The Open Network

The next gen network to unite all blockchains and the existing Internet

Primer

November 2021

v2.13

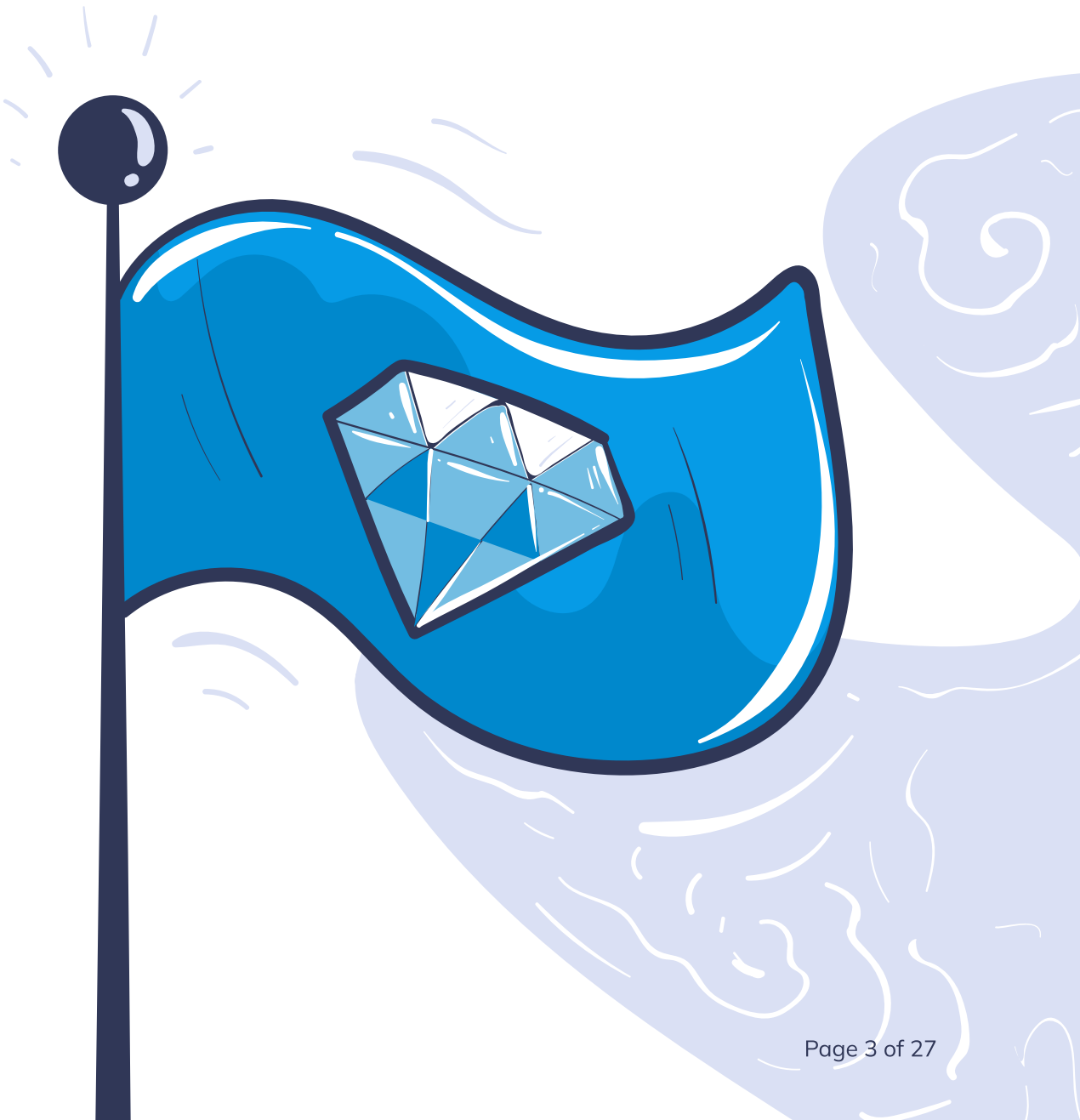
Table of Contents

Introduction

This primer outlines a vision for The Open Network: a blockchain-based network restored and continuously developed by an open-source community.

Apart from processing millions of transactions per second, TON blockchain-based ecosystem has all the chances to give rise to a genuine Web3.0 Internet with decentralized storage, anonymous network, DNS, instant payments and various decentralized services.

TON architecture is designed to enable merging all existing blockchains into a single decentralized network.



Key Components

TON Blockchain Launched

The backbone of The Open Network is a scalable multi-blockchain that is designed to process millions of transactions within seconds. It uses the Proof-of-Stake consensus and can contain up to 2^{92} accompanying blockchains.

TON Payments 90% Ready

TON Payments is a platform for micropayments and a micropayment channel network. It can be used for instant off-chain value transfers between users, bots, and other services. Safeguards built into the system ensure that these transfers are as secure as on-chain transactions.

TON Proxy 75% Ready

TON Proxy is a network proxy/anonymizer layer for TON nodes. Similar to I2P, it allows building decentralized VPN services and blockchain-based TOR alternatives to achieve anonymity and protect online privacy. Combined with the TON P2P Network and TON DNS, TON Proxy gives decentralized apps immunity to censorship.

TON DNS 90% Ready

TON DNS makes blockchain mainstream by assigning human-readable names to accounts, smart contracts, services and network nodes. With TON DNS browsing blockchain becomes similar to surfing the World Wide Web.

TON Storage 50% Ready

TON Storage is a distributed file-storage technology accessible through the TON P2P Network. Think a better version of Dropbox for simplicity. This torrent-like technology relies on smart contracts for availability and has a strong potential with regard to storing and exchanging large amounts of data.

TON Services Launched

TON Services provides a versatile platform for third-party services. It enables smartphone-like friendly interfaces for decentralized apps and smart contracts, as well as a World Wide Web-like decentralized browsing experience.

