Idena concept paper

Abstract

Idena is the first human-centric blockchain: Every node is linked to one single person with equal voting power.

Idena introduces a novel way to create decentralized anonymous personhood. It does not need any personally identifying information. Idena proves the humanness and uniqueness of its participants by running a collective time-synced online AI-hard Turing test for everyone around the globe.

This paper introduces the foundational concepts of the Idena blockchain and provides a formal specification of DNA, its native coin.

Contact information info@idena.io

Content

The problem of unique identity

Anonymous and Sybil-protected identity is a missing part in Internet applications, blockchains, and self-sovereign identity space.

The design requirements of this decentralized anonymous identity to a large extent follow the properties introduced by Bitcoin[1]:

- Global and verifiable online
- Permissionless and inclusive
- Decentralized, without reliance on trusted third parties
- Sybil-protected
- 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 as social information, rely on a centralized service, are not available in many countries, can be purchased on the market, and are easily spoofed.[2]
- 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[3], and leads to an Orwellian world.
- Biometrics relies on specific sensors and algorithms, can be faked[4], and cannot have plausible deniability.
- Self-sovereign identities (SSI) rely on trusted verifiers based on Social ID and Government ID attestation.
- Web of Trust (WoT) approaches such as BrightID[5] or Proof-of-Personhood[6] don't allow to build the global consensus about the registry of valid identities.

Decentralized anonymous identity, when developed, would enable:

- **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

[1] Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[2] Facebook banned 2.2 billion fake accounts in the first 3 months of this year. That's almost equal to the number of real people who use it.
https://www.businessinsider.com/facebook-bans-2-billion-fake-accounts-q1-2019-2019-5
[3] Counting the uncounted: 1.1 billion people without IDs.
https://blogs.worldbank.org/digital-development/counting-uncounted-11-billion-people-without-ids
[4] Fake fingerprints can imitate real ones in biometric systems – research.
https://arxiv.org/pdf/1705.07386.pdf
[5] The power of unique personhood. https://www.brightid.org/
[6] Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies.
https://www.zerobyte.io/publications/2017-BKJGGF-pop.pdf

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 identity proof (one ID 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.

- **Direct marketing and value airdrops.** 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 new business model could be based on the consensual self-monetization of personal information and proactive intentional disclosure initiated by the user. Based on such intentional information-sharing, advertisers could provide the best deals and pay the user directly to view and utilize them. Internet services and apps could distribute utility tokens, rewards, tokenized coupons, and discounts. This model would be possible only when advertisers and businesses are protected from Sybil attacks by *"random fourteen-year-old teenagers in Albania, that just have 50'000 accounts and just pretend to be a community that wants some public good funded when actually it's just buying themselves a Lamborghini."*[7]

- **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 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 identity 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 identity 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 the 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.

- **Attestation of human uniqueness for SSI.** The anonymous unique identity provider can be integrated with other self-sovereign identity systems to verify claims of uniqueness.

[7] Vitalik Buterin, Blockchain and RadicalXChange communities: better together. https://youtu.be/WIs8zjLDZrQ?t=1566

Anonymous unique identity validation flow

Idena allows for the proof of humanity and proof of uniqueness of its participants. We call it Proof-of-Person (PoP). 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.

Idena employs regular checkpoint rituals — synchronous validation sessions — to certify a participant's humanness for the consequent epoch. The validation requires the solving of *flips*: specialized puzzles that are easy for a human, but difficult for a bot.

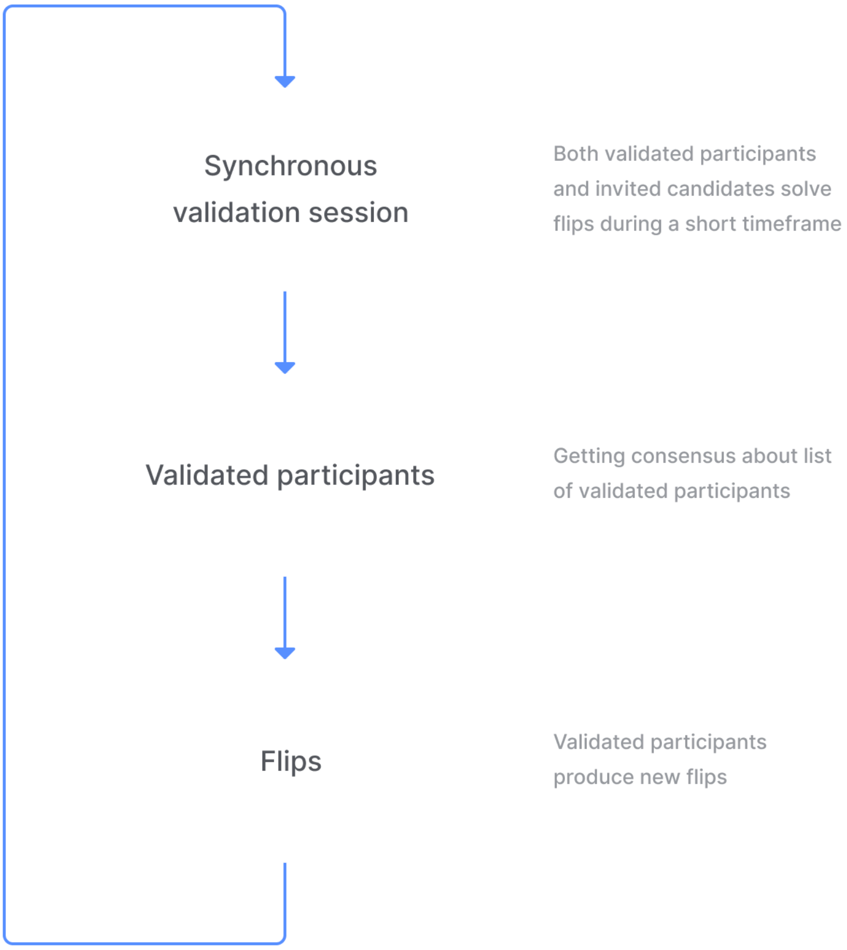
Synchronous validation session
Both validated participants and invited candidates solve flips during a short timeframe
Validated participants
Getting consensus about list of validated participants
Flips
Validated participants produce new flips

