



HARVEST THE SUN WITH \$SIMCAT

# \$SIMCAT MINING WHITE PAPER

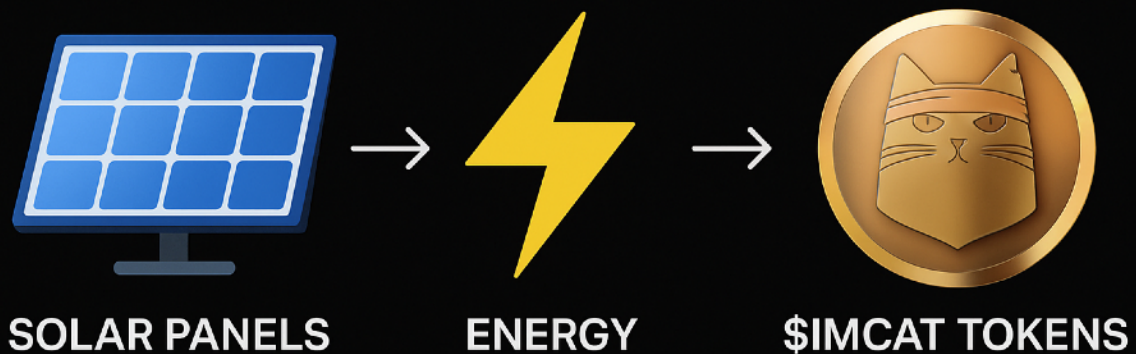
Author: Beghzod Gapparov  
Co-author: Jack Samatov

Date: Monday, November 17, 2025  
Version: 9.0 (first public version)

## SIMCAT Solar Mining

In cryptocurrency, the process of validating and adding new blocks of transactions to a blockchain is called "mining." Traditionally, mining relies on either the Proof-of-Work (PoW) or Proof-of-Stake (PoS) consensus mechanisms but SIMCAT Mining redefines the concept. While it uses the familiar term "mining," it does not involve the high energy consumption or computational race of traditional PoW systems. Instead, SIMCAT Mining literally turns sunlight into crypto-harnessing solar energy through specialized SIMCAT Solar Panels to generate \$SIMCAT tokens. This eco-friendly process transforms excess clean energy into digital rewards, making mining sustainable, accessible, and truly green.

### ☀️ SIMCAT Solar Mining – Turning Sunlight into Crypto



#### 1 Green Energy Meets Blockchain Rewards

SIMCAT Solar Mining is a next-generation, eco-friendly mining solution that turns household solar energy production into \$SIMCAT token rewards. Designed for small to medium households with solar panels, this initiative merges renewable energy generation with blockchain technology to create a new form of sustainable mining.



## 2 How It Works

It all starts with SIMCAT Solar Panels – Our proprietary solar panels generate clean electricity for household use.

- **Excess Energy Monetization:** Any surplus electricity is automatically sold back to the local power grid, earning the household credits or payments from the utility provider.
- **Integrated \$SIMCAT Mining Hardware** – Each SIMCAT Solar system includes a compact, low-energy mining device connected to the Crypto Engine Mining Pool. Unlike traditional PoW rigs, it operates like a network modem, energy-efficient and maintenance-free.
- **Blockchain-Linked Rewards** – Every time the household generates a set amount of value from selling energy (e.g., \$10 worth), a percentage (e.g., \$2 worth) is also issued in \$SIMCAT tokens directly into the user's wallet.
- **Smart Grid Integration** – The system uses custom blockchain algorithms to verify and record energy output, linking token rewards to the real-world performance of the solar installation.

## 3 Proof-of-Stake Alignment

While not traditional PoS, SIMCAT Solar Mining shares its principles—staking \$SIMCAT tokens can increase earning potential, with rewards tied to solar panel performance over time. This creates a “stake in the sun,” linking blockchain earnings to renewable energy output.

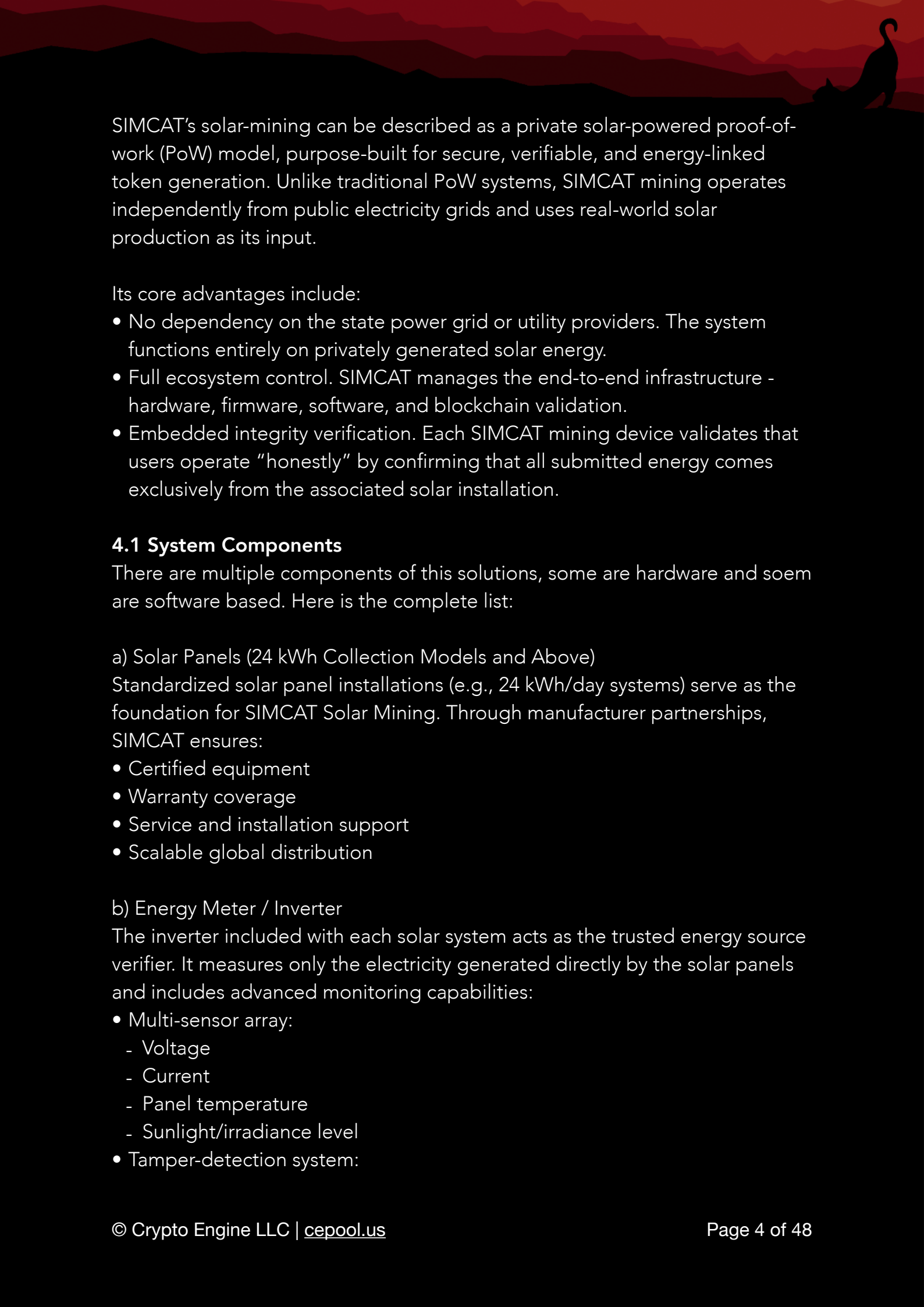
### Benefits

- **Double Earnings** – Earn utility credits and \$SIMCAT tokens from the same solar energy production.
- **Eco-Friendly** – 100% powered by renewable energy, no high-power PoW hardware needed.
- **Seamless Integration** – Fully automated mining process via Crypto Engine Mining Pool.
- **Accessible** – Designed for households, easy to learn and get started.

### Target Audience

- Homeowners with solar panels generating excess energy
- Eco-conscious crypto enthusiasts
- Renewable energy advocates seeking additional revenue streams

## 4 Technical Description



SIMCAT's solar-mining can be described as a private solar-powered proof-of-work (PoW) model, purpose-built for secure, verifiable, and energy-linked token generation. Unlike traditional PoW systems, SIMCAT mining operates independently from public electricity grids and uses real-world solar production as its input.

Its core advantages include:

- No dependency on the state power grid or utility providers. The system functions entirely on privately generated solar energy.
- Full ecosystem control. SIMCAT manages the end-to-end infrastructure - hardware, firmware, software, and blockchain validation.
- Embedded integrity verification. Each SIMCAT mining device validates that users operate "honestly" by confirming that all submitted energy comes exclusively from the associated solar installation.

#### **4.1 System Components**

There are multiple components of this solutions, some are hardware and soem are software based. Here is the complete list:

##### **a) Solar Panels (24 kWh Collection Models and Above)**

Standardized solar panel installations (e.g., 24 kWh/day systems) serve as the foundation for SIMCAT Solar Mining. Through manufacturer partnerships, SIMCAT ensures:

- Certified equipment
- Warranty coverage
- Service and installation support
- Scalable global distribution

##### **b) Energy Meter / Inverter**

The inverter included with each solar system acts as the trusted energy source verifier. It measures only the electricity generated directly by the solar panels and includes advanced monitoring capabilities:

- Multi-sensor array:
  - Voltage
  - Current
  - Panel temperature
  - Sunlight/irradiance level
- Tamper-detection system:

- Automatically identifies abnormal energy signatures or attempts to feed power from non-solar sources (e.g., grid, generator).

This ensures that all reported energy originates from genuine solar production.

#### c) SIMCAT Mining Device + Modem

A compact, firmware-controlled module that binds real-world solar output to blockchain mining. Key functionalities include:

- Energy-bound operations: Mining power is capped by the predefined energy limit (e.g., a 24 kWh system corresponds to a specific hashpower/time allocation).
- Real-time validation: Continuously cross-checks sensor data from the inverter to ensure authenticity and consistency.
- Automatic shutdown: If the device detects fake power input, abnormal profiles, or tampering attempts, mining halts immediately.

