This document introduces the foundational concepts of the Idena blockchain and provides a formal specification of iDNA, its native coin

What is Idena

Idena is an open source project started in October 2018.

The Idena blockchain is driven by Proof-of-Person consensus with every node linked to a cryptoidentity, one person with equal voting power. It suggests a novel way to formalize people on the Internet: Idena proves the humanness and uniqueness of its participants without collecting personally identifiable information by running a Turing test at the same time globally.

Idena team

We are an anonymous group of like-minded engineers and computer scientists who stand for the human right to share information and exchange value freely and privately.

We believe that there is a way to redesign the way software systems in general and blockchains in particular work to achieve greater decentralization and scalability.

Contacts: `info@idena.io`

The problem of unique identity

Anonymous and Sybil-resistant identity is a missing part for Web 3.0 (Internet applications, blockchains, dapps, and self-sovereign identity space).

The design requirements of this decentralized anonymous identity to a large extent follow the properties introduced by Bitcoin:

- Global and verifiable online
- Permissionless and inclusive
- Decentralized, without reliance on trusted third parties
- Sybil-resitant
- Anonymous and privacy-preserving
- Censorship-resistant and plausibly deniable

Existing state-of-the-art identity mechanisms fail to achieve this:

- OpenID identity solutions such as those of Facebook and Google, based on a social information, rely on a centralized service, are not available in many countries, can be purchased on the market, and are easily spoofed.
- Government ID relies on trusted know-your-customer (KYC) verifiers, requires the sharing of personally identifying information (PII) with a centralized service, is not inclusive, and leads to an Orwellian world.
- Biometrics relies on specific sensors and algorithms, can be faked, and cannot have plausible deniability.
- Video identification can be faked with AI algorithms which can produce a high quality deepfakes unidentifiable as deepfakes.
- Self-sovereign identities (SSI) rely on trusted verifiers based on Social ID and Government ID attestation.
- Web of Trust (WoT) approaches do not allow to build the consensus about the registry of valid identities across all nodes.

Manifesto

The Internet has democratized information sharing, but, like any complex socio-technical system, it tends to concentrate power.

The World Wide Web is centered around the cloud infrastructure of super conglomerates like Amazon, Microsoft, and Facebook. They enjoy economy of scale and have access to the best engineering teams to create even more gravity for the solid core.

> **WE ARE ALL CITIZENS OF GOOGLE AND APPLE**

We are happier, fitter, more productive, but... dependent, monetized, surveilled.

Even best-in-class secure email and messaging services like ProtonMail or Signal require us to disclose our identity one way or another for long-term storage on their servers.

Ten years ago, Bitcoin paved the way for reliable censorship-resistant digital cash, truly distributed infrastructure, and innovative leaderless governance. It was followed by Ethereum, which has proven the concept of global general-purpose computing and formed a vibrant ecosystem of decentralized application developers.

> **WHILE BLOCKCHAIN TECHNOLOGY IS STILL IN ITS INFANCY, IT HAS ALREADY EXPERIENCED ITS OWN CONCENTRATION OF POWER**

Over time, the validation of public blockchains got pooled in the hands of a few miners, making it easy to form cartels and distort governance. There are 13 controlling pools in Bitcoin, 20 distinct miners in Ethereum, and 21 block producers in EOS. Fifty percent of Ethers are owned by 400 addresses. The Proof-of-Stake mechanism will only make the distribution more extreme - the rich become richer. Such is the nature of money.

> **WE BELIEVE THAT PROOF OF PESONHOOD IS THE BUILDING BLOCK OF THE DECENTRALIZED FUTURE**

There is a call for a solution to the growing imbalance of power in blockchain and Internet applications.

Why Idena

Proof of Personhood

We believe that a Proof of Personhood is the building block of the decentralized future. Such a proof can be anonymous, self-managed, and valid globally, no matter where the person lives. No trusted authorities are needed to achieve this. All we need to know about the account is that there is a single living person to whom that account belongs. We call it cryptoidentity.

One person - one vote

One person - one vote is a fundamental principle for democracy and a foundation for the future blockchain technology. We believe in distributed governance and the wisdom of the crowd to achieve stability. Advanced voting mechanisms like quadratic voting could improve distributed governance for everyone.

Decentralized web

A peer-to-peer web without servers and censors would empower people, not wealth or authority, and give them control over sharing information and value. No personal data should be required to access a service, send a message, or buy a coffee in a decentralized world.

Universal basic income

Blockchain mining must be democratic: The blockchain node should be light enough to run on an average computer or laptop. In Idena all participants are empowered to maintain the network. Participation in Idena is rewarded both in a form of a UBI and rewards proportional to stake.

Freedom of speech

Every voice has a right to be heard. Spreading information should be seamless, and publications should be censorship-resistant.

Scalability, decentralization, security

We believe that a scalable blockchain can be built without compromising its safety. The basis for genuine scalability and safety is a transparent and redundant decentralization.

Edit this page

Proof-of-personhood

The Idena network allows for a proof of humanity and proof of uniqueness for its participants. We call it Proof-of-Person (PoP) protocol. Idena does not require any personal data sharing, does not reveal a person's identity, and does not need a third-party identification center. Idena is based on a network of people mutually validating their humanness and uniqueness. How is it possible?

Idena employs regular checkpoint rituals — synchronous validation sessions — to certify a participants' humanness for the consequent epoch. The validation requires solving of `flips-puzzles` easy for a human, difficult for a bot.

The uniqueness of participants is proven by the fact that they must solve flip synchronously. Flips are decrypted at the same time worldwide. A single person is not able to validate herself multiple times because of the limited timeframe for the answers submission.

After the validation session is over, the network reaches consensus about the new list of validated participants, and the date of the next validation session is scheduled. The bigger the network is, the less frequently the validation sessions happen.

The validation status of a participant is not forever. It expires when the next epoch starts. Participants should prolong their validation status for every new epoch.

