MANTLE

Yellow Paper

AUTHORS

Jesse Berger	indoness@aol.com
Josh Berger	josh.a.berger@gmail.com
Adonis Gaitatzis	backupbrain@gmail.com
Jon Owens	jro92024@gmail.com
Vishnu Seesahai	vish@healthmatica.com
Eric Shuss	eric@perytonsystems.com

Abstract

Mantle is a mesh network where users are incentivized to run routing nodes and earn cryptocurrency on an open blockchain. The resulting mesh network is encrypted end-to-end and point-to-point, embedding security into the mesh protocol.

By contributing high-quality bandwidth to the network, Mantle users effectively become miners of Mantle’s native cryptocurrency, MNTL. Users’ eligibility to receive block rewards are determined by their ability to meet the minimum bandwidth contribution standards to keep the network healthy and active.

Users with high-quality connections can monetize their connection by sharing bandwidth with others who have less access, helping to solve the “last mile” problem facing current Internet infrastructure.

1. Problem / Current Tech

The people who created the Internet likely would not have imagined that more than twice as many devices would be connected to the Internet than there are people on earth, and that people’s identity could be stolen without anyone ever noticing. Since that time, several problems have emerged with current Internet Technology:

Limited bandwidth

Since its adoption in 1983, the Internet has expanded across the world and enabled entirely new forms of business to operate, for example Uber, Netflix, and AirBnB. Many of these companies, especially streaming services such NetFlix, YouTube, and Pandora require near real-time data transmission. Users tend to consume these services at the same time, leading to high demand during peak times that can overextend the data pipeline.

More Connected Devices

The rise of Internet of Things and automation have caused an explosion in both the number of connected devices and in the amount of traffic on the Internet. Some of these systems are mission-critical and require near time data such as those that exist in self-driving cars and medical applications. As the competition for bandwidth grows, the quality of these applications may be reliant on local network conditions.

Traffic Monitoring and Shaping

The Internet was created without an opinion about, traffic monitoring or traffic shaping. Today, the Internet is used heavily in these ways. Internet Service Providers and other companies that router Internet traffic are able to see what their users are watching, reading, and doing online. Oppressive governments block access to content that is deemed offensive, challenging, or against the party line.

Net neutrality

Internet Service Providers are often local monopolies that set the terms of use and rates for their users, despite the Internet being a public good. Recent changes in Net Neutrality Laws in the United States will enable censorship and bandwidth throttling at the ISP level, allowing Internet Service Providers to partner with content producers and force users to pay extra for content that isn't part of that partnership, leading to potentially wealth-based access to knowledge; the very thing the Internet was intended to eliminate.

Security

The creation of the Internet has ushered in a world of hacking. Despite constant upgrades to protocols, hacking is rampant because the owness of data security lies with companies who make money from user data. Aside from the public relations costs, leaking user data mostly an externalized cost. Security on the Internet is end-to-end at its best, so if a user connects to a rogue ISP that intercepts their data along the way, nobody's the wiser.

2. Solution

The solution to this is a high speed, encrypted mesh network that connects vastly more devices and more evenly distributes the points of connectivity and incentivizes users to provide connectivity to others.

Mantle is a solution that does exactly this, and enables new businesses and technologies in the process.

Mesh Networking

Mantle uses cjdns for connectivity and routing. Cjdns nodes is self-healing, meaning that users will continue to be connected even when a gateway drops out. It is self-optimizing, meaning that the network will always route data as quickly as possible.

Mantle is connection technology agnostic, so that users can connect via Ethernet, WiFi, Bluetooth, satellite, or whatever technology suits them. Users can connect from anywhere in the world.

Encryption

Cjdns uses IPv6, allowing for more connected devices than there are stars in the galaxy. It encrypts traffic end-to-end, so that onlookers can't see what content a user is accessing. It encrypts traffic point-to-point, so that onlookers can't see where a user's content is coming from or going to. It hashes the addresses of each connected device on the network, so that onlookers can't see what a user's address is.

This prevents traffic monitoring and shaping, and many types of hacking including man in the middle and metadata attacks.

Blockchain Incentivized

Users are paid for their contribution to the network. Mantle uses Blockchain technology to incentivize users to contribute their spare bandwidth to the network so that a people everywhere will independently build a healthy global mesh network.

Forward-Looking Backwards Compatibility

Mantle is compatible with the existing Internet, meaning people lose nothing by being early adopters. Yet as both a mesh and a blockchain, Mantle supports and enables future technologies and business models to exist, such as distributed applications that can only exist on a mesh and autonomous organizations that can only exist on the Blockchain.

3. What is Mantle?

Mantle is a new incentivized mesh Internet that bypasses the powerful oligopoly of ISPs, online surveillance and obstruction to net neutrality. Mesh networking is not a new idea, however, it previously lacked the economic angle to inspire adoption and sustained use. Blockchain technology offers a solution to this problem and provides users with the incentive to build and support a decentralized Internet.

Mantle combined with cjdna replaces the current ISP ecosystem and is building a faster, more private, and lower cost incentivized mesh network. In addition, using a software-defined network architecture, Mantle enables source routing for optimal latencies. This new decentralized Internet is a viable alternative to ISPs and empowers its users to maintain the network.

Mantle’s objectives are:

- An open access global meshnet
- A “last mile” edge computing alternative to existing ISPs
- Allow communities to connect to the Internet with user-operated infrastructure
- Low latency (as fast as current Internet and faster on a native network)
- High performance (designed for high throughput applications and data)
- Privacy (traffic passing cannot be traced back to your IP address)
- 3rd parties forwarding traffic cannot read or link packet contents to a user

- Supports operation over antenna (meshnet)
- Users are eligible to earn Mantle coin rewards by providing network resources
- Network services can be paid for via micropayments in MNTL and other altcoins

A “mesh network” is another way of saying that Internet traffic is routed through the users of the network. The core value of a mesh network is that there is no central point of failure — should a node lose connection, other nodes can re-route the traffic. Decentralized systems are designed so that no individual has control over the entire network and each node is its own ISP, providing connectivity for other nodes.

Mantle is based on the well-known open source, software-based networking project called cjdns. Cjdns powers an encrypted IPv6 network using public-private key cryptography to autonomously generate IP addresses independent of an ISP. Traditional IP addresses are replaced with a public key, so no one can read traffic to a destination, without knowing the private key pair that identifies the destination. This system operates without the need for certificate authorities. The default link layer and end-to-end cryptography ensures everything is encrypted, unlike the current Internet architecture.

