



(51) International Patent Classification:

G08G 1/01 (2006.01) G07B 15/06 (2011.01)
G08G 1/14 (2006.01)

(21) International Application Number:

PCT/EP2016/060171

(22) International Filing Date:

06 May 2016 (06.05.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: RWE INTERNATIONAL SE [DE/DE];
Opernplatz 1, 45128 Essen (DE).

(72) Inventor: STÖCKER, Carsten; Verdstraße 5, 40724
Hilden (DE).

(74) Agent: BÜCKER, Hendrik; Cohausz & Florack, Bleich-
straße 14, 40211 Düsseldorf (DE).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,
HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA,
LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN,
MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE,

PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE,
SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: TRAFFIC SYSTEM

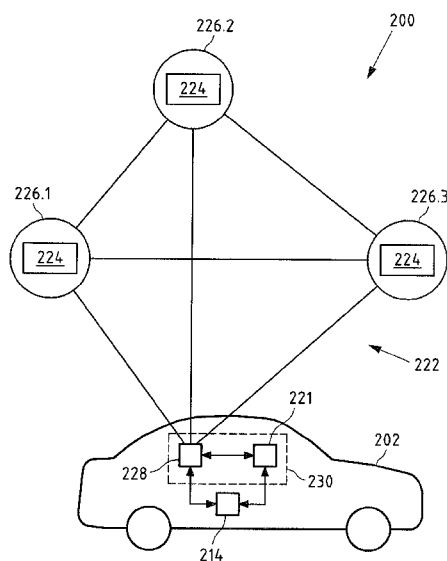


Fig.2

(57) Abstract: The invention relates to a traffic system (200, 300, 400, 600) comprising at least one vehicle (202, 302, 304, 402, 602.2, 604.2), at least one sensor module (221, 321, 421) configured to detect at least one motion parameter relating to the vehicle (202, 302, 304, 402, 602.2, 604.2), at least one peer-to-peer module (228, 328, 426.2) assigned to the vehicle (202, 302, 304, 402, 602.2, 604.2) and configured to communicate with at least one peer-to-peer application (224, 324, 424, 524) of at least one peer-to-peer network (222, 322, 422, 622), wherein the peer-to-peer module (228, 328, 426.2) is configured to transmit at least the detected motion parameter to the peer-to-peer application (224, 324, 424, 524) and/or to receive at least traffic information data from the peer-to-peer application (224, 324, 424, 524).



Traffic system

The invention relates to a traffic system comprising at least one vehicle and at least one sensor module. The invention relates also to methods, an arrangement for a vehicle, a vehicle, and a peer-to-peer application.

5

Traffic systems for providing traffic information to one or more vehicles or to navigation module(s) of respective vehicles are known from prior art. A typical prior art system 100 is shown in figure 1.

10 The depicted traffic system 100 usually comprises a plurality of vehicles 102, 104. In the present case, each vehicle 102, 104 comprises a transceiver module 112. The transceiver module 112 is connected to a navigation module 114. A central instance 106, such as a server 106 is adapted to send traffic information data to the navigation module 114 via a suitable communication channel 118 and the transceiver module
15 112. The traffic information data may comprise current traffic status data about the traffic situation of the traffic routes of the vehicles 102, 104. For instance, traffic jam information can be included in the sent traffic information.

Further, a vehicle may comprise a sensor module 121 e.g. in form of a GPS (Global
20 Positioning System) sensor. Such a sensor may be included in the navigation module 114. The sensor module 121 is configured to detect the current location of a vehicle 102, 104 based on a communication with a satellite system 110. For instance, via a specific communication channel 120 and the transceiver module, respective location parameter values can be received by the vehicles 102, 104.

25

A conventional navigation module 114 is configured to calculate an optimal traffic path/route for each vehicle 102, 104 based on the received traffic information and the received location parameter of the vehicle 102, 104.

Environmental data (e.g. video data, temperature, air quality, precipitation, humidity, traffic density data, traffic way damages or congestions) can also be received from or transmitted to one or more central system(s) by a vehicle 102, 104.

5

In recent traffic systems 100, a sensor module 121 of the vehicle 104 may also be configured to detect a further motion parameter (besides the location parameter) relating to the vehicle 104 in form of the current velocity of the vehicle 104. The transceiver module 112 is configured to regularly transmit the motion parameters (current location and current velocity) of the vehicle 104 to a further central server 108 via communication channel 123. It shall be understood that central server 106 and central server 108 may be realized by one server.

The central server 108 is configured to evaluate the motion parameter values received from the one or more vehicle(s) 104 and additionally traffic information received from further sources 126, such as traffic information providers. The evaluated data is used by the central server 106 to prepare and transmit traffic information to the vehicles 102, 104, as described above.

In prior art traffic systems mobile terminals (operated while using a vehicle) such as a smart phone or mobile embedded device can be used instead of navigation or communication modules built into a vehicle via a fixed installation.

Common to all prior art traffic systems are that a central subsystem, a central process and/or a central organization or instance is provided in order to manage and provide the traffic information and to control a traffic action. In particular, the evaluation and transmission of traffic information are centrally controlled by a central instance/server.

Technically speaking, a corresponding traffic system is realized according to prior art by a client-server structure. The central organization or instance is created by one or a

plurality of central servers. A server of this kind or a platform can be distributed and located on different computing devices, for example. This means that a virtual server can be realized by a cloud. For example, a centrally arranged database can be provided.

5

In particular, a central instance/server is configured to evaluate motion data of user's vehicles and to transmit, based on the evaluation, traffic information to the vehicles. Thereby, the central server is used as a confidential instance for the vehicle's data. The central instance, such as a server or a platform, defines the rules. The central server ensures that the processes are carried out correctly for all entities/vehicles involved. In other words, a central instance prevents tampering by one of the participating entities and/or by third parties.

10

The disadvantage of server-client structures of this kind, particularly the server (or platform), apart from the high transaction costs, is that the central instance or central server manages the confidential user data of the users of vehicles. A persistent problem affecting the central instance is that of protecting the user data stored on one server or a plurality of servers from access by unauthorized third parties. In particular, a high degree of security expenditure is required in order to prevent user data (e.g. registered identifications), billing data, location data of the user, etc. from being tampered. This in turn leads to higher transaction costs.

15

20

Therefore, the object of the present invention is to provide a traffic system which simplifies an operation of the traffic system and, at the same time, offers a high level of security.

25

The object is solved according to a first aspect of the invention by a traffic system according to claim 1. The traffic system comprises at least one vehicle. The traffic system comprises at least one sensor module configured to detect at least one motion parameter relating to the vehicle. The traffic system comprises at least one peer-to-peer module assigned to the vehicle and configured to communicate with at least one

30

peer-to-peer application of at least one peer-to-peer network. The peer-to-peer module is configured to transmit at least the detected motion parameter to the peer-to-peer application. Alternatively or additionally, the peer-to-peer module is configured to receive at least traffic information data from the peer-to-peer application.

In contrast to the prior art, a traffic action can be easily performed and controlled – without a central instance – by means of a peer-to-peer application of a peer-to-peer network and a peer-to-peer module assigned to the vehicle. Thereby, the peer-to-peer module is capable of communicating with the peer-to-peer application and peer-to-peer network, respectively. By the fact that instead of a central server or a platform, a peer-to-peer network (also called a framework) undertakes the in particular tamper-proof controlling of the data e.g. to be provided to a vehicle or received from a vehicle by means of a peer-to-peer application a high level of security is provided. In the case of a peer-to-peer network, high security standards are achieved in that all computers (peer nodes or simply nodes) in the peer-to-peer network, at least a part of the peer computers in the peer-to-peer network, monitor(s) at least the accuracy of the data relating to a vehicle and/or traffic information data. Transaction costs can be reduced. No central, superior platform, server, cloud, etc. is required.

The traffic system may be configured to support the controlling of one or more traffic process(es) and action(s), respectively. A traffic system according to the invention comprises at least one vehicle. Generally, a traffic system may comprise a plurality of vehicles. A vehicle may be any mobile transport unit. Exemplified vehicles are cars, trucks, ships, railway vehicles, planes, bicycles, motor bicycles, drones, mobile machines, boats, planes, submarines, space vehicles, etc.

Further, the traffic system comprises at least one sensor module. A sensor module may comprise one or more sensor(s) configured to detect or sense one or more motion parameter(s). The sensor module can be a single device or can be formed by two or more separate units, such as separate sensors. The sensor module can be at

least partly integrated in the at least one vehicle. For instance, the sensor module can be at least partly formed by one or more sensor(s) already integrated in the vehicle, such as a velocity sensor, location sensor, acceleration sensor, a sensor for monitoring a state of a component of the vehicle, measuring environmental data, traffic way data, video/photo camera, etc. Further, the sensor module may be at least partly formed by an external unit. An external unit is not arranged in the vehicle. For instance, an external unit may be positioned at a path of the vehicle for detecting passing vehicles. Such a sensor may be configured to detect an identification (e.g. number plate) of the passing vehicle.

The at least one detectable motion parameter relates to the vehicle. In particular, in the present case a motion parameter is characterized in that it comprises any kind of information about a movement state of the vehicle. Further, detecting at least one motion parameter means in particular that a current value of said motion parameter is detected. The at least one detected motion parameter and its value, respectively, can be provided by the sensor module to the peer-to-peer module. For instance, a communication connection can be established between these modules in order to provide the motion parameter to the peer-to-peer module.

Moreover, the traffic system comprises at least one peer-to-peer module. The peer-to-peer module is (uniquely) assigned to the vehicle. This means that the peer-to-peer module can at least communicate and/or act on behalf of the vehicle. Furthermore, since the vehicle can be assigned to one or more user, the peer-to-peer module can be (indirectly) assigned to the at least one user. On the other hand, the peer-to-peer module can be (directly) assigned to a user and via the user (indirectly) to a vehicle of the user.

For example, the peer-to-peer module can be integrated in the vehicle or it can be formed by separate processing device, such as mobile terminal, owned by a user of the mobile unit, or it can run on a remote processing device (e.g. in a data centre).

Furthermore, the peer-to-peer module may be configured to access an (electronic) wallet of a cryptocurrency for a vehicle or a user. The wallet may be part of a vehicle.

5 A mobile terminal can be a smart phone or an embedded device. Such a device may be configured to communicate with one or more (electronic) modules of the vehicle (sensor module, transceiver module or navigation module) via wired or wireless communication. An embedded device comprising the peer-to-peer module module and preferably the peer-to-peer application can also be connected to the vehicle via an interface. An interface can be a standard On-board diagnostics (OBD) connector or
10 another vehicle specific connector. For instance, a user can connect a peer-to-peer module module via OBD to a vehicle in order to enable the vehicle to participate in the peer-to-peer module application and network, respectively. The peer-to-peer module module may get access to vehicle data via the OBD connector. In this case the peer-to-peer module module may act as an OBD adapter. The (OBD) adapter can be an
15 installed module that is fixed to a vehicle or a mobile module that a user can plug into the actual vehicle he is using.

In an alternative embodiment the peer-to-peer module module can be a connected with a battery of an electric vehicle. The peer-to-peer module module can be
20 integrated in one or more battery connector(s) of the battery of the vehicle. In a further alternative embodiment the peer-to-peer module module can be comprised in or connected with a navigation module or entertainment module of the vehicle.

In case of a remote processing device the vehicle may encrypt data on application
25 level or may have a secure communication channel to the processing device of the data centre and the processing device itself may have a connection to the peer-to-peer network. In an alternative embodiment the remote processing device may be a gateway to the peer-to-peer network. This means that the mobile unit has a secure access to the peer-to-peer network via a communication channel with the gateway.

It shall be understood that there may be further peer-to-peer modules. For instance, a further peer-to-peer module may be (uniquely) assigned to a previously described external sensor module.

5 In a further embodiment a mixed architecture can be used comprising at least one peer-to-peer application and a central system. A central system can for example be used to manage traffic control parameter(s) from a central authority. These parameters can be uploaded into the peer-to-peer application. In a further embodiment the peer-to-peer application can communicate with a central service to
10 execute optimisation algorithm(s) in order to optimize traffic flows or prevention of traffic accidents or propose traffic way changes or upgrades to improve the traffic flow or reduce accidents. A central system may be configured to control traffic lights, signals or access systems to further improve or control traffic flows. Control traffic lights, signals or access systems can be managed via the peer-to-peer application.

15 In comparison to a client-server network in which a server provides a service and a client uses the service, these roles are cancelled in a peer-to-peer network. Each participant of the peer-to-peer network can use a service and the like and offer such a service. In particular, a peer-to-peer network is self-determined and/or self-organized
20 (without any higher-level units). In the present case preferably each computer of the peer-to-peer network comprises a peer-to-peer application. In particular, the peer-to-peer module is configured to transmit data e.g. by sending one or more message(s) to the peer-to-peer application and/or receive data by e.g. reading data stored in the peer-to-peer application or receiving one or more messages from the peer-to-peer
25 application. The peer-to-peer module may be a peer of the peer-to-peer network.

The peer-to-peer module is configured to communicate with the peer-to-peer application of the peer-to-peer network. In particular, the peer-to-peer module is configured to transmit at least the detected motion parameter to the peer-to-peer
30 application. Preferably, the peer-to-peer application can evaluate said received data. For instance, traffic information data can be generated. Alternatively or additionally,

the peer-to-peer module receives traffic information data. Traffic information data relates to or comprises data regarding traffic status data and/or regarding any traffic action.

- 5 The list of all (anonymised or pseudonymised) participants or entities of the at least one peer-to-peer network can preferably be made known to each participant, so in particular to each entity of the traffic system, as a peer-to-peer identification, e.g. in the form of a communications address. A mixer logic (i.e. mixing of identifications and using random identifications for a specific vehicle or user for its individual
- 10 transactions) can be used to disguise user identifications of individual transactions to avoid analysis of movement profiles.

A peer-to-peer module can be at least partially formed by a software module and/or at least partially formed by a hardware module. There may be two or more different

15 peer-to-peer networks each configured for one or more different traffic action(s).

According to a first embodiment of the traffic system of the invention, the at least one motion parameter relating to the vehicle may be at least one of the group comprising velocity of the vehicle, acceleration of the vehicle, a state of a component of the

20 vehicle, in particular, the state of the motor of the vehicle, and/or the location of the vehicle and/or environmental data (e.g. video data, radar/lidar data, temperature, air quality, precipitation, humidity, traffic density data, traffic way damages, traffic way conditions or congestions) in the surroundings of the vehicle. Preferably, at least the velocity of the vehicle and the location of the vehicle can be detected by suitable

25 sensors of the sensor module. As described above, the current value of the respective motion parameters can be detected and preferably transmitted to the peer-to-peer application. By providing this data to a peer-to-peer application, the data about the user, such as the location data of the user, is particularly secure handled.