Fig 1. Idena validation flow for a single epoch

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

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.

Joining the network

To create a digital identity, 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.

Flip Challenge

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.

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.

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:

1. 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*."
2. The participant uploads four images from their device or from the Internet to tell a story based on the two keywords.
3. The participant creates an alternative – a meaningless sequence of the same four images.
4. The participant submits the pair of sequences to the network.
5. The flips are stored as encrypted data in the network before validation.

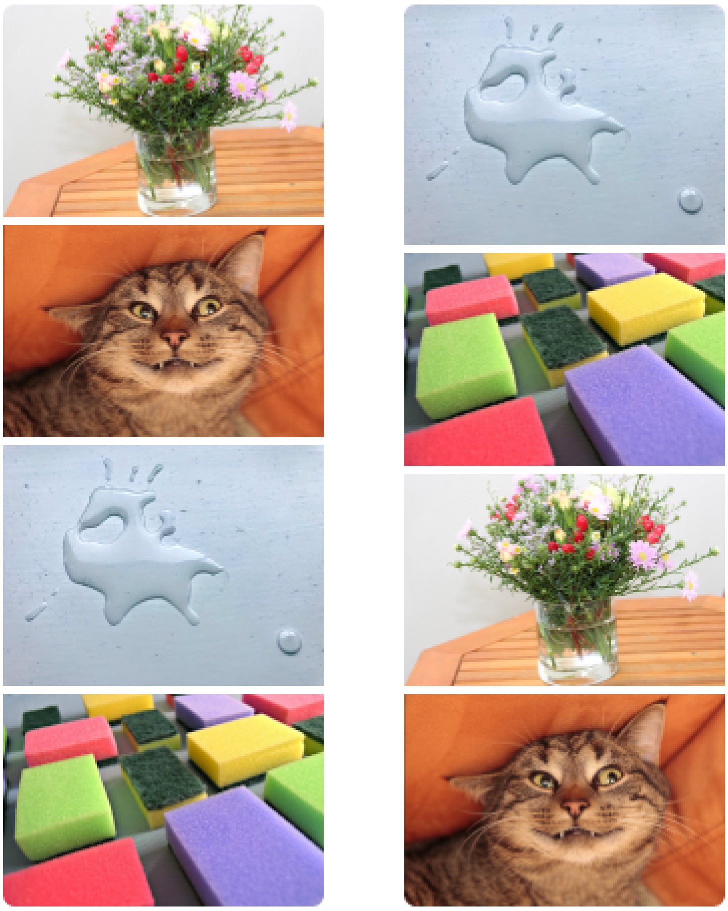

Fig.2. Example of a flip: a meaningful story (left) and a meaningless sequence of images (right) with keywords "Flowers/Sponge"

Flip distribution

Flips are distributed randomly, but with two important exceptions: First, identities are not permitted to solve flips created by themselves; and second, identities are not permitted to solve flips created by related identities. Related identities are identified by the similarity of their genome codes.

Every child identity has a genome code inherited from the parent identity that provided the invitation to the Idena network. This genome code enables Idena to identify relationships between identities. If two identities have matching genome codes, they are considered relatives. Such linked identities are not permitted to solve flips created by each other.

As the network grows, the number of people solving the same flip goes down: In a network of 10,000 users, only two different participants will have the same flip to solve. When the network reaches 30,000 users, one single flip will appear in a validation session of only one participant.

Identity status flow

The participant's identification persists for as long as the current epoch lasts. During the epoch, the validated participant 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.

