

COMMUNICATION NETWORK NODE, METHOD, AND MOBILE TERMINAL

TECHNICAL FIELD

The present disclosure generally pertains to a communication network node, a method for operating a smart contract, a method for controlling a communication network, and a mobile terminal.

TECHNICAL BACKGROUND

Generally, it is known to distribute a ledger over multiple nodes such as entities, e.g. electronic devices, servers or the like, which record digital transactions. Distributed ledgers can be based on the known blockchain technology, on which, for example, the known cryptocurrency bitcoin is based, but also the well-known Ethereum project, etc. Generally, a distributed ledger may also be implemented on other technologies than the blockchain technology and examples of distributed ledger projects which are not based on blockchain are BigchainDB and IOTA or the like. For instance, IOTA is a crypto currency which uses linked lists.

Moreover, mobility as a service (MaaS) is known, where a user or passenger uses mobility as a service without owning, for example, a car or the like. Mobility as a service may combine public (e.g. train, bus, etc.) and private (e.g. car sharing, bicycle sharing, etc.) transportation services from associated operators or providers.

Known MaaS solutions typically involve a central and unified gateway through which a trip or journey is planned and booked, wherein a user may pay with a single account.

Although there exist techniques for providing a distributed ledger and mobility as a service and associated communication, it is generally desirable to provide a communication network node, a method for operating a smart contract, and a method for controlling a communication network for providing a distributed ledger.

SUMMARY

According to a first aspect, the disclosure provides a communication network node for providing data to a distributed ledger, wherein the node comprises circuitry configured to obtain first position data from a mobile terminal and second position data from a sensor, provide a location condition for a smart contract, and verify whether the location condition is met, wherein the location condition is verified based on the first position data and the second position data, thereby performing a double check.

The disclosure provides a communication network node for providing data to a distributed ledger, wherein the node comprises circuitry configured to recognize a service disturbance, the service being defined on the basis of a smart contract, and adapt the smart contract on the basis of the recognized service disturbance.

According to a second aspect, the disclosure provides a method for controlling a communication network comprising multiple nodes for providing a distributed ledger, the method comprising obtaining first position data from a mobile terminal and second position

data from a sensor, providing a location condition for a smart contract, and verifying whether the location condition is met, wherein the location condition is verified based on the first position data and the second position data, thereby performing a double check.

The disclosure provides a method for controlling a communication network comprising multiple nodes for providing a distributed ledger, the method comprising recognizing a service disturbance, the service being defined on the basis of a smart contract, and adapting the smart contract on the basis of the recognized service disturbance.

According to a third aspect, the disclosure provides a mobile terminal for communicating with a network node for providing data to a distributed ledger, wherein the mobile terminal comprises at least one sensor providing first position data, and circuitry configured to provide the first position data to the network node for verifying whether a location condition of a smart contract is met, wherein the location condition of the smart contract is verified based on the first position data and second position data obtained from a sensor, thereby performing a double check.

The disclosure provides a mobile terminal for communicating with a network node for providing data to a distributed ledger, wherein the mobile terminal comprises circuitry configured to recognize a service disturbance, the service being defined on the basis of a smart contract.

Further aspects are set forth in the following description and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments are explained by way of example with respect to the accompanying drawings, in which:

Fig. 1 schematically illustrates a blockchain;

Fig. 2 schematically illustrates hashing in a blockchain;

Fig. 3 is a flowchart illustrating an embodiment of a consensus protocol;

Fig. 4 illustrates a data flow in a MaaS system;

Fig. 5 illustrates an embodiment of a blockchain including journey log data;

Fig. 6 illustrates an embodiment of a communication network for providing a blockchain;

Fig. 7 illustrates a data flow of an embodiment of a MaaS system implementing a blockchain oracle;

Fig. 8 shows a transition diagram illustrating transitions of a state of a smart contract;

Fig. 9 illustrates a flow-chart of an embodiment of a method implementing a smart contract trigger with a blockchain oracle;

CLAIMS

1. A communication network node for providing data to a distributed ledger, wherein the node comprises circuitry configured to:
 - obtain first position data from a mobile terminal and second position data from a sensor,
 - provide a location condition for a smart contract, and
 - verify whether the location condition is met, wherein the location condition is verified based on the first position data and the second position data, thereby performing a double check.
2. The communication network node of claim 1, wherein the location condition is a condition for a ticket.
3. The communication network node of claim 2, wherein the condition is an off-peak condition.
4. The communication network node of any one of claims 1 to 3, wherein the circuitry is further configured to update the distributed ledger in dependence on the verification whether the location condition is met.
5. The communication network node of any one of claims 1 to 3, wherein the distributed ledger includes a blockchain.
6. The communication network node of any one of claims 1 to 3, wherein the distributed ledger includes data for mobility as a service.
7. The communication network node of any one of claims 1 to 6, wherein the circuitry is further configured to grant access to the distributed ledger based on a permission right.
8. The communication network node of any one of claims 1 to 6, wherein the node is part of a consortium.

9. A method for controlling a communication network comprising multiple nodes for providing a distributed ledger, the method comprising:
 - obtaining first position data from a mobile terminal and second position data from a sensor,
 - providing a location condition for a smart contract, and
 - verifying whether the location condition is met, wherein the location condition is verified based on the first position data and the second position data, thereby performing a double check.
10. The communication network node of claim 9, wherein the location condition is a condition for a ticket.
11. The communication network node of claim 10, wherein the condition is an off-peak condition.
12. The communication network node of any one of claims 9 to 11, further comprising updating the distributed ledger in dependence on the verification whether the location condition is met.
13. The communication network node of any one of claims 9 to 11, wherein the distributed ledger includes a blockchain.
14. The communication network node of any one of claims 9 to 11, wherein the distributed ledger includes data for mobility as a service.
15. The communication network node of any one of claims 9 to 14, further comprising granting access to the distributed ledger based on a permission right.
16. The communication network node of any one of claims 9 to 14, wherein the node is part of a consortium.
17. A mobile terminal for communicating with a network node for providing data to a distributed ledger, wherein the mobile terminal comprises at least one sensor providing first position data, and circuitry configured to:

provide the first position data to the network node for verifying whether a location condition of a smart contract is met, wherein the location condition of the smart contract is verified based on the first position data and second position data obtained from a sensor, thereby performing a double check.

18. The mobile terminal of claim 17, wherein the mobile terminal is a smartphone.

19. The mobile terminal of claim 17, wherein the circuitry is further configured to perform an application, the application configured to provide the input data to the network node.

20. The mobile terminal of claim 19, wherein the application is a mobility as a service application.

21. The mobile terminal of claim 19, wherein the application is configured to determine a check in of a user, based on sensor data provided by a sensor of the mobile terminal.