July 6, 2022

Digital Assets Research
Cryptocurrencies

Author:

Ali Mostafa
ali.mostafa@crosstower.com | Linkedin

Contributor:

Mitch Goulson
Linkedin

Algorand Primer

Overview

Algorand is a smart-contracts platform and blockchain network capable of performing rapid transactions with low fees and carbon output.[1] Silvio Micali, a Turing award winner[2] and professor at MIT whose work provided the foundation for modern cryptography, founded the project in 2017. Algorand can process over 1,000 transactions per second (TPS) while achieving transaction finality almost instantaneously.

The protocol charges a tiny fraction of ALGO, the blockchain's native token, to perform transactions on the network as well as to participate in consensus and governance. The supply of ALGO is capped at 10 billion, which was minted entirely at genesis. While a portion of the ALGO supply is withheld, there is a schedule to distribute the remaining supply into circulation transparently by 2030.

Users incur little risk and cost to participate in Algorand's consensus protocol. The network uses a novel variant of the Proof of Stake (PoS) consensus mechanism, called Pure Proof of Stake (PPoS), to resolve the tradeoffs between scalability, decentralization, and security. Although users may find consensus participation reasonably straightforward, there are no rewards tied to the activity.[3] However, users can earn rewards for their participation in governance.

Algorand is a relatively new blockchain platform with an active research and development team. Algorand launched its TestNet in April 2019[4] and its MainNet in June 2019[5]. Later that same year, smart contracts and other new features were introduced to the platform. More recent features include expanding smart contract

Contents	***Page***

1 https://algorandcom.cdn.prismic.io/algorandcom%2Fece77f38-75b3-44de-bc7f-805f0e53a8d9_theoretical.pdf

2 http://www.ams.org/notices/201306/rnoti-p762.pdf

3 https://www.coindesk.com/markets/2017/04/04/no-incentive-algorand-blockchain-sparks-debate-at-cryptography-event/

4 https://www.algorand.com/resources/algorand-announcements/algorand-publicly-opens-testnet

5 https://www.algorand.com/resources/blog/the-borderless-economy-is-here

capabilities and establishing an interoperability standard utilizing post-quantum cryptography.

Two entities independently oversee the Algorand ecosystem: Algorand Inc. and the Algorand Foundation. The former is a private company focused on developing the Algorand technology and the latter is a non-profit that focuses on the developing the ecosystem. The team consists of accomplished business leaders and experts with backgrounds in mathematics, cryptography, and economics. Algorand collaborates with academic institutions around the world through partnerships and other initiatives and has successfully raised capital from the private sector to develop its ecosystem and fund its initiatives.

Pure Proof of Stake

PoS protocols, while efficient, face a dilemma on how the network can scale without compromising security and decentralization. PPoS innovates on previous PoS mechanisms by employing a cryptographic sortition process driven by a Verifiable Random Function (VRF). PPoS is relatively eco-friendly because participants do not need to exhaust significant resources to compete with one another.

PPoS connects the security of Algorand to the stake of the majority of honest users on the network. The term "stake" in the context of PPoS refers to the stake of all coins held by online participants. “Honest users” are online users that do not deviate from the protocol.[6] To prevent centralization on the network, Algorand employs random selection at each stage of the consensus protocol. In other words, validator selection under PPoS behaves as a weighted lottery draw. The size of a participant’s stake only increases the chance of being chosen; the outcome of the lottery draw decides the voting power. This design protects the system from spam by discouraging users from generating multiple accounts. The secret and randomized process ensures the safety of the network and concurrently provides security for consensus participants. The process is resilient to network-level attacks, as the attacker must own a substantial majority of the online participation stake.

Non-Relay Nodes

PPoS, unlike PoW, is neither an energy-intensive nor a resource-intensive consensus protocol. Consensus participants face low hardware requirements as each user runs the same functions with little computational effort. There are over 1,700 nodes on the Algorand network since MainNet launch.[7]

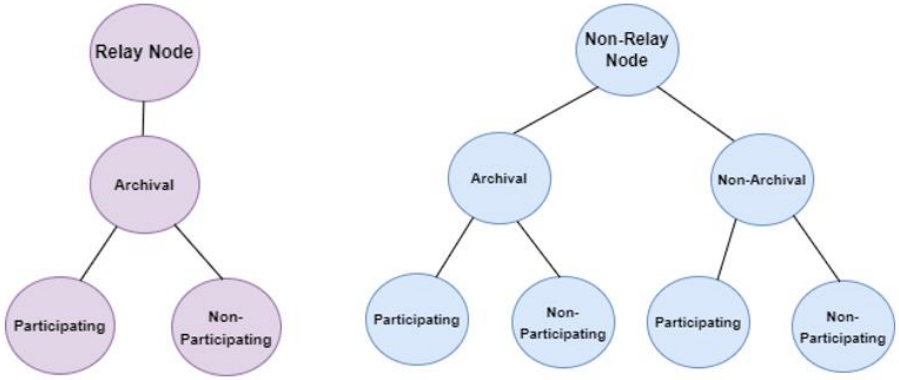
Nodes on the Algorand network can primarily be either Relay or Non-Relay. Each type holds different properties and performs separate functions on the network. Non-Relay nodes connect only to other Relay nodes but never to other Non-Relay

6 https://github.com/algorandfoundation/specs/releases/download/untagged-953b268814f6ffb693e4/abft.pdf

7 https://metrics.algorand.org/#/decentralization/

nodes. Also, Non-Relay nodes can connect to several Relay nodes simultaneously. Relay nodes must be Archival and store the entire blockchain, whereas Non-Relay nodes can be Non-Archival and only store the last 1,000 blocks of the Algorand blockchain[8]. Users running Archival nodes have the option of installing the Algorand Indexer[9], a service that allows Archival nodes to search and retrieve information much faster than alternative methods.