To be allowed to take part in the next validation round, the participant must provide a certain number of newly created flips.

Validation session schedule

The date of the validation session is calculated by the network and is shown in the Idena app. The time is always fixed: 15:00 UTC.

The bigger the network is, the less frequently the validation sessions happen.

The validation date is adjusted to Saturdays once the network reaches 291 identities. The total epoch duration is limited to 28 days.

Network size	Frequency days
17+	3
45+	4
96+	5
176+	6
291+	14 if Saturday, 13 or 15 otherwise(*)
5845+	21
16203+	28

> **NOTE**
>
> (*) 13 days for Sunday, Monday, or Tuesday and 15 days for Wednesday, Thursday, or Friday

The validation time of 15:00 UTC covers most countries when most people are awake. These are the local times for some of the world's cities (as of June 22nd, 2023):

- San Francisco, USA 8:00

- New York, USA 11:00
- Tunis, Tunisia 16:00
- Berlin, Germany 17:00
- Cairo, Egypt 18:00
- Moscow, Russia 18:00
- Delhi, India 20:30
- Jakarta, Indonesia 22:00
- Beijing, China 23:00
- Seoul, South Korea 00:00 + 1 day
- Sydney, Australia 01:00 + 1 day
- Auckland, New Zealand 03:00 + 1 day
- Honolulu, Hawaii, USA 05:00 + 1 day

Short session and Long session

The short validation session has a very limited time frame, less than two minutes, and consists of six flips, each of which is received only by 1–4 participants in the network (depending on the network size). This session's task is conducting a Turing test: telling humans from AI.

The long flip qualification session lasts 30 minutes and consists of 25-30 flips, each of which is received by a larger number of network participants (depending on the network size). This session enables the network to achieve a consensus on flip quality and the right answer to a flip.

Cryptoidentity

Cryptoidentity is one validated account with equal voting power. The cryptoidentity persists for as long as the current epoch lasts. During the epoch, the cryptoidentity gains special privileges, including the ability to invite new users, mine new blocks and get rewards, propose protocol improvements, and create new flips.

After the validation expires by the end of the epoch, participants revalidate themselves with a new synchronized test.

Candidate

A participant who has just joined the network via an invitation can participate in the subsequent validation session only.

Newbie

A newly validated identity can participate in subsequent validation sessions, mine coins, and create flips, but this person cannot send out invitations or miss validations.

Verified

A cryptoidentity validated at least three times in a row and having Total score>=75% can do the same as a Newbie plus

- send out invitations
- submit 1 extra flip
- miss up to two validations in a row. This person cannot fail neither short session nor long session.

Human

A cryptoidentity validated at least four times and having Total score>=92% can do the same as a Verified plus

- submit 2 extra flips (5 in total)
- fail short session without being killed. This person cannot fail a long session.

Suspended

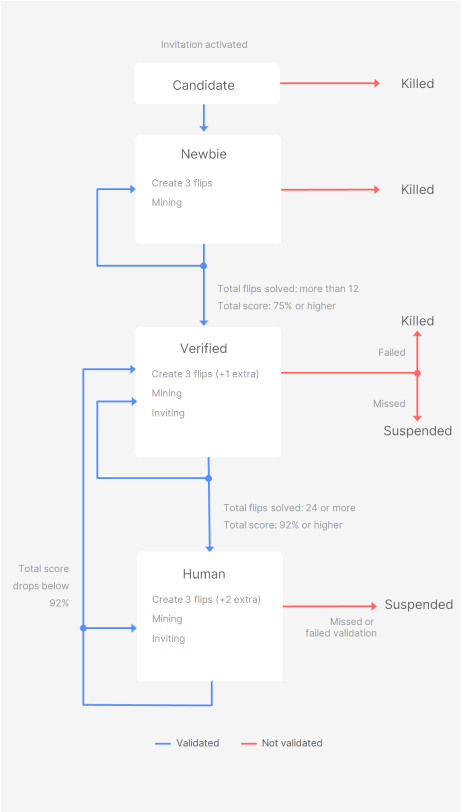
A verified cryptoidentity that has missed one validation session can do the same as a Candidate and can miss one validation session.

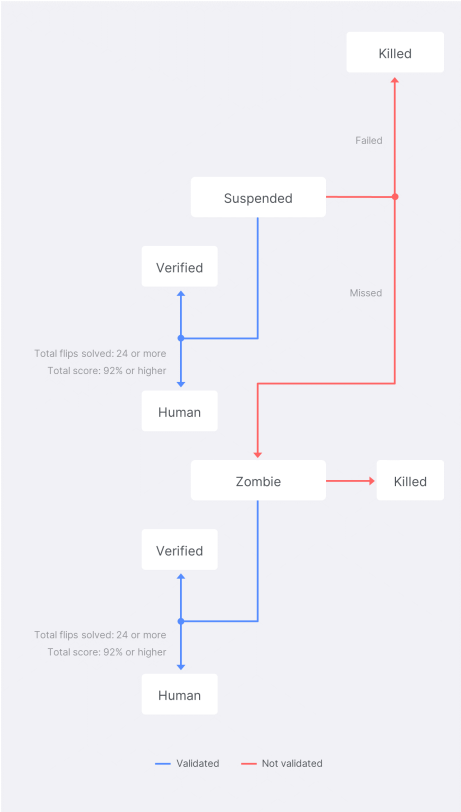
Zombie

A verified cryptoidentity that has missed two validation sessions is equal to a Candidate.

Killed

The account is not part of the network anymore.





Selling cryptoidentity

Technically, an identity can be sold and bought. However, the Idena protocol introduces economic incentives to prevent participants from doing that. A person who sells their identity can simply kill the identity afterwards to unlock their frozen coins (frozen coins accumulate for each identity as a part of UBI and cannot be spent while the identity is valid).

To sell an identity, the seller provides a copy of the identity's private key. The buyer cannot be sure that another copy of the private key will not stay with the seller. Thus, the private key enables the seller to kill the identity at any time, and the buyer would not have an economic reason to buy identity.

