CoinShares

ASSET HIGHLIGHT

ALGORAND

coinshares.com

ALGORAND

PURPOSE

From decentralised finance to generative NFT art (and everything in between), Algorand aims to be a sustainable blockchain powering the economic models of the future.

THE SYSTEM

Smart Contracts
Carbon Negative
Proof of Stake

Source: Algorand, Coinshares, as of July 19th 2022

THE ASSET

Staking
Governance
Network Fees

Source: Algorand, Coinshares, as of July 19th 2022

PRICE ACTION

2019*	-93.73%
2020	46.90%
2021	442.17%
2022 (YTD)	-83.62%

**Since June 2019*
Source: ALGO/USD, Compass Financial Technologies. The figures shown relate to past performance. Past performance is not a reliable indicator of future results and should not be a sole factor of consideration when selecting a product. Transaction costs, fees and expenses not included. Figures do not include any Staking Rewards.

GENERAL INFO

Creator	Silvio Micali
Launch	June 2019
Consensus	Pure Proof of Stake
Asset	Algo
Max Supply	10 billion
Smallest Unit	1 Algo = 1 million microAlgos
Core Contributors	Algorand Foundation
Language	Java, Python, Go, JavaScript

Source: Algorand, Coinshares, as of July 19th 2022

QUICK STATS

Market Cap	$2.5 billion
Circulating Supply	6.95 billion
Staked Algo	2.5 billion
Consensus nodes	1,500
Average Block time	4.5 seconds
Average transaction fee	$0.004

Source: Algorand, Coinshares, as of July 19th 2022

EXECUTIVE SUMMARY

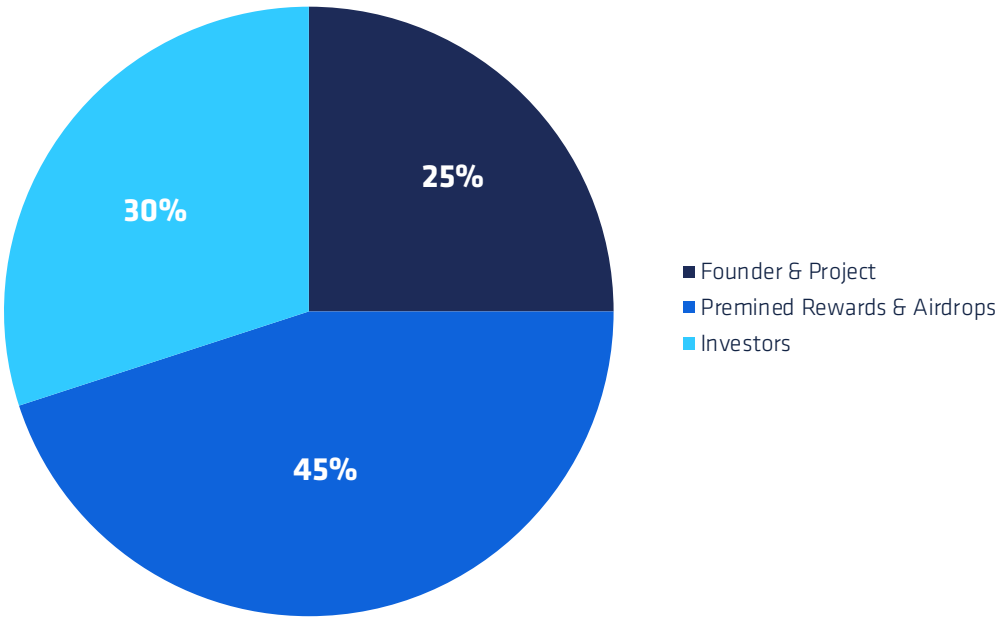
This report simplifies and clarifies what Algorand is and what it does; the problem Algorand tries to solve and its development since its launch. Furthermore, it covers the people behind the protocol, the core components, and how the network runs.

Algorand Inc. is a technology firm focused on reducing friction in financial exchanges. Algorand Inc. created the first open-source, permissionless, Pure Proof of Stake (PPoS) blockchain system in the world. PPoS, in contrast to other Proof of Stake (PoS) models, does not offer rewards and does not expose validator funds to slashing. This PPoS mechanism allows the entire network of online stakers to participate in consensus without minimum stake requirements. Silvio Micali, a recipient of the Turing Award, created the Algorand protocol, the foundation of this blockchain.

Algorand has three strategic pillars when making high-level decisions about the network; i) Core protocol properties, ii) Smart contract platform, and iii) Interoperability. We highlight these pillars in greater detail below.

i. Core protocol properties - The backbone of the Algorand network, an optimised protocol serves as the foundation for the remaining pillars. Key metrics include high TPS, lower latency, strong trust model, and affordable.
ii. Smart contract platform - Algorand aims to be the go-to platform for decentralised applications (dApps). This involves strong partnerships and making it easy for developers to build.
iii. Interoperability - Algorand also sees the importance of composability and bridging with other blockchains and ecosystems. As such, interoperability requires the creation of trust-minimised bridges and verified proofs.

