# Quantum1Net
Distributed Private Network:
Explained

The Internet of Everything

Internet includes Billions of computers, people, servers, devices, and objects that are interconnected and combined into one giant network globally without a single center, the Internet of Everything "IoE". This massive web is a universal network of networks that exists physically, in the form of wires, links, and connections joining all the devices, objects, people, and computers in a global network system thought of as the World Wide Web.
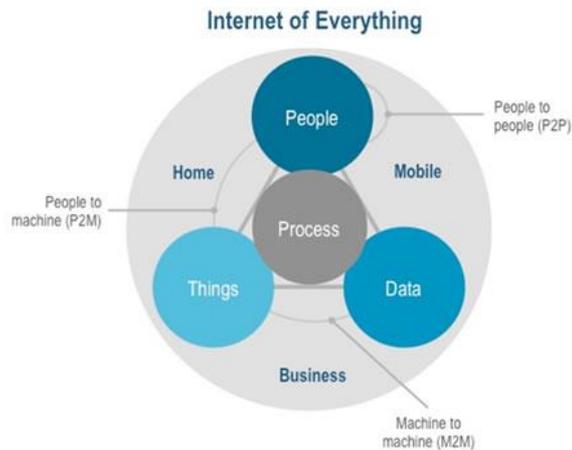
The Distributed Private Network: Description

The Distributed Private Network (" DPN") is a number of nodes within a network that are not defined by the physical network topology but by a temporary (virtual) overlay to the network. The idea of the DPN is that it is not rigid or fixed but only exists dynamically, "on demand" precisely for a given user and lives only for as long as that connection is needed.

The distributed private network "DPN" uses a network entirely in a new way to make dynamic unique one-time connections ("OTC") for each connection request, which only exist for as long as a user requires it. Each OTC can be encrypted using unique encryption credentials that are never reused. When the OTC is closed, it literally dissolves without a trace of having existed.

The Quantum1Net "Q1N DPN" Explained

All people, computers, devices, or objects currently within the IOE may also be connected via Q1N DPN One Time Connections. Such connections are both - dynamic and transient, existing only for the time the data transfer is active. By design, the Q1N DPN OTC is invisible to all other participants on the Internet and Quantum encrypted making it impossible to either intercept or read the data being transmitted within it.

The Q1N DPN enables any nodes, such as servers and clients, within the IOE to be uniquely and securely connected over the entire existing network infrastructure.

Your Communications are Secured by Quantum

Security is the intrinsic part of the Q1N DPN, ensuring secure data transfer for all communicating parties. All Q1N Coin Holders will be able to buy access to, and utilize the unique Q1N DPN security and infrastructure.

Use cases:

1. No one would have access to your data: all data is transmitted directly between sender and receiver and is only stored on your local devices or your local data center.
2. When using the Q1N DPN to visit various sites or while using various programs installed on your computer, they will be unable to collect and send curtail marketing information about your Internet activity or browsing history.
3. The Q1N DPN enables you to take online privacy into your own hands and under your own control to protect your anonymity.
4. The Q1N DPN makes you invisible to Bots, Viruses, Trojans and hackers, which inhabit the Internet. They simply cannot attack you, when using the Q1N DPN because you do not "exist" for them. With Q1N DPN, you are safe when you connect to the Internet via an open Wi-Fi network in the airport, coffee shop or any other public place.
5. The Q1N DPN prevents attackers from gaining access to everything stored on your computer (e.g., important passwords, etc.)
6. The Q1N DPN ensures that any online session, such as communication with your banking site or money transfer is safe and secure.

None of these protections currently exist on the Internet at DPN level.

Privacy

Whenever you are connected to the Internet, you are assigned an IP address–a numerical combination that is essentially similar to a regular street address. With an IP address, you can be tracked down as easily as with a regular street address. You will be amazed how much one can learn about you; just visit this page: http://addgadgets.com/IPaddress/. Q1N DPN is designed to mask your IP address from the other client or server you are communicating with, by routing your data through DPN nodes and uniquely encrypting all content.

The Uniqueness of Q1N DPN:

- There are no centralized servers
- Dynamically allocated DPN nodes define the network topology
- All connections are End-to-end encrypted
- All payload data is Quantum Safe
- Exit points and DPN nodes can be random or chosen by geographic area or network performance
- No central point (node) of failing
- There are no logs kept anywhere in the system
- Nothing is ever saved on DPN nodes for longer than needed to relay chunk of data
- Uses port 80/443 (http/https) to negotiate a tunnel through any university/corporate Lan
- Uses port 80/443 (http/https) to negotiate a tunnel through country "firewalls"
- No ugly fine print in user agreement, no logs no data saved period!
- Works on restricted network