Exhibit 1. Node Types on Algorand



Note: Algorand does not recommend running a Relay Participating node.
Source: Algorand & CrossTower Research

Consensus participants generally run online Non-Relay Participation nodes. Participation nodes propose and vote on new blocks to add to the Algorand blockchain. Non-Relay nodes are suitable for consensus participation, as their operation does not require specialized hardware. Users can run a Non-Relay node with an ordinary laptop and internet connection.[10] There is no monetary incentive to run a Participation node. Instead, users are encouraged to run Participation nodes to secure and decentralize the Algorand network.

Relay nodes perform separate functions besides participating in consensus. Both Relay and Non-Relay nodes can operate as Participation nodes; however, Relay nodes runners are discouraged from consensus participation so that they can operate on the network safely.[11]

Relay Nodes

Relay nodes serve as hubs on the Algorand network, routing information to both Relay and Non-Relay nodes. A valid Relay node accepts incoming connections publicly and has both a public IP address and an assigned port registered in Algorand's service (SRV) records.

8 https://developer.algorand.org/docs/run-a-node/reference/config/

9 https://developer.algorand.org/docs/run-a-node/setup/indexer/

10 https://algorand.foundation/algorand-protocol/network

11 https://developer.algorand.org/docs/run-a-node/reference/artifacts/#phonebookjson

While anyone can run a Relay node[12], the average user may find running one very expensive or simply infeasible due to their location. On the Algorand network, Relay nodes are highly connected and must be able to support a great deal of traffic. Since Algorand can process millions of transactions per week[13], relay node operators must be capable of storing sizable amounts of data.[14] In contrast, users can run a Non-Relay node with consumer-grade equipment and a network connection.[15] Moreover, there is no reward mechanism for running Relay nodes outside of token rewards issued by the Algorand Foundation to early backers of the project. The distribution occurred through a non-inflationary algorithm called "Algorithmic Vesting."

Due to the performance requirements, both public and private institutions lead the effort of running Relay nodes. Algorand Inc. and the Algorand Foundation run Relay nodes themselves alongside early backers of the project. There are currently over 100 Relay nodes running on the Algorand network.[16] The Algorand Foundation funded early backers of the project through incentive programs[17]. Early backers and many universities agreed to commit their resources to Algorand to ensure that messages are transmitted throughout the network optimally. The Algorand Foundation set 25% of the total supply of ALGO aside to distribute as rewards according to a multi-year vesting schedule slated to end in 2030.[18]

The Algorand Foundation set a course to decentralize Relay nodes on the network.[19] The Foundation recently announced that their new community pilot program, which went live on March 1st, 2022[20] has added 21 Relay nodes on six continents. Most Relay nodes currently are verified, but it is possible to run a permissionless Relay node.

Relay nodes run publicly on the Algorand network and the majority are permissioned by the Algorand Foundation. Algorand's SRV records contain the list of all verified Relay nodes. All valid Relay nodes publicize themselves when connecting to the Algorand network, either by using the SRV records or through other verified Relay nodes. Additionally, Relay nodes must connect to a verified Relay node and advertise their IP address to operate publicly.

The concentration of institutional involvement in the operation of Relay nodes raises the issue of centralization; however, it is important to consider that Participation nodes, not Relay nodes, perform consensus under PPoS. Relay nodes

12 https://developer.algorand.org/docs/run-a-node/reference/relay/

13 https://metrics.algorand.org/

14 https://forum.algorand.org/t/whats-the-current-mainnet-testnet-archival-nodes-ledger-data-size/3146

15 https://www.algorand.com/resources/blog/algorand-raspberry-pi

16 https://algorand.foundation/faq#running-nodes-

17 https://algorand.foundation/faq

18 https://algorand.foundation/governance/algo-dynamics/

19 https://algorand.foundation/news/community-relay-node-running-pilot

20 https://algorand.foundation/news/community-relay-node-program-live-march

are public message routers, propagating messages throughout the network. Non-Relay nodes operate privately because they send and receive messages with every connected Relay node and never with another Non-Relay node. Although Relay nodes can technically participate in consensus, their influence is limited to their participation stake, and Relay nodes would be unable to participate in consensus privately.

A malicious actor cannot influence consensus under PPoS -- even if they could compromise every Relay node on the network -- because the attack still requires a substantial majority of the participating stake of ALGO. If one or more Relay nodes behave maliciously or suffer an outage, all online nodes will connect to other valid Relay nodes. The difference is that offline Relay nodes cannot transmit messages.

