AIOS: A Blockchain-based AI Matrix

Satoshi Nakamoto Jr.[1], Logic[1]

[1]**AIOS Lab**

V1.0
March 2025

Abstract

The convergence of AI and blockchain technology presents a transformative opportunity to address contemporary challenges in ethics, security, and social inequality. While AI promises efficiency and innovation, its deployment has raised concerns regarding transparency, accountability, and bias. Blockchain offers solutions by ensuring transparency, decentralization, and trust. This whitepaper proposes a framework for integrating blockchain with AI to create a decentralized **AIOS** (AI Operating System)-a platform designed to foster fairness, security, financial inclusion, and autonomy. By utilizing blockchain's inherent features, this paper explores algorithms, models, and formulations that will drive the AIOS, envisioning a world of equality, freedom, and trust in AI systems. Additionally, the paper introduces Federated Learning and Neural Networks as critical components for achieving data privacy, model scalability, and efficient decentralized training within the AIOS framework.

1. Introduction

The world is facing significant challenges in deploying AI systems that are transparent, secure, and equitable. The lack of trust in AI decisions, especially in critical areas such as healthcare, finance, and law, has led to concerns about AI's potential for reinforcing social inequalities. Blockchain technology offers a solution to some of these challenges, with its features of immutability, decentralization, and transparency. When integrated with AI, blockchain has the potential to create the AIOS-an operating system that ensures the AI-driven decision-making process is transparent, fair, secure, and accessible to all. This whitepaper presents a technical framework for combining AI and blockchain in the creation of AIOS, focusing on the implementation of Federated Learning, Neural Networks, smart contracts, and cryptographic proofs. We also propose formulations that demonstrate how the AIOS will function to uphold equality, freedom, and autonomy.

2. Blockchain for Security and Transparency

2.1. Basic Concepts

The core of blockchain's security comes from its decentralized nature and cryptographic techniques. Blockchain utilizes a distributed ledger to record transactions (or data points), making it virtually immutable. Each block in the chain is cryptographically linked to the previous one, making tampering with the data computationally infeasible. Let $\{\mathcal{B}\}=\{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, ..., \boldsymbol{b}_n\}$ represent the blockchain where each $\boldsymbol{b}_i$ is a block containing the following:

- $\boldsymbol{H}(\boldsymbol{b}_i)$: The block hash, a unique fingerprint of the data contained within block $\boldsymbol{b}_i$).
- $\boldsymbol{H}(\boldsymbol{b}_{i-1})$: The hash of the previous block, ensuring the chain's immutability.
- $\boldsymbol{Data}_T$: Transaction Data, information that needs to be stored securely, such as personal or financial data.

The data structure of each block can be represented as:

$$\boldsymbol{b}_i = \{\boldsymbol{Data}_T, \boldsymbol{H}(\boldsymbol{b}_{i-1}), \boldsymbol{H}(\boldsymbol{b}_i), \boldsymbol{Timestamp}, \boldsymbol{Nonce}\} \tag{1}$$

2.2. PoC(Proof of Contribution)

While **PoW** (Proof of Work) is a well-known consensus algorithm of Bitcoin [1], it can be inefficient in terms of energy consumption. To address this challenge in the AIOS, we propose a **PoC**(Proof of Contribution) mechanism. PoC allows participants to contribute resources (computational power, data, or decisions) toward the development and governance of the AIOS without relying on resource-intensive mining processes. In the PoC model, participants are rewarded based on the value they add to the system rather than simply processing power. For example, a participant who contributes a high-quality dataset for training an AI model, or who proposes an important model update, will receive a proportional reward in the form of tokens or governance rights. The mathematical formulation for PoC can be expressed as:

$$\boldsymbol{C}_i = \boldsymbol{f}(\boldsymbol{contribution}_i, \boldsymbol{value}_i) \tag{2}$$

where:

- $\boldsymbol{C}_i$: The contribution score of participant $\boldsymbol{i}$,
- $\boldsymbol{contribution}_i$: The actual contribution (whether computational, data-related, or other forms of work),
- $\boldsymbol{value}_i$: The perceived value of the contribution (determined by the community, stakeholders, or DAO).

