PRIVACY-PRESERVING MOBILITY AS A SERVICE SUPPORTED BY BLOCKCHAIN

TECHNICAL FIELD

The present disclosure generally pertains to a communication network node, a communication network and a method for providing a distributed ledger.

TECHNICAL BACKGROUND

Generally, it is known to distribute a ledger over multiple nodes such as entities, e.g. electronic de vices, 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 ser-vice 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, it is generally desirable to provide a communication network node, a communication network 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 configured to provide data to a distributed ledger, wherein the node comprises circuitry configured to provide a user data management part for separating sensitive user data and non-sensitive user data, and provide the non-sensitive user data to the distributed ledger, wherein personal user data or the non-sensitive user data can be erased in response to a request from the network node, wherein the data is erased by invalidation of a key.

According to a second aspect, the disclosure provides a communication network comprising multiple nodes configured to provide a distributed ledger, wherein at least one node comprises circuitry configured to provide a user data management part for separating sensitive user data and non-sensitive user data, and provide the non-sensitive user data to the distributed ledger, wherein personal user data or the non-sensitive user data can be erased in response to a request from the at least one node, wherein the data is erased by invalidation of a key.

According to a third aspect, the disclosure provides a method for controlling a communication network comprising multiple nodes configured to provide a distributed ledger, the comprising providing a user data management part for separating sensitive user data and non-sensitive user data, and providing the non-sensitive user data to the distributed ledger, wherein personal user data or the non-sensitive user data can be erased in response to a request from at least one node, wherein the data is erased by invalidation of a key.

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 an embodiment of separating sensitive and non-sensitive data;

Fig. 8 illustrates blocks of a blockchain including journey data;

Fig. 9 illustrates pseudonymization of passenger data;

Fig. 10 illustrates anonymization of passenger data;

Fig. 11 illustrates an embodiment of using different keys of data protection in a blockchain;

Fig. 12 illustrates separation of non-sensitive data and sensitive data, where the sensitive data is protected;

Fig. 13 illustrates third party encryption of data;

Fig. 14 illustrates third party access to data, wherein the sensitive data are anonymized;

Fig. 15 illustrates an application programming interface for third party access for big data analysis;

Fig. 16 illustrates a first embodiment for erasing data from the blockchain by invalidating a key;

Fig. 17 illustrates a second embodiment for erasing data from the blockchain, by erasing blocks;

Fig. 18 illustrates an embodiment of a general-purpose computer on the basis of which a network equipment or a communication device is implemented in some embodiments; and

CLAIMS

1. A communication network node configured to provide data to a distributed ledger, wherein the node comprises circuitry configured to:

provide a user data management part for separating sensitive user data and non-sensitive user data, and

provide the non-sensitive user data to the distributed ledger,

wherein personal user data or the non-sensitive user data can be erased in response to a request from the network node,

wherein the data is erased by invalidation of a key.

2. The communication network node of claim 1, wherein the circuitry is further configured to store the sensitive user data in a database of the node.

3. The communication network node of claim 1, wherein the distributed ledger includes a blockchain.

4. The communication network node of claim 3, wherein the blockchain includes multiple blocks, the blocks including the non-sensitive user data.

5. The communication network node of claim 1, wherein the distributed ledger includes data for mobility as a service.

6. The communication network node of claim 1, wherein access to the distributed ledger is granted based on a permission right.

7. The communication network node of claim 6, wherein the node is part of a consortium.

8. A communication network comprising multiple nodes configured to provide a distributed ledger, wherein at least one node comprises circuitry configured to:

provide a user data management part for separating sensitive user data and non-sensitive user data, and

provide the non-sensitive user data to the distributed ledger,

wherein personal user data or the non-sensitive user data can be erased in response to a request from the at least one node,

wherein the data is erased by invalidation of a key.

9. The communication network of claim 8, wherein the circuitry is further configured to store the sensitive user data in a database of the node.

10. The communication network of claim 8, wherein the distributed ledger includes a block-chain.

11. The communication network of claim 10, wherein the blockchain includes multiple blocks, the blocks including the non-sensitive user data.

12. The communication network of claim 8, wherein the distributed ledger includes data for mobility as a service.

13. The communication network of claim 8, wherein access to the distributed ledger is granted based on a permission right.

14. The communication network of claim 13, wherein the nodes are part of a consortium.

15. The communication network of claim 8, wherein personal user data in the distributed ledger are pseudonymized or anonymized.

16. The communication network of claim 15, wherein the personal user data are pseudonymized by scrambling the sensitive user data.

17. The communication network of claim 15, wherein the personal user data are anonymized based on applying a hash algorithm.

18. The communication network of claim 8, wherein an access control for the non-sensitive user data is provided.

19. The communication network of claim 18, wherein the access control is performed on the basis of a key, the key being used for encryption of the non-sensitive user data.

20. The communication network of claim 19, wherein the access control provides different keys for different parties.

21. The communication network of claim 18, wherein the access control gives access to the non-sensitive user data over an application programming interface.

22. The communication network of claim 8, wherein the data is erased by erasing data from the distributed ledger.

23. The communication network of claim 22, wherein the distributed ledger includes a block-chain and wherein at least one block is erased.

24. A method for controlling a communication network comprising multiple nodes configured to provide a distributed ledger, the method comprising:

providing a user data management part for separating sensitive user data and non-sensitive user data, and

providing the non-sensitive user data to the distributed ledger,

wherein personal user data or the non-sensitive user data can be erased in response to a request from at least one node,

wherein the data is erased by invalidation of a key.

25. The method of claim 24, further comprising storing the sensitive user data in a database of a node.

26. The method of claim 24, wherein the distributed ledger includes a blockchain.

27. The method of claim 26, wherein the blockchain includes multiple blocks, the blocks including the non-sensitive user data.

28. The method of claim 24, wherein the distributed ledger includes data for mobility as a service.

29. The method of claim 24, wherein access to the distributed ledger is granted based on a permission right.

30. The method of claim 29, wherein the nodes are part of a consortium.

31. The method of claim 24, wherein personal user data in the distributed ledger are pseudonymized or anonymized.

32. The method of claim 31, wherein the personal user data are pseudonymized by scrambling the sensitive user data.

33. The method of claim 31, wherein the personal user data are anonymized based on applying a hash algorithm.

34. The method of claim 24, wherein an access control for the non-sensitive data is provided.

35. The method of claim 34, wherein the access control is performed on the basis of a key, the key being used for encryption of the non-sensitive data.

36. The method of claim 35, wherein the access control provides different keys for different parties.

37. The method of claim 34, wherein the access control gives access to the non-sensitive data over an application programming interface.

38. The method of claim 24, wherein the data is erased by erasing data from the distributed ledger.

39. The method of claim 38, wherein the distributed ledger includes a blockchain and wherein at least one block is erased.