

Building the *human* layer of the internet.

How Kin Identity proves that people are real and unique, keeps who they are private, and shares the value of the network with the people who build it.

KIN ID Live on iOS and Android	LANGUAGES 19 from the first screen	\$KIN SUPPLY 1.5 billion, fixed
TO THE COMMUNITY 70% mining and rewards	CHAIN BNB Smart Chain (planned)	TEAM SHARE 2.5%, locked 5 years

Abstract

The internet can no longer tell people apart from machines. Kin Identity is building the layer that can: proof that someone is a real, unique person, and nothing more.

AI can now write, talk and look like a person. Bots fill comment sections, fake accounts decide what trends, and the image puzzles that once kept machines out are solved by machines in seconds. Every app is left with the same impossible job: work out who is real, without asking people to give up who they are.

Kin Identity answers that with one idea: **one person, one account, private by default**. A Kin identity proves that its owner is a real and unique human. It does not reveal their name, face, email or history to anyone they meet or any app they use.

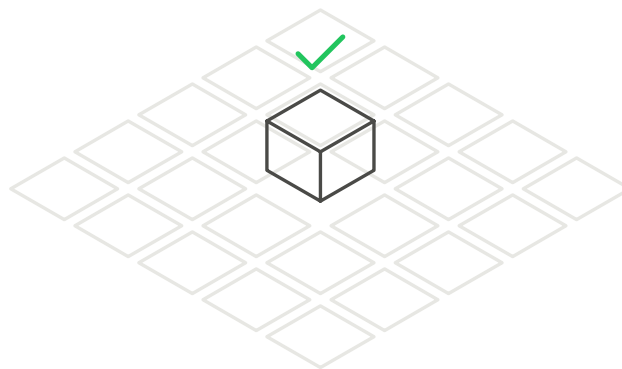


Figure 1. One person stands out from many accounts.

What we are building

- **Kin ID**, the app for real people, live on iOS and Android in 19 languages. It is where a Kin identity is created and where people meet, chat and show up every day.
- **Proof of human**, the private checks behind every Kin identity: a real device, a live person, and one account per person.
- **Kin OAuth**, a sign in button that lets any app know its users are real and unique, without collecting who they are.

- **Kin Pass**, a one tap replacement for the "I'm not a robot" puzzles that AI now solves.
- **\$KIN**, the reward of the human network: a fixed supply of 1.5 billion, of which 70% goes to the people who mine and show up.

Why now

In 2025, bots made up more than half of all web traffic for the first time, and AI solved the image puzzles meant to stop them. The cases in [The problem](#) show what that already costs people and businesses. The internet needs a human layer, and it needs it to be private.

How this paper is organised

The first part explains the problem, our approach and how it compares with the alternatives. The second describes each product. The third covers \$KIN in detail: supply, mining, invites, the airdrop and listings. The last part sets out our commitments on privacy, how Kin makes money, how the community takes part, and the risks.

Important \$KIN is a community reward. It is not an investment, and nobody can promise what it will be worth. Plans in this paper, including any token launch, airdrop or exchange listing, depend on legal approvals and partners, and may change or not happen. See [Risks and legal notice](#).

Contents

INTRODUCTION

01 The problem

Why the internet can no longer tell who is real, and why asking for more personal data makes it worse.

02 Our approach

The human layer of the internet: one person, one account, private by default, and a fair share for the people who build it.

03 Alternatives compared

How the usual ways of telling people from bots compare with Kin, on strength, privacy, effort and inclusion.

PRODUCTS

04 Kin ID

The app for real people, where a Kin identity is created and where people meet, chat and show up every day.

05 Proof of human

How Kin confirms that every account is one real, unique person, without collecting who they are.

06 Kin OAuth

Proof of human for every app. One tap tells an app that a user is real and unique, and nothing else.

07 Kin Pass

The robot check robots can't pass. One tap replaces image puzzles, with no tracking.

\$KIN

08 \$KIN at a glance

The reward of the human network. A fixed supply of 1.5 billion, 70% of it for the people who mine and show up.

09 Supply and allocation

How the 1.5 billion \$KIN are split into four shares, each with a hard cap.

10 Mining and rewards

How mining speed is set, how halvings work, and the daily rewards in Kin ID.

11 Invites and teams

Inviting pays in three ways, and none of it is taken from your friends.

12 Keeping it fair

How Kin stops bot farms, multiple accounts and reward abuse, and how real people can appeal.

13 Mining phase, airdrop and listings

How in app \$KIN becomes a BEP-20 token on BNB Smart Chain, who can claim it, and how listings are planned.

COMPANY

14 Roadmap

From launch to 2028, quarter by quarter.

COMMITMENT

15 Privacy and security

What Kin collects, what it never collects, and how accounts and data are protected.

16 Business model

How Kin Identity makes money, and why it doesn't depend on selling data or \$KIN.

17 Community and governance

How the people who use Kin shape it.

18 Risks and legal notice

The risks of \$KIN and Kin's plans, and what this paper is and isn't.

APPENDIX

19 Frequently asked questions

Short answers to the questions people ask most about Kin and \$KIN.

20 Glossary

Terms used in this whitepaper.

21 References

Sources for the facts and cases in this whitepaper.

22 Version history

Changes to this whitepaper over time.

The problem

IN SHORT

Machines now pass as people online, the robot checks that kept them out are broken, and asking for more personal data only creates more to leak. Apps need a small, private answer: is this a real, unique person?

The internet was built on a quiet assumption: that behind every account there is a person. That assumption no longer holds.

Machines now pass as people

Language models write replies that read like a friend's advice. Voice and video models copy real faces and voices. A single operator can run thousands of accounts that post, like, follow and argue around the clock. Ask whether a reply was written by a person and, more and more often, there is no way to tell.

The cost is trust. When you cannot tell who is real, you start to doubt everyone: the review that convinced you, the account that agreed with you, the stranger who was kind.

The old defences have fallen

For two decades, websites kept bots out with puzzles: blurry letters, traffic lights, crosswalks. Today, image models solve those puzzles as well as people do, and often faster. The puzzles still slow down real people, especially people with low vision or slow connections, while barely slowing down machines.

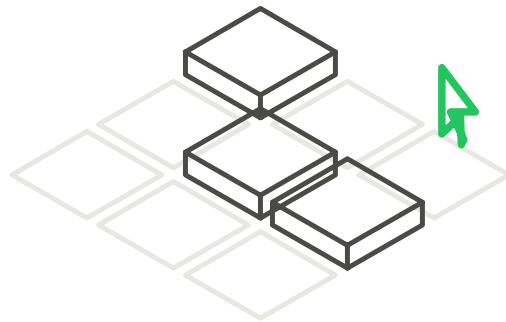


Figure 2. The old robot check: a grid of pictures, solved by a bot.

Some newer checks quietly watch how visitors move and browse to guess whether they are human. That keeps some bots out, but it is tracking by another name.

More personal data is not the answer

The usual fix is to ask for more: a phone number, an ID document, a selfie stored on a server. Each of these creates something new to leak, sell or misuse, and each excludes the billions of people who do not want to, or cannot, hand them over.

The question most apps actually need answered is much smaller: **is this a real person, and is it the only account they have here?** Today there is no simple, private way to ask it.

It's already happening

These are not predictions. Each of these happened in the last two years.

