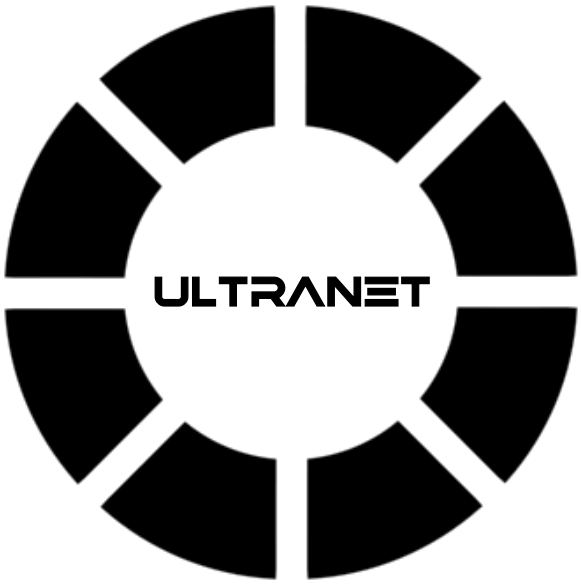


Technical White Paper

28 Apr 2022

(Continuously updated)

https://ultranet.org

Abstract: Ultranet introduces an open decentralized infrastructure for publishing, distribution, verification and delivery of any kind of software, particularly a new generation of non-Web-based Internet applications that blur the distinction between Web, mobile and desktop platforms. Three major components – RDN, DMS and AMPP – cover the delivery, management and protection aspects of Ultranet. The peer-to-peer and blockchain components of Ultranet revolutionize the way in which software is published and delivered to users. A distributed permission-less cryptography-protected database is in turn used to manage software distribution and may be considered as a hybrid of an "app store" and a domain name service. A special protocol is also used as a decentralized verification service and signaling network for protecting the whole ecosystem from malicious software and other threats.

Contents

Glossary

Blockchain a growing list of records, called blocks, which are linked using cryptography

dApp Decentralized application (dapp, Dapp, dApp, or DApp): a computer application that runs on a distributed computing system. DApps have been mostly popularized by distributed ledger technologies (DLTs), specifically Ethereum Blockchain, where dApps are often referred to as smart contracts.

DDOS Distributed denial of service: a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet. In a DDOS attack, the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

GUI Graphical user interface: a form of user interface that allows users to interact with electronic devices through graphical icons and visual indicators such as secondary notation

HTML Hypertext Markup Language: the standard markup language for creating Web pages and Web applications

HTTP Hypertext Transfer Protocol: an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, wherein hypertext documents include hyperlinks to other resources that the user can easily access.

IPFS InterPlanetary File System: a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system.

OS Operating system: system software that manages computer hardware and software resources and provides common services for computer programs

TTI Time to interact: the performance metric that measures the time between a point when the user has requested the application and when the user can start to interact with it.

VR Virtual reality: an experience taking place within simulated and immersive environments that can be similar to, or completely different from, the real world.

The Challenges

A long-standing problem with the Internet is its server-centric architecture. Every Web request to every website is processed by Web servers. Because of this, they often suffer from heavy loads, but more importantly, this makes them ideal targets for censorship, DDOS, and hacker attacks. Decentralized application platforms (dApp) is a promising new technology that has the potential to eliminate the need for centralized servers by transforming the current Web architecture into a homogeneous peer-to-peer network. However, it only deals with the server applications layer and still has to rely on conventional infrastructure for application and UI delivery. There are also other issues related to creating a decentralized Web server:

- High node hardware requirements, as a result of which such networks degenerate into conventional highly centralized clouds.
- Difficulties with efficient load balancing and session synchronization
- Existing P2P solutions work for static content only.

The same problem concerns downloadable applications as well, as they rely on centralized locations from where they are published, downloaded and updated.

