MFC NETWORK

A Decentralized Internet Protocols Suite

v0.1

Michael Dye, Johndis, Bumbr, Jared Grey

2019.12.18

Abstract

In this paper, we present a new framework for decentralized internet protocols called ‘The MFC Network’. This network will be anonymous, scalable,flexible and will allow users to access data and services in a private and censorship-resistant manner. An underlying utility token, MFC Coin (FOR), serves multiple purposes which range from an incentivization mechanism for service delivery and quality thereof to a tool for agreement over simultaneous network consensus and serves as a secure means of transferring encryption keys between participating nodes. The MFC Network will empower people around the world to access information and secure networks even under the most oppressive regimes, allowing information to existing free from removal and unauthorized manipulation.

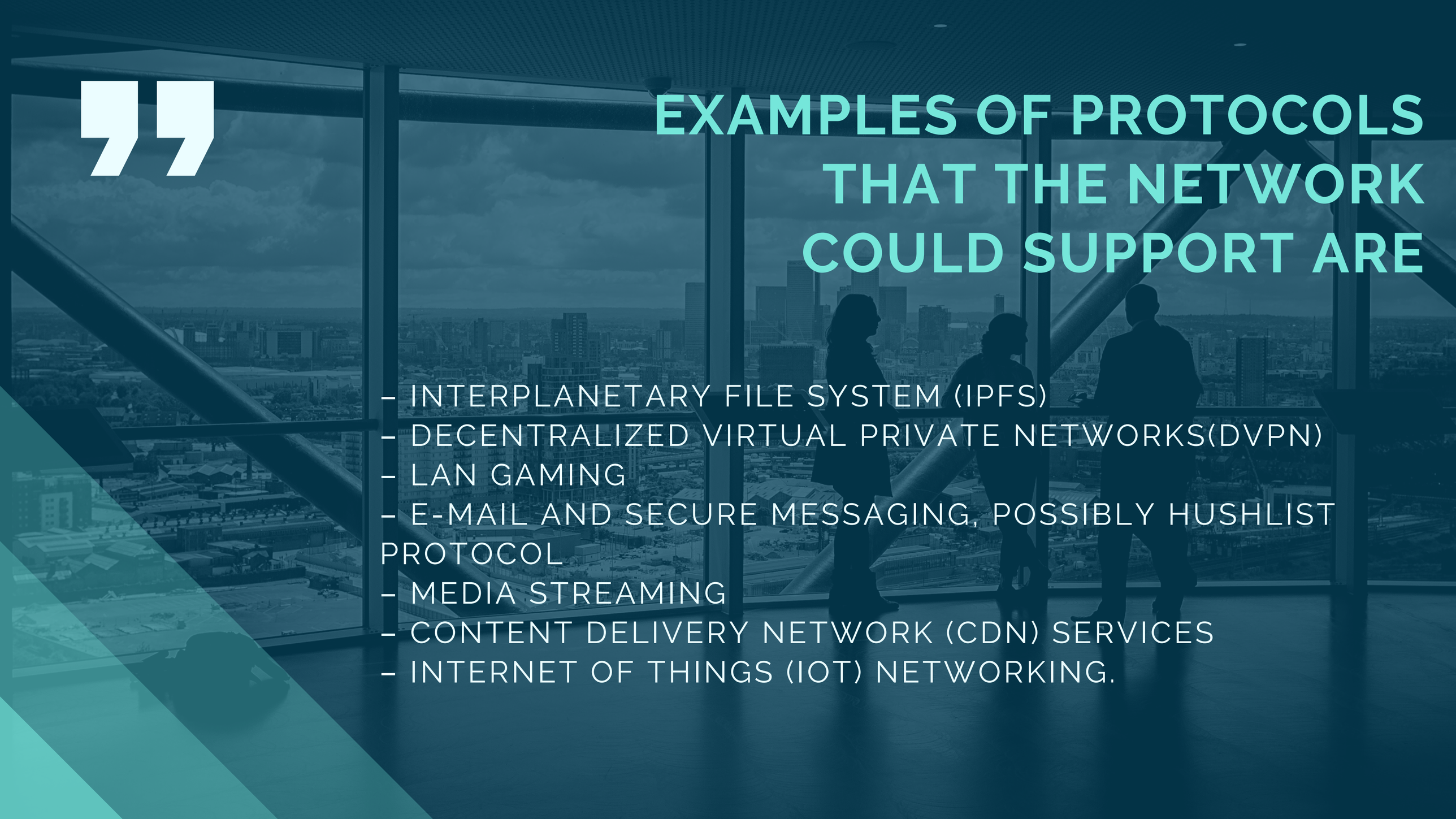
I Introduction

The MFC Network aims to be fully anonymous, a scalable,
and flexible set of protocols that offer censorship-resistant access to data and network services. We refer to this set of protocols as Decentralized Scalable Network Services (DSNS). The MFC team will develop the underlying utility token called MFC Coin (FOR), the distribution network infrastructure, and the system that will allow net nodes to provide an ever-expanding list of different network protocols. Independent developers will be able to build applications utilizing The MFC Network on top of any other 3rd party platform.
After successfully connecting to The MFC Network, connecting to the applicable service net nodes will feel the same as connecting to a physical local area network (LAN).

