

confidentiality because, by design, all smart contract instructions are available to all nodes on the distributed network.

Summary

[005] It is an object of the present invention to substantially overcome or at least ameliorate one or more disadvantages of existing arrangements.

[006] In a first aspect there is provided a method of performing a transaction in relation to an identity centric dataset, wherein the method comprises: establishing, by a consortium network, a set of permitted data operations for a service network using a plurality of identity centric privacy schemas; receiving, by the service network, a transaction request to perform the transaction in relation to the identity centric dataset associated with a data owner; identifying, by the service network from the plurality of schemas and based on the transaction request, a privacy schema from the plurality of privacy schemas for use in performing the transaction; performing the transaction by executing, in a trusted execution environment of the service network, one or more data operations from the set of permitted data operations upon the identity centric dataset of the data owner as permitted by the identified privacy schema thereby generating a manipulated dataset and transaction metadata; recording the transaction metadata to a distributed ledger of the service network; and transferring the manipulated dataset to a data receiver indicated by the transaction request.

[007] In certain embodiments, the privacy schema is identified from the plurality of privacy schemas based on at least one of the data owner and the data receiver as indicated by the transaction request.

[008] In certain embodiments, the method further comprises transferring a transaction identifier of the transaction to the data owner.

[009] In certain embodiments, the one or more data operations comprise at least one of: a data transformation operation; a data encryption operation; a data privacy preservation operation; a data anonymization operation; a data pseudo-anonymisation operation; a data tokenization operation; a data enrichment operation; a data label assignment operation; a data classification label assignment operation; and a data dissemination marker assignment operation.

[010] In certain embodiments, the transaction metadata is indicative of: one or more identity attribute identifiers; a transaction context; consent of the data owner; an identifier of the data

[019] In a second aspect there is provided a system of performing a transaction in relation to an identity centric dataset, wherein the system comprises one or more processing systems configured to: establish a set of permitted data operations for a service network using a plurality of identity centric privacy schemas; receive a transaction request to perform the transaction in relation to the identity centric dataset associated with a data owner; identify, from the plurality of schemas and based on the transaction request, a privacy schema from the plurality of privacy schemas for use in performing the transaction; perform the transaction by executing, in a trusted execution environment of the service network, one or more data operations from the set of permitted data operations upon the identity centric dataset of the data owner as permitted by the identified privacy schema thereby generating a manipulated dataset and transaction metadata; record the transaction metadata to a distributed ledger of the service network; and transfer the manipulated dataset to a data receiver indicated by the transaction request.

[020] In certain embodiments, the privacy schema is identified from the plurality of privacy schemas based on at least one of the data owner and the data receiver as indicated by the transaction request.

[021] In certain embodiments, the consortium network is configured to transfer a transaction identifier of the transaction to the data owner.

[022] In certain embodiments, the one or more data operations comprise at least one of: a data transformation operation; a data encryption operation; a data privacy preservation operation; a data anonymization operation; a data pseudo-anonymisation operation; a data tokenization operation; a data enrichment operation; a data label assignment operation; a data classification label assignment operation; and a data dissemination marker assignment operation.

[023] In certain embodiments, the transaction metadata is indicative of: one or more identity attribute identifiers; a transaction context; consent of the data owner; an identifier of the data owner; an identifier of the data receiver; and an identifier of each identifiers of the one or more data operations.

[024] In certain embodiments, the transaction request is indicative of the consent of the data owner and the transaction context.

[025] In certain embodiments, the privacy schema is identified from the plurality of privacy schemas based on at least one of the consent of the data owner and the transaction context.

