client servers. The CSC is equipped with the capability to execute commands received from remote sources and serves as the bridge to the provider's allocated virtual machine. With a binary size of only 6MB, this client is highly deployable, even on compact modules like Raspberry Pi. It swiftly establishes a secure and private communication channel with the Cyborg Blockchain's hosting node, functioning as both a command sender and a gateway. Notably, the client supports the Oblivious Transfer of Information from the Blockchain to the provider's virtual machine, ensuring secure and efficient data exchange.

Cyborg L1 Blockchain - The Cyborg Blockchain is meticulously crafted to oversee a myriad of interconnected Cyborg Smart Clients (CSCs) and

uphold the network's holistic state. Powered by the substrate framework, it boasts the ability to transmit, receive, manage, and authenticate a substantial volume of messages traversing the network. This multifaceted functionality underpins the uninterrupted operation and dependability of the system. Furthermore, the Cyborg Blockchain seamlessly integrates as a parachain within the Polkadot network. This integration leverages the Cross Consensus Messaging (XCM) protocol, affording us the capacity to collaborate with other projects in the Polkadot ecosystem seamlessly. Additionally, it equips us to support EVM-based Solidity smart contracts, expanding our service scope to encompass EVM-based projects. Importantly, the blockchain is deployed as a container chain within Tanssi's parachain, enhancing infrastructure management and enabling easy forkless upgrades. We also employ multi-party computation (MPC) techniques to enhance security and privacy. To ensure efficient operation, we modularize the system's entire functionality into a series of pallets, each serving a distinct purpose, collectively ensuring the seamless operation of the system.

Cyborg Connect Application - The Cyborg Connect Application serves as a dynamic web and mobile-friendly platform that functions as a marketplace where customers can conveniently rent serverless compute power strategically located based on data source preferences. To streamline the user experience, we offer carefully curated product segments in response to popular customer demands.This innovative platform leverages the Polkadot JS API, enabling seamless blockchain indexing. It empowers every network participant with personalized insights into their deployments and crucial metrics. The Cyborg Connect Application offers two distinct versions tailored to meet providers' and customers' specific needs and preferences. To further enhance user experience and ensure robust security, each participant is required to connect their wallet, linking its address to PEAQ's Decentralized Identity (DID) for efficient mapping of network activity. Within this setup, each connected machine is assigned a machine NFT, serving as a comprehensive record of its state over time. Multiple Machine NFTs can be associated with a single DID, offering flexibility. Users can effortlessly transition between the provider and customer interfaces with a simple click of a button, ensuring a smooth and intuitive experience.

- **Provider End -** At the provider end, compute providers gain access to essential information regarding their connected devices. This includes usage metrics, performance scores, and revenue generation data, offering comprehensive insights into the performance of their assets.
- **Customer End -** Customers, at their end, can explore information related to their deployments and associated metrics. Moreover, they have access to an inbuilt terminal, allowing them to monitor the real-time state of running processes, enhancing transparency and control.

6. Use Cases

The Cyborg Network's decentralized edge computing platform can be applied to a wide range of industries and applications, including:

- **Smart Cities**: Powering smart city applications, such as traffic management, public safety, and energy management, by providing real-time data processing and analysis at the edge [13].
- **Industrial Automation**: Enabling more efficient and cost-effective industrial automation, such as predictive maintenance, quality control, and real-time monitoring of equipment and processes [14].
- **Gaming and Entertainment**: Supporting immersive and real-time gaming experiences, such as virtual and augmented reality, by reducing latency and improving data processing and transmission at the edge [15].
- **Finance**: Facilitating more secure and efficient financial transactions, such as payment processing and identity verification, by leveraging smart contracts and blockchain technology for improved security, transparency, and auditability [16].
- **Edge AI**: Providing a secure and decentralized infrastructure for Edge AI applications, where blockchain technology can manage the ownership and usage of AI algorithms and models, ensuring that intellectual property rights are protected and properly attributed [17].

6.1. Smart Cities and the Role of Edge Computing

As urban populations continue to grow, smart city initiatives have become increasingly important for managing resources, infrastructure, and public services. The increasing complexity and interconnectivity of urban systems require innovative solutions capable of addressing the unique challenges modern cities face. Edge computing plays a critical role in these efforts by enabling real-time data processing and analysis for applications like traffic management, public safety, and energy management.

