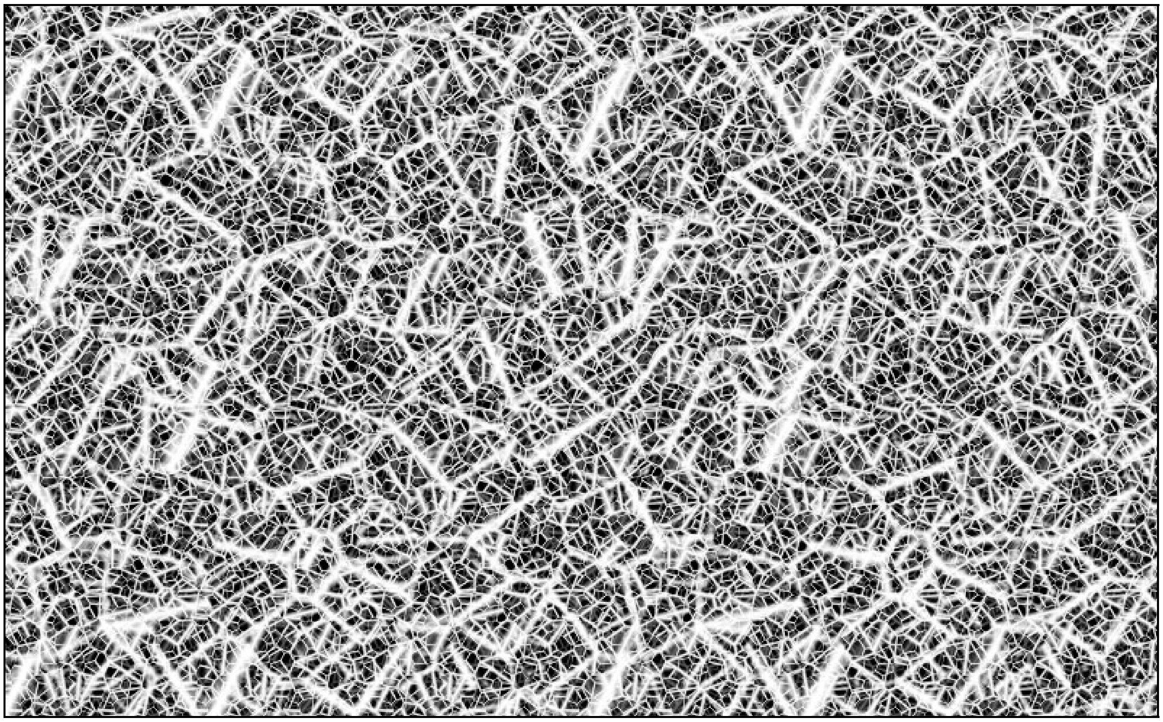
QUANTUMGATE

NEXT GENERATION PEER-TO-PEER NETWORK

V 1.0

By Karel Donk
http://www.miraesoft.com/karel
karel@miraesoft.com
Phone: +597 - 8593120



THE QUANTUMNETWORK
An infinite network of interconnected QuantumGate nodes.

INTRODUCTION

PEER-TO-PEER NETWORKS

A peer-to-peer (or P2P) computer network is a network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. P2P networks are typically used for connecting nodes via largely ad hoc connections. Such networks are useful for many purposes. Sharing content files (see file sharing) containing audio, video, data or anything in digital format is very common, and realtime data, such as telephony traffic, is also passed using P2P technology.

A pure peer-to-peer network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually to and from a central server. A typical example for a non peer-to-peer file transfer is an FTP server where the client and server programs are quite distinct, and the clients initiate the download/uploads and the servers react to and satisfy these requests.

Today there are many peer to peer networks that exist on the Internet. Right now the most popular one is BitTorrent with its many different clients (QTorrent, BitComet etc.). Then there's also the Gnutella network, also with many possible clients that connect to that network, one of which is LimeWire.
All of these peer to peer applications and protocols have their strengths and weaknesses, advantages and disadvantages.

QUANTUMGATE

This is where QuantumGate comes in. The goal with QuantumGate is to create a P2P network based on a P2P protocol that eliminates many of the most important disadvantages and issues that the other P2P protocols have, while introducing a unique new architecture with next generation features and capabilities.

