

CLAIMS

1. A computer-implemented method for controlling authorization of access to data, the method comprising:

receiving a first request by a first user to register a first data record in a decentralized identifier (DID) blockchain, wherein the first request~~that~~ includes a first digital activity DID~~decentralized identifier (DID)~~ and a first hash value of first digital activity data, and wherein the first digital activity ~~decentralized identifier~~DID is associated with a first ~~decentralized identifier~~DID of ~~a the~~ first user and a first business ~~decentralized identifier~~DID associated with a first consortium blockchain;

storing the first digital activity ~~decentralized identifier~~DID and the first hash value in a first record in ~~a the decentralized identifier~~DID blockchain that is configured to store records associated with a plurality of ~~decentralized identifier~~DIDs of a plurality of users;

receiving a second request associated with a second user to access the first data record of the first user, wherein the second request includes i) a second DID of the second user, ii) a second hash value for the first data record, and iii) the first digital activity DID associated with the first data record; and

controlling authorization of access to the first digital activity data stored in the first consortium blockchain ~~using information stored in the first record in the decentralized identifier blockchain, including determining whether to authorize another user access to the first digital activity data based on the information stored in the first record in the decentralized identifier blockchain~~in response to the second request, wherein the controlling comprises

verifying validities of the second DID of the second user, the first digital activity DID, the first DID of the first user and the first business DID associated with the first consortium blockchain,

determining whether the second hash value for the first data record received with the second request matches the first hash value stored in the first record in the DID blockchain to determine whether the first record is pre-registered by the first user in the DID blockchain,

sending an authorization request message to a first digital wallet decentralized application of the first user to request authorization from the first user for the second request from the second user to access the first data record, wherein the authorization request message includes information about the second request from the second user,

receiving authorization from the first digital wallet decentralized application of the first user to provide access to the second user for the first data record, wherein receiving the authorization comprises verifying the first user based on the first DID of the first user,

sending, to the first consortium blockchain, an authorization indication message indicating that the second user is authorized to access to the first data record of the first user,
and

sending a second authorization indication message to a second digital wallet decentralized application of the second user to indicate that access to the first data record of the first user is authorized.

2.The method of claim 1, wherein the first request is sent from a first consortium blockchain node associated with the first consortium blockchain.

3.The method of claim 1, comprising sending a first message to a first application program associated with the first user, wherein the first message includes the first hash value of the first digital activity data;

receiving a second message from the first application program indicating whether the first hash value is correct;

storing the first hash value in the first record if the second message indicates that the first hash value is correct; and

not storing the first hash value in the first record if the second message indicates that the first hash value is not correct.

4.The method of claim 3, wherein the first application program comprises a digital wallet decentralized application program.

5.The method of any of the preceding claims, comprising determining whether the first digital activity ~~decentralized identifier~~DID is valid by comparing the first digital activity ~~decentralized identifier~~DID with pre-stored digital activity ~~decentralized identifier~~DIDs that are stored in the ~~decentralized identifier~~DID blockchain.

6. The method of any of the preceding claims, comprising:

receiving a second request that includes the first digital activity ~~decentralized identifier~~DID and a second hash value of second digital activity data;

storing the second hash value in the first record in the ~~decentralized identifier~~DID blockchain; and

controlling authorization of access to the second digital activity data stored in the first consortium blockchain using information stored in the first record in the ~~decentralized identifier~~DID blockchain, including determining whether to authorize another user access to the second digital activity data based on the information stored in the first record in the ~~decentralized identifier~~DID blockchain.

7. The method of claim 6, wherein the second request is sent from the first consortium blockchain.

8. The method of any of the preceding claims, comprising:

receiving a second request that includes a second digital activity ~~DID~~decentralized identifier and a second hash value of second digital activity data from a second consortium blockchain network that maintains a second consortium blockchain, wherein the second digital activity ~~DID~~decentralized identifier is associated with the first ~~DID~~decentralized identifier of the first user and a second business ~~DID~~decentralized identifier associated with the second consortium blockchain;

storing the second digital activity ~~DID~~decentralized identifier and the second hash value in the first record in the ~~DID~~decentralized identifier blockchain; and

controlling authorization of access to the second digital activity data stored in the second consortium blockchain using information stored in the first record in the ~~decentralized identifier~~DID blockchain, including determining whether to authorize another user access to the second digital activity data based on the information stored in the first record in the ~~decentralized identifier~~DID blockchain.

9. The method of any of the preceding claims, comprising:

receiving a second request that includes a second digital activity ~~decentralized~~

~~identifierDID~~ and a second hash value of second digital activity data from the first consortium blockchain, wherein the second digital activity ~~decentralized identifierDID~~ is associated with a second ~~decentralized identifierDID~~ of ~~thea~~ second user and the first business ~~decentralized identifierDID~~ associated with the first consortium blockchain;

storing the second digital activity ~~decentralized identifierDID~~ and the second hash value in a second record in the ~~decentralized identifierDID~~ blockchain; and

controlling authorization of access to the second digital activity data stored in the first consortium blockchain using information stored in the second record in the ~~decentralized identifierDID~~ blockchain, including determining whether to authorize another user access to the second digital activity data based on the information stored in the second record in the ~~decentralized identifierDID~~ blockchain.