A higher $\boldsymbol{C}_i$ will result in greater rewards or influence within the AIOS ecosystem. The PoC model ensures that participants are incentivized to contribute meaningfully, thereby ensuring the decentralized and collaborative nature of the system.

2.3. Patricia Tree and "Pash" Value

To further enhance the efficiency of the blockchain in the AIOS, we introduce the concept of the **Patricia Tree** and the **Pash** for managing data integrity, access speed, and contribution tracking within the decentralized ecosystem.

2.3.1. *Patricia Tree*

A **Patricia Tree** (or **P**ractical **A**lgorithm to **R**etrieve **I**nformation **C**oded in **A**lphanumeric, or **Radix Tree**) [2] is a type of compressed tree data structure that is particularly effective for storing a set of keys that share common prefixes. In blockchain systems, Patricia Trees can be used to efficiently store and retrieve blocks and transaction records, reducing the storage and computational overhead. The Patricia Tree algorithm works by merging nodes with common prefixes, reducing the depth of the tree and the number of comparisons required to look up a value. This tree structure can be used to represent the global model in an AIOS that undergoes frequent updates through Federated Learning. Each participant's contribution to the global model (e.g., updates or weights) can be tracked and stored in the Patricia Tree, ensuring efficient retrieval and verification of contributions. Mathematically, the Patricia Tree can be defined as:

$$\boldsymbol{T = PatriciaTrie}(\{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, ..., \boldsymbol{b}_n\}) \tag{3}$$

where $\boldsymbol{T}$ is the Patricia Tree that holds transaction or block information, and $\boldsymbol{b}_i$ represents each block or transaction.

2.3.2. *"Pash" Value*

Different from **Hash** value, the **"Pash"** value is introduced as a dynamic metric for quantifying the value of each participant's contribution in the AIOS. Unlike fixed reward models, the **"Pash"** value takes into account the quality and relevance of contributions in a decentralized system. The Pash Value$\boldsymbol{P}_i$ can be formulated as:

$$\boldsymbol{P}_i = \boldsymbol{g}(\boldsymbol{value}_i, \boldsymbol{reputation}_i, \boldsymbol{impact}_i) \tag{4}$$

where:

- $\boldsymbol{P}_i$: The **"Pash"** value assigned to participant $\boldsymbol{i}$,
- $\boldsymbol{value}_i$: The direct contribution of participant $\boldsymbol{i}$ (e.g., model update),
- $\boldsymbol{reputation}_i$: The trust or reliability score based on past behavior or contributions,
- $\boldsymbol{impact}_i$: A measure of how much the contribution improved the system or model.

The **"Pash"** value ensures that participants are rewarded not only for the quantity of their contributions but also for the quality and long-term impact they have on the system. This concept helps prevent manipulation or exploitation of the system by malicious actors, and instead, rewards those who contribute meaningfully and positively.

3. AI for Decision Making and Automation

3.1. AI Algorithms and Model Training

AI models, particularly ML (machine learning) and DL(deep learning) [3], can be used to automate decision-making processes in various domains such as healthcare, law, and finance. To ensure fairness and transparency, the data used to train these models must be decentralized, verifiable, and free from biases. Let $\{\mathcal{D}\}$=$\{\boldsymbol{d}_1, \boldsymbol{d}_2, \boldsymbol{d}_3, ..., \boldsymbol{d}_m\}$ represent a dataset used to train an AI model. The model's output $\boldsymbol{f}(\boldsymbol{x})$ can be formulated as:

$$\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{\theta}_0 + \sum_{i=1}^{n} \boldsymbol{\theta}_i \boldsymbol{x}_i \tag{5}$$

where $\boldsymbol{\theta}_i$ are the parameters learned during training, and $\boldsymbol{x}_i$ is the input feature for the model. However, to ensure fairness, we must address potential biases in $\mathcal{D}$. One approach is to use blockchain-based data verification mechanisms to ensure that the data is unbiased, complete, and accurately represents the diversity of the population.