TON provides a searchable registry of decentralized services and applications.

TON Workchains 50% Ready

TON consists of the masterchain and up to 2^{32} workchains with different rulesets, i.e. different formats of account addresses and transactions, virtual machines for smart contracts and basic cryptocurrencies, etc. Yet, workchains can still interact using consistent basic rules.

Today there is a wide variety of operating blockchains that are loosely connected to one another. Current attempts to use Bridging to establish interaction between them leave much to be desired in terms of both performance and decentralization levels. TON design will allow pooling all existing blockchains into a unified decentralized network.

TON Blockchain

The heart of the platform is the unique blockchain with a scalable and flexible architecture consisting of a master chain and up to 2^{92} accompanying blockchains. Top-notch approaches and methods implemented in TON make sure it will live up to its bold promise of processing millions of transactions per second.

Infinite Sharding Paradigm

Scalability was the Holy Grail previous blockchains failed to find. TON achieves it through sharding as blockchains in it can automatically split and merge to accommodate load changes. Thus block generation speed remains unaffected by the transaction volume, no queues build up and costs remain low regardless of the demand.

Instant Hypercube Routing

Smart routing mechanisms ensure swift exchange between any two blockchains regardless of the network size. Given the logarithmic relation between data transfer time and number of blockchains in TON, scaling to even millions of chains is possible without impairing the processing speed.

Proof-of-Stake Consensus

TON relies on the advanced Proof-of-Stake consensus where validator nodes use deposit stakes to guarantee their dependability and reach consensus through a variant of the Byzantine Fault Tolerant protocol. This resource saving mechanism enables TON to focus nodes computing power on handling transactions and smart contracts further increasing speed and efficiency.

2D Distributed Ledgers

To avoid unnecessary forks, TON can grow new valid blocks on top of any invalidated blocks. This self-healing mechanism saves resources and guarantees that valid transactions are not discarded due to unrelated errors.

TON Commandments

Exchanging value should be as easy as exchanging information and blockchain technology ideally service the purpose. With this goal in mind we worded the key principles of TON design and development:

- **Speed and scalability** to process millions transactions per second, accommodating an unlimited number of active users and sustaining operations of numerous apps.
- **Intuitive user interfaces** to make blockchain about people, not geeks and nerds, to help everyone buy, store and transfer assets in a convenient, familiar way.
- **Decentralization** to ensure reliability, stability and safety and to take steps towards a safer, self-governed world.

TON Timeline

2018

Failing to find a suitable blockchain in the market to accommodate their ambitious ecosystem plans, Pavel and Nikolai Durov backed by a unique developer team embarked on creating TON: the next-gen blockchain with Gram coin.

2018

The Telegram team raised $1.7bn in a private ICO to launch Gram.

2019

Having put a huge effort into the project, the team completed design and development of the core TON components, drafted documentation.

The Telegram team launched the first TON test network in Spring 2019, then the code was open-sourced and testnet2 started on November 15, 2019.

11 Oct 2019

Out of the blue the US SEC announced an emergency action against Gram and obtained temporary restraining order against Telegram on alleged unregistered, ongoing digital token offering in the U.S. and overseas that has raised more than $1.7 billion of investor funds.

Telegram argued SEC claims were ungrounded but agreed to postpone the network and coin launch till all legal matters are resolved.

Investors accepted Telegram's suggestion to revise the launch date.

Mar 2020

Telegram threw the towel in its battle with the US regulator that prohibited the issuance of Gram. All resistance appeared to be futile.

May 2020

The Telegram team shut the project down and stopped supporting testnet2 after obtaining the court approval of settlements that involved a penalty of $18.5m. Yet, Telegram has neither denied nor accepted charges.

The company then made it up with investors and suggested a money back road-map. It was then that independent developers and teams picked up the TON flag and continued the project.

May 2020

Two developers known as Anatoliy Makosov and EmelyanenkoK initiated Newton open-source community aimed at further development and support of TON on the open source principles.

More developers who never worked for Telegram, members of the open developer community, validators, winners of public TON Blockchain Contests and crypto enthusiasts from all over the world joined them.

May 2020 — May 2021

Upon researching TON source code, architecture and documentation, Newton resumed developing in compliance with the original whitepaper and ideas.

May 2021

Testnet2 remains stable for a long time and the community votes for renaming it as Mainnet. Newton team, in turn, is renamed as TON Foundation — a not-for-proft community focused on further support and development of the network.

Toncoin History

1. When testnet2 later renamed as Mainnet was launched, 5bn coins were generated with a small fraction (1.45% of the total supply) distributed between testers and developers.

2. After the court ruling prohibiting Gram, the Telegram team gave up TON blockchain development with the most part of testnet2 coins (98.55% of the total supply) transferred to Proof-of-Work Giver smart contracts. So, mining coins is only possible through calling these smart contracts which takes a solid computation capacity.

3. At the point when testnet2 was renamed as Mainnet coins had already been organically distributed between a large number of various users. The price was determined by the cost of mining hardware.

Toncoin Factsheet

As of 15 Jun 2021

Distribution of Toncoins reminds the way coins were organically distributed in early days of the Bitcoin network. In other words, no ICOs or airdrops took place.

5BN

Total coin supply

70,172

Total account number

112M

Total validators' stake

73M

PoW Givers' holdings

16.4M

TON Foundation holdings

The annual inflation rate derived from the fundamental parameters of TON is 0.6%. This inflation represents a payment made by all members of the community to the validators for keeping the system functional.

