$SIMCAT TOKEN
POWERED BY THE SUN

WHITEPAPER (v. 9.77)

Author: Jack Samatov
Co-author: Beghzod Gapparov

Date: Sunday, November 23, 2025
Version: 9.0 (first public version)

SIMCAT is a new utility token with the ticker symbol **$SIMCAT**. The initiative launches with the SIMCAT Solar Miner as its flagship innovation, a device that transforms unused solar energy into $SIMCAT tokens through a patented solar-mining system supported by the Crypto Engine Mining Pool. The projects is introduced to the community through CryptoCat, a tap-to-earn game introducing gamified education in crypto and blockchain. While CryptoCat accelerates adoption and airdrop distribution, SIMCAT Solar Mining delivers the token's core long-term value: turning renewable energy into digital assets.

Learn more at **cryptocat.io** and follow the ecosystem at **simcat.io**

1. SECURITY

1.1 SIMCAT Authenticator

User Dashboard of **simcat.io** is a comprehensive ecosystem that provides a single access point for seamless interaction across various platforms, including Web, Staking, audited Smart Contracts and Crypto Exchange software. Whether users are managing their assets, participating in staking, or engaging in trading activities, they can access all functionalities through a unified interface. This streamlined approach leverages verifiable Smart Contracts to ensure a secure and trusted single environment, eliminating the need for multiple logins and offering a single secure environment for all financial and digital asset operations.

One of our top priorities is security, which is why SIMCAT.Auth has implemented a three-step security mechanism. This system is designed to securely store and protect the user's essential information, ensuring a convenient, high level of safety and reliability for all transactions.

Security Module

The primary requirement for security activation is enabling the Authenticator. SIMCAT.Auth operates with a three-step authentication process which is more advanced than the common two-factor authentication. Activation Process:

1. Phone Number Verification – The systems authentication process is initiated through a valid phone number of the user.
2. Authenticator Scan – A unique code is generated by an authenticator app.

3. Secure Password Storage – The authentication key is stored securely for all future verifications and invoked whenever the 1st step of the authentication process is completed.

When accessing the SIMCAT Dashboard, users receive notifications via email and can monitor active sessions directly within the dashboard. This approach ensures users privacy and prevents unauthorized access.

1.2 Enhanced Security with SIMCAT Mobile Wallet

SIMCAT Mobile Wallet introduces a new encryption feature that allows users to securely encrypt their private keys, significantly enhancing wallet security. By implementing industry-standard encryption mechanisms, it ensures that sensitive user information remains protected from unauthorized access, providing safer and more reliable experience for managing all digital assets.

Industry-Standard Encoding & Decoding: Encoding and decoding all online transactions is essential for securing and transmitting data across digital platforms. These processes ensure that data remains protected while enabling authorized users to retrieve information securely and conveniently.

Common Encoding Methods (Data Protection & Transmission)

- Base64 Encoding: Converts binary data into ASCII characters for safe transmission over text-based systems (e.g., email, JSON, URLs). Commonly used in cryptographic applications, API keys, and embedded certificates.
- PIN-Based Encryption: In security-sensitive applications like mobile wallets, a PIN code is selected by the user and used to encrypt private keys. Decoding is only possible with the selected PIN, the data remains inaccessible without the correct PIN so users have to make sure to choose a PIN that is unique to them and easy to remember. Users are advised to avoid easy-to-guess PINs consisting of repeated numbers or number sequences.

Decoding & Authentication

- Base64 Decoding: Converts Base64-encoded text back to its original binary format, often used for decrypting authentication tokens and digital certificates.
- Multi-Factor Authentication (MFA) Encryption: Combines PIN, biometric authentication, and one time passcodes (OTP) to secure access, adding multiple layers of protection against unauthorized entry. When (and only) all

layers of security request are satisfied, the session is created and maintained across the infrastructure so the user gets access to all services of the platform.

PIN Code Encryption for SIMCAT Mobile Wallet

SIMCAT Mobile Wallet will be featuring a new, PIN-based encryption replacing the previous secondary password option for improved security and ease of use.

How It Works:

1. Users must enter their existing secondary password to set up a new PIN code.
2. Once set, the PIN serves as the decryption key, allowing access to private keys and other sensitive wallet data.
3. Every login or critical transaction requires PIN verification to unlock encrypted information.

This enhanced security model ensures that only authorized users can access their digital assets while protecting against unauthorized access and data breaches

1.2.1 Problems with Current Wallets

MetaMask, Binance, Coinbase, Exodus, and Ledger are undoubtedly among the most popular wallet brands in the crypto space. However, they each come with limitations that impact user experience and security.

- MetaMask – While widely used, it is centralized and so controlled by a single business entity which raises concerns about data privacy and potential external control or abuse.
- Binance & Coinbase – These too are centralized exchanges, meaning users rely on third parties for funds security, introducing potential points of failure as shown with similar solutions in the past.
- Exodus & Ledger – Although decentralized, they lack mobile-friendly functionality, making them less convenient for on-the-go users.

These limitations highlight the need for a new secure, decentralized, and user-friendly wallet that balances accessibility with full control over private keys. Crypto wallets are essential apps for interacting with blockchain networks. However, the wallet brands currently dominating the market tend to provide only basic functionality.

Moreover, these established wallet providers rely on their early market success and display little desire to innovate or improve the user experience. As a result, they fail to introduce meaningful enhancements, adapt to newer technology solutions that could simplify processes and bring more value to end users.
This lack of innovation highlights the need for a next-generation wallet that prioritizes user convenience, enhanced functionality, security and improvements beyond just the basic blockchain interaction.

1.2.2 SIMCAT Wallet: The Easiest and Most Secure Crypto Wallet

SIMCAT Wallet aims to be the most user-friendly and secure crypto wallet for investors of all experience levels. It goes beyond basic functionality by offering a wide range of features, enhanced capabilities, and additional benefits, ensuring a seamless and secure blockchain experience. With a mission to capture 20% of the crypto wallet market by the end of 2028, SIMCAT Wallet is set to revolutionize the Web3 experience by offering competitive benefits to its users, it aims to redefine how people interact with blockchain technology, making it more accessible, secure, and rewarding for everyone.

SIMCAT Wallet is built on a fully decentralized ecosystem, with the SIMCAT Token playing a key role in enhancing user trust and driving adoption. By supporting the IMCAT ecosystem, the token helps reduce transaction fees, providing users with a more cost-effective way to manage their assets. It also grants exclusive early access to the most exciting new pre-sales and public announcements of AirDrops to give users competitive edge in emerging opportunities. Additionally, IMCAT aims to attract more users through strategic airdrops, further strengthening its presence in the market. By providing these type of unique advantages to its users, the $SIMCAT is set to become the leading wallet token in the decentralized finance space.

SIMCAT Wallet offers unparalleled value to its users through its custom-built new portal called "USA News Token” that provides a gateway to invest in new crypto projects still in their pre-sale phase.

This unique feature allows users to access promising tokens before they are listed on exchanges and hit the broader market, securing them at the lowest possible prices. Such pre-sales events present a major opportunity for investors to gain early access to high-potential projects, a feature that sets SIMCAT Wallet apart from other crypto wallets. With its exclusive Initial Coin Offering (ICO) integration, SIMCAT Wallet delivers an innovative investment advantage that no other wallet currently offers, making it a game-changer in the crypto space.

