Algorand Investment Report

Project Overview

Built as a blockchain protocol and cryptocurrency that aims to empower people by giving them access to borderless, decentralized financial services, Algorand's novel ***pure proof-of-stake*** mechanism provides users with a network that achieves consensus securely and efficiently. In addition to giving developers the tools to create and deploy their own cryptocurrencies, NFTS, securities, and stablecoins, Algorand's proprietary technology enables a set of high-performing Layer-1 blockchains that provide security, scalability, transaction finality, privacy, sidechains, and advanced smart contract capabilities essential to DeFi.

Project Description

      With over 92% of millennials distrusting current financial systems and 2.5 billion lacking access to them- Algorand's blockchain facilitates a system where people can transact across borders without having to go through legacy financial systems. Created by Silvio Micali, one of the pioneers of the field of cryptography and an MIT professor, Algorand's origins began in academia and has been under development for years. Built as a blockchain that is developed from principles first, Algorand is on a mission to become one of the leading blockchains in cryptocurrency today. Leveraging their proprietary PPoS that is far superior to Bitcoin's outdated Proof of Work technology, Algorand's blockchain is able to scale to billions of users and process thousands of transactions per second with an average transaction confirmation time of 4.3 seconds. Utilizing Byzantine agreements and a committee of verifiers at its core, Algorand's public and permissionless network allows any participant to contribute to the blockchain's consensus.

ALGORAND FEATURES & CAPABILITIES IN LAYER-1

SMART CONTRACTS	ALGORAND STANDARD ASSETS	ATOMIC TRANSFERS	REKEYING

Unique Value Proposition

Aiming to revolutionize current Proof of Work and Proof of Stake consensus mechanisms, which require vast amounts of computation and concentrate power in the hands of the few, Algorand's PPoS securely and efficiently achieves consensus in a fully decentralized network with a supermajority of honest users agreeing on what should be added to the chain. Utilizing the ALGO coin and their attractive suite of products, the Algorand foundation is creating a global network of borderless decentralized finance. By providing developers with a blockchain that is scalable, secure, and decentralized - Algorand seeks to compete with first-generation blockchains that are slow to propagate, costly, and unscalable. Algorand currently has the following features and capabilities as a layer-1 solution:

1) Pure Proof-of-Stake (PPoS): Algorand uses a pure proof-of-stake (PPoS) protocol built on Byzantine consensus. Each user's influence on the choice of a new block is proportional to its stake (number of tokens) in the system. Users are randomly and secretly selected to propose blocks and vote on block proposals. All online users have the chance to be selected to propose and vote. The likelihood that a user will be chosen, and the weight of its proposals and votes, are directly proportional to its stake.[1]

2) Non-Forkable Chain: One of the prime factors that set Algorand apart is non-forkable chains. Forking is when a blockchain splits into two branches leaving behind only one chain and a lot of uncertainty. For example, if a user makes a payment, they can't be certain whether it has been made as it could either be in the lost branch or the surviving one. As only one block can have the required threshold of committee votes in the Algorand system, forking is brought down to zero, and all transactions are finalized. A block that appears is etched on the chain forever. If a new block reveals a

---

[1] https://www.algorand.com/technology/pure-proof-of-stake

payment that has been forwarded to a user, they can count it as paid and go ahead and take the necessary steps to deliver the product or service in return.[2]

3) Security: In the Algorand protocol, participants change every round of block selection in order to protect the network against attackers. Before they participate, no one knows who the users are, and once they participate, their message is already propagating through the network so it is too late for an attacker to benefit from attacking them.[3]

4) Scalability: A single, short, and fast computed message has to be propagated by each member after they have been selected. Regardless of the number of users in the system, this ensures that the maximum number of short messages that are propagated is 1000. This way, Algorand offers a scalable blockchain solution.[4]

5) Decentralization: There are no fixed few users who are in charge of choosing the next block or approving it. Committees are randomly picked in secrecy from time to time so that everyone has an opportunity to participate in the generation of a new block.[5]

Use Case

With hundreds of organizations comprising fintech startups, financial services, institutions, and defi currently building on Algorand- the robust community is creating a healthy ecosystem of contributors that are aligned with protocols' longer-term vision for the future of finance.[6] Some examples include Circle (USDC stablecoin), IDEX (world's leading decentralized smart contract exchange), Republic (private investing platform and technology services provider), Marshall Islands (first country to adopt a national currency), StakerDAO (a platform for governing financial assets in a decentralized, secure, and compliant manner),