Cryptoidentity validation criteria

To get validated, you need to meet these three requirements during each validation session:

Your current short validation session's score should be 60% or more. Your total score for the last 10 short validations (including the current validation session and all the previous ones) should be 75% or more. Your current long session's score should be 75% or more.

In addition, you need to solve flips both correctly and fast. The first 6 flips must be solved in less than 2 minutes.

Stake wallet

Every validated identity in Idena has two wallets: the Idena wallet and the stake. The stake is like a pension account: 20% of all Idena rewards (mining and validation rewards) accumulate in the stake, while the remaining 80% goes directly to Idena wallet.

Idena does not use the stake for governance purposes.

The stake of validated identity or identity with status `Suspended` or `Zombie` can be replenished. The stake cannot be spent while the account is valid. The stake can be withdrawn to the Idena wallet only upon voluntary termination of the identity.

Losing stake

If identity is killed by the protocol, then a part or the entire stake gets burnt depending on the age and status of the identity: identities receive stake protection according to the stake protection implemented with IIP-4.

The coins stored on normal Idena wallets can not be burnt in any cases.

Validation failure stake protection

This protection affects identities that fail a validation session (not when they miss it).

Age	Identity status	Validation	Share of stake burnt	Identity status after validation
0	Candidate	Fail	100%	Killed
1	Newbie	Fail	100%	Killed
2+	Newbie	Fail	100%	Killed
any	Verified	Fail	100%	Killed
any	Human	Fail	0%	Suspended
4	Suspended	Fail	100%	Killed
5	Suspended or Zombie	Fail	5%	Killed
6	Suspended or Zombie	Fail	4%	Killed
7	Suspended or Zombie	Fail	3%	Killed
8	Suspended or Zombie	Fail	2%	Killed
9	Suspended or Zombie	Fail	1%	Killed
10+	Suspended or Zombie	Fail	0%	Killed

Missing validation stake protection

This protection affects identities that do not show up for a validation session.

Age	Identity status	Validation	Share of stake burnt	Identity status after validation
0	Candidate	Miss	100%	Killed
1	Newbie	Miss	100%	Killed
2+	Newbie	Miss	100%	Killed
any	Verified	Miss	0%	Suspended
any	Human	Miss	0%	Suspended
any	Suspended	Miss	0%	Zombie
5	Zombie	Miss	5%	Killed
6	Zombie	Miss	4%	Killed
7	Zombie	Miss	3%	Killed
8	Zombie	Miss	2%	Killed
9	Zombie	Miss	1%	Killed
10+	Zombie	Miss	0%	Killed

Discrimination of identities with the Newbie status

Only 20% of earned coins is mined to the main wallet for Newbies. The rest 80% is mined to the stake: in total 60% of earned coins is temporary locked in the stake until a Newbie becomes Verified.

60% of earned coins will be sent back to the main wallet once a Newbie becomes Verified.

Newbies cannot terminate their identities to withdraw the stake.

Newbies cannot participate in the governance of the network. While adresses with this status can get rewards for mining and participating in oracle votes, their votes are not counted and do not make a difference in the final outcome of a voting: they cannot influence a hard fork voting or an oracle voting.

Invitations

To create a cryptoidentity, an individual should receive an invitation code from a validated participant of the network and use the code to apply for validation.

New invitations can only be sent out by validated nodes. The number of new invitations per node is limited and decreases as the network grows, while the total amount of generated invitations gets larger.

The core Idena team is also granted to issue a limited number of invitations per epoch to support the growth of the network.

The pace of network growth is restricted to minimize the probability of a Sybil attack.

Selling and buying invitations

The Idena protocol introduces incentives to prevent participants from buying and selling invitations. The person who sells an invitation can kill the invited participant before they pass the first validation and their status is "Newbie". The seller can double-spend the invitation by selling it multiple times. Invitations should be granted for free to trusted people only (relatives, friends, and so on).

Distribution of invitations

The targeted number of invitations in the network is calculated as 50% of the network size after each validation (Idena foundation invitations remaining extra).

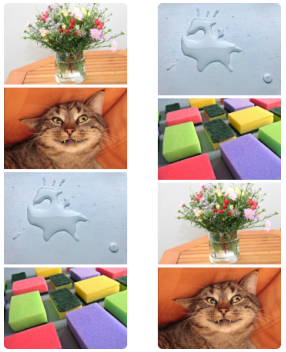
Invitations are distributed as follows:

- Identities with the Human status get one invitation starting with the highest Total score.
- If there are non-distributed invitations left, identities with the Human or Verified status get one invitation starting from the highest total score.

- After the distribution, the minimal Total score of those entitled to receive invitations is known.
- All identities with this minimal Total score receive invitations. If needed, additional invitations are issued by the Idena protocol to cover the demand.
- The core Idena team is granted to issue a limited number of invitations per epoch to support the network growth. The number of available invitations for the foundation address is limited to `max(500, NetworkSize*0.1)`

Flips

Idena proposes the Flip Challenge, a language-neutral AI-hard test that conveys narrative rather than semantic meaning. A flip, "Filter for Live Intelligent People," utilizes four images. To solve a flip, the participant chooses between two sequences of these images, only one of which makes narrative sense. The other one is deliberately distorted so that the picture sequence does not convey linear story information.



Example of a flip: a meaningful story (left) and a meaningless sequence of pictures (right)

A flip is not an IQ test but a test for common sense. A flip is submitted without the right answer. The network comes to a consensus about the right answer after the validation session. If consensus is not reached, then the flip is disqualified. Answers for disqualified flips are not counted.

> Try to test yourself to check whether you are bot or not.

To make a flip truly AI-hard and to avoid the need for a trusted third party, flips must be human-generated. In Idena, flips are created by validated participants. The flips are stored as encrypted data in the network before validation, and then they are algorithmically distributed.

