

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 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, 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 first aspect of the present disclosure, there is provided a communication network node configured to provide data to a distributed ledger, wherein the node comprises circuitry configured to: separate sensitive user data and non-sensitive user data, provide the non-sensitive user data to the distributed ledger, store the sensitive user data off-chain and only in a database of the node in which the sensitive user data originated, and restrict access control based on a purpose of data use, wherein in a case where the node is a mobility service provider, pseudonymization of the sensitive user data is required for a mobility service provider to write the sensitive user data to a blockchain, wherein in a case the node is a ticket issuer, the ticket issuer is limited to redetermined information and pseudonymization of the sensitive user data is required for the ticket issuer to write the sensitive user data to a blockchain, wherein in a case where the node is providing

data to a third party for data analysis, anonymization is required for the third-party data analysis, and wherein in a case where the node received a request from a passenger to delete their data, the node permits access to the passenger to delete their sensitive user data.

~~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 second aspect of the present disclosure, there is provided a communication network comprising multiple nodes configured to provide a distributed ledger, wherein at least one node comprises circuitry configured to: separate sensitive user data and non-sensitive user data, provide the non-sensitive user data to the distributed ledger, store the sensitive user data off-chain and only in a database of the node in which the sensitive user data originated, and restrict access control based on a purpose of data use, wherein in a case where the node is a mobility service provider, pseudonymization of the sensitive user data is required for a mobility service provider to write the sensitive user data to a blockchain, wherein in a case the node is a ticket issuer, the ticket issuer is limited to predetermined information and pseudonymization of the sensitive user data is required for the ticket issuer to write the sensitive user data to a blockchain, wherein in a case where the node is providing data to a third party for data analysis, anonymization is required for the third-party data analysis, and wherein in a case where the node received a request from a passenger to delete their data, the node permits access to the passenger to delete their sensitive user data.

~~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.~~

According to a third aspect of the present disclosure, there is provided a method for controlling a communication network comprising multiple nodes configured to provide a distributed ledger, the method including: separating sensitive user data and non-sensitive user data, providing the non-sensitive user data to the distributed ledger, storing the sensitive user data off-chain and only in a database of the node in which the sensitive user data originated, and restricting access control based on a purpose of data use, wherein in a case where the node is a mobility service provider, pseudonymization of the sensitive user data is required for a mobility service provider to write the sensitive user data to a blockchain, wherein in a case the node is a ticket issuer, the ticket issuer is limited to predetermined information and pseudonymization of the sensitive user data is required for the ticket issuer to write the sensitive user data to a blockchain, wherein in a case where the node is providing data to a third party for data analysis, anonymization is required for the third-party data analysis, and wherein in a case where the node received a request from a passenger to delete their data, the node permits access to the passenger to delete their sensitive user data.

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~~separate 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~~

store the sensitive user data off-chain and only in a database of the node in which the sensitive user data originated, and

restrict access control based on a purpose of data use,

wherein in a case where the node is a mobility service provider, pseudonymization of the sensitive user data is required for a mobility service provider to write the sensitive user data to a blockchain,

wherein in a case the node is a ticket issuer, the ticket issuer is limited to predetermined information and pseudonymization of the sensitive user data is required for the ticket issuer to write the sensitive user data to a blockchain,

wherein in a case where the node is providing data to a third party for data analysis, anonymization is required for the third-party data analysis, and

wherein in a case where the node received a request from a passenger to delete their data, the node permits access to the passenger to delete their sensitive user data.

~~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.~~

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

43. The communication network node of claim 32, wherein the blockchain includes multiple blocks, the blocks including the non-sensitive user data.

~~54.~~ The communication network node of claim 1, wherein the distributed ledger includes data for mobility as a service.

~~65.~~ The communication network node of claim 1, wherein access to the distributed ledger is granted based on a permission right.

~~76.~~ The communication network node of claim ~~65~~, wherein the node is part of a consortium.

