CONFIDENTIAL

UNITED KINGDOM INTELLECTUAL PROPERTY OFFICE

PATENT APPLICATION

Applicant

The Bitcoin Corporation Ltd

Title of Invention

ClawMiner: A Hardware AI Agent Device with Multi-Chain Audit Inscription on a Blockchain

Field of the Invention

The present invention relates to a hardware computing device that integrates an artificial intelligence agent with multi-chain blockchain wallet capabilities and a unified audit inscription engine. More particularly, the invention concerns a portable hardware device that performs autonomous computational tasks whilst simultaneously recording an immutable, cryptographically signed audit trail across one or more blockchain networks, with a primary inscription layer on the Bitcoin SV (BSV) blockchain.

Background of the Invention

Problem Statement

Modern AI agent systems operate as opaque software processes. When an AI agent performs actions on behalf of a user — executing transactions, signing documents, managing digital assets, or interacting with external services — there is no standardised, tamper-proof mechanism by which those actions are recorded in an independently verifiable manner.

Existing solutions suffer from several deficiencies:

1. **Lack of Auditability** — Software-based AI agents typically log actions to local databases or centralised cloud services that can be altered, deleted, or become unavailable. There is no guarantee of immutability.

2. **Key Security** — AI agents that manage cryptographic keys on behalf of users typically store those keys in software wallets or cloud-based key management services, both of which are vulnerable to remote exploitation, insider threats, and single points of failure.

3. **Fragmented Multi-Chain Activity** — Users operating across multiple blockchain networks (e.g., Bitcoin SV, Ethereum, Solana) have no unified mechanism to create a single, coherent audit trail of all cross-chain activity. Each chain's records exist in isolation.

4. **Consensus Inefficiency** — Traditional Proof of Work (PoW) consensus mechanisms consume vast quantities of energy performing computations that serve no purpose beyond securing the network. There is no mechanism to redirect that computational effort toward useful indexing, cataloguing, or data-processing work.

5. **IP and Data Provenance** — When an AI agent generates intellectual property (text, images, code, datasets), there is no built-in mechanism to timestamp, sign, and register that output in a manner that establishes provenance and ownership at the moment of creation.

Prior Art Limitations

Hardware wallets (e.g., Ledger, Trezor) provide secure key storage but lack any AI capability and do not perform autonomous actions. Software AI agents (e.g., LangChain-based agents, AutoGPT) can perform complex tasks but lack secure hardware key storage and do not natively produce blockchain audit records. Mining hardware (ASICs, GPUs) performs consensus work but serves no broader computational or AI function.

No existing device combines secure hardware key storage, an autonomous AI agent, multi-chain wallet management, and a unified blockchain audit inscription engine in a single portable unit.

Summary of the Invention

The present invention provides a hardware device ("ClawMiner") comprising:

a. A secure key storage module for holding one or more private cryptographic keys in tamper-resistant hardware;

b. An AI agent module capable of autonomous decision-making and task execution;

c. A multi-chain wallet module supporting transaction signing and submission across a plurality of blockchain networks;

d. An inscription engine that records a unified audit trail of all AI agent actions, transactions, and generated outputs as immutable inscriptions on a primary blockchain (BSV), with optional cross-references to secondary chains;

e. A Proof of Indexing (PoI) consensus mechanism whereby the computational work performed by the AI agent in indexing, cataloguing, and processing data is itself used as the basis for token minting, replacing wasteful proof-of-work hashing with productive computational labour.

The device operates as an autonomous hardware AI agent that can be deployed to perform tasks — data indexing, content generation, transaction management, monitoring — whilst every action is cryptographically signed by the device's secure hardware keys and permanently inscribed on the blockchain.

Detailed Description of the Invention

1. System Architecture

The ClawMiner device comprises the following principal components:

1.1 Secure Element / Key Storage Module

A tamper-resistant hardware secure element stores one or more private keys. The secure element is designed such that private keys cannot be extracted from the device; all signing operations occur within the secure element itself. The secure element supports key derivation for multiple blockchain networks from a single master seed, enabling the device to hold keys for BSV, Ethereum, Solana, and other supported chains simultaneously.

The secure element is physically bonded to the device's main processor board to prevent removal or substitution. Tamper-detection circuits cause key erasure if physical intrusion is detected.

1.2 AI Agent Module

The AI agent module comprises a processor (ARM-based or RISC-V) running a lightweight inference engine capable of executing AI models locally. The AI agent is configured to:

- Accept task instructions from the device owner via a local interface (USB, Bluetooth, Wi-Fi) or via authenticated remote commands;
- Execute tasks autonomously, including but not limited to: data retrieval, content generation, file processing, API interaction, transaction construction, and blockchain monitoring;
- Generate structured action logs for every operation performed;
- Submit action logs to the inscription engine for on-chain recording.