When Relay nodes behave maliciously, they send inconsistent messages to every node on the network. Honest nodes will ignore these messages because they will receive legitimate messages from valid Relay nodes. If only one Relay node remains valid, all traffic will route to that node, and the network may function slowly. If all Relay nodes are offline or behave maliciously, the network stalls until valid Relay nodes come back online.[21]

Consensus

PPoS has minimal performance requirements because the VRF computation is fast and not computationally intensive. The mechanics of the VRF are technical and beyond the scope of this primer[22]; however, VRF's role in PPoS is to enable the sequence of lottery draws involving all online participants and their ALGO.[23]

Only online Participation nodes on the Algorand network can propose and vote on new blocks. A user who wants to set up a Participation node must use their account to generate a set of participation keys[24]. These keys are then registered online with the network through a registration transaction[25]. Later, the keys are stored in the node's ledger directory once the transaction processes on the blockchain.

Participation keys are a VRF key pair and a set of single-round voting keys. The collection of one-time use keys is aptly named "ephemeral keys" because the key is removed from the set after every round. Spending keys are different from Participation keys as the former authorizes transactions while the latter provides a layer of security for consensus participants.[26] Since the selection process requires accounts to use their Participation keys, account balances are safe from

21 https://www.algorand.com/resources/algorand-announcements/algorands-instant-consensus-protocol

22 https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf

23 https://developer.algorand.org/docs/get-details/algorand_consensus/#verifiable-random-function

24 https://developer.algorand.org/docs/run-a-node/participate/generate_keys/

25 https://developer.algorand.org/docs/get-details/transactions/#register-account-online

26 https://developer.algorand.org/docs/get-details/algorand_consensus/#participation-keys

unauthorized transactions. Also, a malicious node cannot use old voting keys to forge an old block because the ephemeral set does not contain used keys.

PPoS employs VRF to select committees to complete the consensus process. Algorand achieves consensus and finalizes blocks in three steps: block proposal, soft vote, and certification vote. Every block on the Algorand blockchain reveals a new unpredictable seed that is propagated to all online nodes. Participation nodes privately evaluate the VRF with a public random seed and their credentials. Since the selection process occurs privately, an adversary cannot know which nodes to target in advance to disrupt consensus.[27]

Exhibit 2. Steps in Algorand Consensus

Source: Algorand & CrossTower Research

Recall that the term "stake" refers to the amount of ALGO held in the accounts of consensus participants. PPoS does not impose commitments or penalties on consensus participants regarding their account balance. The VRF component of the participation key enables the lottery draw that will determine participants at each step. The lottery consists of all ALGO held by online participants, where each token functions as a lottery ticket. Participants are selected with voting power based on their stake of ALGO, or winning lottery tickets.

PPoS has properties that make Algorand resilient against blockchain forks.[28] Block agreement and finality occur instantly in each round under PPoS; two different block candidates cannot appear simultaneously in the same round because one block at most can be certified and written to the ledger.[29] The speed of PPoS allows transactions to process on the Algorand network quickly and securely. Algorand can process 1,000 TPS while offering low transaction fees to its users.

The first stage in the consensus protocol is the block proposal stage. Online Participation nodes will aggregate pending transaction data they receive to form blocks. A new round in consensus begins by selecting an account to propose a block. Each online participant executes the VRF to determine their status as block proposers. Selected participants will distribute their proposal to all other online nodes, along with cryptographic proof that the proposer was legitimately selected.

27 https://www.algorand.com/technology/protocol-overview

28 https://www.algorand.com/resources/blog/runtime-verification

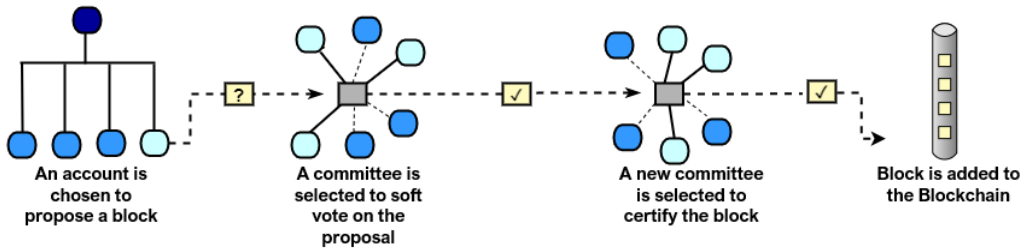
29 https://www.algorand.com/resources/algorand-announcements/algorands-instant-consensus-protocol

The sortition process may select several accounts simultaneously to propose blocks that are filtered at the next stage.

Newly proposed blocks are circulated among Participation nodes for verification in the next stage for a soft vote. The goal is to narrow down block proposals to one primary block that will move ahead for a final vote. Online participants will use VRF to compare hashes from the cryptographic proof to rank blocks by priority. Next, VRF is used to conduct a second lottery draw that will form a committee to vote on block proposals. Participation nodes will again run the VRF on their managed accounts to determine committee membership. The voting power of selected committee members and committee size depends on the outcome of the lottery. Participants selected for the soft vote committee will vote to verify or reject the block proposal. All other online nodes observe the outcome of the soft vote by counting votes and verifying signatures. When a supermajority is reached to approve a block proposal, the block will go on to the final stage for certification.

