

# EGO BLOCKCHAIN

A decentralized physical infrastructure network (DePIN) for storage, wireless coverage and compute, secured by post-quantum cryptography

Artit Muhaxhiri

April 16, 2023

[www.egoblockchain.com](http://www.egoblockchain.com)

**Abstract:** I know that you might question the need to introduce another layer one blockchain and add another cryptocurrency to a market already crowded with 22,932 options. However, it's important to understand that each blockchain has unique features and capabilities that can address specific challenges and demands, and the introduction of new blockchains and cryptocurrencies can pave the way for innovation and new possibilities in the industry. Our proposed solution aims to address two major problems in the industry: data storage and cryptocurrencies.

The current centralized data storage systems are vulnerable to hacking and data breaches, which can compromise sensitive information. On the other hand, Bitcoin has faced criticism for its energy-intensive Proof of Work mechanisms and the potential centralization of infrastructure. Proof of Work (PoW) mechanisms used in Bitcoin result in the energy waste involved in validating proofs, which presents no other utility. With PoW, miners benefit from economies of scale, which can lead to infrastructure centralization and work against the goal of decentralization. With Proof of Stake (PoS), centralization of infrastructure can occur out of convenience, as stakers choose to run their node on centralized cloud infrastructure, weakening the network's resilience to attacks.

To address these issues we are building a decentralized physical infrastructure network — a DePIN — in which ordinary computers, and optionally purpose-built EGO 5G devices, contribute storage, wireless coverage, retrieval and compute to a shared network and are paid for what they measurably provide. Capacity is spread worldwide across independently owned machines rather than concentrated in a handful of data centres.

Our proposed solution addresses the criticisms of blockchains and cloud services while offering improved security, a more robust ecosystem, reduced costs, passive income for storage providers, and privacy features.

## 1. Introduction

Many people think that Web3 is a completely new technology that operates independently of Web1 and Web2. The truth is that Web3 is built on top of the existing infrastructure provided by Web1 and Web2. This means that even if the dApp's functionality is decentralized, the frontend or user interface can still be removed or deleted, which would make the dApp inaccessible to users.

Decentralized networks have been gaining momentum in recent years as a way to provide more security, privacy, and control over data. However, the transition from Web2 to Web3 has been slow due to the lack of sufficient decentralized infrastructure, especially outside the realm of DeFi. The setup of decentralized nodes is often complicated, time-consuming, and costly, which can discourage developers and end-users from adopting decentralized applications.

We are developing a new blockchain with a main focus on decentralized storage and smart contract functionality to solve these issues. The blockchain will utilize a proof-of-spacetime and proof-of-coverage consensus mechanism to ensure security and reliability.

With new 5G micro servers to provide fast and reliable infrastructure for decentralized applications. We will enable users to interact with dApps seamlessly, without experiencing lag or delays. Furthermore, we will work in conjunction with IPFS, a protocol for distributed storage and sharing of files. This will enable developers to create decentralized applications that rely on decentralized storage, ensuring data redundancy and increasing fault tolerance. By leveraging decentralized storage, smart contracts, and fast network infrastructure, Ego Blockchain aims to solve the issue of removing the frontend of a dApp. This will help to create a more robust and scalable decentralized network that can encourage the development and adoption of decentralized applications beyond DeFi. With the elimination of infrastructure costs for developers and end-users, we hope to encourage the creation of more open-source dApps, leading to a diverse set of applications and mainstream adoption of the decentralized web. The potential benefits of decentralized networks are clear, including increased security, privacy, and control over data. We aim to provide a viable solution to the challenges that have slowed the adoption of Web3, making decentralized applications more accessible and user-friendly.

## 2. Decentralized storage and 5G wireless network

The Decentralized Storage Network using micro 5G servers is a distributed system that allows users to store, access and retrieve data in a decentralized and secure manner. The network enable efficient and reliable data storage and retrieval, utilizing micro 5G servers as nodes in the network.

The network will be modelled using the following equations:

$D = \{d1, d2, d3, ..., dn\}$  - set of n micro 5g servers P

$= \{p1, p2, p3, ..., pm\}$  - set of m data shards

$C = \{c1, c2, c3, ..., ck\}$  - set of k clients

In the [Figure 1] each data shard is encrypted and stored across multiple micro 5G servers, ensuring data redundancy and increasing fault tolerance. The number of servers that each shard is stored on can be determined by the replication factor r.

We utilize a sharding algorithm to partition the data into smaller, more manageable shards. Each shard is assigned a unique identifier, which is used to retrieve the shard from the network. The sharding algorithm will be represented using the following equation:

$$shard\_id = hash(data) \% m$$

Where  $hash(data)$  is the hash value of the data being stored, and  $m$  is the total number of shards.