30 According to a further embodiment of the present traffic system the traffic system may comprise at least one navigation module assigned to the vehicle and connectable

with the at least one peer-to-peer module. The navigation module may be configured to display the received traffic information data. More particularly, based on a plurality of motion parameters of a plurality of vehicles and/or other traffic state data from other sources the peer-to-peer application may determine the current traffic state of different areas (road, street, etc.). The current traffic state can be provided to the at least one navigation module via the respective peer-to-peer module.

In addition, the navigation module may provide further data, such as a desired destination of the vehicle, at least one specific criterion, such as avoiding toll roads or highways, preferring shortest or fastest route, etc. The peer-to-peer application may be configured to calculate based on the plurality of motion parameters of the plurality of vehicles and/or other traffic state data from other sources and said further data the optimal route to the desired destination. The route data can be provided to the at least one navigation module via the respective peer-to-peer module. A secure, accurate and powerful navigation system can be provided.

Furthermore, the sensor module may comprise a location sensor, in particular, a satellite positioning sensor, such as a GPS or Galileo sensor, a ground-based location sensor, or a combination of both (e.g. differential GPS) configured to locate the (current) location of the vehicle. Alternatively or additionally, the sensor module may comprise a camera sensor configured to detect at least one optical marking unit positioned on a path of the vehicle. Each marking unit may comprise a detectable (unique) identification. Based on this identification, the location of the marking unit, and thus, the (current) position of the vehicle can be determined.

25

In addition, the sensor module may comprise one or more sensor(s) configured to detect environmental parameter(s) (e.g. temperature, traffic density, CO₂ data, surrounding data, photos, geo data, radar/lidar data, traffic way conditions, congestions). Further, technical status of components of the vehicle can be detected by one or more sensors of the sensor module.

30

Furthermore, the sensor module may comprise a reader configured to detect at least one electromagnetic field emitted by at least one marking unit positioned on a path of the vehicle. The emitted field may comprise an (unique) identification of the emitting marking unit. Based on this identification, the location of the marking unit, and thus,
5 the (current) position of the vehicle can be determined.

The sensor module may comprise a vehicle identification sensor configured to detect the identification of a vehicle passing the vehicle identification sensor. For instance, an optical or electromagnetic sensor can be configured to detect an (unique)
10 identification of a vehicle passing said sensor. For instance, the sensor can be arranged on a bridge, traffic light, traffic sign, surveillance system, gates, law enforcement device (e.g. speeding camera) or the like. This sensor module may be connectable with a further peer-to-peer module. The further peer-to-peer module may be configured to transmit the at least one detected identification together with
15 location information of said sensor to the peer-to-peer application. Based on this information the current location of a vehicle can be determined by the peer-to-peer application. Such an external sensor may additionally detect further motion parameter (e.g. speed, direction, vehicle traffic dynamics / user behaviour) or location parameters (e.g. vehicle inside or outside allowed traffic ways). This may allow to
20 detect the current traffic situation (e.g. traffic jam or not) or to monitor a toll-liaible route by means of the peer-to-peer application and/or to monitor whether the vehicle is operated in compliance with traffic laws for law enforcement purposes (e.g. speeding, incorrect use of one-way street, parking in non-parking areas, overtaking cars when it is prohibited) or operating in accordance to agreed traffic ways.

25

According to a further embodiment, the sensor module comprises at least one sensor configured to monitor the movement of a vehicle (at least one tire and/or axis rotation sensor and/or speed sensor) in order to provide Vehicle Logbook or Tachograph data (e.g. speed, operating times, rest periods). The sensor can be registered as a smart
30 asset in the peer-to-peer application of the peer-to-peer network. The data measured by the sensor can be transmitted to the peer-to-peer application. Preferably, the data

to be transmitted can be hashed, time-stamped, signed and/or encrypted (via e.g. telemetry systems) by the sensor. The sensor can comprise a peer-to-peer module and/or can be connectable with a peer-to-peer module. Said provided Vehicle Logbook data can be stored in the peer-to-peer application. Further (authorized) entities (of the peer-to-peer network) can access this data and can, preferably, use said data for e.g. law enforcement and/or for monitoring of operating and rest periods. Data can be stored in decentral file storage (e.g. IPFS) or decentral database (BigchainDB). It shall be understood that a user of a vehicle can authenticate himself via his peer-to-peer identification prior to conducting a vehicle operation. Vehicle peer-to-peer identification and/or user peer-to-peer identification may be stored in the Vehicle Logbook. By analysing user peer-to-peer identification across multiple logbooks single user behaviours can be monitored. Data can be encrypted to ensure that only authorised entities can conduct vehicle or user monitoring.

As will be described in more details hereinafter, the registration process of a vehicle and a Vehicle Logbook sensor can be validated by a central system which is connectable to a peer-to-peer network via a peer-to-peer module and operated by government authorities or by authorities using the peer-to-peer application to validate the registration process. This validation process can make use of production data stored during the manufacturing process of the sensor (e.g. sensor ID, quality assurance data).

It shall be understood that such a registration and validation process can be applied for all other sensors and/or actors that need to fulfil regulatory requirements.

In a further embodiment of the present invention, the peer-to-peer network and a peer-to-peer application, respectively, can be configured to assist a vehicle for autonomous driving. Also in this embodiment, a mixed architecture can be used comprising at least one peer-to-peer application and a central system. As described before, environmental data and/or analytics can be gathered and provide for a one or more vehicle(s) about e.g. road obstacles, constructions sites, weather conditions

and/or road conditions (e.g. ice on the road), passing manoeuvre or platooning of vehicles in a convoy. The at least one peer-to-peer application, such as a block chain, can be configured to facilitate the process of exchanging secure messages between one or many vehicles and/or a central system and or amongst individual vehicles by means of secure identities or smart assets. Peer-to-peer and/or peer-to-central system communication can be conducted via hashed and/or signed and/or time-stamped and/or encrypted message(s) to ensure authenticity and correctness of messages/data, to avoid manipulation or identify outdated messages.

Furthermore, one or more individual sensor(s) in a vehicle can be registered in the peer-to-peer application with a (unique) peer-to-peer identification. Data/Messages sent by a registered sensor can be hashed, signed, time-stamped and/or encrypted to ensure authenticity and correctness of the data.

Furthermore, one or more individual actors(s) in a vehicle can be registered in the peer-to-peer application with a (unique) peer-to-peer identification. An actor can validate authenticity and/or correctness of messages sent from a peer of the peer-to-peer network, such as one or more peer vehicles (or central system or traffic systems), by means of the peer-to-peer identification, and preferably, by means of (proper) hashing, signing, time-stamping and/or encrypting. It shall be understood that an actor can be connected to a peer-to-peer application via a peer-to-peer module. Examples for actors are components in a vehicle and/or traffic lights, signals or access systems.

According to a preferred embodiment of the traffic system of the present invention at least one peer-to-peer module may be configured to cause generating of at least one access transaction agreement about at least one access action of the vehicle by means of the at least one peer-to-peer application (e.g. for managing authorised or paid access to private or otherwise restricted areas). Preferably, a peer-to-peer module, such as the peer-to-peer module assigned to the vehicle or another peer-to-peer

module may initiate or cause the generation of an access transaction agreement. In other words, access of a vehicle on a particular private or public space may require that a peer-to-peer module is configured to cause or trigger the generation of an agreement between e.g. the user of the car and the provider of the space. The access transaction agreement can comprise data, such as involved entities (e.g. identifications of the vehicle, access areas space, time of use, user, provider, etc.) and at least one access transaction criterion (e.g. amount of cryptocurrency to be paid e.g. per time unit). Without a central instance, two entities can cause the generation of a access transaction agreement in a simple manner.

In addition, one or more (external) actor(s) (e.g. a gate) may be connected to the peer-to-peer application. By the means of the access transaction agreement a vehicle or user of the vehicle can trigger an actor (e.g. the gate that opens when the vehicle user is in front of the gate or a traffic light that is switched from red to green). It should be understood that the external actor can be configured with an external sensor to identify a vehicle or user in order to ensure that access is granted in accordance to the access transaction agreement. Trigger or access events may be stored in the peer-to-peer application for monitoring or reporting purposes.

The access transaction agreement may include on-ground mobility, mobility in or under water or for mobility in air or space. Accessing restricted spaces with no access transaction agreement can be prohibited and/or penalised.

Law enforcement, military and/or emergency vehicles can be registered in a peer-to-peer application to get (automatic, priority) access to an area. These vehicles are registered in the peer-to-peer application with e.g. a flag as priority vehicles.

According to a preferred embodiment of the traffic system of the present invention at least one peer-to-peer module may be configured to cause generating of at least one parking transaction agreement about at least one parking action of the vehicle by means of the at least one peer-to-peer application. Preferably, a peer-to-peer module,

such as the peer-to-peer module assigned to the vehicle or another peer-to-peer module may initiate or cause the generation of a parking transaction agreement. In other words, parking of a vehicle on a particular parking space may require that a peer-to-peer module is configured to cause or trigger the generation of an agreement
5 between e.g. the user of the car and the provider of the parking space. The parking transaction agreement can comprise data, such as involved entities (e.g. identifications of the vehicle, parking space, user, provider, etc.) and at least one parking transaction criterion (e.g. amount of cryptocurrency to be paid e.g. per time unit). Without a central instance, two entities can cause the generation of a parking
10 transaction agreement in a simple manner.

Furthermore, the peer-to-peer application may be preferably configured to detect based on the at least one motion parameter relating to the vehicle whether the vehicle is in a parking state within a predefined area. A predefined area is a specific
15 geographic area (e.g. defined by geographic coordinates) comprising at least one parking space. In order to detect whether the vehicle is within a predefined area, the location parameter(s) provided by the peer-to-peer module of the vehicle can be compared with the stored location parameter(s) defining the at least one predefined area.

Further, based on at least one further motion parameter relating to said vehicle, such as the current velocity, current state of the motor, and motion parameter(s) (e.g. velocity of the respective vehicles) of further vehicles located in vicinity to the other vehicle, it can be determined whether the vehicle is in a parking state or e.g. in a
25 driving state.

For instance, according to an access and/or a parking transaction agreement, the access and/or parking within a predefined area requires the conduction of a parking transaction criterion transaction. Preferably, after the conduction of an access and/or
30 a parking action, the peer-to-peer application may be configured to conduct an access and/or a parking criterion transaction action based on the generated parking

transaction agreement. For instance, the peer-to-peer application can initiate, control and/or conduct the transfer of an agreed amount of cryptocurrency from an user of a vehicle and a provider of the parking space of the predefined area.

- 5 In the case, the amount depends on the duration of the access and/or parking action, the peer-to-peer application may be configured to detect the duration of the access and/or parking state of the vehicle. Alternatively or additionally, the sensor module assigned to the vehicle may be configured to detect the duration of the access and/or parking state vehicle. In the case, also the vehicle checks the duration, the correct
10 calculation of the amount of cryptocurrency depending on said duration can be verified by the user of the vehicle.

- By way of example, the one or more vehicle may be registered vehicle(s) in a access and/or parking peer-to-peer network. Further, one or more predefined areas having
15 one or more access and/or parking space(s) may be registered in said peer-to-peer network. For instance, private providers can generate such a peer-to-peer network in order to offer parking places to each other. In this access and/or parking network one or more (general) access and/or parking transaction agreements may be generated. Based on the at least one access and/or parking transaction and by means of the peer-
20 to-peer application and network, respectively, each access and/or parking action can be conducted and charged in an automatic and simple and at the same time secure way. Pricing data for access and/or parking can be defined in the peer-to-peer application by dynamic or user-/vehicle specific pricing schemes.

- 25 According to a further embodiment, at least one peer-to-peer module may be configured to cause generating of at least one toll transaction agreement about at least one toll-labile action of the vehicle by means of the at least one peer-to-peer application. For instance, for the use of at least one specific road or other route tolls or similar user charges have to be paid. The control of such a traffic system can be
30 performed by the peer-to-peer application. User or vehicles may be registered with the peer-to-peer application via an identification or a wallet, as will be described

hereinafter. Based on received motion parameters of a vehicle and e.g. a vehicle identification (e.g. number plate, RFID transponder or another identification that can be read out via optical and/or electromagnetic waves) of said vehicle, a toll-liable action can be controlled and charged (e.g. via cryptocurrencies) by means of the peer-to-peer application. Preferably, after the conduction of at least one toll-liable action, the peer-to-peer application may be configured to conduct a toll criterion transaction action based on the generated (general) toll-liable action transaction agreement. This action agreement may be an agreement valid for all vehicles passing said toll-liable route.

In order to reduce traffic jams, the at least one toll criterion may be a location-based and/or dynamic toll criterion (e.g. between a minimum and maximum value to be paid) wherein the actual value may depend on a location, an expected traffic state or current traffic state (e.g. low traffic volume or high traffic volume) of said toll-liable route and/or time (e.g. higher toll prices at peak times). Furthermore, at least one toll criterion may be a priority toll criterion (e.g. between a minimum and maximum value to be paid) for using less congested traffic ways with higher priorities (e.g. fast lane or fast track). Traffic jams may be at least reduced and/or better controlled. Pricing schemes of toll-liable actions can depend on dynamic traffic parameters and/or user-/vehicle specific attribute(s) which are defined in the peer-to-peer application (e.g. different prices for cars or trucks depending on density of traffic). Dynamic pricing via the peer-to-peer application can be used to steer or optimise traffic flows.

In a further embodiment, at least one peer-to-peer module may be configured to cause generating of at least one law enforcement agreement about at least one law enforcement action of the vehicle by means of the at least one peer-to-peer application.

For instance, if a user or a vehicle of the user is not operating in compliance with laws the law enforcement external sensor data and the vehicle data may be written into the peer-to-peer application and linked to the identification of the vehicle. In case a

breach of a traffic law is measured/detected by the external sensor (e.g. speeding camera) a penalty can be paid. By the means of comparison of vehicle's sensor data and external sensor data it can be (directly) proofed that a user or a vehicle breached traffic laws. The proof(s) may be stored in the peer-to-peer application.

5

Furthermore, one or more traffic law enforcement algorithm(s) including penalties can be directly build into the vehicle. Data of the vehicle may be used to detect breaches of law(s). In this case, an external sensor is not needed. Penalties can be payments, locking and/or stopping of a vehicle or a vehicle/user operating licence restriction. A build in law enforcement logic can be considered as "Law Enforcement in Advance". Taxes schemes can incentivise this logic with specific tax cuts (for e.g. vehicle registration or operating taxes).

10

A check of a vehicle/user operating licence restriction may require that vehicle(s) check by means of the peer-to-peer application whether a user has the right to operate a vehicle. In a further embodiment, the peer-to-peer application may hold user or vehicle data about user or vehicle operating licences. A vehicle can be for example unlocked for operations only if a user has a valid (e.g. signed by central authorities) operating licence without relevant restrictions or limitations (maybe caused by breach of laws or missing licence for a specific vehicle type; e.g. a truck or a plane).