The final stage of the PPoS consensus protocol certifies blocks proposals that were verified at the previous stage. The voting process and formation of committees in the certification stage are analogous to the soft vote stage. Another committee is formed using VRF to select members. The new committee first checks the proposal for any inconsistencies before validating the block for a certification vote. If the block is deemed valid, committee members will vote to certify the block. The results of the vote are sent to all other Participation nodes on the network. Votes are counted and validated until a supermajority is reached. Once a quorum is met by the network, the block will be certified and written to the Algorand ledger. The newly added block reveals a new random seed that is announced to the network, which begins a new round in the consensus protocol.

Exhibit 3. PPoS Consensus Protocol



Source: Algorand & CrossTower Research

In conventional consensus mechanisms such as PoW and some variants of PoS, blocks undergo a time-lapse between proposal, agreement, and finality. In the case of PoW, valid blocks must be confirmed on the network several times before they are final.[30] During this time, the blockchain can fork if the network cannot agree on

30 https://www.sciencedirect.com/science/article/pii/S2352864819301476

the order to add candidates to the blockchain. Conversely, agreement on PPoS is instant, and the Algorand network is resilient against a network attack or partition.

Attempts to maliciously influence consensus are costly since PPoS ties consensus to all ALGO held by online participants. In theory, the Algorand protocol is secure so long as at least 2/3 of the voting stake is held by honest participants at any given time.[31] Algorand also protects the history of the blockchain by using ephemeral voting keys to prevent an adversary from repropagating old blocks. Moreover, Algorand would recover quickly if the network stalls.

During a network partition or an outage, users will enter partition recovery mode. When partition recovery mode is activated, users will continuously transmit recovery messages. Once a valid Relay node resumes operation, these messages are circulated throughout the network rapidly until a threshold is reached that will trigger synchronization by nodes and allow the blockchain to advance.

Governance

Algorand moved to a decentralized governance model to facilitate community participation in economic and policy decisions surrounding the platform and ecosystem. The Algorand Foundation launched the Community Governance program in October 2021.[32] There are four quarterly governance periods per calendar year with at least one voting session per period. Users can participate in governance and earn rewards by committing their ALGO for the duration of the governance period.

The Community Governance program allows the Algorand community to shape the future of the platform and ecosystem. Similar to consensus participation, governance participation is voluntary and voting power is commensurate with the amount of ALGO held by the participant.[33] Unlike consensus participation, users participating in governance are rewarded for their effort and are required to lock their tokens for the duration of the governance period. Governance does not require users to run a Participation node; however, consensus participants are encouraged to participate in governance.

Algorand users can become Governors by visiting Algorand's Governance portal during the signup period and connecting their non-custodial wallet to commit their ALGO. Since one ALGO equals one vote, voting power is proportional to the amount of ALGO committed during the governance period. Governance works in quarterly periods, during which the Algorand Foundation submits at least one proposal to all Governors each period. Proposals include an information package to assist Governors in making informed decisions. Governors vote on a variety of issues such as grant approvals and platform developments.

31 https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf

32 https://algorand.foundation/governance

33 https://www.algorand.com/resources/blog/decentralizing-algorand-governance-nov2020

There is no maximum nor minimum number of Governors, as the program is open to all users willing to commit their ALGO. Governors that fulfill their obligations can claim rewards at the end of the period, but Governors that leave the program early will lose their rewards for the period.[34] To be compliant, users must commit their ALGO for the 90-day voting period and vote on all measures. There is an option to vote with the Foundation, which places a Governor's vote on the Algorand Foundation's preferred choice. It is important to note the Foundation does not participate in governance, and hence cannot earn rewards.

Tokenomics

The native token on the Algorand blockchain is ALGO, which has a maximum supply of ten billion. The minimum divisible unit of an ALGO is a microAlgo, or 0.000001 ALGO.[35] The entire supply was minted at the genesis block, but a portion remains outside circulation. The Algorand Foundation has released a multi-year schedule to diffuse the non-circulating ALGO into the ecosystem.

The Algorand ecosystem is accessible to all types of users because transactions on Algorand are quick and inexpensive. The ALGO token has several trading pairs listed on many exchanges. The token is used to pay fees associated with processing transactions and smart contract functions. Fees on Algorand are low, as most transactions cost 0.001 ALGO to process.

The Algorand Foundation minted the ALGO token and released it into circulation in June 2019.[36] The Foundation sold 25 million ALGO using a public Dutch auction which raised a total of $60 million, or $2.40 per ALGO.[37] The auction came with the right of token holders to resell their tokens at a later date back to the Foundation at 90% of the purchase price.[38] About 80% of the tokens sold during the auction were returned by investors, amounting to approximately $19.9 million.[39] These tokens were redeemed and burned by the Foundation, in addition to 609,343 ALGO that addresses would have received as participation rewards.[40]

Algorand previously had an algorithmic vesting program in place designed to reward early backers. The early backers committed resources to bootstrap the project in exchange for future token allocations when certain conditions were met. Vesting of the token would be slow and linear under normal market conditions according to the algorithm but would accelerate if the market conditions were

34 https://community.algorand.org/blog/ensuring-true-decentralization-on-algorand-with-the-proposed-right-to-participate-in-governance/

35 https://www.algorand.com/resources/blog/rewards-technical-overview

36 https://algorand.foundation/news/algorand-foundation-transparency-report----june-19th