Getting Toncoins

Hurry up
to mine before PoW Givers are not dry

Use bridge
if you have Wrapped TONCOIN in Ethereum or BSC

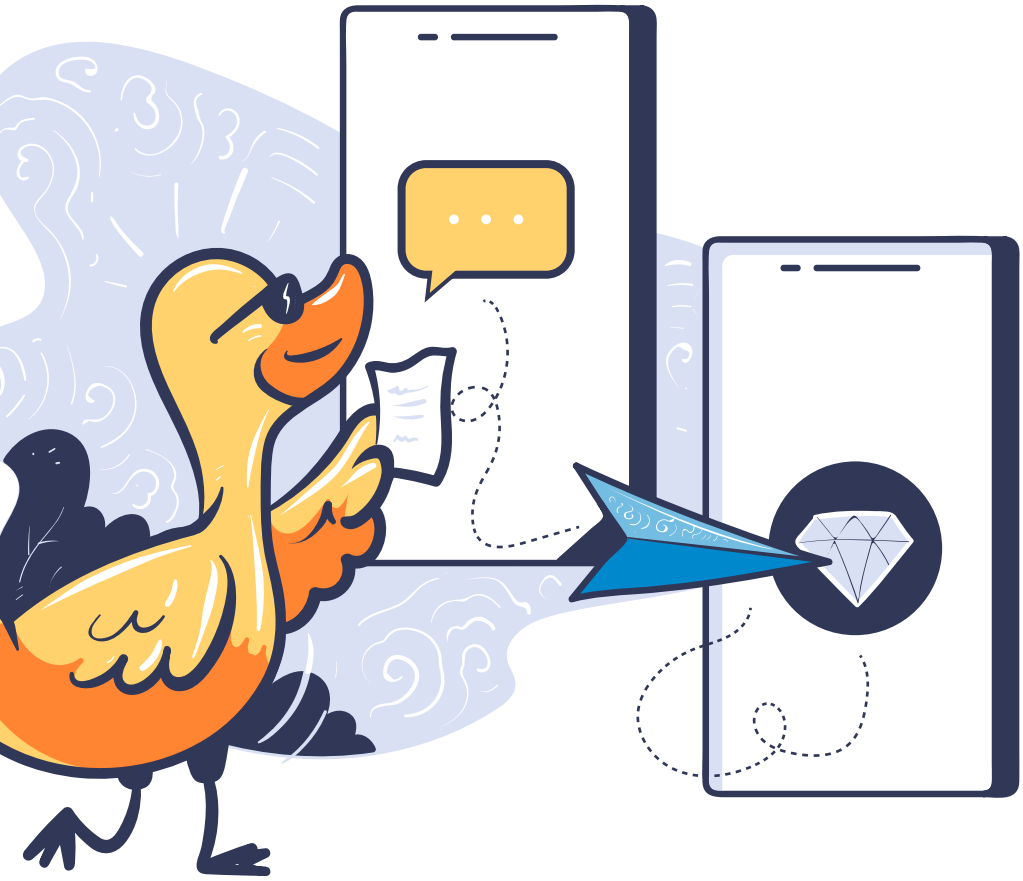
Become a validator
and get your revenues

Buy/exchange
Toncoins at third-pary services.

Wait for TON Storage, TON Proxy and TON DNS
to join them and earn coins

Toncoin Uses

As the ecosystem expands, we see a huge potential of Toncoin and numerous ways for it to work in the new economy. We expect it to go beyond a means of payment.



- Stakes deposited by validators to be eligible to validate transactions and generate new blocks and coins.
- Voting power to support or oppose changes in the parameters of the protocol.
- Income (gas) paid to validator nodes as reward for processing transactions and smart contracts under the PoS consensus.
- Loans to validators extended against a share of their reward.
- Payment for services and options implemented by TON Services, TON Storage, TON DNS, TON Proxy, TON WWW. In particular, for bypassing censorship, storing data, hiding identity, using blockchain-based domain names.