---

[2] https://www.accesswire.com/610310/What-Makes-Algorand-Stand-Apart-From-Other-Blockchain-Platforms

[3] https://www.algorand.com/technology/core-blockchain-innovation

[4] https://www.accesswire.com/610310/What-Makes-Algorand-Stand-Apart-From-Other-Blockchain-Platforms

[5] https://www.accesswire.com/610310/What-Makes-Algorand-Stand-Apart-From-Other-Blockchain-Platforms

[6] https://www.algorand.com/ecosystem/use-cases

and Tether (USDT stablecoin). Hoping to continue expanding their narrative of being the protocol to lead the future of finance, Algorand currently offers the following use-cases for project developers including:

- Smart Contracts: Algorand's smart contracts enable the disruption of economies and the creation of new business models across different industries with efficient and automated transactions and applications, allowing for a trustless execution of the agreement.

- Algorand Standard Assets: Algorand's standard assets (ASA) are able to provide a standardized, layer 1 mechanism that is capable of representing any type of asset on-chain. These can include fungible and non-fungible assets and synthetics.

- Atomic Transfers: Providing a trustless way to simultaneously transfer a number of assets among a group of parties, Algorand's atomic transfers provide a trustless solution to exchange assets on the blockchains layer 1 infrastructure.

- Rekeying: Solving operational inefficiencies by allowing users to change their Private Spending key without the need to change their Public Address.

Technology

Algorand's Protocol is built around the following key components[7]:

1) <u>Permissionless Blockchain</u>: Algorand is an entirely permissionless and decentralized public blockchain. The Algorand blockchain has only one class of users. Since Algorand's protocol is based on pure proof-of-stake, no user or group of users is distinguished to play a special role in the protocol. Every user can play any role in the protocol in proportion to their stake. All users who possess ALGOs and are online are automatically eligible to participate in all functionalities of the protocol, including proposing blocks and voting on blocks.[8]

2) <u>Immediate Transaction Finality</u>: The Algorand blockchain does not fork. Unlike with proof-of-work protocols, two different blocks can never be added to the chain in the same position. Only one block can have the required threshold of signatures in order to be certified in a given round.

3) <u>Cryptographic Sortition</u>: Neither a few delegated users nor a fixed committee is responsible for proposing blocks in Algorand. Instead, all users are randomly, secretly, and continuously selected to participate in the Algorand consensus protocol. Every block in Algorand reveals a new unpredictable selection seed that determines which users participate in the next round of block selection. An online user checks whether they were selected to participate by evaluating a Verifiable Random Function (VRF) with their secret key and the selection seed. The VRF acts similar to a weighted lottery where the number of ALGOs that the user has affects the user's chance of being selected.

---

[7] https://algorand.foundation/algorand-protocol/core-blockchain-innovation
[8] https://algorand.foundation/algorand-protocol/about-algorand-protocol/permissionless-blockchain

4) <u>Consensus-Level Security</u>: Algorand's decentralized 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. First, the adversary does not know which users to corrupt. In fact, the users who are called to certify a new block are secretly and individually selected. Second, when the adversary realizes which users are selected, it is too late for them to benefit from attacking the users. Those users have already fulfilled their responsibility in the consensus protocol. In the next round of block certification, a new set of users will again be privately and individually chosen.

5) <u>Network Architecture:</u> The Algorand network has two types of nodes to simultaneously optimize decentralization and high transaction throughput. Relay nodes allow for highly efficient communication paths. Participation nodes propose and vote on blocks. Any user is free to register as a relay or participation node. To ensure network security, relay nodes are both diverse and decentralized. Relay nodes are run by a number of entities representing a wide array of technical, political, and organizational backgrounds across many different countries and continents. Any network participant may host a relay node.