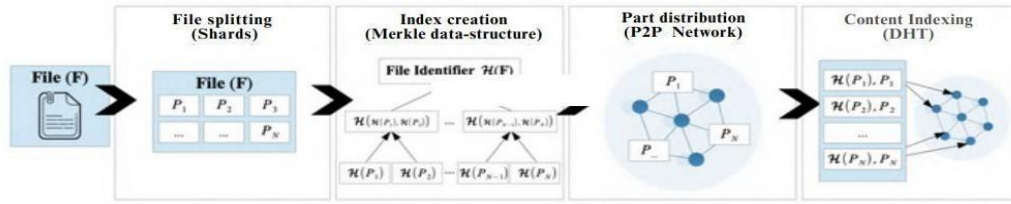
Clients can access the data by sending a request to the network. The request is forwarded to the micro 5G servers storing the required data shards, which then send the requested data back to the client.

The network will be modelled using the following equation:

$$request = \{shard\_id1, shard\_id2, ..., shard\_idn\}$$

Where  $shard\_id1$  is the unique identifier of the  $i$ th shard required to fulfil the client's request. We use consensus mechanism, such as *proof-of-spacetime*, to ensure the security and reliability of the data storage and retrieval process.

The equation is:  $L = H(x) \bmod N$  where  $L$  is the location where the data is stored,  $x$  is the unique identifier of the data,  $H()$  is a hash function, and  $N$  is the total number of servers in the network. Using micro 5G servers as nodes, and employing encryption/decryption, sharding, and consensus mechanisms we ensure efficient and reliable data storage and retrieval.



**Figure 1.** Block scheme of the decentralized storage protocol for splitting a file  $F$  into  $N$  pieces  $P_n$  stored along with the hash  $H(P_n)$  in the peers.

### 3. Quantum resistant key pairs

Quantum-resistant algorithms are a new generation of cryptographic algorithms designed to be secure against attacks by quantum computers. Quantum computers have the potential to break many of the traditional cryptographic algorithms that are currently in use, such as RSA and Elliptic Curve Cryptography (ECC), by using Shor's algorithm to factor large numbers and solve the discrete logarithm problem.

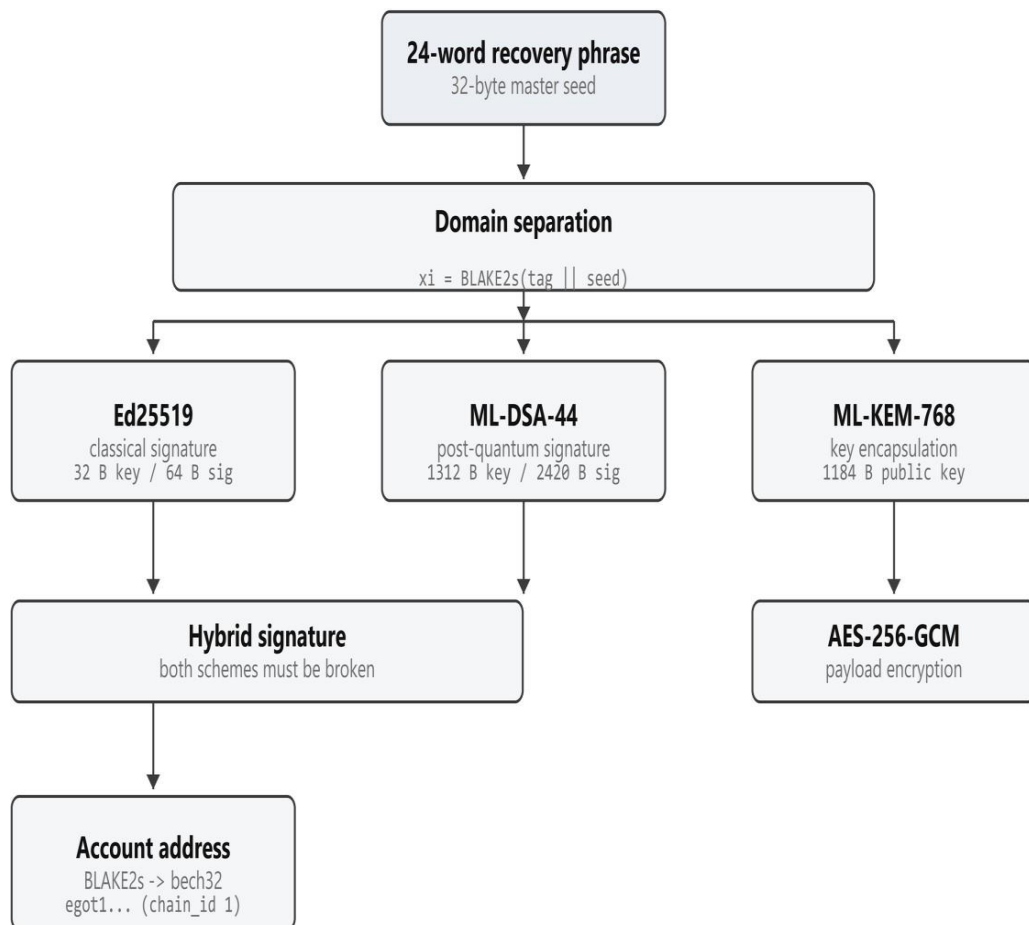
To address this threat, NIST ran a multi-year standardisation process and in 2024 published the first post-quantum standards. Ego implements those standards directly: ML-DSA-44 for signatures (FIPS 204, from the CRYSTALS-Dilithium family) and ML-KEM-768 for key encapsulation (FIPS 203, from CRYSTALS-Kyber).