1.3 Wallet (SIMCAT.Auth)

By offering a blockchain-based financial platform, we strive to meet all financial needs within $SIMCAT’s unique infrastructure. A wide range of $SIMCAT cryptocurrencies, including SIMCAT Coin, as well as stablecoins such as SIMCAT Cash and SIMCAT USD, are designed to facilitate various financial transactions.

In addition to providing comprehensive services such as decentralized exchange, easy access to opportunities, new SIMCAT Transfer and an online payment gateway, the $SIMCAT also has taken measures to enhance security by offering a diverse set of wallets built on the SIMCAT Blockchain. This includes dedicated mobile wallets for iOS and Android. Essentially, this involves a duplication of the tokens for demonstration purposes, specifically for the press release to showcase liquidity using internal components available within the ecosystem.

1.3.1 Exchange (SIMCAT.Auth)

SIMCAT Exchange enables fast, secure, and cost-effective cryptocurrency transactions while allowing users to manage their crypto portfolios within a single mobile application. By linking the customer account directly to the crypto wallet, the exchange process becomes more efficient, reducing transaction times and minimizing fees. With support for payments in Euros and US dollars, SIMCAT Exchange ensures a seamless, affordable, secure and convenient trading experience.

1.3.2 Seamless and Profitable P2P Crypto Exchange

With SIMCATs P2P exchange, you can seamlessly conduct direct cryptocurrency trades between users, ensuring a more profitable and decentralized transaction experience. The platform allows you to find the best currency exchange rates and purchase any cryptocurrency using a credit card or a bank transfer, making the process more flexible, efficient, and cost-effective.

1.3.3 SIMCAT Payment Gateway

SIMCAT Payment Gateway is an API-driven solution designed for eCommerce. Its integration enables seamless payment transactions for goods and services using the $SIMCAT and other supported cryptocurrencies. By integrating directly with online platforms, the gateway will provide merchants with a secure and efficient way to accept crypto payments for online purchases. Similar to industry leaders like Stripe and Skrill, SIMCAT Payment Gateway facilitates real-time transaction processing, invoice generation, and automated settlement, ensuring a smooth and reliable payment experience. Its robust API allows developers to easily integrate payment functionalities into websites and mobile applications, offering a scalable and flexible solution for businesses looking to embrace digital currency payments.

SIMCAT Payment Gateway introduces an innovative approach to crypto transactions by enabling seamless transfers and real-time exchanges between different cryptocurrencies. Merchants can set a preferred digital asset for payments, while customers have the flexibility to pay using any supported cryptocurrency. The system will automatically convert the chosen by the user cryptocurrency into the merchant's preferred currency, ensuring smooth and efficient transactions. With support for SIMCAT Coin, SIMCAT Cash, SIMCAT E, as well as Bitcoin, Litecoin, and Ethereum, this breakthrough solution streamlines crypto payments and provides users with a transparent final cryptocurrency output accepted at the checkout.

The balance of expenses is calculated in proportion to the coins that need to be deposited online. Additionally, the user is provided with a QR code containing all the necessary payment details, including the wallet address, cryptocurrency type, and the amount of cryptocurrency paid. By scanning this QR code with any wallet, particularly the SIMCAT Wallet, the user is seamlessly redirected to the Payment Gateway for transaction processing.

This process takes place outside the online store's website, ensuring that customer wallet data is never stored on the eCommerce platform.

- Once the invoice is settled, the customer can wait for the receipt to be issued. Payments received through the SIMCAT Payment Gateway will be transferred to the seller's account as quickly as possible and the system automatically notifies both, the buyer and the seller, that the transaction has indeed been completed successfully. If the buyer cannot obtain a guarantee of the seller’s authentication, both parties can conduct the financial transaction through the SIMCAT Transfer service for added security. This payment gateway service is built around high level of security and convenience befitting both customers and sellers.

- Customer security – No wallet or payment method information is required from the customer, nor is any data stored anywhere, ensuring complete privacy and protection.
- Seller security: Transactions and receipts are only processed after the necessary confirmations have been obtained, providing an additional layer of reliability for merchants.
- Ease of use: The gateway allows users to complete transactions without being redirected to another website or required to provide additional information, ensuring a seamless and hassle-free payment experience.

Any failure in any step of the process will nullify the transaction on the eCommerce platform that initiated the transaction and automatically notify the seller and the buyer about the failure.

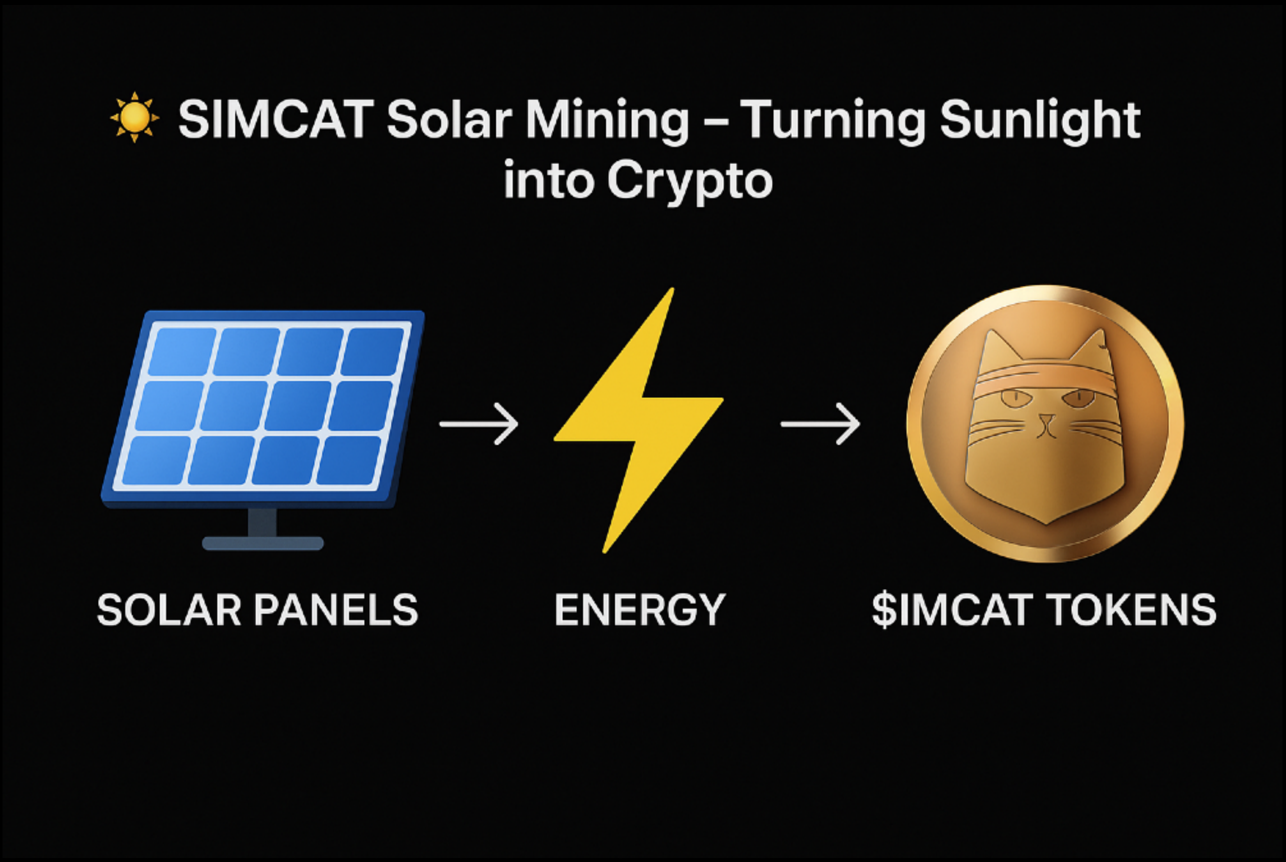
2. SIMCAT Solar Mining

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.