15

20

The control of a traffic system in form of a law enforcement and vehicle operating licence system can be performed by the peer-to-peer application. User or vehicles may be registered with the peer-to-peer application via an identification and/or a wallet. Based on received sensor and/or motion parameter(s) of a vehicle, vehicle operating licence information and e.g. a vehicle identification (e.g. number plate, RFID or another identification that can be read out via optical or electromagnetic waves) of said vehicle, a law enforcement action can be controlled and charged via cryptocurrencies by means of the peer-to-peer application.

25

30

Preferably, after the conduction of at least one law enforcement-liable action, the peer-to-peer application may be configured to conduct a law enforcement criterion transaction action based on the generated (general) law enforcement(-liable) transaction agreement. This transaction agreement may be an agreement valid for all
5 vehicles passing said route.

In a further embodiment route side infrastructure can be used by a vehicle (i.e. sensors along a route such as differential GPS sensors). By means of a peer-to-peer application and a sensor usage agreement a vehicle can be allowed to use sensor data
10 and pay in cryptocurrency.

It shall be understood that sensor data of vehicle(s) can be shared with other entities (traffic analysis systems, weather systems, air quality system, etc.). By means of a peer-to-peer application and a sensor usage agreement another entity can be allowed
15 to use vehicle sensor data (swarm intelligence) and pay in cryptocurrency. Using these data a peer-to-peer application (in combination with off-chain algorithms) can provide analytics traffic system and environmental analyses for further optimisation options for authorities or private owners or for an accident prevention system or for environmental or authority reporting purposes.

Furthermore, according to a further preferred embodiment, the at least one peer-to-peer module may be configured to cause generating of at least one vehicle autonomous driving transaction agreement about at least one vehicle autonomous driving action of the vehicle by means of the at least one peer-to-peer application. A
25 vehicle autonomous driving agreement may comprise an autonomous driving service and/or vehicles in the surrounding. The autonomous driving service may be provided, facilitated and/or paid via the peer-to-peer application. The autonomous driving service may provide (reliable) data beyond the "(visible) sight" of a vehicle (e.g. obstacles, road conditions, accidents, objects hidden from the sensors of a vehicle, etc.) in order to improve security and/or convenience of vehicle operations.
30 Alternatively or additionally, one or more vehicle(s) in the surrounding of said vehicle

may generate an autonomous driving agreement to share data in the (visible) sight of each vehicle in order to improve the (visible) sight of said (individual) vehicle. This may improve security and/or convenience of vehicle operations.

- 5 Preferably after the conduction of a vehicle autonomous driving action, the peer-to-peer application may be configured to conduct a vehicle autonomous driving transaction action for improving the sight of individual cars.

Under the vehicle autonomous driving agreement environmental data are gathered,
10 shared and/or analysed (e.g. road obstacles, constructions sites, weather / road conditions (e.g. ice on the road) or passing manoeuvres). Another example may be platooning of vehicles in a convoy. This platooning can be agreed in a vehicle autonomous driving agreement. One or more new vehicle(s) joining a traffic way browse the peer-to-peer application for an already existing platoon and/or
15 communicate with one or more vehicles in the surrounding of said new vehicle via e.g. a car-to-car network to identify a platoon. A vehicle may register itself in the peer-to-peer application. The peer-to-peer application may then adjust speed and/or distance of the two or more vehicles in a platoon accordingly. Secure data exchange among sensor(s) and/or actor(s) can be done via peer-to-peer communication with e.g.
20 hashed, signed, time-stamped and/or encrypted data.

Furthermore, according to another embodiment, the at least one peer-to-peer module may be configured to cause generating of at least one vehicle sharing transaction agreement about at least one vehicle sharing action of the vehicle by means of the at
25 least one peer-to-peer application. A vehicle sharing transaction agreement may be generated in a similar way as described above in connection with e.g. the parking transaction agreement. Preferably after the conduction of a vehicle sharing action, the peer-to-peer application may be configured to conduct a vehicle sharing criterion transaction action based on the generated vehicle sharing action transaction
30 agreement. For instance, based on a vehicle sharing criterion (e.g. a particular amount of cryptocurrency per time unit) the peer-to-peer application may cause the

transmission of said agreed amount from e.g. an account of a user of a vehicle to an account of a provider of said vehicle (e.g. pay per use). The price for using a vehicle may depend on the user's operating licence information stored in the peer-to-peer application (e.g. experience in number of years or distance driven, traffic law enforcement penalties, operating behaviour data from previous sharing agreements). It shall be understood that validity of a vehicle sharing transaction agreement (checked by business logic in the agreement) or activation of a vehicle can depend of law enforcement and operating licence data of the user stored in the peer-to-peer application (checked by the vehicle prior to operations).

In this case, the peer-to-peer application may be a vehicle sharing peer-to-peer application of a vehicle sharing peer-to-peer network. One or more providers of one or more vehicle can generate such a peer-to-peer application and network, respectively, to offer the at least one vehicle to each other (and further user), wherein the provider may define the rules for a car sharing action.

According to a further embodiment, the at least one vehicle may comprise at least one locking module configured to lock an access unit of the vehicle and/or an activation of at least one function of the vehicle. The locking module may be configured to release the access unit of the vehicle and/or to activate the function of the vehicle based on a receipt of a release information provided by the peer-to-peer application. Preferably, the release information can be generated by the peer-to-peer application based on a generated vehicle sharing transaction agreement. Preferably, an identification assigned (directly or indirectly) to a user may be stored in said agreement. In order to unlock the locking module, an identification received from an user (e.g. from an user terminal of the user) may be transmitted e.g. by an interface module of the vehicle to the peer-to-peer application. For instance, the interface module can comprise a peer-to-peer module or can be connectable with a peer-to-peer module. After a verification of the received identification by means of the peer-to-peer network, the release information can be provided to the locking module. For instance, the locking module

can comprise a peer-to-peer module or can be connectable with a peer-to-peer module. Then, the user can use the vehicle.

- In a further embodiment, a vehicle may store sensor data in the peer-to-peer application for the purpose of maintenance (physical and/or chemical parameters, technical system status (of e.g. embedded device(s)), usage parameters of component of the vehicle). The peer-to-peer application can propose maintenance activities (based on data of other vehicles of the same or a similar type). Maintenance proposals can be predicted via machine learning or artificial intelligence algorithms (partly off-chain). Vehicle maintenance activities can be planned and coordinated in accordance to location, usage or route planning data. This type of coordination may be especially important for (logistic) transport units, such as trucks, that are maintained along their logistics route.
- Preferably, before receiving data from a peer-to-peer module of a vehicle or of another entity or before providing data to a peer-to-peer module of a vehicle or of another entity, by means of the peer-to-peer application and at least by some of the nodes of the peer-to-peer network, at least one received identification assigned to a mobile unit or an entity assigned to said vehicle can be checked. Preferably, all identifications of all entities of a peer-to-peer network are stored and registered, respectively, in the peer-to-peer application and/or in a database or decentral file system (such as IPFS) or decentral database (such as BigchainDB) controlled by the peer-to-peer application, such as by a smart contract of the peer-to-peer application.
- In addition a traffic system may comprise a distributed block chain database such as BigChainDB. The advantages of the immutable distributed block chain database may be that the data are immutable and any units or smart contracts or user in the system can run queries to analyse data and further optimise and automate a process.

Data stored either on a decentral file storage or a distributed block chain database may be encrypted. The peer-to-peer application, such as a block chain, is then used to facilitate access management to the data by handling the encryption keys.

- 5 Then, the at least one identification can be compared with the registered identifications. Only in the case the at least one identification is a valid identification, i.e. corresponds to at least one registered identification, a communication between said entity and the peer-to-peer application is enabled. A decentral and trustful authorization process can be provided by means of the peer-to-peer application
10 without the need of a central server or the like.

Further, a user can participate in the traffic system by having a peer-to-peer module in the vehicle or connected to the vehicle. It is also possible that a user participates by using a mobile terminal. In addition – and in order to enable a discriminatory free
15 service – a user can participate by registering as a user or a vehicle at web service or at a stationary terminal (e.g. stationary toll terminal). The central system of the web service or the stationary terminal (or its back-end system) may then be connected via a peer-to-peer module to the peer-to-peer application. The user may register via its identification or the identification of his vehicle. The user may do a pre-payment in a
20 (crypto-)currency to use the service. A peer-to-peer application detecting a vehicle that is not registered for a toll-labile service may send a message to a law enforcement unit including a proof (e.g. photo) stored in the peer-to-peer application.

According to a further embodiment, each entity (e.g. vehicle, mobile terminal,
25 predefined area, user, stationary terminal, existing back-end system, etc.) can be registered in the peer-to-peer application as e.g. a so called smart asset. According to an embodiment of the traffic system according to the present invention, a peer-to-peer module assigned to an entity may be configured to cause a registration of the entity (or peer-to-peer module) in the peer-to-peer application by transmitting a
30 registering message comprising at least an identification assigned to the entity. The identification might be already a peer-to-peer application identification or another

identification suitable to uniquely identify the entity, such as a serial number of e.g. the vehicle, number plate of a vehicle, an RFID transponder (another identification that can be read out via optical or electromagnetic waves), the user's name, a communication address of a communications device, etc. In e.g. the case of a name of the user, the peer-to-peer application may be configured to generate a unique peer-to-peer identification for the vehicle and/or user and/or any other entity involved in the traffic system. In particular, the peer-to-peer application may register the respective entities by storing at least the peer-to-peer identification in the peer-to-peer application or a database controlled by the peer-to-peer application.

Prior to the registration of a vehicle or other entity, at least part of the peers of the peer-to-peer network may check whether the registering requirements predefined by the peer-to-peer network are met by the entity requesting registration. In order to perform the check, preferably, further data may be included in the registering message. In particular, the peers of the peer-to-peer network may provide registering rules or registering requirements which must be fulfilled by an entity to be regarded as a trustful entity. By way of example, each entity to be registered must comprise an account and/or a particular amount of a cryptocurrency. Other rules/requirements may be individually defined by the peers of a peer-to-peer network. E.g. it may be necessary that a new entity must be recommended by an entity which is already a participant of the peer-to-peer network. In addition, it may be necessary that this participant must have a reputation factor which increases a predefined minimum reputation factor. Furthermore, a reputation factor can be calculated e.g. by way of algorithms (e.g. by using parameters, such as user or vehicle location, law enforcement, licensing, motion/behaviour parameters/data, to calculate a reputation score). It shall be understood that the reputation score can be used to determine (user-/vehicle specific) pricing data within the traffic system.

Furthermore, it may be advantageous if in the registering process also further e.g. technical details of the vehicle, predefined area, and/or user terminal can be stored together with the respective peer-to-peer identification in the peer-to-peer

application or the database accessible by the peer-to-peer application. Example of technical details may be a maximum parking capacity of a predefined area, dimensions of the at least one parking space, dimensions of the vehicle, type of motor of the vehicle, a provided electrical charging station, etc. Since the peer-to-peer application provides respective technical details, a vehicle can select a predefined area having at least one parking space which is particular suitable for the vehicle.

Furthermore, a communication module of a vehicle can be shared for the purpose of the peer-to-peer application and/or other car communication application(s). The communication module can be part of other components in the car and connected to the peer-to-peer module. Communication networks can be mobile data communication networks or Car-to-Car communication and/or meshed networks.

The peer-to-peer application may provide a peer-to-peer communication capability. This means nodes in a network can directly communicate with each other (e.g. via signed and/or encrypted direct messages). Movement, location and environmental data can be shared via the peer-to-peer application. This means vehicle(s) and its (their) respective peer-to-peer module(s) may know which other vehicle(s) is(are) in its(their) direct surroundings. In case of an emergency or malfunction a vehicle can directly communicate via signed/encrypted messages to its surrounding vehicle(s) in order to trigger collision prevention or emergency response action(s). For example a status of a broken braking system of a vehicle can be shared in a secure way and surrounding vehicles might trigger response actions to prevent a further collision. Another example is that a "collision prevention" module or a "foreign object identification" module may identify physical objects, humans or animals on a traffic way or on a collision path. It may trigger an emergency response that is shared with surroundings vehicles to ensure they react accordingly (and in advance). With such a traffic system a secure way to exchange messages via a peer-to-peer communication is established and manipulation of communication data can be avoided.

Real-time traffic jam, foreign object or traffic way damage/congestion data can be shared via the peer-to-peer application with other entities and used for traffic re-routing, further optimisation of traffic routes.

- 5 In addition, traffic way environmental data can be used for improving of a geo database or traffic way data base (e.g. road damages). Traffic way database may be used to prioritise and trigger traffic way maintenance actions. A peer-to-peer application may store geo data and traffic way data into decentral file storage or decentral database or a cloud database. Geo data may be used for traffic control,
10 navigation or other geo service purposes.

According to a further embodiment, the peer-to-peer application may comprise a reputation store and/or may be configured to access a reputation store. The reputation store comprises at least the peer-to-peer identification of at least one of a
15 registered vehicle and/or other entity together with a reputation factor assigned to the respective vehicle and/or other entity. The peer-to-peer application may be configured to update the at least one reputation factor based on a validation result, preferably a plurality of validation results. For instance, a conducted traffic action can be analyzed by the peer-to-peer network and used for updating reputation factors. For
20 instance, if a traffic action was performed correctly, a reputation factor can be increased while a reputation factor can be reduced if issues occurred in connection with a traffic action. In addition, further information, such as feedback data about the satisfaction of the entities involved in a traffic action, can be provided by at least one peer-to-peer module to the peer-to-peer application. Also this data can be used for
25 adapting reputation factors.

The reputation system can be provided by the peer-to-peer application to preferably all participants of the peer-to-peer network. A vehicle and/or a provider of a vehicle, tool-labile route, access to public or private areas, and/or a parking space can select
30 authorized vehicles based on the (current) reputation factor assigned to the vehicles.

According to a further embodiment, the at least one peer-to-peer application can be a decentralized register or a shared database storing transaction and data with given certain proofs or signatures. In addition to transactions and data, the decentral register can store computer code acting as e.g. means for evaluating or sending data.

- 5 In particular, the code can be invoked by a transaction to the address of the code in so called 'smart contracts'. This code is processed on the nodes of decentral register.

- 10 A decentralized register can be readable at least by a part of the participants of the peer-to-peer network. In particular, every computer node including e.g. the at least one peer-to-peer module assigned to vehicle can comprise the peer-to-peer application. The decentralized register may be read at least by each participant of the peer-to-peer network. In particular, all peer-to-peer modules and all other computers of the peer-to-peer network can preferably read all information in the peer-to-peer application formed as a register. Preference is also that all peer-to-peer modules and
- 15 all other computers of the peer-to-peer network can send messages to or write messages to the peer-to-peer application. A message or transaction sent to a smart contract will start the execution of the code of the smart contract while using data stored in the smart contract.

- 20 The peer-to-peer application can be built upon the following elements: PEER-TO-PEER network, Consensus System / Protocol, Data Structure, Merkle Trees, Public Key Signatures, Byzantine Fault Tolerance. It replicates data based on a consensus principle. It is auditable and traceable.