To overcome the above challenges and to achieve complete decentralization, we propose to move away from pure Web-based and traditional stand-alone application paradigms and proceed with a more advanced approach. Let's summarize all the requirements of a new technology:

- True decentralization of publishing, distribution and delivery
- Free for users; free or as cheap as possible for publishers
- High scalability
- High resistance to DDOS, censorship and other threats
- Minimizing malicious activity on infrastructure, local system, and user data
- Open platform to avoid any patent infringement cases, profit-oriented evolution strategy, and promotion of proprietary software

We hereby propose the technology that is set to meet all these requirements: **Ultranet**, the next step in the evolution of the Internet. The following are the major components of Ultranet technology:

RDN Resource Delivery Network – provides free and decentralized storing and distribution of applications and any other resources, implemented as p2p distributed file system simialar to IPFS and BitTirrent protocols.

DMS Distribution Management System – a decentralized permission-less cryptography-based registry and MBV consensus protocol (DLT technology) that are used to manage product distribution. It allows publishers to register globally unique author names (similar to Web domains) and publish product releases under them.

AMPP Anti-malware Protection Protocol – a protocol and special DMS functions that serve to minimize the impact of malicious activity on the Ultranet ecosystem. Its primary purpose is to perform independent anti-malware verification of application releases and publish reports for all users in a trustworthy manner.

UOS Unified Operation Superstructure – a platform-independent local system layer that provides a safe execution environment with a unified UI and exposes a standard API for uApp applications.

uApp UOS Applications – a new class of platform-independent non-Web-based Internet applications that are distributed via RDN and DMS, run under UOS, and must comply with the uApp Open Standard, whose specifications cover API, building, packaging, and distibution of UOS applications.

UMI Unified Morphable Interface – a concept of a unified UI for uApp applications that is able to adapt a platform-independent virtual user environment to desktop, mobile, and VR devices, and to leverage the full power of local hardware. All implementations must strictly comply with a special technical standard to guarantee the same look and feel across all platforms.