Mantle’s network protocol also implements enhanced privacy. As a packet is routed, each node only knows the previous hop and the next hop in the route. This is in contrast to IPv4, in which each packet contains the destination and the source, reducing privacy and security.

In the Mantle network, each node provides bandwidth, can forward information, and the data transmission is optimized for the fastest path in order to minimize data congestion. By adding bandwidth and storage space from a growing number of user nodes, as the network grows performance continuously improves.

Mantle also uses an innovative reward mechanism to incentivize users. Each node submits a Proof of Minimum Bandwidth, or PoMB score to the Blockchain, and each node finds random other nodes on the network to validate. Nodes with a verified PoMB are allowed to submit transactions to the Block and are therefore eligible for the Block reward. Nodes that fail to meet the PoMB minimum aren't allowed to submit that Block and are ineligible for the Block reward. The ping delay data and quality reports are then printed onto an ever-growing distributed hash table (DHT). Nodes that provide PoMB are segregated and become eligible for a random block reward (golden ticket). The probability of reward is divided equally amongst all eligible nodes. This DHT also provides valuable, real time routing data and improves the network service quality by providing fastest path routing.

As mentioned, mesh networks require an economic incentive to keep the system going, and that's the reason behind Mantle's native currency MNTL. Instead of traditional Proof of Work (PoW) mining, using longest hash algorithms, Mantle's "harvesting" technique incentivizes users with rewards, while also doing useful work. A blockchain payment protocol is embedded into each node to record payments and each node's public-private key pair serves as the payment address. Nodes can use MNTL to pay for services on the Mantle platform, as well as micro payments within Mantle's larger marketplace ecosystem.

To power the network, Mantle has designed a powerful hardware device called the Mantle Harvest. This hardware enables users to provide bandwidth utility to the network and earn rewards for assessing the quality of other nodes and printing this data to the DHT. Mantle Harvest is designed to encrypt, decrypt, transfer content, transfer traffic and earn rewards. This hardware is "plug and play" and designed to help unskilled users to easily deploy their own node and earn randomized rewards. Nodes can also connect to a neighbor via an antenna and use, or provide, bandwidth resources in a point-to-point manner.

With Mantle Harvest hardware and incentivized distributed mesh network, all participants have the opportunity to work together to promote and reshape the Internet for the betterment of the world.

4. How Mantle Works

4.1 Network Architecture

Network Topology

The traditional Internet relies on powerful central servers that deliver content to connected devices, for example smart TVs, laptops, and smartphones. This model is a hub and spoke architecture. It has inherent speed and latency limitations, for instance when whole neighborhoods start watching Netflix at the same time.

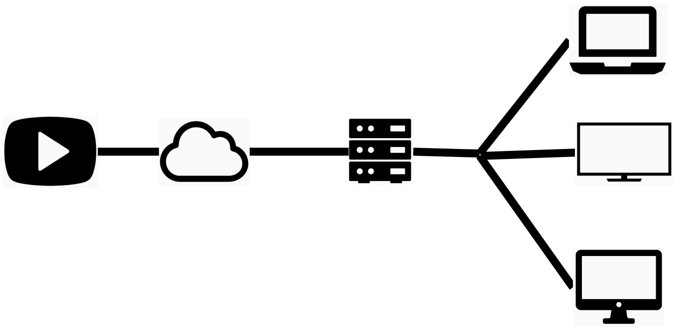

Figure 4.1.1: Traditional Internet network

All Nodes on the edge are sharing the same limited-bandwidth connection to the ISP and from there connect to a CDN such as Netflix, YouTube, or Amazon.

The Mantle network is a mesh that interfaces with the traditional Internet. Each Mantle Node acts as a point-to-point router so that data can be delivered within the mesh in a distributed way. Nodes may be connected to the traditional Internet, a network LAN, or to other Mantle Nodes.

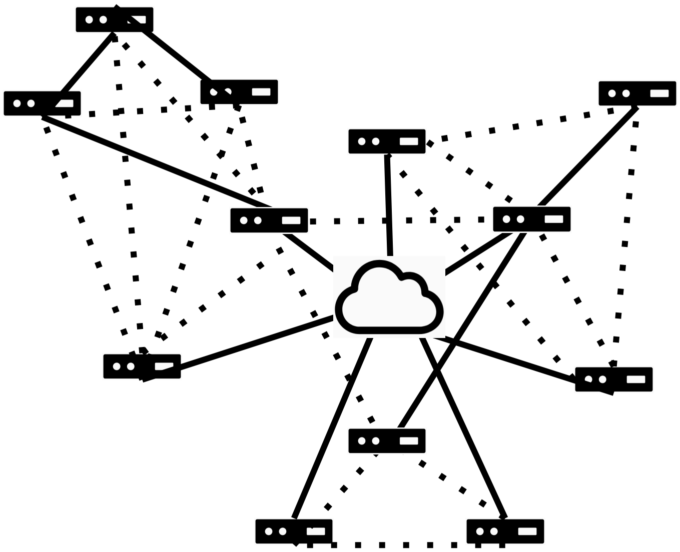

Figure 4.1.2: Mantle Mesh Network

A Node on the Mantle network can be any type of network computing device that supports the Mantle networking stack. This includes powerful devices such as rack mount servers and routers, to mid-range devices such as home computers and smartphones, to low-end devices such as network appliances and Internet of Things applications.

Addressing

When a Node connects to the network, it is assigned a hashed IPv6 address by one of its Peers on the Network. Each Node maintains a list of nearby hashes in a Distributed Hash Table (DHT). If a Node does not have any addresses in its DHT, it will request one from a Peer.

Network Optimization & Healing

Each Node periodically runs a speed test on addresses in it’s DHT to discover which ones have the fastest response. Nodes will keep the three fastest addresses in its DHT to maximize routing speed and three random addresses to maximize network connectivity.

Periodically Nodes will exchange random DHT tables so that new addresses can be tested and the fastest three connections kept. In this way, the network continually optimizes for speed.

When a Node disconnects, this process results in nearby Nodes no longer routing to the disconnected Node. When a new Node appears, this process will help it find and become part of the fastest routes.

This provides an opportunity for users with a high quality Internet connection who live in areas that have poor network infrastructure to provide high quality Internet to their local area using alternative infrastructure or to invest in infrastructure development. Doing so allows them to monetize their Internet connection by leasing spare bandwidth to their local area.

Traffic Shaping & Bandwidth Contribution

The Mantle network works because each Node acts a router for nearby Nodes. This traffic routing is possible in part because each Node allocates some amount of spare bandwidth toward routing traffic between Peers.

