Hermez

Hermez
White Paper

9 October 2020

Contents

Executive summary

Hermez is a **zk-rollup** which allows for scaling payments and token transfers on top of the Ethereum public blockchain. It is designed with high-frequency tokens like ETH, DAI, Tether, and wBTC in mind.

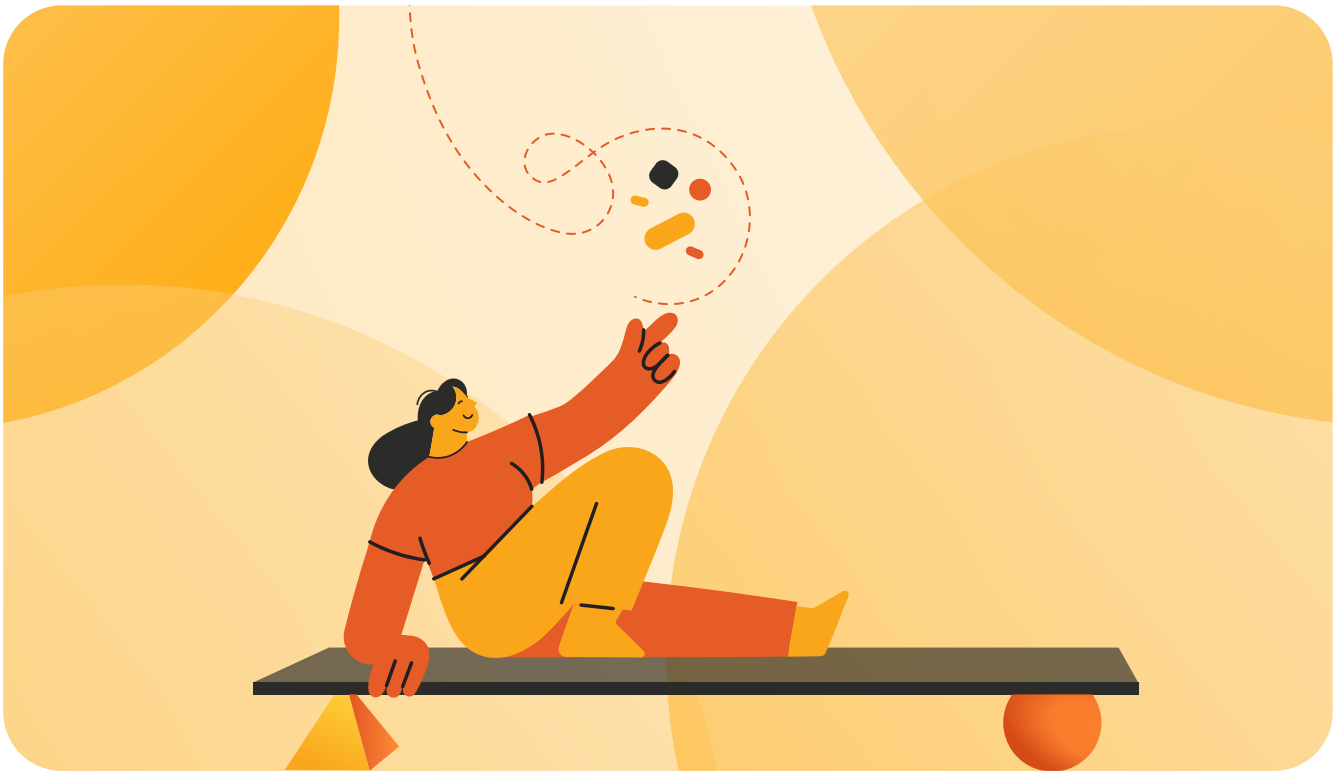
Hermez uses the Ethereum public blockchain for data storage instead of computation, i.e. it handles data availability on-chain but does computation offchain. In addition, by utilising zero-knowledge proofs, it attaches an easily verifiable on-chain proof that the off-chain computations have been carried out correctly.

Since both the data and zero-knowledge proof are available on-chain, Hermez relies on the same security assumptions as Ethereum. This means Hermez is as censorship-resistant as Ethereum.

One of the most important things about Hermez, is the way in which it decides who the next rollup batch creator should be. Hermez integrates an auction where everyone intending to become a coordinator – the batch creator in the Hermez ecosystem - bids the number of tokens they are willing to donate in order to obtain the right to create the next batch.

The winning bid is the highest amount of tokens. And this address is assigned the right to create the next batch.