While centralized networks are prone to censorship, content access restrictions,and singular points of failure, their advantage over their decentralizedcounterparts is that they are in a better position to commit persistenthigh-end resources with full failover redundancy and availability due to their centrally planned nature.
The MFC Network will be a decentralized network where service provider participation is voluntary, we will outline our proposed solution to keep said providers incentivized to maintain their services long-term and prevent service interruptions and sub-sequent user experience degradation.

The first protocol to be implemented will be the Hypertext Transfer Protocol (HTTP). This means that anyone will be able to connect to The MFC Network using a customized,in-wallet web browser framework. This browser will be a cross-platform for both mobile and desktop devices and interact with our network and the regular internet alike, with the difference being that content from the network of decentralized net nodes will be distributed using end-to-end encryption. While using The MFC Network, the uploaded or downloaded content will be undecipherable by outside entities such as internet service providers.

Distributed, private internet is just the beginning. The MFC Network also aims to allow net nodes to host any pre-defined network protocol. MFC net nodes will be grouped by the protocol they provide (Distributed Service Hive or DSH), as well as by access permission levels, enforced at the network level.



EXAMPLES OF PROTOCOLS THAT THE NETWORK COULD SUPPORT ARE

- INTERPLANETARY FILE SYSTEM (IPFS)
- DECENTRALIZED VIRTUAL PRIVATE NETWORKS(DVPN)
- LAN GAMING
- E-MAIL AND SECURE MESSAGING, POSSIBLY HUSHLIST PROTOCOL
- MEDIA STREAMING
- CONTENT DELIVERY NETWORK (CDN) SERVICES
- INTERNET OF THINGS (IOT) NETWORKING.

II Key Points of Competitive Differentiation

The MFC Network is intended to be a large-scale, decentralized network where participants are encouraged to provide and consume a broad range of network services in a trustless, private and secure way. The MFC Network aims to accomplish these goals using economic incentivization. For the network to be self-sustaining and successful in this endeavor, it must demonstrate its worth in the face of other solutions that operate in a similar space.

In the interest of assessing the market potential of The MFC Networks services and its ability to disrupt the current landscape, we have created a list of several key points that we believe are strong differentiators from existing competitors that will drive The MFC Networks long term viability.

1. Full network privacy and data encryption.
The MFC Network is the only protocol coin that is fully private, end-to-end encrypted, with content that is resistant to take-downs from forces outside the network. The MFC Network goes to great lengths to ensure that:

– The clients IP is never directly revealed
– Content providers IP is never directly revealed
– Data cannot be traced back to the client or host
– Data cannot be deciphered by any intermediary.

2. Fully independent from traditional, technically constrained solutions. Other projects are attempting to provide a decentralized internet using regular web browsers. While using stock web browsers would be ideal from a user perspective, it presents too many logistical problems for the secure and private network services we wish to provide.

– DNS protocols: Using existing web frame-work forces the network to comply with, and be subject to, the constraints imposed by existing web protocols, including DNS. DNS has historically been the first point of attack for censoring content. Some solutions, such as DNSchain, attempt to solve this problem, but cannot do so in a fully-encrypted way that hides the final destination IP. Further, while it allows sites to keep their existing domain if needed, it runs the risk of centralization and fails to meet our criteria for true censorship-resistant and self-contained network.

– SSL encryption: Using regular web browsers means the only encryption scheme available is SSL. This requires browser modification for the import of custom SSL certificates and cannot natively implement Forces' much more powerful multi-encryption scheme.

– By using existing web browsers, there is no way to obfuscate the client and host IP. This is essential to keeping MFC private and censorship-resistant.
To make the network truly private, MFC opts to develop a custom browser, delivered in-wallet. This allows The MFC Network to use its name resolution and encryption protocols, ensuring anonymous traffic on the network stays secret and censorship-resistant.

With the above considered, unencrypted public pages will be available to view with regular web browsers. This service will allow everyone to view public information such as services, prices, and payment node wallet addresses in the easiest way possible. The unencrypted public pages also provide a familiar entry-point to contract services on The MFC Network.

3. MFC is a multi-protocol network, enabling a broad suite of decentralized and scalable network services. In addition to the privacy features of The MFC Network, we aim to be much more than just a web solution. We plan to deliver an entire array of private network services and protocols, building off The MFC Network base protocol as described in section III.

This is the point that highly distinguishes The MFC Network from similar technologies. In becoming more than a limited, non-expandable,web-only solution, The MFC aims to be a protocol-agnostic and expandable framework. The MFC Network can support a multitude of services of various natures, effectively providing a full substitute to existing large-scale traditional networks.

4. Granular, service-specific payment model. The MFC Network makes full use of economic surplus, by utilizing a smart pricing mechanism (MFC) and the node health information database. The network continuously monitors for areas of service (DSHs) that are under or over-served and adjusts pricing accordingly, network-wide, to ensure that participants constantly strive towards equilibrium of quality and availability across the range of services provided by the network.

This is a radically different approach to traditional load balancing mechanisms that exist in single-task services. The load is no longer regarded to be network resources that aren't being optimally used to deliver a service. But rather, the economic value that is left untapped as entire service areas are balanced against each other to reach a harmony between the supply and the demand sides.