Bots now outnumber people online. In 2025, automated traffic made up more than 53% of all web traffic, up from 51% the year before, according to Imperva's annual Bad Bot Report. Humans are now the minority on their own internet. ^[1]

The robot check no longer works. In 2024, researchers at ETH Zurich built an AI that solved 100% of Google's reCAPTCHA v2 image challenges, needing about as many attempts as a person. ^[2]

A video call where everyone else was fake. In early 2024, an employee at the engineering firm Arup in Hong Kong joined a video call with people he believed were the company's finance chief and colleagues. All of them were deepfakes. He transferred about HK\$200 million, roughly US\$25 million, in 15 payments. ^[3]

Impersonation is a multi billion dollar business. People in the United States reported losing \$12.5 billion to fraud in 2024, 25% more than the year before, with nearly \$3 billion of it lost to scammers pretending to be someone they are not. ^[4]

Fake reviews became illegal, because they became normal. In August 2024, the US Federal Trade Commission banned fake reviews and testimonials, explicitly including ones written by AI and fake social media followers. ^[5]

Fake accounts are counted in billions. Meta reported acting on about 1.4 billion fake accounts in the last three months of 2024 alone. ^[6]

Rewards go to whoever makes the most accounts. When the crypto project LayerZero prepared its 2024 airdrop, it flagged 803,093 addresses, about 13% of those eligible, as likely belonging to people farming rewards with many wallets. ^[7]

Collecting IDs creates new risks. In 2024, it was reported that AU10TIX, an identity verification company used by TikTok, X and Uber, had left administrator credentials exposed for more than a year, potentially giving access to people's names, birth dates and photos of their identity documents. ^[8]

What each case needs

CASE	WHAT WOULD HAVE HELPED	WHERE KIN ANSWERS IT
Bots outnumbering people	A cheap way to tell people from machines	Proof of human
Broken robot checks	A check machines cannot pass	Kin Pass
Deepfake calls and impersonation	Knowing an account belongs to one real, verified person	Kin ID , Kin OAuth
Fake reviews and followers	One real person per account	Kin OAuth
Farmed airdrops and rewards	One claim per human, provably	The airdrop
Leaked ID documents	Proof of human without collecting IDs	Privacy and security

Who pays the price

- **People** lose trust in what they read and who they talk to, and lose time to puzzles and checks.
- **Communities and games** are overrun by fake accounts that farm rewards and drown out real voices.
- **Businesses** pay for fake sign ups, fraud and moderation, and carry the risk of storing personal data.
- **Rewards and giveaways** end up with whoever can create the most accounts, not with real people.

Our approach

IN SHORT

Kin gives each person one private proof that they are human, and lets them carry it to any app. One person, one account, private by default, with most of the value shared through \$KIN.

Kin Identity starts from the other end. Instead of asking every app to collect more about its users, we give each person one private proof that they are human, and let them carry it wherever they go online.

Three principles

One person, one account. Every Kin identity belongs to one real, unique person. Duplicate and automated accounts are kept out, which keeps the network fair and its rewards honest.

Private by default. A Kin identity proves one fact: that its owner is a real, unique human. It does not hand over names, faces, emails, locations or browsing history. People decide what, if anything, they share beyond that.

A fair share for the people who build it. Networks become valuable because people show up and bring their friends. Through \$KIN, most of the value goes back to them, under rules written down for anyone to read.

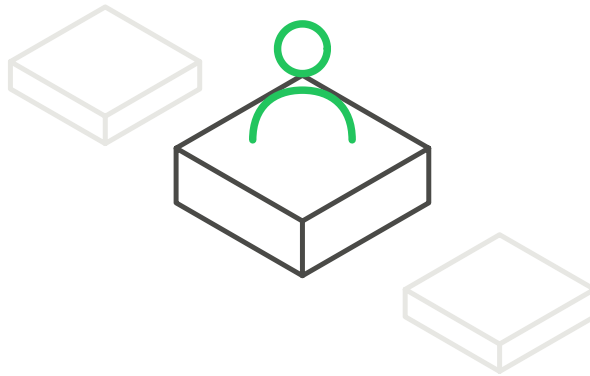


Figure 3. Real people first.

How it fits together

A person proves they are human once, in Kin ID. From then on, their Kin identity answers for them, privately, wherever they go.

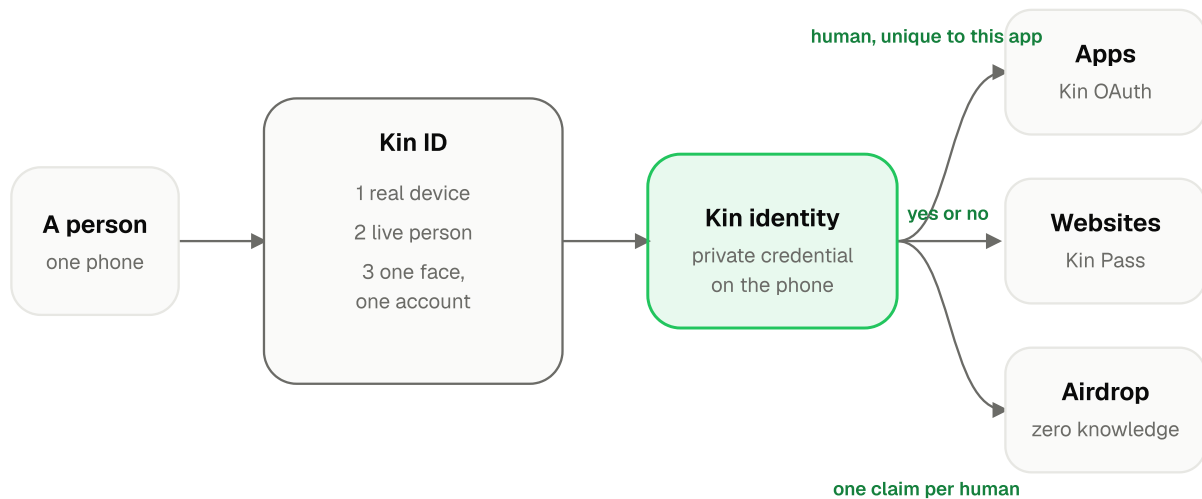


Figure 4. Prove once in Kin ID, then answer apps, websites and the airdrop without revealing who you are.

The human layer

The products in this paper fit together as layers:

LAYER	WHAT IT DOES	STATUS
Kin ID	Creates the identity; a place to meet, chat and grow together	Live on iOS and Android
Proof of human	Confirms a real device, a live person and one account per person	Rolling out
Kin OAuth	Lets any app check that a user is human and unique	In development
Kin Pass	Replaces image puzzles with one tap	In development
\$KIN	Rewards the people who build the network	Live in Kin ID

Each product starts from the same promise, and each makes the others more useful: every person who joins Kin ID strengthens Kin OAuth and Kin Pass, and every app that adopts them gives people another reason to join.

Alternatives compared

IN SHORT

Today's options either fail against AI, reveal too much about people, or leave many of them out. Kin aims to be strong against bots, private, quick and open to anyone with a phone.

Many tools try to answer "is this a real person?". Each makes a trade off between how well it stops machines, how much it reveals, how much effort it asks of people, and who it leaves out.

At a glance

APPROACH	AGAINST MODERN AI	WHAT IT REVEALS	EFFORT FOR PEOPLE	WHO IT LEAVES OUT
Image puzzles	Weak: AI solves them	Sometimes behaviour and browsing	Repeated puzzles	People with low vision or slow connections
Phone number checks	Medium: numbers can be bought in bulk	Your phone number	A code by text message	People who share or can't afford a number
Social logins	Weak: one person can open many accounts	Name, email, often a photo	One tap	Few, but uniqueness isn't checked
ID document upload	Strong, though forged and AI made documents are rising	Your full legal identity, stored by a third party	Minutes, sometimes days	People without official ID, or who won't share it
Iris scanning hardware	Strong	A biometric scan taken at a special device	A visit to a device location	Anyone far from a device
Kin	Strong: real device, live person, one face per account	Only that you're human and unique	One selfie once, then one tap	Few: works on any phone, in 19 languages, free

Why the trade offs matter

Puzzles were cheap and private enough when machines couldn't see. Now they mostly slow down people (see [The problem](#)).