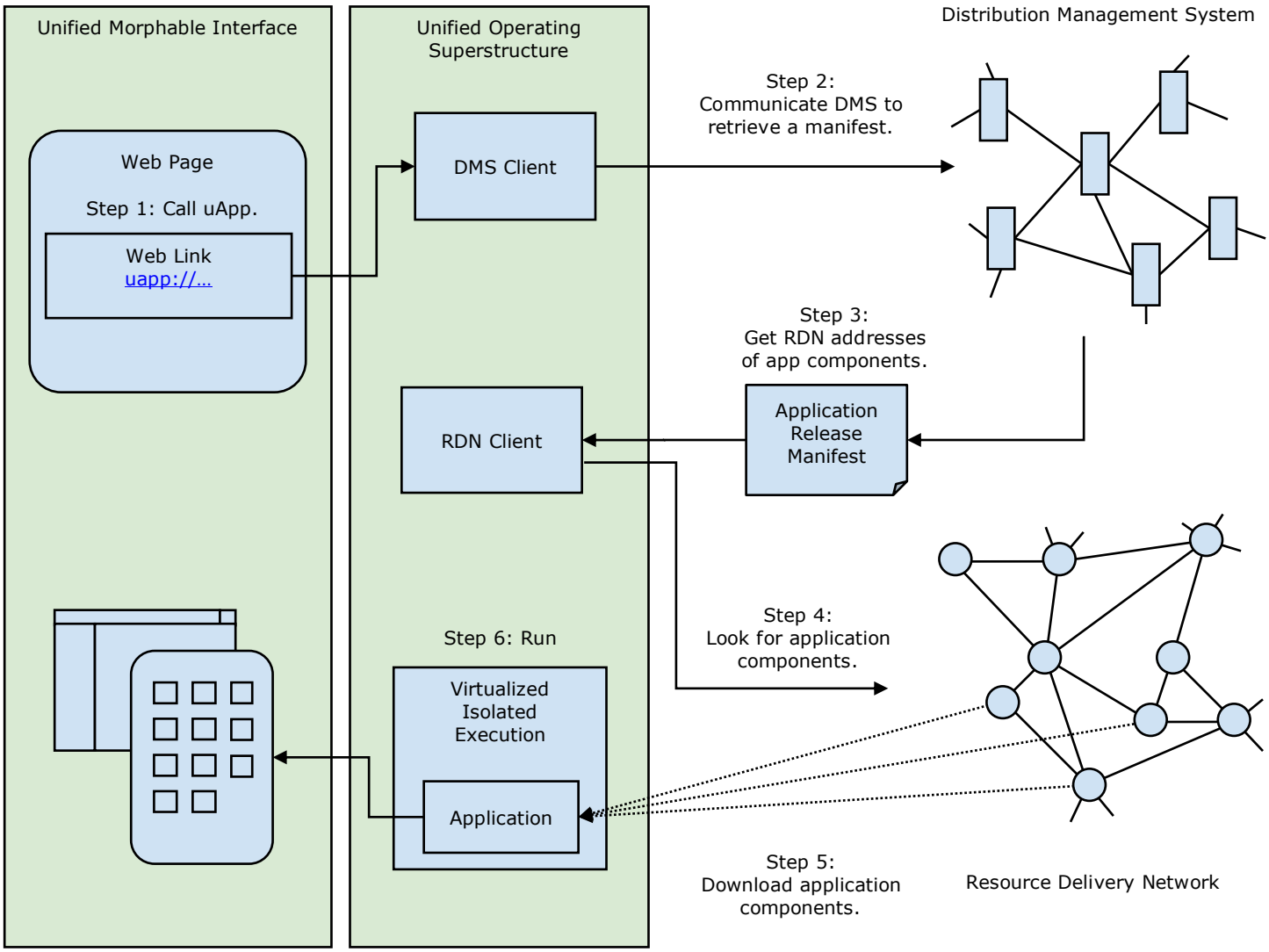
Resource Delivery Network

RDN allows participation in the storing and distribution of any data resources and is implemented using Distributed Hash Table (DHT) technology similar to IPFS and BitTorrent. Anyone can publish files there, and anyone can download and seed them. An RDN address is not the same as a webpage URL – it strictly identifies a particular file and so cannot point to dynamic content. It is therefore guaranteed that the user always get exactly what s/he requests. The technology is completely peer-to-peer and highly censorship- and DDOS-resistant. Not only standalone applications can be distributed in the RDN, but any kind of resources, such as shared components or assets

When the user requests to run a uApp via web link, the system performs the following steps:

1. If the link protocol identifier is "uapp://", then UOS connects to a random DMS node to obtain the corresponding uApp manifest.
2. Depending on request parameters, DMS node may return a manifest of the latest or a specific release.
3. The system reads the manifest and shows a visual stub in the UI environment with notification of the download's progress.
   Simultaneously, the system reads identifiers of core and dependency components from the manifest and sends corresponding requests to the RDN, looking for peers to download packages from. Anti-malware approval reports are sent as a header before downloading package content itself (explained in the next section).
4. Once the application download is complete, its integrity and high approval level are either confirmed or manually overridden by the user. It then runs in default configuration in a virtualized and isolated execution environment.