The name "QuantumGate" was chosen because of the nature of the basic piece of software, or kernel, that will power the network. This software will find its way onto many different devices in the future, not just personal computers (PCs), but also entertainment devices such as Xbox, Playstation and mediacenters. Basically any device that's connected to the Internet, and can in some way benefit from the functionality that QuantumGate offers.
The software will function as a gateway that connects a device to many other devices on a large and infinite network. This gateway is the elementary entity in this large network, hence the name QuantumGate.

This basic piece of software will be provided free of charge and will be available for download. Manufacturers of devices will be able to distribute QuantumGate on their device free of charge as well.

The functionality and the services on the QuantumNetwork can be extended by developing QuantumGate Extenders. These are software components that run on top of QuantumGate, and provide additional services on the network, such as filesharing or distributed computing. Manufacturers will be able to build their own extenders to provide their own services on the QuantumNetwork, and will also be able to make use of existing services and resources on the QuantumNetwork in their own products.

Although the basic QuantumGate software is free, developers of extenders may charge for usage of the services their extenders provide.

If we view the Internet as a large network of connected devices, many of these devices are not being used optimally or efficiently. For example, most devices, such as PC's, are connected almost 24 hours a day to the Internet while remaining idle most of the time. They also contain hard disks with gigabytes of unused storage, and use a small amount of the available Internet bandwidth.
QuantumGate will enable us to use all these unused resources by making them available to everyone on the QuantumNetwork. When a user installs QuantumGate on their device, they allocate a specific amount of the resources on that device to QuantumGate. These resources can include CPU processing power and storage. QuantumGate then combines all the resources on these devices and makes them available on the QuantumNetwork for everyone to use. It's easy to see that QuantumGate won't simply be another P2P network, but will become a platform for distributed computing in the future. A platform for the people, by the people, with equal rights and control for everyone.

Quantum Distributed File System

Along with QuantumGate, a QuantumGate Extender will be developed which will provide distributed filesystem services on the QuantumNetwork. This extender will be called QuantumDFS and will also function as a proof of concept for a QuantumGate Extender. Essentially this extender will provide filesharing and storage capabilities, both publicly and privately, on the QuantumNetwork.

Users will be able to store and share files and information publicly on the QuantumNetwork through QuantumDFS. While doing this, they will also benefit from all the functionality QuantumGate offers, such as security, anonymity and no single point of failure or censorship.
Content providers will also be able to publicly share large files on the QuantumNetwork, similar to BitTorrent, making use of the large amounts of shared resources available on

the network, while keeping the need for their own bandwidth and storage requirements to a minimum.

Users will also be able to privately store their files on the QuantumNetwork. This will be similar to the services Microsoft and Google want to provide in the near future, namely LiveDrive and GDrive, except for the fact that they will be investing in their own large datacenters to provide online storage to users, while QuantumDFS will simply use existing shared resources on the QuantumNetwork. Any files that a user stores privately on the QuantumNetwork will only be accessible to that user.
Similarly, content providers can also store their own files and information privately on the QuantumNetwork, and make it available only to paying customers.

It's easy to imagine how much money content providers can save because of not having to invest in large amounts of storage and bandwidth requirements.