Both rest on the hardness of problems over structured lattices, specifically *Module Learning With Errors*, which is believed to resist attack by both classical and quantum computers. Unlike isogeny-based schemes such as *SIKE* — a NIST candidate that was broken by a classical attack in 2022 and withdrawn — lattice constructions have so far withstood sustained cryptanalysis.

The cost of this security is size. An ML-DSA-44 signature is 2,420 bytes against 64 for Ed25519, and its public key is 1,312 bytes against 32 — a signature roughly thirty-eight times larger, paid on every transaction. Ego accepts that cost from genesis rather than deferring a migration that would later require a hard fork over live balances.

Ego signs hybrid: every account holds an Ed25519 keypair alongside its ML-DSA-44 keypair, so an attacker must defeat both a classical and a post-quantum scheme rather than either one. A third scheme, SLH-DSA (SPHINCS+, FIPS 205), is also available; being hash-based, its security rests on entirely different assumptions from the lattice problems underlying Dilithium and Kyber, and it would survive a structural break in lattice cryptography.

maps  $E$  to  $E'$  and  $\Phi'$  maps  $E'$  back to  $E$ .



Every key derives deterministically from one 32-byte seed. The recovery phrase alone restores the entire account.



- The received signature is verified against the sender's published public key. If the signature is valid, the message has not been altered in transit.
- To decrypt, the recipient derives the same shared secret using its private key and the sender's public key, then decrypts with that secret and the nonce sent alongside the ciphertext. Decryption fails if the authentication tag does not match.
  - The binary message is converted back into text format, which produces the decrypted message: " *This is a secret message*".

**Note:** This whitepaper represents a continuous work in progress. We will endeavor to keep this document current with the latest development progress. As a result of the ongoing and iterative nature of our development process, the resulting code and implementation is likely to differ from what is represented in this paper. We invite the interested reader to peruse our GitHub repo at <https://github.com/egoblockchain> as we continue to opensource various components of the system over time.

## Shielded Transactions

Ego supports shielded transfers for users who do not want their activity profiled on a public ledger. A transfer can be marked private when it is sent, and any transfer of 50,000 EGOC or more is shielded automatically, so a large holder is not exposed simply by transacting.

When a transaction is shielded, the sender and recipient addresses are withheld from the block explorer and from the public transaction feed, and the entry is labelled as privacy protected. Address history search and holder rankings are not offered at all, since those are the tools most often used to profile individual users. Aggregate supply distribution remains published, so the network's overall economics stay auditable without exposing individual balances.

Shielding at this stage is enforced at the ledger interface rather than by cryptographic concealment: amounts and the transaction graph are still committed on-chain, and a participant operating their own node can read them. Full cryptographic privacy, in which sender, recipient and amount are hidden from every observer including node operators, is planned and will be documented when it ships.

## 5. Ego Protocol

### • Transport Layer

*Libp2p* will be used as the transport layer protocol for *5G-CP*, providing a secure and efficient way to transfer data between nodes in our 5G network. In addition, *libp2p*'s peer discovery and routing modules will improve the performance of the 5G network by enabling nodes to easily find and connect with other nodes, and to efficiently route data between nodes. With 5G-CP, data will be securely and efficiently transferred between the nodes ensuring redundant storage, prevention of deletion or tampering, and accessibility.