In the context of smart cities, edge computing provides the following advantages:

- **Scalability**: As the number of connected devices and data sources in urban environments continues to increase, edge computing allows for more efficient and scalable data processing by distributing the computational workload across multiple edge servers.
- **Latency reduction**: Edge computing allows data processing to occur closer to the source, reducing the latency associated with transmitting data to and from centralized data centers. This is particularly important for time-sensitive applications like traffic management and emergency response systems.
- **Enhanced security**: Decentralized edge computing platforms, like the Cyborg Network, employ advanced encryption and security measures to protect sensitive data from unauthorized access and tampering. This is critical for

maintaining the privacy and security of personal and sensitive information collected by smart city applications.

- **Improved resilience**: By distributing computational resources across multiple edge servers, edge computing platforms can improve the resilience of smart city systems, reducing the impact of localized failures and ensuring continuous operation in the face of disruptions.

6.2. Industrial Automation and Decentralized Edge Computing

In the realm of industrial automation, decentralized edge computing can deliver significant benefits by transforming the way industries manage and optimize their processes. As the Industrial Internet of Things (IIoT) becomes more prevalent, there is a growing need for secure, low-latency data processing and transmission to support the myriad of connected devices and applications in manufacturing, logistics, and other industrial sectors.

By processing data closer to the source, edge computing enables real-time monitoring of equipment, predictive maintenance, and quality control, which offers the following advantages:

- **Reduced downtime**: Real-time monitoring and predictive maintenance allow industries to identify potential equipment failures before they occur, minimizing downtime and reducing the costs associated with unexpected maintenance.
- **Improved efficiency**: Decentralized edge computing enables more efficient data processing and decision-making, allowing industrial processes to be optimized and streamlined. This can lead to reduced waste, lower energy consumption, and increased productivity.
- **Enhanced flexibility**: Edge computing supports implementing more agile and flexible production systems, making it easier for industries to adapt to changing market conditions and customer demands.
- **Greater data privacy and security**: Cyborg Network's decentralized infrastructure ensures a secure and transparent platform, allowing industries to maintain data privacy and protect sensitive information from unauthorized access or tampering.

6.3. Gaming, Entertainment, and the Impact of Low-Latency Edge Computing

The gaming and entertainment sectors are rapidly evolving, driven by advancements in technology and the growing demand for more immersive, interactive experiences. Emerging technologies like virtual reality (VR), augmented reality (AR), and cloud gaming require low-latency data processing and transmission to deliver seamless, real-time experiences to users. In this context, low-latency edge computing plays a crucial role in enhancing the overall quality of gaming and entertainment applications.

The Cyborg Network's decentralized approach to edge computing offers several advantages for the gaming and entertainment sectors:

- **Reduced latency**: By processing data closer to the users, the Cyborg Network significantly reduces the latency associated with data transmission and processing, ensuring smooth and responsive gaming experiences, especially in applications that require real-time interaction, such as VR and AR experiences.
- **Improved performance**: Decentralized edge computing can distribute the computational workload across multiple edge servers, allowing for more efficient and scalable processing of complex gaming and entertainment applications. This can result in better performance, even for users with limited local hardware resources.
- **Enhanced security and data privacy**: The Cyborg Network's blockchain-based infrastructure ensures that user data and digital assets are protected through advanced encryption and security measures, maintaining data privacy and security while still enabling high-quality gaming and entertainment experiences.
- **Support for innovative business models**: The Cyborg Network's decentralized nature and native tokenomics can facilitate the development of new, innovative business models in the gaming and entertainment sectors, such as decentralized content distribution, in-game asset ownership, and peer-to-peer trading.

6.4. Finance, Blockchain, and Decentralized Edge Computing

The financial sector is undergoing a significant transformation as it increasingly adopts blockchain technology and other innovative solutions to enable more secure, efficient, and transparent transactions. Decentralized edge computing platforms like the Cyborg Network can play a pivotal role in enhancing financial transactions' security, speed, and reliability, such as payment processing, identity verification, and asset management, by leveraging the inherent advantages of blockchain technology and smart contracts. This ensures that sensitive financial data remains secure while reducing the time and cost associated with traditional financial services.

Key benefits of incorporating decentralized edge computing in the financial sector include:

- **Enhanced security**: Decentralized edge computing platforms like the Cyborg Network employ advanced encryption and security measures to protect sensitive financial data from unauthorized access, tampering, and fraud. This is critical for maintaining trust and confidence in financial systems and services.
- **Reduced latency**: By processing financial transactions closer to the source, edge computing can significantly reduce latency, enabling faster and more

responsive financial services. This is particularly important for time-sensitive applications like high-frequency trading and real-time payment processing.