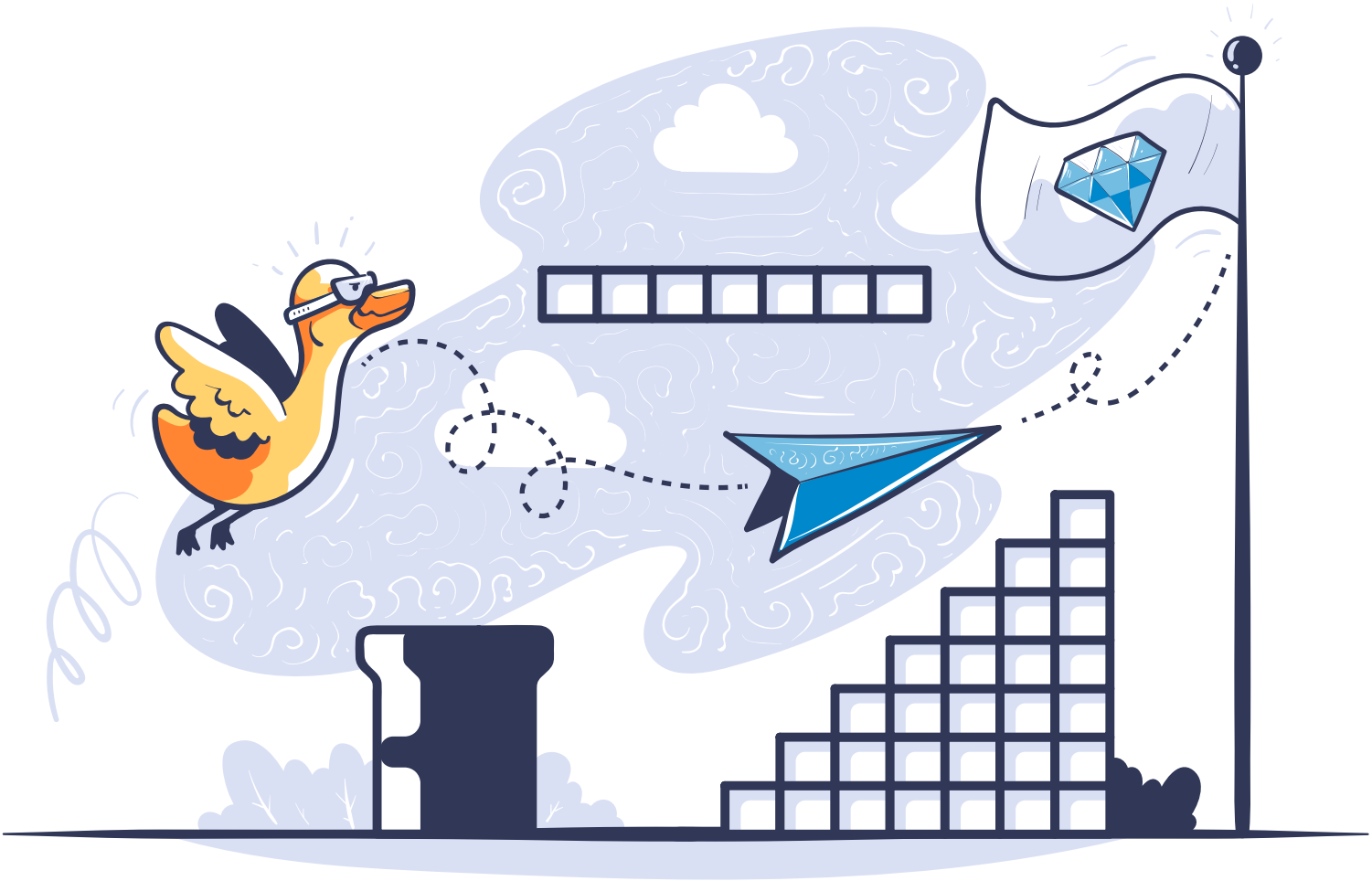
Toncoin Roadmap

Initial distribution of Toncoins was carried out spontaneously via PoW mining.

This type of distribution has obvious advantages like decentralization and equal conditions of obtaining coins for all.

Yet, there are challenges: risk of uneven distribution of coins, miner anonymity and zero knowledge of their further plans regarding the use of coins.

TON Foundation announces its **TON Nominators** component that will enable utilization of large number of Toncoin to increase the stability and scalability of TON Blockchain, while mitigating some of the threats related to PoW mining. Implementation of that component will benefit the overall network: the more coins are allocated to a more diversified group of enthusiasts who are willing to run validators, the more stable the network will get. We also expect that TON Nominators component will help to achieve further decentralization of the network: more new participants from different geographies will be able to join the network and benefit it as validators while receiving reward in Toncoins for their efforts.



TON Nominators Q4 2021

In Proof-of-Stake consensus network operations are carried out by validator nodes that verify suggested blocks and allow recording them in the blockchain.

Anyone can launch a validator node, but it takes a powerful server and a **serious** amount of Toncoins to make a stake.

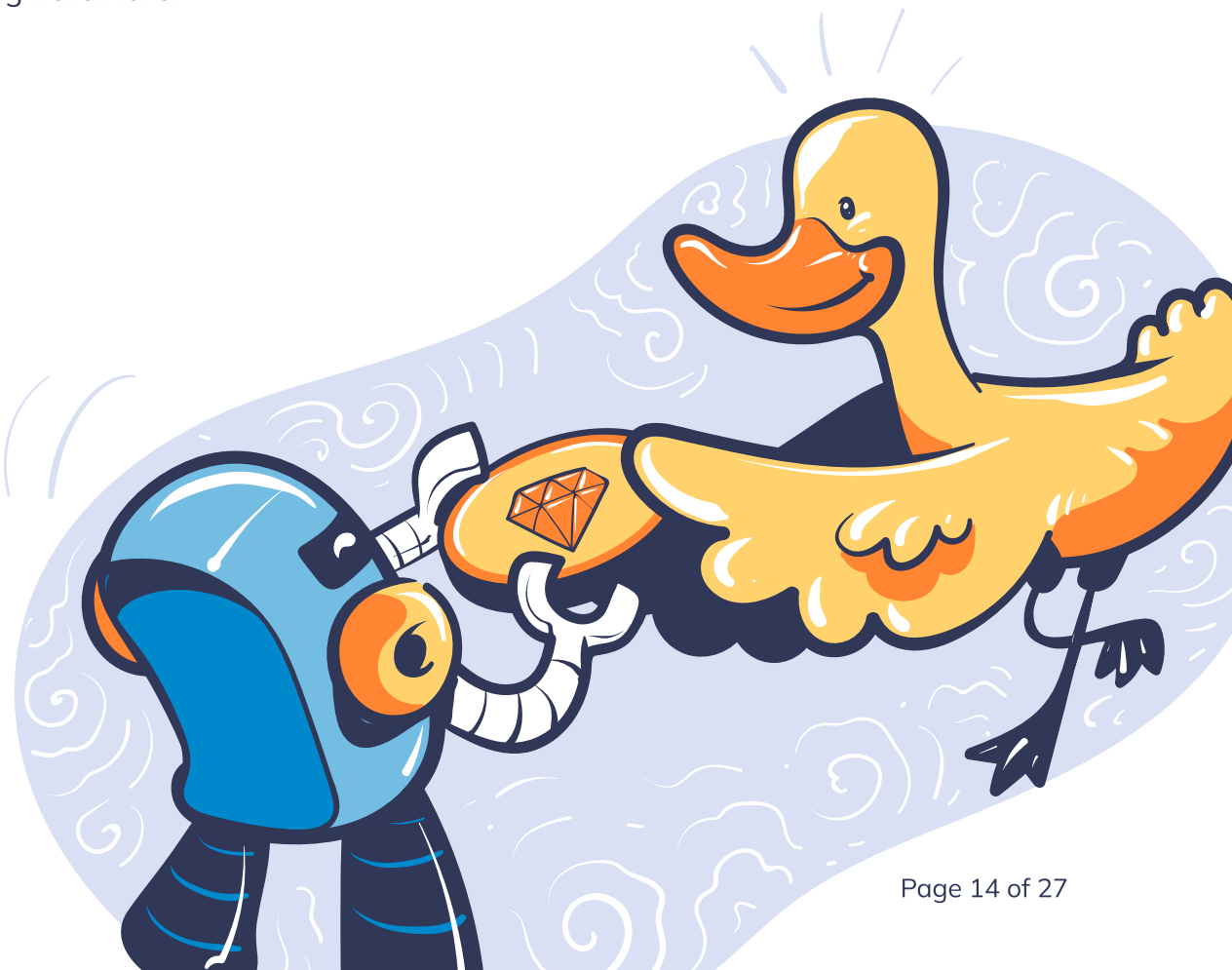
TON Nominators allows lending Toncoins to hardware owners so they could start a validator node. Validation income is then distributed between the parties involved.