In the Hermez Network this mechanism is referred as **proof-of-donation** because asignificant fraction of this bid is donated to the protocols and social services that run on top of Ethereum.



Background

During the last year, it has become clear that rollups will be the dominant scaling paradigm on the Ethereum public blockchain for at least the next couple of years: with this in mind, iden3 has developed and is preparing to launch Hermez, a zkrollup focused on scaling payments and token transfers on the Ethereum public blockchain.

Why focusing on transfers? It turns out that more than 50% of transactions on the Ethereum network are transfers, and a large percent of these are deposits and withdrawals from exchanges. Demand could be reduced by a significant amount if exchanges started using rollups, or (in the ideal case) even agreed to meet on the same rollup. In addition to significantly reducing transaction costs for users, this could have the added benefit of greatly reducing gas prices, and freeing up the base chain for more complex contracts.

Zero-knowledge rollups

A zk-rollup, such as Hermez, is a layer 2 construction which uses the Ethereum blockchain for data storage instead of computation.

All funds are held by a smart contract on the main-chain. For every batch of transactions, a zk-SNARK is generated off-chain. This zk-SNARK proves the validity of every transaction in the batch which means it is not necessary to rely on the Ethereum main-chain to verify each signature transaction.

The significance of this is that it allows verification to be carried out in constant time regardless of the number of transactions. This ability to verify proofs both efficiently and in constant time is at the heart of all zk-rollups.

In addition to this, all transaction data is published cheaply on-chain, without signatures—under call data. Since the data is published on-chain, there are no data availability problems that have plagued other L2 solutions such as Plasma.

Importantly, anyone can reconstruct the current state and history from this onchain data. This prevents censorship and avoids the centralization of coordinators (rollup batch producers)—since anyone can build the state tree from scratch (and therefore become a coordinator).

Why the need for zk-rollups?

Trust-minimised blockchain scaling mechanisms are sorely needed if blockchain applications are ever to achieve mass adoption.

For context, the Ethereum network can handle approximately 15 transactions per second (tps), while the Visa network averages around 2,000 tps.

Zero-knowledge rollups

As outlined in an earlier Iden3 post, zk-rollups have the potential to increase the Ethereum network's maximum tps by two orders of magnitude, making it comparable to the Visa network's average.

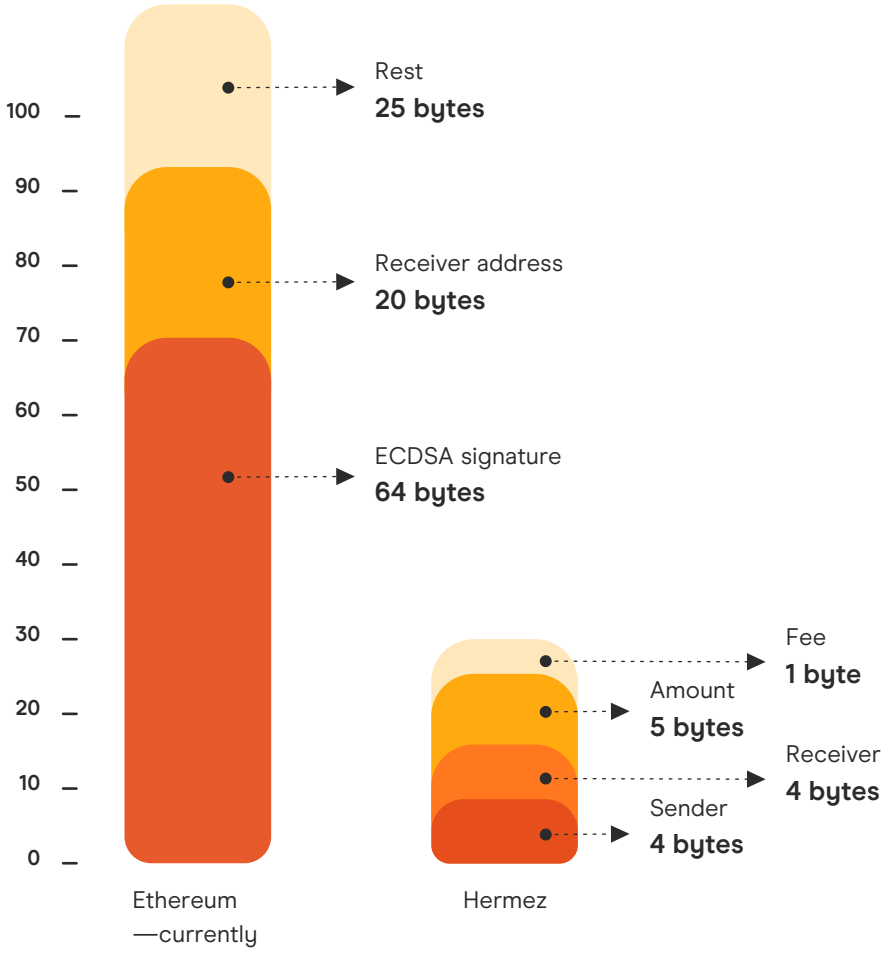
How is 2000 tps possible?