ALGORAND INITIAL SUPPLY BREAKDOWN



Source: Algorand, Messari, CoinShares, data available as of close 18 July 2022

PURPOSE, MOTIVATION AND SOLUTION

Algorand was founded by Silvio Micali, a Turing award winner, co-inventor of zero-knowledge proofs, and a world-renowned leader in the field of cryptography and information security. He founded Algorand with a vision to democratise finance and deliver on the blockchain promise.

The blockchain trilemma, which is when security, scalability, and decentralisation are all sacrificed, is a problem with many blockchains. By creating a novel PPoS consensus system, which is the protocol that the Algorand blockchain utilises, Silvio and his team were able to make select tradeoffs within the system.

In the Algorand network, stakers do not receive any rewards, instead, Algo tokens are rewarded to users who participate in governance. So while anyone with some Algo in their wallet can stake, only those who vote on governance proposals receive tokens. Algorand's decentralised Byzantine agreement protocol can tolerate an arbitrary number of malicious users as long as honest users hold a supermajority of the total stake in the system.

CORE PEOPLE

Silvio Micali
Silvio established Algorand in 2017 and is in charge of all research at Algorand, including theory, security, and cryptocurrency financing. In particular, Silvio is credited for co-inventing many of the protocols that form the basis of contemporary cryptography, including verifiable random functions, zero-knowledge proofs, and probabilistic encryption. Silvio has won the RSA prize, the Gödel Prize, and the Turing Award for computer science. He belongs to the American Academy of Arts and Sciences, Accademia dei Lincei, National Academy of Sciences, National Academy of Engineering, and National Academy of Engineering of China. The University of Rome awarded Silvio a Laurea in Mathematics, and the University of California, Berkeley awarded him a Ph.D. in computer science.

Steve Kokinos
Algorand's Former CEO, Steve, stepped down in July 2022 to focus on scaling the Algorand network and still remains as an advisor. Steve is a seasoned entrepreneur who most recently served as Executive Chairman and CoFounder of Fuze, where he oversaw corporate strategy. Fuze now employs over 700 people to serve more than 1500 business clients globally. Steve co-founded BladeLogic, Inc., a global leader in data center automation, before launching Fuze. Among its Fortune 500 clients are GE, Time Warner, Microsoft, Cable & Wireless, Walmart, and Sprint. After a successful IPO, BMC Software paid over $800 million to purchase BladeLogic. Prior to founding BladeLogic, Steve served as the co-founder and CEO of Web Yes, Inc., a pioneer in the Web hosting and application service provider industries that offered infrastructure services to companies including Sun Microsystems, Netscape, and Lycos, among others. Breakaway Solutions purchased Web Yes in 1999.

W. Sean Ford

Algorand's interim CEO, Sean, is in charge of the company's entire corporate vision and strategy. Sean joins Algorand from LogMeIn where he served as the Chief Marketing Officer and was in charge of demand creation, e-commerce, communications, brand leadership, and global marketing strategy. In the beginning of 2018, he oversaw the Integration Management Office for LogMeIn's acquisition of Jive Communications. Sean, a seasoned operations and go-to-market executive, was a member of the executive leadership team of Avid Technology, where he oversaw operations and global marketing strategy. Sean has also held a number of executive leadership positions, including vice president of global business unit marketing at Oracle, where he was in charge of the company's vertical industry applications globally, as well as chief marketing officer and chief operating officer of Zmags, Syncsort, and Oracle. Sean spent the first seven years of his professional life working as a senior strategy consultant for Monitor Group. He co-founded Upromise, Inc. in 1999 and served as vice-president of product management and product marketing there. Sean graduated from Williams College with a Bachelor of Arts in English and the Harvard University Graduate School of Business with a Master of Business Administration.

CORE TEAMS

Algorand™

Algorand Inc. is an open-source software firm with headquarters in Boston that was created by cryptography pioneer Silvio Micali. Its platform offers decentralisation, scalability, and security. The first-of-its-kind, permissionless, PPoS protocol from Algorand supports scalability, open participation, and transaction finality.

Algorand™ FOUNDATION

The Algorand Foundation is committed to ensuring that the open-source environment, decentralised governance, and sound monetary supply economics of the Algorand blockchain contribute to realising the worldwide potential of this technology.

DEVELOPMENT

In 2015, Silvio first started looking at Bitcoin and blockchain technologies. While doing an investigation, he discovered certain issues with Bitcoin and made the decision to present his own concept for a permissionless blockchain online. Though sceptical, his colleague Nickolai Zeldavich, the Head of Distributed Systems suggested testing it to see whether the technology promises were true. Subsequently, they rented tens of thousands of servers from Amazon and used them to run simulations ranging from 10,000 to 500,000 people. After receiving positive test results, Silvio decided to launch an entity to carry out his dream of a *borderless economy*. There were 11 persons in the firm at the beginning, 8 of them were from MIT. For the first three months, the Algorand crew worked out of Silvio's house.