5. The MFC Network uses a dynamic Plug-and-Play, Uber-like, service providing model. Being the counterpoint to paragraph number 4, above, and enabling smart pricing to take place, nodes can dynamically detach from and attach to any DSH, based on their preferences, without the need to install any additional hardware. It is a seamless transition that allows the network, as a whole, to provide very little downtime, the superior quality of service and user experience, while fully compensating service providers in the process.
Withdrawing from the network as a service provider will incur a cost, however, it will be significantly lower than that which typically accompanies the process. This will only apply during active service delivery and will be free of charge if the node is idle.

This model of cost allocation helps to level the playing field and increases accountability for all participants. Currently, the cost associated with service switching overwhelmingly burdens consumers, while service providers incur minimal cancellation fees (for example, the cancellation fee for any recurring service termination).

The MFC Network also anticipates more advanced net node management tools will be developed to intelligently assist net node providers in maximizing utilization of their nodes (thus income), such as internal services that automatically monitor the market and perform soft (fee-less) transitions from low demand services to high demand services.

III Network Infrastructure Overview

III. A NETWORK LAYERING

We propose a three-layer network model to provide The Network Forces services. These three layers interact with each other to ensure that The MFC service is operational.

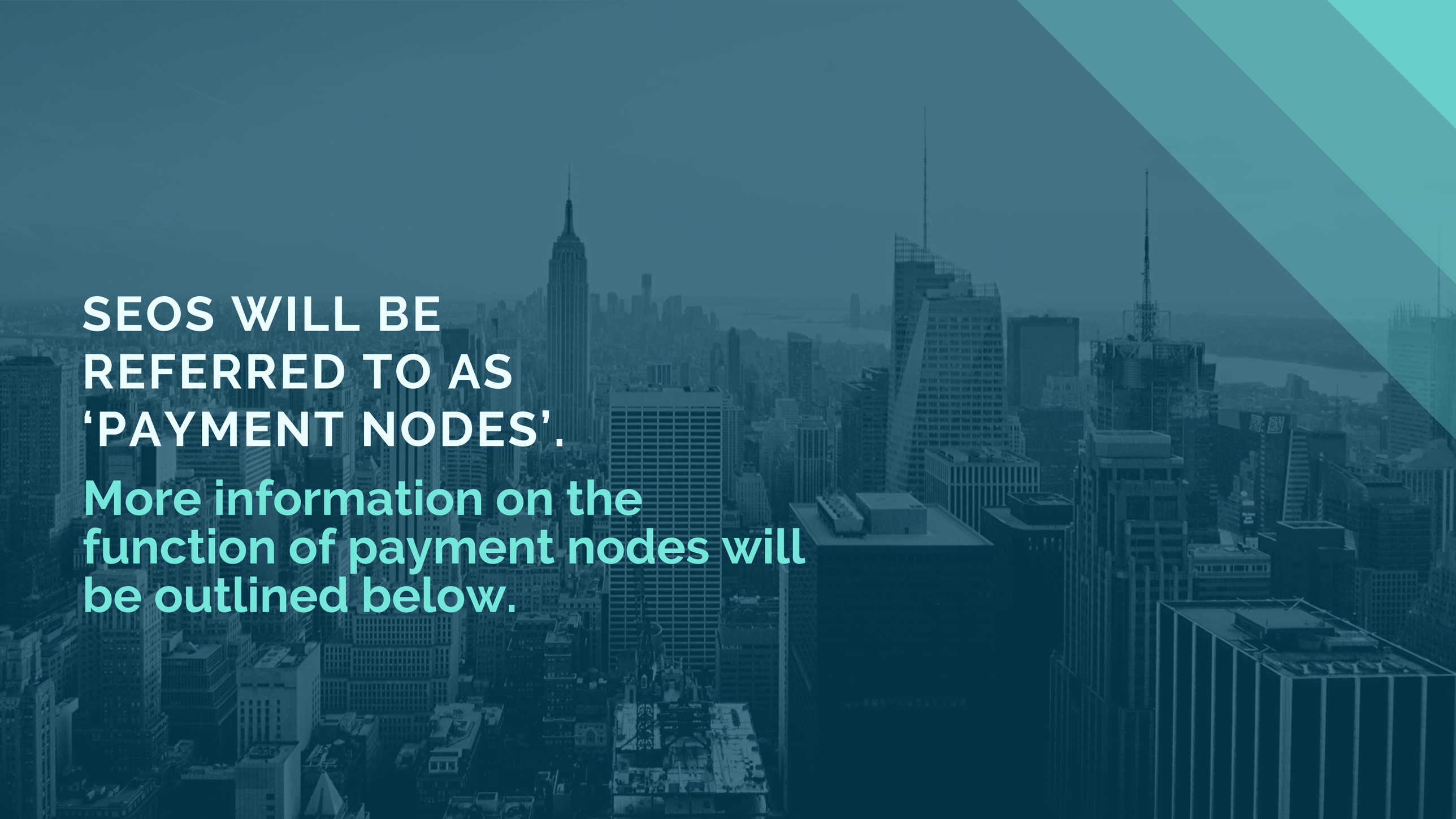
Layer 1 will be the base proof-of-stake consensus protocol, with a private blockchain attached. This is where transactions on The MFC Network will take place and utilize proof-of-stake validation. Encryption keys and entry point IPs will also be transferred using Layer 1.