The AI agent operates within a sandboxed execution environment to prevent unauthorised modification of its behavioural parameters. Model updates are signed by the device manufacturer and verified by the secure element before installation.

1.3 Multi-Chain Wallet Module

The multi-chain wallet module manages addresses, balances, and transaction construction for a plurality of blockchain networks. The module comprises:

- A chain adapter layer providing a unified interface for constructing, signing, and broadcasting transactions across supported blockchains;
- A UTXO manager for UTXO-based chains (BSV, BTC, BCH) and a nonce manager for account-based chains (Ethereum, Solana);
- A fee estimation engine that determines appropriate transaction fees for each target chain;
- A transaction queue that batches and prioritises outgoing transactions.

All transaction signing is performed by the secure element. The wallet module constructs unsigned transactions and passes them to the secure element for signing; signed transactions are returned to the wallet module for broadcast.

1.4 Inscription Engine

The inscription engine is the core novel component. It receives structured action logs from the AI agent module, transaction records from the wallet module, and any generated content (files, data, intellectual property), and inscribes them as immutable records on the BSV blockchain using the BSV-20 or BSV-21 token protocols.

The inscription engine operates as follows:

1. **Action Capture** — Every action performed by the AI agent generates a structured log entry comprising: timestamp, action type, input parameters, output summary, cryptographic hash of any generated content, and a reference to any blockchain transactions executed as part of the action.

2. **Merkle Aggregation** — Action log entries are aggregated into a Merkle tree at configurable intervals (e.g., every N actions, every T seconds, or every block). The Merkle root is the primary datum inscribed on-chain, with full log data available off-chain via content-addressable storage.

3. **On-Chain Inscription** — The Merkle root, together with metadata (device ID, epoch number, chain references), is inscribed as a BSV transaction output using the OP_RETURN or OP_PUSH_DATA protocol. This creates an immutable, timestamped record on the BSV blockchain.

4. **Cross-Chain References** — When the AI agent or wallet module executes transactions on secondary chains (Ethereum, Solana, etc.), the transaction hashes from those chains are included in the BSV inscription, creating a unified audit trail that links activity across all chains back to a single BSV record.

5. **Recursive Inscription** — Inscriptions may reference prior inscriptions, forming a chain of audit records (an “audit chain”) that can be traversed to reconstruct the complete operational history of the device.

1.5 Proof of Indexing (PoI) Consensus Mechanism

The Proof of Indexing mechanism replaces traditional Proof of Work with productive computational labour. Rather than performing arbitrary hash computations to mine tokens, the ClawMiner device earns tokens by performing verifiable indexing work:

1. **Task Assignment** — The PoI protocol assigns indexing tasks to participating devices. Tasks include: indexing blockchain transaction data, cataloguing content inscriptions, building search indices for on-chain data, verifying the integrity of existing inscriptions, and processing structured datasets.

2. **Work Verification** — Upon completion of an indexing task, the device submits a proof comprising: the task identifier, the resulting index data (or a hash thereof), and a cryptographic signature from the device’s secure element. Verifier nodes check the submitted proof against independently computed results.

3. **Token Minting** — Upon successful verification, tokens (e.g., $402 HTM tokens under the BSV-21 protocol) are minted and assigned to the device’s wallet address. The minting rate is proportional to the quantity and complexity of verified indexing work performed.

4. **Difficulty Adjustment** — The PoI protocol adjusts task difficulty and token reward rates to maintain a target token emission schedule, analogous to Bitcoin’s difficulty adjustment but applied to indexing work rather than hash computation.

1.6 Recursive Tokenisation

The ClawMiner device supports recursive tokenisation, whereby:

- The device’s operational output (indexed data, generated content, audit records) can itself be tokenised as BSV-20 or BSV-21 tokens;
- Tokens representing the device’s output can reference the audit inscriptions that prove the output’s provenance;
- Token holders can verify the entire chain of provenance from token back to the original AI agent action that generated the underlying asset.

This creates a closed loop: the device performs work, inscribes proof of that work, mints tokens representing that work, and the tokens carry embedded references back to the proof — all anchored to the BSV blockchain.

