ABSTRACT

Existing Internet protocols have proven to be insecure and limited in throughput, and a better network topology is needed to ensure performance and privacy

A peer-to-peer networking protocol with end-to-end encryption and distributed routing can provide part of the solution, but the benefit is lost if peers do not maintain high quality network connections and hardware for lack of incentive.

Mantle proposes a solution to this incentive issue by employing a proof-of-work adaptation in which nodes mine blocks by contributing to network health and performance. Scores based on various service quality metrics make nodes eligible to receive block awards, aligning the interests of the network with the interest of the individual nodes.

INTRODUCTION

The many computers connected to the Internet are organized into a tiered structure, with requests from various computers funneled through large commercial machines arrayed in layers for routing, or the process of finding the correct address to send the requests off to and returning the response.

Due to the high cost of hardware maintenance and monopolies of scale inherent in this arrangement, massive Internet Service Providers (ISPs) have formed and the Internet has become centralized and inefficient, leading to bottlenecks when many nearby machines download data at the same time.

Additionally, vulnerability and exploitation at the ISP level remains a major weakness in global cybersecurity, as these choke-points also make Internet traffic easier to censor, redirect and disrupt.

These weaknesses can be addressed by moving to a peer-to-peer networking model, known as mesh networking, in which computers route traffic collectively, allowing users with direct Internet connections to share data without connecting to central routers.

By incorporating a native cryptocurrency paid out in return for participation in the network, the costs of maintaining infrastructure can be justified and the network can bootstrap itself.

THE MANTLE NETWORK

Mantle is a cryptocurrency that injects economic incentives into the cjdns mesh networking protocol by enabling users to mine currency in return for contributing network resources to their peers.

The cjdns protocol creates a peer-to-peer network with end-to-end encryption and distributed routing, maintaining privacy and security while allowing shared connections.

Mantle adopts cjdns and rewards users for maintaining network infrastructure based on the quality of service they provide. Providing Proof-of-Minimum Bandwidth (a score based on service quality metrics) makes nodes eligible to receive block awards, aligning the interests of the network (more nodes and higher quality of service) with the interest of the individual node operators (higher quality of service and rewards).

SECURITY LAYER

All cjdns traffic, and thus Mantle traffic, is encrypted end-to-end with perfect forward secrecy across the network. Data is secure during transit between sender and recipient and historical data is protected even if the sender or recipient's encryption is compromised.

THE DISTRIBUTED NETWORK EFFECT

All nodes monitor the network's health and collaborate to provide reports on node health to the network. Nodes monitor the connectivity of their peers so that when a peer disconnects, or degrades, it is dropped from their peer list. Peers are then assigned new nodes to monitor for better connections.

Six nodes are monitored at a time, with the three fastest peers kept as optimal routes and three random peers kept in order of network connectivity. In this way, the network self-heals when a node connects, degrades or disconnects and the network seeks to maintain both the fastest routes and the widest connectivity.

INFRASTRUCTURE

The Mantle network will support a wide array of consumer hardware, from low-power edge devices (such as smart TVs, smartphones, computers, and IoT) to specialized network infrastructures such as rack-mount switches and CDNs. These devices can connect to the Mantle network via Bluetooth, WiFi, Ethernet, and virtual network connections over the Internet, as well as any other network protocol.

Like any network infrastructure, the value comes from the accessibility it provides to a wide range of devices, so the Mantle network will aim to be as open and accessible as possible, allowing any device to connect that conforms to the network protocol.

However, users who want to have access to the Mantle network incentives and block rewards must be able to write to the blockchain and route traffic on the Mantle network, so only nodes with enough processing power and storage to maintain an entire copy of the blockchain are eligible for rewards.

MANTLE HARVEST™

To help build the initial backbone of the network, Mantle is creating a custom router and low power, proof-of-work miner called the Mantle Harvest™. It is designed to connect to reliable Internet connections and to share that connection with peers on the network.

MANTLE BLOCKCHAIN

MNTL

MNTL is the native coin that powers the Mantle mesh network. MNTL serves as the payment incentive for nodes to provide a high-quality connection, calculated in the form of a minimum Quality of Service (QoS) and Proof of Minimum Bandwidth (PoMB) score, thus motivating people to provide high speed, low latency connections to the Mantle network.

When all the MNTL are allocated, miner rewards will be derived from transaction fees. This incentivizes miners to continue accepting transactions and to maintain the Mantle mesh network even after the last coin is mined.

PROOF OF MINIMUM BANDWIDTH

In order to qualify for the block reward, nodes must provide Proof of Minimum Bandwidth to the network. Nodes intermittently submit a PoMB score, which is verified by peers on the network.