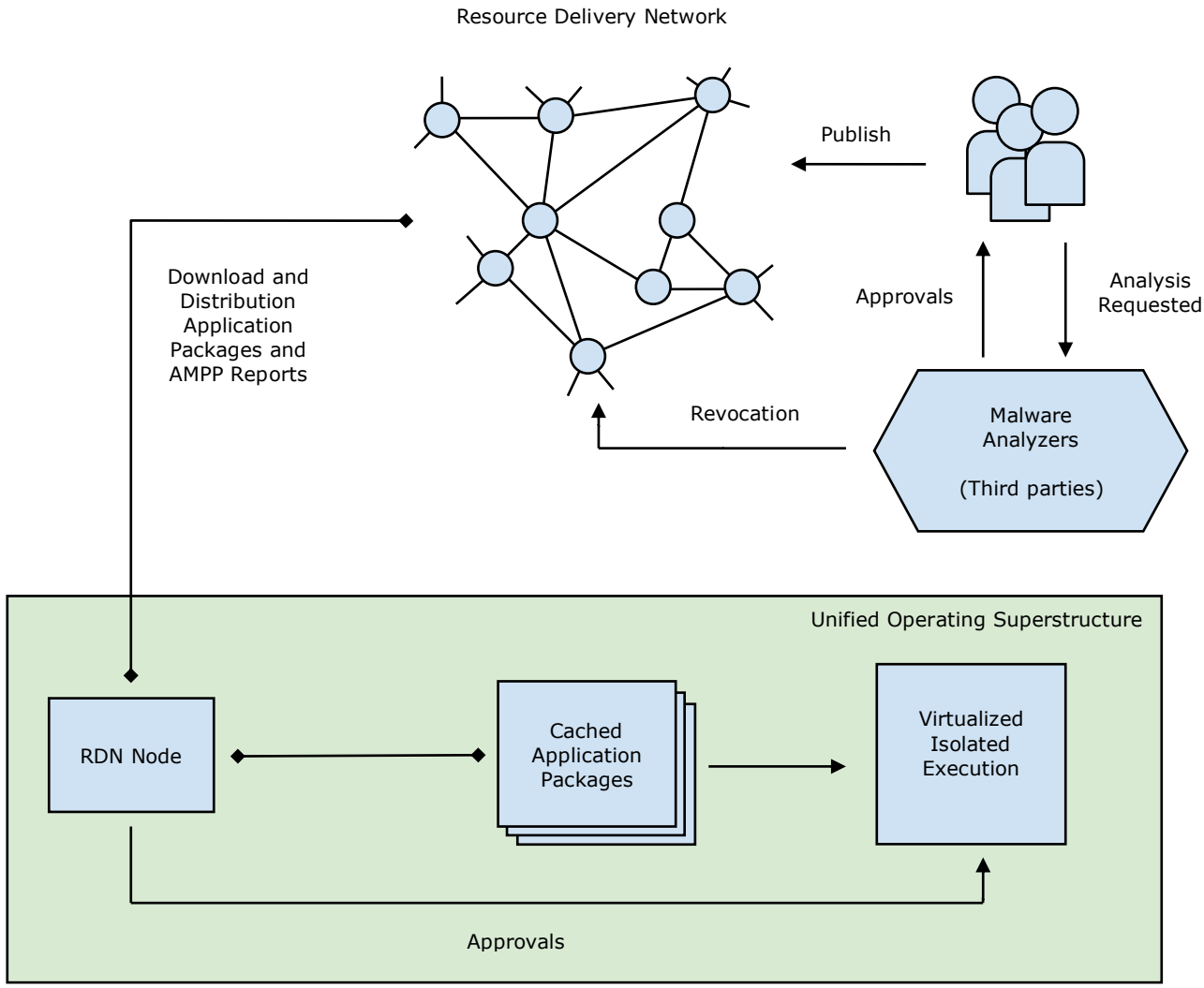
Figure 1. Decentralized Publishing, Distribution and Delivery



Anti-Malware Protection

The Anti-Malware Protection function carries out a fast check of just-requested applications for malicious code. It uses the RDN to store malicious analysis reports and adds to its protocol a real-time signaling for the rapid broadcasting of recently identified treats. Independent third parties perform malware analysis by a publisher request. Since Ultranet is a permissionless network, anyone can generate such reports, but users don't need to check all of them. Using a list(s) of well-known and trusted Malware Analyzers (MAs), the anti-malware subsystem of the UOS checks verification reports of these entities only, ignoring the rest. The list of trusted anti-malware analyzers may vary depending on particular requirements. Ultranet Organization always provides the default list of certified analyzers.