6) Governance (Number of Nodes): The Algorand blockchain is entirely decentralized, which means there is no powerful central authority or single point of control. A unique committee of users is randomly and secretly selected to approve every block. Nodes are run by entities representing diverse backgrounds across many different countries.[9]
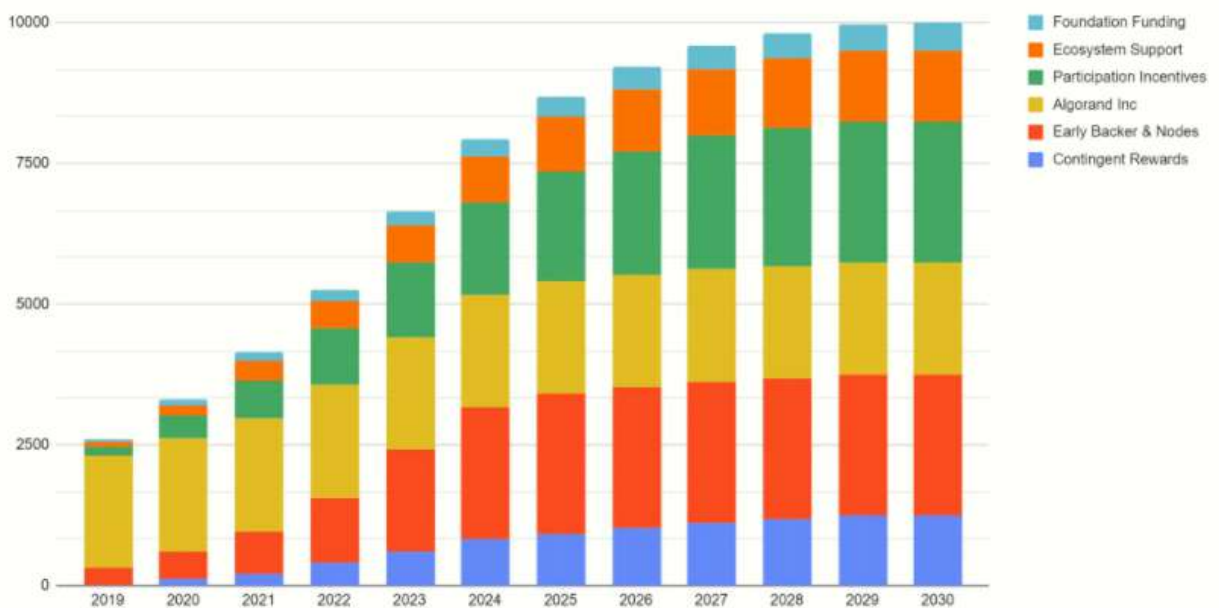
---

[9] https://algorand.foundation/algorand-protocol/about-algorand-protocol

Token Utility & Tokenomics

      Algorand's native currency, ALGO has two main functions, staking and paying for fees. Since Algorand's consensus mechanism is a form of proof-of-stake protocol, users are allowed to stake their tokens to earn passive income. All addresses that contain 1 ALGO or more will receive rewards from staking their tokens. The current annual yield on Algorand is around 5 to 6%.[10] Besides staking to earn an additional yield on your tokens, ALGO can be used as a payment facility to pay for fees within the network. Partnered with universities, institutions, and companies - Algorand is committed to secure the growth of its network by instilling a long-term plan of supply allocation(3 billion algos) as rewards to users in accordance with their participation, usage, and community governance. According to the Algorand team, Algo's tokenomics will benefit from the precise allocation of funds to community efforts such as incentives, governance participation, and ecosystem support. The table below depicts Algorands long-term distribution schedule:

Long Term Algo Distribution Schedule

Legend: Foundation Funding, Ecosystem Support, Participation Incentives, Algorand Inc, Early Backer & Nodes, Contingent Rewards

---

[10] https://www.ledger.com/staking-algorand

Nature of Token Supply

Even though the entirety of the supply was minted at the launch of the network, thus giving Algorand a fixed outstanding supply, the liquid supply will inflate as pre-minted tokens unlock and are distributed, as described below. End-user grants are dedicated to open-source developers and community members to help incentivize protocol development and innovation. ALGO's will be distributed via various programs like hackathons, competitions, and events. There will be a maximum of 10 billion ALGOs in circulation (minus the 20.5 million burned ALGOs from the inaugural auction early redemption program in Aug. 2019 as well as the 5 million burned Algos from the final auction redemption window in Jul. 2020). The ALGOs will be introduced into the network over time as follows:

- Estimated ALGOs to be injected into circulation (initially via auction, distributed over time) - 2.5 billion

- Estimated participation rewards (distributed over time) - 1.9 billion

- Early relay node runners (distributed over time) - 3.1 billion

- Algorand, Inc. - 2.0 billion & Algorand Foundation - 0.5 billion[11]