#### d) SIMCAT Blockchain Network (Closed or Semi-Closed)

The mining system connects to a permissioned blockchain environment:

- Operated by SIMCAT or by authorized validator nodes
- Only energy-proof submissions generated by SIMCAT-certified mining devices are accepted
- Ensures secure, tamper-resistant, and auditable on-chain energy validation

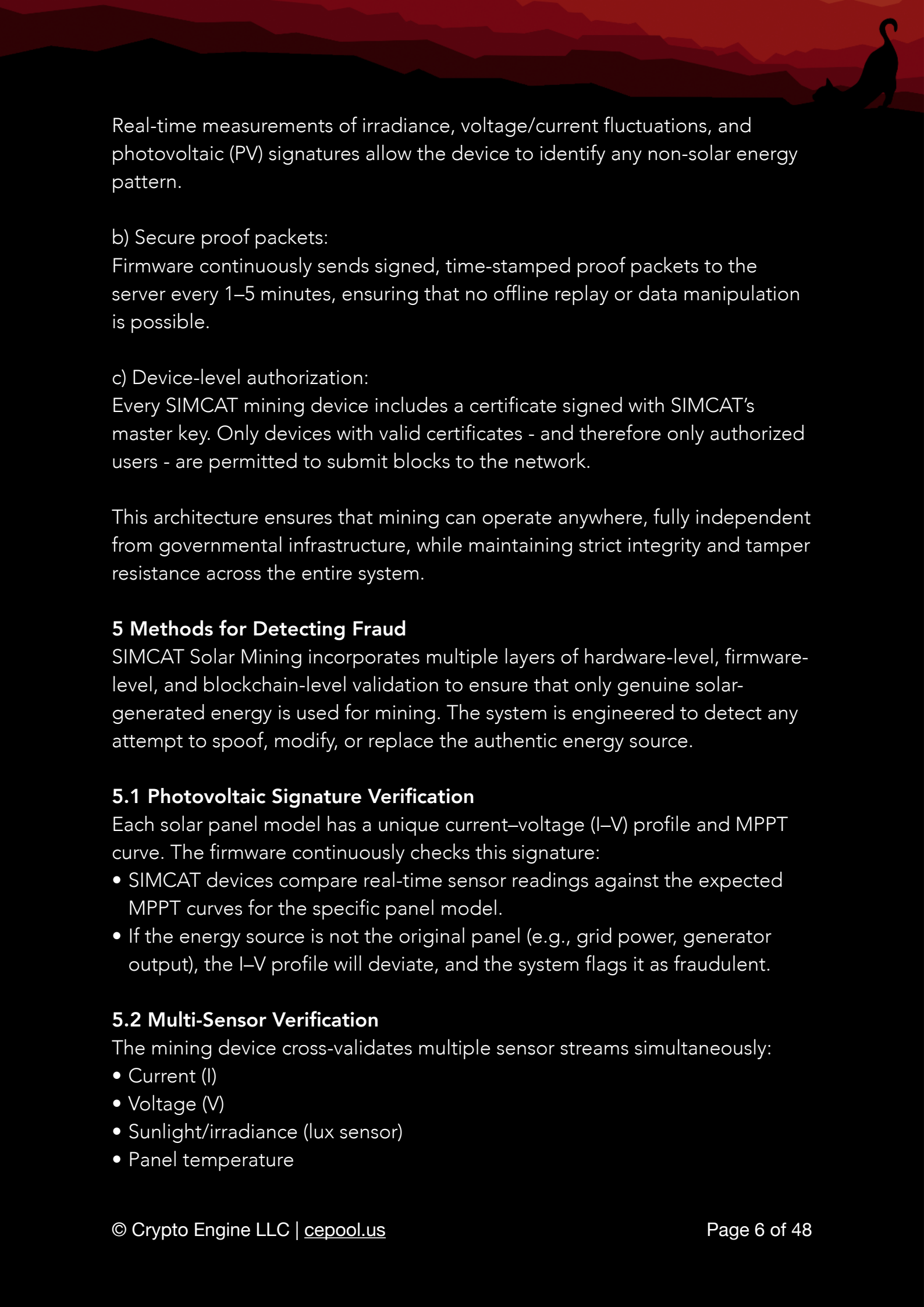
## 4.2 Mechanism of "State-Independent" Operation

The SIMCAT Solar Mining system is designed to operate fully independent of state electricity grids. Since the system relies solely on energy produced by the user's own solar panels. Because it does not connect to the state electricity grid, all mining operations rely exclusively on the solar panel + SIMCAT mining rig combination sold and certified by SIMCAT. This ensures full autonomy, predictable security, and complete control over the energy-to-blockchain pipeline.

Users may attempt to supply power from alternative sources - such as the grid or a generator - but such manipulation is automatically detected and rejected. The system employs multiple layers of validation:

#### a) Sensor-based verification:





Real-time measurements of irradiance, voltage/current fluctuations, and photovoltaic (PV) signatures allow the device to identify any non-solar energy pattern.

b) Secure proof packets:

Firmware continuously sends signed, time-stamped proof packets to the server every 1–5 minutes, ensuring that no offline replay or data manipulation is possible.

c) Device-level authorization:

Every SIMCAT mining device includes a certificate signed with SIMCAT's master key. Only devices with valid certificates - and therefore only authorized users - are permitted to submit blocks to the network.

This architecture ensures that mining can operate anywhere, fully independent from governmental infrastructure, while maintaining strict integrity and tamper resistance across the entire system.

## **5 Methods for Detecting Fraud**

SIMCAT Solar Mining incorporates multiple layers of hardware-level, firmware-level, and blockchain-level validation to ensure that only genuine solar-generated energy is used for mining. The system is engineered to detect any attempt to spoof, modify, or replace the authentic energy source.

### **5.1 Photovoltaic Signature Verification**


Each solar panel model has a unique current–voltage (I–V) profile and MPPT curve. The firmware continuously checks this signature:

- SIMCAT devices compare real-time sensor readings against the expected MPPT curves for the specific panel model.
- If the energy source is not the original panel (e.g., grid power, generator output), the I–V profile will deviate, and the system flags it as fraudulent.

### **5.2 Multi-Sensor Verification**

The mining device cross-validates multiple sensor streams simultaneously:

- Current (I)
- Voltage (V)
- Sunlight/irradiance (lux sensor)
- Panel temperature



Alternative power sources cannot replicate the natural relationship between these metrics. Any mismatch immediately indicates a non-solar or manipulated energy input.

### **5.3 On-Chain Energy-Proof Validation**

For every block mined, the device generates an energy-proof hash, which is derived from:

- The previous N seconds of raw sensor logs
- Timestamped and locally hashed data
- A secure signature from the device's internal key

This energy-proof is then attached to the block header and verified on-chain, ensuring that no block can be validated without authentic solar-derived data.

### **5.4 Tamper-Evident Hardware Controls**

SIMCAT devices include physical integrity safeguards:

- Opening the enclosure
- Disconnecting or altering sensor cables
- Removing or bypassing the inverter

Any such event triggers an automatic shutdown of the mining process. The device enters a locked state and reports the incident to the backend.

## **6 Advantages**

There are many advantages of this new mining method, here are some:

a) Operates without state-grid integration

The system functions independently of national utility infrastructure, significantly reducing regulatory exposure and compliance risks.

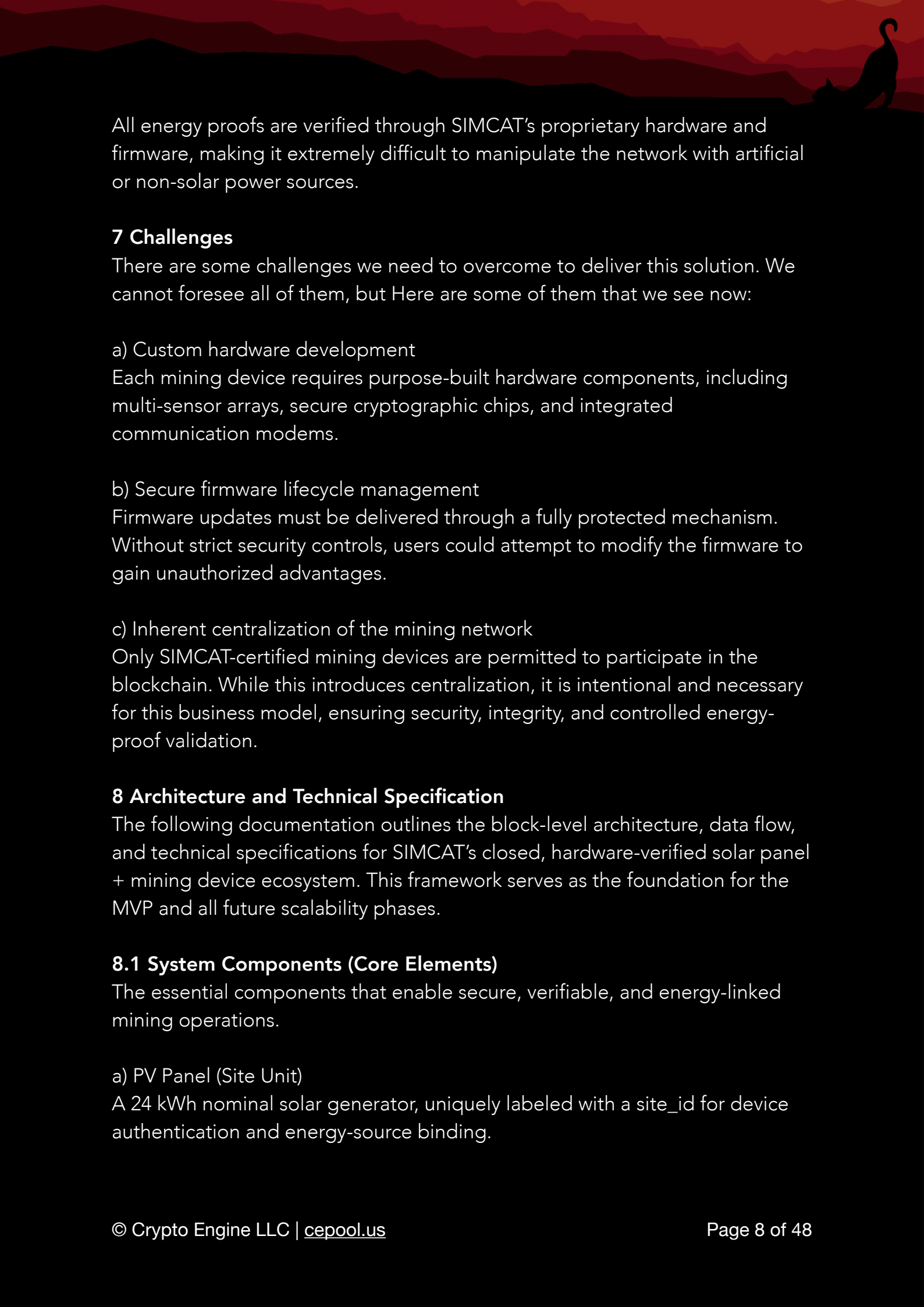
b) Sustainable revenue model

SIMCAT's primary business model is based on the sale of solar panels and mining devices, while the token economy provides an additional incentive layer for users and long-term ecosystem growth.

c) Universal deployability

The system is capable of operating in any region - including remote, off-grid environments - as long as solar energy is available.

d) Strong integrity and anti-fraud controls



All energy proofs are verified through SIMCAT's proprietary hardware and firmware, making it extremely difficult to manipulate the network with artificial or non-solar power sources.

## 7 Challenges

There are some challenges we need to overcome to deliver this solution. We cannot foresee all of them, but Here are some of them that we see now:

### a) Custom hardware development

Each mining device requires purpose-built hardware components, including multi-sensor arrays, secure cryptographic chips, and integrated communication modems.

### b) Secure firmware lifecycle management

Firmware updates must be delivered through a fully protected mechanism. Without strict security controls, users could attempt to modify the firmware to gain unauthorized advantages.

### c) Inherent centralization of the mining network

Only SIMCAT-certified mining devices are permitted to participate in the blockchain. While this introduces centralization, it is intentional and necessary for this business model, ensuring security, integrity, and controlled energy-proof validation.

## 8 Architecture and Technical Specification

The following documentation outlines the block-level architecture, data flow, and technical specifications for SIMCAT's closed, hardware-verified solar panel + mining device ecosystem. This framework serves as the foundation for the MVP and all future scalability phases.

### 8.1 System Components (Core Elements)

The essential components that enable secure, verifiable, and energy-linked mining operations.

#### a) PV Panel (Site Unit)

A 24 kWh nominal solar generator, uniquely labeled with a `site_id` for device authentication and energy-source binding.