Phone numbers and social logins are convenient, but they prove that someone has a number or an email, not that they are one person. Farms buy numbers and open accounts by the thousand.

ID documents prove who someone is, which is far more than most apps need. Every stored copy is something that can leak, and many people in the world have no ID they can, or want to, upload.

Special hardware can prove uniqueness strongly, but asks people to visit a device and hand a biometric scan to an operator, which limits reach and trust.

Where Kin fits

Kin combines the strength of a liveness and uniqueness check with the privacy of a yes or no answer. The selfie is deleted within seconds, only a one way template is kept to catch duplicates, and apps and blockchains receive proofs that reveal nothing else. It runs on the phone people already have.

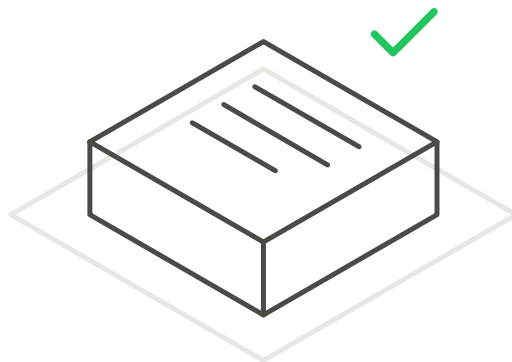


Figure 5. Only a single answer leaves the vault.

No method is perfect. Kin is designed so that the cost of faking many humans is high, while the cost of being one is a single selfie.

Kin ID

IN SHORT

Kin ID is the live app where a Kin identity is created. People meet, chat, check in every day and mine \$KIN, in 19 languages, for free.

Kin ID is the first Kin product and the home of every Kin identity. It is live on the App Store, Google Play and as an APK for Android, and speaks 19 languages from the first screen.

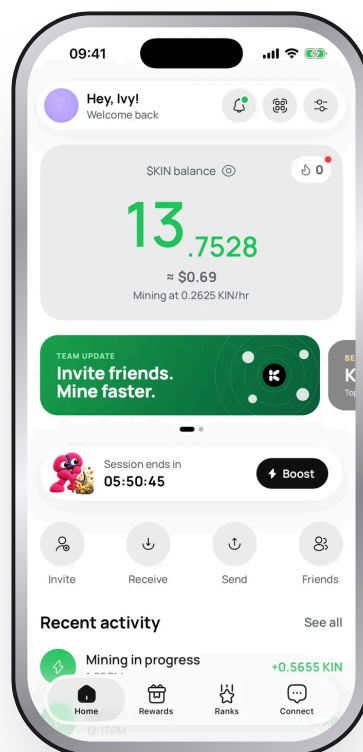


Figure 6. The Kin ID home screen: balance, mining session and friends in one place.

Joining

People join in seconds with a sign in they already have. Each account belongs to one person: duplicate and automated accounts are not allowed, and the checks described in [Proof of human](#) keep it that way. Joining is free, and every account can be deleted from settings at any time, with no forms and no waiting.

Meeting real people

Kin ID has groups, rooms and private chats. Rooms have rules, moderators and reporting tools so that they stay safe and kind. Inside chats, people can send each other \$KIN, share a "rain" of \$KIN with a room, and run small challenges.

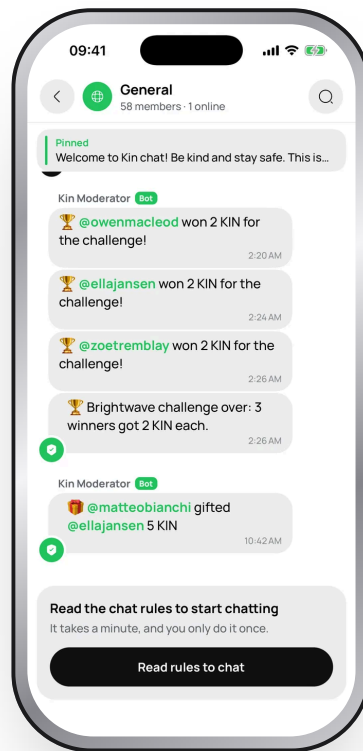


Figure 7. A group chat in Kin ID.

Showing up every day

Kin ID rewards people for showing up:

- **Mining sessions.** Tap start and a session runs for 8 hours. The speed is shown before it starts and is paid in full when it ends. See [Mining and rewards](#).
- **Daily check in and streaks.** Checking in every day pays a growing reward (10 to 60 \$KIN a day, plus streak bonuses), and mining on days in a row raises mining speed.
- **Tasks.** Simple tasks, such as watching a short video, following Kin or sharing your invite link, pay \$KIN.
- **Learn and earn.** Short quizzes about Kin, each with a chapter of this whitepaper to read first, pay \$KIN when every answer is right.

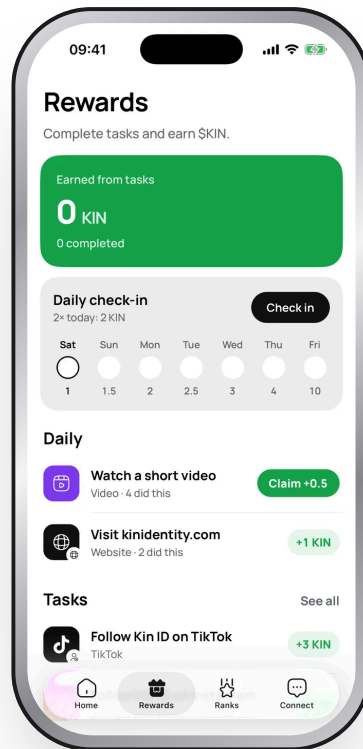


Figure 8. Rewards: daily check in, tasks and streaks.

Rising together

Friends who invite each other mine faster together (see [Invites and teams](#)). Monthly ranks show the top miners, all the way to the crown: King of Kins.

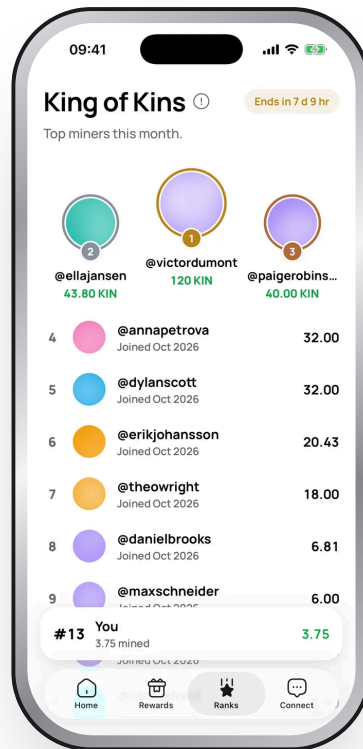


Figure 9. The monthly ranks.

The Kin crew



Figure 10. Green, Magenta and Plush: the Kin crew.

Three characters show people around: **Green**, the host, who welcomes new members and keeps them company; **Magenta**, the miner, who looks after everything \$KIN; and **Plush**, the champion, who keeps streaks alive and cheers people up the ranks.

Proof of human

IN SHORT

Three layers: a real device for everyone, a liveness and one face, one account check for verified humans, and private proofs that let them prove it anywhere without being tracked. No names or ID documents.

Every promise Kin makes depends on one thing: that each Kin identity belongs to one real, unique person. This chapter explains how we check that, and why the checks reveal so little.

What we need to know, and what we don't

To keep the network fair, Kin needs to answer three questions about an account:

1. Is it running on a **real device**, not an emulator or a script?
2. Is there a **live person** behind it, not a photo, a mask or a deepfake?
3. Is this person's **only account**?

Kin does not need anyone's name, address, ID document or social profiles to answer them, so it does not ask for them.

Three layers of checks

1. A real device (every account)

When Kin ID runs, the phone's own security services confirm that the app is genuine and running on a real, untampered device. Combined with one active account per device and a sign in method that cannot be created in bulk, this stops most automated and farmed accounts before they start. Nothing personal is shared in this step.