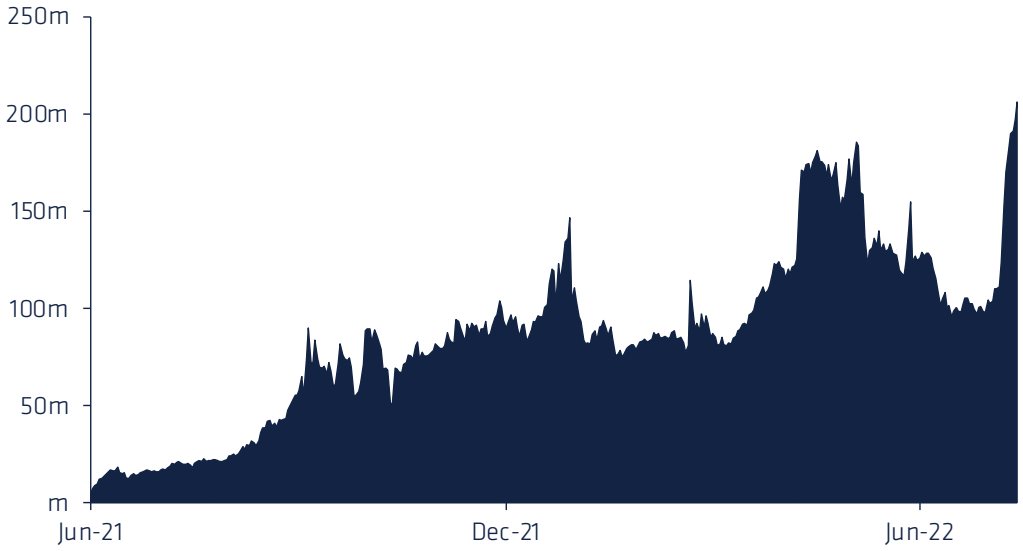
In February 2018, Algorand received $4M in initial investment from Pillar and Union Square Ventures followed by another $62M round from a number of additional investors in October that same year. In June 2019, the Algorand Foundation launched the Global University Program with the goal of advancing strong technical research in blockchain for a borderless economy. Leading universities from the USA, Canada, Europe, the Middle East, and China were invited to participate in the program's first university research phase. Peking University, Sapienza University of Rome, Massachusetts Institute of Technology, Stony Brook University, Tel Aviv University, Tsinghua University, University of California, Berkeley University of Salerno, Università della Svizzera Italiana, and the University of Waterloo are a few of the founding members. The first round of the Dutch auction for Algorand Tokens was held that same month.

In the fourth quarter of 2021, Algorand started its community governance which commenced the shift to a phase in which the community began to take more charge of the network, and rewards were distributed in return for verifiable engagement in the program. This means that Algorand has stopped rewarding validators for securing the network, instead, only those who participate in the governance process are issued tokens. The assumption that Algorand holds is that if you're invested in Algorand then you'll want to protect it by operating nodes anyway (without the need for any external rewards). If validators believe others are participating at a rate that could put their investment at risk then they'll participate more. The community governance rewards are scheduled to continue until 2029 whereby the remaining 3.3 billion tokens will have been distributed. In an effort to dampen centralisation forces, the Algorand foundation will not vote or earn rewards in community governance and will only set up the voting options while indicating its preference. The governance process is as follows; Proposed changes are first posted on the blockchain, then the community uses Algorand's consensus protocol to vote for or against. If accepted, the community agrees on the block where the change happens, and then everyone switches to the new protocol at the same time.

Replacing staking rewards with voting rewards is a novel approach to security and governance and it remains to be seen whether these game theoretic assumptions will hold in the long term. However, if any issues arise in this model, governance will always try to address them.

In 2022, Algorand's upgrade bestowed smart contracts the ability to call one another, allowing for greater composability and for more complex applications to be built. This highlights how early Algorand is in the development cycle as smart contract platforms like Ethereum have had this capability since its launch in 2015. However, the DeFi landscape continues to grow as shown below, Total Value Locked in Algorand reached an all-time high in July 2022.