~590k TON	~10k TON	60%	40%
nominator stakes	**validator stakes**	**of profits go to a nominator**	**of profits go to a validator**

for an average network stake of 600k TON

The smart-contract assures the proper use of coins and due distribution of profits in compliance with the agreed-upon conditions.

With TON Nominators one can start a validator node having less coins then needed or not having them at all. On the other hand, there is an opportunity for Toncoin holders to invest their assets and profit from validation without buying and maintaining hardware.



We envisage various service scenarios and configurations, but we expect that the most popular will be the one when a validator stakes the amount sufficient to cover potential penalties for poor work, while an investor (nominator) provides the bulk of the stake. 60% of the validation reward then goes to the investor and 40% to the validator node owner.

With more validators in the network and bigger collective validators stake, the network becomes more stable and secure.

After the launch of TON Nominators, the total number of validators may potentially top 400 with 1bn Toncoins locked in validations (about 20% of the total issue).

Note that nominators can only lend coins to owners of validator nodes, but they have no access to their hardware or software. Therefore, TON Nominators stimulates further decentralization.

TON Nominators for Bridging Oracles

TON-Ethereum and TON-Binance Smart Chain bridges resemble a small PoS-blockchain (for more details see Appendix: Bridge operation principle). Just like validator nodes, bridging oracles have stakes that guarantee their fair operations and are rewarded by transfer fees.

TON Nominators is designed to enable coin holders to lend those to owners of oracle nodes in exchange for a share in their profits.

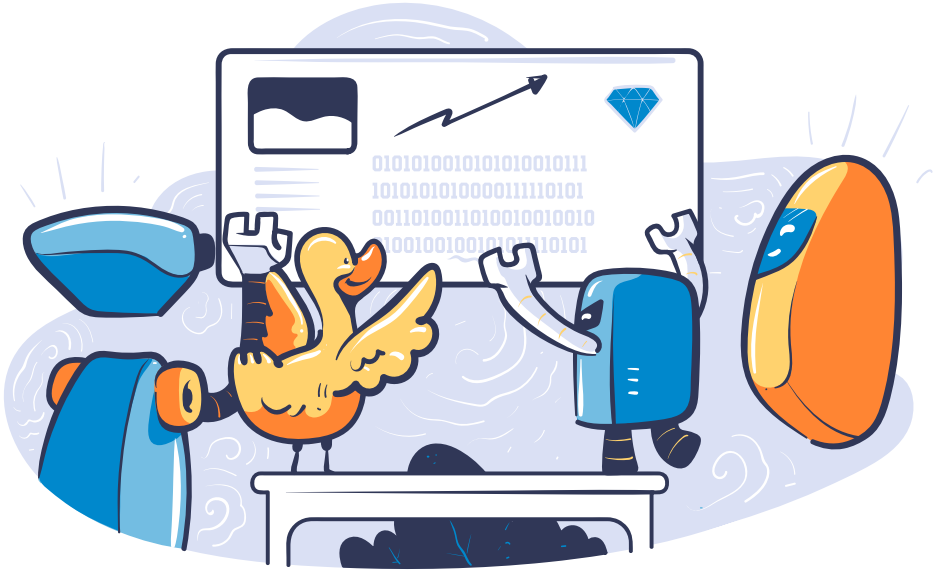
After the component is launched, the total oracles stake may potentially reach 100m Toncoins.

TON Foundation

After Telegram was forced to quit the project, the open-source developer community led by EmelyanenkoK and Anatoliy Makosov went on developing and supporting the blockchain sticking to the original whitepapers where possible.

By now over 40 independent non-incorporated developers from various geographies work on the project as TON Foundation not-for-proft community funded by donations. You can find their profiles on GitHub section People.

We welcome all developers to join TON Foundation and contribute to the technology.