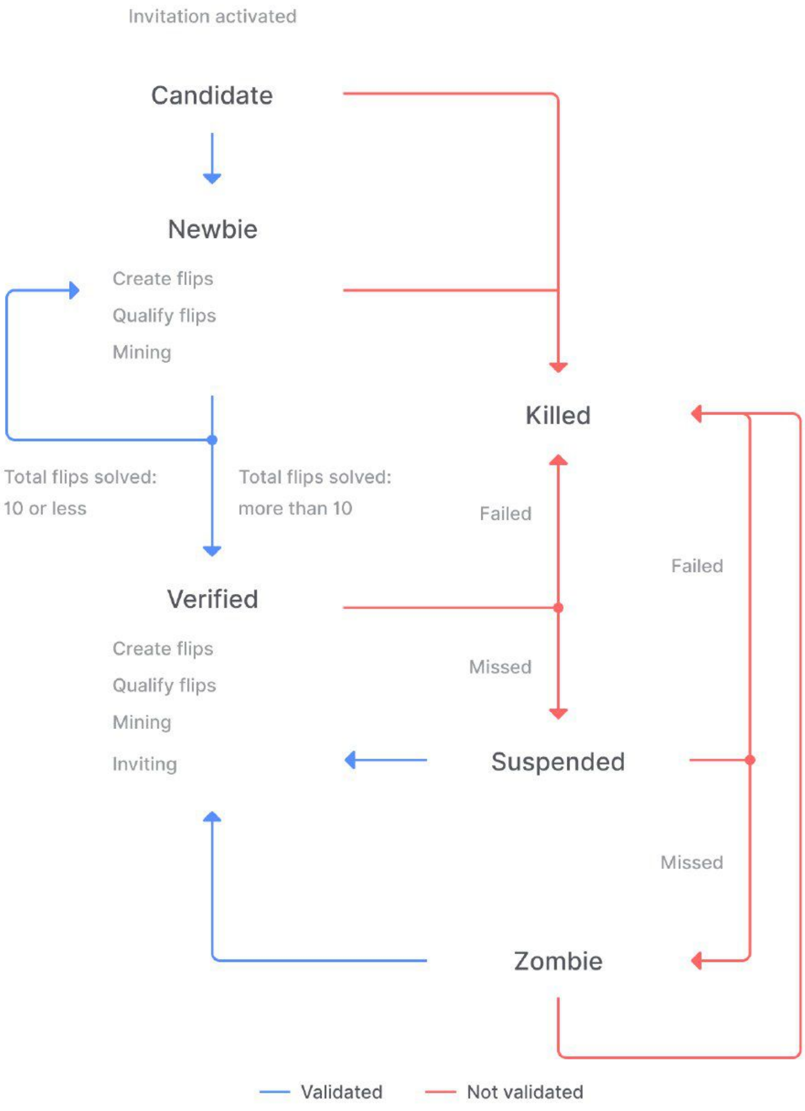

Fig 3. Identity status flow

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.

Validated identity. An identity validated at least three times in a row can do the same as a Newbie plus send out invitations and miss up to two validations in a row.

Suspended identity. A valid identity that has missed one validation session can do the same as a Candidate and can miss one validation session.

Zombie. A valid identity that has missed two validation sessions is equal to a Candidate.

Killed identity. This identity is not part of the network anymore.

Selling identity

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.

Consensus mechanism

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

Every validated participant has an equal voting power in the network 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.

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 can be safely split into thousands of groups (or *shards*) that are processing transactions at the same time.

Economics of the DNA

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 DNA Coins minting.

Total minting is capped at 51 840 DNA 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 DNA**
Mining reward cap per day	25 920 DNA (50%)
Validation session reward cap per day	25 920 DNA (50%)

Mining reward is capped at 25 920 DNA per day. It includes block proposer reward (paid to block proposer) and block committee reward (distributed to members of final committee validating the block):

Mining reward cap per day	**25 920 DNA**
Block proposer reward cap per day	8 640 DNA (~33%)
Block committee reward cap per day	17 280 DNA (~67%)
Minimum block time	*12 sec*
Maximum number of blocks per minute	*3*
Maximum block size	*1 Mb*
Maximum number of blocks per day	*4 320*
Block proposer reward (per block)	*2 DNA*
Block committee reward (per block)	*4 DNA*

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

Validation rewards	24%
Flip rewards	32%
Valid invitation rewards	32%
Idena foundation payouts	10%
Zero wallet fund	2%

Validation reward is distributed proportional to age to all validated identities, who have no flips with inappropriate content irrelevant to seed words for the session.

Flip reward fund is distributed equally to all validated identities who’s flips were qualified (proportional to number of qualified flips).

Valid invitation reward fund is distributed equally to all validated identities who’s invites were validated (proportional to number of successful invites).

Fees are estimated based on the average occupancy of blocks, targeting 50% fill rate. Miners get 10% of transaction fees, 90% of the fees are burnt.

Premint

Total preminted amount of coins is 36’000’000 DNA. It is distributed as follows:

Distribution	**%**	**DNA**
Founders & Core Team	42%	15 120 000
Seed investors	27%	9 720 000
Core team	10%	3 600 000
Ambassador program	3%	1 080 000
Reserve fund	18%	6 480 000
Total premint	**100%**	**36 000 000**

Governance

The Idena network implements various types of internal governance mechanisms:

- Network improvements proposals (soft forks)
- Network upgrade proposals (hard forks)
- Zero-wallet fund allocation proposals