- 25 In a simple way information can be made available to preferably all participants. This allows to carry out a review of the information stored in the decentral register or the code executed in the decentral register. Particularly preferably, each computer in the peer-to-peer network can be configured to review new information, in particular based on older information stored in the peer-to-peer application.

Moreover, preferably each computer can in each case comprise the complete data content, but include at least a portion of the data contents of the peer-to-peer application, in particular of the decentral register. For example, it may be provided that after a positive verification of written information in the peer-to-peer application this information is saved by all computers, at least by a part of the computers. The tamper resistance of the data stored in the peer-to-peer application can thereby be further improved.

In order to store new information in a tamper-proof way, the peer-to-peer application can comprise encryption means and/or signature means and/or verification means, wherein at least one of the encryption means and/or signature means and/or verification means is configured to store data, such as motion parameter(s) and/or traffic information. In particular, it can be provided that by the hash function a link is established with at least one previously stored information in the decentral register. Further data, such as request messages, ordinary, contextual and/or transaction data of an entity, such as a vehicle, can be stored.

The peer-to-peer application may be formed by a Directed Acyclic Graph (DAG). A directed acyclic graph, such as IOTA or Tangle, means that blocks (or nodes of the graph) are coupled to each other via directed edges. Thereby, direct means that the (all) edges have (always) a same direction similar to time. In other words, it is not possible to step back. Eventually, acyclic means that loops do not exist.

In a particularly preferred embodiment of the present system, the peer-to-peer application can be a block chain or decentral ledger comprising at least two blocks coupled to each other (e.g. Ethereum Block chain with Smart Contracts). The block chain technology or "decentral ledger technology" is already used in the payment by means of a crypto currency, such as Bitcoin. It has been recognized that by a particular configuration of a block chain, at least the correctness of a received or provided data can be checked without the need of a central server. In addition, the block chain can be used to generate a release information caused by at least the peer-to-peer module in a

tamper-proof manner. The block chain according to the present embodiment is particularly a decentralized, peer-to-peer-based register in which all data related to a traffic action and other messages sent by peer-to-peer modules can be logged. A block chain is particularly suitable as a technical means to replace a central entity/server in
5 a simple and secure manner.

In alternative embodiments of the peer-to-peer application the block chain can be a permissionless or permissioned block chain. In a specific case the block chain can be public, consortium or private block chain.

10

In a further embodiment the peer-to-peer application can be formed by multiple block chains which are connected via mechanisms such as side chains or smart contracts.

15

Data of the peer-to-peer application can be stored on the "decentral ledger technology" and/or the decentral ledger steers (encrypted) data storage accessible via the internet and preferably in de-central data storage entity such as Interplanetary File System (IPFS) or in a distributed Blockchain database (e.g. BigChainDB). Access to the encrypted data to third party entities is managed via identity and access management transactions or smart contracts via the block chain.

20

In addition, data feeds can be provided by the peer-to-peer application (so called "smart oracles", e.g. information about prices, weather, etc.). Data can be captured from trusted sources off-chain and stored on the block chain or stored via the block chain on a decentral data storage entity.

25

Information among peer-nodes can be exchanged by a peer-to-peer messaging system. This means a peer node can send a message to another peer node to submit an information or to trigger an action. Messages can be clear text, signed and / or encrypted. This means that not all data exchanged among peer nodes must be stored
30 on the block chain.

In a further embodiment, the at least one peer-to-peer network can be formed by a plurality of computer nodes and a peer-to-peer module, such as the peer-to-peer module of a vehicle or a peer-to-peer module of a mobile terminal, etc., is only configured to communicate with the plurality of computer nodes. In other words, the peer-to-peer module is not a computer node of the peer-to-peer network but only a participant. Such a peer-to-peer module does not comprise the peer-to-peer application but only provides an interface module, such as an application programming interface (API), and a decentral application for communication with the computer nodes of the peer-to-peer network or the peer-to-peer application, such as a block chain or a smart contract on the block chain. For instance, such a peer-to-peer module can either send clear text or encrypted information or generate a secure connection (e.g. tunnel) to a peer-to-peer gateway (or so called "remote node") in order to communicate with the peer-to-peer network. This allows reducing the required processing power of the peer-to-peer module.

In one implementation of the peer-to-peer network there can be only one validating peer or full node, e.g. only one node can be configured to perform a validation process, and one or more observing nodes. An observing node can validate transactions to establish a trust level but does not validate all transactions which is done by the validating peer.

In an alternative embodiment, the peer-to-peer module is one of the computer nodes. In this case, the peer-to-peer module comprises at least a part of the peer-to-peer application. In particular, the peer-to-peer module can comprise preferably the total data content of the peer-to-peer application or can access the information stored in another node. For instance, the peer-to-peer module might be a so called "light node" or a decentral application (DAPP) connected to a remote node.

It is noted that in the present case, according to an embodiment, the peer-to-peer module comprises at least an API configured to communicate with the peer-to-peer application, such as the block chain. In addition to the API, the peer-to-peer module

comprises a decentral application of software comprising local algorithms at least configured to create and transmit data, transactions or the measured quantity parameter to the peer-to-peer application via the API. The decentral application so called "Dapp" is at least configured to process and transmit the meter data.

5

Preferably, the data is signed or encrypted or can be transmitted via a cryptographically secured tunnel or a secured internet connection to a peer-to-peer node running the peer-to-peer application, such as the block chain. In another particular embodiment, also the peer-to-peer application itself is implemented in the peer-to-peer module, i.e. the peer-to-peer module is a node of the peer-to-peer network comprising the decentral application, the API and the peer-to-peer application, such as the block chain or decentral ledger.

10

Further processing of data, such as evaluating at least one motion parameter, can be done on-chain or off-chain. Off-chain data processing, evaluating and/or validation can be managed by the peer-to-peer application, like the code on the block chain. Powerful means in particular a high computing power. In other words, in the present case a valid entry in the peer-to-peer application, such as a block chain, is assumed if (only) a part of the peers comes to a positive result. It shall be understood that only a single, especially particularly powerful peer can perform the processing or validation process. In an alternative embodiment the block chain may delegate computing tasks to one or more resources. It either trusts one resource or it applies a consensus principle while delegating similar processing tasks to many resources.

15

20

Data and transactions stored on the block chain do not provide "transactional privacy". Transactions between pseudonyms may be (often) stored in clear text on the block chain. In some cases data stored on the block chain are encrypted and the keys may be handled via the block chain. Privacy preserving, secure transactions or execution of computer code can be achieved with cryptographic tools such as zero knowledge (zk) proofs or zk Succinct Non-interactive Arguments (zk-SNARK). Transactions or algorithms are separated into two parts: a smart contract on the block

25

30

chain and a private contract. A privacy preserving protocol ensures the privacy of data and the correctness of code execution (SNARK verification is done via the smart contract on chain). The private contract computation can be done by a set of nodes, off-chain computers or done in measured launch environment or a secure HW enclave for attestation and sealing that cannot be manipulated by other software code running on the devices. In an alternative embodiment secure Multi-Party-Computing (sMPC) systems can be used for transactional privacy. Examples for privacy preserving protocols and computation are HAWK and MIT Enigma.

10 With zero knowledge proof (zk Proofs) the parties can see that the algorithm is executed correctly in a private contract, but the input data are not disclosed to the party. In addition selective privacy can be achieved by sharing keys to decrypt transactions for reporting and auditing purposes.

15 Similarly, in an alternative (not shown) embodiment a particularly large peer-to-peer network may be divided in two or more (physical or logical or dynamically virtual) clusters. In a corresponding peer-to-peer network, for example, a validation (of a subset of transactions) may only be carried out by the members of one cluster (a subset of nodes; e.g. sharding of a block chain to improve the scalability). In a further embodiment the peer-to-peer application can be formed using multiple block chains. These block chains are connected via frameworks such as sidechains or smart contracts.

Financial values can be (instantaneously) exchanged with a transaction via a cryptocurrency. In an alternative embodiment micropayment channels are used for a constant payment stream that can be handled party off-chain to reduce the amount of on-chain transactions. In a further embodiment so called state channels or state networks (e.g. Raiden Network) may be used to exchange digital tokens off-chain in a secure way. Opening and/or closing of state channels may be registered on the block chain. This means that individual transactions may not be stored on the block chain in order to improve scalability and avoid movement tracking of pseudonyms on the

block chain. According to the present invention, a man-in-the-middle is not necessary. Fully automated processes from authentication to charging and billing can be provided.

- 5 In a further embodiment, at least one entity of the traffic system may have a digital wallet to exchange value in form of digital tokens and/or cryptocurrency.

- In a further embodiment, at least one financial and/or traffic system transaction among at least two entities, such as vehicles, toll, parking, access, sensors, actors or
10 law enforcement devices and/or users may be secured via at least one smart contract. A transaction may invoke the execution of the smart contract. With this transaction a deposit or escrow in form of a cryptocurrency may be stored in the smart contract by the entity that orders a product. The entity may send a signed confirmation to the smart contract when it has triggered or executes (e.g. entering a toll and/or access
15 area or parking space) the activity. The deposit may be sent to a unit or an entity of a traffic system when activities are performed as defined in the transaction agreement and/or it receives the signed confirmation message (or in accordance to any other payment conditions defined in the transaction agreement). At the end of a traffic journey (e.g. planned route or car sharing agreement or traffic way usage agreement)
20 all remaining funds may be sent back to the entity that provided the deposit. In case there are open EV car charging, maintenance, toll, parking, access or law enforcement activities parts or the full deposit will remain in the deposit until a defined time (defined in transaction agreement business logic). In addition payment condition(s) such as pre- or post-payments can be implemented in the smart contract logic as well.
25 Overall the smart contract provides a secure and transparent payment process with no middle man involved. In an alternative embodiment Micropayment Channels are used.

- 30 The peer-to-peer application can be connected to a central system (e.g. central system connected to a peer-to-peer module or a remote node). Central government or private

authorities can provide access, law enforcement or pricing parameters into the peer-to-peer application. Or the peer-to-peer application is connected with a central traffic system control or optimisation service that dynamically adjusts traffic system parameters or provides traffic control and route optimisation data.

5

In a further embodiment the vehicle data are shared with central or decentral maintenance applications.

A further aspect of the invention is a method. The method comprises:

- 10
- detecting at least one motion parameter relating to the vehicle, and
 - transmitting at least the detected motion parameter by at least one peer-to-peer module to at least one peer-to-peer application.

The method can be used for operating a previously described traffic system. The peer-to-peer module can be assigned to a vehicle and/or a sensor module configured to
15 detect the at least one motion parameter relating to at least one vehicle. For instance, vehicle data can be shared with a traffic or environmental control system.

A further aspect of the invention is an arrangement for a vehicle. The arrangement
20 comprises at least one sensor module configured to detect at least one motion parameter relating to the vehicle. The arrangement comprises at least one peer-to-peer module assigned to the vehicle and configured to communicate with at least one peer-to-peer application of at least one peer-to-peer network. The peer-to-peer module is configured to transmit at least the detected motion parameter to the peer-to-peer application and/or to receive at least traffic information data from the peer-to-peer application.
25

The arrangement can be formed by a single device including hardware and/or software modules. Such a single device can be integrated into a vehicle. Alternatively,
30 the arrangement can be formed by two or more separate components including

hardware and/or software modules. Some components may be already installed in a vehicle and connectable to the further installable components.

Furthermore, an aspect of the invention is a vehicle comprising at least one of the
5 previously described arrangement.

According to an embodiment of the vehicle, at least one peer-to-peer module assigned to the vehicle may be connected to the vehicle via an interface of the vehicle, in particular, via an on-board diagnostics connector of the vehicle.

10

A still further aspect of the invention is a further method. The method comprises:

- generating at least traffic information data by evaluating at least one motion parameter relating to at least one vehicle by means of at least one peer-to-peer application, and
- providing the generated traffic information data to at least one peer-to-peer module assigned to at least one vehicle.

15

The method can be realised as a computer program. The method can be performed by
20 at least one peer-to-peer application.

20

A further aspect of the invention is a peer-to-peer application. The peer-to-peer application comprises means for generating at least traffic information data by evaluating at least one motion parameter relating to at least one vehicle. The peer-to-peer application comprises means for providing the generated traffic information data to at least one peer-to-peer module assigned to at least one vehicle.

25

The means for generating and/or the means for providing may be preferably formed by code of one or more smart contracts.

30

The features of the methods, systems or networks, devices, units, arrangements, modules and computer programs can be freely combined with one another. In particular, features of the description and/or the dependent claims, even when the features of the dependent claims are completely or partially avoided, may be
5 independently inventive in isolation or freely combinable with one another.

These and other aspects of the present patent application become apparent from and will be elucidated with reference to the following figures. The features of the present application and of its exemplary embodiments as presented above are understood to
10 be disclosed also in all possible combinations with each other.

In the figures show:

- | | | |
|----|--------|---|
| 15 | Fig. 1 | a schematic view of an embodiment of a traffic system according to prior art, |
| | Fig. 2 | a schematic view of a first embodiment of a traffic system according to the present invention, |
| 20 | Fig. 3 | a schematic view of a further embodiment of a traffic system according to the present invention, |
| | Fig. 4 | a schematic view of a further embodiment of a traffic system according to the present invention, |
| 25 | Fig. 5 | a schematic view of an embodiment of a peer-to-peer application according to the present invention, |
| | Fig. 6 | a schematic view of a further embodiment of a traffic system according to the present invention, |
| 30 | | |

Fig. 7 a diagram of an embodiment of a method according to the present invention, and

Fig. 8 a diagram of a further embodiment of a method according to the present invention.

Like reference numerals in different figures indicate like elements.

Figure 2 shows a first embodiment of a traffic system 200 according to the present invention.

The traffic system 200 comprises at least one vehicle 202. Usually, the traffic system 200 comprises a plurality of vehicles. Exemplified vehicles are cars, trucks, ships, railway vehicles, planes, bicycles, drones, etc. In the following embodiments, aspects of the invention will be described in connection with a car. However, the statements made can be easily transferred to other kinds of vehicles.

The car 202 comprises a navigation module 214. The navigation module 214 may comprise a display unit configured to display traffic information data. Additionally or alternatively, traffic information data can be displayed using other user interfaces, such as loud speakers.

A substantial difference compared with prior art traffic systems, such as system 100 according to figure 1, is that no central instance is provided. In the present case, the traffic system 200 comprises a peer-to-peer network 222 or a computer-computer network 222. The peer-to-peer network 222 comprises a plurality of nodes 226.1, 226.2, 226.3 or computers 226.1, 226.2, 226.3. A peer-to-peer network 222 is characterized in the present case in that each node 226.1, 226.2, 226.3 and/or participant 228 is preferably connectable to every other node 226.1, 226.2, 226.3 and/or participant 228. For instance, at least one physical standard network can be

used for connection. For communicating via the at least one physical standard network, suitable transceiver modules may be arranged the respective entities.

