

[06] However, many problems exist with providing and utilizing identities. The traditional nature of some existing identities and authorization procedures presents a danger of fraud as developing technologies prove increasingly effective at counterfeiting such identities. For example, traditional identity cards, documents, etc., even if they contain anti-counterfeiting measures such as incorporated marks, holograms, etc., are increasingly subject to successful reproduction by modern techniques. Even digital identities remain vulnerable to correspondingly digital techniques.

[07] The large variety of identities, identity providers, and third party systems also has resulted in a highly differentiated identity environment. An individual typically needs to interact with a multitude of identity providers to create a corresponding number of identities, which the individual must then maintain and provide in a varying fashion to a multitude of different third parties. Likewise, many third parties find it necessary to accept, and thus provide a corresponding verification mechanism, for a variety of different identities. Such a fractured identity environment creates inefficiencies in producing and utilizing identities for both individuals and third parties.

[08] Thus, a need exists for devices, systems and methods to create, verify, and maintain identities with increased security and efficiency.

SUMMARY OF INVENTION

[08a]

According to a first aspect of the present invention, there is provided a method of providing identity services, the method comprising: receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider; generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system; sending the transaction to at least one node of the distributed system; generating, by the identity system, an identity token incorporating the identifier representing the identity data; and providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system.

[08b] According to a second aspect of the present invention, there is provided a method of verifying an identity, the method comprising: receiving, by a user system of an individual, an

identity token generated by an identity system, the identity token incorporating an identifier representing identity data of the individual generated by an identity provider, the identifier stored in a data structure on a blockchain of a distributed system, wherein the identity data is validated by the identity provider; presenting, by the user system to a restricted access system, the identity token to request an access from the restricted access system; receiving, at the identity system from the restricted access system, data extracted from the identity token, wherein the extracted data includes the identifier representing the identity data; determining whether a data structure containing the extracted identifier representing the identity data is stored on the blockchain of the distributed system; outputting, by the identity system to the restricted access system, an indication of a validity of an identity associated with the identity data based on the determination; and receiving an authorization for the access based on the indication of the validity of the identity.

[08c] According to a third aspect of the present invention, there is provided at least one non-transitory, machine-readable storage medium having program instructions, which when executed by a processor perform a method of providing identity services, the method comprising: receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider; generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system; sending, by the identity system, the transaction to at least one node of the distributed system; generating, by the identity system, an identity token incorporating the identifier representing the identity data; and providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system.

[08d] According to a fourth aspect of the present invention, there is provided at least one non-transitory, machine-readable storage medium having program instructions, which when executed by a processor perform a method of verifying an identity, the method comprising: receiving, by a user system of an individual, an identity token generated by an identity system, the identity token incorporating an identifier representing identity data of the individual generated by an identity provider, the identifier stored in a data structure on a blockchain of a distributed system, wherein the identity data is validated by the identity provider; presenting, by the user system to a restricted access system, the identity token to request an access from

the restricted access system; receiving, at the identity system from the restricted access system, data extracted from the identity token, wherein the extracted data includes the identifier representing the identity data; determining whether a data structure containing the extracted identifier representing the identity data is stored on the blockchain of the distributed system; outputting, by the identity system to the restricted access system, an indication of a validity of an identity associated with the identity data based on the determination; and receiving an authorization for the access based on the indication of the validity of the identity.

[08e] According to a fifth aspect of the present invention, there is provided a method of providing identity services, the method comprising: receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider; generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system; sending the transaction to at least one node of the distributed system; generating, by the identity system, an identity token incorporating the identifier representing the identity data; and providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system, the provided identity token being configured to be presented by the user system to a restricted access system to request an access from the restricted access system.

[08f] According to a sixth aspect of the present invention, there is provided a system, comprising: at least one processor; a non-transitory, machine-readable storage medium having program instructions, which when executed by the at least one processor cause a method of providing identity services to be performed, the method comprising: receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider; generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system; sending the transaction to at least one node of the distributed system; generating, by the identity system, an identity token incorporating the identifier representing the identity data; and providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system.

[08g] According to a seventh aspect of the present invention, there is provided a system, comprising: at least one processor; a non-transitory, machine-readable storage medium having program instructions, which when executed by the at least one processor cause a method of verifying an identity to be performed, the method comprising: receiving, by a user system of an individual, an identity token generated by an identity system, the identity token incorporating an identifier representing identity data of the individual generated by an identity provider, the identifier stored in a data structure on a blockchain of a distributed system, wherein the identity data is validated by the identity provider; presenting, by the user system to a restricted access system, the identity token to request an access from the restricted access system; receiving, at the identity system from the restricted access system, data extracted from the identity token, wherein the extracted data includes the identifier representing the identity data; determining whether a data structure containing the extracted identifier representing the identity data is stored on the blockchain of the distributed system; outputting, by the identity system to the restricted access system, an indication of a validity of an identity associated with the identity data based on the determination; and receiving an authorization for the access based on the indication of the validity of the identity.