2. One face, one account (verified humans)

To become a **verified human**, a person takes a short selfie video. A liveness check confirms that a live person is present, not a photo, video, mask or deepfake.

The face is then turned into a **template**: a string of numbers that describes it well enough to recognise a second account, but that cannot be turned back into a picture. The template is compared with those of other verified humans to catch duplicates. The selfie itself is deleted within seconds of the check, and the comparison runs in protected hardware so that no one at Kin can browse faces.

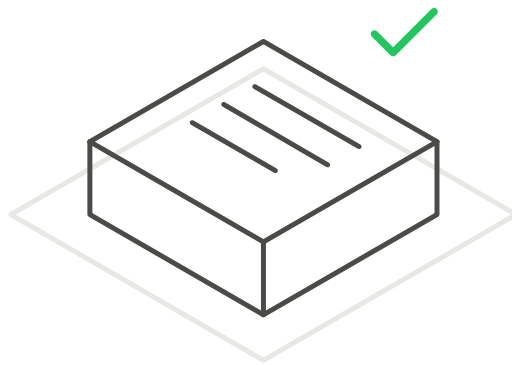


Figure 11. What leaves the phone is a yes, not a face.

Verification is optional for chatting and mining. It is required for the verified human badge, for the airdrop, and for apps that ask for it through Kin OAuth.

3. Proving it elsewhere, without being tracked

Once verified, a person can prove they are human to other apps, and to the blockchain, without becoming traceable:

- **In apps.** Through Kin OAuth and Kin Pass, each app receives a different anonymous identifier for the same person, together with a simple answer: human, and unique to this app. Two apps cannot compare notes to follow someone around.
- **On chain.** For the airdrop, each verified person holds a private credential. When claiming \$KIN on BNB Smart Chain, they submit a zero knowledge proof: a cryptographic proof that they are

one of the verified humans and have not claimed yet, which does not reveal which one. The blockchain can check the claim; neither the public nor Kin can link the wallet to the account.

Inclusion

Not everyone can or wants to take a selfie video. Verified humans will be able to vouch for a small number of friends, giving them a lighter level of trust for most of Kin. Vouching has limits, and vouching for fake accounts costs the voucher their own standing. The airdrop will still require the face check.

Consent and law

Face templates are biometric data in many countries. Verification will only ever happen with explicit consent, templates will be deleted when an account is deleted, and our approach will be reviewed against data protection law, including the GDPR and state biometric laws in the United States, before it launches.

Proposed Templates are kept only while the account exists, and deleted with it. Selfie videos are never stored. The verification provider is named in the Privacy Policy, processes data only on Kin's instructions, and is reviewed every year.

Kin OAuth

IN SHORT

A sign in button that tells any app a user is real and unique to that app, and nothing else.
Built on OpenID Connect; in development.

Kin OAuth lets any app, game or community check that each user is a real, unique person, with one tap and without collecting who they are. It is in development.

How it works

1. **The app asks.** It adds a Kin OAuth button where it needs to know someone is real: sign up, rewards, voting or posting.
2. **The person confirms in Kin ID.** They see exactly what the app will learn and approve with one tap.
3. **The app gets a proof.** A signed answer that the person is human and unique to this app, with an identifier that is the same every time they return, and different in every other app.

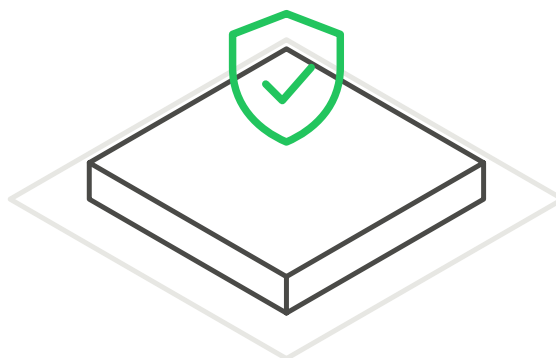


Figure 12. Kin OAuth: one tap, one answer.

What an app receives

FIELD	MEANING
human	The person passed Kin's proof of human checks
unique	This is the only account this person has in this app
sub	An identifier for this person in this app only
Name, email, photo	Never shared

Kin OAuth follows open standards, OpenID Connect and OAuth 2.0, so it works like the sign in buttons developers already know. We are designing it for the web, iOS and Android, with SDKs for the most common platforms.

Where it helps

- **Social apps and communities** keep feeds, comments and groups free of bots and fake followers.
- **Games** get fair leaderboards and matchmaking, with one player per person.
- **Rewards and giveaways** reach real people, once each.
- **Polls and voting** count one person, one vote, without asking who anyone is.
- **Marketplaces** reduce fake reviews and repeat fraud.

Timeline

A private beta with partners is planned for early 2027, and general availability for developers later that year. See the [Roadmap](#).

Kin Pass

IN SHORT

A one tap replacement for image puzzles. Sites learn that a real, unique person is here, and nothing more; in development.

Image puzzles were built to stop bots. Now AI solves them faster than people do. Kin Pass replaces the puzzle with one tap that only a verified human can make. It is in development.

Why the old check is broken

- **AI solves the puzzles.** Modern image models pick out traffic lights, crosswalks and bicycles as well as any person.
- **People pay the price.** Real people squint, fail and try again; many give up and leave.
- **Privacy pays too.** Some checks decide who is human by watching how people move and browse.

How Kin Pass works

A site adds the Kin Pass widget to a form: sign up, login, comments or checkout. A visitor taps once and confirms in Kin ID. The site's server receives a signed answer, a real and unique person is here, and checks it with one request.

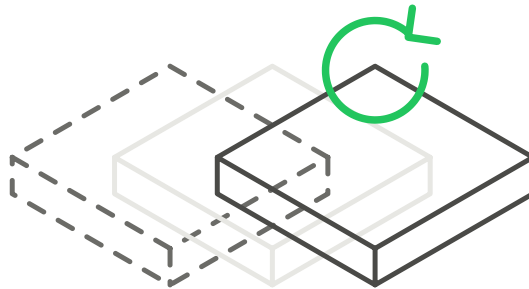


Figure 13. Repeated puzzles versus one tap.

	PUZZLE CHECKS	KIN PASS
What people do	Solve puzzles, often more than once	Tap once
Against modern AI	Weaker every year	Only verified humans pass
What the site learns	Often behaviour and browsing	One answer: a real, unique person
Accessibility	Hard with low vision or a slow connection	One button, in 19 languages

Kin Pass and Kin OAuth

Kin OAuth is for apps that want an account system built on proof of human. Kin Pass is for sites that only need to stop bots at a single step and do not want to know anything about the visitor at all. Both use the same checks and the same privacy promise.

Fallback

During the beta, sites can keep their current check as a fallback for visitors who do not use Kin ID yet, so nobody is locked out.

Timeline

A private beta with partner sites is planned for early 2027, and Kin Pass is planned to open to every website later that year.

\$KIN at a glance

IN SHORT

\$KIN is the reward of the human network: 1.5 billion, fixed forever, 70% for the people who mine and show up. Planned as a BEP-20 token on BNB Smart Chain.

\$KIN is the reward of the human network. People earn it in Kin ID for mining, showing up every day and bringing their friends. There will only ever be 1.5 billion.