Blockchain Integration

Each Node tracks the amount of bandwidth it contributes and reports that contribution on the Mantle's blockchain. This contribution is validated by Peers on the network in a process called *Proof of Minimum Bandwidth* (PoMB). To incentivize users to contribute bandwidth to the network, there is an in-network currency called Mantle Coin (MNTL).

Hardware

The Mantle Network is designed to work on a variety of devices, from low-power appliances to high powered servers. However, only Nodes with enough processing power and storage to maintain an entire copy of the blockchain are eligible for the MNTL Block Reward.

Compatibility with the Internet

The Internet is a foundational technology that the Mantle network is built upon. One or more Nodes may physically connect to the Internet and connect virtually to each other to establish the Mantle Mesh network. Nodes may also connect physically to one another without a direct connection to the Internet.

In this way, Nodes without direct Internet access may still access content from the Internet.

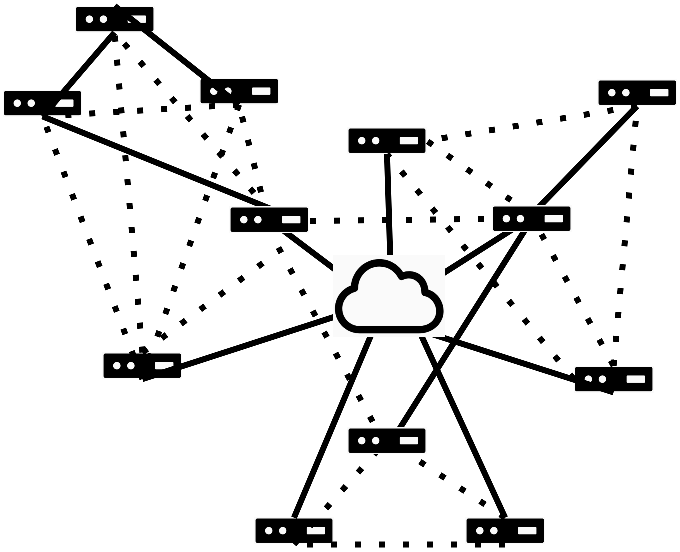

Figure 4.1.3: Mixed Nodes connected to Internet and to other Nodes

All Nodes on the network route traffic via other Nodes, allowing users within subnets to share data without connecting to central servers. This network architecture reduces stress on traditional ISPs and CDNs and enables consumers to monetize their spare bandwidth.

Defense Against Attacks

Like many networks and blockchain technologies, Mantle is susceptible to malicious use by bad actors. In anticipation of these scenarios, Mantle implements anti-hacking technologies to combat the best known attacks, including:

- Bandwidth Spoofing,

- Majority,
- Sybil,
- Distributed Denial of Service,
- Man in the Middle, and
- Metadata attacks.

Bandwidth Spoofing

To combat this, Nodes validate each other's PoMB score. Nodes receive demerit points when their reported PoMB isn't verified by its Peers, and after too many demerit points they are kicked off the network. This is similar to the event based reputation system or ERBS proposed by Xia Feng *et al* for defending VANET ad-hoc traffic networks against Sybil attacks.

Nodes can connect to existing Peers if they are known. If they are not known, nodes can connect to a supernode with a fixed address to ask for nearby peers. As a result, each Node belongs to a sort of randomly created neighborhood and it is difficult to use traffic shaping to spoof minimum bandwidth contribution because randomly assigned Peers must agree with the routing and bandwidth contribution of the others.

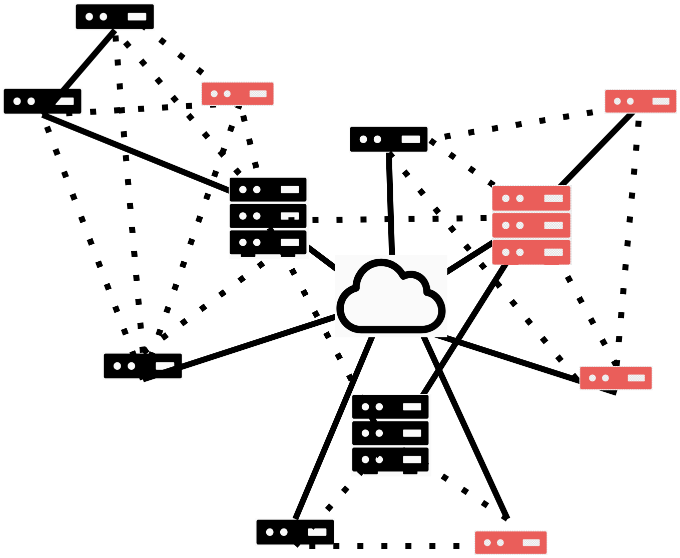

Figure 4.1.6: Attempted Network Spoofing

One possible problem is that people run nodes in a data center, expecting to provide minimum bandwidth within a closed loop, but without any of that bandwidth benefitting outside users.

To combat this, Mantle will will have a maximum throughput cap that affects the reputation score. Nodes with extremely low ping times, only found in data centers will not have preferential treatment on the blockchain. Only nodes that provide real routes with

Majority[1]

The Mantle network is designed to limit the effectiveness and scope of a Majority attack by initially allowing only Mantle-approved hardware to connect to the blockchain during the initial stage of Mantle network development. This will establish a reliable PoMB history and a large number of Nodes to validate against PoMB spoofing, limiting the ability for bad actors to acquire the resources necessary to take over the network in this way.

[1] https://en.bitcoin.it/wiki/Majority_attack

The Mantle hardware and deployment strategy will be discussed in greater detail in the **Distribution Strategy** section.

Sybil[2]

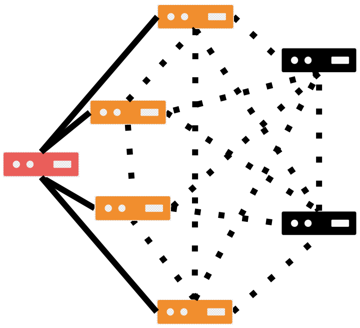

Figure 4.1.7: Sybil Attack Example

The Mantle network is resistant to this attack because physical resources are required to win the PoMB reward, and access to the reward is based on the Node's reputation. Each Node on the network must contribute the minimum bandwidth, so there is a cost to creating a false identity and a physical limit to the number of false identities possible. The ERBS protocol referenced earlier also works this way.

Distributed Denial of Service[3]

Cjdns limits the effectiveness of DDoS attacks by enforcing routing timeouts on packets, preventing them from entering infinite loops or for lasting more than a few hops.