BRIEF DESCRIPTION OF THE DRAWINGS

[09] So that the features of the present invention can be understood, a number of drawings are described below. However, the appended drawings illustrate only particular embodiments of the invention and are therefore not to be considered limiting of its scope, for the invention may encompass other equally effective embodiments.

[10] FIG. 1 is a schematic diagram depicting an embodiment of a system to provide identity services.

[11] FIG. 2 is a schematic diagram depicting an embodiment of an integrated identity system.

[12] FIG. 3 is a schematic diagram depicting an embodiment of a distributed identity element repository.

[13] FIG. 4 is a schematic diagram depicting an embodiment of a distributed smart contract system node.

WHAT IS CLAIMED IS:

1. A method of providing identity services, the method comprising:
receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider;
generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system;
sending the transaction to at least one node of the distributed system;
generating, by the identity system, an identity token incorporating the identifier representing the identity data; and
providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system.
2. The method of claim 1, wherein the transaction invokes an identity creation function of an identity services contract stored on the blockchain.
3. The method of claim 1, further comprising generating the identifier representing the identity data by performing at least one cryptographic hash function on the identity data.
4. The method of claim 1, further comprising:
presenting, by the user system, the identity token to a restricted access system to request an access from the restricted access system; and
receiving an authorization for the access as a function of the presented identity token.
5. The method of claim 1, wherein the identity data includes at least one of: a name of the individual, an identification number of the identity of the individual, or an address of the individual.
6. The method of claim 1, wherein the identity data includes at least one representation of a biometric trait of an individual.
7. The method of claim 6, wherein the representation of the biometric trait includes at least one of: a picture of the individual, a fingerprint of the individual, a facial pattern of the individual, an iris pattern of the individual, a retina pattern of the individual, a representation of a voice of the individual, or a deoxyribonucleic acid (DNA) pattern of the individual.

8. The method of claim 1, wherein generating the identity token includes encoding into the token at least one of: the identifier representing the identity data, an identification of the identity provider, or a digital signature of the identity provider.
9. The method of claim 1, further comprising:
receiving metadata associated with the individual;
generating a transaction to store the metadata or a representation of the metadata on the block chain in association with the identifier representing the identity data; and
sending the transaction to at least one node of the distributed system.
10. The method of claim 9, wherein the transaction invokes a metadata creation function of an identity services contract stored on the blockchain.
11. The method of claim 1, wherein the presenting the identity token by the user system to the restricted access system includes displaying the identity token by the user system to the restricted access system.
12. The method of claim 1, wherein receiving the authorization for the access as the function of the presented identity token occurs in response to determining that data extracted from the identity token matches the identifier stored in the data structure on the blockchain of the distributed system.
13. A method of verifying an identity, the method comprising:
receiving, by a user system of an individual, an identity token generated by an identity system, the identity token incorporating an identifier representing identity data of the individual generated by an identity provider, the identifier stored in a data structure on a blockchain of a distributed system, wherein the identity data is validated by the identity provider;
presenting, by the user system to a restricted access system, the identity token to request an access from the restricted access system;
receiving, at the identity system from the restricted access system, data extracted from the identity token, wherein the extracted data includes the identifier representing the identity data;
determining whether a data structure containing the extracted identifier representing the identity data is stored on the blockchain of the distributed system;

outputting, by the identity system to the restricted access system, an indication of a validity of an identity associated with the identity data based on the determination; and receiving an authorization for the access based on the indication of the validity of the identity.

14. The method of claim 13, wherein the determining includes invoking an identity verification function of an identity services contract stored on a blockchain, the invocation including the extracted identifier representing the identity data.

15. The method of claim 13, wherein the extracted data further includes a digital signature of the identity provider extracted from the identity token, and the method further comprises verifying the digital signature using a public key of the identity provider.

16. The method of claim 13, wherein the data extracted from the identity token includes a representation of a biometric trait of the individual, and the method further comprises verifying the representation of the extracted biometric trait against a biological feature of the individual.

17. The method of claim 16, further comprising authorizing the individual to access the restricted access system based on the validity of the identity and the verification of the biometric trait.

18. The method of claim 13, wherein the identifier representing the identity data includes data formed by performing at least one cryptographic hash function on the identity data.

19. At least one non-transitory, machine-readable storage medium having program instructions, which when executed by a processor perform a method of providing identity services, the method comprising:

receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider;

generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system;

sending, by the identity system, the transaction to at least one node of the distributed system;

generating, by the identity system, an identity token incorporating the identifier representing the identity data; and

providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system.

20. The non-transitory machine readable storage medium of claim 19, wherein the transaction invokes an identity creation function of an identity services contract stored on the blockchain.

21. The non-transitory machine readable storage medium of claim 19, the method further comprising generating the identifier representing the identity data by performing at least one cryptographic hash function on the identity data.