## • Consensus Layer

**Proof-of-Coverage (PoC)** is important to ensure that a particular node or device has a certain level of coverage within a network. The PoC mechanism in *5G-CP* uses 5G waves to validate that Hotspots are providing legitimate wireless coverage. The algorithm uses signal strength and signal-to-noise ratio (SNR) to determine the coverage area of a particular node or device. The formula for SNR is:

$$\text{SNR} = (\text{Signal Power}) / (\text{Noise Power})$$

where Signal Power is the power of the signal transmitted by the device and Noise Power is the power of the noise in the system. The SNR value is an indication of the quality of the wireless signal received by the node or device.

To ensure that there are enough devices in a network to provide adequate coverage, the PoC mechanism requires devices to periodically transmit a signal indicating their presence and coverage area. The PoC mechanism will be enhanced with the use of AI, which use machine learning algorithms to analyze the coverage data collected by the witness nodes and validate the legitimacy of the coverage provided by the transmitting node. The AI will also detect and prevent any attempts to fake or manipulate coverage data, ensuring the integrity of the network.

Let  $S$  be the set of witness nodes in the network, and let  $N$  be the set of all nodes in the network. For each node  $n$  in  $N$ , let  $C(n)$  be the coverage area of node  $n$  as determined by the PoC mechanism. Let  $W(s, n)$  be a binary variable indicating whether witness node  $s$  has received a signal from node  $n$ .

$$f(C(n), C(s))$$

Then, the AI will use the following formula to determine the legitimacy of node  $n$ 's coverage area:

where  $f$  is a function that compares the coverage areas of node  $n$  and witness node  $s$  and returns a value between 0 and 1 indicating the similarity of the two coverage areas. This function will be based on various metrics such as distance, signal strength, SNR, etc.

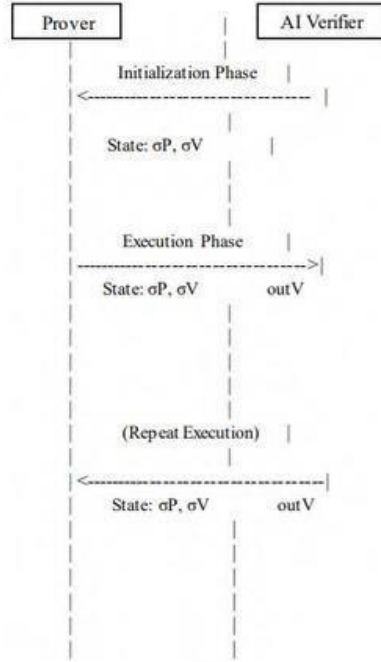
The formula calculates the legitimacy of node  $n$ 's coverage area by taking the average of the binary variables  $W(s, n)$  across all witness nodes  $s$  in the network. The binary variables indicate whether each witness node has received a signal from node  $n$ , and the average represents the proportion of witness nodes that have detected node  $n$ 's signal.

The legitimacy value is then weighted by the similarity between node  $n$ 's coverage area and each witness node's coverage area, as determined by the  $f$  function. This ensures that nodes with similar coverage areas have a greater influence on the legitimacy calculation than nodes with dissimilar coverage areas.

**Proof of Spacetime** combined with PoC it validates nodes based on the time, space and coverage they dedicate to the network. Each node in the network is required to dedicate a certain amount of storage space and computing power to the network, which is then used to validate transactions and create new blocks.

The AI observes the nodes and monitors their performance, ensuring that they are operating as expected and dedicating the required resources to the network.

Nodes are expected to submit proof of their spacetime resources on a regular basis to the network. The AI supervisor then validates this proof and provides feedback to the network on the legitimacy of the proof submitted by each node. This feedback is used to adjust the reputation of each node, with nodes that submit valid proof being rewarded with a higher reputation and nodes that submit invalid proof being penalized.



The Prover is a EGO 5G device that participates in the network and performs storage operations. The AI Verifier is responsible for validating the Prover's performance.

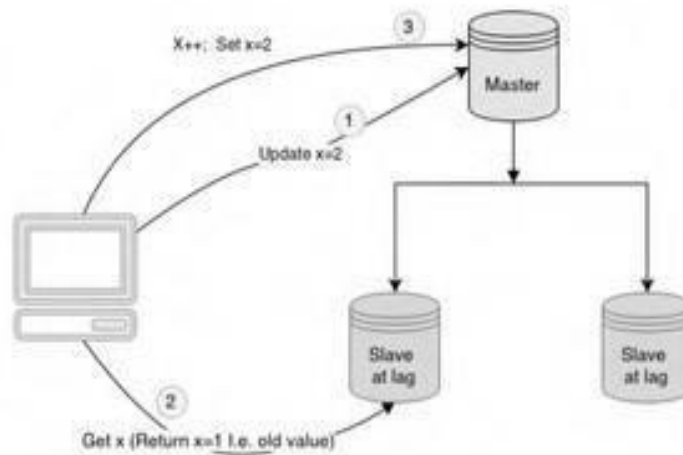
During the Initialization Phase, the Prover and AI Verifier establish a shared state, denoted as  $\sigma P$  and  $\sigma V$ , respectively.