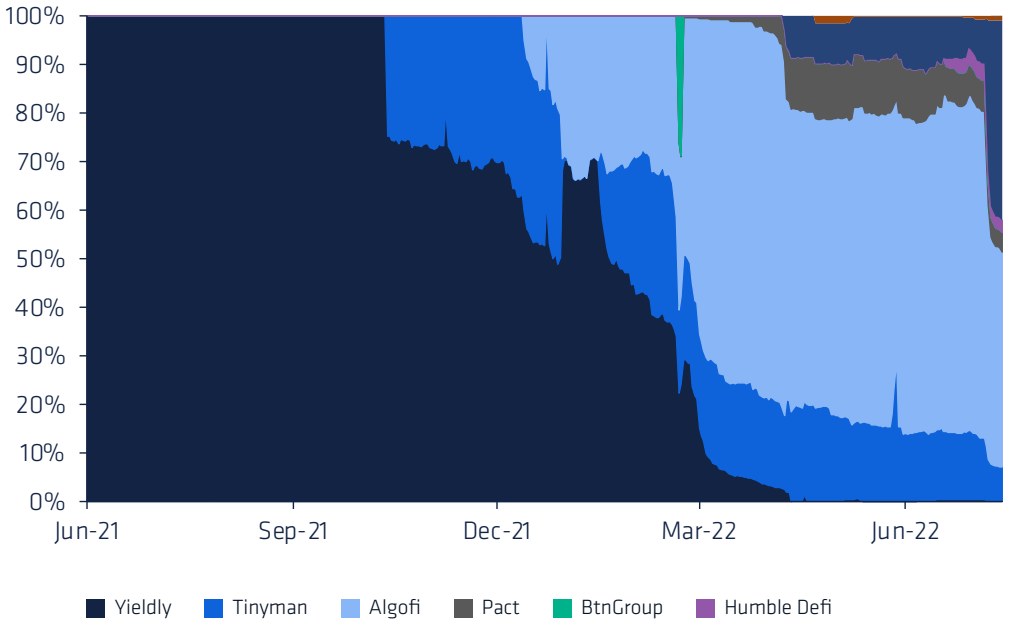
TVL across DeFi protocols in Algorand (in USD)



Source: DeFi Llama, CoinShares, data available as of close 17 July 2022

Furthermore, we note that Algorand's DeFi ecosystem is broadening as it grows, a healthy trend. Below we show the evolution of the top DeFi protocols by TVL on Algorand for the past year.

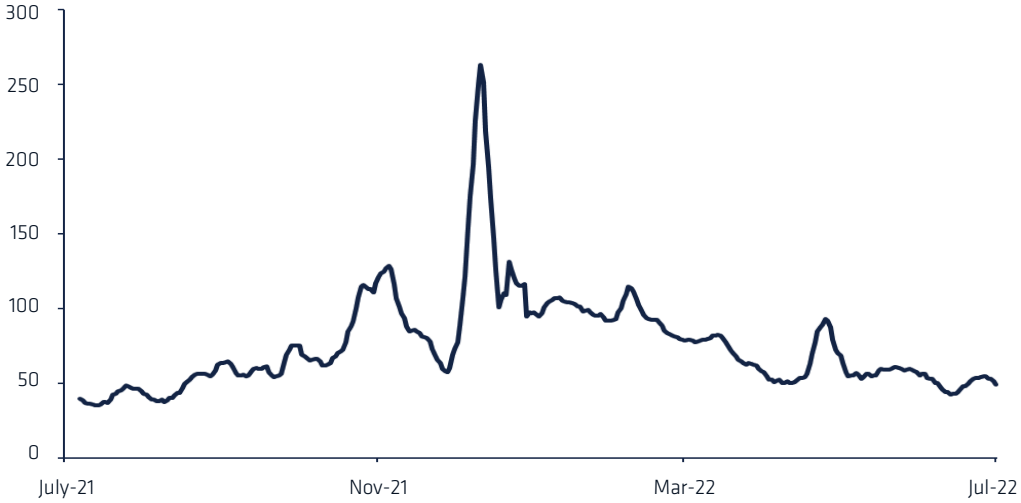
Algorand DeFi TVL by project (%)



Source: DeFi Llama, CoinShares, data available as of close 18 July 2022

Below we show the 7-day moving average for transactions per second within the Algorand network for the past year.

Transactions per second July 2021 to July 2022



Source: CoinMetrics, CoinShares, data available as of close 18 July 2022

CORE COMPONENTS

Below we highlight a comparison of Algorand's PPoS to other popular consensus mechanisms. It should be noted that most other chains incentivise the block producers or validators while Algorand only incentivises governance participation. Considering that this strategy uses different assumptions, comparisons are less likely to be *apples to apples*.

	Proof of Work	**Delegated Proof of Stake**	**Bonded Proof of Stake**	**Pure Proof of Stake**
Resource Usage	High	Low	Low	Low
Consensus participants	Requires complex machinery	Requires delegation for most	Requires a high capital	Any amount can be staked
Validation Rewards	High	Depends	Depends	None
Governance Rewards	N/A	N/A	N/A	Rewards users who vote
Finality	Probabilistically Guaranteed	Guaranteed	Guaranteed	Guaranteed
Dynamically Available (stall-proof)	Strong	Weak	Weak	Weak

Source: Algorand, CoinShares, PPoS specific to Algorand, as of July 19th 2022

NETWORK PARTICIPANTS

Algorand allows for any instrument to be tokenised, transferred, and programmed. With a single transaction, users can create fungible tokens, NFTs, and security tokens (no smart contract code required). Users can also leverage Algorand smart contracts to create complex decentralised apps (dApps). We show below the key participants in the network and their roles.