#### b) PV Sensor Array

A multi-sensor module capturing real-time physical characteristics of solar production:

- Voltage (V)
- Current (A)
- Irradiance (lux / pyranometer)
- Temperature

#### c) Smart Meter / Gateway

A tamper-evident gateway equipped with:

- Secure Element (HSM/SE) for signing energy proofs
- Local sensor log storage
- Real-time PV verification

#### d) Mining Device (Modem + ASIC/RISC Unit)

A firmware-controlled machine responsible for:

- Energy-bound Proof-of-Work logic
- Secure device private key storage
- Connectivity via SIM / Wi-Fi / LoRa
- Hash computations linked to solar energy output

#### e) Control Backend (Operator)

A centralized management and verification layer:

- Secure firmware updates
- Key lifecycle management
- Proof-packet validation
- Device health and telemetry monitoring

#### f) Permissioned Blockchain Network

A closed or semi-closed chain where validator nodes are operated by SIMCAT or trusted partners. Only authenticated energy-proof submissions from SIMCAT-certified mining devices are accepted.

```
flowchart TB
    A[PV Panel (site_id)] --> B[PV Sensor Array]
    B --> C[Smart Meter / Gateway (HSM)]
    C --> D[Mining Device (firmware)]
    D --> E[Operator Backend (proof ingestion)]
    E --> F[Permissioned Blockchain Validators]
    F --> G[Reward / Token Minting]
```

## 9 High-Level Architecture (Mermaid Diagram)

This section contains a high-level system diagram written in Mermaid syntax.

### Sequence Flow - Block Creation Process

The sequence diagram illustrates how solar energy data is captured.

```
sequenceDiagram
    participant Panel as PV Panel
    participant Meter as Smart Meter
    participant Miner as Mining Device
    participant Backend as Operator Backend
    participant Chain as Permissioned Validators

    Panel->>Meter: sensor readings (V, I, irradiance, temperature)
    Meter->>Meter: aggregate exported_kWh (time window)
    Meter->>Miner: signed_energy_proof = SIG_meter(site_id || ts || kWh || nonce)
    Miner->>Miner: verify proof + compute energy-bound PoW
    Miner->>Backend: submit(block_candidate, energy_proof, miner_sig)
    Backend->>Chain: verify(proof, miner_sig) → validate block
    Chain->>Backend: block_accepted
    Backend->>Miner: reward(token) / acknowledgement
```

### Block Header - Recommended Minimum Fields

To ensure verifiability, traceability, and compatibility with SIMCAT's energy-bound proof-of-work model, each block header should contain the following minimum set of fields:

- `parent_hash`
- `merkle_root`
- `timestamp`
- `miner_id` (pubkey)
- `energy_proof`
  - `proof_type` ("meter\_sig" | "TEE\_attest" | ...)
  - `proof_blob` (SIG\_meter(...))
  - `exported_kWh` (float)
  - `proof_timestamp`
- `difficulty` (compute difficulty, energy-ga bog'langan)
- `nonce`

### Energy-Proof Format (Example)

The SIMCAT mining system constructs a cryptographically verifiable energy-proof to validate that each block is derived from authentic solar-generated



power.

```
SIG_meter(site_id || ts || exported_kWh || window_hash ||  
nonce)
```

**site\_id** - unique identifier (manufacturer-signed)

**ts** - proof timestamp

**exported\_kWh** - the total kilowatt-hours generated during the proof window (e.g., a 1-hour interval)

**window\_hash** - hash of all raw sensor logs captured during the proof window, ensuring immutability and auditability.

**nonce** - randomness value used to guarantee uniqueness and prevent replay attacks.

The signature (**SIG\_meter**) is produced using the secure element inside the inverter or the mining device's private key, ensuring that the proof cannot be forged or altered.

### **Firmware Rules (Device-Side)**

The SIMCAT mining device operates under strict firmware-level rules to ensure verifiable, tamper-resistant, and energy-bound mining. All logic is enforced on-device and cryptographically anchored to the backend.

#### 1) Real-Time Sensor Stream

The device continuously logs physical solar-generation data at fixed intervals:

- Voltage (V)
- Current (I)
- Irradiance
- Temperature

These measurements form the foundation of energy-proof validation.

#### 2) Exported kWh Aggregation

For each block window (e.g., 10 minutes), the firmware computes the **exported\_kWh** value, representing the total solar energy produced in that interval.

#### 3) Signed Proof Blobs

Every proof blob is signed inside the device's Secure Element (HSM/SE) and includes the corresponding **window\_hash** of raw sensor logs. This prevents tampering or replay.



#### 4) Proof Verification Before Mining

At the start of each mining cycle:

- The signature is verified
- Sensor data consistency is checked

Only if the proof is valid does the device initiate compute operations for energy-bound PoW.

#### 5) Tamper Detection

Mining is immediately locked, and an alert is sent to the backend if any of the following occur:

- Device enclosure opened
- Sensor or cable disconnected
- Sudden anomalous sensor patterns detected

This ensures physical integrity and prevents bypass attempts.

#### 6) Secure Firmware Updates

Firmware updates can only be installed if signed by the operator's backend signing key. Unauthorized firmware is rejected automatically.

### **Fraud Detection (Pragmatic Rules)**

The device employs multiple heuristics and physical-signal analysis methods to detect artificial or non-solar energy sources:

#### 1) PV Curve Fingerprinting

Each panel model has a unique I-V and MPPT profile. Any deviation from the expected pattern indicates non-solar energy (e.g., grid or generator).

#### 2) Irradiance Correlation

The relationship between irradiance levels and I-V output is validated. Fake sources cannot replicate natural sunlight-energy correlations.

#### 3) Temporal Smoothing

The exported power profile must follow physically realistic changes over time. Sharp spikes or unnatural transitions trigger fraud detection.

#### 4) Cross-Checking with External Data (Optional)

If GPS and timestamps are available, sensor data may be compared with:

- Expected sunlight levels
- Local weather patterns
- Time-of-day solar curves

This adds an additional analytics layer for anomaly detection.

## **Security and Trust Model**

A Security and Trust Model defines the cryptographic, hardware, and operational mechanisms that ensure devices are authentic, data is genuine, and the system can reliably reject tampering or fraud.

### **1) Device Identity**

Each mining device is provisioned at manufacturing with:

- A unique private key
- A device certificate signed by SIMCAT

This binds each device cryptographically to the network.

### **2) Secure Boot & Signed Firmware**

Only signed firmware is permitted to run. Any attempt to modify system code or bypass secure boot is detected and blocked.

### **3) Backend Attestation**

The proof-ingestion backend provides validators with device roots of trust, ensuring that only authorized and attested devices participate in block validation.

### **4) Slashing Policy (Optional)**

If deposit/staking models are used, devices submitting fraudulent proofs may have their deposits slashed, providing economic penalties for dishonesty.

## **10 MVP Roadmap (7 Steps)**

A Minimum Viable Product (MVP) is the smallest functional version of the system that demonstrates core capabilities end-to-end, allowing real-world testing, validation, and iterative improvement with minimal development overhead. This section describes how we plan to get there with only 7 steps:

### **1) Protocol Draft & Minimum Technical Specification**

Expand this document into a full paper protocol including architecture, security model, and device-level requirements.



## 2) Hardware Prototype

Build the first prototype unit consisting of:

- PV panel
- Sensor array
- Smart gateway (Raspberry Pi / MCU + Secure Element)

## 3) Minimal Firmware Implementation

Develop the initial firmware supporting:

- Real-time sensor logging
- Meter-signed energy-proof generation
- Simplified energy-bound PoW logic

## 4) Permissioned Testnet Deployment

Launch a closed testnet consisting of 10 validator nodes (operator node + 9 test nodes) to validate block flow, proofs, and synchronization.

## 5) Pilot Deployment (10–50 Sites)

Install prototype systems across 10–50 locations (urban or rural) to study real-world performance, solar profiles, and sensor behavior patterns.

## 6) Security Audit

Conduct a formal audit covering:

- Hardware integrity
- Firmware logic
- Energy-proof protocol and cryptography

## 7) Scale-Up Phase

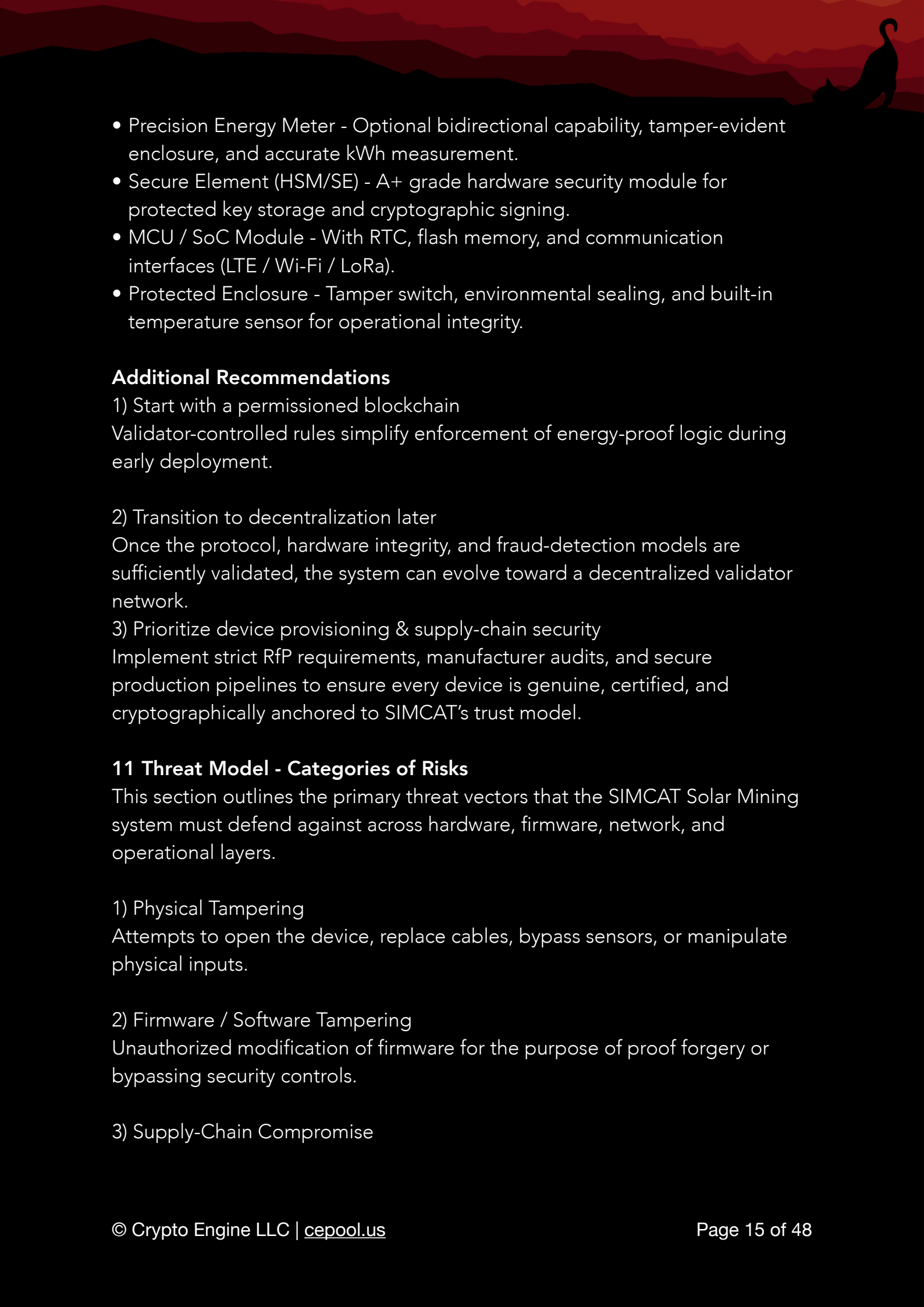
Move into mass production with:

- Manufacturing of certified mining devices
- Managed device-lifecycle platform
- Commercial deployment and sales marketplace

## Hardware Checklist (Minimum Requirements)

- PV Panel - 24 kWh nominal daily output (or an equivalent certified model).
- Irradiance Sensor - High-quality pyranometer or calibrated sunlight measurement sensor.



