

CLAIMS

What is claimed is:

1. A method comprising:
 - receiving a message from a first autonomous vehicle, the message including a signed body portion and a triple, ~~the triple including components selected from the group consisting of~~ comprising a public identifier of the first autonomous vehicle, a public key of the first autonomous vehicle, and a certificate of the first autonomous vehicle, wherein the public identifier is generated at least in part on a unique device secret of the first autonomous vehicle and wherein the certificate comprises an encrypted ciphertext generated by encrypting the public key;
 - authenticating the message by verifying the certificate of the first autonomous vehicle;
 - logging the message into a blockchain storage structure, the blockchain storage structure storing a plurality of blocks, each blocking including the signed body portion; and
 - executing one or more orders included within the signed body portion.
2. The method of claim 1, the ~~components triple~~ triple generated using a Device Identity Composition Engine (DICE)- Robust Internet of Things (RIoT) core layer.
3. The method of claim 1, the signed body portion signed using a private key corresponding to the public key of the first autonomous vehicle.
4. The method of claim 1, the signed body portion comprising an order to remotely control a second autonomous vehicle.
5. The method of claim 1, the signed body portion comprising a response to an order to remotely control a second autonomous vehicle.

~~6. The method of claim 1, the signed body portion comprising a freshness indicator.~~

~~7.6. The method of claim 1, the authenticating the message comprising doubly decrypting the triple to obtain a result and comparing the result to the public identifier.~~

~~8.7. The method of claim 1, the authenticating the message further comprising confirming an identity of the first autonomous vehicle by querying a remote database using the triple.~~

~~9.8. A non-transitory computer readable storage medium for tangibly storing computer program instructions capable of being executed by a computer processor, the computer program instructions defining the steps of:~~

~~receiving a message from a first autonomous vehicle, the message including a signed body portion and a triple, the triple comprising including components selected from the group consisting of a public identifier of the first autonomous vehicle, a public key of the first autonomous vehicle, and a certificate of the first autonomous vehicle, wherein the public identifier is generated at least in part on a unique device secret of the first autonomous vehicle and wherein the certificate comprises an encrypted ciphertext generated by encrypting the public key;~~

~~authenticating the message by verifying the certificate of the first autonomous vehicle;~~

~~logging the message into a blockchain storage structure, the blockchain storage structure storing a plurality of blocks, each blocking including the signed body portion; and~~

~~executing one or more orders included within the signed body portion.~~

~~10.9. The non-transitory computer readable storage medium of claim 98, the ~~components~~ triple generated using a Device Identity Composition Engine (DICE)- Robust Internet of Things (RIoT) core layer.~~

~~11.10.~~ The non-transitory computer readable storage medium of claim ~~98~~, the signed body portion comprising an order to remotely control a second autonomous vehicle.

~~12.11.~~ The non-transitory computer readable storage medium of claim ~~98~~, the signed body portion comprising a response to an order to remotely control a second autonomous vehicle.

~~13.12.~~ The non-transitory computer readable storage medium of claim ~~98~~, the authenticating the message comprising doubly decrypting the triple to obtain a result and comparing the result to the public identifier.

~~14.13.~~ The non-transitory computer readable storage medium of claim ~~89~~, the authenticating the message further comprising confirming an identify of the first autonomous vehicle by querying a remote database using the triple.

~~15.14.~~ A device comprising:

a processor; and

a storage medium for tangibly storing thereon program logic for

execution by the processor, the stored program logic comprising logic performing ~~the~~ steps of:

receiving a message from a first autonomous vehicle, the message

including a signed body portion and a triple, the triple comprising ~~including components selected from the group~~

~~consisting of~~ a public identifier of the first autonomous

vehicle, a public key of the first autonomous vehicle, and a

certificate of the first autonomous vehicle, wherein the

public identifier is generated at least in part on a unique

device secret of the first autonomous vehicle and wherein

the certificate comprises an encrypted ciphertext generated

by encrypting the public key;

authenticating the message by verifying the certificate of the first autonomous vehicle;

logging the message into a blockchain storage structure, the
blockchain storage structure storing a plurality of blocks,
each blocking including the signed body portion; and
executing one or more orders included within the signed body
portion.

~~16.15.~~ The device of claim ~~15~~14, the ~~components triple~~ generated using a Device Identity Composition Engine (DICE)- Robust Internet of Things (RIoT) core layer.

~~17.16.~~ The device of claim ~~15~~14, the signed body portion comprising an order to remotely control a second autonomous vehicle.

~~18.17.~~ The device of claim ~~15~~14, the signed body portion comprising a response to an order to remotely control a second autonomous vehicle.

~~19.18.~~ The device of claim ~~15~~14, the authenticating the message comprising doubly decrypting the triple to obtain a result and comparing the result to the public identifier.

~~20.19.~~ The device of claim ~~15~~14, the authenticating the message further comprising confirming an identity of the first autonomous vehicle by querying a remote database using the triple.

20. The method of claim 6, wherein doubly decrypting the triple to obtain a result and comparing the result to the public identifier comprises:

decrypting the certificate of the first autonomous vehicle using the public key of the first autonomous vehicle to obtain a resulting key; and
decrypting the public identifier of the first autonomous vehicle using the resulting key to obtain the result.