- **Improved scalability**: Decentralized edge computing platforms can distribute computational workloads across multiple edge servers, allowing financial systems to scale more efficiently as transaction volumes and data processing requirements grow.
- **Increased transparency**: Blockchain technology, which underpins the Cyborg Network, offers a transparent and auditable record of financial transactions, ensuring that all stakeholders have access to accurate, up-to-date information and promoting trust in the financial ecosystem.
- **Support for new financial products and services**: The combination of blockchain technology and decentralized edge computing can enable the development of innovative financial products and services, such as decentralized finance (DeFi) applications, tokenized assets, and digital identity solutions.

6.5. Edge AI and the Need for Decentralized Infrastructure

Edge AI refers to deploying artificial intelligence algorithms and models at the edge of the network, closer to the data sources. This approach enables faster processing, real-time decision-making, and reduced data transmission latency while optimizing bandwidth usage. As the demand for Edge AI solutions grows, there is an increasing need for a secure, scalable, and decentralized infrastructure to support their deployment and management. Cyborg Network's decentralized infrastructure addresses this need by providing a reliable platform for Edge AI applications, ensuring that data privacy, security, and ownership are maintained.

Key advantages of using decentralized infrastructure for Edge AI include:

- **Enhanced data privacy**: By processing data closer to the source, Cyborg Network's decentralized edge computing platform ensures that sensitive information remains secure and is less vulnerable to potential breaches or unauthorized access.
- **Improved performance**: Decentralized infrastructure allows for more efficient processing and decision-making at the edge, resulting in better performance for Edge AI applications and a more seamless user experience.
- **Scalability**: The Cyborg Network's decentralized edge computing platform can distribute computational workloads across multiple edge servers, allowing Edge AI applications to scale more efficiently as data processing requirements grow.
- **Reduced network congestion**: By processing data at the edge, the Cyborg Network minimizes the amount of data that needs to be transmitted across the network, reducing congestion and optimizing bandwidth usage.
- **Ownership and control**: The Cyborg Network's blockchain-based infrastructure enables the secure and transparent management of Edge AI algorithms and models, ensuring that data ownership, usage rights, and intellectual property are protected and respected.

7. Technical Details

The Cyborg Network utilizes the Rust programming language and Substrate framework for its core development, along with ink! smart contracts for implementing business logic on the platform. The initial consensus algorithm employed is Proof of Authority (PoA), which provides a secure and efficient method for validating transactions and maintaining the integrity of the blockchain. The platform may transition to a different consensus algorithm based on evolving requirements and technological advancements.

7.1. On-chain entities

- **Runtime -** A custom substrate runtime plays a pivotal role in facilitating the functionalities required to ensure the system runs harmoniously across various ends. It manages smart contract execution, transaction processing, state management, resource allocation, consensus rule enforcement, security measures, and gas fee calculation, all while integrating seamlessly with the network layer to maintain the integrity and reliability of the blockchain platform.

