

WE CLAIM:

1. A method for identity verification of a user, the method comprising:
 - sensing, by at least one sensor, biometric information from the user;
 - generating, by a sensor device, biometric data from the biometric information;
 - transmitting, by the sensor device, the biometric data to a user device;
 - hashing, by the user device, at least a portion of the biometric data and at least a portion of additional identifying information to generate a biometric digital signature for the user;
 - storing, by the user device, at least a portion of the biometric digital signature for the user to a host biometric digital signature of user devices corresponding to each of at least n number of persons, such that a combination of the host biometric digital signatures for at least m number of the n number of persons comprises all of the biometric digital signature for the user, wherein the m number is a number greater than half of the n number;
 - transmitting, by the user device, the biometric digital signature to a verification node;
 - obtaining, by the verification node, host biometric digital signatures from other user devices corresponding to other users associated with the user, wherein each of the host biometric digital signatures comprise a portion of a previous biometric digital signature for the user;
 - reconstructing, by the verification node, the previous biometric digital signature from the portions of the host biometric digital signatures;
 - comparing, by the verification node, the biometric digital signature to the previous biometric digital signature for the user; and
 - verifying, by the verification node, the user when the verification node determines that the biometric digital signature is identical to the previous biometric digital signature for the user.
2. The method of claim 1, further comprising, when the user is verified, generating and transmitting, by the verification node to the user device, a confirmation verification signal indicating that the user is verified.
3. The method of claim 1, further comprising not verifying, by the verification node, the user when the verification node determines that the biometric digital signature is not identical to the previous biometric digital signature for the user.

4. The method of claim 3, further comprising, when the user is not verified, generating and transmitting, by the verification node to the user device, an abort verification signal indicating that the user is not verified.
5. The method of claim 1, wherein when the user is verified, the method further comprises at least one of:
- allowing the user to transfer assignment of a data block from the user to a beneficiary;
 - allowing the user to transfer ownership of property from the user to the beneficiary;
 - allowing the user to obtain medical records for the user;
 - allowing the user to vote on behalf of the user;
 - allowing the user to obtain travel documentation for the user; or
 - allowing the user to make banking transactions on behalf of the user.
6. The method of claim 1, wherein the biometric information comprises at least one of at least three fingerprints, at least a portion of a deoxyribonucleic acid (DNA) sequence, at least a portion of at least one facial feature, isotopic information from odor, at least a portion of an eye feature, audio information from a voice, a three-dimensional surface scan of at least a portion of the user, or a two-dimensional surface scan of at least the portion of the user.
7. The method of claim 1, wherein the user device utilizes one of a hash algorithm or a fuzzy hash algorithm to hash the at least a portion of the biometric data.
8. The method of claim 1, wherein the user device utilizes one of a SHA-256 algorithm, a Merkle-Damgard algorithm, a MD5 algorithm, a SHA-1 algorithm, a SHA-2 algorithm, a RACE Integrity Primitives Evaluation Message Digest-160 (RIPEMD-160) algorithm, a Whirlpool algorithm, or a BLAKE2 algorithm to hash the at least a portion of the biometric data.
9. The method of claim 1, wherein the additional identifying information comprises at least one of location information, temperature information, humidity information, date information, time information, elevation information, range information, or personal information.

10. The method of claim 1, wherein the biometric digital signature is a private identity key for the user.
11. The method of claim 1, wherein the user device is one of a smart phone, a tablet device, a personal computer, a laptop computer, a smart watch, a smart television (TV), a car, or a computing device.
12. The method of claim 1, wherein the user device comprises at least one of the at least one sensor, the sensor device, or the verification node.
13. A method for identity verification of at least one user, the method comprising:
sensing, by at least one sensor, biometric information from a user;
generating, by a sensor device, biometric data from the biometric information;
transmitting, by the sensor device, the biometric data to a user device;
hashing, by the user device, at least a portion of the biometric data to generate a biometric digital signature for the user;
storing, by the user device, at least a portion of the biometric digital signature for the user to a host biometric digital signature of user devices corresponding to each of at least n number of persons, such that a combination of the host biometric digital signatures for at least m number of the n number of persons comprises all of the biometric digital signatures for the user, wherein the m number is a number greater than half of the n number;
obtaining, by the user device, the host biometric digital signatures from the user devices corresponding to the at least m number of persons;
reconstructing, by the user device, a biometric digital signature for the user by using the host biometric digital signatures obtained from the at least m number of persons;
transmitting, by the user device, the reconstructed biometric digital signature to a verification node; and
receiving, by the user device from the verification node, a confirmation verification signal indicating that the user is verified by comparing the reconstructed biometric digital signature to a previous biometric digital signature for the user and determining the reconstructed biometric digital signature is identical to the previous biometric digital signature.

14. A system for identity verification of a user, the system comprising:
- at least one sensor sensing biometric information from the user;
 - a sensor device generating biometric data from the biometric information and transmitting the biometric data to a user device;
 - the user device hashing at least a portion of the biometric data and at least a portion of additional identifying information to generate a biometric digital signature for the user, transmitting the biometric digital signature to a verification node, and storing at least a portion of the biometric digital signature for the user to a host biometric digital signature of user devices corresponding to each of at least n number of persons, such that a combination of the host biometric digital signatures for at least m number of the n number of persons comprises all of the biometric digital signatures for the user, wherein the m number is a number greater than half of the n number; and
 - the verification node obtaining host biometric digital signatures from other user devices corresponding to other users associated with the user, wherein each of the host biometric digital signatures comprises a portion of a previous biometric digital signature for the user, reconstructing the previous biometric digital signature from the portions of the host biometric digital signatures, comparing the biometric digital signature to the previous biometric digital signature for the user, and verifying the user when the verification node determines that the biometric digital signature is identical to the previous biometric digital signature for the user.
15. The system of claim 14, wherein when the user is verified, the verification node further generates and transmits to the user device, a confirmation verification signal indicating that the user is verified.
16. The system of claim 14, wherein the verification node does not verify the user when the verification node determines that the biometric digital signature is not identical to the previous biometric digital signature for the user.
17. The system of claim 14, wherein the user device comprises at least one of the at least one sensor, the sensor device, or the verification node.

18. The system of claim 14, wherein the user device utilizes one of a hash algorithm or a fuzzy hash algorithm to hash the at least a portion of the biometric data to generate the biometric digital signature for the user.

19. The system of claim 14, wherein the user device utilizes one of a SHA-256 algorithm, a Merkle-Damgard algorithm, a MD5 algorithm, a SHA-1 algorithm, a SHA-2 algorithm, a RACE Integrity Primitives Evaluation Message Digest-160 (RIPEMD-160) algorithm, a Whirlpool algorithm, or a BLAKE2 algorithm to hash the at least a portion of the biometric data.

20. The system of claim 14, wherein the additional identifying information comprises at least one of location information, temperature information, humidity information, date information, time information, elevation information, range information, or personal information.