37 https://www.coindesk.com/markets/2019/06/19/algorand-raises-60-million-in-token-sale/

38 https://algorand.foundation/auction-refund

39 https://algorand.foundation/news/the-algorand-foundation-today-confirm-token-burn

40 https://algorandfoundation.cdn.prismic.io/algorandfoundation/5c80fdd2-fe08-4bda-8ac5-981b37908031_Early+Redemption+Confirmation.pdf

considered sufficiently positive by the algorithm to absorb vesting without inflationary effects. The early part of 2021 triggered multiple accelerated events and strong price action in September of that year led to the program's conclusion the following month. Consequently, 3.1 billion ALGO tied to the program have vested, leading to over 6 billion ALGO entering the supply years ahead of schedule.

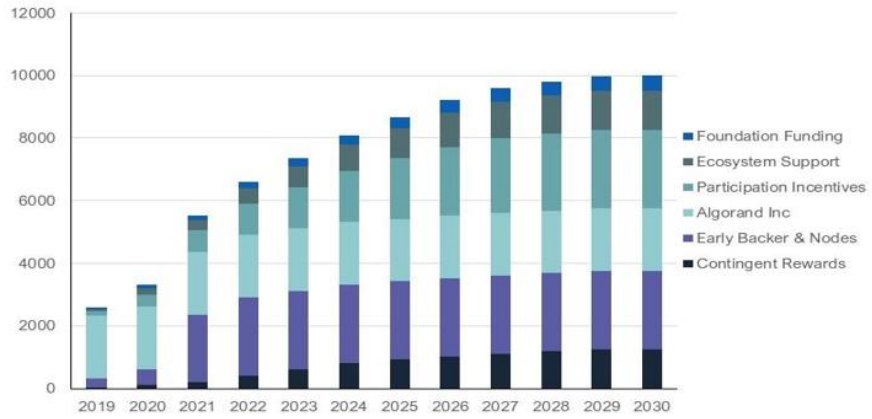
Exhibit 4. Long Term ALGO Distribution Schedule I

Token Allocation	Supply (MM)	% of Total
Community Incentives		
Participation Rewards	2,500	25%
Early Backers Relay Nodes	2,500	25%
Contingent Incentives	1,200	12%
Total	6,200	62%
Ecosystem Support		
Innovation Fund	400	4%
Protocol R&D and Capital Markets Innovation	400	4%
Foundation Algo Grant Program	250	3%
Research and Social Good Program	200	2%
Total	1,250	13%
Initial Allocation		
Algorand Inc	2,000	20%
Algorand Foundation	500	5%
Already Injected for Operations and Ecosystem	50	1%
Total	2,550	26%
Grand Total	10,000	

Source: Coin98 and CrossTower Research

Algorand defines circulating supply as available on-chain ALGO without contract restrictions.[41] About 66% of the total supply of ALGO is in circulation.[42] The tokenomics of Algorand is currently inflationary. However, a revised distribution schedule was launched by the Algorand Foundation in 2021 to provide clarity on how non-circulating ALGO will diffuse into the total supply.

Exhibit 5. Long Term ALGO Distribution Schedule II



Source: Algorand & CrossTower Research

Algorand's Long Term Algo Dynamics (LTAD) allocated approximately 3.2 billion ALGO to support the ecosystem over the next several years.[43] The ALGO is held

41 https://algorand.foundation/governance/algo-dynamics

42 https://algoexplorer.io/

43 https://prismic-io.s3.amazonaws.com/algorandfoundationv2/dcbe6c89-251a-41b3-9c78-

in the Algorand Ecosystem Resource Pool that is governed by the Algorand Community Governance program.[44] The multi-year program was designed to allocate resources to long-term activity on the blockchain such as community incentives, governance participation, and ecosystem support. Other ALGO earmarked for rewards fall under "contingent incentives," which are reserve funds to help the Foundation and Governors address unexpected challenges to growing Algorand. The LTAD program is expected to conclude in 2030 when the ALGO supply is in full circulation. However, any long-term plan is subject to change by community governance, as Governors can influence the allocation flow. While the Foundation's 500 million ALGO will be "used for the independence and autonomy of the Foundation and the Foundation activities", the Foundation will not use it for governance, meaning they will not vote nor receive direct network rewards.[45]

Community rewards and transparency are key facets of Algorand's tokenomics. The Algorand Foundation has provided transparency reports every six months since November 2019.[46] Transparency reports offer the Algorand community insights into token holdings, usage, and flows of accounts managed by Algorand, as well as updates on the dynamics of the ALGO supply. Additionally, the Algorand Foundation publicly displays the list of accounts managed by Algorand, partners, and early backers.[47]

Development

Algorand Inc. built the Algorand protocol and oversees its technological development. Its development team releases new updates, products, and features and implements changes approved by the Algorand community. Since February 2022, Algorand has maintained an official non-custodial wallet in collaboration with Hipo Labs.[48] Currently, Algorand offers software developer kits in four languages: Python, JavaScript, Go, and Java.[49] In November 2019, a few months following its MainNet launch, Algorand released Algorand 2.0 that introduced primary layer-1 capabilities such as smart contracts to its network.