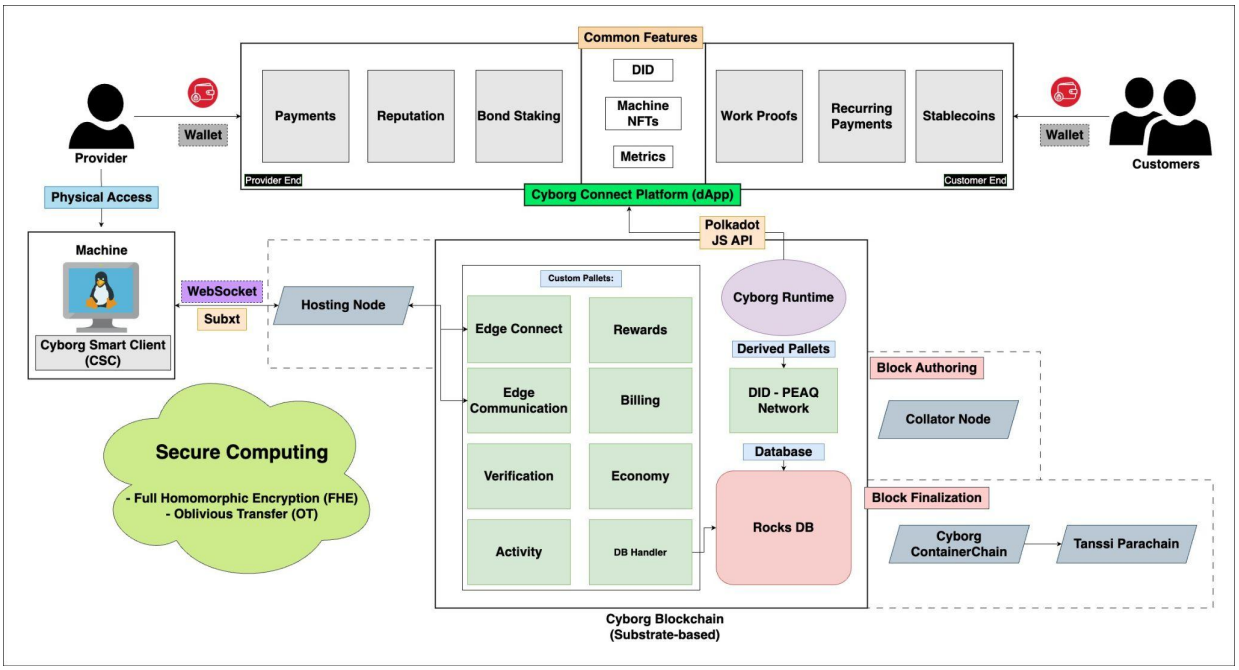


Fig. 2. Cyborg Network technical Architecture

- **RocksDB -** Our custom RocksDB implementation is adept at efficiently managing the state transition records of the blockchain and crucial business-related information. This specialized implementation ensures the integrity, persistence, and fast retrieval of data, making it a cornerstone for

maintaining the operational efficiency and reliability of the blockchain system.

7.2. Custom Pallets

Cyborg Network utilizes custom pallets as modular parts that construct the runtime to be able to perform as expected.

- **Pallet Edge Connect** - The Edge Connect custom substrate pallet is purpose-built to streamline and ensure uninterrupted communication between edge servers under provider management and the Cyborg substrate blockchain. Its primary function is to establish a seamless connection, guaranteeing the continuous availability and reliability of the connected machines.
- **Pallet Edge Communication** - At the core of the system, the Edge Communication pallet encompasses the foundational structure responsible for implementing an encrypted communication protocol. Leveraging lattice-based cryptography techniques, it performs a Full Homomorphic Encryption (FHE) on the data intended for transmission to the provider. Collaborating closely with the Edge Connect pallet, these components work in tandem to facilitate the seamless operation of the hosting node, enhancing security and privacy in the network.
- **Pallet Verification** - The verification pallet introduces essential functionality for validating preprocessed computation results obtained from random providers who assume the role of verifiers within this assignment. It establishes a task pool akin to the Ethereum mempool, from which verifiers can select tasks. These tasks involve re-running portions of the proof and conducting distance calculations to assess the validity of the computations. The resulting distances, in conjunction with the threshold calculated during the profiling stage, are utilized by the chain to determine the consistency of the verification with the provided proof. This critical process ensures the integrity and reliability of the blockchain's computational results.
- **Pallet Activity** - Our custom functionality is designed to meticulously log the network activities of participants and machines within the network. Collaborating seamlessly with the DID pallet, it generates a reputation score for connected entities by analyzing their diverse interactions over time. This reputation score is pivotal, serving as a mechanism to instill discipline among providers and as a foundation for fostering trust within the decentralized ecosystem. Furthermore, it opens the door to introducing innovative product segments, enhancing the overall dynamics of the system.
- **Pallet Rewards** - This custom pallet is responsible for calculating the rewards to be distributed to providers and verifiers based on their execution of computational tasks. It leverages key metrics and information obtained from the verification pallet, specifically focusing on successfully verifying tasks. Subsequently, it issues instructions to the runtime,

facilitating the disbursement of rewards in the form of BORG tokens ensuring that participants are duly compensated for their contributions.