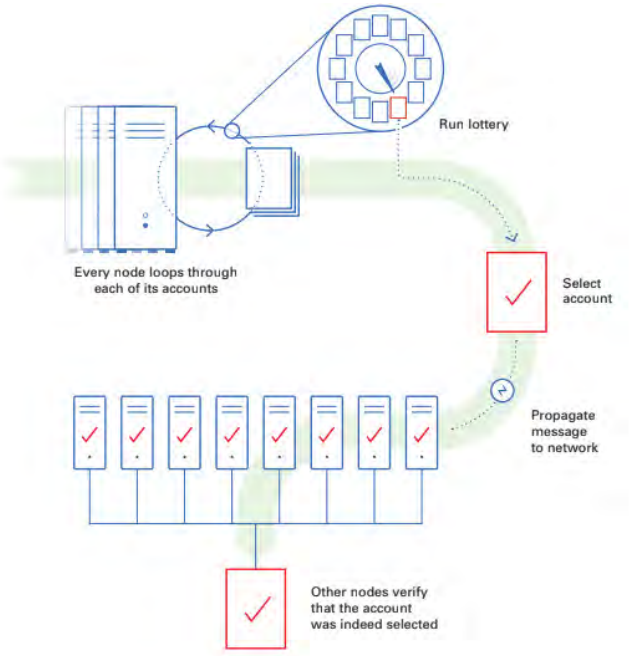
	Relay Nodes	Non-Relay Nodes	Governors
Role	Primarily used for communication over the network	Participate in the Algorand consensus protocol	Governors are Algo holders who commit a stake for a 3-month governance period
Statistics	120 relay nodes	1,500 non-relay nodes. Minimum of 0.1 Algo needed	Minimum of 0.1 Algo needed
Process	Although anybody can host a relay node, in theory, an Algorand node will by default only connect to a relay node on a list that is kept by the Algorand Foundation	Anyone can run a non-relay node and participate in consensus	Quarterly governance periods
Reward	N/A	N/A	6.96% APR

Source: Algorand, Staking Rewards, CoinShares, as of July 19th 2022

NETWORK PROCESS

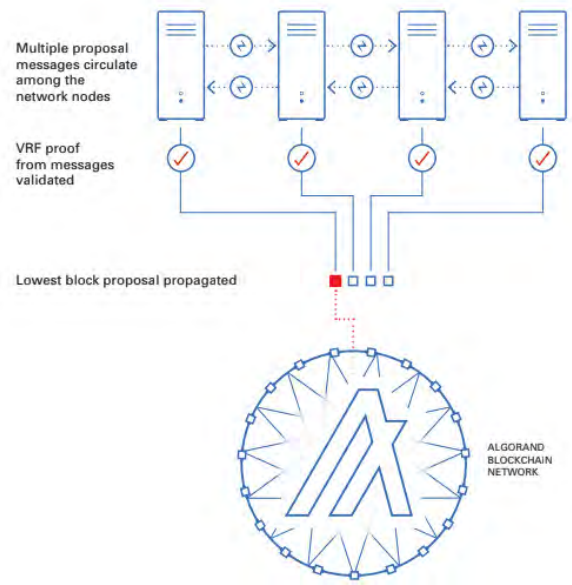
Algorand's consensus algorithm has a few steps as outlined below.

Block Proposing - In this step, accounts are chosen to propose new blocks to the network. In order to decide if an account is chosen to propose the block, each node in the network loops over all of the eligible online accounts. A weighted lottery is then performed, with each account's likelihood of being chosen depending on the amount of Algos that are actively engaging online. The node propagates the proposed block together with proof, demonstrating that the account is a legitimate proposer.



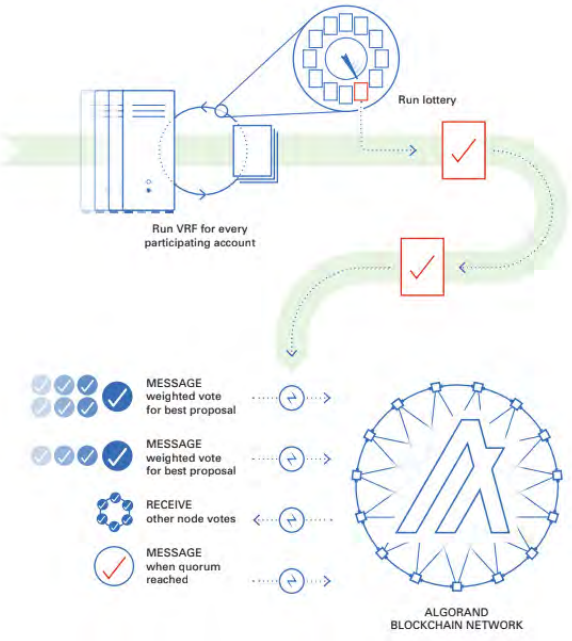
Source: Algorand (copied from https://developer.algorand.org/docs/get-details/algorand_consensus/), as of July 19th 2022

Soft Voting - To ensure that only one block is certified, this step's goal is to reduce the number of proposals to one. Numerous proposal messages will be sent to each node in the network. The node will then identify which validated winner's proof has the lowest hash by comparing them, and it will only propagate the block proposal with the lowest hash. In order for votes to spread throughout the network, this procedure continues for a certain period of time.