CLAIMS:

1. A method of performing a transaction in relation to an identity centric dataset, wherein the method comprises:
 - establishing, by a consortium network, a set of permitted data operations for a service network using a plurality of identity centric privacy schemas;
 - receiving, by the service network, a transaction request to perform the transaction in relation to the identity centric dataset associated with a data owner;
 - identifying, by the service network from the plurality of schemas and based on the transaction request, a privacy schema from the plurality of privacy schemas for use in performing the transaction;
 - performing the transaction by executing, in a trusted execution environment of the service network, one or more data operations from the set of permitted data operations upon the identity centric dataset of the data owner as permitted by the identified privacy schema thereby generating a manipulated dataset and transaction metadata;
 - recording the transaction metadata to a distributed ledger of the service network; and
 - transferring the manipulated dataset to a data receiver indicated by the transaction request.
2. The method according to claim 1, wherein the privacy schema is identified from the plurality of privacy schemas based on at least one of the data owner and the data receiver as indicated by the transaction request.
3. The method of claim 1 or 2, further comprising transferring a transaction identifier of the transaction to the data owner.
4. A system of performing a transaction in relation to an identity centric dataset, wherein the system comprises one or more processing systems configured to:
 - establish a set of permitted data operations for a service network using a plurality of identity centric privacy schemas;
 - receive a transaction request to perform the transaction in relation to the identity centric dataset associated with a data owner;
 - identify, from the plurality of schemas and based on the transaction request, a privacy schema from the plurality of privacy schemas for use in performing the transaction;

perform the transaction by executing, in a trusted execution environment of the service network, one or more data operations from the set of permitted data operations upon the identity centric dataset of the data owner as permitted by the identified privacy schema thereby generating a manipulated dataset and transaction metadata;

record the transaction metadata to a distributed ledger of the service network; and

transfer the manipulated dataset to a data receiver indicated by the transaction request.

5. The system according to claim 4, wherein the privacy schema is identified from the plurality of privacy schemas based on at least one of the data owner and the data receiver as indicated by the transaction request.

6. The system of claim 4 or 5, wherein the consortium network is configured to transfer a transaction identifier of the transaction to the data owner.

7. The system of any one of claims 4 to 6, wherein the one or more data operations comprise at least one of:

a data transformation operation;

a data encryption operation;

a data privacy preservation operation;

a data anonymization operation;

a data pseudo-anonymisation operation;

a data tokenization operation;

a data enrichment operation;

a data label assignment operation;

a data classification label assignment operation; and

a data dissemination marker assignment operation.

8. The system of any one of claims 4 to 7, wherein the transaction metadata is indicative of:

one or more identity attribute identifiers;

a transaction context;

consent of the data owner;

an identifier of the data owner;

an identifier of the data receiver; and

an identifier of each identifiers of the one or more data operations.

9. The system according to claim 8, wherein the transaction request is indicative of the consent of the data owner and the transaction context.
10. The system according to claim 8 or 9, wherein the privacy schema is identified from the plurality of privacy schemas based on at least one of the consent of the data owner and the transaction context.
11. The system according to any one of claims 4 to 10, wherein the manipulated dataset comprises one or more transaction data records and the transaction metadata.
12. The system according to any one of claims 4 to 11, wherein the transaction metadata is appended to the one or more transaction data records.
13. The system according to any one of claims 4 to 12, wherein the service network includes a service application programming interface (API), wherein the transaction request is received from a data owner device via the service API.
14. The system according to claim 13, wherein at least some of the manipulated dataset is encrypted by the service network based on the one or more data operations, wherein the consortium network is further configured to:
 - receive, via the service API, a data access request;
 - determine, based on the data access request, if the data receiver is permitted to perform decryption of the at least some of the manipulated dataset; and
 - if the data receiver is determined to be permitted:
 - generate and transfer, to the data receiver, a decryption key to enable the data receiver to decrypt the at least some of the manipulated dataset; and
 - record, by the service network, further transaction metadata to the distributed ledger.
15. The system according to any one of claims 4 to 14, wherein the one or more processing systems configure the service network by initialising one or more system nodes based on a plurality of smart contracts and the plurality of privacy schemas distributed via a further distributed ledger, wherein the plurality of smart contracts encode the plurality of data operations.

16. The system according to claim 15, wherein the consortium network includes a plurality of system nodes, wherein the one or more processing systems are configured to establish the service network, wherein the one or more system nodes are part of the plurality of system nodes.