Algorand 2.0 was a crucial update that enabled the blockchain to provide solutions for real-world use cases.[50] Key features included smart contracts, the Algorand standard asset (ASA), and atomic transfers. Recent developments on Algorand include establishing an interoperability standard using advanced smart contract capabilities and post-quantum cryptography. The development team is also

23d8ecabd6c1_Algo+Economic+Evolution+Report+Sept+2021.PDF

44 https://algorand.foundation/news/accelerated-vesting-complete

45 https://algorand.foundation/the-algo/transparency-report-september-2021

46 https://algorand.foundation/governance/transparency

47 https://algorand.foundation/updated-wallet-addresses

48 https://blog.perawallet.app/its-official-algorand-wallet-is-now-pera-wallet-171561597664

49 https://developer.algorand.org/docs/sdks/

50 https://www.algorand.com/resources/algorand-announcements/algorand-foundation-launches-protocol-upgrade-2.0

working to improve core capabilities such as decreasing block finality and increasing TPS up to 45,000.[51]

Algorand smart contracts enable decentralized application (Dapp) development. The Algorand Virtual Machine (AVM) is akin to the Ethereum Virtual Machine[52] (EVM) except that AVM supports Transaction Executed Approval Language[53] (TEAL)[54]. The latest version of the AVM allows smart contracts to generate transactions and function as escrow accounts.[55] Although Algorand is not EVM-compatible, developers can write smart contracts in higher-level languages such as Python with the PyTEAL library or Reach.[56] However, the Algorand Foundation sponsors initiatives that aim to bring EVM-compatibility in the future.[57]

There are two types of smart contracts on Algorand: Smart contracts and Smart Signature contracts. The difference between the two is that Smart Signature contracts do not store any on-chain data or access on-chain values, whereas Smart contracts live on-chain and access several on-chain values. Both types of contracts allow developers to build Dapps that use Algorand's layer-1 features, but Smart Signature contracts allow for larger or more complex interactions to occur off-chain.[58] Algorand also supports Contract-to-Contract calls which allow smart contracts to call or create another smart contract using additional transactions.[59] Contract-to-Contract calls extend the functionality of smart contracts to enable efficient and trustless interactions between Dapps.[60]

The ASA allows for the creation of assets on the blockchain.[61] ASA assets are on-chain and inherit the security, compatibility, and speed from the Algorand network. Algorand supports both fungible assets and non-fungible assets. Examples of fungible assets include currencies, stablecoins, and utility tokens. Users can create non-fungible tokens[62] (NFTs) at low cost without the risk of duplication by a fork in the chain[63]. Algorand accounts must opt-in to receive a specific asset as it increases the minimum wallet balance by 0.1 ALGO.[64] Accounts with sufficient ALGO balances can create an ASA on Algorand or through open-source web-

51 https://www.algorand.com/resources/blog/algorand-building-scalable-sustainable-blockchain-ecosystem

52 https://ethereum.org/en/developers/docs/evm/

53 https://developer.algorand.org/docs/get-details/dapps/avm/teal/

54 https://cypherpunks-core.github.io/ethereumbook/13evm.html

55 https://developer.algorand.org/articles/discover-avm-10/?from_query=avm%201.0

56 https://developer.algorand.org/docs/get-started/dapps/

57 https://www.coindesk.com/tech/2022/02/18/algorand-pushes-for-ethereum-compatibility-with-20m-incentive-program

58 https://developer.algorand.org/articles/stateful-smart-contracts-rekeying-fast-catchup/

59 https://developer.algorand.org/articles/contract-to-contract-calls-and-an-abi-come-to-algorand/

60 https://medium.com/algorand/hello-contract-calling-abff8fc00939

61 https://developer.algorand.org/docs/get-details/asa/

62 https://developer.algorand.org/articles/building-nfts-on-algorand/

63 https://www.algorand.com/resources/blog/issuing-nfts-on-a-forkless-blockchain

64 https://developer.algorand.org/docs/get-details/asa/#receiving-an-asset

based tools[65]. Accounts are not limited to the number of assets they can create or hold.[66]

Other layer-1 features include Atomic transfers and Rekeying. Atomic transfers guarantee the simultaneous transfer of assets among several parties.[67] Up to 16 transactions can be submitted as a group, but the transfer will only succeed if none of the transactions fail.[68] Rekeying allows accounts to change their private spending key while preserving their public wallet address.[69] This allows for both continuity and operational efficiency in that users no longer need to create a new wallet should their private keys be compromised.[70]

Algorand's latest upgrade introduces an interoperability standard generated by post-quantum cryptography.[71] In March 2022, Participation nodes began to generate and register a set of Falcon keys alongside their participation keys.[72] Falcon keys are used to generate Algorand State Proofs (ASPs), a post-quantum chain of certificates[73] attesting to the state of the Algorand blockchain. Algorand State Proofs (ASPs) is an interoperability standard that facilitates cross-chain communication with post-quantum security.[74] ASPs allow Algorand to connect to other blockchains without trust in an intermediary, while providing a robust and verifiable source of truth about the state of the Algorand blockchain.

Partnerships

Algorand has fostered ties internationally with both private and public institutions. Several universities have partnered with Algorand to advance blockchain education, and support community development and research. Algorand has also been able to attract millions of dollars in capital from private equity firms interested in the project and the ecosystem.