TECHNICAL ASPECTS

ARCHITECTURE

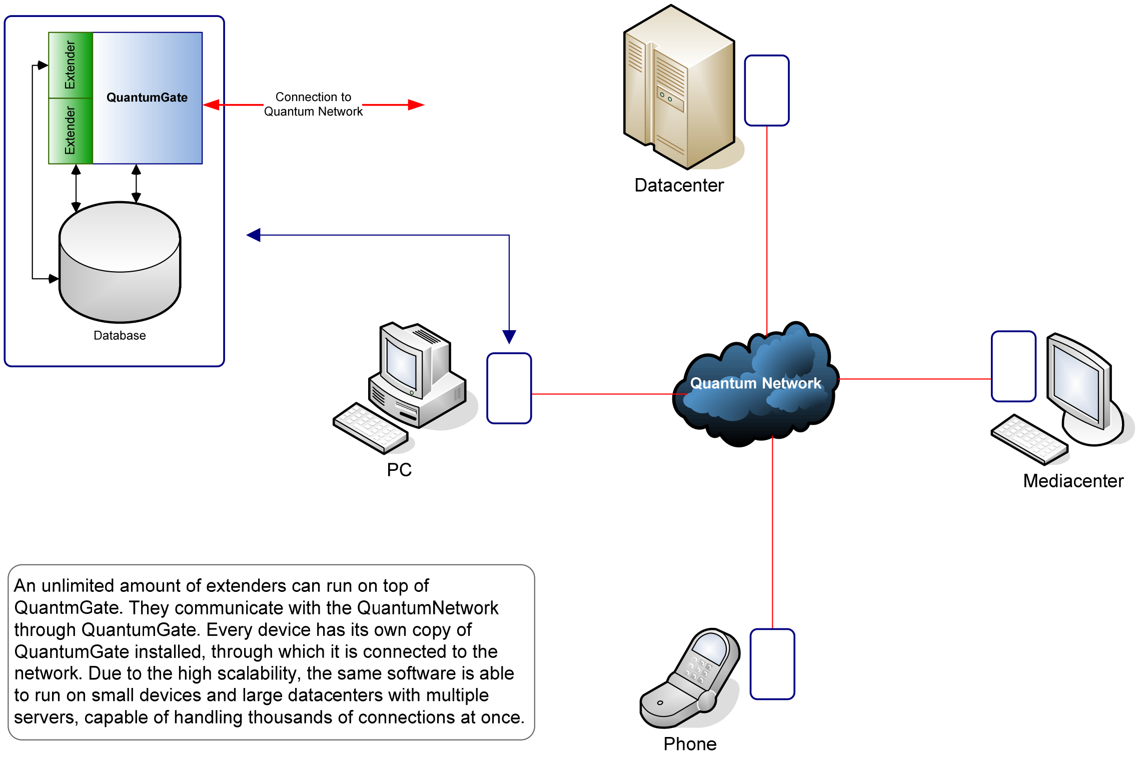
QuantumGate will always be active and running on the background on a device, communicating with the network and performing various tasks the user, or software that makes use of its features, have instructed it to do. It will ofcourse be possible to turn off QuantumGate if needed, and disconnect from the network. However, as a result, software and services on the device that depend on QuantumGate may not work or will only work partially.
The idea however is to have QuantumGate always running in the background and connected to the network. The reason for this will become more apparent in other sections of this document.

QuantumGate will consist of the following main components:

- **The kernel or QuantumGate.** This is the basic piece of software that performs low level operations like connecting to the network and handling communications based on the QuantumGate protocol. Other tasks include finding peers on the network, maintaining a list of peers and routing messages on the network. This is essentially the gateway to the Quantum Network.

- **QuantumGate Extenders.** These are software components that will run on top of the kernel and will provide various services and functionality on the network. An example of this is filesharing. It will be possible for developers to create their own unique services that run on the QuantumGate network and make use of the many possibilities the network offers.
  Not all extenders have to be installed on a particular device. Users and manufacturers can decide for themselves what extenders they want to install on their device based on the services they want to use.

- **The database.** The database will run separate from the kernel and will be a third party database. It will be used to store any data the kernel needs to maintain, such as peer information, and also any data the Extenders need to maintain.



An unlimited amount of extenders can run on top of QuantmGate. They communicate with the QuantumNetwork through QuantumGate. Every device has its own copy of QuantumGate installed, through which it is connected to the network. Due to the high scalability, the same software is able to run on small devices and large datacenters with multiple servers, capable of handling thousands of connections at once.

Communication

Compression

All communications on the QuantumNetwork will be compressed in order to use as little bandwidth as possible.

Encryption

All communications on the QuantumNetwork will be encrypted using the best and most advanced encryption algorithm possible after compression. Right now AES (Advanced Encryption Standard) and 2048-bit RSA are likely candidates. QuantumGate will use a combination of those two encryption algorithms. For every unique connection, there will be a unique encryption key that will be used as soon as the connection is established. If the connection breaks, a new key will be used upon reconnection. If a message travels through various nodes before it reaches its destination, it will be encrypted using a different key by every node it passes. This, among other things, will make it impossible to track a message on the network.