~~10.A computer implemented method for controlling authorization of access to data, the method comprising:~~

~~receiving a first hash value of first digital activity data from a decentralized identifier (DID) blockchain at an application program associated with a first user, wherein the first digital activity data is stored in a first consortium blockchain;~~

~~obtaining the first digital activity data from the first consortium blockchain;~~

~~generating a second hash value of the first digital activity data obtained from the first consortium blockchain;~~

~~comparing the first hash value with the second hash value; and~~

~~upon determining that the first hash value matches the second hash value, sending a message to a decentralized identifier blockchain node associated with the decentralized identifier blockchain indicating that the first hash value is accurate.~~

~~11.The method of claim 10, comprising:~~

~~providing a user interface that shows the first digital activity data obtained from the first consortium blockchain to the first user;~~

~~receiving an indication from the first user indicating whether the first digital activity data are correct; and~~

~~sending the indication from the first user indicating whether the first digital activity data are correct to the decentralized identifier blockchain.~~

~~12.The method of claim 10 or 11, wherein the application program comprises a digital wallet decentralized application program.~~

~~13.A computer implemented method for controlling authorization of access to data, the method comprising:~~

~~receiving a first request to allow a second user to access first digital activity data of a first user, wherein the first request includes a first hash value of the first digital activity data, a first digital activity decentralized identifier associated with a first decentralized identifier of the second user and a first business decentralized identifier associated with a first consortium blockchain, the first request is sent from the first consortium blockchain and received at a decentralized identifier (DID) blockchain that is configured to store records associated with a plurality of decentralized identifiers (DID) of a plurality of users, and the first digital activity data are stored at the first consortium blockchain;~~

~~determining whether the first digital activity decentralized identifier, the first hash value, and the first business decentralized identifier are valid; and~~

~~controlling authorization of access to the first digital activity data stored in the first consortium blockchain by the second user using the determination regarding whether the first digital activity decentralized identifier, the first hash value, and the first business decentralized identifier are valid.~~

~~14.The method of claim 13, comprising prior to receiving the first request, storing a second hash value of the first digital activity data provided by the first consortium blockchain, wherein determining whether the first hash value is valid comprises comparing the first hash value with a stored second hash value, and determining that the first hash value is valid if the first hash value is the same as the stored second hash value.~~

~~15.The method of claim 13 or 14, comprising sending a first message to an application program associated with the first user to inform the first user about the first request to allow the second user to access the first digital activity data.~~

~~16.The method of claim 15, wherein the application program associated with the first user comprises a digital wallet decentralized application program.~~

~~17.The method of claim 15 or 16, comprising receiving a second message from the application program indicating whether the first user authorizes the second user to access the first digital activity data, and wherein the controlling of the authorization of access to the first digital activity data is based at least in part on whether the second message indicates that the first user authorizes the second user to access the first digital activity data.~~

~~18.The method of claim 17, comprising upon determining that the first digital activity decentralized identifier, the first hash value, and the first business decentralized identifier are valid, and receiving the second message indicating that the first user authorizes the second user to access the first digital activity data, sending a third message to the first consortium blockchain to indicate that the first user has authorized the second user to access the first digital activity data.~~

~~19.The method of claim 17 or 18, wherein the second message includes a condition on the access of the first digital activity data by the second user.~~

~~20.The method of claim 19 in which the condition comprises a time limit condition specifying that the second user can only access the first digital activity data within a specified time limit.~~

~~21.A computer implemented method for controlling authorization of access to data, the method comprising:~~

~~receiving a first request to allow a second user to access first digital activity data of a first user, wherein the first digital activity data are stored in a first consortium blockchain, the first request is sent from a decentralized identifier (DID) blockchain node associated with a first decentralized identifier blockchain that is configured to store records associated with a~~

~~plurality of decentralized identifiers of a plurality of users, and the first request is received at an application program associated with the first user;~~

~~providing a user interface to show the first request to the first user;~~

~~receiving an instruction from the first user regarding whether to authorize the second user to access the first digital activity data stored in the first consortium blockchain; and~~

~~sending a first message to the decentralized identifier blockchain node indicating whether the first user authorizes the second user to access the first digital activity data.~~

~~22. The method of claim 21, wherein the first message includes a condition on the access of the first digital activity data by the second user.~~

~~23. The method of claim 22 in which the condition comprises a time limit condition specifying that the second user can only access the first digital activity data within a specified time limit.~~

~~24.~~10. A system for controlling authorization of access to data, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to ~~23~~9.

~~25.~~11. An apparatus for controlling authorization of access to data, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to ~~23~~9.