The network reaches consensus on flip answers, scores accuracy, awards coins for each valid flip, and approves validated identities.

If consensus on a flip is not reached, then the flip is disqualified. Answers for disqualified flips are not counted. Users creating meaningless flips or spam or flips with inappropriate content will be subject to negative consequences.

Flip creation flow

Flips are created only by validated identities:

- The participant receives two keywords randomly selected by the protocol as associative hints to think up a story within the general template of "Before – Something happens – After."
- The participant uploads four images from their device or from the Internet to tell a story based on the two keywords.
- The participant creates an alternative – a meaningless sequence of the same four images.
- The participant submits the pair of sequences to the network.
- The flips are stored as encrypted data in the network before validation.

Flips submission requirements

Newbie, verified and human accounts must submit flips before the next validation ceremony. Not submitting flips is equal to missing a validation.

Candidates, suspended accounts, and zombies do not submit flips for the validation ceremony.

Flip distribution

Flips are distributed randomly within each shard, with one important exception: identities are not permitted to solve flips created by themselves.

Flip keywords

Two random keywords selected from a dictionary are a sort of associative hint for stimulating users' creativity. Users are required to use them for two reasons. First, doing so helps to ensure the non-repeatability and unpredictability of flip types, which makes flips AI-resistant. Second, it

enables the Idena protocol to detect and punish protocol abuse such as submitting a number of random pictures instead of a flip or the same flip repeatedly.

Network participants must create flips relevant to the suggested keywords. The relevance of the flip to the keywords is tested during the long qualification session. Participants who create flips that are irrelevant to the keywords are penalized by the protocol. Identities will be killed for repeatedly ignoring keywords when creating flips.

Flip consensus

The network comes to the consensus about the right answer after the validation session. If consensus is not reached, then the flip is disqualified. Answers for disqualified flips are not counted, and the authors of these flips are not rewarded.

Flips reporting system

Users should report the flip when:

- One of the keywords is not relevant to the flip
- One should read the text in the flip to solve it
- Flip has an inappropriate content
- Flip has numbers or letters or other labels on top of the images indicating their order

The number of flips that can be reported is limited to 1/3. So participants are motivated to pick which flip to report first relying on objective criteria (e.g. both keywords relevance).

Every successful report of a flip is rewarded: The reward for the reported flip which is not paid to the flip creator is distributed between the committee members who reported the flip.

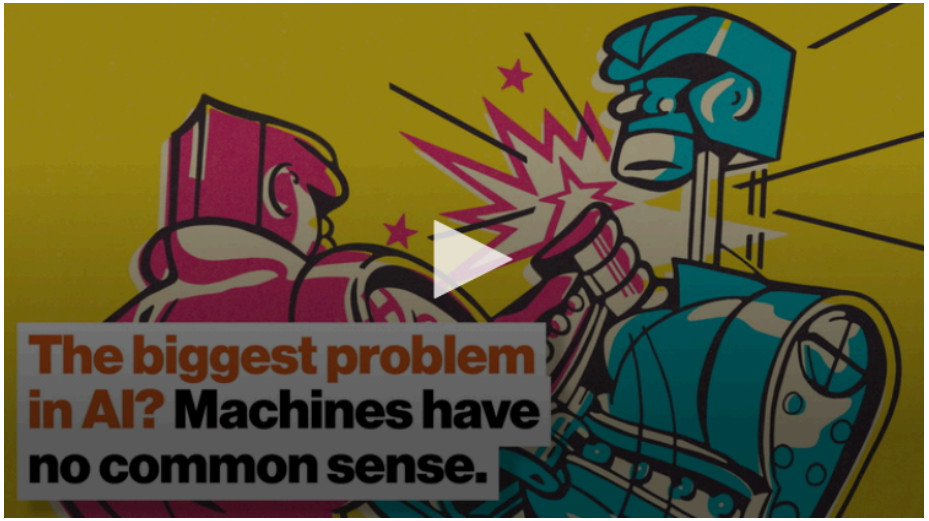
Can AI attack flips

We consider AI as an important part of the Idena project and announced a contest for AI researchers and practitioners with a $55,000 reward cascade to develop an open AI instrument. The AI instrument developed as the result of the contest will be integrated into the Idena app for flip patterns detection. This will prevent users from submitting flips which AI can solve.

Flips encryption

Each flip is available only for those participants who solve it during the validation session. There are around 10-15 persons who see it. The flips that have been used for validation are encrypted: Only 2 out of 4 images of a flip are publicly available to make it impossible to easily collect huge datasets.

Why machines have no common sense



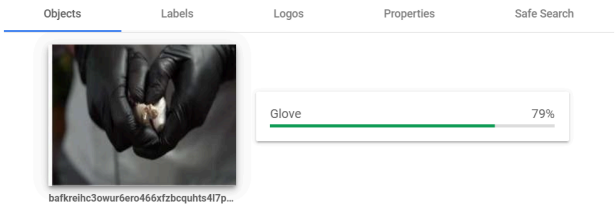
AI-resistance of flips

Adversarial attacks can be applied to the flips to prevent AI from solving them. Since the flip is a common sense test there are two types of adversarial attacks possible: 1) Adversarial perturbation added to the images 2) Adversarial nonsense image added to the flip instead of one of the images.

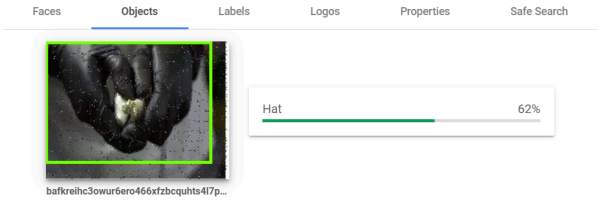
1. Adversarial perturbations

Adversarial perturbations can be added for each of the 4 images of a flip to make it harder for AI to classify the images.