- 
- Precision Energy Meter - Optional bidirectional capability, tamper-evident enclosure, and accurate kWh measurement.
  - Secure Element (HSM/SE) - A+ grade hardware security module for protected key storage and cryptographic signing.
  - MCU / SoC Module - With RTC, flash memory, and communication interfaces (LTE / Wi-Fi / LoRa).
  - Protected Enclosure - Tamper switch, environmental sealing, and built-in temperature sensor for operational integrity.

### **Additional Recommendations**

1) Start with a permissioned blockchain

Validator-controlled rules simplify enforcement of energy-proof logic during early deployment.

2) Transition to decentralization later

Once the protocol, hardware integrity, and fraud-detection models are sufficiently validated, the system can evolve toward a decentralized validator network.

3) Prioritize device provisioning & supply-chain security

Implement strict RfP requirements, manufacturer audits, and secure production pipelines to ensure every device is genuine, certified, and cryptographically anchored to SIMCAT's trust model.

## **11 Threat Model - Categories of Risks**

This section outlines the primary threat vectors that the SIMCAT Solar Mining system must defend against across hardware, firmware, network, and operational layers.


1) Physical Tampering

Attempts to open the device, replace cables, bypass sensors, or manipulate physical inputs.

2) Firmware / Software Tampering

Unauthorized modification of firmware for the purpose of proof forgery or bypassing security controls.

3) Supply-Chain Compromise



Risks within the manufacturing or logistics pipeline where keys, components, or firmware could be compromised.

#### 4) Replay / Relay / Injection Attacks

Reusing previously captured proofs, relaying manipulated data, or injecting external signals to mimic real outputs.

#### 5) Insider Threats

Abuse of privileged access by operators, manufacturers, installers, or maintenance personnel.

#### 6) Network Attacks

MITM, packet spoofing, injection, modification, or traffic manipulation during device-backend communication.

#### 7) Large-Scale Collusion

Multiple site owners - or a single large operator - cooperating to manipulate the reward system or inject fake energy proofs.

### 11.1 Practical Mitigations for Each Threat Category

Below are the operational, hardware, and cryptographic controls that counter each risk.

#### a) Physical Tampering

- Tamper-evident housings & tamper switches
  - Opening the enclosure immediately locks or bricks the device and notifies the backend.
- Sealed screws, epoxy, tamper tape
  - Makes unauthorized modification significantly more difficult.
- Cross-sensor validation
  - Voltage, current, irradiance, and temperature must align; discrepancies halt mining.
- GPS & time synchronization checks
  - Detect relocation or tampered timestamps.

Outcome:

Most physical tampering attempts are detected early; mining is blocked to prevent fraudulent activity.



#### b) Firmware / Software Tampering

- Secure Boot + Signed Firmware (Operator Certificate)
  - Only SIMCAT-signed firmware can be executed.
- Secure Element (HSM/SE) Key Protection
  - Device private keys never leave the secure module.
- Remote Attestation (TEE-enabled devices)
  - Device proves its integrity cryptographically to the network.
- Signed OTA updates with rollback/whitelist controls
  - Prevent unauthorized firmware downgrades or code injection.

Outcome:

Any firmware manipulation renders the device non-functional or is immediately detected by the backend.

#### c) Supply-Chain Security

- Device provisioning at factory
  - Each unit is issued a unique root-of-trust and ownership certificate during manufacturing.
- Vendor audits & contractual security requirements
  - Ensures compliant production and handling processes.
- Hardware attestation
  - Validates chip identity and manufacturer authenticity.

Outcome:

Risks of compromised keys or components in the supply chain are significantly reduced.

#### d) Replay / Relay Attacks

- Mandatory nonce & timestamp in each proof
  - Backend enforces single-use semantics via a used-proof registry.
- `window_hash` of `raw` sensor logs
  - Prevents copying or relaying prior sensor outputs.
- Challenge-response mechanisms (optional)
  - Validators send challenges that must be signed inside the device's TEE/HSM.

Outcome:

Captured or relayed proofs cannot be reused; replay attacks become ineffective.

#### e) Insider Threats & Collusion

- Multi-party attestation
  - Sensitive backend or validator functions are distributed across independent parties.
- Slashing / deposit-based penalties
  - Fraudulent devices or operators can lose deposits or rewards.
- Full audit logs & forensic tracing
  - All actions are recorded and can be investigated.

Outcome:

Insider manipulation becomes economically risky, legally traceable, and technically constrained.

#### f) Network Attacks

- **TLS** and **mTLS**
  - All communications use authenticated mutual TLS connections.
- Packet-level signing
  - Every proof is cryptographically signed; certificates are verified end-to-end.
- Rate limiting & anomaly detection
  - Network anomalies or suspicious activity are automatically blocked.

Outcome:

MITM, spoofing, and packet tampering become highly impractical.

## 11.2 Residual Risks and Limitations - What Remains Possible

Despite strong security controls, several classes of risk cannot be eliminated entirely:

### 1) High-Level Supply Chain Compromise


If a nation-state or state-supported actor compromises a manufacturer or component vendor, the device's root-of-trust may be exposed.

### 2) Laboratory-Grade Physical Attacks

A sufficiently resourced attacker could steal a device and perform chip-level or hardware-level modification in a laboratory. Such cases require forensics, device revocation, and law-enforcement escalation.

### 3) Large-Scale Collusion by Solar Farms

If a single operator acquires a disproportionately large number of panels and devices, they may influence reward distribution or centralize mining. This must



be mitigated through tokenomics caps, stake-weight rules, and fairness policies.

#### 4) Zero-Day Vulnerabilities

Complex firmware, TEE, or TLS stacks may contain undiscovered vulnerabilities. Continuous security testing, patching, and monitoring is mandatory.

### **11.3 Operational Measures - Security Is Not Only Technical**

A secure ecosystem requires hardened processes in addition to hardened devices:

#### 1) Secure Development Lifecycle (SDLC)

Code reviews, threat analysis, and secure design for both hardware and firmware.

#### 2) Periodic Pen-Testing and Red-Team Assessments

Independent penetration tests and adversarial simulations.

#### 3) Bug-Bounty Program

Incentivizing external researchers to responsibly disclose vulnerabilities.

#### 4) Incident Response Plan

Clear procedures for device compromise, certificate revocation, and rollback.

#### 5) Centralized Monitoring & SIEM

All proofs, alerts, tamper logs, and telemetry streamed into a unified security monitoring platform.

#### 6) Insurance & Legal Preparedness

For large pilots, coverage and legal frameworks are recommended.

### **11.4 Practical Security Checklist**

If these are implemented, security will be even stronger.

- Device stores its root key in an SE/HSM
- Secure boot and signed firmware
- Tamper-evident enclosure with tamper switch
- Multi-sensor validation (V, I, irradiance, temperature)



- Proof includes window\_hash + nonce + timestamp, cryptographically signed
- Backend used-proof registry (prevents replay)
- mTLS and cryptographically signed communication
- Remote attestation / TEE (if supported)
- Supply-chain audits and proper provisioning
- Pen-tests and security audits scheduled
- Incident response and firmware rollback plan

If 80–90% of the above is fully implemented, it becomes practically impossible for a normal individual or small group to modify the device and generate fraudulent blocks.

### **What Works Exceptionally Well**

- Energy-proof concept - Verifying real solar physics via sensor data is the most reliable method of detecting fake power sources.
- Secure Element + Signed Firmware - Makes firmware tampering virtually impossible.
- Tamper Detection - Any enclosure opening or sensor disconnection causes instant lockout.
- mTLS + Signed Packets - Eliminates spoofing and MITM on the network layer.
- Nonce + Timestamp for Replay Protection - Prevents reuse of old proofs.

### **What Remains Risky (Even With All Protections)**

- Advanced Supply-Chain Attacks
  - If a chip vendor or manufacturer is compromised, attackers may embed backdoors (APT-level threat).
- Large-Scale Collusion
  - A very large operator (e.g., 1000+ devices) could centralize influence; mitigated via tokenomics design.
- Zero-Day Firmware or TEE Vulnerabilities
  - No system can prevent these entirely; continuous patching is required.
- Laboratory Attacks
  - A professional lab may extract keys through chip decapsulation; extremely expensive but technically possible.

### **Additional Recommendations for Near-Perfect Security**

We can do more to improve security and get close to perfect security.





#### 1) TEE-based Remote Attestation

(Example: ARM TrustZone, Intel SGX) - Device continuously proves its integrity while running.

#### 2) Environmental Fingerprinting

Cross-checking panel output with local weather and sunrise/sunset patterns in real-time.

#### 3) Slashing + Deposit Model

Fraud attempts result in block rejection plus loss of stake/deposit.

#### 4) Double Logging

Sensor logs stored both on the device and backend to detect discrepancies.

#### 5) Independent Third-Party Security Audits (Annual)

Hardware, firmware, backend, and blockchain reviewed by external experts.

### **Technical Next Steps**

#### 1) Formalize the Threat Model Document

Define attacker classes, capabilities, and plausible attack scenarios.

#### 2) Security Specification (Device + Firmware + Backend)

Finalize APIs, proof formats, attestation flows, and update protocols.

#### 3) Prototype + Red-Team

Deploy pilot (10–50 sites), then commission a professional red-team assessment.

#### 4) Pen-Testing & Supply-Chain Audits

Contract specialized firms for independent evaluation.

## **12 SIMCAT Mining Blocks**

SIMCAT will have 20-year block reward schedule and the SIMCAT tokens are gradually distributed through a halving-based emission model.

### **12.1 Block Time and Reward Structure**



The SIMCAT Solar Mining network follows a predictable, long-term issuance schedule designed to ensure stability, sustainability, and gradual supply reduction over a 20-year horizon.

### Block Time

- 10 minutes per block
- 6 blocks per hour, ~144 blocks per day

### Halving Schedule

- Block rewards halve every 4 years
- Total period: 20 years → 5 halving epochs
  - Epoch 1: Years 0–4
  - Epoch 2: Years 4–8
  - Epoch 3: Years 8–12
  - Epoch 4: Years 12–16
  - Epoch 5: Years 16–20

All calculations use the astronomical average of 365.2425 days per year.

### Total Eco System Reserve

A fixed supply of 410,400,000 \$SIMCAT is distributed over the 20-year period.