5 In addition, the computers 226.1, 226.2, 226.3 have equal rights, something which distinguishes them from a server-client structure.

The depicted nodes 226.1, 226.2, 226.3 (each) comprise a peer-to-peer application 224. As can be seen from figure 2, the same peer-to-peer application 224 is preferably implemented on each node 226.1, 226.2, 226.3. The peer-to-peer application 224 may
10 preferably be a public register 224 that can, in particular, be inspected by all participants 226.1, 226.2, 226.3, 228 (not only the nodes 226.1, 226.2, 226.3) of the peer-to-peer network 222. Each node 226.1, 226.2, 226.3 preferably has the (entire) public register 224. It may also be envisaged that only part of the register can be provided on a node (light node). In a particularly preferred embodiment, the peer-to-
15 peer application 224 may be a block chain 224 which will be explained in more details hereinafter.

In addition, it can be seen from figure 2 that in the present embodiment the at least one car 202 comprises an arrangement 230 with a peer-to-peer module 228 and a
20 sensor module 221. Preferably, the peer-to-peer module 228 and a sensor module 221 assigned to the car 202 can be fixedly integrated in the car 202. In other variants, at least parts of the modules 221, 228 can be formed as separate units.

A peer-to-peer module 228 is (generally) configured to communicate at least with the
25 peer-to-peer network 222, i.e. the nodes 226.1 to 226.3 of the peer-to-peer network 222. In other words, the peer-to-peer module 228 or the car/entity 202 corresponding or assigned to the respective peer-to-peer module 228 is at least a participant of the peer-to-peer network 222.

30 It shall be understood that a communication module in a car can be shared for the purpose of the peer-to-peer application and/or other car communication applications.

The communication module can be part of other components in the car and connected to the peer-to-peer module. Communication networks can be mobile data communication networks or Car-to-Car communication and/or meshed networks.

- 5 Protocols for the communication modules and firmware for other modules can be deployed in a secure way using the peer-to-peer application. These protocols can for example define a quality of service for prioritising emergency data (e.g. for collision prevention). Therefore it may be important that communication protocols and
10 firmware upgrades for other component are deployed in a secure way in order to guarantee proper working of system effecting health and security of vehicles and users.

In the case of Car-to-Car communication access to the internet can be shared among many cars. The car that provides the access may be incentivised via the mean of
15 cryptocurrency.

Preferably, all participants 226.1, 226.2, 226.3, 228 (including all nodes) of the peer-to-peer network 222 are known to each participant 226.1, 226.2, 226.3, 228 of the peer-to-peer network 222.

20

In the present case, the at least one peer-to-peer module 228 is not a node of the peer-to-peer network 222 but only a participant 228. While the nodes 226.1, 226.2, 226.3 or computers 226.1, 226.2, 226.3 in the peer-to-peer network 222 comprise at least a part of the peer-to-peer application 224 a participant of a peer-to-peer network, like
25 the present peer-to-peer module 228, does not comprise the peer-to-peer application 224. Such a peer-to-peer module 228 is configured to provide access to the peer-to-peer application 224 e.g. via an API. Each peer-to-peer module (also a node) may comprise a decentral application and at least an API. In the case, the peer-to-peer module is formed as a node the peer-to-peer module (also) comprises at least partly
30 the peer-to-peer application 224.

The peer-to-peer module 228 may comprise a communication connection to the sensor module 221 and/or the navigation module 214. The sensor module 221 may be configured to sense or detect at least one motion parameter (or environmental parameter) relating to the vehicle 202. By way of example, the sensor module 221 may comprise a sensor (e.g. already implemented in the car 202) for sensing the current velocity of the car 202. Alternatively or preferably, additionally, the sensor module 221 comprises a location sensor, in particular, a satellite positioning sensor, (e.g. already implemented in the car 202) configured to detect the current location of the car 202. Further movement parameters can be directly and/or indirectly detected e.g. by detecting further state parameters of the car, such as a state parameter of a component (e.g. active state of the motor or inactive state of the motor, system status or technical component data). From an inactive state it can be followed that the car 202 is currently not moving.

The sensor module 221 is configured to provide at least one of the above mentioned motion parameters relating to the car 202 to the peer-to-peer module 228. Preferably, the sensor module 221 can at least provide the current location of the car 202 and the current velocity of the car 202 to the peer-to-peer module 228. The peer-to-peer module 228 may provide the at least one motion parameter value to the peer-to-peer application 224 e.g. by transmitting or writing said data to the peer-to-peer application 224. By providing said data to the peer-to-peer application 224 e.g. the current traffic situation can be monitored and evaluated by the peer-to-peer application 224 or by an algorithm (running maybe off-chain) that is controlled by the PEER-TO-PEER application.

Alternatively or additionally, the peer-to-peer application 224 is configured to provide traffic information data to the peer-to-peer module 228 of the car 202. This traffic information data may comprise an optimized route for arriving at a particular destination. In order to provide the optimized route, the navigation module 214 may provide the set destination of the car 202 to the peer-to-peer module 228. The peer-to-peer module 228 may forward this destination to the peer-to-peer application 224.

The peer-to-peer application may comprise means to determine an optimal route based on the set destination, movement parameters of this and further vehicles and/or further traffic status information, such as current traffic jams, closed roads, usage restrictions, and the like. Such further traffic status information can be provided
5 by the peer-to-peer application e.g. using decentral or central data feeds and/or traffic optimization algorithm(s) (running maybe off-chain) that are controlled by the peer-to-peer application 224.

In a further embodiment, the peer-to-peer application may provide data to a vehicle
10 about allowed or restricted ground, water or air traffic ways (e.g. allowed air traffic corridors for drone movements). Breaches can be penalised by the peer-to-peer application. In case of breaches an emergency control logic module (not shown) can take over control of a vehicle to bring it back into the allowed traffic ways or an automatic message is sent to one or more law and/or traffic way enforcement unit(s).
15 Control logic can be agreed in advance in an access transaction agreement. Allowed and restricted areas can be defined by governmental or private parties. Allowed and restricted area data, control logic can be stored in the peer-to-peer application.

It shall be understood that according to other variants, the peer-to-peer application
20 224 provides traffic status information to the peer-to-peer module 228. In this case the navigation module 214 may be configured to determine the optimal route based on the set destination and the provided traffic status information on its own.

Figure 3 shows a further embodiment of a traffic system 300 according to the present
25 invention. The depicted system 300 comprises two cars 302, 304. Each of these cars 302, 304 comprises an arrangement 330 with a peer-to-peer module 328 and a sensor module 321.

Furthermore, each of the peer-to-peer modules 328 is a participant 328 of the peer-to-
30 peer network 322. By way of example, the peer-to-peer network 322 comprises two nodes 326.1, 326.2 each comprising the peer-to-peer application 324.

As can be seen from figure 3, two predefined geographic areas 332.1, 332.2 are provided. Such an area 332.1, 332.2 may be defined by location parameters, such as coordinate parameters (e.g. latitude, longitude and/or elevation parameters) of a specific geographic coordinate system. In particular, a geographic area 332.1, 332.2 may be defined by its outer boundaries 331, 332 and their location parameter values, respectively. The respective data of said predefined geographic areas 332.1, 332.2 can be stored in the peer-to-peer application 324 and/or a database controlled by the peer-to-peer application 324.

In a predefined area 332.1, 332.2, at least one parking space may be provided. It may be possible that a predefined area 332.1, 332.2 comprises only one parking space. It may be possible that there is a plurality of predefined areas comprising one or more parking space(s). The parking space may be provided/offered by an owner of the parking place. Access to the parking space may be provided via an access transaction agreement (which can be part of the parking transaction agreement). The providence of a parking space may be associated with a parking transaction criterion, as will be described in more details hereinafter. Thereby, the parking transaction criterion of the first predefined area 332.1 may be different from the parking transaction criterion of the further predefined area 332.2. These data may be stored in the peer-to-peer application and/or a file storage, such as a decentral file storage system, controlled by the peer-to-peer network 324.

The sensor module 321 of a car 302, 304 is configured to detect at least the current location of the car 302, 304 and the current velocity of the car 302, 304 and/or the current state of the motor of the car 302, 304. For instance, the current location can be detected using a satellite positioning system 310, such as GPS or Galileo System. A satellite positioning sensor may communicate with the satellites of the satellite positioning system 310 via a specific communication channel 320.

The current values of these motion parameters can be transmitted by the peer-to-peer module 328 to the peer-to-peer application 324. The peer-to-peer application 324 comprises means to evaluate the provided data. In particular, the peer-to-peer application 324 comprises means configured to detect whether a car is in a parking state/condition within a predefined area 332.1, 332.2.

For instance, the peer-to-peer application can comprise means or can access to means which are configured to evaluate the provided current location parameter(s) by comparing said value(s) with the stored location parameter value(s) of the one or more predefined area(s) 332.1, 332.2. As a result of the comparison process it can be determined whether a car 302, 304 is within a predefined area 332.1, 332.2 or not.

Further, the velocity data and/or motor state data of the car 302, 304 can be evaluated by the peer-to-peer application 324. In one embodiment, the current velocity value of a car 302, 304 can be evaluated by comparing said value with other velocity values of vehicles which are (currently) located in a predefinable proximity to said car 302, 304. If e.g. all cars have the velocity $v = 0$, it can be followed that there is a traffic jam. On the other hand, if the other cars have a velocity $v > 0$, it can be followed that the car 302 is in a parking state. It shall be understood that it can be checked whether the velocity is $v=0$ for a predefined duration (e.g. 1 min or the like) or whether the user has left the car (user detection module or vehicle alarm system detecting human objects in a vehicle).

Additionally or alternatively, the motor state of the car 302, 304 can be checked by the peer-to-peer application 324. If the motor state is "inactive", it can be followed that the car 302, 304 is in a parking state. On the other hand, if the motor state is "active", it can be followed that the car 302, 304 is still in a driving state.

Preferably, the peer-to-peer application and/or the car 302, 304 may measure the duration of the parking state of the car 302, 304 within a predefined area 332.1, 332.2. Based on the actual duration and at least one parking transaction criterion, a parking

transaction can be conducted by means of the peer-to-peer application, as it will be described in more details in the following. In particular, the sensor module 321 and the peer-to-peer application can measure the time in order to verify whether the duration was correctly measured.

5

Further, the above motion parameter(s) may be detected by a sensor module 321 and/or transmitted from a peer-to-peer module 328 (almost) continuously, regularly or at predefinable time points. For example, a transmission can be initiated each time the motor is activated. Then, data, such as the current location and the duration of the inactive motor state can be transmitted to the peer-to-peer application 324. Based on these values, a parking criterion transaction can be initiated by the peer-to-peer application 324

10

According to other variants, the location sensor may be configured to detect marking units located at the predefined areas. The marking units are arranged in order to define said predefined areas. For instance, electromagnetic marking units configured to send an electromagnetic field having a predefined range (corresponding to the predefined area) and an unique field identification can be provided. The location sensor of a car may be configured to sense such a field. The read field identification may be transmitted by the peer-to-peer module to the peer-to-peer application in order to determine the current location of the car, in particular, the predefined area corresponding to the detected field identification.

15

20

Figure 4 shows a further embodiment of a traffic system 400 according to the present invention. The traffic system 400 comprises a peer-to-peer network 422 with two depicted nodes 426.1, 426.2 wherein each of the nodes 426.1, 426.2 comprises the peer-to-peer application 424. As can be seen from figure 4, in the present embodiment the peer-to-peer module 426.2 of the car 402 is formed as a node 426.2.

25

Besides a sensor module 421, the present car 402 comprises a locking module 436 and a first interface module 438. The locking module 436 comprises at least a

30

communication connection with the peer-to-peer module 426.2 and/or the first interface module 438. The first interface module 438 may also comprise a communication connection with the peer-to-peer module 426.2.

- 5 The locking module 436 may be configured to lock an access unit, such as a car door, of the car 402. In addition, it may lock the activation of the motor of the car 402. The access unit and/or the activation of the motor of the car 402 may be released if the locking module 436 receives a release information preferably provided by the peer-to-peer application 424.

10

Furthermore, the present system 400 comprises a user terminal 440, such as a mobile phone, tablet computer, notebook, smart card, portable navigation device, etc. In the present embodiment, it will be assumed that the user terminal 440 is a (conventional) mobile phone 440. Said mobile phone 440 comprises at least one further interface
15 module 442 configured to communicate with the first interface module 438. For example, the interface modules 442, 438 may be configured to establish a nearfield connection, such as a RFID connection, Bluetooth connection, infrared connection and/or the like.

- 20 In addition, the depicted mobile phone 440 comprises a peer-to-peer module 428. The peer-to-peer module 428 may be a software module installable on the mobile phone 440.

- By way of example, in a generated car sharing agreement, the identification of an user
25 authorized to use car 402 and an identification of the car 402 can be stored. By using the mobile terminal 440, a nearfield communication between the respective interface modules 442 and 438 can be established in order to transmit the identification of the user to the peer-to-peer module 426.2 of the car 402. The received identification and the identification of the car 402 can be written to the peer-to-peer application by the
30 peer-to-peer module 426.2. After a positive verification of the identifications e.g. by comparing said identifications with the stored identifications, generating means of the

peer-to-peer module can generate traffic information data in form of a release information. After receipt of this release information by the locking unit 436, the access unit and/or the activation of the motor of the car 402 may be released.

- 5 After the car sharing action, a car sharing criterion transaction can be performed. E.g. an agreed amount of cryptocurrency can be transferred from an account of the user to an account of the provider of the car 402. It shall be understood that when a sharing transaction agreement is initiated the user may put a defined amount of
- 10 cryptocurrency into a deposit to ensure security of the financial transaction including car sharing, maintenance and insurance. In a further embodiment, the usage of a vehicle can be paid for with Micropayment Channels. The sharing transaction agreement may define minimum usage units (e.g. usage per second). Micropayments can be streamed to the vehicle and/or its owner per each minimum usage unit. In case micropayment transactions stop, operations of the vehicle can be stopped accordingly
- 15 (considering health and/or safety requirements for when stopping the vehicle).

Figure 5 shows a schematic view of an embodiment of a peer-to-peer application 524 according to the present invention.

- 20 The depicted peer-to-peer application 524 is a register readable, in particular, by the participants of the peer-to-peer network. Thereby, data e.g. in form of messages can be written and/or read into/from the register 524 by a peer-to-peer module of a vehicle/entity and/or any other participants in the peer-to-peer network. In a preferred embodiment, the peer-to-peer application 524 may be a block chain 524.

25

- Hereinafter, it is assumed in the following description of the present embodiment that the at least one peer-to-peer application 524 is a block chain 524. However, the following remarks can be easily transferred to other peer-to-peer applications, such as a Directed Acyclic Graph (DAG). A directed acyclic graph, such as IOTA or Tangle,
- 30 means that blocks (or nodes of the graph) are coupled to each other via directed edges. Thereby, direct means that the (all) edges have (always) a same direction

similar to time. In other words, it is not possible to step back. Eventually, acyclic means that loops do not exist.

