THE ETHEREUM NETWORK:

The Ethereum network is a peer-to-peer network where nodes participate in order to maintain the blockchain andcontribute to the consensus mechanism. Networks can be divided into three types, based on requirements and usage.

MainNet : MainNet is the current live network of ethereum. Thecurrent version of MainNet is homestead.

TestNet : TestNet is also called Ropsten and is the test network forthe Ethereum blockchain. This blockchain is used to test smart contracts and DApps before being deployed to theproduction live blockchain. Moreover, being a test network, it allows experimentation and research.

Private net(s):

As the name suggests, this is the private network that can be created by generating a new genesis block. This is usually the case in distributed ledger networks, wherea private group of entities start their own blockchain

Supporting protocols:

There are various supporting protocols that are in development in order to support the complete decentralized ecosystem. This includes whisper and Swarm protocol.

Whisper

Whisper provides decentralized peer-to-peer messaging capabilities to the ethereum network. In essence, whisper is a communication protocol that nodes use inorder to communicate with each other.

SWARM

Swarm is being developed as a distributed file storage platform. It is a decentralized, distributed, and peer-to-peer storage network. Files in this network are addressed by the hash of their content

APPLICATIONS DEVELOPED ON ETHEREUM:

There are various implementations of DAOs and smart contracts in Ethereum, most notably, *the DAO*, which was recently hacked and required a hard fork in order for funds to be recovered. The DAO was created to serve asa decentralized platform to collect and distribute investments.

Augur is another DAPP that has been implemented onEthereum, which is a decentralized prediction market. Various other decentralized applications are listed on http://dapps.ethercasts.com/.

SCALABILITY AND SECURITY ISSUES:

Scalability in any blockchain is a fundamental issue. Security is also of paramount importance. Issues such as privacy and confidentiality have caused some adaptability issues, especially in the financial sector. However, a great deal of research is being conducted in these areas. Even though various use cases and proof of concept systems have been developed and the technology works well for many of the scenarios, there still is a need to address some fundamental limitations that are present in blockchains in order to make this technology more adaptable.

At the top of the list of these issues comes scalability and then privacy. Both of these are important limitations to address, especially as blockchains are envisioned to be used in privacy-demanding industries too. There are specific requirements around confidentiality of transactions in finance, law and health, whereas scalability is generally a concern where blockchains do not meet the adequate performance levels expected by the users. These two issues are becoming inhibiting factors toward blockchain technology's wider acceptance.

Scalability:

This is the single most important problem that could mean the difference between wider adaptability of blockchains or limited private use only by consortiums. As a result of substantial research in this area, many solutions have been proposed from a theoretical perspective, the general approach toward tackling the scalability issue generally revolves around protocol-level enhancements. For example, a commonly mentioned solution to bitcoin scalability is to increase its block size. Other proposals include off-chain solutions that offload certain processing to off-chain networks, for example, off-chain state networks. Based on the solutions mentioned

above, generally, the proposals can be divided into two categories: on-chain solutions that are based on the idea ofchanging fundamental protocols on which the blockchain operates.

Privacy:

Privacy of transactions is a much desired property of blockchains. However, due to its very nature, especially in public blockchains, everything is transparent, thus inhibiting its usage in various industries where privacy is of paramount importance, such as finance, health, and many others. There are different proposals made to address the privacy issue and some progress has already been made. Several techniques, such as indistinguishability obfuscation, usage of homomorphic encryption, zero knowledge proofs, and ring signatures.

Security:

Even though blockchains are generally secure and make use of asymmetric and symmetric cryptography as required throughout the blockchain network, there still are few caveats that can result in compromising the securityof the blockchain.

There are a few examples of transaction malleability, eclipse attacks, and possibility of double spending in bitcoin that, in certain scenarios, have been shown to work by various researchers.