3.2. Blockchain-based Data Source for AI

To ensure that AI models are trained on fair and verified data, we integrate blockchain to track the provenance of datasets used in training. Let $\boldsymbol{S}$ represent the source record of a dataset, which includes information about its source, modification history, and intended use. Each time a new dataset is added or modified, a blockchain transaction is recorded to guarantee the authenticity and integrity of the data:

$$\boldsymbol{S_{new}} = \boldsymbol{BlockchainTransaction}\,(\mathcal{D}, \boldsymbol{H(S)}, \boldsymbol{Timestamp}, \boldsymbol{Metadata}) \tag{6}$$

The provenance record ensures that the data used by AI models is transparent and verifiable, reducing the risk of bias.

4. Federated Learning and Neural Networks

In the context of AIOS, Neural Networks can be deployed across a federated system to leverage decentralized learning while ensuring transparency and integrity through blockchain. The blockchain logs the training updates made by each federated node and guarantees that no malicious updates can corrupt the global model. The following **3** rules need to be followed:

- Each device participates in training a Neural Network using Federated Learning.
- Blockchain ensures Transparency of the model updates, and Smart Contracts [4] enforce fairness and compliance with ethical standards.
- A DAO(Decentralized Autonomous Organization) governs model updates and ethical guidelines, ensuring that the system operates autonomously while maintaining human oversight.

4.1. Federated Learning for Privacy-Preserving AI

Federated Learning is a decentralized machine learning approach that allows multiple participants (e.g., users, devices, or organizations) to collaboratively train a shared model without exchanging raw data. This allows users to retain control over their private data while benefiting from the model's training process. Federated Learning fits perfectly within the AIOS as it ensures that no centralized authority gains access to sensitive data while also allowing collective improvements to the AI system. The process of Federated Learning can be formulated as follows:

$$\boldsymbol{M_{new}} = \sum_{\boldsymbol{k=1}}^{\boldsymbol{n}} \frac{\boldsymbol{\Delta M_k}}{k} \tag{7}$$

where:

- Let $\boldsymbol{M}$ be the global model, which is initially trained using a local dataset at each device. Each device $\boldsymbol{k}$ has a local dataset $\mathcal{D}_{\boldsymbol{k}}$=$\{\boldsymbol{d}_1, \boldsymbol{d}_2, \boldsymbol{d}_3, ..., \boldsymbol{d}_n\}$.
- Each participant computes local updates to the model, denoted by $\boldsymbol{\Delta M_k}$. These updates are shared (not the raw data) with the AIOS VM [4](Virtual Machine), which aggregates the updates to form the global model.

- k is the number of participating devices.

This process ensures that sensitive data is never shared, thus preserving user privacy. Federated Learning combined with blockchain guarantees the integrity and transparency of the model updates, ensuring that all participants can verify the process and the outcomes of the training without exposing private information.

4.2. Neural Networks for AI Decision Making

Neural networks, particularly deep learning models, are essential for tasks like image recognition, natural language processing, and complex decision-making. Neural networks consist of layers of interconnected nodes (neurons) that transform input data into predictions or classifications. The mathematical formulation for a basic neural network can be expressed as:

$$y = \sigma(W_2(\sigma\ (\ W_1 x + b_1) + b_2) \tag{8}$$

where:

- x:The input features,
- $W_1,\ W_2$:The weight matrices,
- $b_1,\ b_2$:The bias terms,
- σ:Activation function (e.g., ReLU, Sigmoid),
- y:The output prediction.

The layers in the network adjust the weights W_1, W_2 during training via backpropagation, minimizing the loss function $\mathcal{L}(y, \widetilde{y})$ where $\widetilde{y}$ is the target output.

