Q 1:
What is the Lightning Network?

A:
The Lightning Network is currently under development. It will become a decentralized network that enables instant off-chain transfer of the ownership bitcoin, without the need of a trusted third party.
The system utilizes bidirectional payment channels that consist of multi-signature addresses.
One on-chain transaction is needed to open a channel and another on-chain transaction can close the channel.
Once a channel is open, value can be transferred instantly between counterparts, who are exchanging normal bitcoin transactions, but without broadcasting them to the bitcoin network.
New transactions will replace previous transactions and the counterparts will store everything locally as long as the channel stays open.

Q 2:
Is the Lightning Network open source?

A:
Yes, Lightning is open source. Anyone can review the code, just in the same way as the bitcoin code.

Q 3:
Who owns and controls the Lightning Network?

A:
Similar to the bitcoin network, no one will ever own or control the a Lightning Network.
The code is open source and free for anyone to download and review.
Anyone can run a node and be part of the network.

Q 4:
Who is the inventors of the Lightning Network?

A:
Joseph Poon and Thaddeus Dryja wrote The Lightning white paper.
Lightning is an open source project so anyone is free to contribute with code.
There are currently 5 independent implementations under development:

Blockstream's C lightning:
Blockstream currently have two employees who are dedicated to Lightning development.

Blockchain’s Thunder network

ACINQ have successfully implemented Bitfury's Flare routing algorithm into Eclair, and tested it on a live network of 2500 servers

Amiko Pay

KimDotCom's BitCache lightning network (confirmation needed, I’m not sure about this one)

Q 5:

Does the Lightning Network have its own “Lightning coins”?

A:
No, that’s not how it works.
A Lightning Network will be using real bitcoin transactions with actual bitcoins in them

Q 6:
Is the Lightning Network dependent on consensus to be implemented?

A:
No, a Lightning Network builds an additional layer on top of the bitcoin network.
Therefore it is not dependent on consensus in the bitcoin network itself.

Q 7:
Will there be any form of custodian risk in a Lightning Network?
Do I need to trust anyone to hold my money on my behalf?

A:
No, this system is not based on trust; you remain in full control of your money.
If anything goes wrong you simply broadcast the latest state of your channel as a normal on-chain bitcoin transaction.
All your money will be returned to your address, and it will be recorded on the blockchain as a normal on-chain bitcoin transaction.

Q 8:
I’ve heard that Lightning transactions is happening “off-chain”...Does that mean that my bitcoins will be removed from the blockchain?

A:
No, your coins will never leave the blockchain.
Instead your coins will be held in a multi-signature address as long as your channel stays open.
“Off-chain” is not a perfect term, but it is used due to the fact that the transfer of ownership is no longer reflected on the blockchain.

Q 9:
I’ve heard that the Lightning Network will require my bitcoins to be locked up...
You do realize that no one wants to lock up their bitcoins?

A:
If your interpretation is that Lightning will make your money less accessible, then you are clearly misinformed.
The fact is that your money will actually become more accessible when held in a Lightning channel.
First of all, you do not need to wait for conformations in a Lightning Network, your money can be moved almost instantly within this network.
Second, bringing your money “back on chain” is just as easy as sending a normal bitcoin transaction. You just wait for the first confirmation and your money is no longer “off chain”
The only exception is the rare case that your channel breaks down in the middle of a transaction (counterpart goes offline)

In this exceptional case; you will be subjected to a short time delay before you can spend your money. The length of this delay will vary, depending upon the parameters you have applied to your channel.

Q 10:
Will a Lightning Network have its own blockchain?

A:
No, Lightning is dependent on the bitcoin blockchain. On-chain bitcoin transactions are needed to open and to close “channels” between peers (nodes) in the network.
Once a channel is open, the ownership of bitcoin can be transferred off-chain in both directions.
The transactions inside a channel are real bitcoin transactions, but they are not broadcasted to the bitcoin network as long as the channel stays open.
Instead those involved in a channel will store the transactions locally.
This enables instant transactions and a near unlimited capacity within a Lightning Network.

Q 11:
Will there be any form of mining to secure the Lightning Network?

A:
No, security is provided by the bitcoin miners in the underlying bitcoin network

Q 12:
The main chain of bitcoin is secured by a hash rate of 2 ExaHash/s, but a Lightning Network doesn't have any hash rate at all...
So how can a Lightning Network be as secure as the main chain?

A:
The security in a Lightning Network is extracted from the underlying Bitcoin Network.
A Lightning Network can not operate on its own, it is completely dependent on the underlaying bitcoin network for security.

Basically the bitcoin network takes the role as a safety net underneath the Lightning Network. If something goes wrong in a Lightning channel (like your counterpart going offline) you will always have the option to fall back into the safety-net.
(You simply broadcast the latest state of your channel as a normal on-chain bitcoin transaction)

Q 13:
Does a Lightning Network have its own public ledger or some sort of database of all transactions?

A:
No, a Lightning Network does not have its own ledger and there is no database.
Holding value on a Lightning Network means that you are in possession of double-signed transactions. The transactions are valid, but they are not yet broadcasted to the Bitcoin Network.
The transactions you are holding are of the 2 of 2 multi-signature type.
Both you and your counterpart will sign, and you will both store the transactions locally.

These transactions will use a multi-signature address as their input (the funding address) and they will point at two different addresses for their output.
One output is pointing to an address that only you can control, and the other output is pointing to an address that only your counterpart can control.

