NEURAI

DRAFT

Last update | 24, November 2023

Connecting the real world with blockchain

02, October 2023

Abstract

Neurai is a platform for exploring the convergence and interoperability of hardware for microcontrollers with three technologies: blockchain for integrity and traceability of information, Internet of Things (IoT) for the generation of real-time data on a massive scale, and Artificial Intelligence (AI) for processing and analyzing this data for decision-making. We have developed a series of cryptographic tools to achieve autonomy in IoT devices, such as unique identifiers, messaging through the blockchain network, specific assets for providing traceability, a decentralized DNS, token mining for AI utilization, and the use of Proof of Work (PoW) as a guarantee for consensus.

1. Introduction

The technological revolution in recent years has led to a world where interconnectivity and digitization are at the center of all aspects of our lives, with billions of devices connected to the Internet. It's not just computers, servers, or mobile phones anymore; there are also vehicles, information panels, cameras, appliances, televisions, radios, drones, robots, etc. More and more devices are connected, aiding and improving all aspects of life, but this revolution has also brought about a high degree of service centralization in a few companies.

We propose a series of cryptographic tools based on Satoshi's concept with Bitcoin and expanded upon by the developers of Ravencoin. For PoW consensus, we adopt the KAWPOW algorithm due to its resistance to ASIC machines and to prevent specific mining farms. A set of specific assets are created to establish cryptographic signatures for the transfer or validation of information in IoT devices, and development boards are produced using microcontrollers to leverage the technology presented here.

2. Decentralization

The creation of a decentralized and censorship-resistant system presents a series of technical challenges that make it technically complex. Ensuring that all nodes have a coherent view of the global state is a non-trivial problem, and consensus algorithms like PoW (proof of work) solve this issue. As more nodes join the network, performance and efficiency do not scale linearly, but they do expand the network's protection by blocking any transaction attempts outside of consensus and allowing for better connectivity from any geographic area.

We use part of the Ravencoin codebase to establish a set of suitable tools for achieving this decentralization, which we can detail in the following points:

- Extended Bitcoin code with integrated assets in the main layer.
- ASIC-resistant and GPU-friendly PoW.
- Integrated assets in the code and main layer.
- Block time every 1 minute.
- Block size of 8 MB.

- Adjusted block reward to be more dynamic.
- Custom assets for unique identifier services and traceability.

Running a node is a straightforward process; it increases the network's decentralization and allows quick access for the operator, not depending on external machines or third-party services for necessary interactions with the Neurai network. Managing a node allows for privacy for the operator and also greater control over one's own management

3. IoT

An IoT device is a piece of equipment that works in a coordinated manner to collect data from the environment, process it, and communicate it to other devices or systems through a network, usually the Internet. These data are used for decision-making, such as gathering information from a greenhouse, counting traffic, collecting climate data, inventorying a warehouse, or monitoring household consumption. With the option of using artificial intelligence in decision-making based on the collected information, it is possible to improve the outcomes compared to those generated by monolithic algorithms.

IoT devices generally rely on centralized services, whether from large or small companies, which can easily be compromised. There is a constant increase in data theft or service alterations with significant implications for privacy and security due to this proliferation of connected devices.

We have developed a series of tools that ensure the secure transfer of information through cryptographic systems managed solely by the owner and with global connectivity determined only by the need for a connection to a service node. We also expand a messaging system to issue commands or update statuses through the Neurai network itself.

For this connectivity, IoT devices connected to the blockchain network will need an assigned unique identifier:

One or multiple identifiers are created by burning a certain amount of coins.

- These identifiers are then assigned to a cryptographic key.
- This identifier is sent to an address that will be used by the IoT device.
- The IoT device configures this identifier through a digital signature.
- Through this digital signature, unique communication is established between the owner and the IoT device.
- This communication can be bidirectional, with a limited number of bytes.
- An external connection can be configured while maintaining encrypted communication through the identifier itself.
- The owner will have full control over the identifier and can transfer it, move it, and delete it.
- Connectivity can be achieved through various protocols

DIAGRAM HERE

3.1 Simple connectivity

The IoT device establishes a connection to the network using the assigned unique identifier and exchanges information through the owner of the identifier. This will be carried out as follows.

DIAGRAM HERE

3.2 Mesh Connectivity

Interconnections between IoT devices are made through branch identifiers to ensure the exchange of information between them and the owner. The interconnection between the devices can be via the internet or connected through any of the existing connectivity protocols such as Zigbee, Bluetooth, LoRa, Matter, Thread, or any new ones that may emerge.

DIAGRAM HERE

3.3 Hub-Based Connectivity

The connectivity of IoT devices is facilitated through an intermediary that will be responsible for connecting to the blockchain network. It will serve as a storage, processing, and task assignment center for the devices, and will also allocate AI tasks for the generated data. A unique branch-specific identifier will be assigned to it to receive tasks specified by the creator.

Using one or multiple hubs allows for the expansion of managing multiple linked IoT devices for the same task, with the capability to connect up to 256 devices per hub, leveraging computational power and storage to handle complex tasks.

DIAGRAM HERE

---

4. Identifiers

IoT devices that will be connected to the network will do so either through a hub or directly via an internet connection. To govern these devices and achieve secure communication of information between these devices and the owner, encryption must be used.