Blockchain scalability is improved by compressing each transaction to ~10 bytes: instead of including signatures on-chain, we send a zk-SNARK which proves that 1000's of signature verifications and other transaction validation checks have been correctly carried out off-chain.

Since signatures make up a large percentage of transaction costs (gas), in practice zk-rollup has the effect of significantly reducing the average cost per transaction.

This allows Hermez to fit more transactions per batch, which results in a greater overall throughput.

Bytes breakdown: vanilla Ethereum transaction (109+ bytes) vs zk-rollup transaction (14 bytes)



Model and actors

Hermez network

Hermez provides the decentralized components in the form of smart contracts and open source tools to enable a new ecosystem of actors to participate in the network.

Users

Network users will be provided with easy-to-use interfaces to register their L1 Ethereum addresses as Hermez L2 accounts. They will then be able to deposit and withdraw their funds, ETH, ERC-20 compatible tokens, into or out of these L2 accounts.

Initially, users will access the Hermez Network through an interface based on a non-custodial individually owned wallet solution that relies initially on Metamask for the management of private keys.

Through this interface, users will be able to:

- Register their Ethereum L1 address into the Hermez network and obtain an internal address - one for each type of token they wish to deposit;
- Deposit L1 tokens into their Hermez Network addresses with a simple transaction;
- Transfer tokens between Hermez addresses fast and for very low fees;
- Transfer tokens from Hermez Network addresses back to their chosen L1 addresses.

Hermez provides protection mechanisms (enforced in the smart contract) which guarantee that all tokens locked in the L2 solution can always be recovered by the users, even in the unlikely event that the auction-winning coordinator is malicious — in other words, stealing, censoring or blocking transactions is impossible.

The Hermez network do not provide custodial or exchange services in any way. Hermez only and exclusively provides a L2 scaling solution for faster and cheaper Ethereum tokens transfers.

Model and actors

Coordinators

Coordinators are Hermez network's version of block producers. This means they are the ones who effectively run the network by computing the zero-knowledge proof of validity of the transactions made by the users.

Coordinators use systems infrastructure to sync with the Hermez network, receive transaction requests from users, and process transaction requests in order to build rollup batches, which Merkle root is then saved (together with a zk-proof of correctness and the data necessary to reconstruct the full Merkle tree) on Ethereum.

Third-Party Volume aggregators

Third-Party exchanges and other volume aggregators will have specific modules for such participants to connect to the network and exploit its full potential.

Hermez will provide a special feature of atomic transactions, which implements a link between transactions that need to be executed together, and it's very useful for token swaps.

All volume aggregators will be able to access the decentralized platform through API integration.

Proof-of-Donation

One of the most important things about Hermez is the way it decides who the next batch creator should be. We call this mechanism, **proof-of-donation.**

A decentralized auction is conducted automatically, (more information in the "Auction model and efficiency" section) and in which everyone intending to act as a Coordinator bids the amount of tokens they're willing to place in order to obtain the right to create the next batch.

The winning bid is the highest amount of tokens. And this address is assigned the right to create the next batch.

This mechanism is referred to as proof-of-donation because a significant fraction of this bid is contributed as a donation to the protocols and services that run on top of Ethereum.

Why is this important? Scaling and sustainability go hand-in-hand. Innovations in scalability are a rare opportunity to realign incentives around the community and the public goods they provide.

In a nutshell, if it is not possible to figure out how to make blockchain infrastructures self-sustaining, then the question of how to scale them becomes irrelevant.

Hermez Network token

Hermez has its own network token: **HEZ**.

HEZ is an ERC-20 utility token used to place bids in the Coordinators auction. Every time a rollup batch is created, a fraction of HEZ tokens placed during the proof-of-donation auction will be burned, and therefore permanently removed.

Read more in the "Token Economy" section.

Auction model and efficiency

The right to forge is structured in time slots, which are defined to be 10 minutes long.