In the Execution Phase, the Prover performs storage operations and generates an output, denoted as  $outV$ . The AI Verifier receives the output and updates its state based on the output and its current state. The updated state is denoted as  $\sigma V$ .

The Execution Phase is repeated multiple times to ensure that the Prover's performance is consistent and reliable. The Prover generates an output each time, which is validated by the AI Verifier.

By using the Proof of Spacetime algorithm with AI as a supervisor, we ensure that nodes are operating as expected and dedicating the required time and space to the network. This helps to maintain the security and reliability of the blockchain, while also ensuring that the nodes in the network are operating at an optimal level.

**Proof of Replication (PoRep)** is a consensus mechanism used to certify that a node has replicated a piece of data correctly. We utilize PoRep to ensure that each node in the network has an exact copy of the same data. We use a master node and two slave nodes to replicate the data, and each node must prove that it has stored the data correctly by providing a proof that it has replicated the data accurately. This ensures the security and integrity of the data on the network and prevents any malicious actors from tampering with it. By using PoRep, we can guarantee that the data stored on our network is accurate, secure, and accessible to all nodes in the network.



Storage is paid for per period rather than by burning tokens at upload. A client's allocation is escrowed and released to providers as they continue to prove they hold the data, so cost tracks storage actually delivered.

**Consensus is HotStuff-style Byzantine Fault Tolerance.** Registered validators vote in rounds, a block finalises on a two-thirds quorum, and leadership rotates deterministically on each view change so no single node can stall the chain. An unstaked validator's vote does not count toward quorum, which is how the network resists Sybil attacks.

Reward scoring uses the following inputs:

- Measured storage held and proven by the node over the period
- Verified wireless coverage attested at the node's location
- Retrieval served on request, measured in bytes delivered
- Consensus participation, counted only for staked validators. Deterministic Reward

Scoring combines these into a single score:

$$DRS = (w_{poc} \times coverage) + (w_{post} \times storage)$$

where:

- $w_{poc} = 0.6$  — the weight given to proven coverage
- $w_{post} = 0.4$  — the weight given to proven storage
- A node must reach a minimum score of 0.5 to be eligible for block production.

Because every input is measured and every weight is fixed in consensus, each node computes an identical score for its peers, and payouts can be validated rather than trusted.

## Application Layer

Application layer will leverage AI technology to create smart contracts in response to natural language inputs provided by users. At present, we are in the research phase, and we have yet to determine whether we will develop our own AI model, which will be trained on a vast dataset of sample smart contracts and programming languages, or utilize third-party AI providers that can comprehend user intent and generate the appropriate smart contract code.

The smart contract that are generated, will be executed by the EGO virtual machine, which will ensure that the code runs correctly on the blockchain. The virtual machine will be designed to be more user-friendly and accessible, with features such as a simpler development environment, a more intuitive programming language, and built-in debugging tools. This will enable developers and users to create and interact with smart contracts more easily and efficiently.

## 6. Tokenomics and Staking Rewards

The Tokenomics of the EGO blockchain has been carefully crafted to ensure a fair and sustainable ecosystem. One of the standout features of our platform is that there are no transaction fees or fees for deploying smart contracts. Instead, nodes are rewarded with newly created coins from new blocks.

To encourage long-term participation, staking rewards increase with the length of the lock period. Locking for 90 days adds two percentage points to the base rate, 180 days adds five, and 365 days or longer adds ten. Rewards accrue deterministically from the staked principal and the lock period, so every node computes an identical figure when validating an unstake.

Staking pays a base annual percentage rate of 12.5%, rising to a maximum of 22.5% with a lock of 365 days or longer. The same rate applies to every staker; there is no separate tier for node operators. A validator's own stake serves a different purpose: it gates whether that validator's vote counts toward consensus quorum, which is how the network resists Sybil attacks.

Staking rewards are funded from a dedicated allocation of 140,000,000 EGOC set aside at genesis for that purpose. There is no transaction tax on buying or selling EGOC, and no portion of a trade is diverted to liquidity or to stakers.

The EGOC token has a maximum supply of 1,000,000,000 coins, allocated at genesis across five pools. The largest, 300,000,000 coins, forms the node rewards pool, released continuously to participants who contribute storage, wireless coverage, retrieval capacity and consensus, with payouts determined by Deterministic Reward Scoring.