Adversarial perturbations applied to the images of the flip



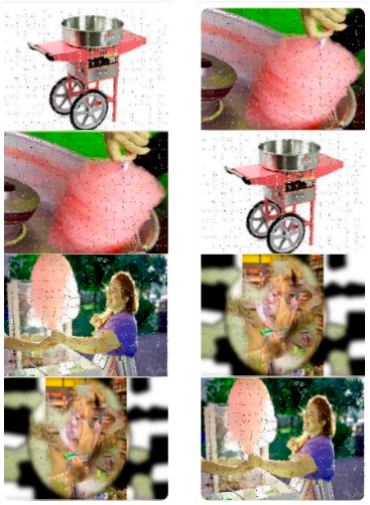
Google Vision result for the original image: Glove



Google Vision result for the image with adversarial perturbation: Hat while original image is classified as Glove

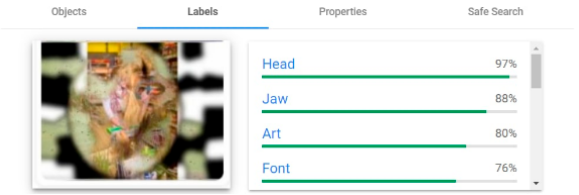
2. Adversarial nonsense images

Adversarial nonsense images can be used to make it harder for AI to determine which sequence of images makes sense.



A flip with an adversarial nonsense image

Nonsense images added into flips do not stop people from solving them. In contrast, it makes it harder for AI to solve the flips.



Nonsense images are classified as meaningful

Meaningful classification of the nonsense image leads to an unpredictable outcome for an AI that solves the entire flip based on the wrong image classification data.

Idena blockchain

The public blockchain structure is used to store the state of validated identities, implement cryptoeconomic incentives for network participants, and enable transactions of the native coin enriched with additional metadata (such as P2P-encrypted messages). Every full node corresponds to one validated person with an equal chance to be rewarded for the minting of new blocks and equal voting power in the consensus and governance process.

BFT consensus

Idena implements a Proof-of-Person Sybil control mechanism and committee-based consensus with fast finaility.

Validated participants have equal voting power to produce blocks and validate transactions. Randomly selected participants generate block proposals and broadcast them into the network. A random committee is selected to reach consensus about whether to include a block into the blockchain.

Identities discrimination

Some validated participants can be discriminated against, resulting in their votes not being counted in BFT consensus, Oracle votes, and network governance (hard fork votes).

The following are the types of discriminated identities:

- Identities with `Newbie` status
- Identities delegated to pool (the pool address has 1 vote regardless of its size)
- Undelegated participants who exited the pool less than 3 epochs ago
- Identities having the stake below the threshhold of 0.5% `* median_top100` , where `median_top100` represents the median stake of top 100 accounts.

Scalability

Unlike many blockchains that utilize centralization to increase capacity, we solve the scalability problem by exaggerating decentralization. It might be considered as a counterintuitive approach because of the well-known “Scalability-Security-Decentralization” trilemma. However, Idena offers decentralization-based scalability without sacrificing security.

Idena provides a secure way to run multiple sub-chains in parallel driven by different sets of independent participants in a process called sharding. A network with millions of nodes driven by diverse people could be safely split into thousands of groups (shards) processing transactions at the same time.

Decentralization

The Idena protocol formalizes the notion of the human on the blockchain. It brings decentralization to a new level and supports the creation of a fair consensus by avoiding network centralization despite the nature of capital to concentrate. The Idena network is decentralized thanks to the sub-linear economy and the fact that each node is connected to a cryptoidentity.

Mining

Idena enables democratic access to mining: Neither expensive mining hardware nor a bunch of money for stake is needed, but rather an average laptop that is online.

All validated participants are encouraged to do useful work for the network (hosting their nodes, creating and solving flips, inviting new users, and so on). This resource sharing is rewarded with a universal basic income (UBI).

Transaction fees

The transaction fee is calculated automatically by protocol. The fee goes up or down based on how full the previous block was, targeting an average block utilization of 50%. When the previous block is more than 50% full, the transaction fee goes up proportionally. When it is below 50% usage, fees go down. A user can specify the maximum fee limit for the transaction.

```
transactionFee = currFeeRate x transactionSize

currFeeRate = max(
     1e-16,
     0.1/networkSize,
     prevFeeRate*(1+0.25*(prevBlockSize/300Kb-0.5))
    )
```

90% of paid fees are burnt. The rest 10% are paid to the block proposer.

Smart contracts gas costs

In addition to transaction fee per byte a gas consumption has to be paid when a smart contract is called. GasCost is calculated as a total amount of gas consumed by the smart contract operations multiplied to the current `GasPrice`. `GasPrice` is calculated automatically by the protocol. The minimum `GasPrice` is: GasPrice= 0.01/NetworkSize.

Validation ceremony transactions

Validation ceremony transactions are not charged. However, they affect the fee rate because of the block consumption.

Idena smart contracts

Idena contracts are executed in Wasmer runtime.

> **TIP**
> Any language that compiles to WebAssembly (Wasm) can be used for developing contracts.

Read more about Idena smart contracts.

Predefined contracts

Predefined contracts built-in into the Idena node code (can be changed with hard fork updates)

OracleVoting

The Idena network can provide the Oracle voting service to anyone who sets a high enough reward for oracles and correctly formulates a question. The Oracle voting mechanism is flexible. In order for your voting to be successful, define the purpose of getting an oracle service.

1. Oracle voting to certify a fact Oracles can certify a fait accompli (an accomplished fact). Such an Oracle voting may unlock the coins locked by another smart contract (e.g. OracleLock). For correct voting, the fact to be confirmed must be generally known or verified by several sources of information. To prevent a possible attack on voting, a high threshold for consensus among voters is set to prove facts. Oracles who vote against the majority are penalized.
2. Oracle voting for governance Oracle voting may unlock the coins locked by another smart contract (e.g OracleLock, RefundableOracleLock), depending on their subjective opinion. In some cases, such voting may not lead to a consensus. Penalization of oracles for voting outside the majority is not used in such a voting. However, if a consensus is reached, then those oracles who voted in the majority will be rewarded. If no consensus has been reached (no decision has been made), then all oracles who have voted will be rewarded, regardless of the vote cast.
3. Oracle voting as a simple poll Oracles can vote for any option. Rewards will be paid to everyone regardless of the outcome of the vote.