- **Pallet Billing** - This custom pallet introduces a subscription-based customer billing system seamlessly integrated with OAK Network's automated recurring payments feature. Engineered for efficiency, this pallet specializes in aggregating monthly billing aligning charges with customer usage patterns. The objective is to streamline the billing process, eliminating individual payment requirements for each instance and instead delivering a unified invoice associated with their Decentralized Identities (DIDs). This approach simplifies billing and enhances the overall user experience by providing a consolidated, user-friendly billing system.
- **Pallet Economy** - This custom pallet introduces a novel billing mechanism based on stablecoins, designed to enhance the customer experience. While loosely coupled to the Billing pallet, it seamlessly facilitates payments using fiat stablecoins provided by Pendulum. Simultaneously, it contributes to the stability and growth of the native token economy by sharing profits with the Cyborg treasury. This innovative approach combines the benefits of stablecoins with the native token ecosystem to ensure a robust and versatile billing system.
- **Pallet DB Handler** - The DB Handler custom pallet is intricately designed to oversee all interactions with the on-chain RocksDB database, guaranteeing the seamless operation of the system. It closely collaborates with other pallets, facilitating database queries and record updates to cater to a wide range of functional requirements beyond the chain state information. This pallet plays a pivotal role in maintaining the integrity and efficiency of the on-chain database, enhancing the system's overall functionality.

7.3. Derived Pallets

Other than using our own pallets, we would also utilize pallets from the ecosystem project to better collaborate, speed up the process, and save time. Some examples are as follows:

- **Pallet DID** (Peaq Network) - This derived pallet is a vital link, associating users with PEAQ Decentralized Identities (DIDs) and mapping their deployments to unique machine NFTs. This strategic connection ensures a seamless and efficient representation of various participants within the network, enhancing the overall mapping and identity management capabilities.

8. Providers Onboarding

Providers onboarding is the process that is really significant to make our network trustworthy and reliable. To make providers' onboarding process as smooth as possible, we designed the steps as follows:

- **Wallet and DID Integration**: Providers are required to integrate their digital wallets with the Decentralized Identity (DID) system within the Cyborg Connect application. This connection associates their identity with the platform, enhancing security and accountability.
- **Machine Addition**: Providers can add a new edge computing machine by entering basic information about the device. This information may include machine specifications, location, and intended usage. Upon submission, the system generates a unique download link for the Cyborg Smart Client (CSC) binary, tailored for the specific machine.
- **CSC Installation**: Providers receive the unique download link for the CSC binary, which they must execute on the target virtual machine (VM) where they intend to dedicate computing resources. The CSC binary is installed with root access to the VM.
- **Connection Establishment**: Once installed, the CSC binary immediately establishes a connection with the nearby hosting node in the edge computing network. This connection enables seamless communication and coordination between the provider's machine and the larger network.
- **Dashboard Update**: Information about the newly connected machine is updated in the provider's dashboard within the Cyborg Connect application. This dashboard serves as a control center where providers can monitor their machines' status, usage metrics, and performance.
- **Machine NFT Minting**: As a confirmation of the successful connection and setup of the new machine, a unique Machine NFT (Non-Fungible Token) is minted and associated with the provider's account. This NFT records the machine's presence and its state over time, providing a valuable resource for tracking and management.

By following these steps, providers seamlessly integrate their machines into the decentralized edge computing network, enabling them to contribute computational resources and participate in the network's activities. The integration process ensures a secure and efficient onboarding experience for providers while promoting transparency and accountability within the ecosystem.

9. Customer Workflow

The typical usage of the protocol involves four distinct stages, with each role performing specific tasks.

9.1. Task Submission

At the outset, users or clients initiate the process by submitting tasks intended for execution on edge devices. Each task encompasses the following vital components:

a. **Task Description and Metadata**: Submitters furnish comprehensive task descriptions, including specifications, metadata, and hyperparameters. This information is presented in a machine-readable and standardized format to ensure seamless compatibility across diverse edge devices.
b. **Task Payload**: The task payload comprises specific instructions and code necessary for executing the task on edge devices. This can be a lightweight binary or a containerized application tailored to the unique demands of edge environments.
c. **Data Location**: Submitters precisely define the location of any requisite data, such as input datasets or reference models. This data may reside in decentralized storage systems like IPFS, Arweave, or Subspace, rendering it publicly accessible to edge devices.

9.2. Execution

Once the task is submitted, the provider's machine undertakes the responsibility of executing the task in accordance with the provided instructions. Upon task completion or the attainment of predefined key milestones aligned with the task definition, the blockchain is promptly updated to record these significant events.

This workflow ensures a systematic and efficient process for task submission, execution, and blockchain-based tracking in the context of decentralized edge computing.