2.1 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.

2.2 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.

2.3 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

2.4 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.

2.4.1 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

2.4.2 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.

2.5 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.

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.4 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.

2.6 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.

2.7 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.

2.8 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.

2.8.1 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.

2.9 High-Level Architecture (Mermaid Diagram)

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

```
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]
```

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 identificator (manufacturer-signed)
`ts` - proof timestamp
`exported_kWh` - he 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.

2.10 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.

2.11 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.

2.11.1 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.

2.11.2 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 tokennomics 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.

2.11.3 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.

2.11.4 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.

2.12 SIMCAT Mining Blocks

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

2.12.1 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)

```
SIMCAT Block Reward Halving (20–Year Emission Schedule)

Block Reward (SIMCAT per block)
|
|   1006.8 ────────────────┐
|                          │  Epoch 1 (Years 1–4)
|
|    503.4 ──────────┐     └───────────────────────
|                    │        Epoch 2 (Years 5–8)
|
|    251.7 ────┐     └─────────────────────────────
|              │         Epoch 3 (Years 9–12)
|
|    125.9 ─┐  └────────────────────────────────────
|           │            Epoch 4 (Years 13–16)
|
|     62.9 ─└───────────────────────────────────────
|                        Epoch 5 (Years 17–20)
|
|________________________________________________________
      0–4y       4–8y      8–12y     12–16y     16–20y
```

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.):

```
blocks_per_year ≈ 52,594.92
```

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

- Blocks per epoch (4 years):

```
blocks_per_epoch ≈ 210,379.68
```

2.12.2 Deriving the Initial Block Reward (R_0)

The total Eco System Reserve of `R₀ = 410.4M` $SIMCAT is emitted over 5 halving epochs.

The halving sum:

`(blocks_per_epoch * sum_{i=0..4} 1/2^i)` -> R0 ≈ **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.

2.13 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.)

2.13.1 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:
  ≈ 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:

```
    multiplier = exp(-beta*(s/T - 1))
```

Recommended values: T = 0.2% (a small portion of the network), beta = 3–5.

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(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.

2.13.2 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.

2.14 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)*

2.15 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.

2.15.1 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 entrypoint 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.

2.15.2 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.

2.15.3 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 ×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.

2.15.4 Gas Optimization Strategy

To reduce on-chain costs:

- Use Merkle root + claim model -> 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)

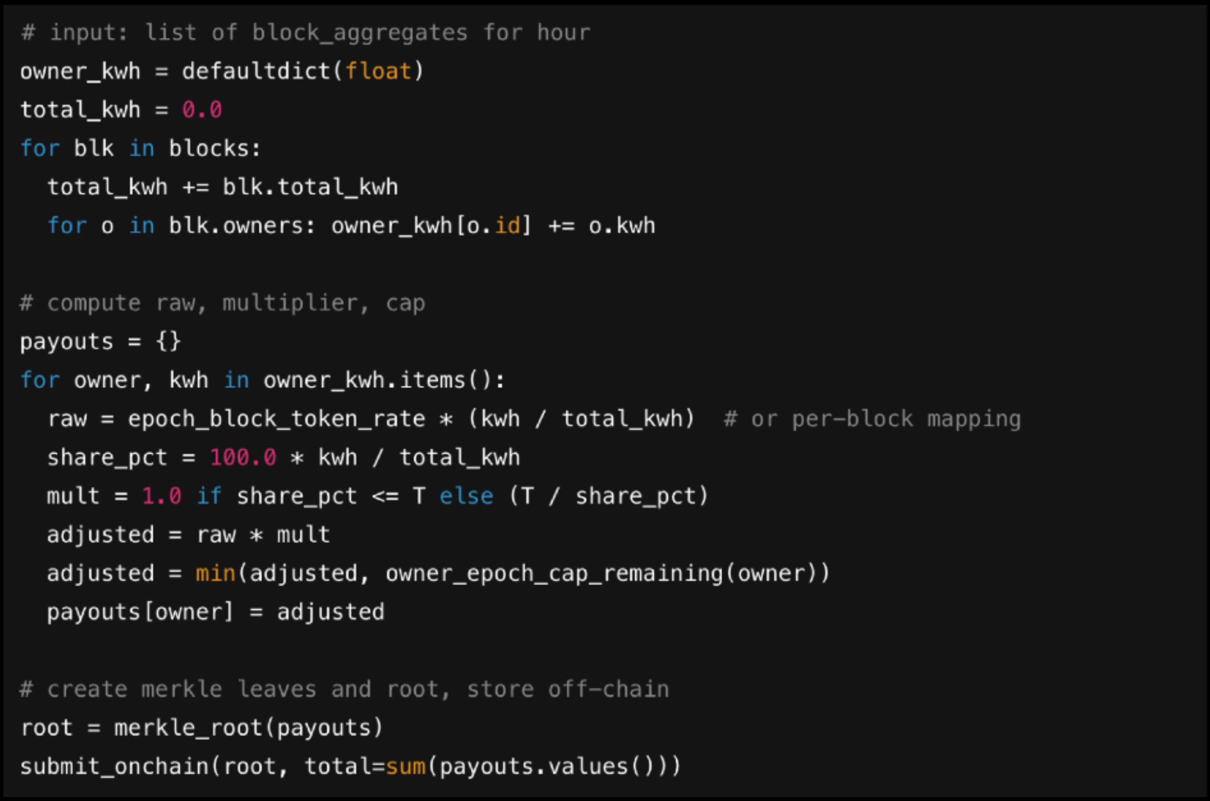
- Device private keys stored in Secure Elements
- mTLS for all device ↔ gateway communication
- TLS for broker and inter-service transport
- HSM or multisig custody for minting keys
- Signed OTA firmware
- Remote attestation for suspicious devices
- Immutable logs + periodic third-party security audits

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.



```
# 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()))
```

2.16 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: ≈ 405,756,256 SIMCAT (lower than the previous ≈409.5M due to penalties and diminishing).
- Top 1% of owners receive ≈ 25.68%
- Top 10% receive ≈ 84.86%
- Number of penalized owners: 3 (these were large, non-compliant owners in the simulation).

Egalitarian Distribution

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

- Top 1% ≈ 2.07%, Top 10% ≈ 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% ≈ 85%). To further reduce centralization, you can:

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

2.17 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.

2.18 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.

2.18.1 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.

2.18.2 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.

2.18.3 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)

Parameter	Value
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)

2.19 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.

2.19.1 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.

2.19.2 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.

2.19.3 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.

2.20 Mining Hardware Architecture

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

2.20.1 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.

2.20.2 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.