Man in the Middle[4]

Mantle is a mesh network that uses cjdns for network addressing and point-to-point encryption, making it resistant to this attack for for three reasons:

[2] https://en.wikipedia.org/wiki/Sybil_attack

[3] https://en.wikipedia.org/wiki/Denial-of-service_attack

[4] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

1) Traffic is randomly routed through the mesh,
2) Node addresses are assigned randomly by their Peers during connection, and
3) Data is automatically encrypted point-to-point and end-to-end.

Bad actors who attempt a MITM attack are unlikely to acquire all the packets necessary to compile a single web page or other data across the network, because the packet routing within a mesh network is random.

The DHT allows each Node on the network to maintain an incomplete anonymized list of connected Peers and their addresses. When a Node connects, its identifying data is hashed and given an address on the network by one of its Peers. A Node may get an address from a different Peer each time it connects, preventing an attacker from targeting a specific target.

Additionally, packets on the network are encrypted point-to-point and end-to-end. Random packet routing prevents an attacker from gaining access to enough packets to decrypt the target's data. End-to-end encryption prevents an attacker from forging an encryption certificate or falsifying the authenticity of that certificate. This level of encryption is called perfect forward secrecy.

Because the Mantle network uses cjdns, MiTM attacks are limited due to the fact that the IPv6 address of a node in the network is the first 128 bits of the double-sha-512 of their public key, therefore MiTM attacks are only considered feasible if neither of the parties has a trusted IP address for the other party.

Metadata collection is largely limited to participants within the network because all traffic is encrypted not only end-to-end but also hop-to-hop.

Metadata accessible to participants within the network includes:

- *Public IP addresses and ports used by participant's directly connected peers*
- *Topology-dependent packet forwarding label*
- *Sender public key (during encrypted session setup messages)*
- *32 bit session identifier, used by the destination to identify the source*
- *32 bit session nonce (auto-incrementing counter)*
- *Packet timing and size*

Metadata accessible to non-participant "bumps on the wire" includes:

- *Public IP address of sender and recipient for a single hop*
- *Public keys for sender and recipient for a single hop (during encrypted session setup messages)*
- *32 bit session nonce (for the "outer" encryption session, between directly connected peers)*
- *Packet size and timing*

Metadata Attacks[5]

Mantle prevents Metadata attacks by using both point-to-point and end-to-end encryption. All user data is secured between each leg in its trip across the network, resulting in perfect forward secrecy. This prevents any user from knowing where traffic came from, where it is going, or the content of that traffic.

[5] https://en.wikipedia.org/wiki/Traffic_analysis

Data Privacy

Thanks to the use of cjdns, all traffic is encrypted end-to-end across the network with perfect forward secrecy. Data is secure during transit between sender and recipient and past data is protected even if the sender or recipient's encryption is compromised.

Types of Hardware

Although initially Mantle Harvest devices will power the backbone of the Mantle network, the network will support a wide array of consumer hardware, from low-power edge devices, such as smart TVs, smartphones, computers, and IoT devices, to specialized network infrastructure such as rack-mount switches and CDNs.

These devices can connect to the Mantle network via Bluetooth, WiFi, Ethernet, virtual network connections over the Internet, or any other other network protocol.

Routing hardware must be able to do this plus allow other devices to connect to it via similar technologies.

Users who want to have access to the PoMB award must be able to write to the blockchain, route traffic on the Mantle network, and provide minimum bandwidth on the network for this routing.

Hardware requirements are discussed in the **Appliance** section.

Addressing

All of IPv4's total of 4.29 million IP addresses were assigned in 2011, and it is estimated that by 2020 there will be 20.4 billion connected devices. This is why Mantle uses IPv6, a new IP address format that allows for approximately 340 trillion trillion trillion potential addresses.

Without a central authority to issue DNS addresses, it is impossible for an organization to allocate or restrict addresses based on geography, political affiliation, or some other quality.

Cjdns

As Mantle uses cjdns for network addressing, it automatically uses the fc00::/8 subnet. This plus the cjdns DHT makes Nodes in the Mantle network compatible with the Hyperboria network, a global decentralized mesh network that has 980 nodes and 2000 link connections at the time of this writing.

Nodes save their peer list so that when they reconnect, they can attempt to re-integrate into the network. If this peer list is stale or if no peers are known, nodes can ask a supernode with a known address for a list of peers.

Cjdns uses a blend of hub and spoke and distributed routing. This approach mitigates the weaknesses of each system. For instance the hub and spoke routing allows for large-scale networks to be implemented efficiently while the distributed routing allows for ad-hoc peer to peer networks to be set up.

BLOCKCHAIN

The Mantle network is powered by blockchain technology. The native Mantle Coin (MNTL) incentivizes users to contribute spare bandwidth to the network by making those who contribute eligible for random rewards.

MNTL

MNTL is the native coin which drives the Mantle mesh network. As such, MNTL functions as a payment incentive for nodes to provide a minimum service level agreement (SLA) score, such that nodes are motivated to provide high bandwidth and low latency across the Mantle network. One of the key challenges to scaling a mesh is to inspire independent Nodes to work together, sharing their resources to provide the highest Quality of Service (QoS). Relaying messages for strangers, and providing the ample resources to do so, is not without costs. Therefore, an incentives model, via a cryptocurrency, can act as a significant impetus for scaling a mesh network.

MNTL is a fully decentralized cryptocurrency that is resistant to regulatory censorship or jurisdiction. MNTL runs on it’s own blockchain which uses Ravencoin as rails. Ravencoin is a Bitcoin based protocol which enables the representation of abstract assets on the blockchain. MNTL tokenizes network bandwidth and rewards users who contribute resources to the network. In this way, MNTL incentivizes the growth and maintenance of the Mantle network.

Mantle’s blockchain is a decentralized ledger where Nodes qualify to receive rewards if their addresses are present in the DHT and provide a minimum QoS to the network as measured by average throughput, latency, and other metrics. These Nodes are called Miners. The ledger contains the IPv6 address of the Node producing the current block to be validated against the DHT and PoMB. The ledger also contains MNTL wallet balances and balance transfer data. MNTL not only acts as an incentive to build the network, it also acts as the immutable record of the underlying state of the mesh network. Therefore the blockchain ensures the network will always be fast and consistent.

The blockchain uses a Proof of Work (PoW) algorithm to issue MNTL fairly and transparently. MNTL leverages the following features from Ravencoin:

1. The ability to store any asset, not only financial transactions. This allows for the storage of metrics related to the current state of the Mantle mesh network.