2. Operational Flow

A typical operational cycle proceeds as follows:

1. The device owner configures a task (e.g., "index all BSV transactions from block 800,000 to 800,100 and catalogue all OP_RETURN data").
2. The AI agent module retrieves the specified blockchain data.
3. The AI agent processes and indexes the data, generating structured index entries.
4. The inscription engine captures the action log and the resulting index data.
5. The inscription engine constructs a Merkle tree of the action logs and index data.
6. The Merkle root is inscribed on the BSV blockchain as an immutable audit record.
7. The PoI module submits the completed indexing work as a proof to the verification network.
8. Upon verification, tokens are minted to the device's BSV wallet address.
9. The minted tokens carry a recursive reference to the audit inscription, establishing provenance.

3. Device Form Factor

The ClawMiner is designed as a compact, portable unit approximately the size of a standard external hard drive. It comprises:

- An ARM or RISC-V system-on-chip (SoC) with integrated neural processing unit (NPU);
- A hardware secure element (e.g., ATECC608 or equivalent);
- Persistent storage (eMMC or NVMe SSD) for model weights, index data, and transaction queues;
- Connectivity: Wi-Fi, Bluetooth, USB-C, and optional Ethernet via adapter;
- An LED status display or small OLED screen for operational status;
- A physical confirmation button for high-value transaction authorisation.

Brief Description of Drawings

The following drawings would accompany this application:

- **Figure 1** — System block diagram showing the principal hardware modules (secure element, AI agent processor, wallet module, inscription engine) and their interconnections.
- **Figure 2** — Data flow diagram illustrating the path from AI agent action through Merkle aggregation to on-chain inscription.
- **Figure 3** — Proof of Indexing consensus flow, showing task assignment, work execution, proof submission, verification, and token minting.
- **Figure 4** — Recursive tokenisation diagram showing the relationship between audit inscriptions, minted tokens, and provenance references.
- **Figure 5** — Cross-chain audit trail diagram showing how activity on multiple blockchains is unified into a single BSV inscription record.
- **Figure 6** — Physical device layout and form factor.

Initial Claims

Note: These claims are provided in sketch form for the purposes of establishing a priority date. Formal claims will be drafted and filed within 12 months in accordance with UKIPO rules.

Claim 1 — Hardware AI Agent Device

A hardware computing device comprising: (a) a tamper-resistant secure element for storing one or more private cryptographic keys and performing signing operations; (b) a processor running an artificial intelligence agent capable of autonomous task execution; (c) a multi-chain wallet module for constructing, signing, and broadcasting transactions across a plurality of blockchain networks; (d) an inscription engine configured to record a unified audit trail of all actions performed by the AI agent as immutable inscriptions on a blockchain; wherein all signing operations are performed within the secure element and the inscription engine produces a cryptographically linked chain of audit records.

Claim 2 — Unified Audit Trail Method

A method of creating a unified audit trail for an autonomous AI agent operating across a plurality of blockchain networks, the method comprising: (a) capturing structured action logs for every operation performed by the AI agent; (b) aggregating the action logs into a Merkle tree; (c) inscribing the Merkle root as an immutable record on a primary blockchain; (d) including, within the inscription, transaction hashes from any secondary blockchain transactions executed by the AI agent; (e) linking successive inscriptions to form a traversable audit chain.

Claim 3 — Proof of Indexing Consensus

A consensus mechanism for a blockchain network comprising: (a) assigning data indexing tasks to participating computing devices; (b) receiving, from each device, a proof of completed indexing work comprising the task identifier, a hash of the resulting index data, and a cryptographic signature from the device's secure element; (c) verifying the submitted proof against independently computed results; (d) minting blockchain tokens to the device's wallet address upon successful verification; wherein the computational work required to earn tokens consists of productive data indexing rather than arbitrary hash computation.

Claim 4 — Recursive Tokenisation

A method of tokenising the output of an AI agent on a blockchain, comprising: (a) recording, as a blockchain inscription, proof of the AI agent's actions that generated the output; (b) minting a blockchain token representing the output; (c) embedding within the token a reference to the blockchain inscription of step (a); such that the provenance of the tokenised output can be verified by traversing the reference from the token to the inscription and thence to the underlying AI agent action logs.

Abstract

A hardware device integrating a secure key storage element, an autonomous AI agent, a multi-chain blockchain wallet, and an inscription engine that records a unified, immutable audit trail of all AI agent actions on the Bitcoin SV blockchain. The device employs a Proof of Indexing consensus mechanism wherein productive data-indexing work performed by the AI agent replaces wasteful hash computation as the basis for token minting. Cross-chain transaction references are consolidated into single BSV inscriptions, creating a unified audit trail spanning multiple blockchain networks. The device further supports recursive tokenisation, whereby generated outputs are tokenised with embedded provenance references linking back to the on-chain audit records.

Document prepared for UKIPO filing. Priority date to be established upon submission. Applicant: The Bitcoin Corporation Ltd Date of preparation: 24 February 2026