5. AIOS Architecture

The AIOS architecture draws inspiration from the classic Von Neumann Architecture [5] while utilizing decentralized technologies like blockchain, distributed storage networks, and AI-driven agents. In this context, various components of the AIOS correspond to the fundamental parts of a computer system, but they are distributed and decentralized to ensure scalability, security, and transparency. The Table 1 shows the analogy between AIOS and Von Neumann's architecture:

Von Neumann		AIOS
Processing Unit	⇔	**Decentralized Computing Network**
Control Unit	⇔	**Blockchain Network**
Memory Unit	⇔	**Distributed Storage Network**
Input	⇔	**Data Pump**
Output	⇔	**AI Agent Hub**

Table 1 | *Comparison of Von Neumann Architecture components and AIOS Architecture components*

The following Figure 1 illustrates the overall AIOS architecture, with the four key components:Processing Unit, Control Unit, Memory Unit, and Input and Output. All these components work together in a decentralized ecosystem.

This architecture ensures that the AIOS is not only efficient but also self-governing, transparent, and fair in its operation.

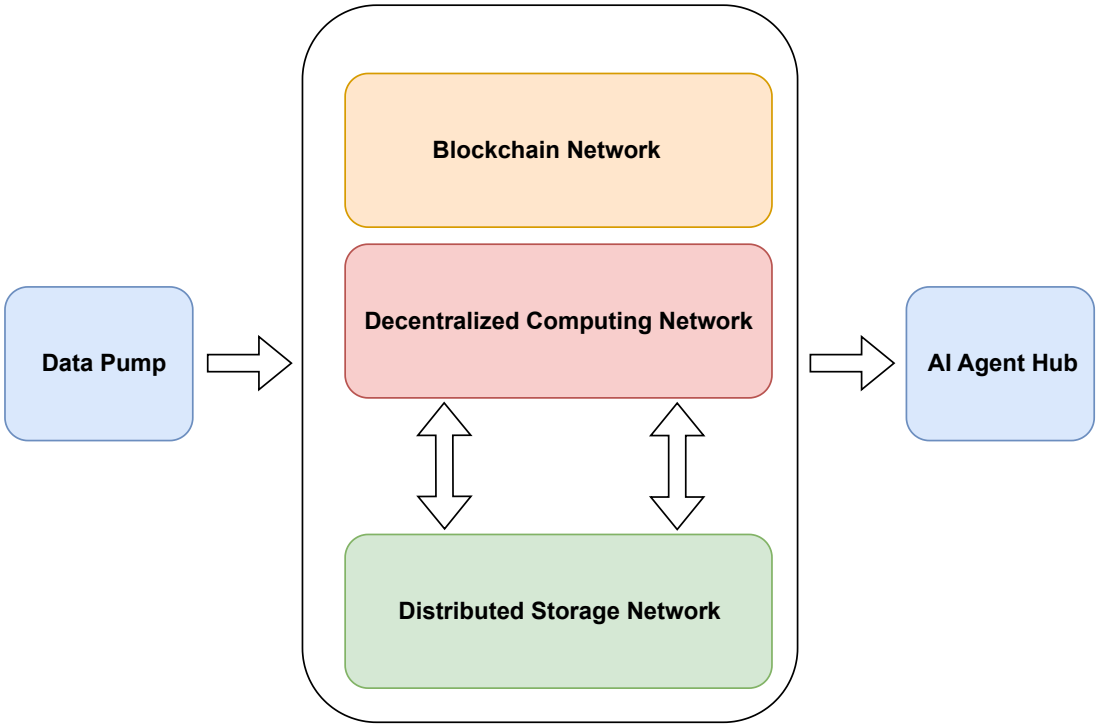

Figure 1 | *AIOS Architecture*

5.1. Processing Unit: Decentralized Computing Network

In the Von Neumann Architecture, the Processing Unit is responsible for executing instructions and carrying out computations. In AIOS, this role is played by a **Decentralized Computing Network** that consists of distributed nodes performing computational tasks across the network. These nodes can be individual devices, servers, or even edge devices that contribute computational resources.

- ***Function***: The Decentralized Computing Network acts as the computational backbone of the AIOS, processing tasks related to AI model training, decision-making, and data analysis. In Federated Learning, for instance, each node (or client) trains local models using its own data, and these updates are later aggregated to form a global model.
- ***KeyBenefits***: This decentralized approach to processing ensures the AIOS remains scalable, allowing for high levels of parallelism and avoiding the bottlenecks associated with centralized processing. It also ensures that no single point of failure can disrupt the system.