The PoMB score is based on a weighted average of various node performance metrics over time, therefore new nodes must build up a reputation to be eligible for rewards. The metrics taken into account by the PoMB score are as follows:

Jitter is the variation, or deviation, in the variability of packet latency on a network. The average jitter between nodes and their peers is measured and an average is compared against the maximum jitter of 20ms imposed by the PoMB mechanism.

Throughput is the quantity of data that can sent or received in a given period of time, with a minimum throughput of 1Mb per second. Throughput is measured constantly and a moving weighted average is calculated.

Packet loss is a measure of how much data sent across the network is lost or fails to be received. Packet loss is sampled in the same manner as latency, with 18 samples over 3 minutes averaged and compared to the maximum packet loss allowed of .1%.

Latency Latency is defined as the round trip time required for a message to reach a certain node and return. Mantle nodes sample latency to peers 18 times over a 3 minute period, and the average latency over this period is calculated and compared to a maximum allowed latency based on network size and peer count.

These metrics are combined into a single PoMB Rate and used to determine the trustworthiness of nodes to provide the minimum performance for healthy inclusion in the network. Nodes that have a consistently good PoMB Rate will be eligible to solve the next block, which if done will unlock the MNTL block reward.

TRANSACTIONS

There are two categories of transactions available on the Mantle blockchain; coin balance transactions and network state transactions.

Coin balance transactions are strictly related to the exchange of MNTL and are incentivized by network fees that get paid to miners.

A network state transaction is a coinbase entry which effectively contains the proof that a node has met the QoS requirements. These are feeless transactions which mining nodes submit to obtain rewards.

BLOCK REWARDS

Users are incentivized to contribute high-quality connections to the network, in the form of Proof of Minimum Bandwidth, in exchange for eligibility for rewards paid in MNTL. The block rewards are allocated to nodes who maintain the Mantle mesh

network, which is done in part by having nodes solve blocks using the X16r proof-of-work algorithm.

X16r is a low-energy, proof-of-work mining algorithm, which enables a fast block time to adapt quickly to network state changes. As X16r is ASIC-resistant, it is more energy efficient than the proof-of-work algorithms implemented in Bitcoin, Ethereum, and other popular cryptocurrencies.

To receive a block reward, a node must:

1. Win the proof-of-work challenge,
2. The block it has solved must be verified by a majority of nodes, and
3. The winning node must meet or exceed the Quality of Service requirements of the network.

Every 60 seconds, the nodes in the mesh network calculate the QoS metrics and prune peers that fail to meet the QoS minimum.

Additional block rewards are generated from wallet to wallet transaction fees. These transactions go into a backlog after validation. During congestion, transactions are prioritized by fees such that only the most lucrative ones are committed to the next block. This incentivizes users to pay higher fees during high network usage to execute their transactions faster.

BLOCK TIME

Fast reputation scoring is necessary to maintain a high quality of service. As people connect and disconnect from the network, the Mantle blockchain must be capable of monitoring and incentivizing good behavior and adapting quickly to changes.

This is possible with a high speed, low-latency network, where block propagation happens quickly. Mantle has a 60-second block propagation to accommodate these needs.

DEFENSE AGAINST ATTACKS

Like many networks and blockchain technologies, Mantle is susceptible to malicious use by bad actors. In anticipation of these scenarios, the Mantle network is designed with attention to the following types of security risks:

BANDWIDTH SPOOFING

Bandwidth spoofing is limited by having a peer-to-peer monitoring system where bad actors are identified and punished by becoming temporarily ineligible from mining. The monitoring is vulnerable to Majority attacks, which is addressed in the next section.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

The risk of distributed denial of service attacks is reduced by limiting the number of hops that can be taken between two peers and preventing circular routing.

METADATA AND MAN IN THE MIDDLE ATTACKS

Man in the Middle (MiTM) attacks are limited due to the fact that the IPv6 address is used as their public key.

MAJORITY & SYBIL ATTACKS

Majority and Sybil attacks are mitigated by the required proof-of-work (in the form of routing traffic and auditing connection quality) provided by nodes. The proof-of-work necessary to receive a block reward will increase over time. As a result, the cost of these attacks will increase over time because physical resources are required to participate

CONCLUSION

The Mantle adopts the cjdns mesh networking protocol and incentivizes individuals to run routing nodes and to increase the connection quality of those nodes over time.

A secure, global mesh network running on cjdns addresses limitations of current Internet infrastructure by allowing traffic to flow horizontally, peer-to-peer, avoiding speed and latency limitations and providing an alternative to monopolistic control by ISPs.

The result is a secure, efficient, global mesh network with game-theoretically sound incentives for users to bring value to both themselves and the network by connecting existing machines to Internet access points and investing in quality hardware. By incentivizing the sharing of network resources and the participation of many nodes, Mantle proposes to bootstrap a private and secure new Internet for all.