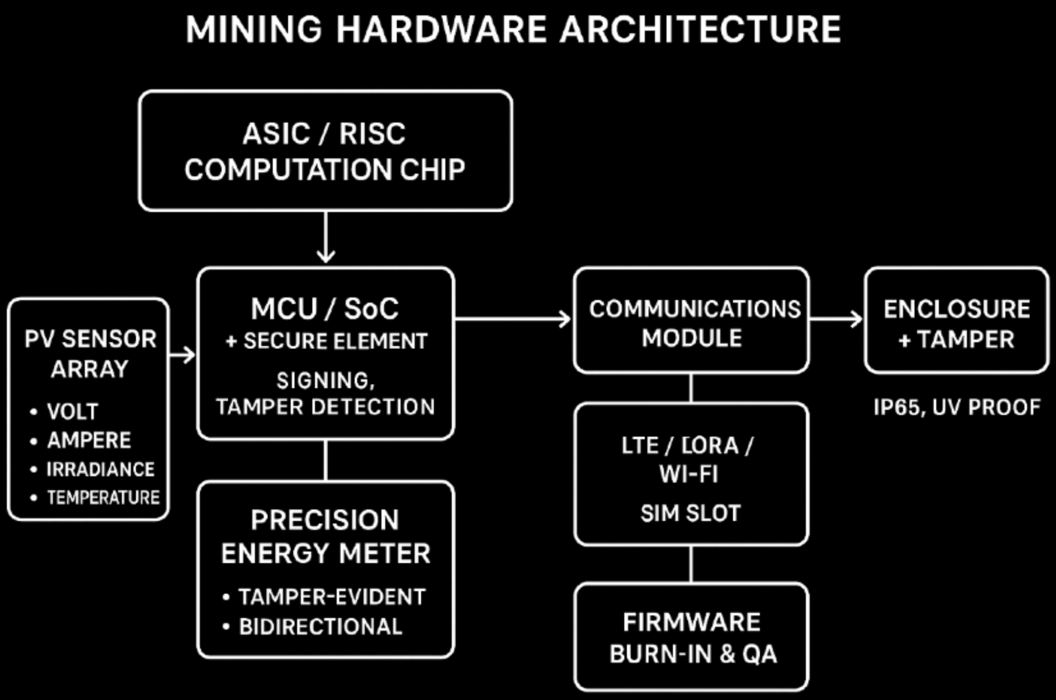
7) PCB Assembly (4–6 Layer Industrial Board)
- Integrates all chips, sensors, and communication modules.
- Designed to meet industrial reliability standards and long-term durability.

8) Firmware & Factory Quality Assurance
- Secure firmware is flashed during production.
- Each device undergoes factory calibration, stress testing, and blockchain connectivity verification.

2.20.3 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.



2.20.4 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.

2.21 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.

2.21.1 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

#	Component	Quantity	Function
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
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

2.21.2 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)

2.21.3 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.

3. Blockchain Banking

$SIMCAT introduces a new Blockchain Bank as a unique, decentralized financial system that provides banking services such as deposits, lending, payments, and investments, all operating on blockchain technology without relying on traditional intermediaries. Built on a decentralized ledger, the bank ensures transparency and immutability, utilizing smart contracts to automate financial transactions, reducing manual oversight, and increasing efficiency. With a consensus mechanism like Proof-of-Stake (PoS), transactions are validated securely, while interoperability allows seamless transfers across multiple blockchain networks. Customers can deposit funds in non-custodial wallets, earn interest through staking, and access collateralized loans without requiring credit scores, all facilitated by smart contracts. Instant peer-to-peer transfers with minimal fees enable global transactions, while tokenized assets provide investment opportunities in digital and real-world assets. Security and compliance are integrated through decentralized identity verification, multi-signature wallets, and auditable smart contracts, ensuring user trust while maintaining regulatory standards. Governance is handled through a decentralized autonomous organization (DAO), allowing token holders to vote on financial policies and system upgrades, ensuring democratic decision-making. To bridge the gap between decentralized and traditional finance, the bank can integrate fiat on-ramps and off-ramps, enabling crypto-to-fiat conversions and partnerships with licensed institutions for seamless withdrawals. By combining decentralized technology with regulatory safeguards, a Blockchain Bank offers an innovative, secure, and efficient financial ecosystem, providing faster transactions, lower fees, and increased accessibility while giving users full control over their assets.

3.1. SIMCAT as franchisee of Metabank

Metabank is the first decentralized bank from MetaTech Ltd, France. It now has a unique franchise system that SIMCAT is partnering to become its major franchisee and plan to open a new and unique digital Blockchain Bank to provide its users with a virtual credit or debit card payment options. Though this partnership we will cooperate with Visa Card and Master Card so users can add $SIMCAT assets to Apple Pay or Google Pay and pay with it everywhere using any smartphone.

3.1.1 Virtual credit or debit cards

Virtual cards work exactly like a physical bank card - they just live in user digital wallet on users phone instead of a physical wallet. Secured by encryption, they offer a safe and convenient way to pay online and in-store. We will provide Visa credit cards and debit cards as well as MasterCard credit and debit cards.

3.1.2 Payments through connected IBAN accounts

IBAN stands for "International Bank Account Number" and is a unique identifier assigned to bank accounts in Europe and in a total of 104 countries worldwide. The IBAN facilitates easier and faster processing of cross-border payments. By using IBAN, major banking systems can connect to microservices delivered through a collaborative infrastructure, accessible via APIs that support the app economy. As a franchisee utilizing the Metabank payment platform, SIMCAT aims to leverage these traditional banking services alongside the flexibility and potential of cryptocurrencies and blockchain technologies.

3.1.3 Crypto payments

The Metabank cryptocurrency payments infrastructure adds an extra layer of convenience for $SIMCAT users, offering features such as order tracking and easy management of crypto earnings through widely accepted, user-friendly crypto payment options. Users can simply scan a QR code to add a wallet address and make payments using any cryptocurrency. Through its partnership with Metabank, $SIMCAT will gain support for both the Ethereum, Solana and BSC (Binance Smart Chain) networks, as established by MetaTech Ltd.

3.1.4 P2P loans

This partnership with Metabank will also give $SIMCAT users access to a pool of lenders and borrowers through matchmaking algorithms, enabling a fully functional, decentralized peer-to-peer lending platform. This will lead to the creation of unique credit funds for our users in the crypto space. Together, SIMCAT and Metabank aim to revolutionize the overly complicated traditional credit creation process, allowing borrowers to access crypto funds and lenders to participate in a decentralized global marketplace. It’s a true peer-to-peer solution-without intermediaries or traditional “middleman” services.

3.1.5 Staking and yield farming

SIMCATs Blockchain Bank will provide its own, Staking-as-a-Service feature that will allow users to stake tokens, specially created for that purpose with earning interests based on a rate set by Metabank. Our logic to calculate the staking interest will be implemented using a Compound protocol designed to ensure fair reward distribution among users pool. The core idea behind the Compound logic is to calculate rewards based on both time and rate, ensuring accurate and equitable distribution. Calculations will be based on these methods of earning:

- Staking: We will offer minimum of 6 months locked staking, or a staking with no fixed duration where the duration is set by the user himself.
- Yield Farming: Gain high interest rates and generate passive income by providing liquidity.

3.1.6 Governance token

A governance token is a type of cryptocurrency that gives its holders the right to participate in the decision-making processes of a blockchain protocol, decentralized application (dApp), or decentralized autonomous organization (DAO). In the context of blockchains, participants have incentives to consolidate power and guide the network in directions that benefit them. Holders can vote on proposals that may affect the future of the protocol-such as updates, new features, fee structures, or how treasury funds are used. Basically, there are three different approaches to on-chain governance:

- Fork-based governance
- Stake-based governance
- Entity-based governance

Some votes are executed automatically on-chain, while others may influence off-chain decisions made by developers or teams.

3.1.7 Smart Contract

Another key concept of the Metabank protocol is the "Smart Contract", which serves as a digital authorization to access an underlying asset (e.g., a bank account or cryptocurrency account) in order to initiate a payment or retrieve information. The protocol will be implemented within the $SIMCAT infrastructure as a combination of Smart Tokens, accessible via an SDK (Software Development Kit) and API (Application Programming Interface).