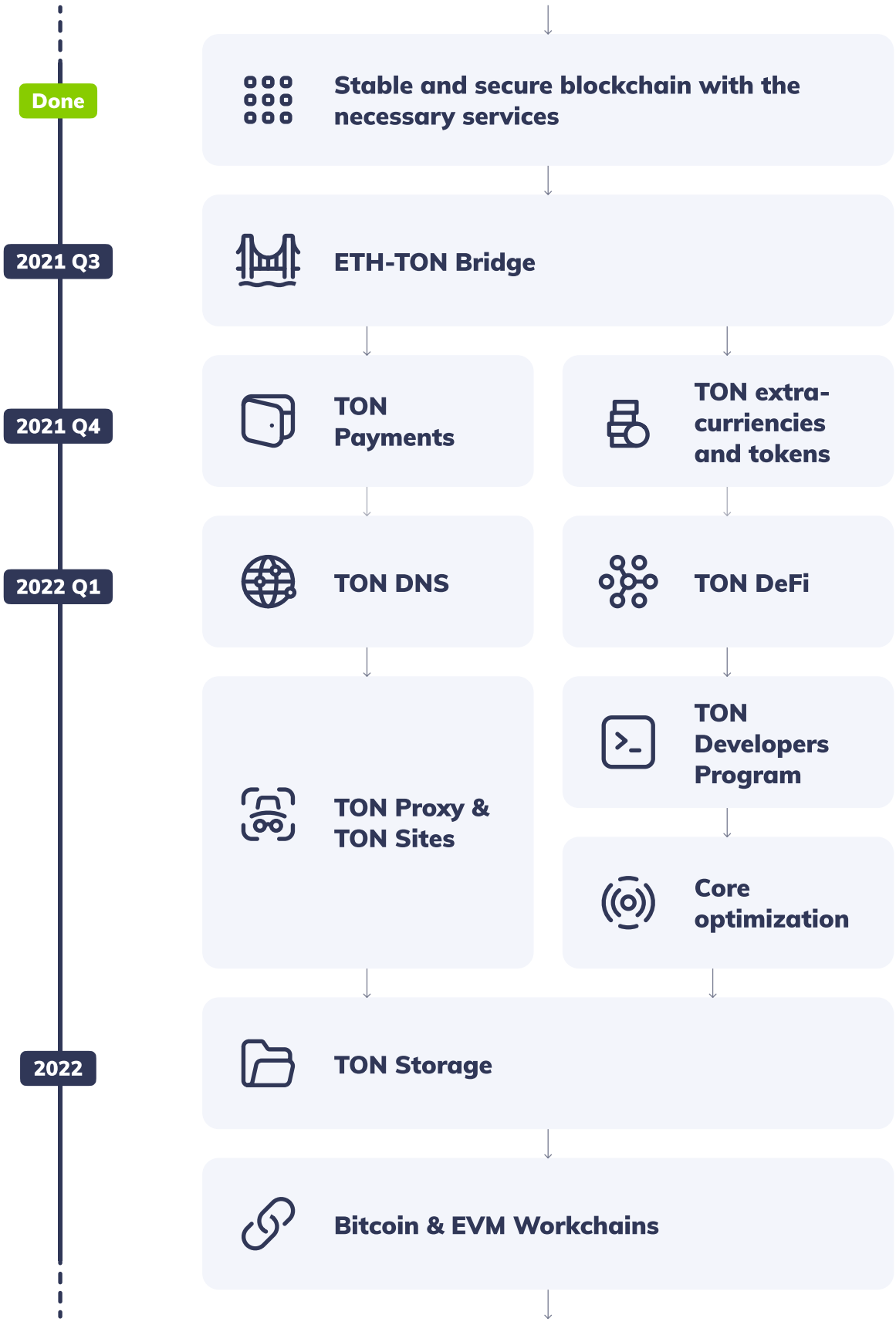


Governance

TON design ensures that network modifications are only possible if approved by the majority of validators via Proof-of-Stake consensus.

There is no way to change network software, configuration or state bypassing the vote.

Roadmap


Done
Stable and secure blockchain with the necessary services
2021 Q3
ETH-TON Bridge
2021 Q4
TON Payments
TON extra-curriencies and tokens
2022 Q1
TON DNS
TON DeFi
TON Proxy & TON Sites
TON Developers Program
Core optimization
2022
TON Storage
Bitcoin & EVM Workchains

How Proof-of-Stake works

1. Becoming a TON network **validator** takes starting a specific software.

   Anyone can do it; the more validators the better for the network.

   An important prerequisite though is a high-performance server with strong connection operating 24/7.

2. A validator stakes their Toncoins for a specific term. This stake is paid back at the completion of a validation round with a surplus or validator **reward** for the effort.

   Should a validator attempt to cheat or stay idle, their stake is fully or partially taken as a **penalty**.

3. Network validators verify user transactions. If all validators achieve consensus that a transaction is valid, it is included into the Blockchain. Invalid transactions are rejected.

4. Therefore, validators have to correctly process user transactions at maximum speed to get rewarded and avoid penalties.

How validators achieve consensus

An ad hoc Byzantine Fault Tolerant Catchain protocol was developed to ensure that stakeholders achieve consensus as long as the number of cheaters among them is 1/3 or less.

Also, the protocol provides mathematical proofs of cheating attempts that is used as evidence for imposing penalties.

Validators reward

A user adds a small surplus amount in Toncoins that represents a fee paid to validators as a reward for their work. Reward is distributed proportionally to the effective stakes of the validators.

Additionally, new Toncoins are generated during validation. These also go to validators. Overall annual coin inflation is about 0.6%.

What if a validator tries cheating?

By design, any cheating attempt in the Catchain Protocol is instantly detected. Upon the receipt of a mathematical proof of cheating, other validators immediately stop interacting with a cheater node. Then validators hold an automated vote to fine the cheater that consequently loses its stake fully or partially.

What if a validator underperforms or fails?

