

COMMUNICATION NETWORK NODE, METHODS, AND A 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 owing, 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 of the present disclosure, there is provided a communication network node for providing data to a distributed ledger, wherein the node includes circuitry configured to: bind a unique user-based identification and a mobile terminal based identification, wherein the unique user-based identification is a user account and the mobile terminal based identification is a plurality of unique cellular identifications selected by a user, provide verification of input data which is used as input to a smart contract, wherein the input data are verified based on sensor data, the sensor data identifying a user, in a case that the input data is verified, transmit a trigger for causing execution of a smart contract, verify that a sensor providing the sensor data is an authentic data source without knowing the unique user-based identification based only on a certificate received from a terminal device that certifies certification of the sensor providing the sensor data, and provide verification whether output data, which is based on an output from the smart contract, is correctly received at a predetermined device, wherein the output data is a ticket state being open, in use, or closed based on a check-in event trigger changing the ticket state from open to in use or a check-out event trigger changing the ticket state from in use to closed.

According to a second aspect of the present disclosure, there is provided a method for operating a smart contract, wherein the smart contract has at least two different states, the method including: binding a unique user-based identification and a mobile terminal based identification, wherein the unique user-based identification is a user account and the mobile terminal based identification is a plurality of unique cellular identifications selected by a

user: providing verification of input data which is used as input to the smart contract, wherein the input data are verified based on sensor data, the sensor data identifying a user; in a case that the input data is verified, transmitting a trigger for causing execution of a smart contract verifying that a sensor providing the sensor data is an authentic data source without knowing the unique user-based identification based only on a certificate received from a terminal device that certifies certification of the sensor providing the sensor data; changing a state of the smart contract in response to receiving a trigger; and providing verification whether output data, which is based on an output from a smart contract, is correctly received at a predetermined device. wherein the output data is a ticket state being open, in use, or closed based on a check-in event trigger changing the ticket state from open to in use or a check-out event trigger changing the ticket state from in use to closed.

Disclosed herein is a method for operating a smart contract, wherein the smart contract has at least two different states, the method comprising changing a state of the smart contract in response to receiving a trigger.

Disclosed herein is a method for controlling a communication network comprising multiple nodes for providing a distributed ledger, the method comprising at least one of providing verification of input data which is used as input to a smart contract, providing verification whether output data, which is based on an output from a smart contract, is correctly received at a predetermined device.

Disclosed herein is a mobile terminal for communicating with a network node for providing data to a distributed ledger, wherein the mobile terminal comprises circuitry configured to provide input data which is used as input to a smart contract.

Further aspects and embodiments 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 an 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;

Fig. 10 illustrates a flowchart of an embodiment of a method of a location-based check-in;

Fig. 11 illustrates a flowchart of an embodiment of a method of a biometric-based check-in;

Fig. 12 illustrates a flowchart of an embodiment of a method of a binding procedure;

Fig. 13 illustrates a flowchart of a method of a verification procedure;

CLAIMS

1. A communication network node for providing data to a distributed ledger, wherein the node comprises circuitry configured to:
 - bind a unique user-based identification and a mobile terminal based identification, wherein the unique user-based identification is a user account and the mobile terminal based identification is a plurality of unique cellular identifications selected by a user,
 - provide verification of input data which is used as input to a smart contract, wherein the input data are verified based on sensor data, the sensor data identifying a user,
 - in a case that the input data is verified, transmit a trigger for causing execution of a smart contract,
 - verify that a sensor providing the sensor data is an authentic data source without knowing the unique user-based identification based only on a certificate received from a terminal device that certifies certification of the sensor providing the sensor data, and
 - provide verification whether output data, which is based on an output from the smart contract, is correctly received at a predetermined device, wherein the output data is a ticket state being open, in use, or closed based on a check-in event trigger changing the ticket state from open to in use or a check-out event trigger changing the ticket state from in use to closed.
2. The communication network node of claim 1, wherein the sensor data are provided by at least one sensor included in a mobile terminal of the user.
3. The communication network node of claim 1, wherein the sensor data are provided by at least one sensor detecting a user.
4. The communication network node of claim 1, wherein the sensor data include location data or biometric data.
5. The communication network node of claim 4, wherein the location data are transmitted to a location server for verification.
6. The communication network node of claim 4, wherein the biometric data are transmitted to a biometric data server for verification.

7. The communication network node of claim 1, wherein the circuitry is further configured to receive or transmit data based on a data integrity functionality.
8. The communication network node of claim 7, wherein the data integrity functionality is based on at least one of: hash function, digital signature, block stream algorithm.
9. The communication network node of claim 1, wherein the verification involves verification of the binding.
10. The communication network node of claim 1, wherein the mobile terminal based identification includes at least one of cellular international mobile subscriber identity, cellular international mobile station equipment identity.
11. The communication network node of claim 1, wherein circuitry is further configured to verify the authentication of a connected device.
12. The communication network node of claim 1, wherein the distributed ledger includes a blockchain.
13. The communication network node of claim 1, wherein the distributed ledger includes data for mobility as a service.
14. A method for operating a smart contract, wherein the smart contract has at least two different states, the method comprising:
 - binding a unique user-based identification and a mobile terminal based identification, wherein the unique user-based identification is a user account and the mobile terminal based identification is a plurality of unique cellular identifications selected by a user:
 - providing verification of input data which is used as input to the smart contract, wherein the input data are verified based on sensor data, the sensor data identifying a user;
 - in a case that the input data is verified, transmitting a trigger for causing execution of a smart contract
 - verifying that a sensor providing the sensor data is an authentic data source without knowing the unique user-based identification based only on a certificate received
 - from a terminal device that certifies certification of the sensor providing the sensor data;
 - changing a state of the smart contract in response to receiving a trigger; and

providing verification whether output data, which is based on an output from a smart contract, is correctly received at a predetermined device. wherein the output data is a ticket state being open, in use, or closed based on a check-in event trigger changing the ticket state from open to in use or a check-out event trigger changing the ticket state from in use to closed.

15. The method of claim 14, wherein the trigger is received from a trusted network communication node.
16. The method of claim 14, wherein the trigger is received from a trusted sensor.
17. The communication network node of claim 1, periodically check a lost or stolen mobile terminal database for a status of a mobile terminal associated with the mobile terminal based identification.
18. The communication network node of claim 1, wherein the certificate is an X.509 certificate.