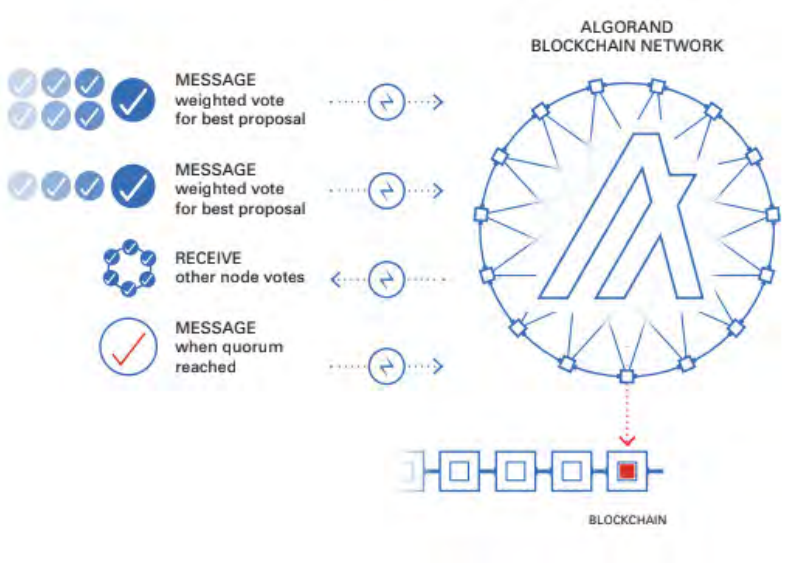
Source: Algorand (copied from https://developer.algorand.org/docs/get-details/algorand_consensus/), as of July 19th 2022

Soft Voting (continued) - Every stage of the procedure has a different committee size, and each one is chosen from scratch. To proceed to the following phase, 2/3 of the committee must agree on their votes. These votes will come from other network nodes, and before they are added to the vote total, each node will verify the committee membership.



Source: Algorand (copied from https://developer.algorand.org/docs/get-details/algorand_consensus/), as of July 19th 2022

Certifying Vote - The block that was approved at the soft vote stage is examined by a new committee to look for overspending, double-spending, or any other issues. The new committee votes once more to certify the block if it is legitimate. Each node gathers and verifies these votes until a quorum is reached, which brings the round to a finish and causes the node to produce a certificate for the block and record it in the ledger. After that, a new round is started, and the entire procedure is repeated.



Source: Algorand (copied from https://developer.algorand.org/docs/get-details/algorand_consensus/), as of July 19th 2022

ALGO, THE TOKEN

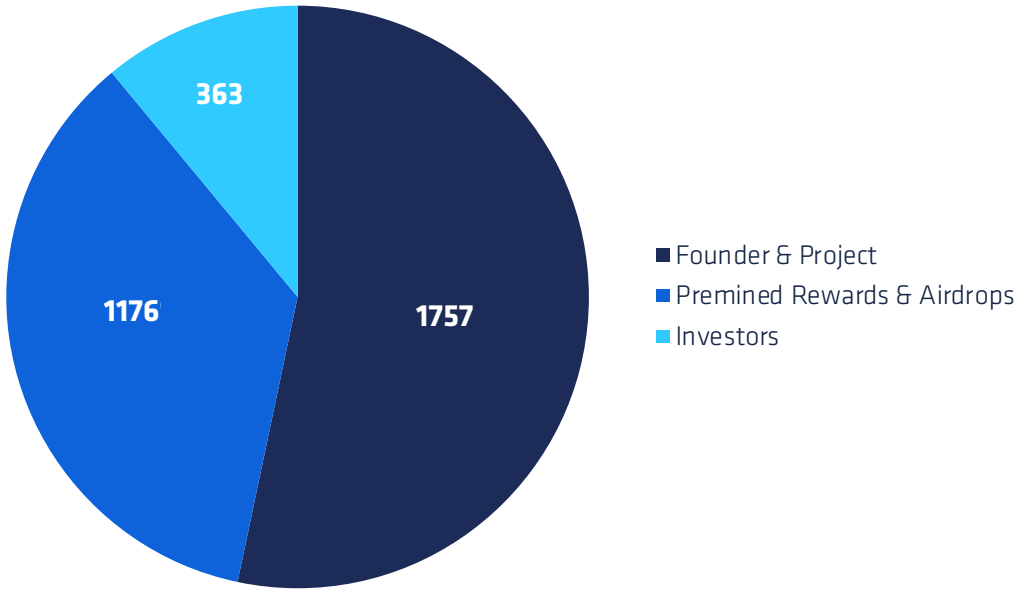
Algo is Algorand's native token that's used for i) paying for transactions across the network, ii) staking to help secure the network, and iii) governance.