9.3. Verification

After task completion, Providers report the task's execution status to the blockchain and provide their proof-of-learning, which is publicly accessible for Verifiers. Verifiers retrieve verification tasks from a common task pool (similar to the Ethereum mempool) and proceed to re-run specific parts of the proof while conducting distance calculations. The resulting distances are then utilized by the chain to determine whether the verification aligns with the provided proof.

This process guarantees the integrity and accuracy of task execution and verification within the system.

9.4. Settlement

Within the settlement phase, participants receive compensation in accordance with the results of probabilistic and deterministic assessments. Various compensation scenarios are enacted, contingent upon the outcomes of prior verifications and challenges.

When the work is confirmed to be executed accurately, and all verifications are successful, both the Provider and Verifier are duly rewarded based on the performed operations.

10. Future Development

10.1. Research

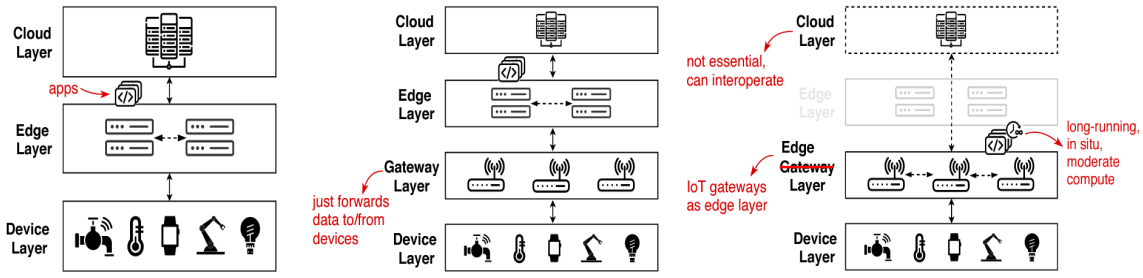
Our dedication to advancing the field of low-latency computing encompasses ongoing research in three critical areas, aiming to optimize the protocol's performance:

- **Advanced Verification Methods**: We will concentrate on developing cutting-edge verification techniques that exploit probabilistic approaches, utilizing metadata generated during optimization processes. This research seeks to fortify work verification, ensuring the integrity of tasks executed in low-latency computing environments [18].
- **Deterministic Work Verification**: Our ongoing research focuses on pinpoint verification techniques. These methods are designed to validate deterministic tasks in low-latency computing on-chain, providing a robust framework for verifying the accuracy and reliability of low-latency computational processes [19].
- **Hardware-Agnostic Parallelization**: To address the unique challenges of low-latency computing, we will explore efficient methods for parallelizing computational tasks across heterogeneous hardware with strict latency constraints. This research initiative aims to optimize the performance of diverse computational workloads and expand the protocol's applicability to various low-latency task types [20].
- **Advanced Hardware Security Enclaving**: A secure enclave provides CPU hardware-level isolation and memory encryption on every server by isolating application code and data from anyone with privileges and encrypting its memory.

Advanced hardware security enclaving for edge computing involves the integration of specialized security measures to safeguard sensitive data and processes at the edge. This includes the deployment of secure elements such as Hardware Security Modules (HSMs) [21], Trusted Platform Modules (TPMs), and Secure Enclave Processors (SEPs). These components create isolated and tamper-resistant environments, ensuring the confidentiality and integrity of critical operations.

10.2. Leveraging IoT Gateway for Edge Computing Platform:

Increasing the responsibility of edge gateways, e.g.running applications directly on the gateways rather than on edge servers, is counterintuitive. Edge servers



(a) Edge Computing Architectures

(b) Actual implementations use gateways

(c) Shift applications to gateways

offer more resources for applications, including storage, memory, and heavy computing (CPU and GPU), and are less prone to failures. However, Nasir et al. [22] make five observations that suggest edge computing can benefit from leveraging these gateways, particularly when applications are using IoT devices. First, since the gateway shaves more deployment flexibility and includes wireless radios to communicate with devices, applications running on gateways can operate one hop from sensors and actuators and leverage protocol-specific information for optimizations. Second, streaming all data to centralized edge servers increases network traffic and application latency. This overhead can be reduced if applications can be executed on gateways instead. Third, advances in single-board computers like the fourth-generation Raspberry Pi have made IoT gateways increasingly performant. Gateways are capable enough to support containerized environments and are increasingly being used for various kinds of edge applications. Fourth, edge servers can be costly (exceeding $ 1,000), and leveraging gateways can make edge computing feasible for cost-conscious deployments. Finally, spatially large IoT deployments already have multiple gateways for network coverage, and leveraging them increases their value without incurring additional hardware and installation costs.