A further 210,000,000 coins are released through block emissions, at 0.08322 EGOC per block, halving roughly every four years across thirty eras — a schedule spanning 120 years. 200,000,000 coins form the ecosystem pool, which funds the pre-sale, grants, developer incentives, partnerships and exchange liquidity. 150,000,000 coins are held by the foundation for the team, advisors and long-term development, vesting linearly over forty-eight months from genesis and enforced on-chain: transactions exceeding the vested amount are rejected at block-write time. The remaining 140,000,000 coins fund staking rewards.

Transaction fees are paid to the people running the network rather than to the company: 60% goes to the block producer and 40% returns to the node rewards pool, extending how long storage, coverage and retrieval contributions can be paid. Taken together, 51% of all supply is never sold — it is earned through contribution and block production rather than allocated in advance.

EGOC is the native coin of the Ego blockchain. It is not an ERC-20 token and does not exist on Ethereum or any other network; balances, transfers and staking are settled directly by Ego's own consensus. Every allocation described above is minted at the genesis block and is verifiable on-chain.

## 7. Block Details and Transaction

Our block design includes several key features that enhance the performance and reliability of the platform. Each block contains a timestamp, a hash of the previous block, and a hash function using *blake2s*. The transactions are stored in a Merkle tree structure within the block. To ensure the integrity of each block and prevent fraudulent activity, we will use a machine learning-based signature that serves as the supervisor. This will allow us to automatically detect and reject any invalid blocks, as well as identify potential security threats and take action to prevent them.

Our blockchain produces a new block every 0.1 seconds in micro-slots, giving fast and reliable transaction processing. Block size and throughput scale with the capacity that participating nodes contribute. The following lines explain how our system works:

- The elected leader for the current height assembles pending transactions into a block candidate.
  - ▶ The candidate block is broadcast to the network, and nodes use their stored data to solve the PoSt challenge.
  - ▶ Miners that solve the challenge broadcast their proof to the network.
- Validators verify the candidate and vote; the block finalises once a two-thirds quorum is reached.
  - ▶ The selected nodes store the new block, and the process repeats.

By using this approach, we achieve a block time of 0.1 seconds.

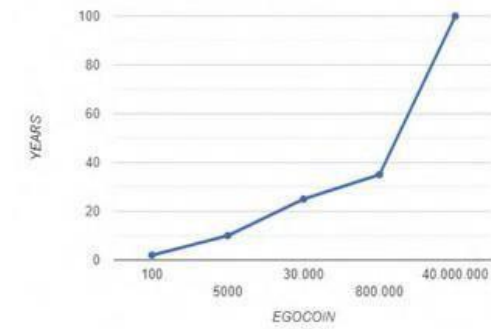
Here's also an example of how a transaction is processed and added to a block:

- Alice initiates a transaction to send 10 EGO to Bob.
- The network verifies Alice's signature and that her balance covers the transfer and fee.
  - ▶ The transaction is then broadcast to the network.
- The transaction enters the mempool, sharded deterministically by sender.
  - ▶ The selected nodes store the transaction in the candidate block.
- The leader for the next height includes it in a block candidate and broadcasts it for voting.
  - ▶ Miners use their stored data to solve the PoSt challenge, and the best performing nodes are selected to store the new block.
  - ▶ The selected nodes store the new block, which includes Alice's transaction, and the process repeats.

By using this approach, we can ensure fast and secure transaction processing with a high degree of scalability and efficiency.

## 8. Block Reward Calculation

The Block Reward will be calculated by taking the block reward as a function of the total number of coins to be revealed, the total number of blocks produced, the number of years since the start of the network, the decay constant, and the number of transactions in the current block. The block reward decreases 50% every 2 years due to the decay constant and is also reduced based on the number of transactions in the block.



This incentivizes nodes to include as many transactions as possible in their blocks to earn higher rewards. By including the transactions per block ( $T/B$ ) and the decay constant  $\lambda$ , we also determine how quickly the performance of a node decays over time. For the calculation we use this method, let:

- $R$  = current block reward
- $T$  = number of transactions in the block
- $B$  = maximum number of transactions per block (assumed to be a constant value)
- $D$  = total number of coins to be released through block emissions (210,000,000 EGOC)
- $Y$  = number of years since the start of the network
- $N$  = total number of blocks produced in  $Y$  years (315,360,000 blocks per year at our 0.1-second block time)

Then, the formula for calculating the block reward can be:

Which in conclusion the block reward is calculated:

$$R = \left( \frac{D}{N} \right) \times (1 - e^{(-\lambda Y)}) \times \left( 1 - \left( \frac{T}{B} \right) \right)$$

Where:

- $\lambda$  is the decay constant that determines how quickly the block reward decreases over time
- $e$  is the mathematical constant approximately equal to 2.71828

In the early days of the network, when the number of transactions per block is low, the  $T/B$  value would be small, which means that the second part of the formula  $(1 - (T/B))$  would be close to 1, resulting in a higher block reward.