[11] https://messari.io/asset/algorand/profile
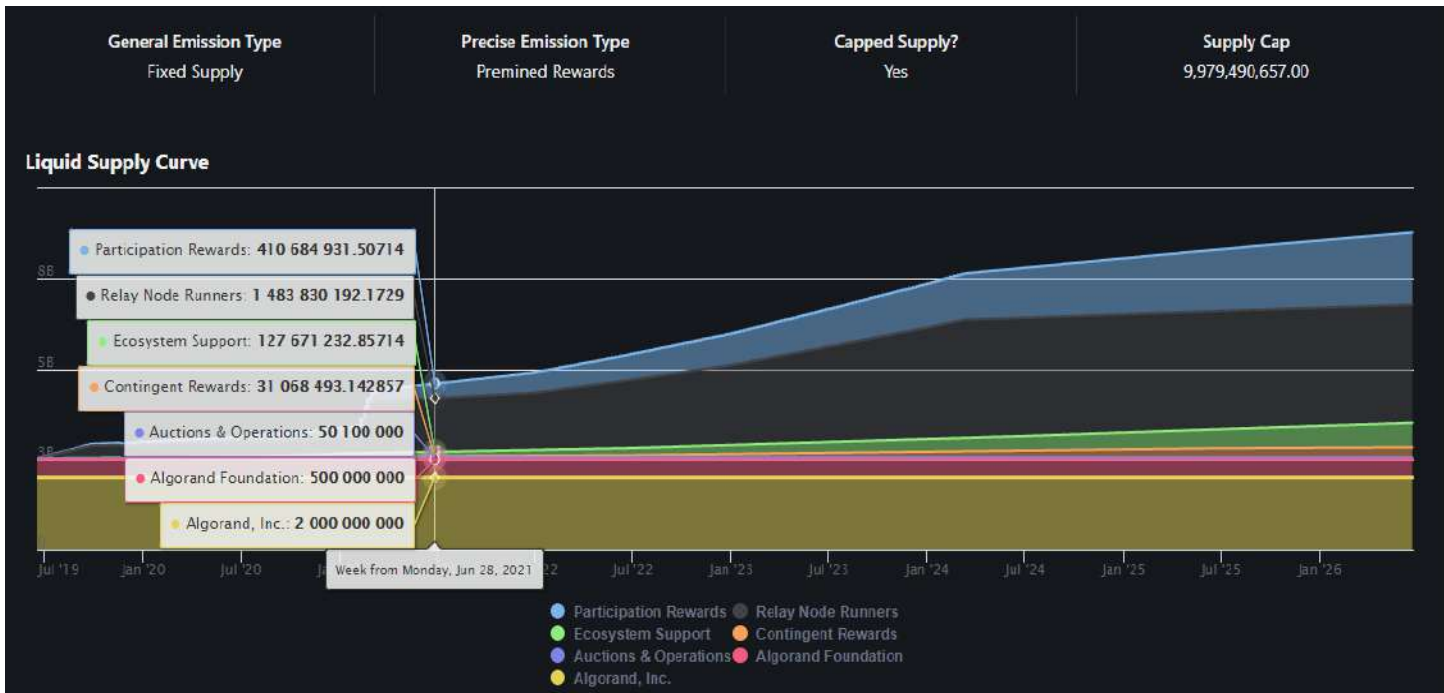
Token Burn

In Aug. 2019, Algorand offered auction investors the opportunity to receive a 90% refund on their purchased tokens. Investor returns totaled $19.9 million tokens, which constituted almost 80% of the original auction supply. The Algorand Foundation later burned these ALGOs as well as the 609,343.1208 AGLOs that address received as participation rewards (aka inflation), permanently removing them from circulation.

In Jun. 2020, the 2019 Algo auction participants who did not avail of the early redemption window in Aug. 2019 qualified to opt for a second and final Auction redemption window. Investor returns totaled five million ALGO. As occurred during the optional early redemption in August 2019, all Algos returned via this refund mechanism were burned (permanently taken out of circulation).[12] These are the only instances of token burn, and there will be no more token burn events.

Exchanges & Fiat Gateways

Algorand is listed on 45+ exchanges.[13] Algorand has 20+ fiat pairs including USD, USDT, BTC, BUSD, EUR, GBP, TUSD, KRW, UST, BNB, ETH,