In order for the coordinators to obtain the right to create rollup batches during a 10 minutes slot, they will need to participate in a decentralized permission-less auction.

The idea is to incentivise efficiency as coordinators are in need to include as many transactions as possible in each time slot in order to compensate for their bidding costs and operative expenses.

This efficiency is key to the performance of the Hermez network in a completely decentralized environment.

Bids in the auction must be placed using the HEZ utility token. The HEZ utility token price and value is not pre-determined or pegged to a reference asset.

To prevent bidders from buying up all the slots in one go, nobody will be able to bid on a specific slot more than one month in advance. And the auction will be closed two time slots before the time of creating the slot.

Auction model and efficiency

The auction will be structured in a series of six time slots to cover one hour (%0-5), with 10 HEZ as the initial minimal bidding price for all of them.

The first bid in each time slot must be over the minimal bidding price in order to be accepted as valid. Thereafter, any bid placed in the auction should outbid the previous bid by at least 10%.

All bids will be processed by the auction smart contract, and all the HEZ tokens placed will be used as follows:

- 30% will be burned (permanently removed) by using a “burn” function;
- 40% will be automatically and permanently transferred to a donations account. These donations will be initially sent to Gitcon quadratic funding grants but with the future-proof ability to donate also to other quadratic funding matching pools as they become available;
- 30% will be allocated as Hermez Network usage incentives, compensating active engagement and network adoption, e.g. rewarding transaction and rewarding the holding of specific tokens in Hermez L2 addresses, instead of on L1 Ethereum addresses.

The minimum bidding amount for each slot in an auction series will be decided by the network governance (see section "Hermez governance"), and it will be possible to change it dynamically, affecting future, even already open, auctions.

Also, governance will be able to implement the effective decentralization of the network by locking the price of specific series of slots (0-5) in the auction to 0 HEZ and so don't requiring any minimal bid, being this an irreversible configuration.

Decentralization and governance

Bootstrapping centralization points

The objective of the Hermez network is to follow a gradual path towards becoming fully decentralized in order to provide stability and security to the network.

Some of the technologies developed and implemented are experimental and there is a learning curve that needs to be managed as this kind of high throughput network has never been deployed before.

Boot coordinator

This initial element is a special seed coordinator which will be assigned to create batches of user transactions by default, until an alternative permissionless operator will place a bid in an attempt to obtain the right to run the network in a future slot of time.

This “Boot coordinator” has a maximum cap to the value that it can be rewarded for creating a slot, equal to the initial minimum bidding price: 10 HEZ.

All so collected rewards will be manually converted into HEZ once per month, with only the maximum cap value retained, while any excess will be processed and 15 allocated with the same proportions described before in the "Proof-of-donation" section.