5 In alternative embodiments of the peer-to-peer application the block chain can be a permissionless or permissioned block chain. In a specific case the block chain can be public, consortium or private block chain. Or it can be a combination of block chains.

10 In a further embodiment, the peer-to-peer application can be formed with multiple block chains which are connected via mechanisms such as side chains or smart contracts.

The block chain 524 is formed by at least one block 551, 553, 555, preferably by a plurality of interconnected blocks 551, 553, 555. The first block 551 may also be called genesis block 551. As can be seen, a block 553, 555 (except for the first block 15 551) refers to each previous block 551, 553. A new block can be created by a computationally intensive process (for example, so called "mining" or through another appropriate process, such as voting) and will be particularly provided to all participants of the peer-to-peer network.

20 The present block chain 524 is particularly adapted to receive data/messages from a peer-to-peer module of a previously described vehicle and/or user terminal and/or from another peer-to-peer device/unit of another participant of the peer-to-peer network. Further, block chain 524 is particularly adapted to save these data/messages in the block chain 524. Furthermore, the block chain 524 is configured to generate 25 data/messages e.g. based on a validation process and/or caused by a peer-to-peer module.

In particular, a (newly) received message can be saved and published in the current block 555 of the block chain 524. Due to the configuration of a block chain 524 as a 30 public register 524, said data message of e.g. a peer-to-peer module of a vehicle can be

read by preferably all participants of the peer-to-peer network and/or data of the message will be stored on decentral file service or distributed block chain database.

5 In the present block chain 524 different types of messages and data, respectively, for example, within a smart contract (algorithm and/or storage at the block chain 524) can be processed and/or stored. By way of example, the message 570 comprises a generated parking transaction agreement 570.

10 A parking transaction agreement 570 can be e.g. generated between an user of a vehicle and a provider of a predefined geographic area having one or more parking places. An example of a generation of such a parking transaction agreement 570 will be described in the following:

A parking transaction agreement 570 may comprise the following data:

15

Identification(s): Identification assigned to vehicle or user of vehicle and/or identification assigned to predefined area (or parking space) or provider of said area

20

Parking criterion: criterion that must be fulfilled by vehicle/user of vehicle for conducting the parking action

The parking criterion may be e.g. an amount of cryptocurrency e.g. per time unit which has to be transferred e.g. after a parking action (e.g. from the user of the vehicle to the provider of the parking space). The parking criterion may be a dynamic
25 criterion. E.g. an amount can range between a maximum value and a minimum value depending on e.g. parking duration of a vehicle, start (and/or end) parking time, vehicle dimensions, vehicle type, a reputation factor, etc. Preferably, at least a part of the agreed amount of cryptocurrency can be locked by the peer-to-peer application 524 prior to the parking action. It shall be understood that other transaction criteria
30 and further information can be included in a parking transaction agreement. More information/criteria can be, for example, a time stamp, geographic coordinates about

the predefined area, an ID of the transaction and other criteria, such as an indication of the motor type (electromotor), a provided electrical charging station, etc.

A parking transaction agreement 570 may be valid for only one parking action, a predefined plurality of parking actions or unlimited number of parking actions. The latter case may be a general parking transaction agreement 570. A general parking transaction agreement 570 may be generated during a registration process of an entity for e.g. a specific parking action peer-to-peer network configured to control parking actions.

In order to generate a parking transaction agreement 570, a peer-to-peer module of a computing device of a provider or user of the vehicle (e.g. the peer-to-peer module assigned to a car) can exchange parking request and response (acceptance) messages via the peer-to-peer application. A request message may comprise indications about the above data (identifications, transaction criteria).

For instance, a provider of a predefined area with one or more parking spaces can send by a peer-to-peer module a message 566 to the peer-to-peer application 524 comprising data, such as an identification assigned to the provider, geographic coordinates of the predefined area and/or at least one parking transaction criterion.

Another message 568 may be an acceptance message 568. An acceptance message 568 may comprise identical or at least similar data details as compared with a request message 566. Additionally, the acceptance message 568 can comprise a reference indication to a previous request, such as the ID of the request message 566.

If, for example, the acceptance message 568 comprises a higher or other transaction criterion, the acceptance message 568 can be called a counter-offer message. This can be accepted by the peer-to-peer module of the requester through an acceptance message. Based on this a peer-to-peer module (e.g. of the computing device of the requester) may cause the generation of a parking transaction agreement 570.

In particular, there can be multiple request messages and/or accepting messages and/or messages comprising a requested parking space for different transaction criteria. Each entity can give guidelines, according to which at least one parking transaction agreement or other agreements can be generated. In a preferably automated, such as iterative process, each request message can be associated to an optimally corresponding acceptance message. The block chain 524 may also be configured to generate, based on the messages of a peer-to-peer module, a parking transaction agreement 570.

Another message may be a toll transaction agreement 572 or a vehicle sharing transaction agreement 574 or an access transaction agreement 576 or a law enforcement transaction agreement 578 or a data sharing agreement 580. A toll transaction agreement 572 may comprise following indications.

Identification of the toll route:	identification, such as a name, coordinates, etc. of the one or more toll routes
Toll criterion	criterion which must be fulfilled for using at least part of at least one toll route

The toll transaction agreement 572 may be generated in a similar manner as a parking transaction agreement. As described above, the toll criterion may be a dynamic criterion.

A vehicle sharing transaction agreement can comprise the following details:

Identifications of involved entities:	identification assigned to a user and an identification assigned to the involved vehicle
Vehicle sharing criterion	criterion which must be fulfilled for using said vehicle and terms and conditions for car sharing pricing

A access transaction agreement 576 can comprise the following details:

5	Identification of access area:	identification, such as a name, coordinates, etc. of the one or more access areas
	Access criterion	criterion which must be fulfilled for using at least part of at least one access area
10	Emergency Logic	emergency logic for the case that a vehicle leaves allowed traffic ways and/or enters a restricted area.

A law enforcement transaction agreement 578 can comprise the following details:

15	Identification of access area:	identification, such as a name, coordinates, etc. of the one or more traffic ways
	Law enforcement criterion	criterion defining the traffic laws and penalties if a vehicle or user breaches them

20 It shall be understood that a law enforcement transaction agreement can be agreed in
advance and in combination with a vehicle sharing, toll, access or parking transaction
agreement.

25 A data sharing transaction agreement for providing movement and environmental
data in order to analyze and/or optimize the traffic system or optimize the route of a
vehicle can comprise the following details:

30	Identification of shared data:	identification of movement and environmental data to be sent by the vehicle and/or data received by the vehicle (traffic system data, differential GPS data, etc.)
----	--------------------------------	---

- Shared data criterion (send) criterion which must be fulfilled for using the vehicle data by an analysis or optimization system (e.g. system pays for gathering the data via the vehicle)
- 5 Shared data criterion (receive) criterion which must be fulfilled for any analysis or optimization system service (e.g. vehicle pays for traffic, route optimization or least cost routing data)
- 10 A vehicle logbook transaction agreement 580 can comprise the following details:
- Identification(s): identification assigned to vehicle or user of vehicle and/or identification assigned to data store (logbook) and/or identities assigned to entities entitled to monitor logbook entries
- 15 Logbook sensor: identification of the sensor(s), data format(s) and protocol(s) to exchange data
- Logbook service: Logbook analytics provided by the peer-to-peer application
- 20 A vehicle autonomous driving transaction agreement 582 can comprise the following details:
- Identification(s): identification assigned to vehicle or user of vehicle and/or identification assigned to predefined autonomous driving service or vehicles in the surroundings
- 25 Sensor and/or actor data identification(s) of the sensor(s) and/or actor(s) involved, data format(s) and/or protocol(s) to exchange data
- 30

Autonomous driving services: Analytics provided by the peer-to-peer application and/or by vehicles in the surroundings

- 5 Data will be stored either on the block chain, in a decentral file system (IPFS) or in a distributed block chain database (BigchainDB) or a cloud database.

It shall be noted that separate peer-to-peer applications, such as two or more block chains can exist for different traffic systems, such as a parking system, a vehicle
10 sharing system, an access system, a law enforcement system, a traffic control system, a data sharing system and/or a toll system.

Preferably, at least the above described messages, such as the agreements and other messages, can be hashed together in pairs in a block of the block chain by a Merkle
15 tree. In particular, only the last hash value, the so-called root hash, is noted as a checksum in the header of a block. Then, the block can be coupled with the previous block. Chaining of the blocks can be performed using this root hashes. Each block can include the hash of the entire previous block header in its header. This makes it possible to clearly define the order of the blocks. In addition, this may also prevent the
20 subsequent modification of previous blocks and the messages stored in the previous blocks, since, in particular, the hashes of all subsequent blocks would have to be recalculated in a short time.

In addition, data feeds can be provided by the peer-to-peer application (so called
25 smart oracles, e.g. information about current traffic situation).

Figure 6 shows a schematic view of another embodiment of a traffic system 600 of the invention. In the present embodiment only nodes and participants 602.2 to 648.2 of the peer-to-peer network 622 are shown. In the present example, it is assumed that all
30 nodes 602.2 to 648.2 comprise at least a part of the peer-to-peer application (not shown).

The nodes 602.2, 604.2, may be cars and the peer-to-peer modules of the cars (or mobile terminals or OBD adapters), respectively. The node 640.1 may be realized by a peer-to-peer module integrated in a user terminal. Node 643.2, 644.1 may be the peer-to-peer modules of other vehicles, such as a truck, train, and/or drone. Further nodes 646.1 and 648.2 may be computing devices, e.g. of owner of parking places and/or of vehicle sharing providers.

As can be seen, two different types of peers or node computers 640.1, 644.1, 646.1 and 602.2, 604.2, 643.2, 648.2 are presently illustrated. All peers 640.1, 644.1, 646.1 and 602.2, 604.2, 643.2, 648.2 are comprised by the peer-to-peer network 622. In the present embodiment, however, only a part of the peers 640.1, 644.1, 646.1 and 602.2, 604.2, 643.2, 648.2, in the present case, the peers 640.1, 644.1, 646.1, check the validity of the data stored in the peer-to-peer application messages, such as the motion parameter data, agreements, traffic information data, request messages, and the like. Furthermore, only a part of the entire peers can be configured to store the peer-to-peer application and/or only a part of the peers can be configured to execute the algorithms of a smart contract. Since the validation/verification of e.g. identification data requires a considerable computational effort, it may be advantageous for reasons of efficiency, if only a part of the peers 640.1, 644.1, 646.1, especially particularly powerful peers 640.1, 644.1, 646.1, perform the validation and/or optimization algorithms taking more complex pricing or the state of the traffic system into consideration.

Validation and optimization can be done on-chain or off-chain. Off-chain validation and/or optimization can be managed by the peer-to-peer application, like the code on the block chain. Powerful means in particular a high computing power. In other words, in the present case a valid entry in the peer-to-peer application, such as a block chain, is assumed if (only) a part of the peers 640.1, 644.1, 646.1 comes to a positive result. It shall be understood that only a single, especially particularly powerful peer can perform the validation and/or optimization process.

Similarly, in an alternative (not shown) embodiment a particularly large peer-to-peer network may be divided in two or more clusters. In a corresponding peer-to-peer network, for example, a validation (of a subset of transactions) may only be carried out by the members of one cluster (subset of nodes, e.g. sharding of a block chain to improve the scalability). In a further embodiment the peer-to-peer application can be formed using multiple block chains. These block chains are connected via frameworks such as sidechains or smart contracts.

Figure 7 shows a diagram of an embodiment of a method according to the present invention. This method can be in particular performed by an arrangement for a vehicle, wherein the arrangement can comprise a peer-to-peer module and a sensor module, as described above.

In a first step 701, a sensor module senses or detects at least one motion parameter of at least one vehicle. The current value of the detected motion parameter is provided to a peer-to-peer module. In a further step 702, the peer-to-peer module transmits the respective value of the motion parameter to a peer-to-peer application. The transmitted data can be saved and/or evaluated by the peer-to-peer application, as described above.

Figure 8 shows a diagram of a further embodiment of a method according to the present invention. This method can be in particular performed by a peer-to-peer application, as described above.

In a first step 801, traffic information data to be provided to one or more vehicles is generated by evaluating at least one motion parameter of at least one vehicle by means of at least one peer-to-peer application. For instance, the at least one motion parameter has been received from a peer-to-peer module of a vehicle.

In a further step 802, the generated traffic information can be provided to at least one peer-to-peer module assigned to at least one vehicle.

- 5 A secure and automated payment by means of a peer-to-peer network, smart contracts and/or deposits without central authority can be provided. Transaction costs can be further reduced.

Claims

1. Traffic system (200, 300, 400, 600), comprising:
 - at least one vehicle (202, 302, 304, 402, 602.2, 604.2),
 - at least one sensor module (221, 321, 421) configured to detect at least one motion parameter relating to the vehicle (202, 302, 304, 402, 602.2, 604.2),
 - at least one peer-to-peer module (228, 328, 426.2) assigned to the vehicle (202, 302, 304, 402, 602.2, 604.2) and configured to communicate with at least one peer-to-peer application (224, 324, 424, 524) of at least one peer-to-peer network (222, 322, 422, 622),
 - wherein the peer-to-peer module (228, 328, 426.2) is configured to transmit at least the detected motion parameter to the peer-to-peer application (224, 324, 424, 524) and/or to receive at least traffic information data from the peer-to-peer application (224, 324, 424, 524).
2. Traffic system (200, 300, 400, 600) according to claim 1, **characterized in that** the at least one motion parameter relating to the vehicle (202, 302, 304, 402, 602.2, 604.2) is at least one of the group comprising:
 - velocity of the vehicle (202, 302, 304, 402, 602.2, 604.2),
 - acceleration of the vehicle (202, 302, 304, 402, 602.2, 604.2),
 - a state of a component of the vehicle (202, 302, 304, 402, 602.2, 604.2), in particular, the state of the motor of the vehicle (202, 302, 304, 402, 602.2, 604.2),
 - environmental data of a vehicle (202, 302, 304, 402, 602.2, 604.2), and
 - the location of the vehicle (202, 302, 304, 402, 602.2, 604.2).
3. Traffic system (200, 300, 400, 600) according to claim 1 or 2, **characterized in that** at least one peer-to-peer module (228, 328, 426.2, 428) is configured to

cause generating of at least one parking transaction agreement about at least one parking action of the vehicle (202, 302, 304, 402, 602.2, 604.2) by means of the at least one peer-to-peer application (224, 324, 424, 524).