Transaction Fees	Staking	Governance
There is no gas market, instead transaction fees are based on the size of the transaction. Fees tend to average just over 0.001 Algo	Every user may propose and vote on blocks with a probability directly proportional to their stake	A governor must commit a prespecified amount of Algo for a minimum 3-month period and vote at least once
Users can use Algo to pay for fees for transacting or interacting with decentralised applications	1,500 non-relay nodes. Minimum of 0.1 Algo needed No strict minimum amount of Algo is required to stake though a minimum account balance of 0.1 Algo is required	Minimum of 0.1 Algo needed No strict minimum amount of Algo is required to govern though a minimum account balance of 0.1 Algo is required
No portion of the fees is burnt	There are no rewards for staking Algo	Governance rewards are currently 6.96%

Source: Algorand, Staking Rewards, CoinShares, as of July 19th 2022

Below we show the allocation of the remaining 3.3 billion tokens.

Distribution of remaining tokens (in millions of Algo)



Source: CoinShares, data available as of close 31st March 2022

STRENGTHS

Algorand possesses a strong team, built around Turing award winner, Silvio Micali. This team has made notable accomplishments as evidenced by Algorand's post-quantum signature keys for state proofs and Verifiable Random Function (VRF). The culture and values are also present as Algorand is also one of the few carbon-negative blockchains due to on-chain carbon credit trading.

With high throughput and low latency, Algorand is one of the fastest smart contract platforms in the market. Algorand boasts a time to finality of 4.5 seconds and can handle 1,000 transactions per second (TPS). This speed is also accompanied by low fees as each transaction costs fractions of a penny. These fast times to finality are due to Algorand not being able to fork (when a blockchain splits into two paths). With no fork choice rule, users can be confident that their transactions will be finalised within a short period of time as long as most validators continue to act honestly.

WEAKNESSES

Without the ability to fork, if validators take long to reach a commitment (whether accidental or a coordinated attack), the blockchain performance will degrade and may eventually stall completely. It should be noted that this has never happened on the Algorand mainnet.

The number of Relay Nodes can't effectively scale higher than a few hundred (currently at 120), limiting the decentralisation potential in this part of the network.

OPPORTUNITIES

Algorand was selected to power $SOV, the first national digital currency for the Martial Islands. If this project is successful, this will expand the use cases for Algorand and potentially encourage other nation states to follow suit.

An upgrade is scheduled to happen in Q3 2022 which will improve both the latency and throughput for the Algorand network. This upgrade is expected to improve Algorand's performance from 1,000 TPS and 4.5-second finality to 10,000 TPS and 2.5-second finality.

Algorand's governance rewards program is a novel experiment that helps strengthen the community, better align incentives and streamline decision-making.

A recently announced partnership with LimeWire to sell music NFTs as well as other types of NFTs may prove to be fruitful.

THREATS

Other Layer-1s also offer high throughput, low latency and cheap transactions. Algorand may have to do more to differentiate itself to improve its market share.

The set of Relay nodes is based on a list managed by the Algorand Foundation, this lack of decentralisation opens up attack vectors for potential adversaries.

The lack of network incentives to participate in consensus may backfire if validators begin to collude as the network continues to decentralise.

MARKET PARTICIPANTS

As of 19th July 2022, Algo is the 31st largest token by market cap. Although it's down c.85% from its peak, it has seen network TVL grow. There are over 100 spot markets, 15 perpetual markets and 1 futures market to trade Algo.

Disclosure

The information contained in this document is for general information only. Nothing in this document should be interpreted as constituting an offer of (or any solicitation in connection with) any investment products or services by any member of the CoinShares Group where it may be illegal to do so. Access to any investment products or services of the CoinShares Group is in all cases subject to the applicable laws and regulations relating thereto.

This document is directed at professional and institutional investors. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. This document contains historical data. Historical performance is not an indication of future performance and investments may go up and down in value. You cannot invest directly in an index. Fees and expenses have not been included.

Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to. This document fairly represents the opinions and sentiments of CoinShares, as at the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

The information presented in this document has been developed internally and / or obtained from sources believed to be reliable; however, CoinShares does not guarantee the accuracy, adequacy or completeness of such information. Predictions, opinions and other information contained in this document are subject to change continually and without notice of any kind and may no longer be true after the date indicated. Third party data providers make no warranties or representation of any kind in relation to the use of any of their data in this document. CoinShares does not accept any liability whatsoever for any direct, indirect or consequential loss arising from any use of this document or its contents.