10.3. Development Phases

The development of the Cyborg Network will progress through three distinct phases: *test network*, *canary network*, and *main network*.

A. Test Network

In the initial development phase, we will focus on creating a test network (*testnet*) implementation of the core technology. Tokens used on the testnet will be non-permanent, and participation will be limited to early adopters and core community members, who will be rewarded during the Token Generation Event (TGE).

B. Canary Network

Following a successful testnet iteration, the protocol will launch as a canary network (*canarynet*) parachain on the Kusama relay chain. The canary utility token with real economic value will be introduced during this phase. The canary network serves as a beta version of the protocol, offering access to the latest features and some level of risk. Typically, canary networks provide slightly lower prices and access to cutting-edge R&D functionality.

C. Main Network

After a successful parachain launch on the Kusama relay chain, the final live parachain as our main network (*mainnet*) will be launched on the Polkadot relay chain. This phase marks the release of the mainnet utility token, which becomes the primary utility token for the protocol. The mainnet is the fully operational, stable protocol available for use by organizations and individuals. Any features or changes undergo testing in the testnet and canarynet phases before being launched on the mainnet.

10.4. Tokenomics

The Cyborg Network will utilize its native utility token, namely Cyborg Token (BORG), to power the platform's ecosystem and incentivize participation. The token will be used for various purposes, including:

- **Transaction fees**: Users will pay transaction fees in BORG tokens for utilizing the platform's edge computing services.
- **Incentives for edge server providers**: Edge server providers will earn BORG tokens as a reward for contributing their resources to the network.
- **Staking and governance**: Token holders can stake their BORG tokens to participate in network governance, proposing and voting on changes to the platform's parameters and policies.

The total supply of BORG tokens will be capped, with an initial allocation for the development team, advisors, and early backers and a reserve for future ecosystem growth and development.

Conclusion

The Cyborg Network is poised to transform the landscape of edge computing by delivering a robust, decentralized, and transparent platform that caters to a wide range of industries and applications. Through real-time data processing and analysis, we're committed to providing unparalleled data privacy and security to meet the growing demand for efficient and low-latency solutions in an increasingly connected world. By leveraging the power of blockchain technology, the Cyborg Network addresses the limitations of traditional cloud computing and data centers. It fosters a vibrant ecosystem of edge server providers, developers,

and end-users. Our innovative platform incentivizes participation and collaboration, ensuring that the benefits of decentralized edge computing are accessible and affordable to all. Our vision is to usher in a new era of edge computing where individuals, businesses, and communities around the globe can harness the potential of decentralized technology to drive innovation, efficiency, and security. To achieve this, we will continue to invest in research, development, and partnerships, ensuring that the Cyborg Network remains at the forefront of technological advancements in edge computing and blockchain solutions. As we embark on this journey, we are dedicated to building a strong and supportive community that shares our passion for decentralized technology and its transformative potential. Through ongoing communication, collaboration, and education, we aim to empower our users and partners with the knowledge and tools they need to harness the full potential of the Cyborg Network. We recognize that the road ahead is filled with challenges and opportunities, but we are confident that our experienced team, innovative technology, and unwavering commitment to our mission will enable us to overcome any obstacles and forge a new path in the world of edge computing. By working together, we believe we can make a lasting and positive impact on the future of technology and the world. In conclusion, the Cyborg Network is not just a project but a bold and ambitious vision for the future of edge computing. We invite you to join us as we strive to revolutionize how data is processed, transmitted, and protected, creating a more connected, secure, and efficient world for all.

References

[1.] J. Xu, B. Palanisamy and Q. Wang, "Resilient Stream Processing in Edge Computing," 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid), Melbourne, Australia, 2021, pp. 504-513, doi: 10.1109/CCGrid51090.2021.00060.

[2.] Carvalho, G., Cabral, B., Pereira, V. et al. Edge computing: current trends, research challenges, and future directions. Computing 103, 993–1023, 2021. https://doi.org/10.1007/s00607-020-00896-5

[3.] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 2008.

[4.] V. Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf, 2014.

[5.] G. Wood. Polkadot: Vision For A Heterogeneous Multi-chain Framework. https://assets.polkadot.network/Polkadot-whitepaper.pdf, 2016.