- Layer 2 will feature master nodes that will act as the first connection point into The Network. The master nodes will host content such as the network service index pages, node health information, and encrypted hop node routes.The index pages will include information such as network service descriptions,pricing, and payment node wallet addresses.
These pages will also be available to view using thetraditional internet.
Network service index pages can only be updated with the correct private key, generated by the payment node when creating the service.
The master nodes will also accumulate and store Network Health Information (NHI) for the payment nodes to monitor. While all real-world identifying information will be encrypted to prevent a breach of privacy, NHI will be publicly visible as a means of providing consumers with much-needed transparency, to aid in the selection process of their future service providers. The master node will not know the direct IP of any nodes. Instead, the payment node will generate unique routes upon completed payment for services (see section III D.). Masternodes periodically hash their databases and ensure they are in sync with the rest of the master node network.

– Layer 3 will be the service hosting and delivery layer, consisting of a variety of different nodes. These are the nodes that provide all of the low levels of network protocol services. (See a list of example network protocols supported in the Introduction section). Each node can, at any given point in time, voluntarily and dynamically enter or exit a Distributed Service Hive (DSH). A DSH is a collection of net nodes concurrently running a service-specific protocol to form a distributed network that hosts and delivers the service. For example, the DVPN service will be its DSH were any number of nodes could concurrently join or leave the said hive, and each hive will be providing its service using its constituent nodes. A node can also be run as a payment node, known as Service Escrow Oracles (SEO). The function of SEOs is to:

– Serve as intermediaries between service providers and consumers;
– Ensure that the service is delivered securely against the delivery of payment;
– Contract nodes;

– Generate hop node chains (see section III.D)
– Multi-encrypt hop chain IPs
– Transfer encryption keys for each step of the hop node chain to the client



SEOS WILL BE REFERRED TO AS ‘PAYMENT NODES’.

More information on the function of payment nodes will be outlined below.

III NETWORK INFRASTRUCTURE OVERVIEW

III. A NETWORK LAYERING

We propose a three-layer network model to provide The Network Forces services. These three layers interact with each other to ensure that The MFC service is operational.

– Layer 1 will be the base proof-of-stake consensus protocol, with a private blockchain attached. This is where transactions on The MFC Network will take place and utilize proof-of-stake validation. Encryption keys and entry point IPs will also be transferred using Layer 1.

– Layer 2 will feature master nodes that will act as the first connection point into The Network. The master nodes will host content such as the network service index pages, node health information, and encrypted hop node routes. The index pages will include information such as network service descriptions, pricing, and payment node wallet addresses. These pages will also be available to view using the traditional internet. Network service index pages can only be updated with the correct private key, generated by the payment node when creating the service. The master nodes will also accumulate and store Network Health Information (NHI) for the payment nodes to monitor.

While all real-world identifying information will be encrypted to prevent a breach of privacy, NHI will be publicly visible as a means of providing consumers with much-needed transparency, to aid in the selection process of their future service providers. The master node will not know the direct IP of any nodes. Instead, the payment node will generate unique routes upon completed payment for services (see section III D.).

Masternodes periodically hash their databases and ensure they are in sync with the rest of the master node network.

III. B AD-HOC CHAIN ROUTING AND LARGE-SCALE TUNNELED NETWORK ARCHITECTURES

The MFC Network utilizes the Ad-Hoc Chain Routing mechanism (AHCR) which means that requests are not broadcast to the entire network. Instead, requests travel only along the hop node chain, with each hop node knowing only the IP address of the node that came before it, and the one to which the transaction is passing to next according to the type of service request. Responses travel back along the same chain until they get to the requestor. Even the node directly after the original requestor does not know who the original requestor is, as it looks like just another hop node.

Within the framework of The MFC Network, Unique Hashed Public Addresses (UHPA) are used to identify nodes. The UHPAs are stored by master nodes alongside other vital service data to produce a dynamic database that payment nodes can use to determine the optimal nodes to include in ad-hoc chains for each service request. UHPA is used to correlate public information with nodes, while traditional IP addresses are only used by payment nodes during the hop node generation process and by hop nodes themselves (see section III D for more in-depth description). IP addresses are used only when necessary to enable base TCP/IP communication between nodes.

To complement the AHCR mechanism, and form a depth-efficient and connectivity-complete mapping and routing solution, The MFC Network will use a LargeScale Tunneled Network (LSTN) architecture, where each participating node will automatically be assigned a UHPA which is known to the array of master nodes. The use of an LSTN keeps all IPs completely hidden from the publicly accessible master node network. The IP of each contracted node is only sent to the payment node after payment for the contract is received.

A node can opt for providing multiple services simultaneously and subsequently join more than a single DSH at the same time.
Before the node joins a new DSH it generates a new UHPA and uploads it to the master nodes. This reduces attack vectors as service identities are more difficult to correlate. DSHs themselves will not contain any routing information and will constitute simple and efficient service-grouping constructs for participating nodes.