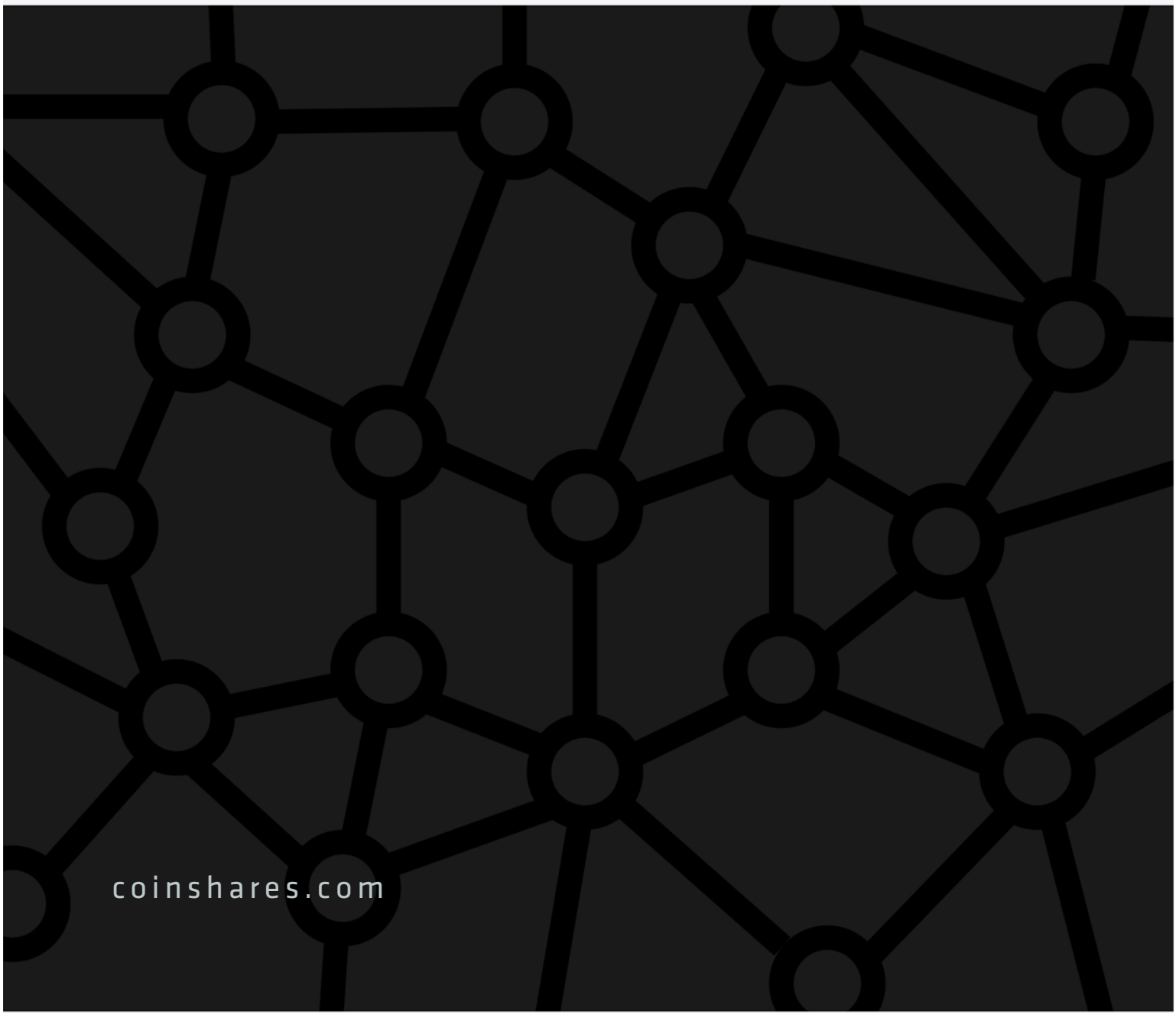
Any forward-looking statements speak only as of the date they are made, and CoinShares assumes no duty to, and does not undertake, to update forward-looking statements. Forward-looking statements are subject to numerous assumptions, risks and uncertainties, which change over time. Nothing within this document constitutes (or should be construed as being) investment, legal, tax or other advice. This document should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

This document is directed at, and only made available to, professional clients and eligible counterparties. For UK investors: CoinShares Capital Markets (UK) Limited is an appointed representative of Strata Global Limited which is authorised and regulated by the Financial Conduct Authority (FRN 563834). The address of CoinShares Capital Markets (UK) Limited is 82 Baker Street, London, W1U 6TE. For EU investors: Napoleon AM (napoleon-am.com) is a French asset management company regulated by the Autorité des Marchés Financiers (AMF), registered under number GP-19000015 since 27/03/2019. Its office is located at 11 rue Paul Lelong, 75002 Paris, France.

CoinShares

ASSET HIGHLIGHT

research@coinshares.com



coinshares.com