Algorand has sparked interest from institutional investors and private equity. As a startup, Algorand raised $4 million in seed money from Pillar Companies and Union Square Ventures in February 2018.[75] In July 2020, Valkyrie set up the Valkyrie Algorand Trust for institutional investors looking for exposure to ALGO.[76] More recent investments include a $100 million Arrington Algo Growth Fund set up in

65 https://algorand.foundation/news/algodesk-development-award

66 https://developer.algorand.org/articles/algorand-unlimited-assets-and-smart-contracts/

67 https://medium.com/algorand/algorand-atomic-transfers-a405376aad44

68 https://developer.algorand.org/docs/get-details/atomic_transfers/

69 https://www.algorand.com/Feature%20Brief_Algorand%20Rekeying.pdf

70 https://developer.algorand.org/articles/stateful-smart-contracts-rekeying-fast-catchup/

71 https://github.com/algorand/go-algorand/releases

72 https://www.algorand.com/resources/algorand-announcements/algorand-network-upgrade-expands-smart-contract-functionality

73 https://people.csail.mit.edu/nickolai/papers/micali-compactcert-eprint.pdf

74 https://medium.com/algorand/algorand-state-proofs-707d64038e35

75 https://xconomy.com/boston/2018/02/15/algorand-nabs-4m-for-blockchain-that-aims-to-avoid-bitcoins-flaws/

76 https://valkyrieinvest.com/trusts/algorand-trust/

June 2021 by Arrington Capital Management.[77] In September 2021, SkyBridge Capital raised $100 million for an Algorand fund capped at $250 million.[78] That same month, the Algorand Foundation launched its $300 million Viridis DeFi fund, with 150 million ALGO going towards accelerating the early growth of DeFi on Algorand.[79] In November 2021, Borderless Capital launched its second $500 million Algorand-focused fund called ALGO Fund II.[80] The first fund, ALGO Fund I, was launched in 2019 by then-Algo Capital, with $200 million of funding that invested in over 100 companies.[81] In November 2021, Hivemind Capital Partners launched a $1.5 billion venture fund to invest in blockchain and digital assets and selected Algorand as a strategic partner to provide technical capability and network ecosystems infrastructure.[82] In March 2022, Grayscale launched a fund targeting non-Ethereum smart contract platforms called Grayscale Smart Contract Platform Ex-Ethereum Fund, of which 4.27% of the capital was allocated to ALGO.[83]

The Algorand Foundation supports blockchain education and development through its global partnerships with academic institutions such as prestigious universities MIT and UC Berkeley.[84] Algorand's partnership with the University of Florida established a "Blockchain Lab" to "support blockchain education with specific usage of Algorand technology, including undergraduate classes and online certificate courses focused on blockchain technology."[85] The foundation also offers a $250 million "ALGO Grants" program to fund activity in the areas of research, development, infrastructure, and use cases.[86]

Ecosystem

ALGO Grants supports the growth of Decentralized Finance (DeFi) on Algorand by funding project development. In February 2022, Applied Blockchain received a grant to develop a bridge between Algorand and Ethereum[87], which will leverage ASPs to enable trustless and efficient integration with other blockchains. The Algorand Foundation announced a $10 million grant for teams that are working on EVM-compatibility on Algorand.[88] Recently, the Foundation gave a grant to

77 https://www.coindesk.com/business/2021/06/10/arrington-capital-launches-100m-algorand-ecosystem-fund/

78 https://cointelegraph.com/news/skybridge-raises-100m-for-algorand-fund-and-files-for-crypto-company-etf

79 https://algorand.foundation/news/viridis

80 https://cointelegraph.com/news/borderless-capital-launches-half-billion-dollar-fund-for-algorand-projects

81 https://cointelegraph.com/news/algo-vc-fund-raises-200-million-to-fast-track-ethereum-rival

82 https://www.prnewswire.com/news-releases/former-citi-top-trading-executive-launches-hivemind-a-1-5b-venture-to-institutionalize-crypto-investing-301432682.html

83 https://cointelegraph.com/news/grayscale-launches-smart-contract-fund-for-ethereum-competitors

84 https://algorand.foundation/ecosystem/education/university-program

85 https://algorand.foundation/news/university-florida-blockchain-lab

86 https://algorand.foundation/grants-program

87 https://algorand.foundation/news/applied-blockchain-bridge-grant

88 https://algorand.foundation/news/10-million-evm-compatibility-grant

TinyCharts, a market analytics and charting platform, to support the establishment of a web and mobile solution for trading ASAs on DeFi.[89]

Algorand powers numerous major real-world use cases. The Italian Society of Authors and Publishers (SIAE) uses Algorand to manage copyrights as digital assets.[90] The Marshallese sovereign digital currency ($SOV), the national digital currency of the Marshall Islands, is built on Algorand.[91] Koibanx has signed a cooperation agreement with El Salvador to develop the government's blockchain infrastructure on Algorand.[92]

The ecosystem of Dapps is small compared to other smart contract platforms but is expected to grow in 2022. Notable projects include AlgoFi[93], a decentralized lending market; Xfinite[94], a decentralized entertainment ecosystem that rewards content consumption; Tinyman[95], a decentralized exchange (DEX) and automated market maker (AMM); and Algorand Name Service[96], a decentralized naming service designed for the Algorand community.