22. The non-transitory machine readable storage medium of claim 19, wherein generating the identity token includes encoding into the token at least one of: the identifier representing the identity data, an identification of the identity provider, or a digital signature of the identity provider.

23. The non-transitory storage medium of claim 19, the method further comprising:
presenting, by the user system, the identity token to a restricted access system to request an access from the restricted access system; and
receiving an authorization for the access as a function of the presented identity token.

24. At least one non-transitory, machine-readable storage medium having program instructions, which when executed by a processor perform a method of verifying an identity, the method comprising:

receiving, by a user system of an individual, an identity token generated by an identity system, the identity token incorporating an identifier representing identity data of the individual generated by an identity provider, the identifier stored in a data structure on a blockchain of a distributed system, wherein the identity data is validated by the identity provider;

presenting, by the user system to a restricted access system, the identity token to request an access from the restricted access system;

receiving, at the identity system from the restricted access system, data extracted from the identity token, wherein the extracted data includes the identifier representing the identity data;

determining whether a data structure containing the extracted identifier representing the identity data is stored on the blockchain of the distributed system;

outputting, by the identity system to the restricted access system, an indication of a validity of an identity associated with the identity data based on the determination; and receiving an authorization for the access based on the indication of the validity of the identity.

25. The non-transitory machine readable storage medium of claim 24, wherein the determining includes invoking an identity verification function of an identity services contract stored on a blockchain, the invocation including the extracted identifier representing the identity data.

26. The non-transitory machine readable storage medium of claim 24, wherein the extracted data further includes a digital signature of the identity provider extracted from the identity token, and the method further comprises verifying the digital signature using a public key of the identity provider.

27. The non-transitory machine readable storage medium of claim 24, wherein the data extracted from the identity token includes a representation of a biometric trait of the individual, and the method further comprises verifying the representation of the extracted biometric trait against a biological feature of the individual.

28. A method of providing identity services, the method comprising:
receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider;
generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system;
sending the transaction to at least one node of the distributed system;
generating, by the identity system, an identity token incorporating the identifier representing the identity data; and
providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system, the provided identity token being configured to be presented by the user system to a restricted access system to request an access from the restricted access system.

29. The method of claim 28, wherein the identity data includes at least one of: a name of the individual, an identification number of the identity of the individual, or an address of the individual.

30. A system, comprising:
at least one processor;
a non-transitory, machine-readable storage medium having program instructions, which when executed by the at least one processor cause a method of providing identity services to be performed, the method comprising:
receiving, by an identity system at a first interface from an identity provider system, identity data for an individual for which the identity provider has generated an identity, wherein the identity data is validated by the identity provider;
generating, by the identity system, a transaction to store an identifier representing the identity data in a data structure on a blockchain of a distributed system;
sending the transaction to at least one node of the distributed system;
generating, by the identity system, an identity token incorporating the identifier representing the identity data; and
providing, by the identity system at a second interface to a user system of the individual, the generated identity token to the user system.
31. The system of claim 30, wherein the method further comprises generating the identifier representing the identity data by performing at least one cryptographic hash function on the identity data.
32. The system of claim 30, wherein the method further comprises:
presenting, by the user system, the identity token to a restricted access system to request an access from the restricted access system; and
receiving an authorization for the access as a function of the presented identity token.
33. The system of claim 30, wherein the identity data includes at least one of: a name of the individual, an identification number of the identity of the individual, or an address of the individual.
34. The system of claim 30, wherein the identity data includes at least one representation of a biometric trait of an individual.

35. The system of claim 30, wherein generating the identity token includes encoding into the token at least one of: the identifier representing the identity data, an identification of the identity provider, or a digital signature of the identity provider.

36. A system, comprising:

at least one processor;

a non-transitory, machine-readable storage medium having program instructions, which when executed by the at least one processor cause a method of verifying an identity to be performed, the method comprising:

receiving, by a user system of an individual, an identity token generated by an identity system, the identity token incorporating an identifier representing identity data of the individual generated by an identity provider, the identifier stored in a data structure on a blockchain of a distributed system, wherein the identity data is validated by the identity provider;

presenting, by the user system to a restricted access system, the identity token to request an access from the restricted access system;

receiving, at the identity system from the restricted access system, data extracted from the identity token, wherein the extracted data includes the identifier representing the identity data;

determining whether a data structure containing the extracted identifier representing the identity data is stored on the blockchain of the distributed system;

outputting, by the identity system to the restricted access system, an indication of a validity of an identity associated with the identity data based on the determination; and

receiving an authorization for the access based on the indication of the validity of the identity.

37. The system of claim 36, wherein the determining includes invoking an identity verification function of an identity services contract stored on a blockchain, the invocation including the extracted identifier representing the identity data.

38. The method of claim 36, wherein the data extracted from the identity token includes a representation of a biometric trait of the individual, and the method further comprises verifying the representation of the extracted biometric trait against a biological feature of the individual.