Routing

Whenever possible, QuantumGate will also route messages through a variable number of other nodes before reaching its destination. This is to ensure that it will be very difficult to determine the original source and the destination of information. Nodes will be passing along messages on the network without knowing exactly where it came from, and without knowing where its final destination is. As a result, it will not be possible to determine the original publisher of information, and it will not be possible to know exactly what a particular node is doing on the network, since it's possible that it could merely be routing messages from other nodes.

Apart from security, all of this will ensure true anonymity and privacy on the QuantumNetwork.

ROUTING GATEWAYS

QuantumGate not only functions as a gateway to the QuantumNetwork for the device it is running on, but it also functions as a gateway for other nodes on the QuantumNetwork through which they can route messages and communicate with other nodes on the network.

It will be possible to set up dedicated gateways as well. These are servers running QuantumGate without any extenders, which do nothing but route messages from one node to another.

CACHING GATEWAYS

On every device a certain amount of storage is used by QuantumGate to maintain a local cache. A certain amount of data that passes through a node is cached locally on the device that node is running on. If certain data is requested often, it will be more likely to be cached.

It will also be possible to set up dedicated caching gateways. A problem ISPs (Internet Service Providers) face today is the high bandwidth usage for users on their network that run filesharing and other P2P applications. QuantumGate will solve this problem to a great extent through caching gateways. These are gateways configured in a special way that an ISP can install on their own servers that will keep the most popular and most requested traffic in their cache. All users that connect to the Internet through that ISP will most likely get their data "locally" from the cache on that ISP's QuantumGate server if it exists there, saving the ISP external bandwidth. The performance for the users who can get data directly from the ISP's cache will also be **much better**.

Imagine, for example, a popular file that is being shared on the QuantumNetwork. Many users at a specific ISP want to download this file. If the ISP has a caching gateway installed, the file can be cached on that gateway on the first request, and all subsequent requests from other nodes can be served from the ISP's cache, saving the ISP loads of external bandwidth and costs. It is also highly efficient because network resources are saved for other use. This can also be used for streaming content, such as broadband television, which will become more mainstream in the future.

GOALS

As mentioned before, QuantumGate will solve some of the issues other P2P protocols have, and will introduce unique new features and capabilities. In this section we'll look at some of them.

Scalability

From the ground up, QuantumGate is designed and will be built with scalability in mind. The QuantumNetwork is an infinitely large network, and this means that the system will have to be able handle the growth of the network seamlessly.
The exact same software will run on any device, from a mediacenter or gaming console to a more powerful PC to an entire datacenter capable of handling thousands of connections at once.
Because QuantumGate is built up out of 3 main components, each of these components can be scaled up in hardware or software as required. For example, if QuantumGate should be able to handle more connections at once, the kernel software can be placed on a cluster of servers which are able to handle the load. The database can be placed on its own cluster of servers which are dedicated to the database functionality. Each of the QuantumGate Extenders can run on their own server or cluster of servers if needed. But all of them can run on a single PC for home use without any modifications as well.
So it is easy to imagine an organization that uses QuantumGate to provide its own services on the QuantumNetwork, starting out with a single server, and seamlessly scaling up as their userbase grows.

Extendibility

QuantumGate will be designed with many possibilities for extendibility. These possibilities can then be used by developers to create their own services on top of QuantumGate, or to extend existing services. One such possibility is the creation of a QuantumGate Extender to provide instant messaging capabilities over the QuantumNetwork. Another possibility is a QuantumGate Extender that provides a World Wide Web service within the QuantumNetwork itself. One of the immediate advantages providers get when they build their services on top of QuantumGate, is access to the wealth of resources available on the QuantumNetwork, that will allow them to simplify their operations, and lower costs. In essence, the QuantumNetwork will be the biggest supercomputer at the disposal of everyone on the planet.
One can come up with all kinds of wild ideas for QuantumGate Extenders and additional services you can provide on such a network. The only limit seems to be one's creativity and imagination. Indeed, the network could allow building our very own Skynet (http://en.wikipedia.org/wiki/Skynet) in the future. ;)

SECURITY AND PRIVACY

From the ground up, QuantumGate will be built with high levels of security and privacy in mind. All data stored on the device QuantumGate is running on, will be encrypted. All communications on the QuantumNetwork will also be encrypted with the most powerful encryption methods available. Encryption between two unique nodes on the QuantumNetwork will be done using a unique key. As a result it will be impossible for people to see what someone is doing on the QuantumNetwork, and wiretaps will be pointless.