There are a plethora of NFT projects currently on Algorand's blockchain. Al Goanna[97], which began as a profile picture collection, later launched an environmental impact fund, "The Gilbert Goanna Tree Fund," which has contributed to the planting of "over 100,000 trees and counting." Alchemon[98] "is the first monster-collecting NFT staking, crafting, and trading card game on the Algorand blockchain." Algogems[99], leveraging Algorand's technology to create a seamless NFT marketplace, "offers zero-fee NFT creation and low fee marketplace trades" using its native asset $GEMS to reward creators and participate in governance. Flemish Giants[100] is growing their community by introducing the Flemmy Casino for poker tournaments and the Flemish Fantasy Football League for sports betting. Finally, Algo Leagues[101] is building a play-to-(L)earn (Learn and Earn) blockchain game model to incentivize players to learn and participate in the Algorand community.

89 https://algorand.foundation/news/tinychart-grant

90 https://www.algorand.com/resources/ecosystem-announcements/siae-launches-4-million-nfts-on-algorand-for-creators

91 https://www.algorand.com/resources/ecosystem-announcements/marshall-islands-to-power-worlds-first-national-digital

92 https://www.algorand.com/resources/ecosystem-announcements/el-salvador-signs-agreement-with-koibanx-to-develop-its-blockchain-infrastructure-on-algorand

93 https://www.algorand.com/ecosystem/use-cases/algofi

94 https://www.algorand.com/ecosystem/use-cases/xfinite

95 https://www.algorand.com/ecosystem/use-cases/tinyman

96 https://algorand.foundation/news/algorand-name-service-grant

97 https://algoanna.com/

98 https://alchemon.net/

99 https://algogemsnft.github.io/

100 https://flemishgiantsnft.com/home

101 https://www.algoleagues.com/

Algorand has collaborated with organizations to offset its carbon emissions to become a carbon-neutral network[102] and for other philanthropic causes. Algorand Inc. has partnered with ClimateTrade[103] to monitor Algorand's carbon footprint and lock the amount as on-chain carbon credits to be issued to environmentally sustainable initiatives. The Algorand Foundation has also committed to match donations of up to 1 million ALGO to support humanitarian efforts in Ukraine.[104]

102 https://www.algorand.com/resources/algorand-announcements/carbon_negative_announcement

103 https://climatetrade.com/

104 https://algorand.foundation/news/matching-ukrainian-algo-donations

DISCLOSURES

The research team may own the cryptocurrencies mentioned in this report, and as such, this should be seen as a disclosure of any potential conflict of interest. This report belongs to CrossTower and represents the opinions of its research team.

This report does not provide legal advice. This report is not an analysis of whether a digital asset is a security or a commodity. There may be restrictions in the United States as to whether entities who offer tokens should obtain licenses and registrations. People should do their own research as to whether the entity that they are utilizing for purchases or sales has appropriate licenses and registrations. In general, people should consult their tax, legal and other advisers as to the risks involved in investing in digital assets.

Nothing herein is tax advice. You should consult your own tax professionals in order to understand the risks of investing.

CrossTower is not a FINRA registered broker-dealer or investment adviser and does not provide investment banking services. This report is not investment advice, it is strictly informational. Do not trade or invest in any tokens, companies, or entities based solely upon this information. Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential for complete loss of principal.

Investors should conduct independent due diligence, with assistance from professional financial, legal, and tax experts, on topics discussed in this document and develop a standalone judgment of the relevant markets prior to making any investment decision.

CrossTower does not receive compensation from the companies, entities, or protocols they write about. Compensation is not received on any basis contingent upon communicating a positive opinion in this report. The authors were not hired by the covered entity to prepare this report. CrossTower did not receive compensation from the entities covered in this report for non-report services, such as presenting at author-sponsored investor conferences, distributing press releases, or other ancillary services. The entities covered in this report have not previously paid the author in cash, token, or any other in-kind consideration for the report or other services. The covered entities in this report are not required to engage with CrossTower.

The research team has obtained all information herein from sources they believe to be accurate and reliable. However, such information is presented "as is," without warranty of any kind whether expressed or implied. All market prices, data, and other information are not warranted as to completeness or accuracy, are based upon selected public market data, reflect prevailing conditions, and the research team’s views as of this date, all of which are accordingly subject to change without notice. CrossTower has no obligation to continue offering reports regarding this topic.

Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances. The graphs, charts, and other visual aids are provided for informational purposes only. None of these graphs, charts, or visual aids can and of themselves be used to make investment decisions. No representation is made that these will assist any person in making investment decisions and no graph, chart or other visual aid can capture all factors and variables required in making such decisions.

The information contained in this document may include or incorporate by reference, forward-looking statements, which would include any statements that are not statements

of historical fact. No representations or warranties are made as to the accuracy of such forward-looking statements. Any projections, forecasts, and estimates contained in this document are necessarily speculative in nature and are based upon certain assumptions. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties, and other factors, most of which are beyond control. It can be expected that some or all of such forward-looking assumptions will not materialize or will vary significantly from actual results.