4. SIMCAT Exchange (Regional Patent #DGU 202407842)

By providing a decentralized exchange service, outside of Metabank infrastructure, the SIMCAT Exchange empowers users to trade directly with peers through blockchain, eliminating the need for intermediaries. Users can seamlessly convert cryptocurrencies into one another or fiat money while maintaining full control over their assets without relying on a third party. Unlike traditional exchanges, SIMCAT Exchange does not require users to deposit their digital assets, reducing the risk of hacks and theft. Acting as a trade verifier rather than a custodian, SIMCAT Exchange ensures transaction security and authenticity while preserving the core principle of decentralization-no middleman, just direct and secure peer-to-peer trading.

SIMCAT Exchange provides a low-cost trading experience by applying minimal commission fees while ensuring secure and direct cryptocurrency conversions. Users can exchange digital assets without relying on intermediaries, reducing unnecessary costs and delays. The platform employs a highly secure multi-key algorithm, where transactions are only finalized when at least two out of three private keys are registered-one for each party and an optional third-party verifier. This ensures seamless and efficient trading while maintaining security, transparency, and cost-effectiveness for all users.

5. The AirDrop

In the crypto industry, an airdrop is a method of distributing free cryptocurrency tokens to a large number of wallet addresses, typically as part of a marketing campaign or community engagement strategy. Blockchain projects use airdrops to raise awareness, reward loyal users, or encourage participation in their ecosystem. Some airdrops require users to hold a specific cryptocurrency at a set snapshot date, while others may ask participants to complete tasks such as social media promotion, referrals, or joining a community. In some cases, tokens are distributed exclusively to early adopters or long-term supporters of a project. Airdrops help decentralize token distribution, drive adoption, and create initial liquidity in the market. $SIMCAT's initial distribution strategy involves allocating over 25.5% of its total token supply to airdrops and game-based rewards, incentivizing early adoption and community engagement.

5.1. CryptoCat the Game

CryptoCat is a play-to-earn game available to anyone on the telegram platform: CryptoCatGame_bot Players join the cat named Simone, a determined and curious cat who digs through the mines, hills, and mountains of Central Asia in search of valuable stones-digital assets representing various cryptocurrencies. Simone works alone, learning and growing as he delves deeper into the world of blockchain technology. The gameplay is centered on a reinvented Tap Farming mechanic. While the basic action is simple-tap to mine-CryptoCat adds depth through a unique learning system. As Simone discovers new crypto gems (quirky representations of cryptocurrencies) and masters blockchain concepts, his earnings per hour increase. This ties progression directly to education, turning gameplay into a light-hearted but meaningful learning experience about crypto. An hourly farming module further enhances Simone's income, which scales based on upgrades and new technologies unlocked during his journey.

5.1.2. CryptoCat AirDrop

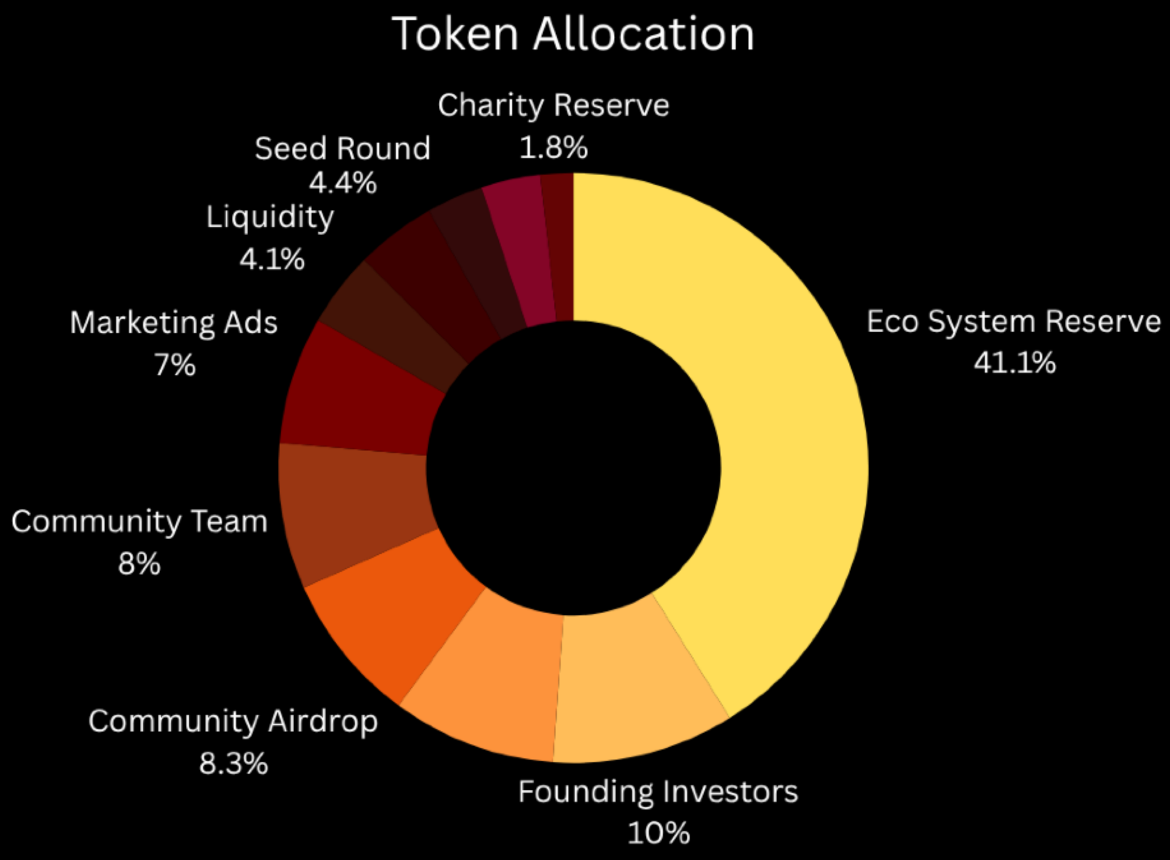
CryptoCat Airdrop is designed as an exclusive giveaway for loyal wallet supporters. Early adopters and campaign participants will receive special rewards, with additional bonuses distributed after the Airdrop period ends. This initiative ensures that those who support the wallet from the beginning are recognized with valuable extras. Participants in the CryptoCat Airdrop can register on the official airdrop website at **cryptocat.io** and earn exclusive rewards by completing daily or weekly tasks. These tasks introduce users to all the wallet's features, including selling, exchanging, and participating in token pre-sales, ensuring early supporters gain first-hand experience with the platform.

As a thank-you to loyal supporters, the CryptoCat Airdrop distributes free tokens and exclusive perks, rewarding users who actively engage with the ecosystem. With a strong user base built over six months, the airdrop has created a dedicated community that has completed over 100 tasks, helping SIMCAT Wallet expand beyond traditional crypto wallets. By the end of July 2025, more than 100,000 active participants were recorded, collectively completing over 1,000 tasks. This initiative not only incentivizes engagement but also sets a new standard for rewarding early adopters and shaping the future of decentralized finance.

6. SIMCAT Tokenomics

It is designed to create a sustainable and efficient ecosystem that benefits both users and investors. The native token, SIMCAT Token, serves as the backbone of the platform, facilitating transactions, reducing fees, and unlocking exclusive rewards within the ecosystem. A fixed total supply ensures scarcity, while a portion of tokens is allocated for ecosystem development, liquidity, staking rewards, and community incentives. Users holding SIMCAT Tokens can enjoy reduced transaction fees, early access to premium features, and participation in governance decisions. Staking mechanisms encourage long-term holding by rewarding users with additional tokens for securing the network.