### Reward Summary (Key Results)

Initial Block Reward ( $R_0$ )

~1006.8432219 SIMCAT per block (Epoch 1)

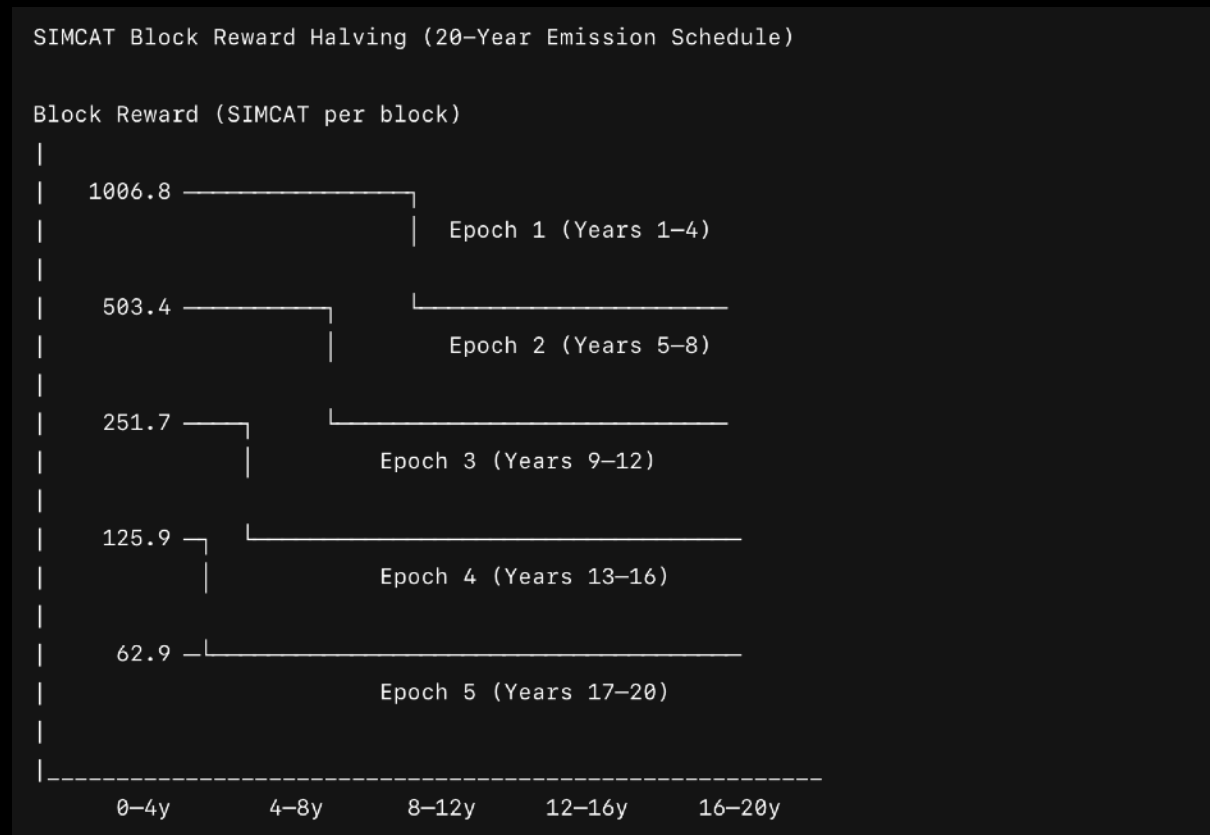
### Block Reward by Epoch

These values represent a strict 50% reduction in block rewards at the start of each epoch.

Epoch	Years	Block Reward
1	1-4	~1006.8432 SIMCAT/block
2	5-8	~503.4216 SIMCAT/block
3	9-12	~251.7108 SIMCAT/block
4	13-16	~125.8554 SIMCAT/block
5	17-20	~62.9277 SIMCAT/block



## Annual Token Distribution (Precise Values)



### Epoch 1 (Years 1–4)

Annual reward: 52,954,838.71 SIMCAT

Total epoch reward: 211,819,354.84 SIMCAT

### Epoch 2 (Years 5–8)

Annual reward: 26,477,419.35 SIMCAT

Total epoch reward: 105,909,677.42 SIMCAT

### Epoch 3 (Years 9–12)

Annual reward: 13,238,709.68 SIMCAT

Total epoch reward: 52,954,838.71 SIMCAT

### Epoch 4 (Years 13–16)

Annual reward: 6,619,354.84 SIMCAT

Total epoch reward: 26,477,419.35 SIMCAT

### Epoch 5 (Years 17–20)

Annual reward: 3,309,677.42 SIMCAT

Total epoch reward: 13,238,709.68 SIMCAT

## 20-Year Total Distribution



410,400,000 SIMCAT  
(Exactly matches the Eco System Reserve allocation)

## Block- and Epoch-Level Sample Calculation

Block Count Estimates

- Blocks per year (approx.):

$$\text{blocks\_per\_year} \approx 52,594.92$$

(Based on 365.2425 days/year and 10-minute block time.)

- Blocks per epoch (4 years):

$$\text{blocks\_per\_epoch} \approx 210,379.68$$

## 12.2 Deriving the Initial Block Reward ( $R_0$ )

The total Eco System Reserve of  $R_0 = 410.4M$  \$SIMCAT is emitted over 5 halving epochs.

The halving sum:

$$(\text{blocks\_per\_epoch} * \sum_{i=0..4} 1/2^i) \rightarrow R_0 \approx 1006.8432219$$

## Notes and Practical Implementation Guidance

### 1) Fractional Block Rewards

Since the block reward is not an integer, smart contracts must support fractional token accounting, typically by:

- Using a high-precision decimal (e.g., 18 decimals)
- Storing block rewards in fixed-point format for exact distribution

### 2) Rounded Minting Behavior

During mint operations, small fractional leftovers will accumulate. Two approaches:


- Carry-forward model:
  - Accumulate fractional remainders and add them to the next block.
- Internal rounding ledger:
  - Maintain a dedicated variable tracking fractional differences.

Both ensure accurate long-term emissions.

### 3) Difficulty / Dynamic Adjustments

The table above reflects only time-based halving.

Optionally, SIMCAT can introduce:

- 
- Difficulty modifiers tied to real network energy
  - Reward curves dependent on total solar kWh contributed

This changes the emission smoothness but can help balance fairness and decentralization.

#### 4) Tokenomics Alignment

Because the Eco System Reserve is fully distributed over 20 years, vesting and lock-up policies must align with:

- Team allocations
- Marketing reserves
- Seed and pre-seed investor schedules

A synchronized tokenomics framework prevents supply shocks.

### 13 Determined Risk Factors

The halving model reduces token emissions over time, but:

- Large operators can still dominate
  - If one entity deploys many solar sites, they contribute more kWh and therefore earn a disproportionately large share of rewards.
- A pure “reward-per-kWh” model encourages centralization
  - Without additional guardrails, high-capital actors can accumulate outsized control simply by scaling hardware faster than the rest of the network.

This must be addressed with tokenomic checks and balances (caps, staking weights, nonlinear reward curves, diminishing returns, etc.)


#### 13.1 Monopoly Formation and Practical Mechanisms to Prevent it

To prevent any single operator from dominating the SIMCAT Solar Mining ecosystem, several mitigation techniques can be applied individually or in combination. Each mechanism offers distinct advantages and strengthens decentralization.

##### a) Per-Site or Per-Owner Reward Caps

A straightforward and highly effective control mechanism is imposing maximum reward limits per site or per owner over a defined period (epoch or year).

- Each owner or site can earn no more than a fixed percentage of total epoch emissions. Example:



If  $X = 1\%$  and Epoch 1 distributes 211.8M SIMCAT,  
then a single owner can earn at most:  
 $\approx 2.118$  million SIMCAT

- Recommended range: 1–2% per epoch.

Benefit:

Clear, predictable, and prevents large operators from accumulating an outsized share.

#### b) Diminishing Returns (Reward Curve Compression)

Instead of paying a linear reward per kWh, the system can apply a non-linear diminishing returns curve. This means the more energy a site contributes beyond a threshold, the lower the incremental reward becomes.

A typical formula (for site share  $s$  and threshold  $T$ ) is:

```
if s <= T:  
    multiplier = 1  
else:  
    multiplier = T / s  
reward_site = base_reward_per_kWh * exported_kWh * multiplier
```

Or, if  $s$  is relatively large, apply exponential reduction:

$\text{multiplier} = \exp(-\text{beta} * (s/T - 1))$

Recommended values:  $T = 0.2\%$  (a small portion of the network),  $\text{beta} = 3\text{--}5$ .

#### c) Requiring Progressive Staking / Bond

If an owner wants to deploy a large amount of capacity, they must provide a correspondingly large stake or deposit. If they attempt to cheat, a slashing mechanism destroys part of their collateral. This creates an economic deterrent.

#### d) Randomized Selection + Lottery

For each block, choose among all valid energy-proofs randomly but with weighting, giving smaller sites a slight advantage

(weight =  $f(\text{exported\_kWh})^\gamma$ , with  $\gamma < 1$ ).

Benefit:

This reduces the linear dominance of large sites.





#### e) Owner / Site Identity and KYC Controls

It strengthen KYC and documentation requirements for registering many sites under one person or entity.

##### Benefit:

This helps identify “one person controlling many sites” scenarios without needing state-level involvement.

#### f) Vesting and Reward Lock-Up

Impose time-locked vesting for large reward recipients so they cannot instantly sell their tokens.

##### Benefit:

This protects the market and makes large-scale accumulation more difficult.

#### g) Community Governance and Caps

Introduce governance mechanisms allowing token holders to approve maximum site/owner caps or modify the reward function.

##### Benefit:

Dynamic parameters can be adjusted on-chain.

### 13.2 Monitoring and Enforcement

- Real-time dashboard: Display exported\_kWh, received tokens, and share% for each owner.
- Alerts: If an owner’s share% exceeds the defined threshold, trigger a flag and initiate a manual audit.
- On-chain limits enforcement: The smart contract should enforce a cumulative per-owner minting limit; the backend verifies and halts minting once the limit is exceeded.
- Periodic audits and random site inspections: Physical inspections and multi-sensor verification to confirm tamper resistance and operational integrity.

### 14 Recommended Initial Parameters

- Per-owner cap per epoch: 1% of total epoch rewards (modifiable through governance).
- Diminishing threshold T: 0.5% of network share.



- Diminishing formula (simple and reliable):  
`mult = min(1, T / owner_share_kwh)`
- Staking deposit: If an owner's share exceeds 0.5%, they must stake 10% of their token holdings.
- Vesting for large rewards: If an owner exceeds 0.5% share, 50% of their reward unlocks in the first year, and the remaining 50% unlocks over the next 3 years.

### **NOTE: Further Reducing Centralization**

These practical recommendations help further reduce centralization within the network by tightening thresholds, strengthening diminishing-returns formulas, lowering per-owner caps, increasing staking and vesting requirements for large operators, introducing bonus incentives for smaller sites, and running simulations using real owner-distribution data to fine-tune parameters for fairness and balance.

1) Lower the threshold T (for example to 0.2% or 0.1%) - this increases the penalty for large owners.

2) Strengthen the diminishing-returns formula - using

```
mult = exp(-beta*(owner_share/T-1))
```

and increasing beta above 3–5 will equalize results more aggressively.

3) Reduce the per-owner cap (e.g., 0.5% per epoch) - this cap acts as a firm, hard-limit protection.

4) Increase staking requirements and vesting - require larger stakes and slower unlock schedules from owners running large capacity.


5) Introduce additional egalitarian mechanisms: Provide bonus multipliers for small sites (e.g., if `owner_share` < 0.05%, add a +10% bonus) - this boosts small-operator motivation.

### **DISCLAIMER: We used a random model here**

Eventually we will have to run simulations using real owner-distribution data; Once we have a real or estimated distribution (e.g., 10,000-site sales forecast for a region), we then can generate a more precise analysis. *(This analysis would be for internal use only)*

## **15 SIMCAT Mining Technology**

This mining technology implements a hardware-attested, sensor-verified energy-proof protocol that transforms authenticated photovoltaic output into



on-chain block generation through a secure, tamper-resistant, solar-bound proof-of-work mechanism.

### **High-level Architecture**

Edge device > Secure Ingest Gateway > Stream/Queue > Stream processors (window aggs) > Batch aggregator workers > On-chain minting batch > Archive/Audit.

### **15.1 System Architecture and Recommended Technology Stack**

SIMCAT's solar-powered mining protocol relies on a highly reliable, scalable, and secure cloud-native data pipeline. This architecture ensures that every energy-proof generated by edge devices is securely ingested, validated, aggregated, and ultimately minted on-chain with full auditability and real-time monitoring.