[6.] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu and W. Lv, "Edge Computing Security: State of the Art and Challenges," in Proceedings of the IEEE, vol. 107, no. 8, pp. 1608-1631, Aug. 2019, doi: 10.1109/JPROC.2019.2918437.

[7.] H. El-Sayed et al., "Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment," in IEEE Access, vol. 6, pp. 1706-1717, 2018, doi: 10.1109/ACCESS.2017.2780087.

[8.] Ernest Bonnah and Ju Shiguang. DecChain: A decentralized security approach in Edge Computing based on Blockchain. Future Generation Computer Systems, Volume 113, Pages 363-379, 2020. https://doi.org/10.1016/j.future.2020.07.009.

[9.] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee. TrustChain: A Privacy Preserving Blockchain with Edge Computing. Wireless Communications and Mobile Computing, Article 2014697, 2019. https://doi.org/10.1155/2019/2014697

[10.] Deepika Natarajan, Andrew Loveless, Wei Dai, Ronald Dreslinski. CHEX-MIX: Combining Homomorphic Encryption with Trusted Execution Environments for Two-party Oblivious Inference in the Cloud. Cryptology ePrint Archive, Paper 2021/1603, 2021.

[11.] Z. Zheng, P. Xie, X. Zhang, S. Chen, Y. Chen, X. Guo, G. Sun, G. Sun, L. Zhou. Agatha: Smart Contract for DNN Computation. Cryptography and Security ePrint Archive, Paper 2105.04919, 2021.

[12.] J. Teutsch and C. Reitwießner. A scalable verification solution for blockchains. Cryptography and Security ePrint Archive, Paper 1908.04756, 2019.

[13.] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang and C. S. Hong, "Edge-Computing-Enabled Smart Cities: A Comprehensive Survey," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10200-10232, Oct. 2020, doi: 10.1109/JIOT.2020.2987070.

[14.] S. Stankovski, G. Ostojić, I. Baranovski, M. Babić and M. Stanojević, "The Impact of Edge Computing on Industrial Automation," 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2020, pp. 1-4, doi: 10.1109/INFOTEH48170.2020.9066341.

[15.] K. Bilal and A. Erbad, "Edge computing for interactive media and video streaming," 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), Valencia, Spain, 2017, pp. 68-73, doi: 10.1109/FMEC.2017.7946410.

[16.] V. Kumar, Z. Wang, J. Lu, M. Li, S. Yang, Y. Wang, X. Cheng. Edge Computing and Blockchain in Enterprise Performance and Venture Capital Management. Computational Intelligence and Neuroscience, Article 2914936, 2022. https://doi.org/10.1155/2022/2914936

[17.] A. Nawaz, T. N. Gia, J. P. Queralta and T. Westerlund, "Edge AI and Blockchain for Privacy-Critical and Data-Sensitive Applications," 2019

Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU), Kathmandu, Nepal, 2019, pp. 1-2, doi: 10.23919/ICMU48249.2019.9006635.

[18.] U. Guin, P. Cui and A. Skjellum, "Ensuring Proof-of-Authenticity of IoT Edge Devices Using Blockchain Technology," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1042-1049, doi: 10.1109/Cybermatics_2018.2018.00193.

[19.] Dongdong Yue, Ruixuan Li, Yan Zhang, Wenlong Tian, Yongfeng Huang. Blockchain-based verification framework for data integrity in edge-cloud storage. Journal of Parallel and Distributed Computing, Volume 146, Pages 1-14, 2020. https://doi.org/10.1016/j.jpdc.2020.06.007.

[20.] A. Ejjeh et al., "HPVM: Hardware-Agnostic Programming for Heterogeneous Parallel Systems," in IEEE Micro, vol. 42, no. 5, pp. 108-117, 1 Sept.-Oct. 2022, doi: 10.1109/MM.2022.3186547.

[21.] S. Mavrovouniotis and M. Ganley. Hardware Security Modules. Secure Smart Embedded Devices, Platforms and Applications, Springer New York, pp 383–405, 2014. https://doi.org/10.1007/978-1-4614-7915-4_17.

[22.] N. Nasir, V. A. L. Sobral, L. -P. Huang and B. Campbell, "NexusEdge: Leveraging IoT Gateways for a Decentralized Edge Computing Platform," 2022 IEEE/ACM 7th Symposium on Edge Computing (SEC), Seattle, WA, USA, 2022, pp. 82-95, doi: 10.1109/SEC54971.2022.00014.