

CLAIMS

1. A computer-implemented method for generating and verifying passwords, the method comprising:

receiving a password setup request, the password setup request comprising a list identifying at least ~~two verifiers~~^{one verifier} and data representing a user-provided password;

~~processing the data representing the user-provided password to recognize the user-provided password;~~

forming a basis password based on the user-provided password;

generating a plurality of system-generated passwords based on the basis password;

encrypting the plurality of system-generated passwords to generate a plurality of encrypted passwords including a first encrypted password ~~and a second encrypted password~~;

submitting the plurality of encrypted passwords to a blockchain system for recordation; ~~and~~

providing a first address of the first encrypted password on the blockchain system to a first verifier identified in the list; ~~and~~

~~providing a second address of the second encrypted password on the blockchain system to a second verifier identified in the list.~~

~~2. The method of claim 1, wherein the plurality of encrypted passwords include a second encrypted password, the method further comprising:~~

~~providing a second address of the second encrypted password on the blockchain system to a second verifier identified in the list.~~

23. The method of ~~any preceding~~ claim 1, further comprising:

receiving a password verification request, the password verification request identifying the first verifier as a target verifier and comprising data representing the user-provided password;

forming the basis password based on the user-provided password in the password verification request;

generating the plurality of system-generated passwords based on the basis password;

encrypting the plurality of system-generated passwords to generate the plurality of encrypted passwords including the first encrypted password; and

providing the first encrypted password to the first verifier for password verification by the first verifier.

34. The method of claim 23, wherein the password verification is deemed successful when the first encrypted password provided to the first verifier matches the first encrypted password recorded at the first address.

~~5. The method of any preceding claim, further comprising:
processing the data representing the user provided password to recognize the user provided password.~~

46. The method of claim 15, wherein the processing comprises voice recognition.

57. The method of claim 15, wherein the processing comprises image recognition.

68. The method of any preceding claim, wherein forming the basis password based on the user-provided password further comprises:
generating an additional password; and
utilizing the additional password in conjunction with the user-provided password to form the basis password.

79. The method of any preceding claim, wherein each of the plurality of encrypted passwords is recorded at a unique address on the blockchain system.

840. The method of any preceding claim, wherein the first address is one of a set of addresses provided to the first verifier, wherein the set of addresses correspond to a set of encrypted passwords.

944. A device for generating and verifying password, 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 840.

~~12. An apparatus for generating and verifying password, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 10.~~

103. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 810.