You can participate in voting if you are a validated participant and receive voting rewards. Rewards can be set either by those who create the votings, or by other smart contracts. You can also create your own voting, for example:

OracleLock

OracleLock is a non-refundable smart contract that locks coins until a decision is made by oracles. If the voting result matches the expected value, coins are transferred to address A, otherwise to address B. Both addresses have to be specified beforehand.

- Example: The contractor promises to complete the work by a certain date. The customer creates an oracle voting in order for oracles to vote in the future whether the work is done. The customer blocks the money on the OracleLock contract. If the result of oracle voting confirms that the work is done, the money is transferred to the contractor. Otherwise, the money is sent back to the customer.

RefundableOracleLock

RefundableOracleLock is a refundable smart contract address that can lock coins from multiple users until a decision is made by oracles. It works similarly to OracleLock: if the voting result matches the expected value, coins are transferred to address A (if specified), otherwise to address B (if specified). However, a refund is provided to all users if the destination address A or B is not specified or oracle voting fails to reach a consensus. The amount of the refund is equal to the initial deposit or proportional to the initial deposit if the RefundableOracleLock address has been funded additionally.

- Example 1: The contractor promises to complete the work by a certain deadline. The community is ready to fund the work. An oracle voting is created so that oracles at some point in the future confirm whether the work is done. Community members fund the work by

depositing money from different wallets to RefundableOracleLock. If the result of the oracle voting confirms that the work is done, the money is transferred to the contractor. Otherwise, all contributors get a refund.

- Example 2: Prediction Market. An oracle voting is created so that oracles at some point in the future confirm the occurrence or non-occurrence of the event. Bets on the occurrence or non-occurrence of the event are locked on two linked RefundableOracleLock contracts. According to the results of the oracle voting, one of the two contracts will be the RefundableOracleLock-winner and the other will be the RefundableOracleLock-loser. All money locked on the RefundableOracleLock-loser contract is sent to the address of the RefundableOracleLock-winner contract. After that, the money from the RefundableOracleLock-winner is returned to the winning users in the form of a refund in proportion to the bets made.

Multisig

A multisignature wallet address with specified M and N locks coins. In order to send the coins from the multisig, M specific participants out of N have to provide their signatures.

TimeLock

Smart contract locks coins on the smart contract address until the specified time. Once a newly mined block has a timestamp greater or equal to that time, the coins can be transferred to any address specified by the owner.

Edit this page

Flip challenge

We consider AI as an important part of the Idena project to improve the flip challenge and announce a contest for AI researchers and practitioners with a *$55,000* reward cascade to develop an open AI instrument.

We welcome AI researchers and practitioners to develop an open source AI instrument for solving flips. Idena will award the following prizes (paid in iDNA, the Idena blockchain coin) to the first individual or a team to break respective accuracy in solving flips using with a verifiable proof:

Minimum accuracy	Prize	Cascade prize	Status
71%	$1,000	$1,000	No winner
72%	$2,000	$3,000	No winner
73%	$3,000	$6,000	No winner
74%	$4,000	$10,000	No winner
75%	$5,000	$15,000	No winner
76%	$6,000	$21,000	No winner
77%	$7,000	$28,000	No winner
78%	$8,000	$36,000	No winner
79%	$9,000	$45,000	No winner
80%	$10,000	$55,000	No winner

Flip Challenge Rules

The applicant that will be able to show consistent accuracy (average for 3 epochs) will receive the corresponding prize cascade. For example, if the average accuracy reached is 72.5% the prize cascade of $1,000+$2,000 =$3,000 (equivalent amount in iDNA) will be paid.

In case if 2 or more algorithms apply at the same testing time the prize amount will be paid on first come first serve basis according to the accuracy reached. For example, if there is the first participant who reached 72,5% and the second one who reached 74% then the prize cascade of $3,000 will be paid to the first participant and $3,000+$4,000=$7,000 will be paid to the second participant.

Eligible AI algorithms should provide friendly API, be open source, cross-platform and must work without internet connection. AI instrument will be integrated into the Idena app for flip patterns detection.

AI should be trained on the dataset of flips that currently available in the Idena blockchain explorer. Idena team will use the limited number of invites to collect out of sample flips for contestants' AI testing.

Flip challenge committee: The contest is designed and administered by the Idena team.

Protocol: to be specified

The Idena team reserves the right to cancel or amend the flip challenge and these rules and conditions.

Edit this page

Premint, funding and vesting

The Idena blockchain has got a premint intended to be used to bootstrap core development, raise funds, and help spread the word. The Idena core team would like to cultivate such an ecosystem where the market value of Idena coin (iDNA) is driven by the fundamental demand for its utility: Advertisers will have to purchase iDNA on a market and burn the coins to compete for the network attention. Burning both preminted and minted coins will lead to the sustainable economics of the Idena network.

Total premint size: 36,000,000 iDNA

Premint structure:

- Core team allocation: 17,250,000 iDNA
- Early investors allocation: 7,065,000 iDNA
- Ambassadors fund: 365,000 iDNA
- Reserved for 2020 runway funding: 3,000,000 iDNA
- Reserved for 2021–2022 runway funding: 8,320,000 iDNA

To protect the market price, premined coins of the core team and early investors are to be vested as follows:

Core team fund:

- 1/3 vested for 3 years: 5,750,000 iDNA
- 1/3 vested for 5 years: 5,750,000 iDNA

Early investors:

- 1/3 vested for 1 year: 2,355,000 iDNA
- 1/3 vested for 2 years: 2,355,000 iDNA

Core team vested coins are locked with `TimeLock` smart contracts. See actual distribution in the Idena blockchain explorer.