2. Block transaction times averaging 60-seconds, allowing the consistent incentivisation of the network through rapid block reward propagation.
3. ASIC and GPU-resistant X16r PoW algorithm. X16r uses a randomly rotating PoW algorithm, which increases the cost of developing specialized mining chips. This contributes to a greater level of decentralization and fair access to the block reward through PoMB.

As the network state is updated in the decentralized blockchain ledger, MNTL coins are created and randomly assigned to qualifying Nodes. These updates are done in blocks, each of which must store a consistent record of all coins produced and owned. Nodes must provide a Proof of Minimum Bandwidth (PoMB) of their bandwidth contribution in order to qualify to produce blocks and possibly receive a reward. The PoMB acts as a score of the Node's QoS and therefore the blockchain measures the mesh network's QoS as a whole. The PoMB is used to filter poorly performing Nodes from the DHT by excluding low QoS Nodes from the block reward.

The inclusion of MNTL creates real-world market incentives that will drive users to scale the Mantle network exponentially, while maintaining a fast, reliable network. Today's mesh networks do not include these incentives.

A Low-Latency Blockchain

Since reputation scoring is necessary to provide a high QoS, the 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 because block propagation happens quickly, resulting in more transactions per second, or TPS. The time it takes to compute PoMB and the current state of the DHT must be less than the average block of 60 seconds time to avoid forking.

Block Propagation

With longer block times and higher latency, block forking becomes a greater risk. Bitcoin mitigates this by maintaining a 1Mb block size and a 10 minute block time. Even with these settings, it is a best practice to wait for 6 or more blocks to clear before considering a Bitcoin transaction valid. If a fork occurs, there is less certainty about which transactions are valid.

As the risk of forks increase, so does the risk of double spend attacks. Double spend attacks occur when a user spends more coins than they have by initiating both spends at different points in the network at the same time, similar to writing cheques at different stores on the same day without the funds to back them up. The blockchain recovers from this attack by forking. One of the blocks eventually gets discarded as the rest of the blockchain network comes to a consensus about which forked block is more accurate.

Discarded blocks can contain legitimate transactions, so this scenario results in the discarding of legitimate transactions such as payment for goods and services. This risk can be mitigated by reducing block propagation times, which is achievable on a low-latency network.

The probability of a fork occurring can be thought of as:

$$probability\ of\ a\ fork\ =\ P\left(fork\ |\ T_b\right) = 1 - e^{\frac{-T_{90}}{600}}$$

Where T_b = Time to produce next block, and T_{90} = Time to achieve 90% block propagation to all Nodes in the network. In bitcoin, T_b = 600 seconds, or ten minutes, and T_{90} = 11.6 seconds. This data can be found in the bloXroute whitepaper. thus the probability of a fork occurring is about 1.915%, which is a non-negligible amount.

By reducing block time to 60 seconds, or 10% that of the blockchain, the probability of forking increases to 17.58%. Decreasing block time alone produces undesirable results. The probability of a fork and the the block propagation time can both be reduced if the time to achieve 90% block propagation time (T_{90}) is also reduced. For example, if $T_{90} = 3$, then P (*fork* | T_b) = 0.0049875 or about .5%

Reducing of block times is possible so long as the time it takes to achieve 90% block propagation is less the the time it takes to produce the next block:

$$T_B > T_{90}$$

Adhering to this relationship allows Mantle to shorten block times while also lowering the probability of forks, including those related to double spends.

To achieve an average of 60 second block times with a 1Mb block size and maintain Bitcoin's current fork probability, blocks must propagate to 90% of the network within 1.7 seconds ($T_{90} = 1.7s$). The Mantle blockchain incentivizes the very low-latency network required to execute this rapid block propagation.

PoMB

Mantle Nodes are given a PoMB score in accordance to the network speed, latency, and reliability they contribute to the mesh network. As these characteristics are critical to the health and quality of the network, a minimum PoMB score is needed to qualify Nodes to receive block rewards. This in turn incentivizes the network.

As the scale and demands of the network increase, so does the minimum required PoMB needed to receive rewards. This incentivizes a network that increases in speed and reliability with use.

A PoMB score is exponential weighted moving average of several individual metrics which include latency, packet loss, jitter, and throughput. Together, these metrics are called the PoMB Rate. The PoMB Rate is measured with pings that calculate the Round Trip Time, or RTT of a message between two Nodes. Multiple consecutive pings are used to measure a single PoMB Rate at a given time, and several PoMB rates are used to calculate the PoMB Score.

Nodes calculate and assign a PoMB Score for their peers by averaging several PoMB Rates over a period of time. A Node will not have a PoMB Score upon connection to the network. They must build a reputation over a period of time by consistently providing high-quality bandwidth to the network. Once a Node is assigned a PoMB Score that meets or exceeds the network minimum, it is eligible for block rewards.

Latency

Latency is the time required to send a packet across the network and back from sender to receiver. As modern networking hardware uses optical or electrical signals to transmit data, this time is affected by the speed of light in the medium of transmission and the number of hops it takes between routing Nodes.

The speed of signal propagation through a medium is calculated as:

$$t = \frac{s}{c_m}$$

where s is the distance between sender and receiver and c_m is the speed of light in the medium

For MNTL's 1.7 second block propagation time, bitcoin’s mean IPV6 latency of 104 ms is, at best adequate. A lower latency is preferable, ideally:

$$Max\,Allowable\,Latency\ =\ 40\,ms$$

MNTL’s latency is acquired from CJDNS. CJDNS samples latency in 10 second windows and averages them into a single sample. Approximately 5 pings occur in a 10 second window. CJDNS returns an array of 18 samples which span a 3 minute period.

To calculate the latency score (L_t) of a Node in a period, we utilize the peer-to-peer latencies observed in the bitcoin network as a baseline.

Percentiles	**IPV4 (Peer To Peer) [ms]**	**IPV6 (Single Beacon) [ms]**
10%	48	40
33%	79	80
50%	109	95
67%	152	95
90%	286	165
Average	135	103
Standard Deviation	88	62

Thus, for an optimized IPV6 network we chose a latency range that exceeds the latency of 90% of the bitcoin network, placing Mantle in the upper 10th percentile with a latency threshold ($R_{latency}$) of 40 ms or better.

$$R_{latency}\ =\ 40\,ms$$

We then treat our latency data (L_t) as a series of successive bernoulli trials that map latency onto the binomial distribution space.