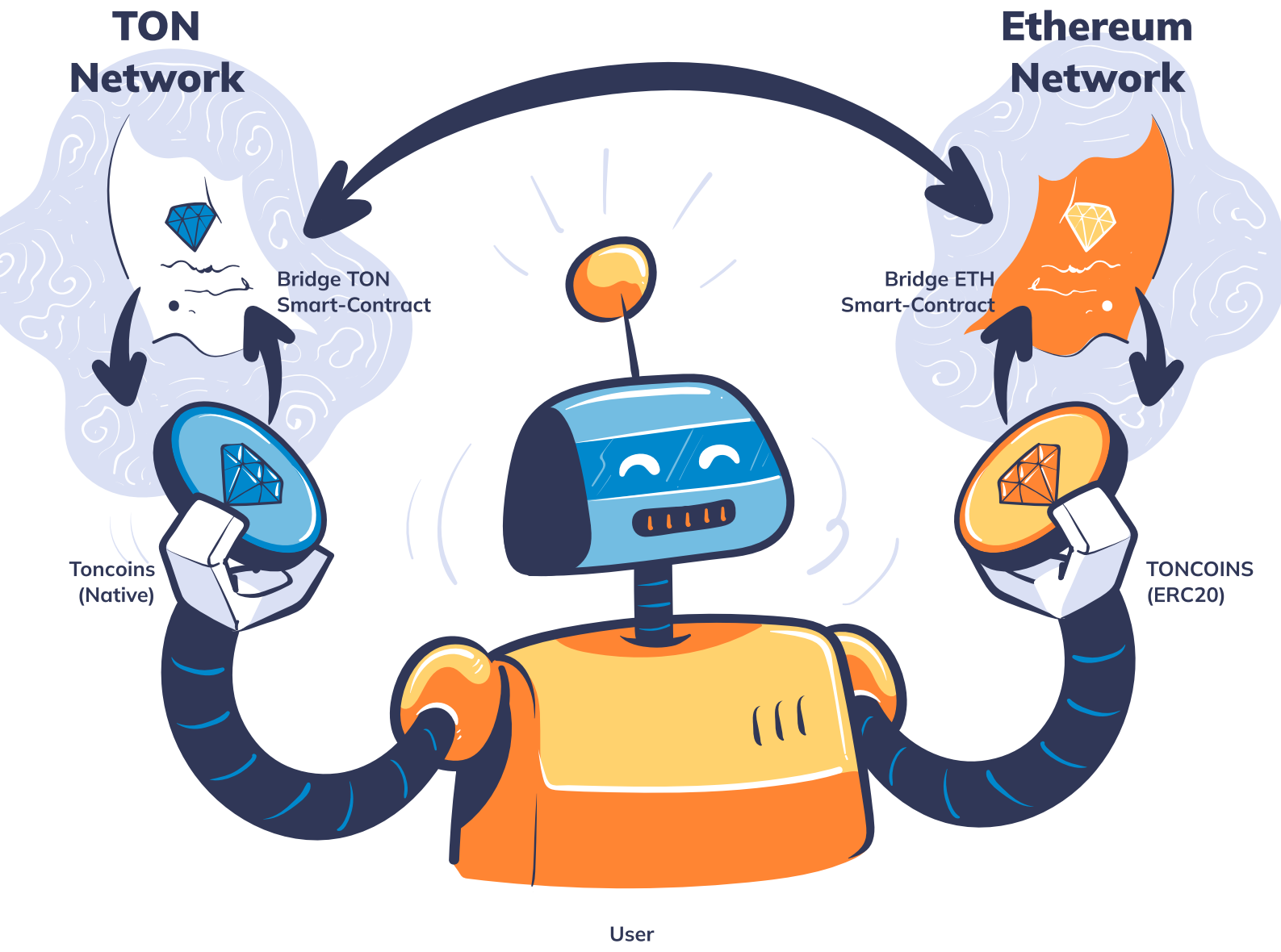
Each validator tracks processing statistics of other validators. If the number of transactions processed per period is too small for a particular node, validators collectively vote to fine it and it loses its stake fully or partially.

Summary

1. Validators maintain the system operations.
2. Any modification of the TON Blockchain requires consensus of all validators.
3. An inevitable penalty for cheating forces validators to comply with the consistent rules.

Bridge operation principle

A decentralized bridge allows transferring Toncoins from the TON network to the Ethereum network and back effortlessly.



Transfer Toncoins

From TON network to Ethereum Network

1. A user sends their Toncoins to an ad hoc smart contract in the network.
2. These coins get locked on the smart contract.

   Another ad hoc smart contract in Ethereum mints the same amount of ERC20 TONCOINS.
3. The Ethereum smart contract forwards newly generated TONCOINS to a user wallet.

1 Toncoin	=	**1 TONCOIN**
Native		ERC20

From Ethereum Network to TON Network

1. A user sends their TONCOINS to an ad hoc Ethereum smart contract
2. These TONCOINS are burnt and a counterpart contract in the TON Blockchain network unlocks the same number of Toncoins.
3. TON Blockchain contract sends the coins to a user wallet.

The total number of coins remains unchanged

Bridge Oracles

Bridging is managed by oracles with PoS tools implemented to maintain system decentralization.

1. Creating an oracle takes starting an ad hoc software. It requires a server with strong connection to the Internet operating 24/7.

2. An oracle temporary releases its Toncoins by transferring them to a bridge smart contract.

   This stake is returned after the work is done with surplus coins to reward the oracle.

   The stake size is determined by the current TON configuration.

   If an oracle tries to cheat or fails to perform, it is fined by other oracles that take hold of its stake.

3. Then TON validators have to vote for including the oracle to the oracle list.

   The oracle list is an element of the TON configuration.

   Validators giving votes to unfair oracles risk being fined.

4. Oracles monitor user applications for Toncoin cross-network transfers and approve transfer transactions in the bridge smart contract.

   A transfer is not approved unless and until at least 2/3 of all oracles approve it.

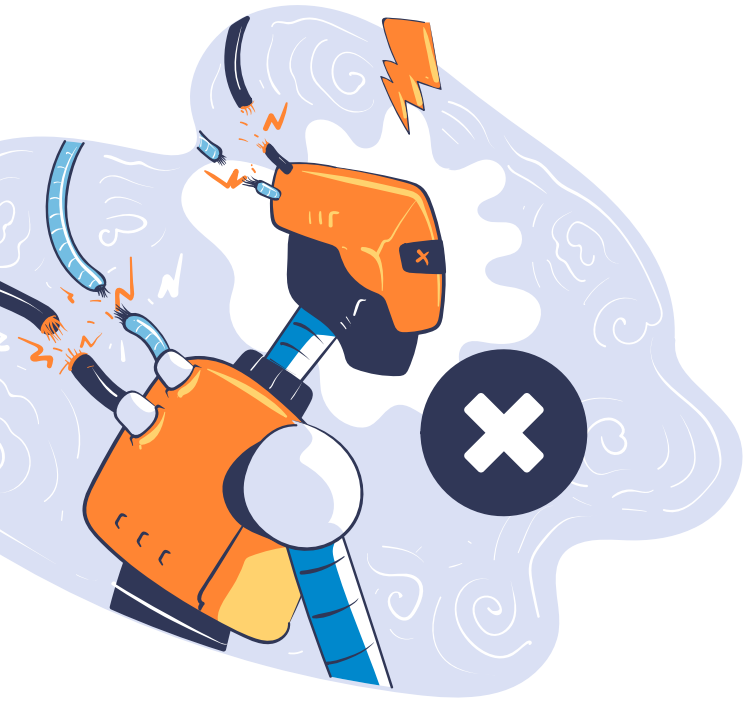
5. Therefore, oracles have to correctly process user transactions at maximum speed to get rewarded and avoid penalties.