Total supply	1,500,000,000 \$KIN, fixed forever
Shares	Mining and rewards 70%, Liquidity 22.5%, Reserve 5%, Team 2.5%
Today	An in app balance in Kin ID, earned and sent between people
Planned chain	BNB Smart Chain, as a BEP-20 token
Planned airdrop	Mined \$KIN claimable by verified humans

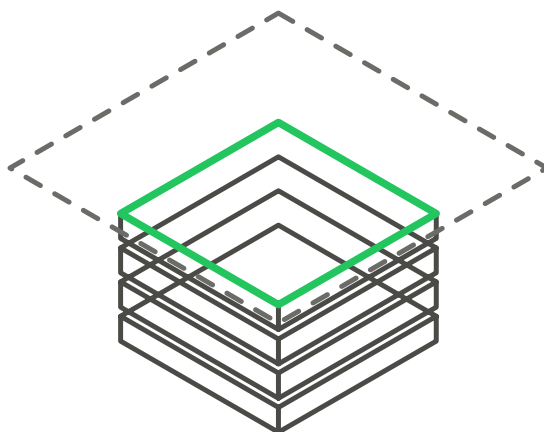


Figure 14. A hard cap: the supply can never grow.

Why a reward

Networks grow because people show up, invite their friends and make them worth being part of. In most networks, that value ends up with the company alone. \$KIN is how Kin shares it: most of the supply goes to the people who build the network, under rules that are written down and enforced in code.

How \$KIN is earned

- **Mining:** an 8 hour session at a known speed, paid when it ends.
- **Rewards:** daily check ins, streaks, tasks, welcome and invite rewards.
- **Community:** challenges, rain and community programs.

What \$KIN is for

Today, inside Kin ID

- Sending \$KIN to friends by username.
- Sharing \$KIN with a whole room as rain.
- Running challenges, where the first members to complete them share a prize.

Planned

- Tipping and paying real people, in Kin ID and beyond.
- Spending \$KIN across future Kin products.
- Taking part in community programs funded from the Mining and rewards share.

\$KIN does not buy votes. Community decisions planned for 2028 count one verified person as one vote, however much \$KIN they hold (see [Community and governance](#)).

Token details (planned)

Standard	BEP-20 on BNB Smart Chain
Total supply	1,500,000,000, created once at launch, with no way to create more
Shares	Each share held in its own published address or contract
Team share	Locked for five years in a time lock contract
Audit	Independent security audit of all contracts before launch, with the report published
Contract address	Published only on kinidentity.com and inside Kin ID

Proposed The token has 18 decimals, like most BEP-20 tokens, and its contract has no function to create new tokens, pause transfers or block holders. Any admin key is held by a multi signature wallet and removed after launch.

Important \$KIN is a community reward, not an investment, a security or a promise of value. Nobody can promise what it will be worth.

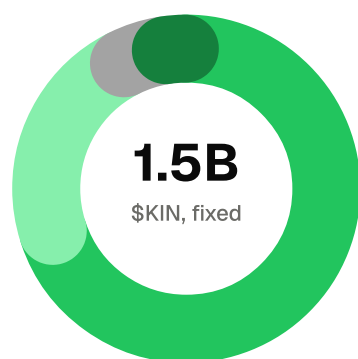
Supply and allocation

IN SHORT

Four shares with hard caps: Mining and rewards 70%, Liquidity 22.5%, Reserve 5%, Team 2.5% locked for five years.

The supply is split into four shares. Every \$KIN is created from one of them, and a share can never give out more than its limit. The system checks this every time \$KIN is created.

SHARE	%	\$KIN	WHAT IT'S FOR
Mining and rewards	70%	1,050,000,000	Paid to the people who show up: mining, friend rewards, daily check in, streaks, tasks, challenges and community programs
Liquidity	22.5%	337,500,000	Liquidity on exchanges, market making and listing costs, and the future needs of the \$KIN ecosystem
Reserve	5%	75,000,000	Kept back for the unexpected
Team	2.5%	37,500,000	The people who build and run Kin Identity



■ Mining and rewards	70%
	1,050,000,000 \$KIN
■ Liquidity	22.5%
	337,500,000 \$KIN
■ Reserve	5%
	75,000,000 \$KIN
■ Team	2.5%
	37,500,000 \$KIN

Figure 15. The four shares of \$KIN.

Mining and rewards (70%)

Almost three quarters of all \$KIN goes to the people who use Kin ID. Mining speed halves as more is mined (see [Mining and rewards](#)), so this share lasts for years and early and late members both have a fair chance to earn.

Liquidity (22.5%)

When \$KIN becomes tradable, people need to be able to buy and sell it at fair prices. This share provides liquidity on decentralized and centralized exchanges, pays market makers who keep trading orderly, and covers listing costs. What is left supports the long term needs of the \$KIN ecosystem. Every release from this share will be announced publicly.

Reserve (5%)

The reserve is kept for the unexpected, such as covering losses from a security incident. It is not spent on day to day operations, and any use will be announced before it happens.

Team (2.5%)

The team share is deliberately small. It is **locked for five years** from the token launch, so the people building Kin share in its success only by building it over the long term.

Proposed The team share stays fully locked for five years, then unlocks in equal monthly parts over the following twelve months, so no single day releases it all. Each share is held in its own public address, listed here before the token launch, so anyone can follow it on chain.

Mining and rewards

IN SHORT

8 hour sessions at a speed you know in advance. Base speed starts at 2 KIN per hour and halves every 150 million mined; streaks, friends and a welcome boost multiply it.

Mining in Kin ID is simple on purpose: you always know your speed before a session starts, and you get exactly that when it ends. Mining uses no battery or computing power; the phone only starts and claims sessions.

A session

Tap start and a session runs for **8 hours**. The speed is fixed when it starts and shown in KIN per hour. When the session ends, the \$KIN is paid to your balance.

Your speed

Speed is the base speed multiplied by three boosts:

Speed = base speed × mining days × team × welcome

Base speed and halvings

The base speed is the same for everyone. It starts at **2 KIN per hour** and **halves each time 150 million KIN has been mined**, like Bitcoin's halvings. Early members earn faster, and the mining share can never be overrun.

MINED SO FAR	BASE SPEED
0 to 150 million	2 KIN per hour
150 to 300 million	1 KIN per hour
300 to 450 million	0.5 KIN per hour
450 to 600 million	0.25 KIN per hour
Every further 150 million	Halves again

Mining days

Mining on days in a row unlocks a higher multiplier, kept for as long as the streak lasts:

DAYS IN A ROW	MULTIPLIER
1	×1.2
3	×1.5
7	×2
14	×3
30	×5

Team

Each friend you invited who is mining when you start a session lifts your speed. See [Invites and teams](#) for the full table, from ×2 with one friend to ×150 with a thousand.

Welcome

New members mine **×2 for their first 3 days**.

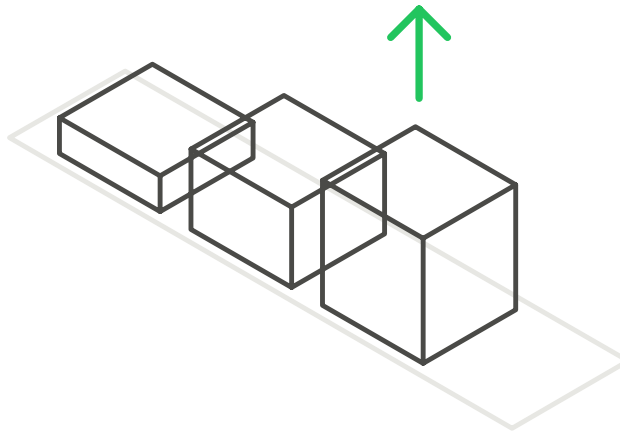


Figure 16. Showing up day after day raises your speed.

An example

At today's base speed of 2 KIN per hour, a member on a 7 day streak (×2) with 3 friends mining (×3) mines at **12 KIN per hour**, or **96 KIN per 8 hour session**.