We define a binomial transformation (Tr) function such that for any time series of data, with random variable X_t changing over time (t) and threshold boundary (R) we have:

$$Tr(X_t\,,\ R)\ =\ \left\{1:\ if\, X_t\ \leq R,\ or\, 0:\ if\, X_t\ > R\right\}$$

Thus, we map (L_t) onto the binomial space using $R_{latency}$ by calculating the latency vector L as:

$$L\ =\ Tr(L_t\,,\ R_{latency}),\quad \forall_t\, time\ intervals\ in\ the\ sample$$

We then calculate the expected value of (L) called L_μ as:

$$L_\mu\ =\ E[L] = \frac{1}{n}\sum_{t=1}^{n} L_t\quad where\ n\ is\ the\ \ number\ of\, samples$$

The latency value L_μ is the average latency for the period after binomial transformation.

Packet Loss

Packet loss (drops) is the number of packets lost per number of packets sent. MNTL’s packet loss is acquired from CJDNS. CJDNS samples packet loss in 10 second windows and averages them into a single sample. CJDNS returns an array of 18 samples which span a 3 minute period, accounting for approximately 5 pings occur in a 10 second window.

For MNTL’s low latency requirements the tolerance for packet loss is minimal. We define the drop throughput as R_{drops}

$$R_{drops}\ =\ .1\ \%\ =\ .001$$

We then treat our drops data (D_t) as a series of successive bernoulli trials that map latency onto the binomial distribution space, using the previous described binomial transformation (Tr) function, $Tr(X_t, R)$.

Thus, we map (D_t) onto the binomial space using R_{drops} by calculating the drops vector D as:

$$D = Tr(D_t, R_{drops}), \quad \forall_t \, time\ intervals\ in\ the\ sample$$

We then calculate the expected value of (D) called D_μ as:

$$D_\mu = E[D] = \frac{1}{n}\sum_{t=1}^{n} D_t \ \ where\ n\ is\ the\ \ number\ of\ samples$$

The latency value D_μ is the average packet loss (drops) for the period after binomial transformation.

Bandwidth

Bandwidth is the quantity of data that can sent or received per unit of time, measured in number of messages that can be delivered per unit of time, using existing tools such as iperf. MNTL's bandwidth is sampled from CJDNS, as well as the blockchain itself.

For the bitcoin network, in 2017 with approximately 9000 Nodes, and with most Nodes connected to 8 - 12 peers, the bandwidth percentiles are as follows:

Percentiles	**Bandwidth**
10%	3.96 Mbps
50%	56 Mbps

99%	438 Kbps

MNTL bounds it’s bandwidth at the upper 50th percentile for bitcoin. Thus, the minimum bandwidth threshold, BW_{50}, is 56 Mbps or 7 MBps.

Consider that the time to make a single hop to a peer, T_{hop}, in the bitcoin network is calculated as follows:

$$T_{hop} = \frac{B}{BW} \quad where\, B = block\, size\, (1\, MB),\ and\, BW = bandwidth = BW_{50}$$

Hence we have:

$$T_{hop} = \frac{1MB}{7MBps} = .143\, s$$

Thus, it will take $8\, T_{hop}$ on average for a bitcoin Node to propagate a block to it’s 8 peers. Ideally, propagation is done sequentially, and not in parallel, since parallel propagation results in a Node’s peers waiting for $8\, T_{hop}$time before they can propagate. In sequential propagation, a Node can propagate a block as soon as it receives the entire block, hence sequential propagation can optimize the MNTL blockchain.

With these parameters we can calculate the time to propagate a block to the majority of the network (90 percentile) as:

$$T_{90} = log_2(m)\ \ T_{hop} \quad where\, m = number\, of\, nodes\, in\, the\, network$$

In bitcoin, it takes $T_{90} = 1.86\, s$ to propagate a block to the majority of Nodes in a 9000 Node network . Since block propagation time $T_B > T_{90}$ at a $T_B = 10\, minutes$for bitcoin, the constraint is satisfied as $10\, minutes = 600\, s > 1.86\, s$.

Given that MNTL's block time is 1 minute , $T_B = 1\,minute = 60\,s$, the block time was reduced by a factor of 10. To account for that we perform the calculation under a symmetric scenario, ie. increasing the block size from 1 Mb to 10 Mb. Hence, T_{hop} is calculated as:

$$T_{hop} = \frac{10\,Mb}{7Mbps} = 1.43\,s \quad for\,the\,Mantle\,blockchain$$

And therefore, $T_{90} = 18.6\,s$. Nevertheless, at MNTL's minimum bandwidth of $BW_{50} = 7\,Mbps$, the constraint $T_B > T_{90}$is satisfied since, $60\,s > 18.6\,s$. Thus the bandwidth threshold, minimum, is set to:

$$R_{bandwidth} = BW_{50} = 56\,mbps = 7\,MBps$$

We then treat our bandwidth data (B_t) as a series of successive bernoulli trials that map bandwidth onto the binomial distribution space, using the previously described binomial transformation (Tr) function, $Tr(X_t\,,\,R)$.

Thus, we map (B_t) onto the binomial space using $R_{bandwidth}$ by calculating the bandwidth vector B as:

$$B = Tr(B_t\,,\,R_{bandwidth}), \quad \forall_t\,time\,intervals\,in\,the\,sample$$

We then calculate the expected value of (B) called B_μ as:

$$B_\mu = E[B] = \frac{1}{n}\sum_{t=1}^{n} B_t \;\; where\,n\,is\,the\;\,number\,of\,samples$$

The latency value B_μ is the average packet loss (drops) for the period after binomial transformation.

Combining the individual QoS scores in a linear fashion yields:

$$PoMB\ rate\ =\ \frac{L_\mu\ +\ D_\mu\ +\ B_\mu}{3}$$

It is now possible to calculate the PoMB score using this rate as:

$$PoMB\ =\ PoMB_T =\ \alpha\left(PoMB\ rate_T\right) + PoMB_{T-1}(1\ -\alpha\ )$$

Given that:

$$\alpha\ =\ \frac{2}{1\ +\ C}$$

The parameter *C* represents the ideal period of time required to be confident that a Node can maintain sufficient QoS. We will revisit the calculation of *C* shortly.