III. C COMMUNICATION WITH THE NETWORK

Establishing services for the first time requires a delicate back-and-forth to maintain privacy and censorship resistance. In this section, we outline the process The MFC Network will undertake to utilize a service from the moment the client connects to a master node to the moment the client receives the requested data.

1. The client requests the list of services hosted by the closest master node and selects a service. Listed are the minimum price required, a wallet address, and the type of service provided.

2. The client sends an amount of FOR to the specified address with the following attached to the transaction:

- The public key of a unique key pair it generates to decrypt the data.
- The approximate location of the client for route optimization (optional)
- Any other information required for the type of service being offered

3. A payment node associated with the wallet address is triggered by the payment and generates a hop node chain. This process sets up an encrypted, anonymous connection between the client and the service provider. (The steps are outlined below in ‘How Hop Node Chains are Created’).

4. The payment node encrypts the entry point IP with the client's public key and sends a micro-transaction back to the client with this data attached.

5. The client decrypts the entry hop node IP using the private key is generated in step 2 and now has an entry point to The MFC Network, and all the encryption keys necessary to multi-encrypt the data request for each hop. (See Hop Node IP Encryption for details).

6. The client can now multi-encrypt and send/receive data as normal for the service to/from the hop chain entry point IP. The entry hop node will forward the data to the next-hop node IP set by the payment node, and the data will continue this way until it reaches the end hosting node.

III. D How Hop Node Chains are Created (Hop Node Chains Generation Process)

Once the client sends payment to the payment nodes' wallet address, the payment node will generate a hop chain for the client to connect to the requested service node. For the network to run quickly and smoothly, payment nodes must be very economical about how they generate hop node chains. Each chain can be generated dynamically, unique to the client requesting it. Chains must also be resilient and provide longevity. Therefore, the chain generation process happens as infrequently as possible.

Masternodes provide a list of every hop node by UHPA which includes wallet address, public encryption key, approximate geolocation, uptime ratio, and the cost for those services. A single node running a single wallet can have multiple UHPAs for different services rendered. Payment nodes use this list to dynamically contract the best nodes for providing the service to the client. In the case of our initial internet-like service, best would mean nodes located near the client to minimize latency.

WHEN A PAYMENT NODE LOCATES SUITABLE HOP NODES, IT SENDS PAYMENT WITH A CONTRACT PACKET ATTACHED AND ENCRYPTED WITH THE NODES' PUBLIC KEY. THE CONTRACT PACKET INCLUDES:

– A service ID to identify this contract
– A passphrase key to identifying and authenticate the end-user
– A private key to decrypt the multi-encrypted data by one stage to make tracking data across nodes impossible
– The IP of the next node in the chain to forward the data to
– Additional hop node IPs if the primary node fails (optional service)

If a service wants to minimize generating additional hop nodes if one fails, alternate next-hop IPs can be provided when the chain is firstgenerated. If the primary point fails, an alternate can be tried without the need for a new hop chain to be generated.

If there is no way for a hop node to pass the data along, a failure is sent back, along the chain, to the client with a refund minus transaction fees.

The client will then send another transaction to the payment nodes' wallet to generate a new chain. These transactions could be micro-payments for the least expensive solution or encompass a larger payment for services purchased in advance.

This upload/retrieval mechanism for the hop chain has multiple benefits:

– The IP of the payment and content hosting nodes is never revealed to theclient.

– The client's IP is never revealed to the payment or content hosting nodes.

– Payment nodes have the option to preemptively monitor node status and send new hop node IP when necessary.

– Hop nodes only know the previous IP and the next IP in the chain. They do not know which stage in the chain they are, so they cannot know if the previous IP is a client, or if the next IP is the final destination.

All communication conducted across The MFC Network will be encrypted using hardware-supported encryption algorithms. This is in contrast with traditional SSL certificates, which require known, centrally-issued domain names as the trust beneficiary. As traditional browsers such as Chrome, Firefox, and Safari are designed to require such SSL certification to reliably inform the user that their communication is encrypted, The MFC Network will use a custom, in-wallet, Chromium-based embedded browser, while maintaining the same level of usability and user-friendliness to which end users are accustomed. The browser and wallet
will be open-source to allow for independent security auditing.

Once the aforementioned technology set is fully developed and secured, the next milestone will be to port some services over to the traditional desktop and mobile browsers by using a custom extension and/or mobile app as a bridge between browser design requirements and The MFC Network architecture. This will enable The MFC to expand its service offerings to a far larger market.

Each DSH will set the number of required hops for its service. This autonomy will allow some services to be more private than others at an increased cost. Some data, like index pages, can be listed as non-private and can be served directly from the master nodes using the traditional internet.

Hop node chains are created by the payment node when payment is received from the client. The payment node can consider multiple factors when designing the requested hop node chain based on the service, bandwidth requirements, approximate location, etc.

III. E How the Payment Node Generates the Chain Backwards for Restricted IP Knowledge

III. E How the Payment Node Generates the Chain Backwards for Restricted IP Knowledge

IP addresses are powerful. An IP address is a method by which content hosts can be identified and content removed. Since we are building a network oftakedown-resistant pages, we must be very careful in the protocol for managing the security for IP addresses, especially the IP of the final hosting node.