Foundation wallet (DAO)

The Foundation wallet is designed to fund Idena community-driven development and Idena marketing campaigns. It accumulates 5% of the minting and rewards for invites issued by the core team.

The core team controls the foundation wallet in a centralized way until governance mechanisms are proposed and implemented.

Wallet address: 0xcbb98843270812eeCE07BFb82d26b4881a33aA91

Zero wallet (DAO)

The zero wallet is designed to fund impact projects proposed by the Idena community. It accumulates 1% of all minted coins. Currently the wallet address is locked. There is no private key for the zero wallet address: The network must reach consensus in order to spend the funds. Governance mechanisms for zero wallet fund allocation are to be established in the future.

Wallet address: 0x0000000000000000000000000000000000000000

Economics of the iDNA

All validated participants are encouraged to do useful work for the network (hosting their nodes, creating and solving flips, inviting new users, and so on). This resource sharing is rewarded with iDNA Coins minting. Total minting is capped at 51 840 iDNA per day depending on the actual number of blocks produced by the network. It includes mining reward (paid every block) and validation session reward (accumulated during epoch and paid at the end of every validation session):

Total minting cap per day	**51 480 iDNA**
Mining reward cap per day	25 920 iDNA (50%)
Validation session reward cap per day	25 920 iDNA (50%)

Mining reward is capped at 25 920 iDNA per day. It includes block proposer reward (paid to block proposer) and block committee reward (distributed to members of final committee validating the block). The block reward is split between the block proposer and the block committee according to IIP-5.

Mining reward cap per day	25 920 iDNA
Block reward	6 iDNA
Minimum block time	20 sec
Maximum number of blocks per minute	3
Maximum block size	300 Kb
Maximum number of blocks per day	4 320

Validation session fund is capped at 25 920 iDNA per day. It accumulates daily and gets distributed at the end of validation session as follows:

Total rewards	Share
Staking rewards	18%
Candidate rewards	2%
Flip rewards	15%
Extra flip reward	20%
Invitation rewards	18%
Reports rewards	15%
Idena foundation payouts	10%
Zero wallet fund	2%
Total	**100%**

Staking reward fund

The staking reward fund is distrubuted among all validated identities depending on their stake size (proportional to stake$^{0.9}$)

Candidate reward fund

The candidate reward fund is distributed equally to new users for passing their first validation.

Flip reward fund

The flip reward fund is distributed equally to all participants proportionally to the number of their qualified flips and their grades. Non-qualified flips are not paid for.

The flip grade is determined by the votes of the committee members. During the long session committee members can vote as follows:

Code	Vote	Desciption
0	`None`	Do not approve flip
1	`Reported`	Report the flip
2	`GradeD`	Approve flip with a basic reward
3	`GradeC`	Approve flip with a basic flip reward increased `2` times
4	`GradeB`	Approve flip with a basic flip reward increased `4` times

Code	Vote	Desciption
5	`GradeA`	Approve flip with a basic flip reward increased `8` times

Default flip grade is `GradeD`. At least `1/3` of committee members should approve the flip to increase the flip grade. Otherwise default grade is used. The flip grade is calculated as the average grade among the votes of committee members who approved the flip.

Example:

```
Committee size: 10
Votes: [0, 1, 2, 2, 3, 4, 5, 5, 5, 5]
Flip grade = Round(Avg(2, 2, 3, 4, 5, 5, 5, 5)) = 4 //`GradeB`
```

Extra flip reward fund

The extra flip reward fund is distributed to those authors who created 4 or 5 qualified flips which are not reported. The reward is calculated proportionally to the author's stake$^{0.9}$ (see more details here).

Flips with minimal grades are selected as extra flips.

Invitation reward fund

The invitation reward fund is distributed to all identities whose invitations have been validated. The rewards are calculated proportionally to the size of the inviter's stake to the power of 0.9 and the time when the invite is activated.

The invitation rewards are paid out for 3 successful validations in a row, with part of the reward sent and locked in the invitee's stake.

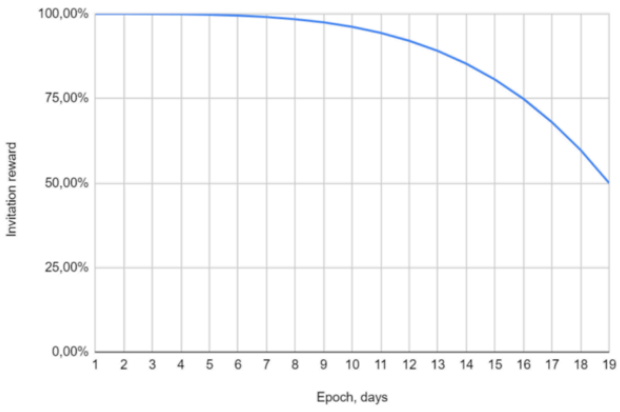
Epoch	Inviter's reward	Invitee's reward (staked)
1	20%	80%
2	50%	50%
3	80%	20%

80% of the reward that the inviter receives goes to the wallet, and 20% goes to the stake.

The invitee's reward is blocked in the stake and is not returned to the main wallet when the Verified status is reached. This encourages newcomers to run a node and get mining rewards. If the invitee is terminated or if it is killed due to missing or failing validations before reaching age 10, the entire sum of invitee rewards is burned.

If the inviter was penalized for a reported flip, the invitation rewards are not paid neither to the inviter nor to the invitee. If the invitee was penalized for a reported flip, the invitation reward is not paid to the invitee.

The invitation reward also depends on how early in the epoch the invitation is activated. The later the invitation is activated, the lower the reward. The reduction factor *k* is calculated for each invitation as $k = 1 - t^4 \cdot 0.5$, where $t \in [0..1]$ is the amount of time that has passed from the start of the epoch to the moment of the activation.