- 5 4. Traffic system (200, 300, 400, 600) according to any of the preceding claims,
 characterized in that the peer-to-peer application (224, 324, 424, 524) is
 configured to detect based on the at least one motion parameter relating to the
 vehicle (202, 302, 304, 402, 602.2, 604.2) whether the vehicle (202, 302, 304,
 402, 602.2, 604.2) is in a parking state within a predefined area (332.1, 332.2).
- 10
5. Traffic system (200, 300, 400, 600) according to claim 4, **characterized in that**
 - the peer-to-peer application (224, 324, 424, 524) is configured to detect the
 duration of the parking state of the vehicle (202, 302, 304, 402, 602.2, 604.2),
 and/or
15 - the sensor module (221, 321, 421) is configured to detect the duration of the
 parking state of the vehicle (202, 302, 304, 402, 602.2, 604.2).
6. Traffic system (200, 300, 400, 600) according to any of the preceding claims,
 characterized in that at least one peer-to-peer module (228, 328, 426.2, 428) is
20 configured to cause generating of at least one toll transaction agreement about at
 least one toll-liable action of the vehicle (202, 302, 304, 402, 602.2, 604.2) by
 means of the at least one peer-to-peer application (224, 324, 424, 524).
7. Traffic system (200, 300, 400, 600) according to any of the preceding claims,
25 **characterized in that** at least one peer-to-peer module (228, 328, 426.2, 428) is
 configured to cause generating of at least one vehicle sharing transaction
 agreement about at least one vehicle sharing action of the vehicle (202, 302, 304,
 402, 602.2, 604.2) by means of the at least one peer-to-peer application (224,
 324, 424, 524).

8. Traffic system (200, 300, 400, 600) according to any of the preceding claims,
characterized in that at least one peer-to-peer module (228, 328, 426.2, 428) is
configured to cause generating of at least one law enforcement transaction
agreement about at least one law enforcement action of the vehicle (202, 302,
5 304, 402, 602.2, 604.2) by means of the at least one peer-to-peer application
(224, 324, 424, 524).
9. Traffic system (200, 300, 400, 600) according to any of the preceding claims,
characterized in that
- 10 - the at least one vehicle (202, 302, 304, 402, 602.2, 604.2) comprises at least
one locking module (436) configured to lock an access unit of the vehicle
(202, 302, 304, 402, 602.2, 604.2) and/or an activation of at least one
function of the vehicle (202, 302, 304, 402, 602.2, 604.2),
- 15 - wherein the locking module (436) is configured to release the access unit of
the vehicle (202, 302, 304, 402, 602.2, 604.2) and/or to activate the function
of the vehicle (202, 302, 304, 402, 602.2, 604.2) based on an receipt of a
release information provided by the peer-to-peer application (224, 324, 424,
524).
- 20 10. Traffic system (200, 300, 400, 600) according to one of the preceding claims,
characterized in that the peer-to-peer module (228, 328, 426.2, 428) is
configured to cause a registration of the vehicle (202, 302, 304, 402, 602.2, 604.2)
in the peer-to-peer application (224, 324, 424, 524) by transmitting a registering
message comprising at least an identification assigned to the vehicle (202, 302,
25 304, 402, 602.2, 604.2).
11. Traffic system (200, 300, 400, 600) according to any of the preceding claims,
characterized in that
- 30 - the at least one peer-to-peer application (224, 324, 424, 524) is a
decentralized register or a shared database,

- wherein the peer-to-peer application (224, 324, 424, 524) is configured to store data with given certain proofs or signatures.

12. Traffic system (200, 300, 400, 600) according to any of the preceding claims,
5 **characterized in that** the at least one peer-to-peer application (224, 324, 424, 524) is a block chain or decentral ledger comprising at least two blocks (551, 553, 555) coupled to each other.

13. Traffic system (200, 300, 400, 600) according to one of the preceding claims,
10 **characterized in that** at least a part of the computer nodes (226.1, 226.2, 226.3, 326.1, 326.2, 426.1, 426.2) and/or participants (228, 328, 428) of the peer-to-peer network (222, 322, 422, 622) is/are configured to validate at least one message received and/or generated by the peer-to-peer application (224, 324, 424, 524).

14. Method, comprising:
15

- detecting at least one motion parameter relating to at least one vehicle (202, 302, 304, 402, 602.2, 604.2), and
- transmitting at least the detected motion parameter by at least one peer-to-peer module (228, 328, 426.2, 428) to at least one peer-to-peer application
20 (224, 324, 424, 524).

15. Arrangement (230, 330) for a vehicle (202, 302, 304, 402, 602.2, 604.2),
comprising:
25

- at least one sensor module (221, 321, 421) configured to detect at least one motion parameter relating to the vehicle (202, 302, 304, 402, 602.2, 604.2), and
- at least one peer-to-peer module (228, 328, 426.2) assigned to the vehicle
(202, 302, 304, 402, 602.2, 604.2) and configured to communicate with at
30 least one peer-to-peer application (224, 324, 424, 524) of at least one peer-to-peer network (222, 322, 422, 622),

- wherein the peer-to-peer module (228, 328, 426.2) is configured to transmit at least the detected motion parameter to the peer-to-peer application (224, 324, 424, 524) and/or to receive at least traffic information data from the peer-to-peer application (224, 324, 424, 524).

5

16. Vehicle (202, 302, 304, 402, 602.2, 604.2), comprising at least one arrangement (230, 330) according to claim 15.

10

17. Vehicle (202, 302, 304, 402, 602.2, 604.2) according to claim 16, characterized in that the at least one peer-to-peer module (228, 328, 426.2) assigned to the vehicle (202, 302, 304, 402, 602.2, 604.2) is connected to the vehicle (202, 302, 304, 402, 602.2, 604.2) via an interface of the vehicle (202, 302, 304, 402, 602.2, 604.2), in particular, via an on-board diagnostics connector of the vehicle (202, 302, 304, 402, 602.2, 604.2).

15

18. Method, comprising:

20

- generating at least traffic information data by evaluating at least one motion parameter relating to at least one vehicle (202, 302, 304, 402, 602.2, 604.2) by means of at least one peer-to-peer application (224, 324, 424, 524), and
- providing the generated traffic information data to at least one peer-to-peer module (228, 328, 426.2) assigned to at least one vehicle (202, 302, 304, 402, 602.2, 604.2).

25

19. Peer-to-peer application (224, 324, 424, 524), comprising:

30

- means for generating at least traffic information data by evaluating at least one motion parameter relating to at least one vehicle (202, 302, 304, 402, 602.2, 604.2), and
- means for providing the generated traffic information data to at least one peer-to-peer module (228, 328, 426.2) assigned to at least one vehicle (202, 302, 304, 402, 602.2, 604.2).