To maintain this security-sensitive information, we will utilize a restricted knowledge scheme so that only the previous node in a chain knows the next IP address in the chain and none of the service nodes are aware of the final destination.

1

Payment node gets hosting node IP either by contracting one or using one which the service providers establish.

2

The payment node contracts the final hop node in the chain and sends it to the IP of the hosting node as the next hop. That hop node sends its IP to the payment node (with another micro transaction).

3

The payment node contracts the final hop node in the chain and sends it to the IP of the hosting node as the next hop. That hop node sends its IP to the payment node (with another micro transaction).

4

Eventually, the payment node gets to the first-hop node in the chain and sends that IP to the client as the entry point.

IV Advanced Service-Supporting Network Features

IV. A A Network Health Information and Hash-based Node Uptime Verification (HNUV)

If a node wishes to discontinue its services, (permanently or temporarily, and regardless of reason), it must go through the proper withdrawal procedure. This entails sending a withdrawal notification to the master node, which can update the node database. This database gets periodically checked by payment nodes to determine node availability for a hop-chain generation as well as downtime payment penalties.

If a node does go down without following the withdrawal procedures, there will be a retry mechanism built into the hop node chain. The node which is located before the failing node will send the IP of the failing node to the payment node with a micro-transaction. The payment node will then either send

a new next-IP to that hop node or generate an entirely new chain and send it to the client. Based on the contracted payment scheme, the payment node will take note of the failed node, penalize it, and send a report to the master node health information database.

To accomplish this, each node will need to have an MFC wallet open and running. The wallet will periodically send encrypted data to the master node network, including UHPA, types of services offered, approximate location for efficient routing, uptime, and status. This will allow new payment nodes to choose the best route for each originator. With enough reports of a failing node, the master node will update the nodes status and uptime ratio in the database then propagate the update to the other master nodes. When the node comes online again, it must re-send its service entry to the master node to get re-listed. As there is no way for hop nodes to send data to payment nodes without a transaction, they instead periodically transmit health information to the master node network so that they may be contacted by new payment nodes.

To further protect the network against malicious actors and ensure QoS, the HNUV mechanism will be put in place. Much like blockchain consensus can elect to accept or reject a node from the network based on the integrity of the data it broadcasts by simply verifying its headers hash, any malicious attempt by a node to retain its active status for payment by altering its client to send false uptime data without rendering the service offered by the DSH of which it is a member, will result in rejection from the network followed by a cool-down period penalty for rejoining. This will be done by verifying the hash of the clients' code, as well as key parameters it periodically broadcasts using a unique hashing and verification algorithm, the HNUV.

IV. B Customizable Privacy Levels

Different types of content can have different levels of security based on how the payment node is established for the service.
We describe the highest levels of security in this white paper, because they are the most difficult to implement. Anything less than this (fewer hops, no hops, less encryption, etc.) will be available for services that desire speed over absolute privacy or content resilience.

IV. C Hosting Content and/or Services on The MFC Network

Content and service providers have numerous methods of getting their content on The MFC Network. For a simple example, let's say you want to host a censorship-resistant web page on The MFC Network.

- Set up (or contract) a payment node and establish a price for your content. Free content is easily distributed through an existing network but, must be accessible to everyone. Content/services that use the permission system to restrict access, must charge a price.

- Set up (or contract) a network of hop nodes to use. The payment node can also be designed to use the master node database to contract hop nodes dynamically for each user with nodes that meets its list of criteria.

- Set up (or contract) a net node that connects to the Web DSH to store and host your content.

- Upload a service index page to the master node network and enable your payment node to accept payment from clients. It can now generate hop node chains for clients to the net node for content delivery.

Developers will build services that automate common tasks on the MFC Network and provide templates.
They will also build full content management suites that sit on top of the MFC Network. One service network or net node might contract another to aggregate content in a single place for user convenience.

IV. D Network Access Control Model

Security and privacy are at the heart of The MFC Network. By our emphasis on security and privacy, we will develop an extensive permission-based access control mechanism at the network level. Malicious actors will have no way to connect directly to the service delivery net nodes.
They must go through the full authorization scheme set up by the payment nodes to even view the IP of the first hop node.
They must also possess the correct service key before the entry node can properly route their request.

To illustrate this power of network-restricted access,
let us compare it to the current model. With the existing internet, there are no built-in restrictions on accessing content. Each web page must have its account management features to secure its content from the public. Anyone has access to these username and password fields. Without restrictions in place,
the traditional internet is constantly vulnerable to injection hacks and brute MFC. Also, the IP of the server is directly available to attackers, which makes the site vulnerable to DDOS and other server attacks.

In contrast, The MFC Network requires a potential user to
navigate multiple layers of security. Unless explicitly granted access, the payment node will not release the IP of the first-hop node to you. Even if you had that, service nodes will not propagate your request, or provide any other services without the correct service key. Based on the service key, requests can even be routed to different net nodes, based on the level of access. This access, controlled at the network level vastly reduces hacker attack vectors.

Each page, file, or service can have its permissions list, with options such as: allow everyone, restricted read access, restricted write access, etc. Since nodes are distributed, there is no need to host restricted information on the same node as public information. This means that a web site could have a publicly accessible index page that is available to everyone and hosted on the free node network. The public index page could explain what the site offers, as well as pricing, and a payment node wallet address. The rest of the site/service would then only be accessible after satisfying the requirements of the payment node for that site.