Oracle reward

A small fee (fraction of a percentage) is charged on each bridged transfer to reward oracles.

The fee size is a part of the Bridge smart contract.

The total collected fee is equally distributed between all oracles upon completion of work to reward them for maintaining the system operational.



What if an oracle tries cheating?

If an oracle approves a transfer amount different from the user original request, it is considered a cheating attempt.

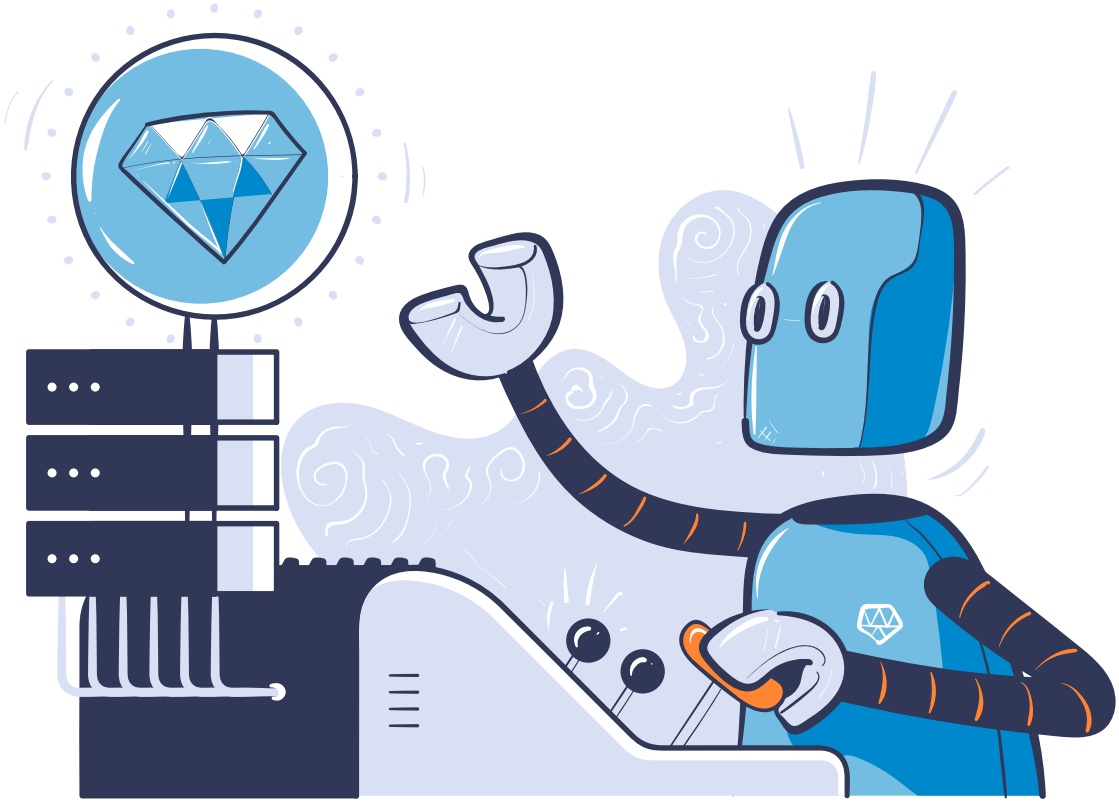
And, given that a transfer is not performed unless approved by 2/3 of all oracles and invalid transaction will be rejected.

Once a rejected transaction is detected, other oracles vote for excluding the cheater from the oracle list and fining the culprit by taking their stake.

Also, validators that originally voted for including the cheater to the list can be fined.

How mining works in TON

TON Blockchain uses the Proof-of-Stake consensus and mining is not required to generate new blocks.



So how come there is Proof-of-Work in TON?

Well, the reason is that the initial issue of 5bn Toncoins was transferred to ad hoc Proof-of-Work Giver smart contracts.

Mining is used to obtain Toncoins from this smart contract.

PoW Giver contracts have their limits and will dry out once users mine all available Toncoins.

Operation principle

Putting it in layman's terms, in any moment of time the PoW Giver contract has a computational puzzle, a challenge. Resolving it is rewarded by a fixed number of coins. Then a new challenge is generated. The only way to resolve the challenge is to brute-force numbers which takes serious computational resources.

If a puzzle is resolved too soon, the PoW Giver contract increases the complexity level which means more power needed to resolve it. Yet, if resolving took too much time, the complexity level is reduced. Thus, the PoW Giver contract maintains stable the number of coins given per day.

The more users participate in the process, the harder the task it. You have to both find a solution and do it faster than other participants.

How is it implemented?

In practice users launch ad hoc software that brute-forces numbers and sends suggested solutions to PoW Giver contracts. The higher is a performance of a miner's computer that operates this software, the higher probability of getting coins is.

The more miners there are in the network, the higher mining computational complexity is and the more computational power is required to mine coins.

Links

ton.org

github.com/newton-blockchain

t.me/tonblockchain