Figure 2. Anti-malware Protection



Providing of approvals increases the level of trust for a particular application. The more records are issued for a particular application by trusted MAs, the higher overall trust level the application gains. If no approvals are provided, an unknown trust level is set. This, in turn, means there is no pre-verification performed and it is completely up to the user whether to allow an application to run or not.

In order to gain approval, the publisher requests an MA to check an application release for malicious code. The publisher pays some amount of money to analyzers for that service. If nothing suspicious is found, then the MA issues an approval report and send it back to the publisher. Anti-malware Analysis Wholesalers help to obtain approvals from many analyzers with a single request so that the publishers don't need to deal with each analyzer company individually.

If the previously approved application is later found to be malicious, then the MA can issue an approval revocation record. This type of record revokes previously issued approvals for this application, and immediate broadcasting is initiated to let other nodes know about that change.

In the future, due to the expected progress in AI, this network may transform into some kind of distributed AI, which would collect and process analytics data from all network nodes and produce ratings that in turn could be used to estimate the safety of published products.

Time-to-Interact Optimizations

There is no longer an installation process – an application is started once all the required components are downloaded. To speed up the loading of the uApp applications, its architecture should be designed to consist of three levels of components:

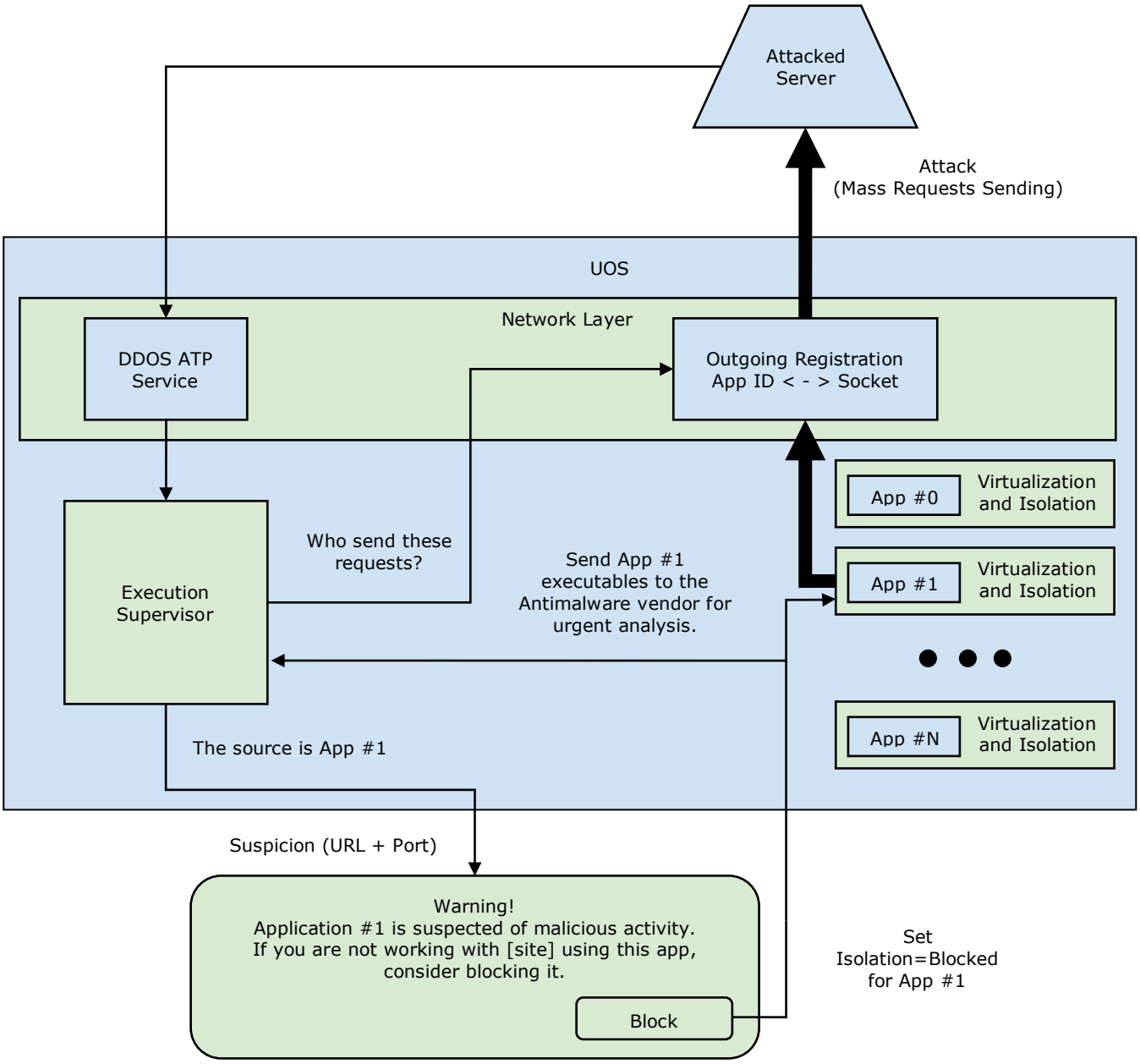
Core When the application is initially requested, only the core components are downloaded, and the default configuration is used to launch the application.