V. TOKEN UTILITY AND ECONOMICS

V. A FOR Token Use Cases

1. To pay for services. These are remitted directly by consumers to escrow payment nodes who in turn relay it to the service providing nodes, minus a fee. The payment node can group payments based on the node payment scheme to reduce the load on the network and transfer fees.

2. To handle the authentication key exchange. Clients pay the wallet address associated with a service, listed in the master node database. A payment node monitors the wallet and sends access keys to the client after generating the network chain.

3. To stake coins to create a node (master, payment, hop, net, etc.) to ensure good behavior

4. To reward master nodes and coin stakers for providing consensus, enhanced services, and securing The MFC Network.

V. B STAKING FOR TOKENS

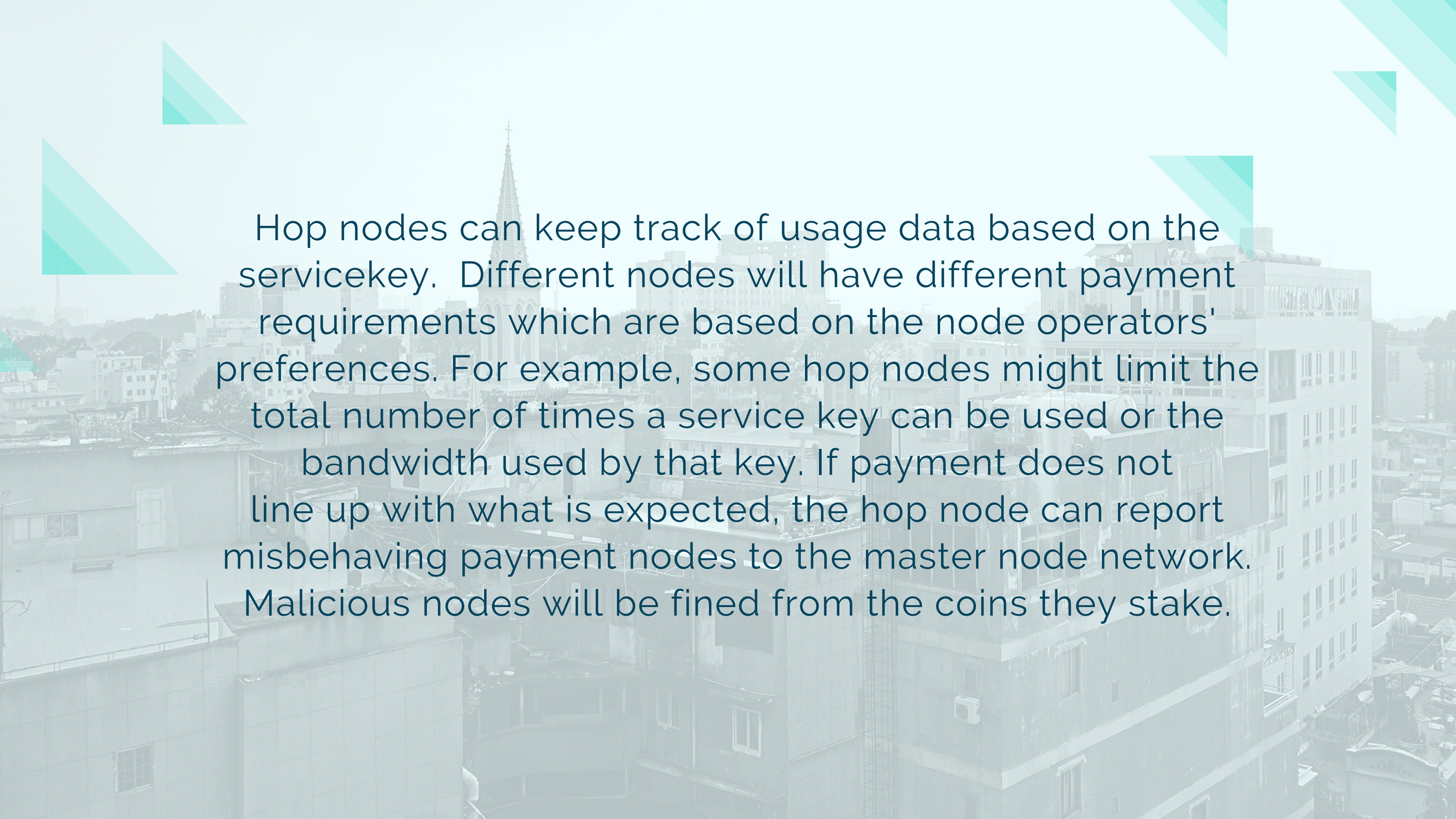
Anyone can turn their device into any type of MFC node they want, depending on the resources they own and wish to allocate to the network. A node type can only be enabled if the node-specific resource requirements are met
(such as token collateral and hardware requirements).

By design, the more critical a type of node is to the network, the higher the collateral it requires for a user to operate it. As a result, the more critical a node becomes, the less likely users are to pursue malicious attack vectors on the network using said node, as they risk an even greater share of their investment. This is the very fundamental premise driving proof-of-stake consensus security applied to The MFC Network.