Daily rewards

Besides mining, Kin ID pays rewards from the same share:

- **Joining:** a 100 \$KIN welcome bonus when an account is created.
- **Daily check in:** 10 to 60 \$KIN a day, growing over the week, with streak bonuses from 25 \$KIN at 2 days up to 50,000 \$KIN at 365 days.
- **Tasks:** daily ones, such as watching a short video or visiting kinidentity.com, pay 10 \$KIN each; one time ones, such as following Kin on X, Telegram, Instagram, TikTok or YouTube, pay 75 to 100 \$KIN. Sharing your invite link can be a task too.
- **Learn and earn:** short quizzes about Kin, each with a whitepaper chapter to read first, pay 100 to 150 \$KIN when every answer is right.
- **Weekly team goals:** you and the friends you invited mine together from Monday to Sunday, and reaching 500, 2,000 and 5,000 KIN pays 150, 600 and 1,500 \$KIN. See [Invites and teams](#).
- **Challenges and rain:** \$KIN shared in rooms, sometimes sponsored by partners.

Changing the numbers

The Kin team can adjust session length, multipliers and rewards as the network grows, for example to keep the mining share lasting. Changes only apply to sessions that start after them, and will be announced in the app and on kinidentity.com. The total supply and the shares cannot be changed.

Invites and teams

IN SHORT

Inviting pays three ways: a joining reward for both of you, an instant reward each time your friend starts mining, and a faster team, up to ×150. Milestone bonuses and weekly team goals add more.

Kin grows through people bringing people they know. Inviting pays in three ways, and none of it is taken from the friend you invite.

Your invite link

Every member has an invite link with their username, such as `kinidentity.com/@alex`. A new member adds the person who invited them within 7 days of joining, and both get a reward.

Three ways inviting pays

- 1. A joining reward.** When a new member adds you as their inviter, you each get **100 \$KIN**, on top of their 100 \$KIN welcome bonus.
- 2. An instant friend reward.** Every time a friend you invited starts a mining session, you get 5 hours of the current base speed straight away. At today's base speed, that is **10 \$KIN** each time.
- 3. A faster team.** Each friend you invited who is mining when you start a session lifts your speed:

FRIENDS MINING	TEAM MULTIPLIER
1	×2
3	×3
5	×5
10	×10
25	×18
50	×25
100	×50
250	×80
500	×110
1,000	×150

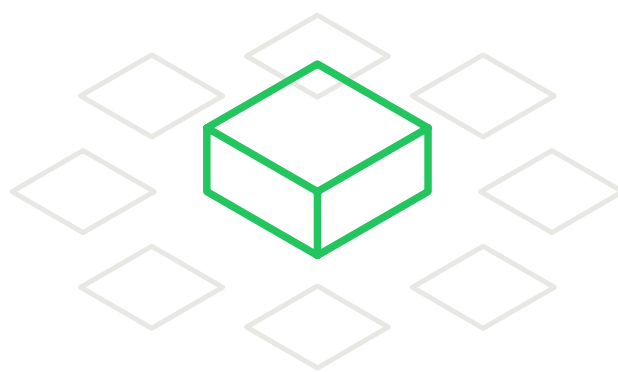


Figure 17. Friends who mine together go faster.

Invite milestones

On top of all that, bonuses arrive as more of your invited friends start mining. A friend counts once they have mined at least once, and each milestone pays once:

FRIENDS WHO MINED	BONUS
1	25 \$KIN
3	75 \$KIN
5	150 \$KIN
10	400 \$KIN
25	1,200 \$KIN
50	3,000 \$KIN
100	7,500 \$KIN

Weekly team goals

You and the friends you invited also share a goal each week, from Monday to Sunday (UTC). Everything your team mines counts, and each goal reached pays you once that week:

MINED TOGETHER THIS WEEK	BONUS
500 KIN	150 \$KIN
2,000 KIN	600 \$KIN
5,000 KIN	1,500 \$KIN

Why it's fair

- Only **active** friends count: a friend lifts your speed only while they are mining.

- Every friend must be a real person with one account, so invites cannot be farmed.
- Invite rewards come from the Mining and rewards share, not from your friend's balance.

Keeping it fair

IN SHORT

Rewards only mean something if they go to real people. Kin checks devices, people and behaviour, removes rewards earned by fake accounts before the airdrop, and lets anyone wrongly flagged appeal to a person.

Every reward system attracts people who try to game it. Kin is designed so that farming is expensive and pointless, and so that honest members never pay for it.

What we stop

- **Bot farms:** scripts, emulators and modified apps starting sessions automatically.
- **Multiple accounts:** one person running many accounts to multiply rewards or team boosts.
- **Invite rings:** groups inviting fake accounts, or each other in loops, to inflate team multipliers.
- **Spam and abuse in rooms:** fake accounts flooding chats, rain and challenges.

How

- **Real devices only.** The phone's own security services confirm that Kin ID is genuine and running on a real device. One active account per device.
- **One face, one account.** Verified humans pass a liveness and uniqueness check (see [Proof of human](#)). The airdrop and the highest trust features require it.
- **Behaviour checks.** Patterns that people don't produce, such as sessions started at machine regular intervals across many accounts, are flagged automatically.
- **Invite limits.** An account can have only one inviter, set once, within its first 7 days. Loops are blocked, and only friends who are actively mining count towards a team.
- **Room safety.** Rules, moderators, reporting and limits on rain and challenges keep rooms usable.

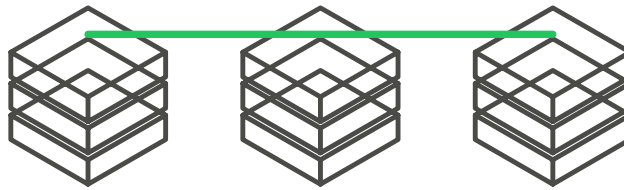


Figure 18. The same rules for everyone.

What happens to abuse

- Rewards earned by fake or duplicate accounts are **removed before the snapshot** and do not reach the airdrop.
- Accounts found farming are suspended, and their invites stop counting towards anyone's team.
- Removed \$KIN returns to the Mining and rewards share, for real members to earn.

Appeals

Automated checks make mistakes. Anyone who believes they were flagged wrongly can appeal from the app, and a person, not a machine, reviews the appeal.

Reporting

We plan to publish regular figures on accounts removed and rewards recovered, so that the community can see that the rules are enforced.

Mining phase, airdrop and listings

IN SHORT

In app \$KIN is planned to move on chain in 2027: a snapshot, a BEP-20 token on BNB Smart Chain, an airdrop to verified humans, then listings.

\$KIN starts as a balance inside Kin ID. This chapter describes how we plan to move it on chain. Each step depends on legal approvals, exchanges and partners, and may change or not happen.

1. The mining phase (from Q4 2026)

Kin ID launched with mining open to everyone, for free. During this phase, every \$KIN earned is recorded in Kin ID's ledger against the share it came from.

2. The snapshot (planned Q2 2027)

The mining phase closes with a snapshot of every balance. The date will be announced in the app well in advance.

3. The token and the airdrop (planned Q2 2027)

\$KIN will launch as a **BEP-20 token on BNB Smart Chain**, chosen for its low fees, speed and wide support across wallets and exchanges.

Mined \$KIN from the snapshot will be airdropped to **verified humans**. Claims use the private proof described in [Proof of human](#): a verified person proves they are one of the verified humans and have not claimed yet, without revealing which account is theirs. Accounts that are not verified, or that are found to be duplicates, cannot claim.

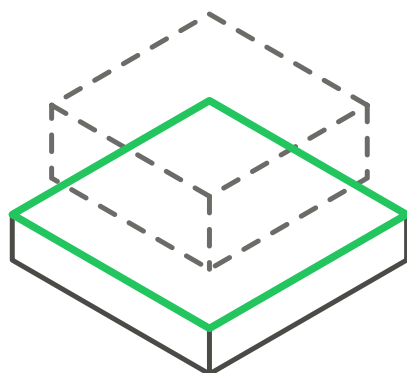


Figure 19. Only the outline of what comes next is fixed.