5.2. Control Unit: Blockchain Network

The Control Unit in the Von Neumann Architecture oversees the operation of the computer, directing the flow of data between different components and ensuring that tasks are executed in the correct sequence. In AIOS, the **Blockchain Network** serves as the Control Unit, ensuring transparency, security, and accountability in decision-making and data flow.

- ***Function***: The Blockchain Network manages the overall governance of the AIOS. It pro-

vides an immutable ledger to record all actions, including AI model updates, token minting/burning, and user interactions. It also ensures decentralized control via smart contracts, which automatically execute predetermined agreements based on specific conditions.

- ***KeyBenefits***: The blockchain serves as the **"brain"** of the AIOS, ensuring that the network remains trustless and transparent. Every transaction, model update, and change in system state is recorded on the blockchain, making the system auditable and reducing the potential for malicious activity.

5.3. Memory Unit: Distributed Storage Network

The Memory Unit in Von Neumann's model is responsible for storing data and instructions. In the AIOS, this role is fulfilled by a **Distributed Storage Network**, where data is stored across multiple nodes in a decentralized manner. This distributed storage system ensures that the AIOS operates efficiently and remains resilient to data loss or tampering.

- ***Function***: The Distributed Storage Network holds the large datasets used for training AI models, as well as logs of transactions and updates that occur within the blockchain network. It ensures that data is stored securely, redundantly, and in a way that is accessible to authorized nodes in the network.
- ***KeyBenefits***: By decentralizing data storage, the Distributed Storage Network ensures that the AIOS is not reliant on any central server or data center. This greatly enhances security and data sovereignty, ensuring that users' data remains under their control.

5.4. Input: Data Pump

The Input function in Von Neumann's model deals with receiving and processing incoming data. In AIOS, this role is played by the **Data Pump**, a high-performance data migration and extraction tool designed to efficiently extract data and metadata between distributed databases.

- ***Function***: The Data Pump facilitates rapid data extraction and movement across the AIOS ecosystem. It employs advanced parallel processing techniques and data compression to enhance the speed and efficiency of data transmission. The tool is designed to seamlessly integrate with various distributed storage solutions, ensuring optimized data flow.
- ***KeyBenefits***: The Data Pump improves the efficiency of AIOS by significantly reducing data transfer times, enhancing data accessibility, and ensuring seamless integration between different network nodes. This results in improved AI model performance and better user experience.

5.5. Output: AI Agent Hub

The Output function in Von Neumann's model deals with interfacing with the outside world. In AIOS, this role is played by the **AI Agent Hub**, a decentralized collection of AI agents responsible for interacting with external systems and users, providing output and decision-making assistance.

- ***Function***: The AI Agent Hub allows external users, devices, and systems to interact with the AIOS. AI agents can process external data, make decisions based on the AI models stored in the system, and provide results to the users. This hub handles various tasks such

as natural language processing, recommendation systems, and decision support systems that directly interface with the user.
- $KeyBenefits$: The AI Agent Hub ensures that the AIOS can interact with users and external systems efficiently, while also providing the flexibility to handle a variety of AI-driven tasks. It acts as the face of the AIOS to the outside world, making it user-friendly and responsive.

6. Trust and Fairness

To ensure that the AIOS operates fairly and transparently, we propose the following fairness metric F for evaluating AI decision-making:

$$F = \sum_{i=1}^{n} |f_i(x) - f_{ideal}(x)| \tag{9}$$

where:

- $f_i(x)$: The decision made by AI model i for input x.
- $f_{ideal}(x)$: The ideal decision-making process, which could be based on ethical guidelines or societal norms.

A low value of F indicates that the AI decision-making process is close to the ideal fairness criteria, and conversely, a high value suggests bias or deviation from fairness. AI models must be continually adjusted to minimize F, ensuring the system operates fairly.