Decentra-lization and governance

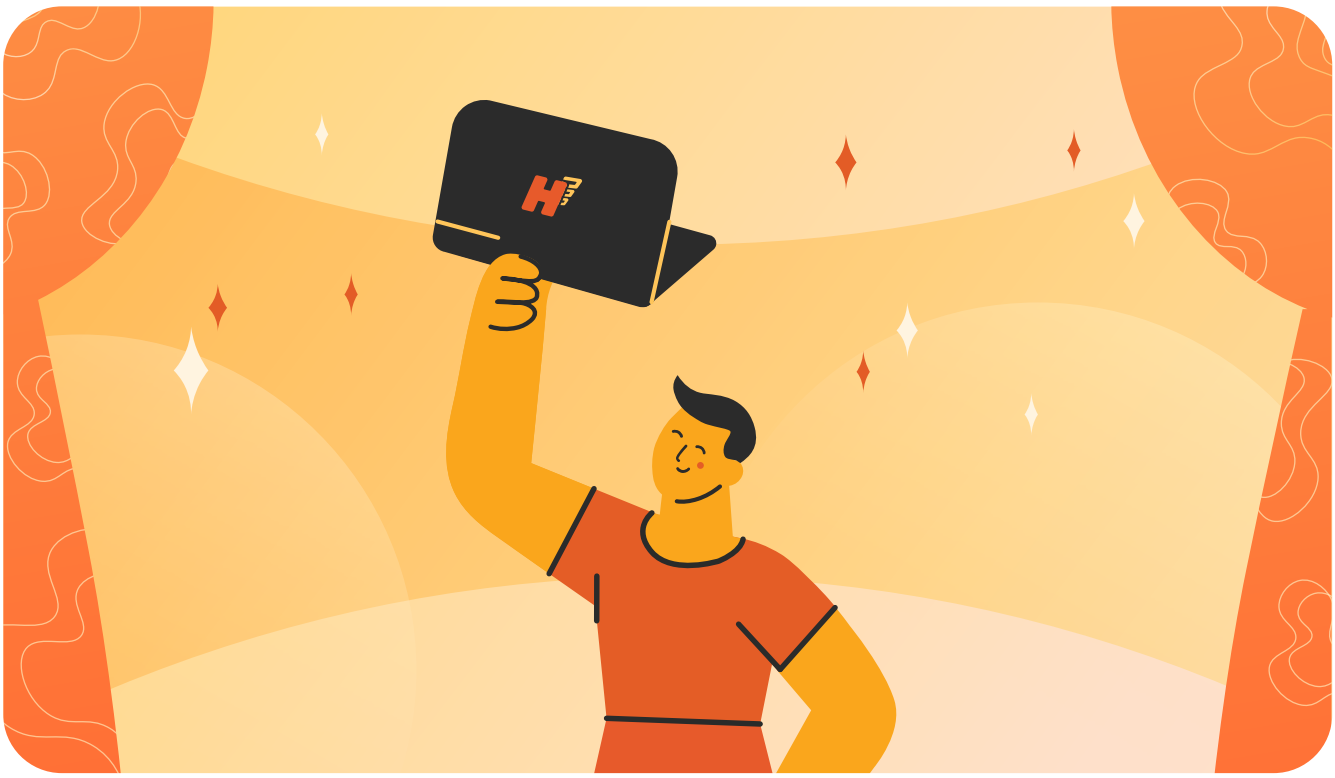
The maximum cap value of the Boot coordinator, in order to compensate for any volatility of the token and to further promote decentralization, will be reduced monthly following a mathematical model that will allow for the gradual entrance of alternative coordinators, thus reducing any barrier of entry and conversely increasing decentralization as the transactions volume processed by Hermez grows, proportionally with the estimated reward amount for each batch.

The governance will be allowed to make the decision for the Boot Coordinator to disappear completely once the network will reach a big enough transaction volume and a number of competing operators and coordinators. If that will not happen then eventually the maximum cap reward would become be so low that the coordinator will be rendered irrelevant.

Hermez Governance

The Hermez network community intends to follow a strategy of “Governance minimization”. This model is intended to be initially a bootstrap governance mechanism to adjust and manage some network parameters mainly for security and stability purposes until the network reaches enough a degree of maturity to become fully decentralized. At that stage the initial bootstrap Governance model will no longer be necessary and will eventually disappear.

The network will start with a governance based on a Community Council formed by some distributed and reputed Ethereum community members. This council will delegate some specific and limited network parameters adjustments into a reduced Bootstrap Council, which is non custodial, in order to be more operationally effective in the initial phase.



Decentra-lization and governance

In case that the protocol or the network needs for further and continued specific parameters governance after the initial bootstrap period (est. 1-2 years), a HermezDAO based on Aragon will be deployed and the weight of the voting will be based on HEZ staking calculated from snapshots.

Some decisions that the initial Community Council will be able to make will be:

- Governance and policies related changes
- Upgrade, maintenance and updates of the smart contracts code and/or zero knowledge circuits.

The bootstrap Council will be enabled to change some of the initial parameters of the Hermez smart contracts such as:

- Minimum bidding amount for the auction slots series;
- Days the auction is open for and slots before closing auction;
- Value of the outbidding variable;
- Boot Coordinator maximum cap reward reduction.

Security

Hermez is a Layer2 solution running on top of Ethereum 1.0. This means that the security of Hermez relies on the security assumptions and guarantees provided by Ethereum.

On top of Ethereum blockchain, Hermez will add another layer of security borrowed from Zcash. Following their work, Hermez integrates a zk-SNARK prover/verifier module to validate in constant time the execution of a series of transactions. The specific zk-SNARK that is used is Groth16. Although it is quite a recent protocol, it has been widely used and tested by Zcash team of researchers and it is currently considered mature enough to be used in production.

At this time, Ethereum precompiled smart contracts only support BN254 elliptic curve operations for zk-SNARK proofs validation. For this reason, Hermez uses this curve for generating and validating proofs and Baby Jubjub for implementing elliptic curve cryptography inside circuits.