Proposed

- **Conversion:** one in app \$KIN becomes one token. Balances that came from accounts later found to be duplicates or automated are removed before the snapshot.
- **Claim window:** 180 days from the start of claims, with reminders in Kin ID. Claiming costs only the network fee.
- **Unclaimed tokens:** return to the Mining and rewards share, to be earned again by active members. They are never moved to the team.
- **After the snapshot:** mining continues in Kin ID on the same halving schedule. New balances become claimable in regular rounds, so no one has to rush.
- **Not verified yet:** balances of members who are not verified at the snapshot are kept, and become claimable once they verify.

4. Listings (planned Q3 2027)

Using the Liquidity share, \$KIN is planned to become tradable first on decentralized exchanges on BNB Smart Chain, then on centralized exchanges. Listings depend on each exchange's own review, and no listing is guaranteed.

Staying safe

- Kin will never ask for your password, seed phrase or private keys.
- The only official claim page will be linked from kinidentity.com and inside Kin ID.
- Claiming will never cost anything beyond the network fee. Anyone asking you to pay to claim, or to send \$KIN or crypto first, is not Kin.

Roadmap

IN SHORT

From launch in Q4 2026 to the human layer in 2028: proof of human, the airdrop, listings, and Kin OAuth and Kin Pass for every developer.

Dates are targets, not promises. Token, airdrop and listing plans depend on legal approvals, exchanges and partners, and may change or not happen.

Q3 2026 · Foundations (done)

- Groups, rooms and private chats
- Daily check in, streaks and ranks
- \$KIN with a fixed supply of 1.5 billion
- 19 languages from the first screen

Q4 2026 · Launch and mining (now)

- Kin ID on the App Store, Google Play and as an APK
- The mining phase opens to everyone, for free
- kinidentity.com in 19 languages
- Safety and moderation tools for every room
- Sign in with Apple

Q1 2027 · Proof of human

- Private ways to prove you're a unique person
- A verified human badge on your profile
- Kin Pass private beta with the first partner sites

- Kin OAuth private beta for partners

Q2 2027 · The airdrop

- A snapshot of every mined balance
- \$KIN launches on BNB Smart Chain
- Airdrop of mined \$KIN to verified humans

Q3 2027 · Listings

- \$KIN on decentralized exchanges
- First listings on centralized exchanges
- Send \$KIN to friends in Kin ID
- Kin Pass opens to every website

Q4 2027 · Open to every developer

- Kin OAuth for every developer
- SDKs for the web, iOS and Android
- A developer console for apps, keys and usage

H1 2028 · Kin everywhere

- More ways to use \$KIN across Kin products
- Tip and pay real people with \$KIN
- Community votes on how ecosystem funds are used

H2 2028 · The human layer

- An open standard any app can use to check a Kin identity

- New Kin products built on your Kin identity, such as Kin Mark (content made by a real person), Kin Vote (one person, one vote) and Kin Drop (fair giveaways, one per person)

Privacy and security

IN SHORT

We collect what Kin needs to work, never sell personal data, never ask for ID documents, and delete everything when you leave.

Proving you're human should never cost you your privacy. These are the rules we build by.

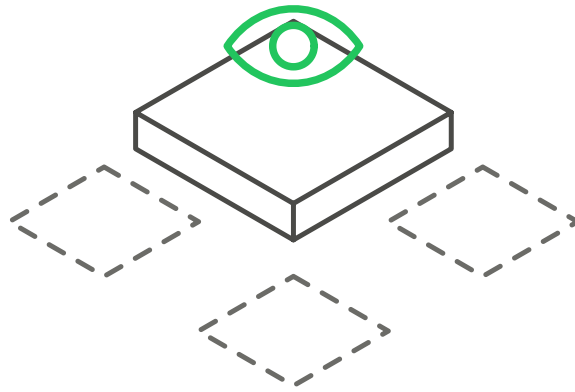


Figure 20. Private by design.

What we collect

- **Account basics** from the sign in method you choose, so you can log in.
- **What you do in Kin ID**, such as messages, mining sessions and rewards, so the app works.
- **Device signals** needed to confirm a real, untampered device and to stop fake accounts.
- **A face template**, only if you choose to become a verified human, as described in [Proof of human](#).

What we never do

- We never sell personal information.
- We never share your name, email or photo with apps that use Kin OAuth or Kin Pass.
- We never ask for ID documents, home addresses or financial details to prove you're human.
- We never ask for your password, seed phrase or private keys.

You stay in control

- Choose who can see your profile and when you were last online.
- Chat anonymously in rooms if you prefer.
- Delete your account from settings at any time. Your data, including any face template, is deleted with it.

Security

- Data is encrypted in transit and at rest.
- Face templates are compared in protected hardware, and selfies are deleted within seconds.
- The rules that limit each \$KIN share are enforced in code every time \$KIN is created.
- We plan independent security reviews before the token launch, and will publish their results.

Our full [Privacy Policy](#) explains everything in detail.

Business model

IN SHORT

Kin earns from optional ads and sponsorships today, and from businesses using Kin OAuth and Kin Pass next. Never from selling data.

A company that protects people's privacy has to make money in a way that doesn't depend on selling it. This chapter explains how Kin Identity pays for itself.

Today

- **Advertising in Kin ID.** Optional rewarded ads, such as watching a short video to boost a session or earn a task reward. Ads are shown without selling personal information.
- **Sponsored moments.** Partners can sponsor challenges, rain and tasks inside rooms, reaching real people rather than bots.

Next

- **Kin OAuth and Kin Pass for businesses.** A free tier for small apps and communities, and usage based plans for larger ones. Proof of human saves businesses money on fake sign ups, fraud and moderation, and lets them stop storing personal data they don't need.
- **Partner programs.** Apps and brands that want to reach verified humans, with consent and without tracking.

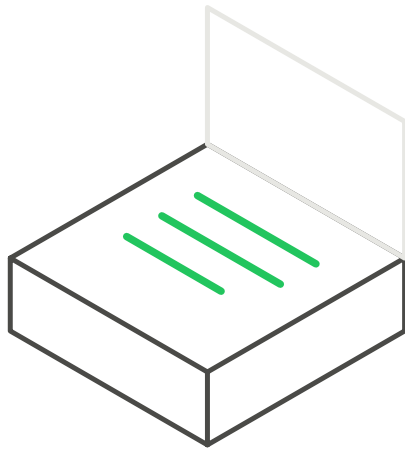


Figure 21. A business built in the open.

What we won't do

- Sell personal information.
- Charge people to join, chat or mine.
- Fund operations by selling the Team or Reserve shares of \$KIN.

Why this matters

Every app that pays to know its users are human makes the network more valuable for the people in it. Revenue from businesses funds the people, servers and safety work that keep Kin free for everyone else.

Community and governance

IN SHORT

The people who use Kin shape it: through community channels and feedback today, and one person, one vote decisions from 2028.

Kin is built with the people who use it.

Today

- **Community channels** on [Telegram](#), [Discord](#) and [X](#), where the team shares progress and people suggest features.
- **Feedback in the app**, which shapes what we build next.
- **Translations** in 19 languages, so that nobody is left out.

Planned

- **Community votes** on how parts of the Mining and rewards share are used for community programs, planned for 2028. Voting will use proof of human, so every verified person gets one vote, however much \$KIN they hold.
- **Public reports** on the state of each \$KIN share, so anyone can check how much has been created and from where.

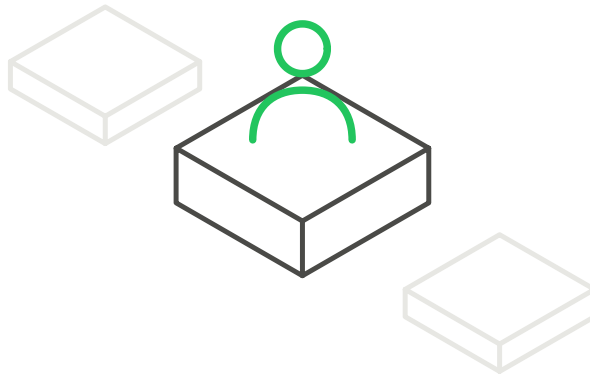


Figure 22. Real people first.