Transaction fees generated within the ecosystem are partially burned or redistributed to active participants, ensuring continued value appreciation. With a structured token distribution model, SIMCAT Wallet aims to maintain a balanced and self-sustaining economic system that supports growth,



innovation, and user engagement.

Only 1B SIMCAT Tokens will be issues

The SIMCAT Token presents an exclusive opportunity for early supporters to purchase at the lowest prices before it gets publicly listed. SIMCAT Wallet and SIMCAT Exchange users will have priority access to buy tokens directly through the SIMCAT Wallet or $SIMCAT web-networks application via the Tokens portal. This early access, available one month before the token sale opens to other wallet providers, allows users to secure their holdings at a better price before wider market availability. In order in increase price value and to comply with the best jurisdictions we decided to lock the amount of $SIMCAT to 1,000,000,000 tokens with the following Tokenomics:

Eco System Reserve	41.10%	411,000,000 $SIMCAT
Founding Investors	10.0%	100 M $SIMCAT
Staking Liquidity	9%	90 M $SIMCAT

Community Airdrop	8.25%	82.50 M $SIMCAT
Community Team	8%	80 M $SIMCAT
Marketing Ads	7%	70 M $SIMCAT
Liquidity	4.1%	41 M $SIMCAT
Seed Round	4.4%	44 M $SIMCAT
Pre Seed round	3.1%	31 M $SIMCAT
Launchpool Market	3.25%	32.5 M $SIMCAT
Charity Reserve	1.8%	18 M $SIMCAT
TOTAL	**100%**	**1 B $SIMCAT**

Total Supply: 1,000,000,000 (1 billion) $SIMCAT
Model: Hybrid (Proof-of-Work + Proof-of-Stake) anchored on Solana
Halving: Every 4 years
Total Mining Period: 20 years

1. Ecosystem Reserve: 41.10% (411,000,000 $SIMCAT)
-The main fund used for mining, blockchain updates, and overall ecosystem development.
-Tokens are stored in a locked state and released automatically through a smart contract.
-A new block is mined every 10 minutes, and halving occurs every 4 years.
-Gradual release over 20 years prevents sudden market pressure.
-This deflationary mechanism helps maintain long-term price stability.

2. Founding Investors: 10% (100,000,000 $SIMCAT)
-Reserved for founding investors only.
-10 year vesting schedule:
 Years 1–5: 0.5% unlocked monthly
 Year 6: 0.833% unlocked monthly
 Years 7–10: 1% unlocked monthly
-All transactions are tracked through smart contracts.
-Investors cannot dump tokens quickly, preventing market pressure.

3. Staking Liquidity: 9% (90,000,000 $SIMCAT)
-Dedicated fund for staking rewards.

-Locked via smart contract.
-Tokens unlock only during reward distribution periods.
-Remaining tokens are used to ensure mining stability.
-Tokens are released gradually to avoid sudden market flooding.

4. Community Airdrop: 8.25% (82,500,000 $SIMCAT)
-Distributed to attract new users and expand the community.
-Conducted in 4 phases, each releasing 25% of tokens; the remaining unclaimed tokens are burned.
-Each phase's tokens are unlocked quarterly (every season, 25%).
-Claim period: 60 days, after which unclaimed tokens are burned.
-Prevents sudden token oversupply and supports a deflationary balance.

5. Community Team: 8% (80,000,000 $SIMCAT$SIMCAT)
-Fund for team incentives and long-term motivation.
-Locked for 5 years, unlocking 0.5% monthly.
-After 5 years, unlock rate increases to 1% per month.
-All operations are transparent and managed via smart contracts.
-Gradual release ensures price stability and sustained team motivation.

6. Marketing & Ads: 7% (70,000,000 $SIMCAT)
-Reserved for marketing, branding, and partnerships.
-Tokens stored in a Marketing Treasury Contract.
-Monthly spending limited to 1.5–2%.
-Marketing is continuous but token releases are phased to ensure sustainability.

7. Liquidity: 4.1% (41,000,000 $SIMCAT)
-Used for market liquidity and CEX/DEX listings.
-Introduced in 4 phases through a smart contract.
-Gradual liquidity injection helps protect the market price.

8. Seed Round: 4.4% (44,000,000 $SIMCAT)
-Allocated for early-stage investors.
-2 year lock period:
Years 1–2: 1% monthly unlock
Year 3: 2% monthly unlock
Year 4: 2.66% monthly unlock

-Sales and transfers are fully controlled via smart contracts.

9. Pre-Seed Round: 3.1% (31,000,000 $SIMCAT)
-For very early investors.
-2 year lock period:
Years 1–2: 1% monthly unlock
Year 3: 2% monthly unlock
Year 4: 2.66% monthly unlock
-Smart contracts ensure transparent sale control and prevent misuse.

10. Launchpool Market: 3.25% (32,500,000 $SIMCAT)
-Reserved for pre-listing Launchpool events.
-Tokens released gradually at a rate of 0.5–1% per month.

11. Charity Reserve: 1.8% (18,000,000 $SIMCAT)
-Dedicated to charity and social impact projects.
-Locked for 2 years.
-After unlocking, 5–10% of the released tokens will be used for charitable purposes each month.

The collected funds will be allocated toward expanding product development and strategic marketing campaigns. Tokens will be designated for the CryptoCat Airdrop, rewards, community incentives, exchange liquidity, and treasury reserves.

7. SIMCAT Staking (Regional Patent #DGU 202407850**)**
The SIMCAT Wallet presale operates in tandem with a powerful staking mechanism, separate from the Staking offered in partnership with Metabank, the SIMCAT Staking meant to reward early adopters of SIMCAT Tokens to encourage long-term holding. Staking is the process of locking up cryptocurrency holdings to support network operations, such as transaction validation, in exchange for rewards. Early buyers of $SIMCAT have an exclusive opportunity to stake their tokens before the public sale, unlocking dynamic annual percentage yield (APY) rewards while contributing to the stability and security of the ecosystem. By staking SIMCAT Tokens during the presale, you gain early access to dynamic rewards and benefit from the highest APYs, ensuring long-term loyalty and deeper involvement in the SIMCAT Wallet community.

7.1 How SIMCAT Staking works

Staking allows users to earn rewards by locking their tokens for a specific period, contributing to network security and liquidity. SIMCAT's staking system offers dynamic rewards, meaning the amount earned fluctuates based on the total number of stakers and each participant's contribution. The earlier and larger the stake, the greater the rewards.

A total of 7% of the SIMCAT Token supply is allocated to the rewards pool, ensuring sustainable tokenomics and long-term growth incentives for participants. Staking rewards are distributed proportionally, meaning each stakers earnings are directly related to their share in the total staked pool. The more a user stakes compared to others, the higher their potential rewards.

Dynamic rewards: SIMCAT staking rewards are dynamic, meaning they fluctuate based on the total number of stakers and each individual's contribution to the staking pool. The earlier you stake and the larger your share in the pool, the greater your rewards will be.

Rewards pool: A total of 7% of the SIMCAT Token supply is allocated for rewards. This ensures a healthy token economy and long-term incentives for participants while promoting sustainable growth for the project.

Proportional rewards: Staking rewards are distributed proportionally based on each holder's share in the total staked amount. The more you stake compared to other participants, the higher your potential rewards will be.