DIAGRAM HERE

We propose two types of identifiers: unique or branch-based.

4.1 Unique Identifier

The identifier is a specific asset assigned to an IoT device, although it can be used with any type of device. This identifier will communicate exclusively with its creator through a digital signature between both parties. They can maintain communication through the blockchain network itself, but also externally if it is necessary to exchange a greater amount of information. This communication prevents external attacks or unwanted intruders, ensuring that the communication arrives intact at the destination by using the decentralized blockchain network

---

DIAGRAM HERE

4.2 Branch Identifier

The branch identifier allows for a type of identifier that has multiple levels according to the creator's own needs. Up to 8 levels can be created, and each level can be managed by hubs or with direct connectivity to the devices.

DIAGRAM HERE

---

5. Encrypted Internal Messages

With the connectivity of devices through unique identifiers, a layer of security is achieved between the devices themselves and their creator. For communication between both parties, the blockchain network itself will be used to send commands to the devices, thereby creating a decentralized information network within the existing network.

The creator of the identifiers will have the option to send information to the assigned identifiers, whether they are unique or branch-based. This process uses the node's mempool, and all nodes will receive the same data, but only the appropriate ones will be able to decrypt the sent information. This allows for secure and decentralized control of these devices, without relying on any external layer other than the blockchain network itself and avoiding any form of network blocking or censorship.

To prevent spamming via this method, the amount of information per message is limited and will have a cost that is sufficiently low for practical use but high enough to deter spam.

DIAGRAM HERE

Specific nodes for the messaging system can be created and rewarded for their own use on the network. This can be done by enabling a specific mempool for this feature, reducing the time for message expiration, and removing the message from the mempool once the recipient decrypts it.

DIAGRAM HERE

---

6. Traceability Through NFT Assets

Traceability is the ability to track and record the history, location, and trajectory of a product, component, or transaction throughout its entire supply chain or lifecycle. This is fundamental in various industries such as manufacturing, logistics, healthcare, and food, among others. It allows for the verification of the origin of elements, thereby ensuring quality, safety, and compliance with applicable regulations and standards.

This information is collected by the companies themselves and recorded in various types of databases, but with documentation for each point along the route to be recorded. This makes the data easily modifiable since the entire information gathering process depends on the company.

DIAGRAM HERE

We introduce a digital traceability system based on assets to ensure information about each of the hop

points, easily verifiable at any time. This could be either public or private, depending on the specific needs of the executor, and these special NFTs will interoperate with IoT devices, which will be responsible for managing traceability through the information input into them. This information will be processed and managed via the assigned identifier.

DIAGRAM HERE

The steps would be as follows:

- Gather the necessary information to add to the NFT for traceability.
- Generate a master NFT for the start and create sub-assets for each traceability to assign. For example, 'neurai-tracking.xxxxxxxx'
- The traceability NFT will reside in the 'xxxxxxxx' portion with a code for tracking, and it will be possible to hang it from the same root to keep all tracking NFTs organized.
- Generate a QR code associated with the NFT to assign to the product or service and facilitate data access.
- It will be possible to use the unique identifiers associated with an IoT device to automate the management of the traceability NFT.
- The traceability log can be either private or public.
- Review can be done from any point, requiring a full node for access.

7. NNS (Neurai Name System)

The DNS (Domain Name System) is a hierarchical system that translates human-readable domain names, such as 'neurai.org', into IP addresses that are used by servers to identify resources on the network. Each time a new domain is entered into a browser, a request is made to a server that contains a database of mappings to indicate to the user what the destination is.

DIAGRAM HERE

This server can be managed by anyone, but the information reaching it can be altered by authorities, blocking or changing the registered valid information. It can also be the target of coordinated attacks to modify or impersonate IPs and thus engage in illicit activities.

We will create a system called NNS (Neurai Name System), with the prefix XNA, which will be responsible for translating names into IP addresses or other types of information such as physical addresses. These domains can be modified, deleted, or transferred, much like an NFT. With this cryptographic system, it will be possible to trust the information stored in these domains and avoid censorship, theft, or external attacks

---

DIAGRAM HERE

The operation of the asset takes advantage of part of its own code and generates a special type of NFT. The underlying operational framework will be as follows:

- A specific asset called NNS will be created to generate domains like neurai.nns.
- It will have a maximum of 25 characters, which will be (a-z), (0-9), and the dash (-).
- The generated data will reside entirely on the main layer of the blockchain.
- The asset will be anchored to the private key of the creator of that name, and they will be able to modify it, move it, transfer it, or delete it as long as they have access to it.

- The domain configuration can contain information about IP addresses, emails, physical addresses, and other types of information. When this domain is generated, there will be a cost in the chain's native currency.
- The entire payment will be sent to one of the code's burn addresses and will not be usable.
- The domain can contain multiple subdomain levels, such as 'paris.france.europe.xna'.
- Electrum servers will be able to translate the information from these domains.

8. AI

8.1 Microcontrollers

8.2 HUB

8.3 External

8.4 AI Mining

9. Connectivity modes in Neurai

10. Tokenomics

11. Conclusion