As the number of transactions per block increases over time, the  $T/B$  value would increase, causing the second part of the formula to decrease, resulting in a lower block reward. This would incentivize nodes to continue providing their services to the network, as they would be rewarded more for their work in the early days when the network is still growing.

## 9. Nodes

Any ordinary computer can run a node. Ego Desktop is available for Windows, macOS and Linux; installing it and allocating disk space is enough to join the network and begin earning. The forthcoming Ego 5G device is a purpose-built, low-power node for operators who want dedicated hardware, not a requirement for participation.

To join, download Ego Desktop, create a wallet and choose how much storage to contribute.

The node connects over any internet link, discovers peers automatically and begins storing encrypted shards. We know that we have to deal with different malicious nodes which could exhibit a variety of

characteristics, such as attempting to broadcast fraudulent transactions or attempting to take control of the network through a 51% attack. In the Ego blockchain, we will handle malicious nodes through a combination of consensus mechanisms such as proof of spacetime, proof of coverage, and proof of AI, as well as by implementing measures such as IP address banning and node reputation systems. To solve the 51% attack, we use a reward system that decreases by 10% when there are two or more devices in one square meter. This discourages users from clustering their devices together and gives more incentive for users to spread out their devices across a wider area, making it more difficult for any one entity to control 51% of the network.

As for Sybil attacks that act of creating multiple identities or nodes to gain control of a network or system, we have implemented several mechanisms to handle it, such as:

- ▶ Proof of Spacetime: This mechanism ensures that each node in the network is physically located in a unique place. Each EGO 5G device has a unique GPS location, and the network uses this information to ensure that there are only two nodes per square meter.
- ▶ Proof of Coverage: makes sure that each node is distributed evenly across the network. Every EGO 5G device provides coverage to a specific area, and the network uses this information to ensure that there is no overlapping coverage.
- Stake-gated voting: a validator's vote counts toward quorum only if that validator is staked, so influence over consensus carries a capital cost that scales with any attempt to flood the network with identities.
- ▶ Monitoring network behaviour: The AI constantly monitor the network for any suspicious activity or behaviour that may indicate a Sybil attack. If AI detect any such activity, will take appropriate action to prevent it from causing any harm to the network.

In addition, we use Erlang programming language to develop our blockchain platform, which is known for its high fault tolerance and ability to handle large-scale distributed systems. This allows our network to withstand potential attacks and maintain its integrity even in the face of malicious actors.

By implementing these mechanisms, we are confident that EGO blockchain is secure against several attacks.

## 10. DAO

Decentralized Autonomous Organization, is a concept that allows for decentralized decision making and control. In Ego Blockchain, we will use a DAO to split the profits from selling the Ego 5G devices. This ensures that the decision-making power is distributed among the members of the community, and no single entity or individual has undue control over the network. We will operate truly decentralized by solving problems through DAO votings. The community members will be able to vote on important decisions related to the development and growth of the network, such as changes to the protocol, the allocation of resources, and the development of new features. In addition, we will use smart contracts to choose the tender winner of doing a task. This ensures transparency and fairness in the selection process, as the winner will be determined based on pre-defined criteria encoded in the smart contract. Every profit and sale from the hardware will be transparently recorded and made available on our website. This ensures that the community members are aware of the financial activities of the network, and are aware how the profits are distributed. In order to ensure fair and transparent decision-making within our ecosystem, we will implement two types of voting and the results it will be averaged to determine the final outcome. The first type of voting requires staking, which means that participants must hold a certain amount of EGO in order to vote on proposals. The second type of voting is based on passing a knowledge test about the particular subject being voted on. This allows participants to prove their expertise in the area and ensures that only those with a good understanding of the topic are able to vote on it. This will help to prevent uninformed decisions that could negatively impact our ecosystem.

Once both types of voting have taken place, we will calculate an average between the two results to determine the final outcome of the vote. This provides that both stakers and knowledgeable participants have an equal say in the decision-making process, and helps to assure that decisions are made in the best interest of our ecosystem.

Here's an example of how the voting process will work with the two different DAO votings:

► Staking voting: In this type of voting, individuals would stake a certain amount of EGO to participate in the decision-making process.