		EXCHANGES				
coinbase	coinbase Pro	BINANCE		5	KuCoin	ALGO/USDT
BINANCE.US	bithumb	Huobi Huobi Global		6	Binance.US	ALGO/USD
OKEX	kraken	FTX BITFINEX		7	Binance	ALGO/BUSD
HitBTC	COINALL ETHFINEX	BitMax KUCOIN		8	Kraken	ALGO/USD
BiKi Bibox	CoinEx coinhako	BLOCKCHAIN		9	Coinbase Exchange	ALGO/EUR
gate.io HOTBIT BitAsset	Bit-Z chiliz	wazirx		10	Coinbase Exchange	ALGO/BTC
ZG CoinPark JEX	Atomars			11	Coinbase Exchange	ALGO/GBP
BiHODL Biloxy BKEX	CoinBene			12	Bitfinex	ALG/USD
Hoo BITTREX ETERBASE IDEX	DRAGON			13	Binance	ALGO/TUSD
				14	Kraken	ALGO/EUR
				15	Bithumb	ALGO/KRW

---

[12] https://messari.io/asset/algorand/profile
[13] https://www.algorand.com/ecosystem

Company History

Algorand, Inc. is a technology company founded in 2017 by cryptography pioneer, Turing award winner, and MIT professor, Silvio Micali. He designed the Algorand platform with an internationally recognized team of researchers, mathematicians, cryptographers, and economists—from first principles—to guarantee true decentralization, scale, and security.

While Micali has been a leader in cryptography since the 1980s, it is only more recently that Algorand was formed when he realized the opportunity to fulfill the promise of blockchain in the global society. With a highly regarded technical team, experienced business leaders, and a strong ecosystem Algorand aims to have an evolving impact on the DeFi space using its unique approach to blockchain.[14]

 The Algorand team is highly active on their YouTube channel and posted 96 videos in the last 2 years. Their YouTube channel includes Developer's Office Hours, Blockchain Basics, and explanations by the founder, Silvio Micali.[15] Silvio Micali also gave a TedX talk in December 2019.[16]

All-Star Team

Algorand's leadership team consists of 13 Employees and 13 Advisors.[17] LinkedIn lists a total of 145 employees. 61 are key employees, which includes 12 from the leadership team and 49 from other positions, such as software engineers and data analysts. 84 are brand ambassadors, investors, etc, who are not included in the count.[18] Algorand's team consists of 9 all-stars. The team is made up of internationally recognized researchers, mathematicians,

---

[14] https://www.algorand.com/about/our-history
[15] https://www.youtube.com/c/Algorand/videos
[16] https://www.youtube.com/watch?v=YW8Tn6Q4TRE
[17] https://www.algorand.com/about/our-team
[18] https://www.linkedin.com/company/algorand/people/

cryptographers, and economists along with proven business leaders from global technology companies.[19]

Silvio Micali - Founder:

- Faculty at MIT, Electrical Engineering and Computer Science Department, since 1983.

- Co-inventor of probabilistic encryption, Zero-Knowledge Proofs, Verifiable Random Functions, and many of the protocols that are the foundations of modern cryptography. Recipient of the Turing Award (in computer science), the Gödel Prize (in theoretical computer science), and the RSA prize (in cryptography).

Steve Kokinos - CEO:

- Co-founder and Executive Chairman of Fuze, a company with 700 employees servicing over 1500 enterprise customers around the world.

- Co-founder of BladeLogic, Inc., a recognized leader in the data center automation market with a Fortune 500 client list. Bladelogic held a successful IPO and was later acquired by BMC Software for ~$800M.

W. Sean Ford - COO:

- Chief Marketing Officer at LogMeIn. He also ran the Integration Management Office for LogMeIn's acquisition of Jive Communications in early 2018 and vice-president of Global Business Unit (GBU) marketing at Oracle.

Chris Hurley - Head of Investor Relations and Capital Markets:

- Member of the executive team at Fuze where he helped to grow the company from an early-stage startup to a global company with several hundred employees.

---

[19] https://www.algorand.com/about/our-team

- Member of the Corporate Development team at Sun Microsystems where he was responsible for M&A and strategic alliances totaling more than $1B in revenue. His time at Sun concluded as part of the team that completed Oracle's $7.5B acquisition of Sun.