V. C PAYMENT FOR SERVICES

The MFC Network operates by hiding as much connectivity information as possible. This section will describe how services are paid for using the FOR cryptocurrency.

The service node keeps track of usage based on the service key generated during network chain creation. It can notify the client when sending data that additional funds are needed and can shut down access to content if required. The client can then send additional funds to the payment node which then updates the payment status in the service node.
The payment node will use those funds to pay the hop nodes using the agreed-upon service scheme.



Hop nodes can keep track of usage data based on the servicekey. Different nodes will have different payment requirements which are based on the node operators' preferences. For example, some hop nodes might limit the total number of times a service key can be used or the bandwidth used by that key. If payment does not line up with what is expected, the hop node can report misbehaving payment nodes to the master node network. Malicious nodes will be fined from the coins they stake.

V. D DYNAMIC SERVICE PRICING (MFC)

As the network will be distributed and service provider participation will be voluntary, the architecture must be able to ensure high standards of service availability to keep up with demand. A relatively simple way of ensuring unparalleled service availability would be to incentivize service providers by creating a fair and dynamically evolving smart pricing mechanism for the services they offer. For this we propose the Dynamic Service Pricing (MFC) mechanism. The MFC is a function computed and verified by the network, whose purpose is to determine the most economical price point for service providers, in as close to real-time as possible, based on a combination of factors:

1. Composite Service Network Requirement Score (CSNRS): The network will gauge the general level of resources needed by each service to provide sufficient quality of service, create a composite score to serve as a multiplier, and, all else being equal, the higher the requirements of the service, the higher the price point will be to ensure adequate compensation.

2. The ratio of the number of active users consuming each service (service demand) Nu to the number of net nodes actively participating in the DHS (service supply) N node.

3. (Optional) Fiat value of the FOR token, based on volume-weighted average retrieved from exchanges data.

Service-specific MFCs will calculate and normalize their data to create a service price ranking. Each normalized MFC score will be multiplied by the Network Price Index (NPI), which will be derived by reviewing number 2, above, both as a ratio and as absolute numbers.

Each node will also receive a base rank determined by its network performance and service reliability. This will create an element of competition between nodes to become the most reliable node per each service. A node that keeps bouncing between services and subsequently creates interruptions will be scored much lower than a node that persists even if service-wide pricing drops.

Pricing information will be propagated by the network and be available to all participants. Based on MFC data, clients will be able to make educated service consumption decisions and service providers will be able to determine which hives their nodes should connect at any given point in time. This will also serve the purpose of adjusting for demand. Too many nodes will not support under-demanded services and conversely, too few nodes will not support over demanded services.

VI. Conclusion

In this paper, we presented a high-level overview of a new decentralized network infrastructure that powers Decentralized Scalable Network Services (DSNS). Under this new paradigm, clients will be able to consume ad-hoc network services rendered by service providers, with very little upfront knowledge or resource requirements. This will be done via a service-agnostic, unbiased, autonomous and trustless client-provider matching mechanism while keeping participant identity fully obfuscated. The protocol features two novel

architectures: Ad-Hoc Chain Routing (AHCR) and Large-Scale Tunneled Network (LSTN). These are designed in such a way that allows the communications and content handled by the network to be censorship-resistant using end-to-end encryption.

Service providers can seamlessly join and/or migrate between services or withdraw from the network altogether and are incentivized to maintain a consistent record of service quality to prevent service degradation, using ranking and real-time pricing algorithms that are maintained by cross-network consensus. Actors responsible for the security and resilience of the underlying infrastructure are regularly compensated by the network for their services using it's underlying economic token, MFC Coin (FOR), whereas network service providers compete directly over service quality and experience for compensation paid directly by end-users in a said token.

Traditional network services are inherently at a disadvantage due to their centralized nature; they require trust on multiple levels to maintain service integrity. For example, global initiatives that seek to undermine net neutrality for honest participants are gaining momentum and can be easily implemented by central authorities and service providers, as long as consensus is concentrated in the hands of a few. As MFC Network relies on a trustless network consensus using a Proof-of-Stake mechanism, it becomes economically infeasible to attempt to breach any aspect of its operation.

MFC Network aims to not only protect freedom of information against undesirable censorship on a global scale but to disrupt the established commercial landscape through its robust and resilient architecture. With very broad market applications, such as encrypted communication, content delivery, media streaming, pay-per-view, and cloud computing and storage services, and at a time where businesses demonstrate an ever-increasing hunger for fully managed services, task automation, hardware outsourcing, rapid service deployment, and big data storage, the opportunity landscape for MFC Network is vast with its low-cost, low-maintenance, frictionless and trustless commercial profile.

Together with an entire set of internet protocols, this network architecture will pave the way for a new kind of internet. This document will serve as a reference for developments and will be improved upon gradually by addressing potential flaws and attack vectors and describing lower level implementations in detail as they are rolled out.

Special Thanks

THE AUTHORS WOULD LIKE TO GIVE A SPECIAL THANKS TO IHACKCOINZ AND PDQ FOR THEIR INSIGHTS AND CONTRIBUTION TO THE WRITING OF THIS PAPER.