For any Node's block to be accepted by another Node in the network,

$$PoMB_T\ \geq PoMB\ Threshold_T$$

Let $PoMB\ Threshold\ Upper$be the upper bound on the $PoMB\ Threshold_T$ requirement, such that:

$$PoMB\ Threshold\ Upper\ =\ \ .999,\ or\ 99.9\%$$

And let the $PoMB\ Threshold_T$ be the current PoMB threshold at time interval *T*. Initially,

$$PoMB\ Threshold_T =\ \ .9\ or\ 90\%\ \ \ .$$

We define a difference *Diff*:

$$Diff = \ PoMB\ Threshold\ Upper - PoMB\ Threshold_T$$

As the difference between the $PoMB\ Threshold\ Upper$bound and the current $PoMB\ Threshold_T$ at time interval *T,* then it follows that:

$$PoMB\ Threshold_T \ = \ PoMB\ Threshold_{T-1} + \frac{Diff}{G}$$

Where G = time to reach upper bound, or $G \ = \ 6\ months$for $T \leq G$, and $T \in \{1...6\}$. The parameter G was set to 6 months to ensure we have ample time to tune the network up to peak efficiency. Given this constraint, the network is always driving itself towards it's optimal upper bound in *G* amount of time. Nodes will need to provide an increasing QoS to meet the changing PoMB scores necessary to qualify for the block rewards.

If a Node's PoMB score must be at least the minimum required PoMB score at a given time:

$$PoMB_T \ \geq PoMB\ Threshold_T$$

Nodes which do not meet this criteria are denied from inclusion into the DHT at time *T*.

In the context of PoMB scores, *C* can be thought of as a time lag in which past PoMB scores have an impact on determining future PoMB scores. With sufficient data, a time series analysis can be used to calculate the ideal *C* parameter. A Dickey Fuller test can be performed to determine stationarity on a sample set of PoMB scores. Raw PoMB scores, PoMB score differencing or log differencing of PoMB scores can be used.

PoMB score differencing is calculated as:

$$PoMB\ difference\ score_T = PoMB_T - PoMB_{T-1}$$

where *T* = time, for all *T* time intervals in our series. PoMB score log differencing is:

$$PoMB\ log\ difference\ score_T = log(PoMB\ score)_T - log(PoMB\ score)_{T-1}$$

Once the best method of stationarity is chosen, the stationary is split into two data sets, one for training and one for testing. From there, the ideal lag values can be calculated so that the error between the training and testing data is minimized by iteratively computing the Autoregressive Integrated Moving Average (ARIMA) model to identify the ideal *P, D, Q* values for the model using the mean square error (MSE) over the training / testing data sets. Finally, *C* can be determined as:

$$C = argmax\left(P, D, Q\right)$$

A conservative ideal interval for C then is the longest lagging value, whereby a PoMB score from the longest lagging relevant period is influential in determining the current PoMB score.

The PoMB score rewards a high QoS and the lag period is determined using machine learning. Nodes meeting the $PoMB_T$ minimum threshold are allowed into the DHT at time *T*, qualifying them for block rewards. Otherwise, Nodes remain in an unconfirmed (un-validated) state until they can meet the minimum. Each Node therefore optimizes and incentivizes high QoS of the network in a distributed fashion.

Transactions

There are two categories of transactions available on the MNTL blockchain; coin balance transactions and network state transactions. Coin balance transactions are strictly related to the exchange of MNTL.

Network State Transactions

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

Each Node's IPv6 address, k-buckets, and routing table are entered into the coinbase entry. When updating their version of the blockchain, Nodes must verify the block producing Node's block by looking up its DHT from its IPv6 address. This lookup time is O(log(N)) for *N* Nodes in the network. That is *N* Nodes on average must be contacted to determine if the IPv6 address of the block producing Node exists in the current DHT. Since each Node independently performs lookups over the DHT, the DHT offers resistance against bad actors who attempt to alter it. This is because any Node can verify that a candidate block winning Node has posted a valid QoS by performing a search over the DHT. If the Node is present in the current DHT it can be assumed that it’s PoMB requirement has been satisfied.

If greater than 50% of Nodes reject the proof, the block will be discarded as will the block reward. In this case, a block will take longer than 60 seconds to produce and transactions will remain unconfirmed until the winner of the next longest chain is found. If Node failure is random and intermittent, it will typically resolve within the next few blocks, and the average block time will remain unchanged. This randomness can be expressed as an intermittent Poisson process.

This allows for a decentralized incentivization of a high QoS mesh network.

Coin Balance Transactions

There are fees associated with coin balance transactions. Users who want to send MNTL to another user's wallet must pay a network fee. Like Bitcoin, mempool jams are resolved by optimizing for processing transactions that pay the highest fees.

As noted earlier, PoMB Score transactions are the exception to this so that market dynamics of the mempool won't affect the operation of the underlying mesh network.

Transactions Per Second (TPS)

Because MNTL’s blockchain is based on Ravencoin, MNTL has a 1Mb block size and an average transaction size of 480b. Therefore the average number of transactions per block is:

$$Average\ Number\ of\ Transactions\ per\ Block\ =\ \frac{Max\ Block\ Size}{Average\ Transaction\ Size} = \frac{1000000b}{480b} = 2083\ transactions$$

Consequently, the number of transactions per second (TPS) is:

$$TPS\ = \frac{Average\ Transactions\ Per\ Block}{Block\ Time} = \frac{2083}{60s} = 34.7\ TPS$$

MNTL therefore transacts ten times faster than Bitcoin, which has a TPS of 3.47. This is possible because the Mantle blockchain operates over a higher speed network.

Tokenomics

There are approximately 6,000,000,000 MNTL which will be allocated over the course of 63 years and 29 days. Miners can earn these unallocated MNTL until the end of this period, when their mining efforts will shift to earning transaction fees.

Every 100 days the block reward reduces by an average of 10%. Approximately 4167 MNTL per block are allocated to miners during the network epoch. With a 60 second average block time, the total number of MNTL allocated per day is roughly 6,000,000. In this way, 600,000,000 MNTL will be allocated after 100 days at which time the allocation rate will decrease by 10%. After another 100 days the allocation rate will reduce to approximately 63 MNTL per block and a total of 540,000,000 MNTL will have been allocated, and so on until all MNTL are allocated.

The coin production rate can be generalized as follows:

- The number of coins (N_i) produced in current interval (i) is:

$$N_i = 6{,}000{,}000\left(1 - .9^i\right)$$

Where,

$$i = \frac{D - D\,mod\,(100)}{100}$$

and *D* is the number of days since epoch

Hence the block reward formula is determined as follows:

The block reward B_i given in interval (i) is:

$$B_i = \frac{N_i}{144{,}000}$$

This reward lifecycle is designed to give the network ample time to scale to full capacity, after which time it is no longer necessary to incentivize high QoS with crypto rewards. Instead, it becomes necessary to reward transactions on the network using the transaction fees.