7. Tokenomics

Karl Marx mentioned in Capital that Money will inevitably be lost in the process of circulation, and "the wearing down of the money demands its constant replacement" [6].
As the world's first encrypted digital crypto currency, a lot of Bitcoins have lost already due to lost private keys, damaged digital carriers and other reasons.
So, the tokenomics of AIOS ensure a sustainable, deflationary model similar to Bitcoin's, but with additional adjustments based on **dormant BTC addresses** to dynamically control token issuance. This combination of factors-clearing and settlement every **10** minutes, halving every **4** years, and minting/burning based on dormant BTC amounts-ensures that the token supply remains flexible, decentralized, and aligned with the broader economic goals of AIOS. This design aims to stabilize the economy of the platform while rewarding early adopters and ensuring fair distribution.

7.1. Token Minting and Burning Mechanism

In the AIOS, tokens are minted based on the amount of dormant BTC addresses found across the blockchain, fostering a connection between the traditional and decentralized finance ecosystems. The tokenomics mechanism consists of the following steps:

1. $Identifying\ Dormant\ BTC\ Addresses$:
   By searching all BTC addresses that have been inactive for latest **5** years, get the total

amount of BTC in these dormant addresses is denoted as **DormantBTC**.

2. **Minting Tokens**:
   The minting process is based on the total dormant BTC found:

$$\boldsymbol{mintAIOS = DormantBTC \times 1000} \tag{10}$$

   This means that for every **1** BTC found in dormant addresses, **1000** AIOS tokens will be minted.

3. **Yearly Updates**:
   Every **12** months, the process is repeated. If SumDormantBTC has increased, additional tokens are minted. If it has decreased, tokens are burned to maintain balance. The formula for token supply is adjusted to always reflect the formula is as shown in step **2**.

7.2. Token Generation Rules

The AIOS token follows a similar model to Bitcoin in terms of its issuance and distribution. Specifically, the token generation rules are as follows:

- **Block Time**:
  A new block is added about every **0.5** seconds, and every **1200** blocks is an **Epoch**, which means settlement is approximately every **10** minutes, just like **Bitcoin**. This ensures a consistent and predictable rate of token issuance.

- **Halving Mechanism**:
  The total number of tokens minted per block is **halved** every **4** years, mirroring the Bitcoin halving model. This gradual reduction in the rate of token generation ensures scarcity over time and helps control inflation within the AIOS ecosystem.

- **Supply Adjustments**:
  Every **4** years, as the block reward halves, the AIOS token supply will decrease, maintaining scarcity and promoting long-term value appreciation. This halving model creates a deflationary system, incentivizing participants to hold their tokens for future value increases.

8. The Future

Integrating blockchain with AI to create the AIOS has the potential to fundamentally reshape how AI systems are deployed and governed, ensuring they are transparent, secure, fair, and inclusive. By combining AI's ability to automate decision-making with blockchain's transparency, security, and decentralization, the AIOS can provide a platform that upholds values of equality and freedom. Through the use of decentralized governance, smart contracts, Federated Learning, and Neural Networks, AIOS can address the ethical and societal challenges posed by AI technologies. The algorithms and formulations presented in this whitepaper offer a blueprint for building a future where AI-driven systems are accountable to the people they serve, ensuring that these systems promote fairness, security, and access to resources for all.

The rules and order of this world are gradually being lost. Hope the AIOS can bring us and our posterity the real **justice**, **tranquility**, **welfare**, and **liberty**. [7]

References

[1] Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4(2):15, 2008.

[2] E Knuth Donald et al. The art of computer programming. Sorting and searching, 3(426-458):4, 1999.

[3] Ian Goodfellow, Yoshua Bengio, Aaron Courville, and Yoshua Bengio. Deep learning, volume 1. MIT press Cambridge, 2016.

[4] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. white paper, 3(37):2–1, 2014.

[5] John Von Neumann. First draft of a report on the edvac. IEEE Annals of the History of Computing, 15(4):27–75, 1993.

[6] Karl Marx. Capital: Volume II, volume 2. Penguin UK, 2006.

[7] United States and Johnny H Killian. The Constitution of the United States of America. US Government Printing Office, 1994.