Leadership

Silvio Micali has been on the faculty at MIT, Electrical Engineering and Computer Science Department, since 1983. Micali's research interests are cryptography, zero-knowledge, pseudorandom generation, secure protocols, and mechanism design, and blockchain. In particular, Micali is the co-inventor of probabilistic encryption, Zero-Knowledge Proofs, Verifiable Random Functions, and many of the protocols that are the foundations of modern cryptography. In 2017, Micali founded Algorand, a fully decentralized, secure, and scalable blockchain that provides a common platform for building products and services for a borderless economy. At Algorand, Micali oversees all research, including theory, security, and crypto finance. Micali is the recipient of the Turing Award (in computer science), the Gödel Prize (in theoretical computer science), and the RSA prize (in cryptography). He is a member of the National Academy of Sciences, the National Academy of Engineering, the American Academy of Arts and Sciences, and Academia dei Lincei. Micali has received his Laurea in Mathematics from the University of Rome, and his Ph.D. in Computer Science from the University of California at Berkeley.[20]

---

[20] https://www.algorand.com/about/from-our-founder

Customers & Partners

With more than 500 global organizations leveraging its technology, Algorand is enabling the simple creation of next-generation financial products, protocols, and exchange of value across defi, financial institutions, and governments.[21] Along with major company partners, Algorand has ~13.3 million users worldwide.[22] One recent key partnership is SIAE, one of the largest rights management companies founded in 1882, launching 4 Million NFTs on Algorand representing the rights of nearly 100,000 creators.[23]

---

[21] https://www.algorand.com/ecosystem
[22] https://metrics.algorand.org/
[23] https://www.algorand.com/resources/news/siae-launches-4-million-nfts-on-algorand-for-creators

Competition

Algorand is the only Pure Proof of Stake (PPoS) platform. Their main competitors include Ethereum, Cardano, & Polkadot. These competitors are also focusing on creating open-source blockchain networks. They are currently leading Algorand as Ethereum is 2nd in overall cryptocurrency market cap, Cardano 3rd, and Polkadot 8th.

- Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform. After Bitcoin, it is the second-largest cryptocurrency by market capitalization. Ethereum is the most actively used blockchain.[24]

- Cardano is a public blockchain platform. It is open-source and decentralized, with consensus achieved using proof of stake. It can facilitate peer-to-peer transactions with its internal cryptocurrency, Ada. Cardano was founded in 2015 by Ethereum co-founder Charles Hoskinson.[25]

- Polkadot is a sharded heterogeneous multi-chain architecture that enables external networks as well as customized layer one "parachains" to communicate, creating an interconnected internet of blockchains. The protocol was created by the Ethereum co-founder Gavin Wood.[26]

---

[24] https://en.wikipedia.org/wiki/Ethereum
[25] https://en.wikipedia.org/wiki/Cardano_(blockchain_platform)
[26] https://en.wikipedia.org/wiki/Polkadot_(cryptocurrency)

Early Investors

Algorand raised $62 million in a venture funding round during October 2018. The funding comes from a list of about 30 blockchain-focused investors from all over the world, including Australia-based Polybius Capital, Singapore-based NEO Global Capital, London-based Eterna Capital, Boston-based venture capital firm Pillar, and New York-based Union Square Ventures.[27]

Community Size

Algorand has a fairly large community:

Telegram - 31,261 members

Reddit - 37,500 members

Discord - 11,688 members

Twitter - 139,800 followers

YouTube - 8,880 subscribers

Facebook - 66,548 followers

---

[27] https://www.bizjournals.com/boston/news/2018/10/24/mit-born-blockchain-startup-algorand-gets-62m-and.html

Verdict

Algorand has the capability to be a major player in the cryptocurrency space in the coming years. Built by an extremely strong team of Ph.D. award winners and researchers, Algorand's unique Pure Proof of Stake blockchain technology stand's out amongst the competition. In addition, Algorand is battle-tested: Over 7 days in September 2021, Algorand had 8.27 million transactions, averaging around 1.1 million per day - peaking at 1,154 TPS. With over 1262 nodes and ~13.3 million users worldwide, Algorand is one of the largest blockchain ecosystems currently.

Algorand is trading near its most recent highs, up more than 100% since August 2021. It is currently down only $.50 from its recent highs of $2.54 in early September 2021. With the current price and market cap, Algorand has the potential to break into the top 10 in the future. Although Algorand does not offer the fastest blockchain in the industry, it does have the potential to attract traditional developers and companies looking to enter the blockchain space. By providing the technical capacity to handle a huge amount of network volume and a stable, robust governance model, Algorand is positioned as the ideal alternative to host transactions for traditional financial networks. Functioning with no downtime and consistently high performance over the past two years, Algorand hopes to absorb market share from other inferior networks.

After evaluating the project in its entirety, the Token Metrics team scored Algorand objectively, and the results were the following:

Fundamental Score - 82%

Community - 5/5	Competition - 4/10	Team - 15/15
Use Case - 19/20	Investors - 14/15	Token Distribution - 6/10
Audit - 0/10	ROI Potential - 8/10	Tokenomics - 7/10