In place of BN254, that offers 100 bits of security, Zcash uses BLS12-381, with 128 bits of security [see here]. Hermez will likely migrate to BLS12-381 curve as soon as it is available for Ethereum. The EIP that implements BLS12-381 curve was already approved and the migration is very likely to happen by the next planned Berlin Hard Fork. This change will improve the security leveland also substitute Baby Jubjub for Jubjub.

Multi-party Computation for the Trusted Setup

The proving and verification keys of the zk-SNARK protocol requires the generation of some random values that need to be eliminated. This elimination process is a crucial step: if these values are ever exposed, the security of the whole scheme is compromised.

Security

To construct the setting, Hermez uses a Multi-party computation (MPC) ceremony that allows multiple independent parties to collaboratively construct the parameters (also called the trusted setup). With MPC, it is enough that one single participant deletes its secret counterpart of the contribution in order to keep the whole scheme secure.

The construction of the trusted setup has two phases: a general MPC ceremony that is valid for any circuit (also known as powers of tau ceremony), and a second phase (phase 2) that is constructed for each specific circuit. Anyone can contribute with their randomness to the MPC ceremonies and typically, before getting the final parameters, a random beacon is applied.

To contribute to the robustness of the setup, Hermez implemented an independent snarkjs module for computing and validating the MPC ceremonies. The software is compatible with current powers of tau, and it allows one to see the list of contributions of a given setup, to import a response and export a challenge of the ceremony (see Hermez' contribution), to run random beacon on a round, and also to check if the whole process has been correctly computed.

Implementing Cryptography inside a Circuit

Hermez makes use of two main cryptographic primitives: a signature and a hash function.

- The signature schema is the Edwards Digital Signature Algorithm (EdDSA) on Baby Jubjub (after the migration, it will use EdDSA on Jubjub). This protocol was implemented making use of the circuit language circom and following the circuit design of Zcash.
- The hash function used is Poseidon, a similar hash to MiMC but with a mixing layer. This function is quite new but it has been extendedly examined by many cryptographers and researchers.

Security

Neither MiMC nor Poseidon have yet been broken, and there are already some important projects that rely on them, like TornadoCash (MiMC) and Semaphore (Poseidon). So, Poseidon can be considered to be secure enough and the work is based on this assumption.

Assumptions (in short):

- Hermez inherits the security assumptions of Ethereum.
- it relies on Groth16 assumptions (p.e. knowledge of exponent assumption).
- it considers at least one participant contributing to the trusted setup MPC is honest.
- it assumes Baby Jubjub curve satisfies security standards (shown here)
- it assumes Poseidon hash function is collision and preimage resistant.
- it relies on circom and snarkjs software security assumptions.

Massive Migrations (Future work)

To achieve a robust ecosystem of rollups, it is important to enable migrations between different rollups and other L2 applications.

To this end, together with the Ethereum community and other researchers from different rollup solutions, some members of the Hermez decentralized community are working on the standardization and compatibility between these technologies. It is possible to follow this line of research here.

Hermez Token Economy

As mentioned in the Hermez Network Token section above, Hermez integrates HEZ token.

The Hermez Network Token (HEZ) is the token that acts as the economic lifeblood of the Hermez network.

Hermez Tokens Initial Team Vesting Schedule

A form of vesting is important for maintaining key founders, initial development team members and active community individuals aligned with the long-term success of the Hermez Network in terms of adoption and usage, and to show the community at large that the project will be consistent and trust-worthy.

All free token allocations will be subject to individual vesting requirements, most being more detailed and articulated than laid out in this section, which is meant to give only an high-level overview.

When tokens are initially assigned, specific private token vesting agreements will be drafted to guarantee continued work on the Hermez Network or the accomplishment of certain milestones/ metrics, but at the protocol-level, each token free allocation will overall follow one of these two broad vesting tiers:

- **Tier 1**: 5% of tokens unlocked initially, then after a 6-month cliff, 0.104% of the total amount released every day for ~2.5 years. All tokens will be unlocked after 3 years.

