Polkadot

Network for interoperable blockchains

MESSARI

Analyst: Blair Marshall (@blairlmarshall)

Updated: May 15, 2018

The Polkadot network aims to be a protocol allowing distinct blockchains or applications to communicate, transact and transfer data from one chain to another in a trustless manner.

Polkadot does not provide application functionality, but instead aims to serve as a relay-chain, hosting dynamic data structures called parallelized chains or parachains with a goal to provide other blockchains with interoperability, scalability and increased security.

Project Overview

Name	Polkadot
Issuer	Parity Technologies
Category	Utility token
Sector	Governance
Sale Start	10/15/2017
Sale End	10/27/2017

Token Overview

Name	Polkadot
Symbol	DOT
Type	Native
Initial Distribution	5,000,000
Current Supply	NA
Max Supply	N/A
Emission Type	Proof-of-Stake

Resource Links

- Website
- Twitter
- Reddit
- GitHub
- Medium
- Whitepaper

Project Background

Polkadot is working to create a protocol that enables interoperability and scalability between multiple blockchain networks. The Polkadot network was established as the initial solution from the Web 3.0 Technologies Foundation which was founded by Ethereum co-founder Dr. Gavin Wood. The foundation aims to solve issues such as scalability, governance, and interoperability. The Foundation is based in Switzerland and governed by the Foundation Council, a governing body consisting of Dr. Gavin Wood (President and Founder), Dr. Aeron Buchanan (Vice President), Peter Czaban, Mathias Bucher and Reto Trinkler.

The Polkadot protocol is intended to be a scalable core that will connect multiple public or private blockchains by allowing distinct networks to communicate and securely transact with each other. This includes common blockchain functionality like ensuring the validity and order of messages.

At the core of the network is a relay chain, which maps addresses to account information, coordinates communications, and provides consensus through a pooled security mechanism utilizing proof-of-stake (PoS). The relay chain lacks features like smart contracts and instead is designed to be a minimal protocol to connect other network participants and provide transaction finality.

Blockchains that are built to interact with the relay chain are called parachains (parallelized chains). These will be used to collect and process transactions while using the relay chain for finality. In an attempt to increase transaction throughput parachains will process transactions concurrently across multiple chains, instead of queuing transactions and processing them sequentially. Outside networks, like Ethereum and Bitcoin, will be similarly connected to Polkadot through a series of bridges that connect them to the main relay chain.

Polkadot is being built by Parity Technologies and plans to integrate other technologies like the Parity wallet. Parity Technologies is part of the Web 3.0 Foundation and was founded by Dr. Gavin Wood and Jutta Steiner.

Technology

The core technology of Polkadot is the relay chain, which reaches consensus through a modified and proprietary PoS mechanism consisting of four key participants: collators, validators, nominators, and fishermen.

Each parachain has a collator that fulfills the task of a miner in a proof-of-work blockchain. A collator must maintain the Polkadot relay chain state as well as the state of the parachain. The collator then manages the queue of transactions going into and out of the parachain from the relay chain. Collators collect parachain transactions, create new candidate blocks and then pass them along to validators in exchange for a fee for their work. In a competitive market with many collators, collators can incentivize validators to choose their block by sharing a portion of their fee with the validator.

Validators are randomly nominated to accept block candidates from parachain collators, verify the information in the block, and republish the block candidate to the Polkadot relay chain. Once a validator confirms a block, they also validate and change the state of the relay chain block by moving the transaction data from the originating parachain's input queue to the destination parachain's output queue. Validators are incentivized through a staking mechanism which requires them to stake Polkadot (DOT) tokens to the network to be chosen as an active validator. Validators that break the consensus algorithm are punished by losing a portion of their stake, while those that correctly secure the network and verify blocks are rewarded with new tokens.

Nominators are those who may be unable to participate in the transaction validation process directly, so they instead contribute tokens to a validator of their choice. Nominators receive a pro rata share of the validator reward based on their portion of the validator's bond, so nominators are incentivized to choose a validator most likely to receive the largest reward. The team believes the nominator process will create a competitive, but honest marketplace for high-quality validators and nominators.

Fishermen do not participate in the transaction validation process with validators and nominators, but instead, act as watchmen monitoring activity across the Polkadot network and identify validators who break consensus rules. Fishermen stake a smaller bond of tokens than a validator but receive a proportionally larger reward than validators for their role in securing the network.

The Polkadot network is building a native Polkadot token (DOT) to use in the relay chain. DOTs are meant to serve three distinct purposes, governance, operations and bonding. The team envisions that community members will vote on protocol upgrades or essential fixes based on their DOT holdings. Additionally, DOTs will be used for the proof of stake system. The staked tokens incentivize validators and fishermen to maintain and secure the network through the described punishment and reward system.

Distribution

At the start of the network, a total of 10 million DOT will be created as a native token. The total supply is not fixed at 10 million but instead will use a to be determined inflationary model to supply the rewards for their proof of stake system. The team envisions that a significant portion of DOT will be used for staking and predominantly remain illiquid. The initial 10 million DOTs will be released to all parties when the genesis block is mined, which it is estimated will take place in Q3 2019.

In Oct. 2017, the Web 3.0 Foundation raised the equivalent of $145 million in ether (ETH) through a token sale which sold 50% of total supply (five million DOT). The sale was split between a private sale, which raised over $80 million, and a public sale, which raised the remainder. Investors were required to use a KYC system called PICOPS, which verifies the identity of each participant. If you were unable to verify yourself, you were deemed ineligible. The sale was also not available to any Chinese or American citizens due to regulatory concerns.

The Foundation will retain 20% of supply (two million DOT) for future fundraising efforts, and the final 30% (three million DOT) will go to the Web3 Foundation for immediate use to develop the Polkadot network and other undisclosed Foundation activities.

On November, 6th 2017, a vulnerability was exploited in the Parity multi-sig wallet containing over 500,000 ETH, including $98 million of the $140 million+ in ETH raised through the Polkadot ICO. These funds are currently frozen, and a debate among the Ethereum community will determine whether these funds can or will ever be recovered. Even if the funds are lost, the Parity team does not believe this will impact their development roadmap.

Team

Dr. Gavin Wood
Co-founder and CTO of Parity Technologies

- President of Web3 Foundation and former CTO of Ethereum

Jutta Steiner
Co-founder and CEO of Parity Technologies

- Previously manager Security Audit and Integration for Ethereum

Investors

Blockchain Capital

Fenbushi Capital

Additional Resources

- YouTube: Gavin Wood on Polkadot
- Video: Parity Team Discusses Polkadot
- Polkadot FAQ
- Parity Wallet Postmortem