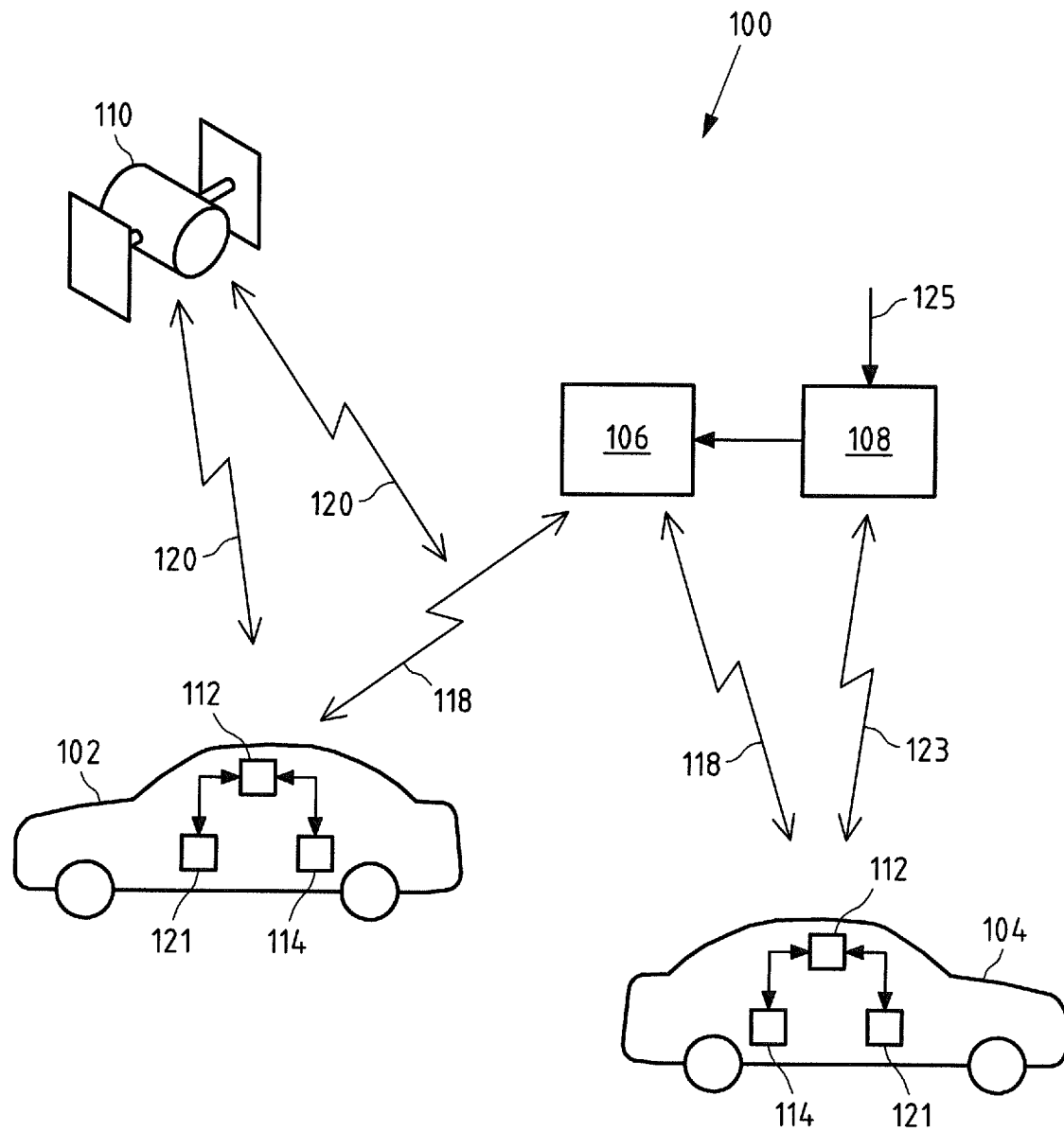


Fig.1 Prior Art

2/6

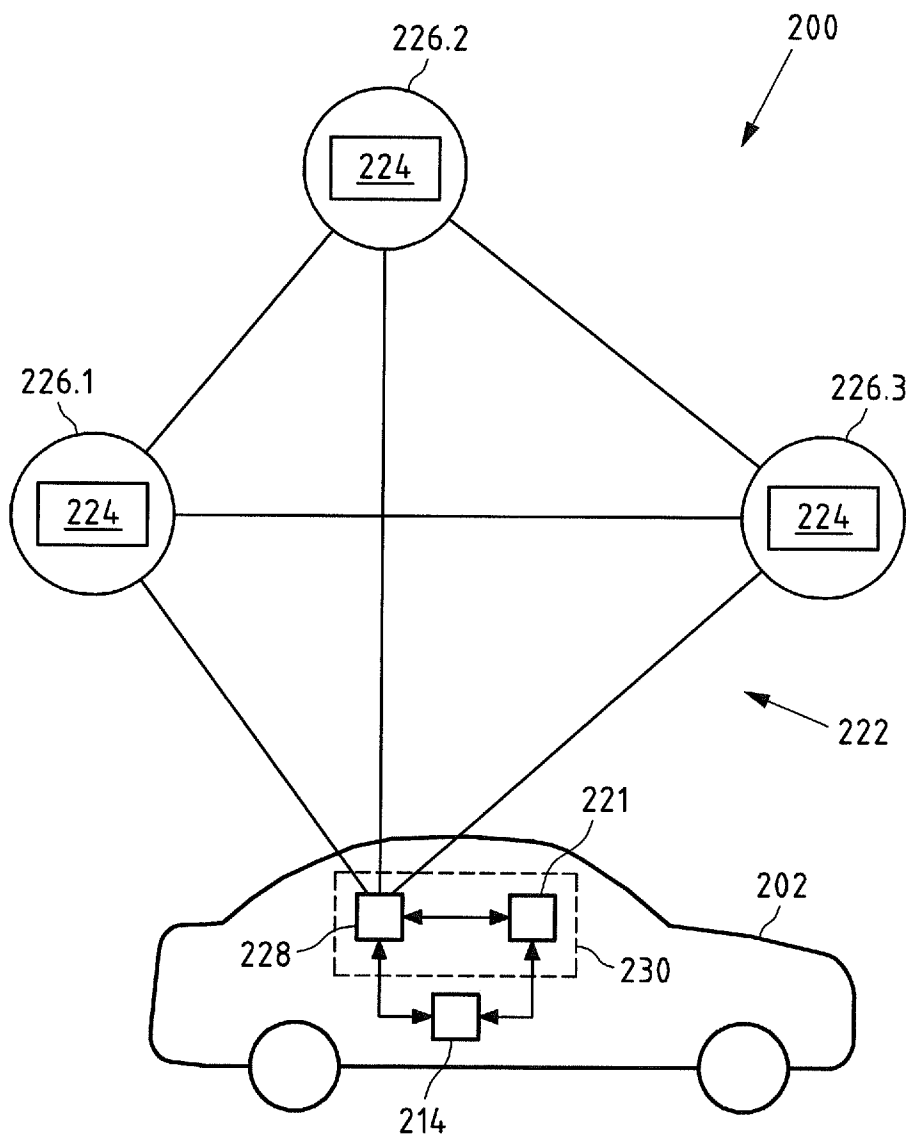


Fig.2

3/6

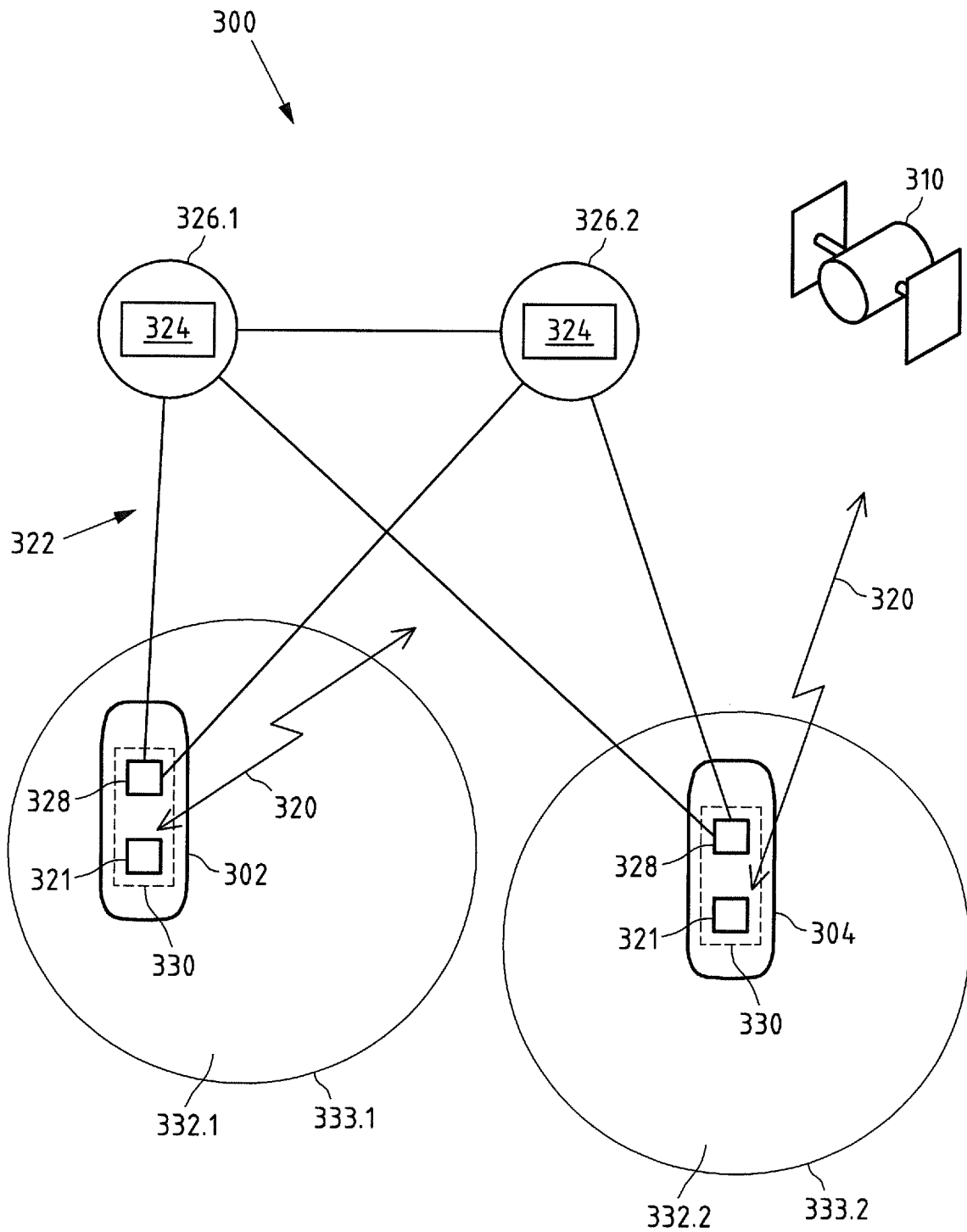


Fig.3

4/6

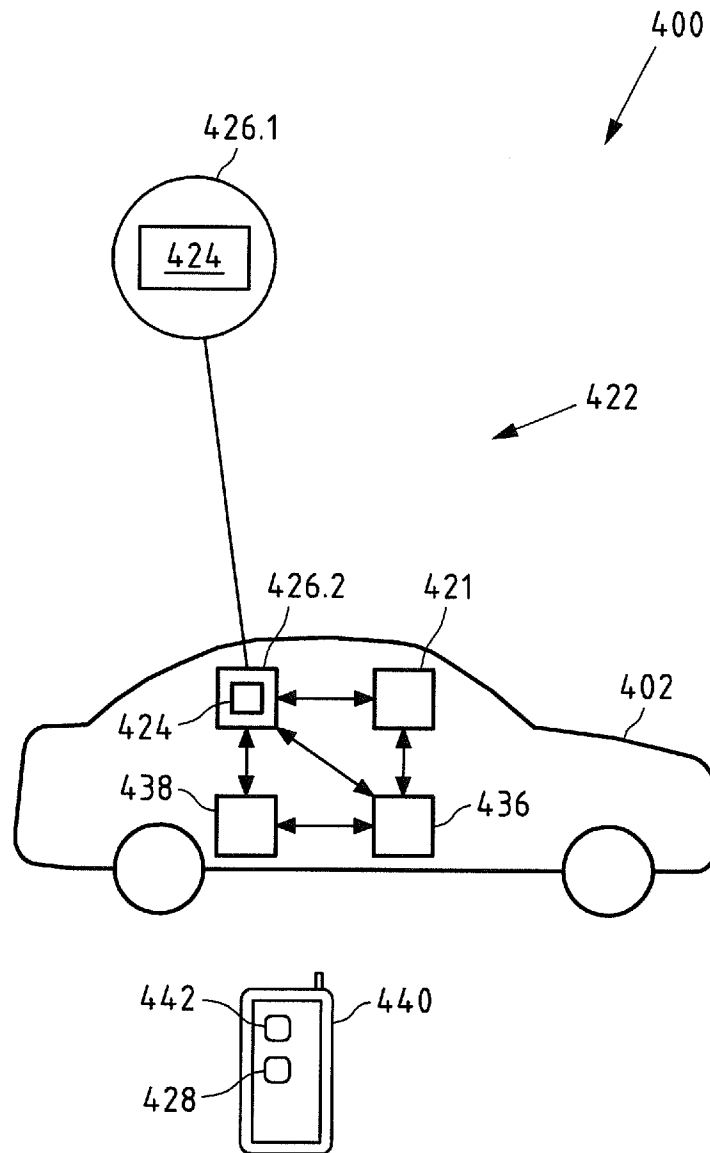
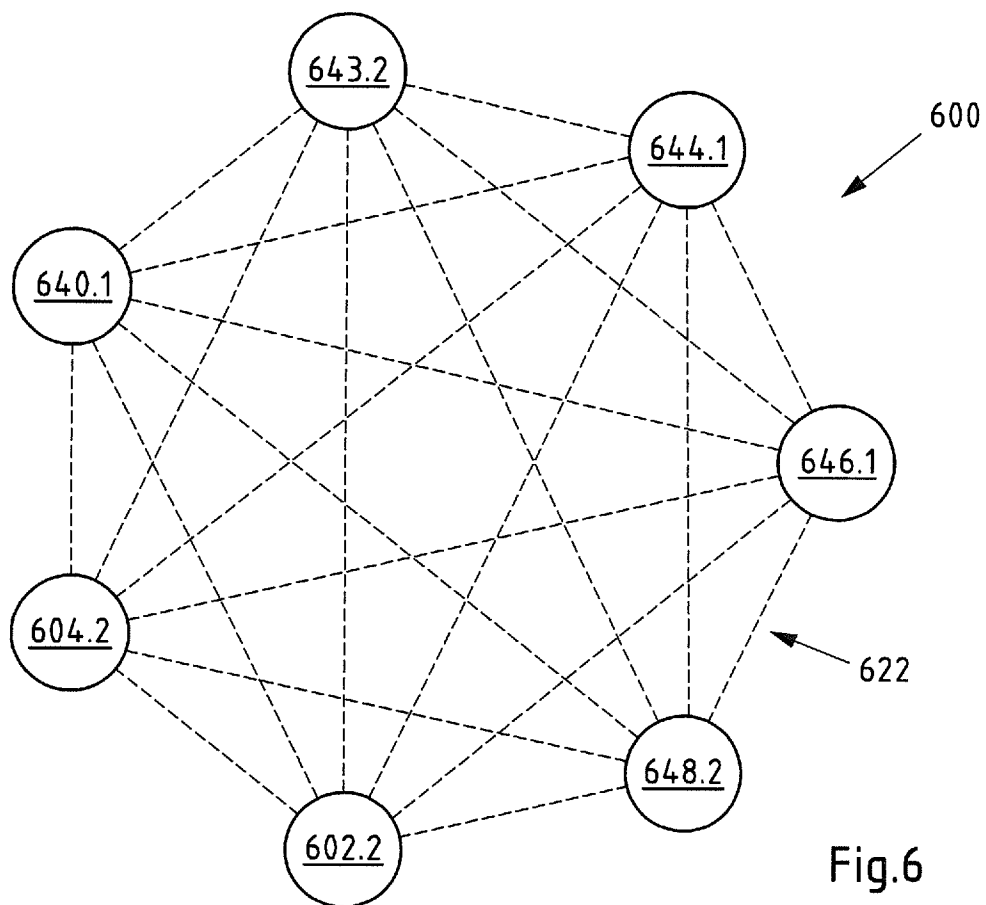
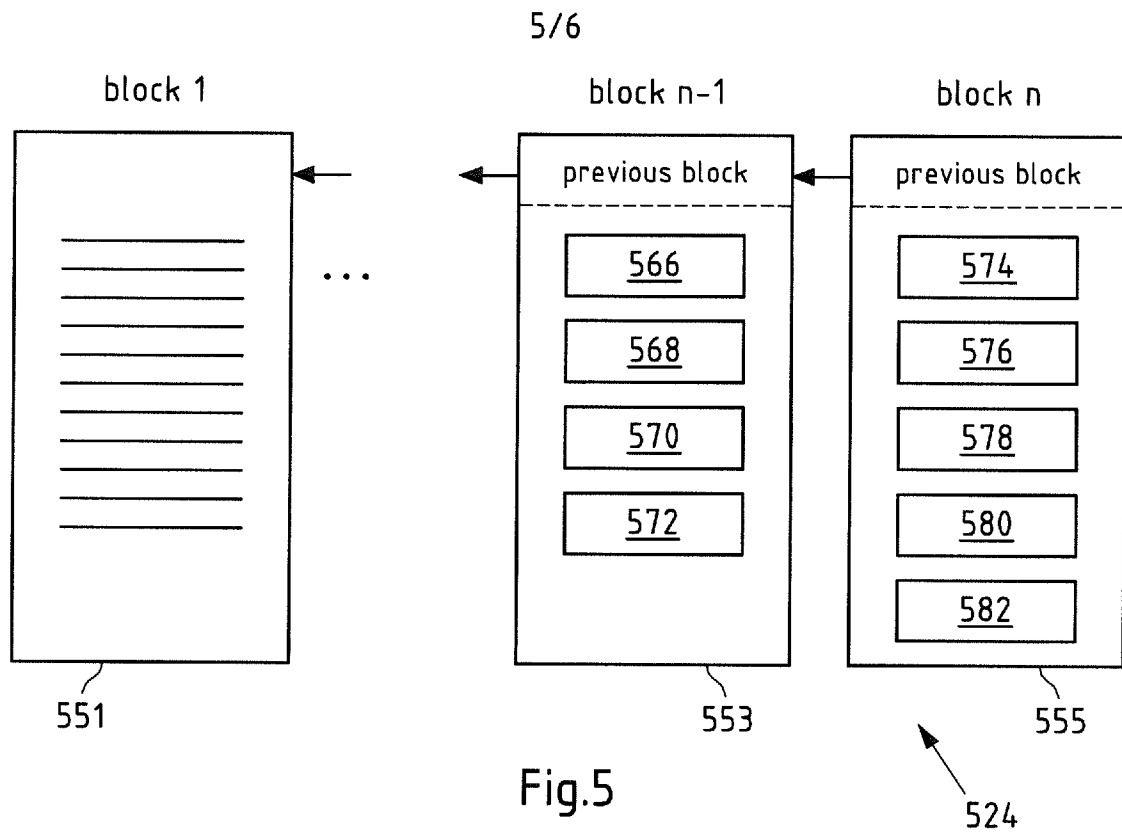


Fig.4



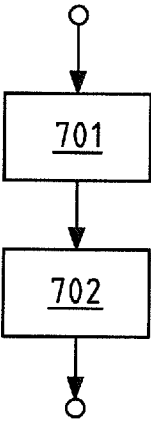


Fig.7

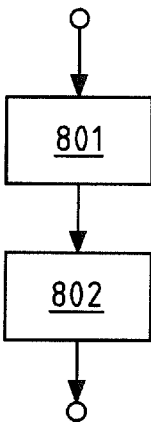


Fig.8

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2016/060171

A. CLASSIFICATION OF SUBJECT MATTER

INV. G08G1/01 G08G1/14 G07B15/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G08G G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/132223 A1 (LIN CHUN-FU [TW] ET AL) 5 June 2008 (2008-06-05)	1,2, 14-16, 18,19 3-5,17
Y	paragraphs [0002], [0004], [0006] - [0011], [0021], [0025], [0026], [0029] - [0032]; figures 2,4 -----	
Y	US 2010/302068 A1 (BANDUKWALA NAVEED [US]) 2 December 2010 (2010-12-02) paragraphs [0001], [0004], [0010] - [0019], [0029], [0031], [0035], [0036], [0049] -----	3-5,17
X	US 2014/180914 A1 (ABHYANKER RAJ [US]) 26 June 2014 (2014-06-26)	1,9,10
Y	paragraphs [0007], [0011], [0019], [0029], [0113], [0119], [0135], [0287]; figure 1 ----- -/-	11,12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

31 January 2017

Date of mailing of the international search report

16/02/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Fagundes-Peters, D

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2016/060171

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
1-5, 9-12, 14-19
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 2-5, 14-19(completely); 1(partially)

A traffic system, a method, an arrangement, a vehicle and a peer to peer application wherein motion data about a vehicle and/or traffic information is transmitted/received via a peer to peer network and a parking transaction is performed also via the peer to peer network.

2. claims: 6(completely); 1(partially)

A traffic system wherein motion data about a vehicle and/or traffic information is transmitted/received via a peer to peer network and a toll transaction is performed also via the peer to peer network.

3. claims: 7(completely); 1(partially)

A traffic system wherein motion data about a vehicle and/or traffic information is transmitted/received via a peer to peer network and a sharing transaction is performed also via the peer to peer network.

4. claims: 8(completely); 1(partially)

A traffic system wherein motion data about a vehicle and/or traffic information is transmitted/received via a peer to peer network and a law enforcement transaction is performed also via the peer to peer network.

5. claims: 9(completely); 1(partially)

A traffic system wherein motion data about a vehicle and/or traffic information is transmitted/received via a peer to peer network and a locking/release action of the vehicle is performed also via the peer to peer network.

6. claims: 10-12(completely); 1(partially)

A traffic system wherein motion data about a vehicle and/or traffic information is transmitted/received via a peer to peer network and a registration of the vehicle is performed via the peer to peer module assigned to the vehicle, the register database is a decentralised database as a block chain ledger.

7. claims: 13(completely); 1(partially)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

A traffic system wherein motion data about a vehicle and/or traffic information is transmitted/received via a peer to peer network and messages are validated by the participants of the peer to peer network.

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2016/060171

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2016/015041 A1 (BLOCKCHAIN TECHNOLOGIES CORP [US]) 28 January 2016 (2016-01-28) paragraphs [0002], [0003], [0005] - [0008] -----	11,12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2016/060171

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008132223 A1	05-06-2008	TW 200825442 A US 2008132223 A1	16-06-2008 05-06-2008
US 2010302068 A1	02-12-2010	EP 2267681 A1 US 2010302068 A1	29-12-2010 02-12-2010
US 2014180914 A1	26-06-2014	NONE	
WO 2016015041 A1	28-01-2016	US 2016028552 A1 WO 2016015041 A1	28-01-2016 28-01-2016