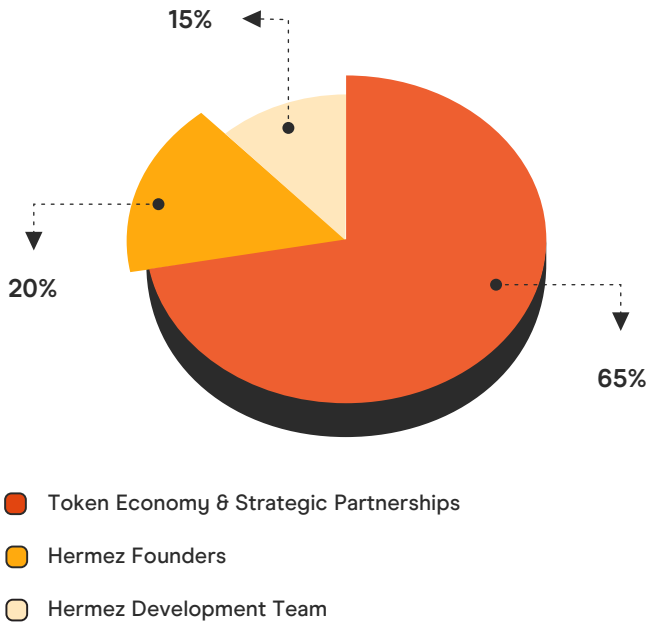
Hermez Token Economy

- **Tier 2**: 10% of tokens unlocked initially, then after a 6-month cliff, 0.164% of the total amount released every day for 1.5 years. All tokens will be unlocked after 2 years.

Hermez Network Token (HEZ) Allocation

Total Supply: 100 million, 8,25 million initial circulating supply.

- 65% -Token Economy & Strategic Partnerships: 65 million HEZ — 9.5% Tier 1 Vesting and 27% Tier 2 Vesting
- 20% - Hermez Founders: 20 million HEZ - 100% Tier 1 Vesting
- 15% - Hermez Development Team: 15 million HEZ - 66.6% Tier 1 Vesting



Token Economy

Rollups are novel networks that can possibly present a different community than traditional blockchains. Hermez recognizes this and is not willing to risk the future of the Network on an uninformed or rushed token economic design.

HEZ is used to bid for slots to become a coordinator and portions are donated, burned, and used to incentivize active Network usage and engagement. This is the only economic design built into the core protocol from the start.

Hermez Token Economy

Because the tokens are not sold, but freely allocated to the initial team and community members with the vesting conditions highlighted above, the Governance might decide to setup liquidity pools in permissionless DEXes and, potentially, a few centralized Exchanges as well, so to allow for the broader community to also participate and become coordinators, further enhancing and growing organically the decentralization aspect of the whole project.

The Governance and the initial development team will at the same time focus on ensuring that the launch of the Hermez network is technically sound. Once the Governance is satisfied that the network is operating as expected, it might sponsor a 'Hermez Token Economy Hackathon" or a similar open call, inviting the community at large to collaborate with the leading token engineering experts in the space to potentially propose different economic designs for the Hermez ecosystem that can also account for broad compliance considerations.

The best designs will then be reviewed, modeled, and eventually implemented to ensure the long-term success of the Hermez Network. This allotment of tokens will be initially controlled by the Governance and some of the initial supply will be kept as reserves to be released, as needed and with a majority decision, to a legal entity additionally set up to represent the Hermez project if there are critical issues that can only be addressed in this way.

Strategic partnerships

In order to encourage exchanges, DApps, and the general Ethereum community to foster adoption of the Hermez network, the Governance might allocate some tokens to important broad ecosystem partners that share its values and are going to be actively engaged in the project.