~~87.~~ 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 separate 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~~

~~store the sensitive user data off-chain and only in a database of the node in which the sensitive user data originated, and~~

~~restrict access control based on a purpose of data use,~~

~~wherein in a case where the node is a mobility service provider, pseudonymization of the sensitive user data is required for a mobility service provider to write the sensitive user data to a blockchain,~~

~~wherein in a case the node is a ticket issuer, the ticket issuer is limited to predetermined information and pseudonymization of the sensitive user data is required for the ticket issuer to write the sensitive user data to a blockchain,~~

~~wherein in a case where the node is providing data to a third party for data analysis, anonymization is required for the third-party data analysis, and~~

~~wherein in a case where the node received a request from a passenger to delete their data, the node permits access to the passenger to delete their sensitive user data.~~

~~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.~~

~~108.~~ The communication network of claim ~~87~~, wherein the distributed ledger includes a block-chain.

~~119.~~ The communication network of claim ~~108~~, wherein the blockchain includes multiple blocks, the blocks including the non-sensitive user data.

~~1210.~~ The communication network of claim ~~87~~, wherein the distributed ledger includes data for mobility as a service.

~~1311.~~ The communication network of claim ~~87~~, wherein access to the distributed ledger is granted based on a permission right.

~~1412.~~ The communication network of claim ~~1311~~, 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.~~

~~1613.~~ The communication network of claim ~~157~~, wherein the personal user data are pseudonymized by scrambling the sensitive user data.

~~1714.~~ The communication network of claim ~~157~~, wherein the personal user data are anonymized based on applying a hash algorithm.

~~1815.~~ The communication network of claim ~~87~~, wherein an access control for the non-sensitive user data is provided.

~~1916.~~ The communication network of claim ~~1815~~, 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.~~

2217. The communication network of claim 87, wherein the data is erased by erasing data from the distributed ledger.

2318. The communication network of claim 2217, wherein the distributed ledger includes a block-chain and wherein at least one block is erased.

2419. 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~~

storing the sensitive user data off-chain and only in a database of the node in which the sensitive user data originated, and

restricting access control based on a purpose of data use,

wherein in a case where the node is a mobility service provider, pseudonymization of the sensitive user data is required for a mobility service provider to write the sensitive user data to a blockchain,

wherein in a case the node is a ticket issuer, the ticket issuer is limited to predetermined information and pseudonymization of the sensitive user data is required for the ticket issuer to write the sensitive user data to a blockchain,

wherein in a case where the node is providing data to a third party for data analysis, anonymization is required for the third-party data analysis, and

wherein in a case where the node received a request from a passenger to delete their data, the node permits access to the passenger to delete their sensitive user data.

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

[2620](#). The method of claim [2419](#), wherein the distributed ledger includes a blockchain.

[2721](#). The method of claim [2620](#), wherein the blockchain includes multiple blocks, the blocks including the non-sensitive user data.

[2822](#). The method of claim [2419](#), wherein the distributed ledger includes data for mobility as a service.

[2923](#). The method of claim [2419](#), wherein access to the distributed ledger is granted based on a permission right.

[3024](#). The method of claim [2923](#), 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.~~

[3225](#). The method of claim [3119](#), wherein the personal user data are pseudonymized by scrambling the sensitive user data.

[3326](#). The method of claim [3119](#), wherein the personal user data are anonymized based on applying a hash algorithm.

[3427](#). The method of claim [2419](#), wherein an access control for the non-sensitive data is provided.

[3528](#). The method of claim [3427](#), wherein the access control is performed on the basis of a key, the key being used for encryption of the non-sensitive data.

[3629](#). The method of claim [3528](#), wherein the access control provides different keys for different parties.

[3730](#). The method of claim [3427](#), wherein the access control gives access to the non-sensitive data over an application programming interface.

[3831](#). The method of claim [2419](#), wherein the data is erased by erasing data from the distributed ledger.

[3932](#). The method of claim [3831](#), wherein the distributed ledger includes a blockchain and wherein at least one block is erased.