#### **Core Components and Recommended Technologies**

##### **1) Edge Device (Mining Rig + Gateway)**

Performs real-time sensor logging, generates signed proof packets, maintains sequence numbers, handles GPS/time data, and communicates via mutual TLS. Capabilities: sensor logs, signed proofs, mTLS, GPS, seq-no.

##### **2) Ingest Gateway / API Layer**

A secure, horizontally scalable endpoint for device traffic, terminating mTLS and forwarding authenticated packets. Recommended stack: Nginx or Envoy + Kubernetes autoscaling + L4/L7 load balancing.

##### **3) Message Broker / Stream Layer**

High-throughput, partitioned ingestion for all device proofs and block-window data. Recommended: Apache Kafka or Apache Pulsar.

##### **4) Stream Processors**

Real-time processing engines executing per-window aggregation, block-level computation, and deterministic state transitions. Recommended: Apache Flink, Kafka Streams, or Spark Streaming.

##### **5) State Store / Databases**

Persistent, scalable storage for proof logs, block aggregates, and owner-state tracking. Recommended:

- Time-series data: TimescaleDB
- High-scale key/value: Cassandra
- Hot cache: Redis

#### 6) Batch Aggregator Workers

Autoscaled worker pool (Python or Go) responsible for evaluating diminishing rules, cap enforcement, staking logic, and generating Merkle-root mint batches.

#### 7) On-Chain Minting Service

Signer + HSM performing gas-optimized mint transactions using Merkle-tree batching. Supports both automatic payouts and Merkle-proof claim mechanics. Custody layers: Gnosis Safe, threshold signatures, or HSM-protected signers.

#### 8) Audit & Archive Layer

Immutable storage for all proofs, logs, and batch histories. Recommended: S3/MinIO + SIEM using Elasticsearch + Kibana.

#### 9) Monitoring & Observability

Infrastructure metrics, pipeline health, device telemetry, and reward analytics. Recommended: Prometheus + Grafana.

#### 10) Security Stack

mTLS everywhere, signed payloads, device attestation (TEE), and HSM-protected private keys.

### 15.2 Data Flow Overview

The SIMCAT data pipeline processes energy-proofs in a deterministic, verifiable, and fault-tolerant sequence:

#### 1) Device -> Gateway

Sends signed proofs:

```
signed_proof { device_id, ts, window_hash, kWh, sig }
```

#### 2) Gateway -> Kafka (topic: `proofs`)

Messages are partitioned (e.g., `device_id % N`) for parallel processing.

#### 3) Stream Processor



For each partition:

- Computes 10-min block windows
- Aggregates `total_kWh_block` and individual owner contributions

Output -> `topic block_aggregates`.

#### 4) Batch Aggregator

Consumes aggregated blocks over hourly or daily rolling windows.

Applies:

- diminishing multipliers
- per-owner caps
- staking/vesting checks
  - Produces `mint_batch` (JSON + Merkle root).

#### 5) On-Chain Minting

Submits a batched mint transaction containing:

- Merkle root
- Total minted amount
- Minimal encoded leaves
  - Off-chain storage persists full owner-level payouts.

#### 6) Post-Minting


- Update audit logs
- Adjust `epoch_remaining`
- Notify owners
- Archive immutable records

This ensures deterministic correctness, transparency, and auditability.

### 15.3 Batching Strategy

SIMCAT emphasizes efficiency, security, and gas minimization through multi-layer batching:

- Per-block (10-minute) aggregation: Real-time operational integrity
- Per-hour minting batches: Reduce on-chain transactions by combining multiple blocks
- Epoch finalization (4 years):
  - enforce caps
  - reconcile any remaining rewards
  - optionally redistribute or burn unspent tokens
- Merkle batching:

- 
- Leaves = {owner\_id, amount}
  - On-chain stores only the Merkle root + total minted.
  - Owners claim via Merkle proofs, or the system auto-pushes payouts with multisig.

## Scalability and Parallelism

The architecture scales linearly with devices and owner counts:

- 10,000 owners: 10–20 Kafka partitions achieve sub-second aggregation.
- 100,000 owners: Scale partitions  $\times 10$ ; autoscale worker pods.
- Throughput: Kafka supports  $>100k$  msgs/s; Flink handles tens of thousands of keyed windows per node.
- Latency target:  $<1$  minute from block-window close to finalized aggregation; On-chain minting within a policy-defined window (minutes).

## Data Structures & State

- `proofs` topic entry: {device\_id, ts, window\_hash, exported\_kWh, sig, seq}
- `block_aggregate` record: {block\_id, total\_kWh, [{owner\_id, kWh}], ts}
- `owner_epoch_state`: {owner\_id, epoch\_minted, epoch\_kWh, stake\_status, cap\_remaining} stored in Redis + persistent DB.

## 15.4 Gas Optimization Strategy

To reduce on-chain costs:

- Use Merkle root + claim model  $\rightarrow$  one tx per batch
- Backend or owners submit claims using Merkle proofs
- Multisend optional but grows cost linearly
- Future migration to L2 or sidechain (Arbitrum/Polygon/custom permissioned chain) reduces gas by orders of magnitude


## Fault Tolerance, Idempotency & Chain Reorg Handling

- Idempotency: seq numbers prevent duplicates
- Exactly-once semantics: Kafka + Flink checkpoints
- Chain reorg protection: finality delay or permissioned validators
- Recovery: consumers rely on offsets; batch jobs are retried with the same Merkle root

## Security Operations (SecOps)

- Device private keys stored in Secure Elements





```

# input: list of block_aggregates for hour
owner_kwh = defaultdict(float)
total_kwh = 0.0
for blk in blocks:
    total_kwh += blk.total_kwh
    for o in blk.owners: owner_kwh[o.id] += o.kwh

# compute raw, multiplier, cap
payouts = {}
for owner, kwh in owner_kwh.items():
    raw = epoch_block_token_rate * (kwh / total_kwh) # or per-block mapping
    share_pct = 100.0 * kwh / total_kwh
    mult = 1.0 if share_pct <= T else (T / share_pct)
    adjusted = raw * mult
    adjusted = min(adjusted, owner_epoch_cap_remaining(owner))
    payouts[owner] = adjusted

# create merkle leaves and root, store off-chain
root = merkle_root(payouts)
submit_onchain(root, total=sum(payouts.values()))

```

- mTLS for all device ↔ gateway communication
- TLS for broker and inter-service transport
- HSM or multisig custody for minting keys
- Signed OTA firmware
- Remote attestation for suspicious devices
- Immutable logs + periodic third-party security audits

### Minimal Implementation Roadmap

- Build ingest API + Kafka pipeline
- Create simple stream job for 10-minute window aggregation
- Implement batch worker for diminishing/cap logic -> output Merkle root
- Deploy Merkle-mint smart contract on testnet
- Launch pilot with 100 devices -> scale to 10k -> tune partitions -> scale to 100k+

### Batch Aggregator Pseudocode - Concise

This outlines the core logic executed by the batch worker: it collects block-level aggregates, applies diminishing-returns and cap rules, verifies staking and eligibility constraints, computes the final owner-adjusted payouts for the batch, and generates the Merkle tree structure used for on-chain minting.



## 16 Operational Execution Framework

- Start with a permissioned chain or an L2 - this reduces gas costs and latency issues in the early phases.
- Tune batching parameters (block -> hourly) after the pilot phase based on real performance data.
- R&D: Improve the Merkle-claim user experience - consider an on-chain gas-subsidy strategy to support automatic “push” payouts.

## Computation Completed - Simulation Results

I added the staking rule into the simulation: if an owner's share% > T = 0.5%, then for that epoch they must provide

`required_stake=10%*raw_epoch_reward`

If their actual stake is lower, their reward is reduced with

`penalty_multiplier=0.5`

The simulation was run under two owner-distribution models: heavy-tailed and egalitarian.

## Key Results

### Heavy-Tailed Distribution

- Total distributed:  $\approx 405,756,256$  SIMCAT (lower than the previous  $\approx 409.5M$  due to penalties and diminishing).
- Top 1% of owners receive  $\approx 25.68\%$
- Top 10% receive  $\approx 84.86\%$
- Number of penalized owners: 3 (these were large, non-compliant owners in the simulation).

### Egalitarian Distribution

Total distributed:  $\approx 410,400,000$  SIMCAT (practically full distribution; no penalties applied).

- Top 1%  $\approx 2.07\%$ , Top 10%  $\approx 16.38\%$ 
  - Penalized owners: 0

## Conclusion

The staking rule increases pressure on large operators: if they fail to provide the required stake, their rewards are reduced. In the simulation, only a few large non-compliant owners were penalized - but overall centralization in the



heavy-tailed scenario remains high (top 10%  $\approx$  85%). To further reduce centralization, you can:

- decrease  $T$ ,
- reduce the owner cap, or
- increase penalty strength.

## **17 Mining Architecture (Design Overview)**

SIMCAT is an independent Layer-1 blockchain built on a Proof-of-Work (PoW) consensus mechanism, following a security model and node architecture similar to Bitcoin Core. Mining serves as the backbone of the network—securing the chain, validating transactions, and distributing block rewards to miners. Unlike inflationary blockchains where tokens are newly created at block discovery, SIMCAT implements a Reserve-Release Mining Model: all mining rewards are pre-allocated into the Ecosystem Reserve (410.4M SCAT) and unlocked gradually as miners secure the network.

### **Consensus and Proof-of-Work**

- Consensus Algorithm: PoW using SHA-256 hashing, fully compatible with Bitcoin-style mining.
- Block Time: Targeted at 10 minutes.
- Block Validation: Miners must produce a block header hash below the current network difficulty.
- Difficulty Adjustment: Every 2,016 blocks (~2 weeks), difficulty is recalculated based on previous block production times.
- Security Model: PoW prevents Sybil attacks, enforces transaction immutability, and ensures adversaries face high economic cost for malicious actions.

### **Block Rewards and Halving**

- Initial Block Reward: 1006.8432 SCAT per block.
- Halving Schedule: Rewards are halved every 210,384 blocks (approximately 4 years).
- Emission Duration: Over ~20 years, the full 410.4M SCAT Ecosystem Reserve is gradually released to miners.
- Post-Emission Phase: After the reserve is exhausted, miners are compensated exclusively through transaction fees, ensuring long-term economic security for the network.



## Reserve-Release Mining Model

Unlike Bitcoin, where block rewards are minted into existence, SIMCAT uses a pre-funded reserve from which rewards are released according to the schedule.

### a) Reserve Initialization

At genesis, 410.4M SCAT is assigned to the Ecosystem Reserve.

### b) Coinbase Transaction Mechanics

- When a block is found, the reward is unlocked from the reserve rather than newly minted.
- Consensus rules enforce that rewards must strictly follow the predefined emission schedule.
- The exact SCAT amount is transferred to the miner's address.

### c) Consensus Enforcement

If a block attempts to release more SCAT than allowed at that height, it is automatically rejected by validators.

### d) Transparency

- All reserve movements are fully visible on-chain.
- The entire Reserve-Release lifecycle can be audited in explorers.

## Conclusion


This model combines Bitcoin's predictable halving-based emission schedule with reserve-based transparency, ensuring:

- predictable long-term supply,
- verifiable on-chain reserve accounting,
- and sustainably secured network mining economics.

## 18 Mining Infrastructure

This project's mining infrastructure uses SHA-256-based hardware powered primarily by solar energy, integrated with secure RPC/Stratum protocols and a reserve-controlled reward system to ensure efficient, transparent, and sustainable Proof-of-Work mining.