Block Rewards

The block rewards are allocated to Nodes who maintain the Mantle mesh network. This is done in part by having Nodes solve blocks using the X16r PoW algorithm, which is more energy efficient than the PoW algorithms implemented in Bitcoin, Ethereum, and other popular cryptocurrencies. To receive a block reward, a Node must:

1. Win the PoW challenge,
2. The block it has solved must be verified by a majority of Nodes, and
3. The Node must meet or exceed the QoS requirements of the network.

Additional block rewards are generated from Wallet to Wallet transaction fees. These transactions go into the mempool after validation. During mempool 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.

After all MNTL are allocated, all rewards are allocated from transaction fees, and this same mechanism acts as an incentive for miners to continue accepting transactions and to maintain the quality of the mesh network.

Appliance

In the process of building a network, Mantle will be the seller of the first generation of Mantle-compatible hardware devices, known as Mantle Harvest devices. As the network matures, Mantle will support an increasing array of 3rd party hardware to make sure that the connecting devices interpolate well and that the network remains healthy until one day when Mantle can be completely agnostic to the devices that connect to it.

These early devices will be produced and sold by Mantle, and will be designed to incentivize early adoption and contribution to the network by being the first devices able to propagate the Mantle blockchain.

Harvesting

The Mantle-branded appliance is called the Harvest. That's because it will harvest MNTL when contributing at least the minimum required bandwidth to the network. It is a powerful Internet appliance designed to contribute to the backbone of the Mantle network by sharing bandwidth, tracking the sharing of its other Nodes, and by verifying the integrity of those Nodes. To incentivize users to share bandwidth, Harvest units that maintain a minimum contribution of bandwidth to the network are eligible for the block reward.

Mantle Hardware

Harvest units therefore must have processing power, memory, and network throughput to perform these tasks. To incentivize early adopters, the first generation of Harvest units will feature state-of-the-art processors, RAM, and network connectivity as outlined in the **First Generation Hardware** section.

Since low-power Nodes don't need to carry a full copy of the blockchain or perform mining activity, they have lower hardware requirements. Nodes only need to connect to the network, share bandwidth and do PoW calculations. These Nodes can therefore run on anything from home computers, to cloud servers, to embedded hardware such as OpenWRT routers.

Integration with the Internet

Nodes can connect to the traditional Internet via an ISP. In this case, they act as routers for any device that connects physically or virtually through the mesh network.

Other Hardware Types

Like other Nodes, low-power devices such as smart TVs, smartphones, embedded devices, and thin clients can also connect to the Mantle network through the Internet or directly through another Node. They can benefit from the Mantle network's enhanced security and transfer speeds, but as these devices won't have the processing power to calculate PoW or provide the minimum bandwidth to contribute to the network. Such devices will not be eligible to receive block rewards.

First Generation Hardware

The first generation of Mantle Harvest machines are intended for early adopters who want to help propagate and build the Mantle network.

Harvest devices will both establish the initial network backbone and provide incentive to early adopters. Harvest devices are high powered and loaded with the Mantle blockchain so that they may harvest MNTL coins by providing minimum bandwidth contribution to the Mantle network and signing other's submitted contributions. As the Mantle network matures, its software will be released as open-source for other users to install on a wide variety of servers, home computers, and network appliances.

Users will be able to host wallets and run Mantle-compatible blockchain software which may be available at a later date.

To support these functions, early Harvest units must:

- Hold an entire copy of the Blockchain,
- Contribute PoMB to the Mesh network and other Nodes,
- Calculate PoMB scores and validate other Nodes,
- Find shortest routing paths and ping times,
- Connect to the Internet,
- Be able to compress and accelerate data transfers, and
- Run Mantle-compatible blockchain software.

To meet these needs, the first generation of Harvest units will have the following specifications:

Processor	4+ Core, 4.20GHz+ Intel® Core™ i7-7700
Memory	16 Gb DDR4 Kingston
Bus	5 GT/s
Network	2 WiFi, 2+ 10Gbps Ethernet
Storage	2Tb 7200RPM Seagate Helium
Video	HDMI
OS	Ubuntu Linux 18.04LTS

Mantle Software will have a software signature that expires after a certain block number is mined. Until then, the software will be semi-closed, available only to early adopters to build the network. After that block is mined, any client can be made that works with the Mantle Blockchain.

Conclusion

By combining mesh networking and blockchain, Mantle will create a peer-to-peer mesh Internet overlay that incentivizes individuals to run routing nodes and to increase the connection quality of those nodes over time.

Glossary

ASIC - An Application Specific Integrated Circuit, a specialized microchip that performs one task extremely well. Sometimes used to mine cryptocurrencies with extreme efficiency.

Bandwidth - The amount of data that can be transmitted between two Nodes during a fixed amount of time.

Bandwidth Spoofing - A network attack where a bad actor falsifies the amount or quality of bandwidth they have access to.

Bitcoin - The earliest and most famous Blockchain and Cryptocurrency.

Block Reward - The Cryptocurrency awarded to a Miner for solving the block.

Blockchain - A type of software that creates a shared, distributed database or ledger of transaction records and a corresponding Cryptocurrency.

cjdns - A mesh networking software that provides distributed addressing and perfect forward secrecy.

Cryptocurrency - A digital coin that can be earned or spent on a Blockchain.

DDoS Attack - A network attack where bad actors overwhelm a server with traffic, preventing others from accessing the server.

DHT - A Distributed Hash Table, set of hashed IP addresses or other data that is stored in parts across a network

IPv4 - An obsolete network address schema used on the internet that features four groups of numbers, for example 192.168.10.123.

IPv6 - A network address schema that features eight groups of four hexadecimal numbers, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334.

Majority Attack - An attack where a bad actor manipulates the majority of Nodes on a network.

Man in the Middle Attack - A Network attack where a bad actor intercepts and/or forges data intended to be private between two other parties.

MantleCoin (MNTL) - MantleCoin, the Mantle cryptocurrency.

Mesh - A type of network where all Nodes route traffic for each other in a point-to-point manner.

Miner - A type of Blockchain user or software that attempts to solve block rewards with the intent of capturing the resulting cryptocurrency block reward.

Node - A network device.

Perfect forward secrecy - A type of cryptographic communication that even when hacked, does not allow a hacker access to future messages.

Proof of Minimum Bandwidth (PoMB) - The

Quality of Service (QoS) - The reliability and speed score of a network.

Ravencoin - A Bitcoin-inspired Blockchain and Cryptocurrency that features fast block processing times.

Statistical Behaviour Modelling Attack - A type of network attack where sufficient data is tracked about a user, then analyzed to discern specific behaviors.

Sybil Attack - A type of network attack where a bad actor creates many virtual identities.

Wallet - A virtual account on a Blockchain that can hold Cryptocurrency.