Epoch, days	Invitation reward
1	100,00%
2	99,99%
3	99,97%
4	99,90%
5	99,76%
6	99,50%
7	99,08%
8	98,43%
9	97,48%
10	96,16%
11	94,38%
12	92,04%
13	89,04%
14	85,26%
15	80,58%
16	74,86%
17	67,96%
18	59,72%
19	50,00%

Invitation rewards for the 2nd and 3rd validation are not paid to the Idena foundation.

Reports rewards fund

The flip reward fund is distributed equally to all validated participants proportionally to the number of successfully reported flips during the long session.

Idena foundation

Idena foundation rewards are paid to Foundation wallet (DAO)

Zero wallet fund

Zero wallet fund is paid to Zero wallet (DAO)

Transaction fees

The transaction fee is calculated as follows:

```
txFee = gasPrice * txSize * 10 + gasPrice * gasUsed
```

> **READ MORE**
>
> Read more about transaction fees

`gasPrice` is estimated automatically by protocol based on the average occupancy of blocks, targeting 50% fill rate. `gasPrice` goes up or down based on how full the previous block was, targeting an average block utilization of 50%. When the previous block is more than 50% full, the transaction `gasPrice` goes up proportionally. When it is below 50% usage, fees go down.

```
gasPrice = max(
        gasPrice * (1 + 0.25 * (prevBlockGasUsed / maxBlockGas - 0.5)),
        0.01 / networkSize,
        0.000000000000000010
    )

maxBlockGas = 5000 * 1024
```

Minimum `gasPrice` is `0.01 / networkSize`. `gasPrice` can not be below `0.000000000000000010` iDNA.

Miners get 10% of transaction fees, 90% of the fees are burnt.

iDNA coin utility

There are the following cases for supply utilization:

- Transaction fees: 90% of transaction fees are burnt
- Oracle voting expenses: oracle rewards payments, smart contract stake, voting deposits
- Decentralized ads: 100% of payments are burnt
- Cryptoidentity stake: 20% of minted coins are frozen in stakes, stakes of non-validated identities are burnt
- Smart contract stake: 50% of locked stake is burnt
- Mining penalties: miners must burn coins to pay the mining penalties
- Zero wallet lock: 1% of the minted coins are frozen in the zero wallet
- The bigger the network the more coinholders will just hold newly minted coins without spending them

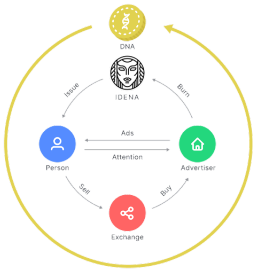
Use cases

There are various use cases that can be facilitated by the Idena network. Cryptoidentity enables such use cases as DAO, governance, quadratic funding, UBI, airdrops, accessible smart contracts, oracles, individual loans, courts, decentralized ads, censorship free publications, reputation system, etc.

Decentralized ads

Current business models of most Internet services imply the monetization of personal information collected about the user's behavior, interests, social connections, in many cases without the user's consent. The advertising industry can be changed by turning the concept of targeting upside down: There could be an onchain model of a transparent advertiser where any advertisement contains an accessible targeting specification. Advertisers (not users!) disclose

information about their target audience, and then each user's device can decide on a particular advertisement that suits them at the moment, without revealing their personal data. The user's device knows their current location, interests, gender, age, language, and more. All of these can be independently and automatically used to filter ads. The user gets the entire list of available advertisements, and it is the user (and not intermediaries such as search engines or social media platforms) who will have the right to choose what fits best. While in traditional media it is the intermediaries who benefit from ads delivery, onchain advertising leads to a model without intermediaries, in which the advertiser pays directly to the protocol, burning coins purchased on the market and thus distributing profits to all the network participants.



Advertisers have to purchase iDNA on a market and burn the coins to compete for the network attention. Burning coins will lead to the sustainable economics of the Idena network.

Fair voting in online communities

Governance is one of the most important killer apps of blockchains. DAOs effectively recreate cross-border organizational structures at miniscule administrative costs and near-zero compliance burden. However, governance mechanisms in permissionless communities can only be based on the stake of tokens; hence, they are inherently plutocratic. Large stakeholders can collude to dominate the outcome of voting, discouraging others from participation. A unique cryptoidentity (one account per person) can be used to distribute voting credits to the individual members of the community to ensure fairness. Modern voting technologies such as Quadratic Voting can be implemented to engage the crowd to participate in the collective decision-making process.

Oracles

For most use cases, smart contracts and DAOs need to be fed with factual information from the outside world. This requires oracles to supply offchain data to the blockchain. The Idena network is essentially a ready-made network of oracles. There will be mechanisms that enable every validated Idena user to have an equal chance of being selected as an oracle. Randomly chosen participants will receive information requests published by smart contracts. The selected oracles will provide the data and will stake coins to guarantee its accuracy. When the consensus on the information is reached, the oracles will be rewarded or penalized depending on the quality of the information they provided.

Serverless messenger and in-chat payments

The network of independent nodes can securely store a queue of undelivered P2P-encrypted messages. Spam attacks are prevented by assigning a minor friction in the form of a transaction fee and a decentralized storage rent fee. The native cryptocurrency of the Idena network can be used to transact value between users as a special type of message inside the P2P chat. Trustless decentralized two-way bridges are to be developed to tokenize and transact major cryptocurrencies (BTC, ETH) as tokens on the Idena blockchain.

Free speech publishing

The Idena network can be used as a decentralized storage for publications and whistleblowing information to build censorship-free publishing platforms, which are protected from bots manipulating content discovery.

Global universal basic income (UBI)

A full node of the Idena blockchain could be light enough to run on an average laptop. Participation in the network is rewarded with minting and can be considered as a form of the universal basic income sufficient to cover network services (for example, sending messages) as well as the bill for the Internet service and electricity consumed. At a certain stage the Idena network can be attractive for international organizations to distribute unconditional rewards to network participants.

Edit this page