Deferred After the application is started, the deferred loading components are downloaded in the background.

Optional Finally, when the user needs some additional features, s/he can ask the system to download corresponding components manually.

The UOS provides the functionality to actively react when a local system is infected and participates in a DDOS attack. This process requires a victim side to support this mechanism.

Figure 3. DDOS Active Termination Protocol



In the case of a DDOS, the attacked server analyzes incoming traffic and sends a special signal (SUSPICION) back to each node that is sending too many requests. On the local side, the UOS stores application-to-destination mapping information and can use it to identify the suspicious application, warn the user about its malicious activity, and then block it if needed.

Once the UOS identifies an infected application, it then sends it to the MAs for urgent analysis. Anti-malware companies then identify malicious code signatures and add rejection records to the DMS database, or revoke approvals if they were issued previously.

With this technology, an attacked server has a weapon to not only to stop a DDOS attack but to shut down a whole botnet permanently.

Additional Benefits

Below are some of the additional benefits that come with Ultranet:

Economy

- It is completely free to use for all users.
- Publishers have to pay only a small fee for publishing and verification.
- The verification stage is optional but significantly increases trust in published software.
- It creates a big, new market for antivirus companies.

Freedom

- It is not possible to ban a particular publisher or application as it does not rely on a specific DNS record or IP address.
- Even publishers have no power to restrict users from using older versions if users are not satisfied with the latest ones.
- Utilizing various dApp platforms as the application server-side (back-end) and Ultranet as the application client-side (front-end) gives rise to an ecosystem that is invulnerable to DDOS attacks. Moreover, Ultranet proposes a special protocol that is capable of actively shutting down any botnet that participates in such types of attack.
- DMS cryptography replaces the need for code-signing certificates.

Performance

- The infrastructure does not require a high-performance BFT protocol -, as even existing solutions are already powerful enough for all Ultranet functions.
- Global unique identifiers of shared products ensure that downloading the same files more than once is avoided , thus minimizing TTI and Internet traffic in general.
- Users no longer need to have locally installed antivirus sacrificing the performance of their hardware.