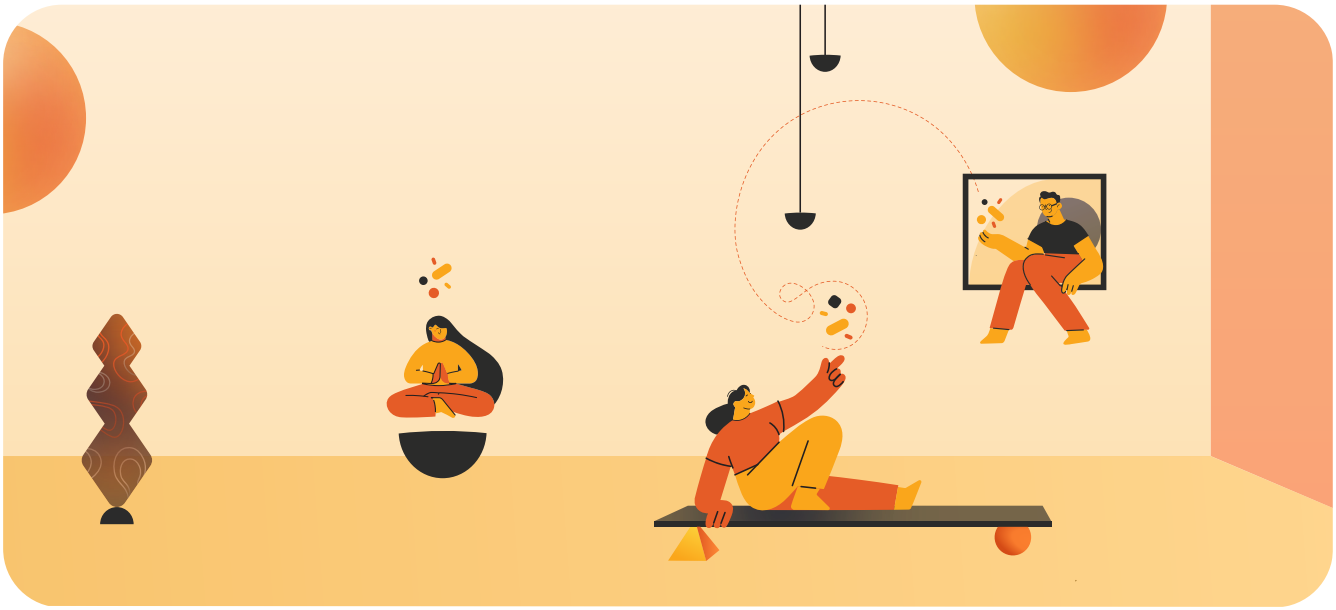
Hermez Token Economy

Founders

These are the initial core contributors who have worked to bring Hermez to life since iden3 started experimenting with rollups in early 2019. They are uniquely positioned to help bootstrap the network and ensure the eventual full decentralization and strategic operational exit to the community, progressively delegating their mentoring and support functions, but always remaining actively engaged.

Development Team

As Hermez is a fully open-source and community-driven project, it is fundamental to ensure the technical contributors and the development team members have a long-term interest in the future adoption of the Hermez Protocol. The tokens allocated to this part of our community will be used to ensure the core developers that originally built the bulk of the Network are incentivized to continue supporting, upgrading, updating and maintaining it. The Governance might choose to also use a portion of the token supply for bounties, audits, and further enhancements to the network, in particular for security and stability.



Hermez' decentralized network original developer team

Chami An
Eduardo Antuña
Cristina Barbero
Jordi Baylina
Marta Bellés
Arnau Bennassar
Arnau Cube
Alberto Elias
Elías García
Griff Green
Raúl J.
Pol Lanski
Jesús Ligero
Antoni Martin
Carlos Matallana
Miroslav Milenkovic
Rafal Nazarkiewicz
Jonathan Pycroft
Toni Ramirez
David Ruiz
Eduard Sanou
David Schwartz
Laia Soler

Legal disclaimer and notes

The decentralized Hermez Protocol, including but not limited to the overall project, network, smart contracts, circuits and, in general, software ("Hermez") is not a Financial, Money transmitting or Payment Service of any kind and in any Jurisdiction. Any Financial or Payment Services terminology used in this Whitepaper, on the Website or on any parts of Hermez is intended only as a basic reference, without any effective or legal meaning of the same terms in a regulated and/or traditional financial environment. Hermez tokens HEZ are strictly utility tokens in any jurisdiction and are not and can not be considered as security or otherwise regulated tokens of any kind nor are in any way akin to e-money and/or fiat or asset backed stablecoins, whether global or limited in scope. HEZ were and are not offered, sold or placed to the general public or to accredited sophisticated investors and/or entities with an ICO, IEO or any other form of token sale, with or without purpose of developing Hermez and the tokens are immediately usable within Hermez. The Hermez users, founders, developers and other governance related roles and/or HEZ token holders do not own or control Hermez, but simply contribute to its development, maintenance and security in a fully open, community driven and decentralized way. This Whitepaper is not a contract or a contractual agreement of any kind, nor a prospectus and/or an invitation or offer to invest in Hermez or acquire or use its tokens in any way. Any prospective or actual user of Hermez declares to have received appropriate technical, administrative and legal advice before and after reading this Whitepaper, the Hermez website and using any part of Hermez (including its tokens) and accepts that there is an inherent high risk in acquiring in any way or using any kind of blockchain and/or crypto token, platform, software, interface and fully discharge from any non-criminal liability any of the persons or entities mentioned here above or within this Whitepaper or on the Hermez Website for any kind of damage suffered, including total loss. The HEZ Token is explicitly not intended to be offered, sold, given and/or used in any way, directly or indirectly, to and by Citizens or Residents of the U.S.A.

visit **hermez.io**