Q 14:
How can you say that the Lightning Network is using real bitcoin transactions?
You do realize that it's not a real bitcoin transaction if it's not recorded on the blockchain?

Short A:
To understand this we first need to understand what a bitcoin transaction really is…
The fact is; That there are no "coins" in Bitcoin…
There are only signed messages and updates to the blockchain.

So lets say that Alice is sending 1 bitcoin to Bob…
We call this a per-to-per transaction due to the fact that the ownership of value is transferred directly from Alice to Bob.
But Bob does not actually receive a "digital coin" from Alice.
The thing that in reality is happening; is that all the nodes in the network will update their local copy of the public ledger.
The public ledger is updated so that; the "coin" that was before registered in an address controlled by Alice, is now instead registered in an address controlled by Bob.

Long A:
The bitcoin transaction that Alice is sending to Bob, is in reality just a signed message that Alice is broadcasting to everybody.
The message is not only received by Bob, but it is broadcasted to all the nodes in the network.

At the time of writing there are more than 5400 so called "full nodes" in the bitcoin network.
The following steps illustrates the process that takes place when Alice is sending a bitcoin transaction to Bob:

1. When Alice is broadcasting her signed message (= bitcoin transaction), it will be picked up by some of the full nodes in the network.

2. These nodes will independently validate the message (transaction) in accordance with the consensus rules. If the nodes find the message to be valid; they will broadcast the message again so that it can be picked up by other nodes on the network.

3. Some other nodes on the network picks up the message, and this process continues until all 5400 nodes have independently validated and re-broadcasted the message (transaction)

4. At some point a miner will succeed in constructing a valid block that includes the message (transaction) from Alice. To make this happen the miner must bear the cost of an enormous amount of electricity.

5. The miner will now broadcast this newly found block. The new block will be picked up by some of the full nodes. The nodes will independently validate the block and all its content.
By doing this they are also validating the message (transaction) from Alice for a second time.

If the nodes find the block to be valid (in accordance with the consensus rules) they will broadcast the block again so that other nodes can also receive the block.

6. Other nodes will pick up the block, validate and broadcast.
This process continues until all the nodes in the network have independently validated the block and thereby also validated the message (transaction) from Alice for a second time.

The six steps above demonstrates that a normal bitcoin transaction from Alice to Bob actually involves everyone on the network.
The message is independently validated two times by 5400 nodes (= 10 800 validations)

Despite this we are still calling it a “per-to-per transaction” because the actual **ownership of value** is transferred directly from Alice to Bob*
(*But everyone still needs to help by updating their local copy of the ledger)

Conclusion:
A bitcoin transaction is just a signed message.

So lets say that Alice wants to send 1 bitcoin to Bob within a Lightning Channel.
Alice is storing some of her money in a “2 of 2” multi-signature address.
Alice and Bob will both sign a message that transfers the ownership of 1 bitcoin from Alice to Bob.
This message **is a valid bitcoin transaction**, but it is **not broadcasted to the bitcoin network**.

Instead Alice and Bob both store the transaction (message) locally.

From Bob’s point of view this “double-signed message” has a monetary value of 1 bitcoin.
The monetary value of 1 bitcoin comes from the fact that Bob can spend the money
on-chain at any time by simply **broadcasting the message to the bitcoin network**.

Bitcoin transaction = Signed message = Lightning transaction

The purpose of any monetary transaction is to change the ownership of value.
In the bitcoin network we change the ownership of value by the use of **signed messages**

A Lightning transaction is a **double-signed message,**
therefore a Lightning transaction is a real bitcoin transaction

Q 15:
I have heard that there will be some fees involved in the Lightning Network..
Who will be collecting those fees?

A:
Potentially anyone who is running a Lightning-node.
Example:
Alice wants to send money to Carol, but Alice does not have an open channel with Carol.
But Alice has an open channel with Bob, and Bob has an open channel with Carol.
Instead of opening a new channel with Carol, Alice can route the payment trough Bob:
Alice - Bob - Carol.

In this scenario it is possible for Bob to take a small fee.
16 Q:

In the above scenario; what is preventing Bob from just stealing the money in transit?

Short A:
Bob is actually paying out to Carol first, and then afterwards Bob will get his money back from Alice.

Long A:
1. Carol starts the process by producing a random number (R) that she will keep as a temporary secret.

2. Carol then generates a hash (H) of R

3. Carol gives H to Alice

4. Alice construct a special transaction that can transfer money from Alice to Bob. But this transaction is only valid if R is included. At this point the transaction is not valid due to the lack of R. Alice also gives H to Bob, and Bob knows that H is the hash of the missing component R.

5. Bob will now construct another special transaction that can transfer the money from Bob to Carol. But this transaction is also only valid if R is included. At this point the transaction is not valid since Bob does not have access R.

6. Carol want her money, so she reveals R to Bob; thereby making the transaction valid.

7. Since Bob is already in possession of the transaction made by Alice, he can just include R and that transaction also becomes valid. Bob knows that he has been given the correct R because he can check that H is the hash of R.

8. At the same time Bob also reveals R to Alice.
Alice can now use R as proof that she has paid Carol (R becomes the receipt)

Q 17:
Where can I find more information about Lightning?

A:
http://lightning.network/

https://letstalkbitcoin.com/blog/post/lets-talk-bitcoin-286-drinks-on-a-lightning-network

https://letstalkbitcoin.com/blog/post/the-lightning-network-elidhdicacs

https://github.com/lightningnetwork/lightning-rfc/blob/master/00-introduction.md

https://www.youtube.com/watch?v=8zVzw912wPo