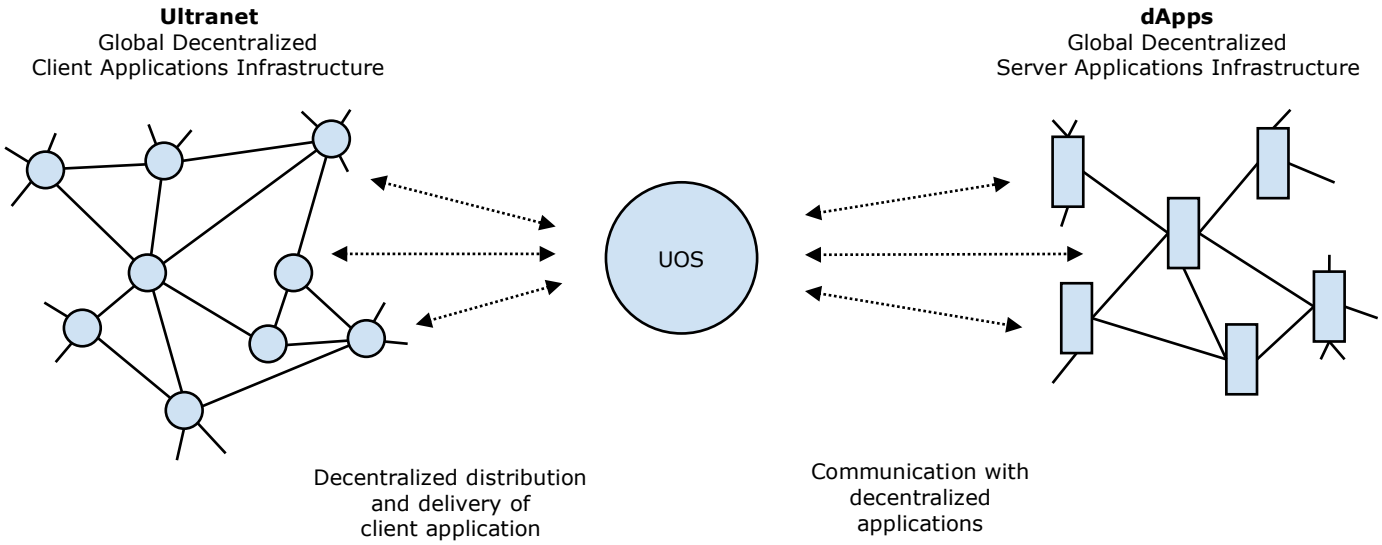
Opportunities

- Various decentralized software stores can be built on top of Ultranet.
- The technology provides a unified mechanism for updating applications so that no special development efforts are required to support auto-updating.
- UOS has the potential to create applications that work on various currently binary incompatible Linux distributions, which would give a new lease of life to the open-source community.
- RDN + DMS = Global Software Registry as a unified replacement for various package/component/library databases – not just for a code.
- Utilizing antimalware companies' specialized infrastructure makes it possible to perform a much deeper (AI) and more comprehensive analysis of application code.
- Together with distributed file systems (cloud, Chia, Sia, Swarm, Storj, etc.), the technology enables server-less thin clients. In this case, both the applications and user data are stored remotely in a decentralized manner. Once a user is authorized in such a system and their profile is loaded, all the required applications and related data are downloaded to a local device for follow-up.

Conclusion

Together with decentralized application platforms (dApps), which would act as a distributed database (server-side), Ultranet revolutionizes the way in which the Internet works: There would no longer be any vulnerable centralized points of denial, such as Web or database servers.

Figure 1. Complete Decentralization



This results in the impossibility of DDOS attacks and censorship, as none of the components rely on IP addresses or DNS records, and so there are no physical targets to attack or block. The scaling is also not an issue for this infrastructure, because RDN, which is built on top of IPFS technology, works in a similar way to the Torrent networks, which in turn can handle load at any scale by design. As for server applications infrastructure, some existing blockchain-based platforms have already shown their potential to bear heavy loads, and there is a strong expectation of major progress in this area in the very near future.

Ultranet is designed to revolutionize and disrupt vulnerable server-centric Internet architecture by decentralizing and improving the way in which applications and services are deployed and delivered to users. By combining and utilizing the most advanced network technologies available, Ultranet is shaping the next era of the Internet.