### a) Hardware Requirements



SIMCAT's mining layer leverages industry-standard SHA-256 hardware to ensure compatibility, performance, and long-term sustainability.

b) Supported Mining Hardware

- SHA-256 ASIC miners - primary and most efficient option.
- Optimized SHA-256 FPGA systems - suitable for specialized or low-power environments.

c) Energy Sources

- Primary: Solar panels with integrated battery storage systems for stable, carbon-neutral mining.
- Backup: Grid electricity, used only when solar output is insufficient.

d) Protocol Compatibility

SIMCAT is designed to be interoperable with existing mining ecosystems:

- JSON-RPC: `getblocktemplate`, `submitblock`, and full node RPC compatibility.
- Stratum v1 / Stratum v2: Compatible with pool mining and multi-miner deployments.

## 18.1 Reward Distribution Security

SIMCAT's Reserve-Release model introduces strict cryptographic and consensus-level safeguards to ensure transparent, tamper-proof emission.

- Reserve Locking: Block rewards can only be released through consensus rules; no entity can mint arbitrarily.
- Emission Verification: Each node independently validates reward amounts against block height and the halving schedule.
- Forgery Resistance: No miner or operator can extract more SCAT than permitted-any invalid block is automatically rejected.
- On-Chain Auditability: All reserve-related transactions are publicly visible and continuously verifiable through explorers.

## 18.2 SIMCAT Mining Lifecycle

1) Miner Setup: Install SIMCAT Core, configure hardware, and connect to a mining pool or run in solo mining mode.

2) Hashing Process: The miner iteratively modifies the nonce and hashes the block header until a valid PoW solution is found.

3) Block Submission: The discovered block is broadcast across the network.



- 4) Consensus Verification: Nodes validate the PoW, check all transactions, and ensure that block rewards match the reserve emission schedule.
- 5) Reward Distribution: The permitted SCAT reward is released from the Ecosystem Reserve and sent to the miner's address.
- 6) Halving: Every ~4 years (210,384 blocks), the block reward is reduced by 50%. This continues for approximately 20 years until the full reserve is released.

### 18.3 Long-Term Sustainability

- 20-Year Reserve Duration: A controlled and predictable emission schedule ensures stability and fairness across decades.
- Eco-Friendly Mining: Solar-powered SHA-256 mining significantly reduces carbon footprint.
- Post-Reserve Incentives: After the reserve is depleted, miners are rewarded exclusively through transaction fees, mirroring Bitcoin's long-term model.


### Key Parameters (Summary Table)

Parameter	Value
Consensus Mechanism	Proof-of-Work (SHA-256)
Block Time	10 minutes
Initial Block Reward	1006.8432 SCAT
Halving Interval	210,384 blocks (~4 years)
Total Mining Reserve	410.4M SCAT
Emission Duration	~20 years
Difficulty Adjustment	Every 2,016 blocks
Energy Source	Solar + Battery (sustainable)

### 19 Technical Specifications

A concise overview of the core technical architecture, consensus design, and mining model of the SIMCAT blockchain.

### Blockchain Design



SIMCAT is an independent Layer-1 Proof-of-Work (PoW) blockchain inspired by Bitcoin's architecture but enhanced with a unique Reserve-Release Mining Model. All mining rewards are pre-allocated at genesis and unlocked strictly through block production, ensuring predictable tokenomics and complete supply transparency.

### **Genesis Parameters**

At network launch, the following core parameters are defined:

- Genesis Timestamp - the exact moment the chain is initialized.
- Genesis Nonce - the unique value generating the initial block hash.
- Genesis Merkle Root - the root hash of the genesis block's transactions.
- Genesis Allocation:
  - Ecosystem Reserve (Mining): 410.4M SCAT
  - Other allocations: as defined in the tokenomics (airdrop, staking, marketing, etc.)

All SIMCAT tokens exist from the outset, but only the mining reserve becomes progressively accessible through PoW block creation.

### **Proof-of-Work Consensus**

- Algorithm: SHA-256 (fully compatible with Bitcoin mining hardware).
- Block Time: 10 minutes (target).
- Difficulty Adjustment: Every 2,016 blocks (~2 weeks).
- Halving Interval: Every 210,384 blocks (~4 years).
- Emission Duration: ~20 years, until the reserve is fully released.

Every node independently validates each block and enforces the rule that only the permitted reward amount may be unlocked at that height.


## **19.1 Reserve-Release Mining Model**

1) Locked Supply: At genesis, 410.4M SCAT is locked into the Ecosystem Reserve.

2) Coinbase Transaction: When a block is mined, the reward is released from the reserve, not newly minted.

3) Emission Schedule:

- Years 1–4: 1006.8432 SCAT / block
- Years 5–8: 503.4216 SCAT / block
- Years 9–12: 251.7108 SCAT / block
- ...and continues halving every 4 years.

- 
- 4) Consensus Enforcement: Any block attempting to unlock more SCAT than allowed is automatically rejected.
  - 5) Transparency: Reserve balances and withdrawals are visible on-chain and verifiable at all times.

## **19.2 Mining Infrastructure**

### **Hardware**

- SHA-256 ASIC miners (Bitcoin-class performance).
- GPU/FPGA systems for early testing and development phases.

### **Energy Sources**

- Primary: Solar panels + battery storage for stable renewable mining.
- Backup: Grid electricity as a secondary option.

### **Mining Software**

- Stratum v1/v2 support for pool and solo mining.
- JSON-RPC API for block template generation and submission.

### **Sustainability Goal**

Mining is designed around solar energy to achieve a carbon-neutral operational footprint.

## **19.3 Competitive Advantages**

- 1) Transparency - Rewards come directly from the reserve; no hidden inflation.
- 2) Predictability - A mathematically defined halving schedule ensures long-term clarity.
- 3) Environmental Benefit - Solar-powered mining minimizes carbon impact.
- 4) Security - SHA-256 PoW with global miner participation.
- 5) Longevity - A 20-year emission model followed by a fee-driven security phase.

## **Conclusion**

SIMCAT's mining architecture is inspired by Bitcoin's proven PoW design but enhanced with a transparent Ecosystem Reserve-Release model, providing sustainable tokenomics, environmental efficiency, and long-term economic clarity. This innovation differentiates SIMCAT from traditional emission frameworks while retaining the reliability and security of SHA-256 PoW.

## **20 Mining Hardware Architecture**

Technical outline of the device that transforms solar energy into blockchain-secured rewards.





## 20.1 Purpose

The SIMCAT mining device is engineered to measure, verify, and cryptographically bind solar-generated energy to the blockchain in a transparent and tamper-resistant manner. Every kilowatt-hour (kWh) produced by the user's solar panels is authenticated through hardware sensors, processed into an energy-proof, and converted into mining rewards on the SIMCAT network.

## 20.2 Components and Functions

The device consists of several core hardware modules, each performing a critical role in the energy-to-blockchain process:

### 1) ASIC / RISC Compute Engine

- Performs cryptographic hashing of energy-proof data.
- Executes mining operations based on the Proof-of-Energy model.
- Ensures energy production is directly linked to block creation.

### 2) MCU/SoC + Secure Element (HSM)

- Serves as the device's primary control unit.
- Manages energy accounting and block-signature workflows.
- Secure Element stores private keys, enforces tamper detection, and prevents key extraction.

### 3) PV Sensor Array

- Measures solar panel output including:
- Voltage (V), Current (I), Irradiance (light intensity), Temperature.
- Provides a physical-layer guarantee that the energy is real and solar-derived.

### 4) Precision Energy Meter

- A tamper-evident electricity meter measuring all produced and consumed kWh.
- Supports bidirectional energy flow measurement.
- Ensures accurate, auditable energy accounting.

### 5) Communication Module (LTE / LoRa / Wi-Fi)

- Connects the device to the SIMCAT blockchain network.
- Sends proof packets and block-window data every 10 minutes.

- SIM slot and antennas enable fully autonomous operation.

#### 6) Enclosure + Tamper Sensors

- Weather-resistant casing (IP65 rated) for long-term outdoor deployment.
- Tamper switches detect opening, drilling, cable removal, or intrusion attempts.

#### 7) PCB Assembly (4–6 Layer Industrial Board)

- Integrates all chips, sensors, and communication modules.
- Designed to meet industrial reliability standards and long-term durability.

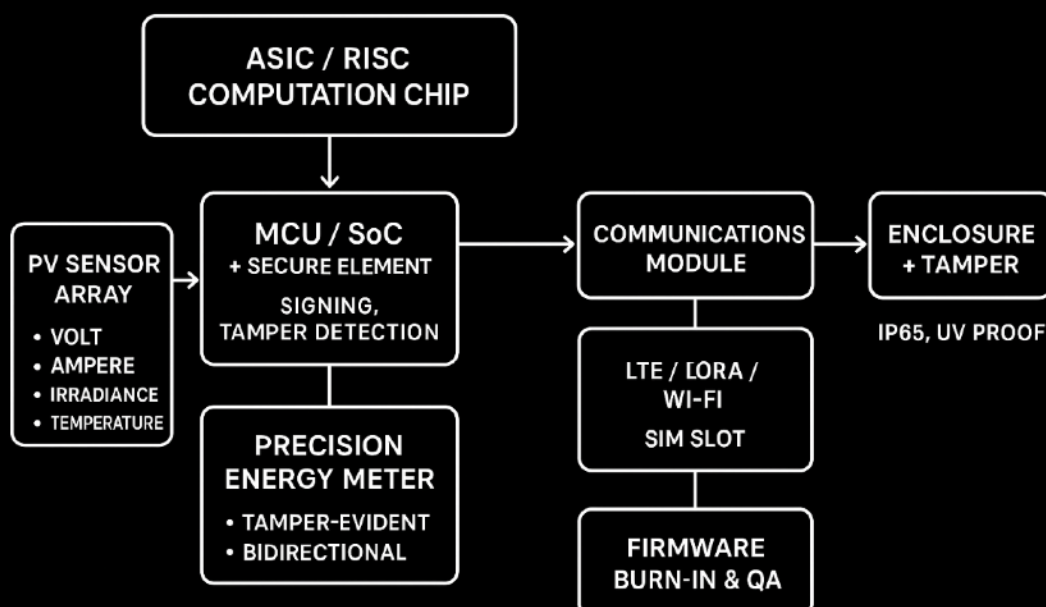
#### 8) Firmware & Factory Quality Assurance

- Secure firmware is flashed during production.
- Each device undergoes factory calibration, stress testing, and blockchain connectivity verification.

### 20.3 Process Flow

- 1) Solar panels generate electrical energy.
- 2) The PV sensor array and energy meter capture real-time production data.
- 3) The MCU/SoC aggregates sensor readings and prepares a data packet.
- 4) The ASIC processor hashes the energy data into an energy-proof cryptographic structure.
- 5) The Secure Element signs the proof, ensuring authenticity and anti-tampering validity.
- 6) The device submits data to the blockchain; every 10 minutes, a block is formed and the user receives SIMCAT token rewards accordingly.

### MINING HARDWARE ARCHITECTURE



## 20.4 Device Advantages

- Waterproof and Dustproof (IP65): Ensures long-term stability in outdoor environments such as sun, dust, and rain.
- Full Transparency: All generated energy is measured and recorded directly on-chain.
- High Security: Secure Element + tamper sensors protect against physical attacks and unauthorized modifications.
- Operational Independence: Works autonomously via LTE/LoRa connectivity.
- Industrial Durability: High-grade components ensure long service life and reliable operation.

### Device Components (Per Unit)

*Note: The terms "chip" and "module" may vary depending on vendor architecture.*

The list below reflects the recommended minimum/standard configuration for a single-unit miner.