How we decide

Before building anything, we ask three questions:

1. **Does it keep it human?** Everything we ship has to make it easier to know and meet real people, never harder.
2. **Does it protect privacy?** If a feature needs more of your data than it should, we find another way or we don't build it.
3. **Is it fair to everyone?** The same rules for every person, in every language, with nothing hidden.

Risks and legal notice

IN SHORT

\$KIN is a community reward, not an investment. Plans can change, laws differ by country, and technology and markets carry risk.

Please read this chapter carefully.

What this paper is

This whitepaper describes Kin Identity's products and plans as of the date shown below. It is for information only. It is not an offer to sell, or a request to buy, any token, security or financial product, and nothing in it is financial, legal or tax advice.

\$KIN is not an investment

\$KIN is a community reward for the people who build the Kin network. It is not a share in Kin Identity and gives no right to profits, dividends or any part of the company. Nobody can promise what \$KIN will be worth, and it may be worth nothing.

Risks

- **Plans may change.** The token launch, airdrop, listings and other plans depend on legal approvals, exchanges and partners. They may be delayed, changed or cancelled.
- **Regulation.** Laws on digital tokens and biometric data differ between countries and are changing. Some features may not be available everywhere.
- **Technology.** Software, smart contracts and blockchains can have bugs or be attacked. Wallets and keys can be lost.
- **Markets.** If \$KIN becomes tradable, its price may be volatile, and there may be little demand for it.

- **Proof of human.** No verification system is perfect. Some fake accounts may get through, and some real people may be wrongly stopped.
- **Your responsibility.** You are responsible for your own wallet, keys and taxes, and for following the laws where you live.

Contact

Questions about this paper can be sent through the channels on kinidentity.com.

Frequently asked questions

IN SHORT

The quick answers. Each links to the chapter with the full story.

Is Kin ID free?

Yes. Joining, chatting, checking in and mining are all free. See [Kin ID](#).

Do I have to show my ID or my face?

You never show an ID document. A short selfie is only needed to become a verified human, which the airdrop requires. The selfie is deleted within seconds; only a one way template is kept to catch duplicate accounts. See [Proof of human](#).

Can apps see who I am?

No. Apps using Kin OAuth or Kin Pass learn that you are a real, unique person, and nothing else. Each app gets a different anonymous identifier, so apps can't track you between them. See [Kin OAuth](#).

Does mining drain my battery?

No. Mining doesn't use your phone's computing power. The phone only starts and claims sessions. See [Mining and rewards](#).

How much \$KIN will there ever be?

1.5 billion, fixed forever. 70% goes to the people who mine and show up. See [Supply and allocation](#).

Why does my mining speed go down over time?

The base speed halves every time 150 million KIN is mined, so the mining share lasts and early and late members both have a fair chance. Streaks and friends multiply your speed. See [Mining and rewards](#).

How do I mine faster?

Mine on days in a row (up to ×5) and invite friends who mine too (up to ×150). New members also mine ×2 for their first 3 days. See [Invites and teams](#).

What blockchain will \$KIN use?

BNB Smart Chain, as a BEP-20 token. See [Mining phase, airdrop and listings](#).

When is the airdrop?

A snapshot and the airdrop are planned for Q2 2027, with listings planned from Q3 2027. Dates can change. See [Roadmap](#).

Who can claim the airdrop?

Verified humans, with one claim per person. Rewards from fake or duplicate accounts are removed before the snapshot. See [Keeping it fair](#).

Will \$KIN be listed on exchanges?

That is the plan, first on decentralized exchanges on BNB Smart Chain, then on centralized exchanges. Each exchange decides for itself, so no listing is guaranteed.

How much will \$KIN be worth?

Nobody can promise that. \$KIN is a community reward, not an investment. See [Risks and legal notice](#).

How much does the team get?

2.5% of the supply, locked for five years. See [Supply and allocation](#).

Can I delete my account?

Yes, from settings, at any time. Your data, including any face template, is deleted with it. See [Privacy and security](#).

How do I avoid scams?

Kin will never ask for your password, seed phrase or private keys, and claiming will never cost more than the network fee. Use only links from kinidentity.com or inside Kin ID.

Glossary

IN SHORT

Plain definitions for the terms used in this paper.

TERM	MEANING
Kin identity	A private proof that its owner is a real, unique person
Kin ID	The app where a Kin identity is created, and where people meet, chat and mine
Verified human	A member who has passed the liveness and one face, one account check
Kin OAuth	A sign in button that tells apps a user is human and unique, and nothing else
Kin Pass	A one tap replacement for image puzzles on websites
\$KIN	The reward of the human network, with a fixed supply of 1.5 billion
Share	One of the four parts of the \$KIN supply, each with a hard cap
Session	An 8 hour mining period at a fixed speed
Base speed	The mining speed everyone starts from; it halves every 150 million KIN mined
Halving	The point at which the base speed halves
Mining days	Days in a row with a mining session; they raise your speed up to ×5
Team multiplier	The boost from friends you invited who are mining, up to ×150
Rain	\$KIN shared with everyone in a room
Snapshot	The moment balances are recorded for the airdrop
Airdrop	Sending mined \$KIN, as tokens, to verified humans
BEP-20	The token standard on BNB Smart Chain
Liveness check	A check that a live person, not a photo, mask or deepfake, is in front of the camera

TERM	MEANING
Face template	Numbers that describe a face well enough to spot a duplicate, but can't be turned back into a picture
Zero knowledge proof	A proof that something is true, such as being a verified human, that reveals nothing else

References

IN SHORT

The public sources behind the cases in this paper.

Sources for the cases in The problem. Links were checked in October 2026.

1. Imperva (Thales). **Bad Bot Report 2026: Bots in the Agentic Age**. April 2026. Automated traffic was more than 53% of all web traffic in 2025, up from 51% in 2024. imperva.com
2. Plesner, A., Vontobel, T. and Wattenhofer, R. **Breaking reCAPTCHA v2**. ETH Zurich, arXiv:2409.08831, September 2024. arxiv.org
3. CNN. **Arup revealed as victim of \$25 million deepfake scam involving Hong Kong employee**. 16 May 2024. cnn.com
4. US Federal Trade Commission. **New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024**. 10 March 2025. ftc.gov
5. US Federal Trade Commission. **Federal Trade Commission Announces Final Rule Banning Fake Reviews and Testimonials**. 14 August 2024. ftc.gov
6. Meta. **Community Standards Enforcement Report**, fake accounts, Q4 2024; figure as cited in written evidence to the UK Parliament. transparency.meta.com, committees.parliament.uk
7. The Defiant. **LayerZero Labs Identifies 800,000 Potential Sybil Addresses in Public List**. 2024. thedefiant.io
8. 404 Media. **ID Verification Service for TikTok, Uber, X Exposed Driver Licenses**. June 2024. 404media.co

Note Kin Identity is not affiliated with any of the organisations above. They are cited only as public evidence of the problems this paper describes.

Version history

IN SHORT

This paper will change as Kin grows. Every version is listed here.

VERSION	DATE	CHANGES
1.0	October 2026	First public draft. Products, proof of human, \$KIN on BNB Smart Chain, four share supply, mining, invites, fairness, airdrop and listing plans, roadmap to 2028.

Items marked **Proposed** are suggestions under review, and items marked **To confirm** are decisions still to be made. Both will be settled, and recorded here, before the token launch.

Kin Identity Whitepaper · Version 1.0 · 2026-10-24 · whitepaper.kinidentity.com