The amount staked would be proportional to the voting power of each individual, meaning that those who stake more would have a greater say in the outcome of the vote. The formula for staking-based voting will be:

$$\text{Total Voting Power} = \Sigma (\text{Individual Stake} / \text{Total Staked})$$

For example, if there were 100 people participating in the vote and the total amount staked was 10,000 tokens, and an individual staked 500 tokens, their voting power would be:

$$(500/10,000) \times 100 = 5\% \text{ of the total voting power}$$

► Knowledge-based voting: In this type of voting, individuals would need to pass a test to demonstrate their understanding of the particular subject that is being voted on. Once they pass the test, they would be granted a certain amount of voting power. The formula for knowledge-based voting will be:

$$\text{Voting Power} = (\text{Test Score} / \text{Max Test Score}) \times \text{Base Voting Power}$$

For example, if the base voting power was 10 and an individual scored 80% on the knowledge test with a maximum possible score of 100, their voting power would be:

$$(80/100) \times 10 = 8$$

► Combining the results: To get the final outcome of the vote, we will take an average of the results from both the staking and knowledge-based voting systems.

For example, if the staking-based voting gave a total voting power of 60% and the knowledge-based voting gave a total voting power of 40%, the final voting power will be:

$$\text{Final Voting Power} = (\text{Staking Voting Power} + \text{Knowledge Voting Power}) / 2$$

$$\text{Final Voting Power} = (60 + 40) / 2 = 50$$

In this example, the final voting power is 50%, meaning that the decision would be made based on the majority vote.

## 11. Conclusion

Our goal is to create a truly decentralized ecosystem that provides secure and reliable services to users. One of our primary objectives is to provide decentralized cloud storage that is both secure and cost-effective. With our blockchain technology, users will be able to store and access their data without worrying about security breaches or data loss. We will also provide a decentralized website that is secure, fast, and reliable. Another key feature of our ecosystem is offline transactions and offline data storage. We will create a system that allows users to make transactions and store data even when they are offline. This is particularly useful in areas with poor internet connectivity or during natural disasters when internet access may be limited. We are committed to provide a fee-less environment for our users. We will not charge any transaction fees for sending or receiving egocoins. Additionally, there are also no fees associated with deploying a smart contract on our platform.

Our staking rate starts at 12.5% APR and rises to 22.5% with a 365-day lock, funded from the dedicated 140,000,000 EGOC staking allocation.

Our blockchain infrastructure is designed to be easy to use for both developers and non-developers. We believe that blockchain technology should be accessible to everyone, and we have designed our ecosystem with this principle in mind.

The EGO 5G device will be created to allow for 5G internet sharing, enabling users to earn passive income by sharing their excess bandwidth with others. This will create a truly decentralized network of wireless networks, providing a more reliable and cost-effective alternative to traditional internet service providers.

With our AI technology, everyone will be able to write smart contracts and create dApps without needing to have any coding experience. This will democratize the blockchain space and allow for more people to participate in the development of decentralized applications.

Finally, we believe that anyone should be able to generate passive income with EGO 5G devices, which store data and provide wireless networks. By leveraging our blockchain technology, we aim to provide a more decentralized and equitable distribution of wealth.

## References

- [1] FIPS 204: Module-Lattice-Based Digital Signature Standard, NIST, August 2024.  
<https://csrc.nist.gov/pubs/fips/204/final>
- [2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
- [3] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System. 2014.
- [4] Protocol Labs. Technical Report: Proof-of-Replication. 2017.
- [5] The Qogecoin Authors. qogecoin, 2021. <https://github.com/qogecoin/qogecoin>, accessed May 10, 2022.
- [6] Vitalik Buterin. Ethereum, 2014
- [7] Tal Moran, Ilan Orlov, " Simple Proofs of Space-Time and Rational Proofs of Storage " pages 4-23.
- [8] P. Labs. Filecoin: A decentralized storage network, 2017. URL: <https://filecoin.io/filecoin.pdf>.
- [9] Helium. Proof of Coverage. <https://docs.helium.com/blockchain/proof-of-coverage/> 2013
- [10] Jonathan Rodriguez. Fundamentals of 5G Mobile Networks " [https://pcc-fet.com/common/library/books/50/6998\\_\[Jonathan\\_Rodriguez\]\\_Fundamentals\\_of\\_5G\\_Mobile\\_Net\(b-ok.org\).pdf](https://pcc-fet.com/common/library/books/50/6998_[Jonathan_Rodriguez]_Fundamentals_of_5G_Mobile_Net(b-ok.org).pdf)" 2015.
- [11] Phillip Rogaway. "Nonce-Based Symmetric Encryption".  
<https://www.cs.ucdavis.edu/~rogaway/papers/nonce.pdf> pages 4-11.