It will be possible for users to store their encryption keys on media that is separate from the device QuantumGate is running on. For example, a user may choose to have their encryption key saved on a USB memorystick, and will have to insert the memorystick into his PC and provide the key when QuantumGate loads. When someone else breaks into his PC, it will be impossible to extract the data stored on the PC by QuantumGate. It will also be impossible to trace what the user was doing on the QuantumNetwork based on the data stored on his PC.

ANONYMITY

QuantumGate will provide all users on the QuantumNetwork with true anonymity. Apart from the powerful security and encryption mentioned earlier, QuantumGate will route messages between nodes through a variable number of other nodes, making it impossible to trace who the real sender and receiver of a message are. It will also be impossible, if required, to trace the publisher of specific information on the QuantumNetwork because of anonymity.

RESOURCE POOLING AND EFFICIENCY

Computers become more powerful every day, not just with regards to raw CPU processing power, but also with regards to the available resources such as RAM, storage and bandwidth. Much of this power and resources is never used by the typical home user. There are gigabytes of storage that are never being used on a computer, and computers that are on but mostly just running idle with an email client and a web browser running on them. Furthermore, these computers are often connected to the Internet with increasingly higher speeds and bandwidth allocation, of which only a small fraction is used. Combine all these resources of all the computers on earth together, and you get a very large amount of resources at your disposal, that far exceeds the biggest datacenters around.

That is also one of the goals for QuantumGate, to enable us to combine these unused resources into what will effectively become a global computersystem or datacenter, and put them to good use for the benefit of all. Not only will it give us access to these unused resources, but it will also allow us to use them efficiently.

All the services running on top of QuantumGate by way of a QuantumGate Extender will get these resources essentially for free. Ofcourse, the providers of these services will have to get users to want to install the extenders on their own computersystems before they can make use of (all) the resources on those computersystems. In any case this should be more attractive to providers since investments into setting up their own large datacenters, like Google and Microsoft are doing now, won't be necessary. With every new user joining the network, the network scales upwards with the resources those users make available to the network. But as mentioned before, should providers have a need to have their own servers to provide or coordinate content distribution, that will also be possible.

No single point of Failure

There will be no single point of failure on the QuantumNetwork. Nodes can join in and leave at any time without any significant impact on the network itself. Due to the very distributed nature of the network, it will also be impossible to have a single point of attack to bring the network, or certain services on the network down. Today many popular P2P systems have to deal with this issue. BitTorrent for example, has a single point of attack: the tracker. People can target the tracker and deny all users access to the content being shared through that tracker. Kazaa for example, has central coordinating servers, which can be targeted physically or legally to impact the network and the users on that network.
These kinds of attacks will not be possible on the QuantumNetwork, since it would mean having to target every single node and user on the network in order to stop certain activities taking place on the network.

No Censorship

For many of the reasons described earlier, it will be impossible for people, organizations and governments to censor data or information on the QuantumNetwork. First of all, it will be impossible to see who is doing what on the network. Wiretaps will be pointless as well since all communications are encrypted. There will be no means of taking down content on the network, or denying access to content, unless the provider of the content himself chooses to do so (in many cases, and depending on the way the service the provider uses is designed, it might not even be possible for the provider himself to remove content on the network). There will also be no single point of attack possible. Once content has been distributed on the network, it will be impossible to find out (every instance of) where it is stored, when it is being downloaded and by whom.
This will help ensure freedom of speech and availability of information to everyone. We see today that increasingly, big corporations and governments are trying to get more and more control over the Internet, and the content people are allowed to access. This is a serious problem, and the QuantumNetwork will address this threat in the future. Today we have Google providing easy access to information on the Internet, but even they are vulnerable to governments around the world, as shown recently with China (censorship), and with the USA (providing user's search data to government for

investigation – privacy issues). With QuantumGate, it will be possible to build a Google like service on the QuantumNetwork that will not be vulnerable to outside influences.