8. The Industry (global)

The cryptocurrency industry is experiencing significant developments across various sectors. Komainu, a crypto custody service provider established in 2018, is expanding its operations, particularly in Asia. The company recently acquired Propine Holdings in Singapore and is considering entering the Japanese market. Notably, Komainu raised $75 million in Series B funding entirely in bitcoin, marking a first in the industry. The company is also renewing its focus on the U.S. market, encouraged by President Donald Trump's pro-crypto stance, which has rejuvenated interest in the region.

In the realm of cryptocurrency investment products, Canary Capital Group has filed for an exchange-traded fund (ETF) linked to the spot price of Sui, a cryptocurrency from the Sui Network. This filing adds to the firm's total of six cryptocurrency ETF applications with the U.S. Securities and Exchange Commission (SEC).

The current administration's favorable outlook on cryptocurrency regulation has increased optimism for the approval of various cryptocurrency ETFs by the end of 2025. Regulatory changes include dropping enforcement actions against major cryptocurrency entities and reconsidering tougher custody rules.

On the trading front, Bitcoin has edged higher that $100,000; on the political scene the state of Texas exploring BTC for reserves; Coinbase Institutional's head of research suggests that a rally to new highs expected this year.

These developments underscore a dynamic period in the cryptocurrency industry, characterized by strategic expansions, evolving regulatory landscapes, and fluctuating market conditions.

8.1 New Projects

The global cryptocurrency market is witnessing rapid innovation with projects focusing on scalability, security, and mainstream adoption. Notable initiatives include:

- Solana Ecosystem Growth: Solana continues to attract high-performance dApps and DeFi platforms due to its low transaction fees and high throughput, making it ideal for $SIMCAT’s foundation.
- Wallet-Integrated Tokens: Tokens like Crypto.com’s $CRO and Trust Wallet Token ($TWT) demonstrate how wallet-native utility tokens can drive user engagement and ecosystem loyalty.
- DeFi 2.0 Protocols: Platforms integrating staking, lending, and governance in a single interface (e.g., Aave and Compound) showcase the potential for multi-utility tokens to dominate decentralized finance.

$SIMCAT builds on these advancements, combining wallet-native utility, tap-to-earn gamification, and integrated banking services to stand apart from isolated offerings in the market.

8.2 New Coins

Several emerging tokens align closely with $SIMCAT's vision:

- $BONK (Solana): Community-driven meme token demonstrating strong engagement on Solana.
- $PYTH (Pyth Network): A Solana-based oracle solution enabling low-latency financial data feeds for DeFi platforms.
- $JUP (Jupiter Exchange): A decentralized Solana exchange token showcasing successful DEX integration.

By leveraging Solana's rapidly growing ecosystem and interoperability with such projects, $SIMCAT is positioned to integrate seamlessly with next-generation DeFi and gaming solutions.

8.3 Governments supporting Crypto Currency exchange

Global regulatory attitudes toward crypto are shifting toward acceptance and structured frameworks.

- United States: Recent regulatory clarity under the pro-crypto stance of federal leadership, combined with growing ETF approvals, creates a favorable environment for blockchain-based businesses. SIMCAT adheres strictly to U.S. compliance standards, including KYC/AML.
- European Union (MiCA): The Markets in Crypto Assets (MiCA) framework offers a unified regulatory landscape across EU member states, supporting wallet services and exchange integration.
- Asia-Pacific: Regions such as Singapore and Hong Kong as well as Uzbekistan and Kazakstan have positioned themselves as crypto-friendly hubs through transparent licensing programs.

$SIMCAT's U.S.-based compliance-first approach ensures it is well-positioned for global expansion within these regulated and supportive jurisdictions.

9. Technical Architecture (Solana)

SIMCAT Token ($SIMCAT) is deployed on the Solana blockchain, chosen for its unmatched scalability, low fees, and energy efficiency.

- Transaction Speed: Solana processes up to 65,000 transactions per second (TPS), enabling fast wallet transfers, in-game rewards, and staking.

- Smart Contract Security: $SIMCAT utilizes Solana Program Library (SPL) tokens with audited smart contracts to ensure safe deployment.
- Cross-Chain Potential: While Solana is the core network, SIMCAT plans future integrations with cross-chain bridges for broader DeFi and exchange compatibility.

This technical foundation ensures $SIMCAT's infrastructure can support millions of users while remaining cost-effective and sustainable.

10. Legal and Compliance (USA-Based)

SIMCAT operates with the support of Crypto Engine LLC, a U.S.-based Mining Pool Software company, helping to reach full compliance with applicable federal and state regulations. Learn more about it here: **cepool.us**

- KYC/AML Protocols: All wallet, exchange, and staking functions integrate robust Know Your Customer (KYC) and Anti-Money Laundering (AML) processes.
- SEC and FinCEN Guidance: SIMCAT Token is structured as a utility token, avoiding characteristics of securities under the Howey Test while adhering to FinCEN reporting requirements.
- Data Privacy: All user data and authentication comply with U.S. and international standards, including GDPR compatibility for future EU expansion.

This compliance framework positions $SIMCAT as a legitimate, investor-ready project prepared for regulatory scrutiny.

11. Market Entry Plans

$SIMCAT's entry strategy leverages community engagement, gamified onboarding, and global partnerships to build rapid adoption and long-term sustainability.

1. Community Engagement via CryptoCat
   Our market entry begins with CryptoCat, a Telegram-based tap-to-earn game that introduces users to cryptocurrency concepts in an interactive and rewarding way. By integrating SIMCAT Token rewards directly into gameplay, we foster early engagement and incentivize participation in our ecosystem.

2. Content Channels for Growth
   $SIMCAT's rapidly growing Telegram community, YouTube, x.com and Instagram channels, serve as our uninterrupted outreach tools. Also the "tasks" in the game that earn additional rewards to the player for joining our communities and subscribe to our channels help immensely. We provide continues video reportage with tutorials, updates, and news to users, strengthening community trust and accelerating adoption.
3. Global Partnership Integration
   We are strategically connecting multiple products through partnerships that form the backbone of our ecosystem:
   - Crypto Engine (USA): Mining pool operator delivering regulated hash power solutions.
   - Crypto Mining (Central Asia): Large-scale mining farms supporting network infrastructure and liquidity.
   - Metabank (France): Blockchain banking franchise providing virtual cards, IBAN payment access, and fiat-crypto bridges.
   - Staking Platform (Regionally Patented): A proprietary staking mechanism offering dynamic APYs and long-term token utility.
   - Signal Bot (Regionally Patented): A Telegram-based market analysis bot delivering real-time trading signals and insights to users.

By merging gamified education, financial tools, and real-world utilities, $SIMCAT creates a holistic path from beginner engagement to advanced crypto adoption.

When We Enter

The SIMCAT project has been steadily developing since its inception:

- February 2023: Registration of intellectual property for our Staking platform and Signal bot.
- May 2025: Launch of CryptoCat v1 and deployment of the Crypto Mining Pool.
- June 2025: Release of CryptoCat v2, finalizing core gameplay and educational mechanics.
- July 2025: Public ICO offering for SIMCAT Token ($SIMCAT), granting early supporters pre-listing access.
- Early 2026: Integration of Metabank for blockchain banking and fiat on/off ramps.

- Mid-2026: Launch of the SIMCAT Wallet, consolidating wallet, staking, exchange, and payment functions.
- Early 2027: Completion of $SIMCAT's ecosystem, integrating all services into a unified Web3 platform.