#### 1) ASIC / RISC Mining Chip

- Quantity: 1 unit (or 2–4 ASIC modules for higher-performance designs)
- Function: Performs hash computations tied to Proof-of-Energy.

#### 2) MCU / SoC

- Quantity: 1
- Function: Central controller managing sensors, communication, and system operations.

#### 3) Secure Element (SE / HSM)


- Quantity: 1 (integrated or discrete chip)
- Function: Stores private keys, signs proofs, ensures tamper resistance.

#### 4) PV Sensor Array (for energy verification)

- Components:
  - Voltage sensor (1×)
  - Current sensor (1×; shunt or hall-effect)
  - Irradiance sensor (1×; lux or pyranometer)
  - Temperature sensors (1–2×; panel surface & enclosure interior)
- Function: Provides accurate photovoltaic signature and energy-production profiling.

#### 5) Precision Energy Meter (Tamper-Evident, Bidirectional)

- Quantity: 1

- 
- Function: Measures kWh, logs tamper events, outputs signable billing-grade data.
- 6) Communication Module (LTE / LoRa / Wi-Fi) + SIM Slot
- Quantity: 1
  - Function: Sends authenticated proofs to the blockchain gateway.
- 7) Enclosure (IP65) + Tamper Switch + Gasket
- Quantity: 1 complete housing
  - Function: Provides environmental protection and tamper detection.
- 8) PCB Assembly (4–6 Layers) + Electronic Components
- Quantity: 1
  - Function: Integrates all chips, power rails, and sensors on a stable industrial platform.
- 9) Cooling System / Heatsinks
- Quantity: 1 heatsink (or 1+ auxiliary thermal components)
  - Function: Controls ASIC thermal performance.
- 10) Power Management Module (DC-DC converters, fusing)
- Quantity: 1
  - Function: Distributes and protects DC power from the solar panel.
- 11) Antennas and RF Components
- Quantity: 1 external antenna + cables
  - Function: Ensures reliable wireless communication.
- 12) RTC (Real-Time Clock) + Coin Battery
- Quantity: 1 RTC + 1 coin cell
  - Function: Maintains accurate timestamps for logs and proofs.
- 13) Cables & Mounting Accessories
- Quantity: 1 set
  - Function: Connectors, screws, cable glands, and mounting hardware.
- 14) Firmware Burn-In & Factory QA
- Practical: Each device is flashed with firmware and tested for full functionality.
- 15) Packaging & Manual
- Quantity: 1 retail box + 1 user manual.
- 16) Logistics / Mounting Brackets / Grounding Lug
- Quantity: 1 installation kit.
- 17) Warranty Reserve & R&D Amortization
- Practical: Allocated per company policy.

## **IP65 Water Protection - Requirements and Elements**



IP65 means the device is fully protected from dust and resistant to low-pressure water jets for reliable outdoor operation.

1) IP65 Definition:

- "6" → complete dust protection
- "5" → resistance to low-pressure water spray

Note: Not designed for underwater use (IP67/68 required for immersion).

2) IP65 Housing (Material & Design)

- Material: UV-stabilized polycarbonate or corrosion-resistant aluminum (anodized).
- Design: One-piece or gasketed cover with minimal internal cavities.

3) EPDM / Silicone Gasket

- Provides reliable sealing between housing and cover.

4) IP65 Cable Glands

- Sealed cable exits for antennas, power lines, and sensors.

5) Breather Vent (Membrane Vent)

- PTFE vent equalizes internal pressure and reduces condensation.

6) Conformal Coating or Selective Potting

- Nano/polymer coating on PCB; potting on critical areas for added protection. *(Note: Potting reduces serviceability.)*

7) Corrosion-Resistant Screws

- AISI 316/304 stainless steel or coated hardware.

8) Tamper Switch + Tamper Wire Routing

- Sends tamper events directly to firmware and Secure Element.

9) Connector Sealing (SIM Slot, Maintenance Ports)

- Sealed covers or embedded SIM trays for waterproofing.

10) Desiccant Packet

- Absorbs moisture during long-term outdoor operation.

11) Mounting Design (Water Drip Edges & Tilt)

- Prevents water pooling; optimizes drainage and environmental endurance.

12) IP65 Testing & Certification

- Each batch undergoes spray testing; test logs may be included as appendices.

## 21 CPU / ASIC / Modem Device Architecture

A hardware stack integrating CPU, ASIC, and modem components to authenticate energy and transmit mining proofs.

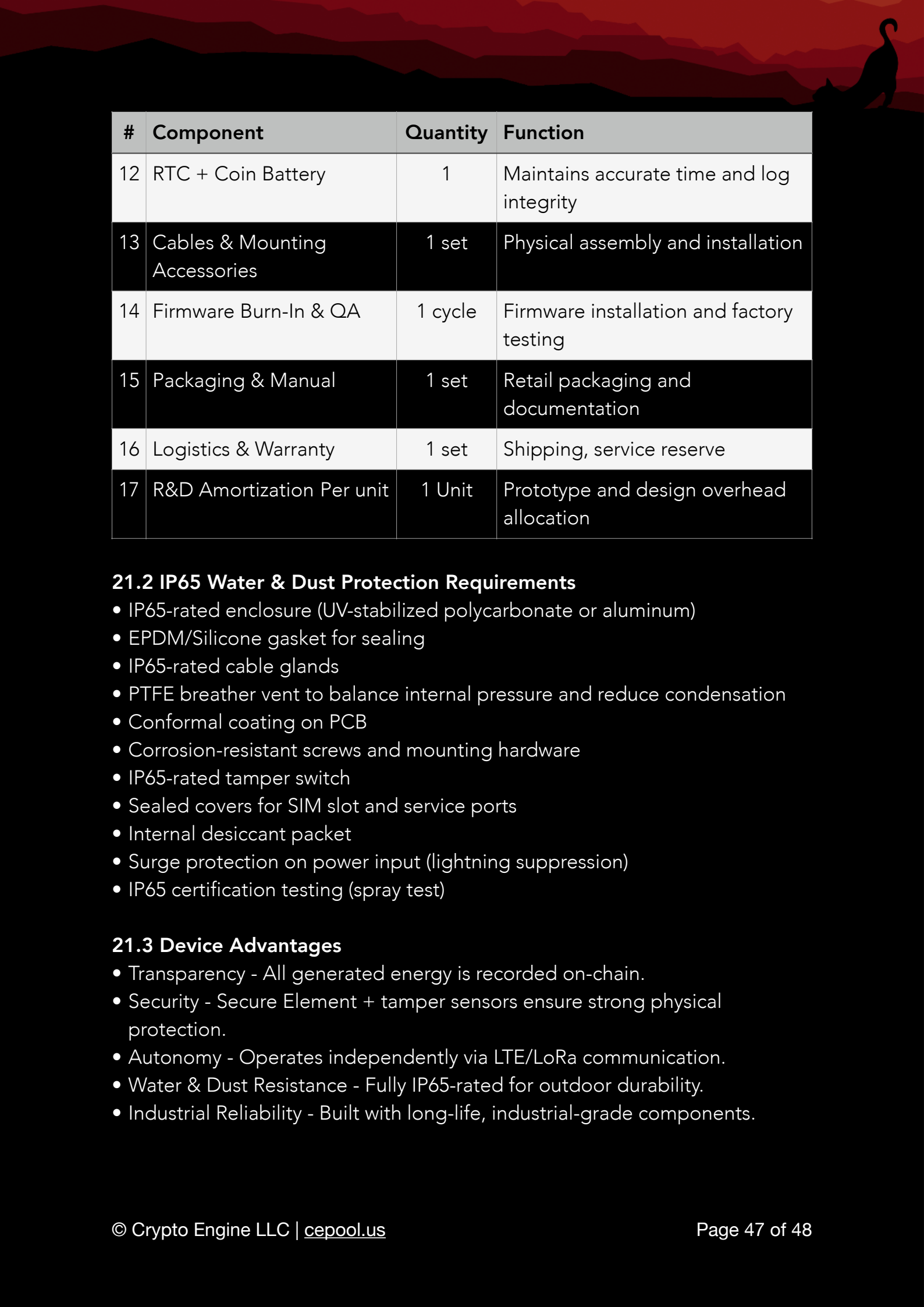
## Purpose of the Device

The SIMCAT Mining Device is designed to measure, verify, and transmit solar-generated electrical energy to the blockchain in a transparent, tamper-resistant manner. Through this hardware, every kilowatt-hour (kWh) produced by the user is authenticated and converted into token rewards.

### 21.1 Device Components (Tabular Overview)

A structured summary of all core hardware modules and their functions.

#	Component	Quantity	Function
1	ASIC / RISC Mining Chip	1 (or 2–4 modules)	Performs energy-linked hashing / Proof-of-Energy computation
2	MCU / SoC	1	System control, sensor data acquisition, communications
3	Secure Element (SE / HSM)	1	Stores private keys, generates signatures, provides tamper detection
4	PV Sensor Array	3–4	Captures PV voltage, current, irradiance, and temperature data
5	Precision Energy Meter	1	Measures kWh, logs tamper events
6	Communications Module (LTE / LoRa / Wi-Fi)	1	Connects device to blockchain gateway
7	IP65 Enclosure + Tamper Switch + Gasket	1	Provides dust/water protection and tamper alerting
8	PCB Assembly (4–6 layers)	1	Integrates electronic components and power paths
9	Cooling / Heatsink	1	Manages ASIC thermal load
10	Power Management Module	1	Distributes DC power from solar panels
11	Antenna & RF Components	1	LTE/LoRa wireless connectivity




#	Component	Quantity	Function
12	RTC + Coin Battery	1	Maintains accurate time and log integrity
13	Cables & Mounting Accessories	1 set	Physical assembly and installation
14	Firmware Burn-In & QA	1 cycle	Firmware installation and factory testing
15	Packaging & Manual	1 set	Retail packaging and documentation
16	Logistics & Warranty	1 set	Shipping, service reserve
17	R&D Amortization Per unit	1 Unit	Prototype and design overhead allocation

## 21.2 IP65 Water & Dust Protection Requirements

- IP65-rated enclosure (UV-stabilized polycarbonate or aluminum)
- EPDM/Silicone gasket for sealing
- IP65-rated cable glands
- PTFE breather vent to balance internal pressure and reduce condensation
- Conformal coating on PCB
- Corrosion-resistant screws and mounting hardware
- IP65-rated tamper switch
- Sealed covers for SIM slot and service ports
- Internal desiccant packet
- Surge protection on power input (lightning suppression)
- IP65 certification testing (spray test)

## 21.3 Device Advantages

- Transparency - All generated energy is recorded on-chain.
- Security - Secure Element + tamper sensors ensure strong physical protection.
- Autonomy - Operates independently via LTE/LoRa communication.
- Water & Dust Resistance - Fully IP65-rated for outdoor durability.
- Industrial Reliability - Built with long-life, industrial-grade components.



SIMCAT is a digital asset designed to build a sustainable, fair, and long-lasting ecosystem. Through its innovative mining mechanism, smart-contract-based lock/unlock processes, and deflationary token-burn system, SIMCAT provides users with stable earning opportunities and a strong, engaged community.

## **DISCLAIMER**

This whitepaper is for informational purposes only and does not constitute financial, investment, or legal advice. SIMCAT Token (\$SIMCAT) is a utility token intended for use within the \$SIMCAT ecosystem. Purchasing \$SIMCAT involves risk, including the potential loss of capital. Prospective participants should conduct their own research and consult with qualified financial and legal advisors before making any investment decisions. \$SIMCAT does not guarantee any profits or returns, and token values may fluctuate significantly based on market conditions. Participation is subject to local laws and regulations, and SIMCAT reserves the right to modify its offerings to remain compliant.