Why We Enter

Our vision is to redefine how users interact with crypto by providing secure, accessible, and utility-driven solutions that merge entertainment with financial empowerment.

By leveraging robust technology and strategic partnerships across mining, banking, and DeFi, $SIMCAT bridges the gap between traditional finance and decentralized ecosystems. This approach not only accelerates adoption but also builds a foundation for a sustainable, community-driven financial network powered by the Solana blockchain.

$SIMCAT is uniquely positioned to transform the way users engage with digital assets-delivering education, rewards, and real-world utility through a seamless, gamified experience backed by a secure and scalable infrastructure.

12. Token Description

The token represents broad usability. It allows users to perform fast and easy global transfers and make payments with minimal fees. The primary purpose of the SIMCAT Token is to improve and simplify the use of banking and crypto applications while supporting the implementation of eco-friendly programs within the $SIMCAT ecosystem.

$SIMCAT will be issued as a Utility Token. To ensure market stability and provide continuous benefits to users who stake their tokens for extended periods, SIMCAT Utility Token will be supported by its own robust ecosystem. First and foremost, SIMCAT Token offers users a Web3-based crypto wallet designed for long-term use. The SIMCAT Wallet allows users to securely store their most trusted tokens and convert or swap them into stablecoins effortlessly. Additionally, SIMCAT Utility Token provides another major advantage-long-term sustainability. The token is designed to remain stable in future markets while supporting key ecosystem services such as SIMCAT Exchange, SIMCAT Wallet, SIMCAT Banking, SIMCAT Payment, and $SIMCAT Mining Pool. Through staking applications and associated fee structures, token holders will receive rewards in $SIMCAT, drawn from the ecosystem revenues generated by these platforms.

SIMCAT Token will be launched primarily on the Solana blockchain, with earlier consideration also given to Toncoin. Solana was selected due to its scalability, high transaction throughput, and low fees, making it one of the fastest-growing blockchains. In recent years, numerous successful tokens have been deployed on Solana, making it an ideal foundation for $SIMCAT.

Services available to SIMCAT Token users include:

- **SIMCAT Wallet:** A low-fee crypto wallet compatible with all major tokens, designed for secure storage and seamless transactions.
- **SIMCAT Exchange:** A trading platform for buying and selling tokens, enhanced with P2P functionality for direct crypto trading.
- **CryptoCat AirDrop:** A Web3-based Telegram airdrop where users can invite friends and earn $SIMCAT daily by mining through a simple tap-to-earn mechanism.
- **SIMCAT Staking:** Users can lock their SIMCAT Tokens for a set duration and receive bonus $SIMCAT rewards upon completion.
- **SIMCAT Payment:** Enables users to make online purchases using SIMCAT Tokens as a payment method, subject to platform rules.

All these services will be powered by custom smart contracts on the Solana blockchain, ensuring security, transparency, and efficiency across the entire $SIMCAT network.

13. Market Expansion

SIMCAT's market expansion focuses on scaling its ecosystem globally through strategic partnerships, compliance-driven operations, and targeted regional integrations. By leveraging its foundation on the Solana blockchain, SIMCAT will deliver high-speed, low-cost transactions while introducing innovative services such as regulated exchange trading in the U.S., government-backed payment utilities in Uzbekistan, and blockchain banking through Metabank in Europe. Combined with gamified user engagement via CryptoCat and mining-backed rewards from Crypto Engine, $SIMCAT is positioned to bridge the gap between emerging markets and mature crypto economies, creating a unified, accessible financial ecosystem for users worldwide.

13.2 Capital Investments

Capital raised through $SIMCAT's presale and token offerings will be strategically deployed:

- 40% – Product Development: Wallet, exchange, staking platform, and blockchain banking integrations.
- 25% – Marketing & User Acquisition: Global campaigns, influencer partnerships, and gamified onboarding.
- 15% – Liquidity Pools: Ensuring $SIMCAT stability across exchanges.
- 10% – Compliance & Legal: Licenses, audits, and U.S.-based legal infrastructure.
- 10% – Ecosystem Growth: Strategic partnerships, grants for dApp developers, and gaming expansions.

13.3 Projects

Key funded initiatives include:

- SIMCAT Wallet Expansion: Launching advanced features such as NFT storage, one-click DeFi access, and enhanced cross-chain compatibility to create a versatile Web3 wallet experience.
- CryptoCat Game Enhancements: Expanding the Telegram-based tap-to-earn game with additional levels, character skins, and educational modules to increase engagement and integrate deeper blockchain learning.
- DeFi Lending & Yield Integration: Introducing seamless staking and decentralized lending protocols built on Solana's DeFi ecosystem, enabling users to earn rewards and participate in on-chain financial services.
- U.S. Compliance-Ready Exchange: Developing a fully regulated P2P and spot trading platform featuring fiat on/off ramps, designed to meet U.S. compliance standards while maintaining decentralization.
- Crypto Engine Mining Pool: Operating a high-capacity 22 EH/s mining pool, distributing rewards in $SIMCAT Tokens and providing the mining pool participants with transparent earnings and real-time performance tracking.
- SIMCAT Solar: SIMCAT Solar Mining production, the world's first household-friendly mining solution that converts excess solar energy into $SIMCAT tokens. Our proprietary SIMCAT Solar Panels come with built-in, low-energy blockchain hardware that connects directly to the Crypto Engine Mining Pool. When a solar system sends surplus electricity back to the grid, owners don't just get paid by the utility-they also earn $SIMCAT rewards automatically, tracked in real time through their mining pool account.

- Utility Payments: Partnering with a new government-backed road assistance and monitoring initiative, offering citizens of Central Asian country exclusive discounts when paying with $SIMCAT

ROADMAP

2022-May
The Partnership Formation
Partnership with GTS is finalized
Financial plan is approved
The Project is funded

2025-August
Game Launch
Test Airdrop game
Upgrade New 1.0 Basic Game
Start Referral System

2025-September
Game V1.5
Open a Special Card
Donate Toncoin to Boost Mining
Charging Staking Boost

2025-October
Game V2.0
Upgrade new 2.0 Basic Game
New Technology Cards
Start Project ICO News printing

2025-November
New Game: Market Quest
New game version Added
CryptoCat Authenticator
Web 3 pre listing App

2025-December
ICO Listing
Audit by CertiK & Token Creation
ICO Launch & Fundraising
Token Listing & Post-ICO Growth

2026- January
$SIMCAT Token Listing
Launch staking and liquidity rewards
Transition toward decentralized governance (DAO)
Marketing maintenance, community AMAs, and exchange PR

2026-February
SIMCAT eco system
Start Mining Pool and Solo Mining SIMCAT AI
Listing crypto market and SIMCAT Authenticator
Release news about SIMCAT eco system

2026-March
Airdrop
Smart Contract & Backend Setup
Claiming & Distribution
Post-Airdrop Retention

2026-May
SIMCAT.Auth
Wallet (SIMCAT.Auth)
Start Wallet staking
Start Wallet exchange Swap

2026-July
Crypto Exchange
Exchange (SIMCAT.Auth)
Seamless and Profitable P2P Crypto Exchange
Star Exchange Spot Trading

2026-September
Payment Gateway
SIMCAT Payment Gateway
Customer security
Seller security

2026-November
Blockchain Banking

Blockchain Banking
Start connection SIMCAT Exchange
Start connection SIMCAT Mobile Wallet

2026-December
Market Expansion
Expand to Central Asia
Start MTL Licensing
USA FiAt Support

Year-2027
TBD

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.