WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

authenticating, by at least one processor, a sponsor device associated with a sponsoring user;

communicating, by at least one processor, a first unique identifier to the authenticated sponsor device;

receiving, by at least one processor, first image data associated with a first image of an enrolling user from the authenticated sponsor device, the first image data comprising the first unique identifier;

recording, by at least one processor, the first image data and the first unique identifier in a ledger;

generating, by at least one processor, a first edge in a tree based on the first image data and the first unique identifier, the tree being stored in the ledger and comprising a plurality of nodes and a plurality of edges, each node of the plurality of nodes being connected to at least one other node of the plurality of nodes by a respective edge of the plurality of edges, the first edge connecting a first node of the plurality of nodes associated with the sponsoring user to a second node of the plurality of nodes associated with the enrolling user;

determining, by at least one processor, a second trust score for the second node based on a respective trust score of each of at least one node of the plurality of nodes connected to the second node by a respective edge of the plurality of edges, the at least one node of the plurality of nodes comprising the first node, the first node being associated with a first trust score;

receiving, by at least one processor, second image data associated with a second image of a government identification document of the enrolling user; and

approving, by at least one processor, the enrolling user and/or the government identification document based on the second trust score.

2. The method of claim 1, wherein the sponsor device comprises a secure mobile application, wherein communicating comprises communicating the first unique identifier to the secure mobile application of the authenticated sponsor device, and wherein receiving comprises receiving the first image data from the secure mobile application of the authenticated sponsor device.

3. The method of claim 2, wherein the sponsor device logs into the secure mobile application via a strong authentication technique.

4. The method of claim 3, wherein the strong authentication technique comprises at least one of two-factor authentication (2FA), Fast IDentity Online (FIDO), or any combination thereof.

5. The method of claim 1, further comprising:

receiving, by at least one processor, a request for the first unique identifier from the sponsor device before communicating the first unique identifier.

6. The method of claim 1, wherein the first image data comprises a checksum value associated with the first image.

7. The method of claim 1, wherein the first image data comprises the first unique identifier embedded in the first image.

8. The method of claim 7, further comprising:

embedding, by the sponsor device, the first unique identifier in the first image by inserting the first unique identifier in metadata of the first image.

9. The method of claim 7, further comprising:

embedding, by the sponsor device, the first unique identifier in the first image by steganography.

10. The method of claim 9, wherein embedding the first unique identifier in the first image by steganography comprises adjusting at least one bit of a plurality of pixel values of the first image based on the first unique identifier.

11. The method of claim 1, wherein the first image comprises a first representation of a face of the enrolling user and the second image comprises a second representation of the face of the enrolling user, the method further comprising:

comparing, by at least one processor, the first image to the second image to determine the first representation matches the second representation.

12. The method of claim 1, further comprising:

receiving, by at least one processor, a request for the second trust score associated with the enrolling user from a relying party system.

13. The method of claim 12, wherein the request comprises the first unique identifier.

14. The method of claim 12, wherein the relying party system creates an account for the enrolling user with the relying party system based on the second trust score.

15. The method of claim 1, wherein the ledger comprises an encrypted distributed ledger.

16. The method of claim 1, further comprising:

identifying, by at least one processor, at least one subset of the plurality of nodes of the tree based on network analysis.

17. The method of claim 1, further comprising:

receiving, by at least one processor, negative event data associated with at least one negative event associated with a third node of the tree;

adjusting, by at least one processor, a third trust score associated with the third node based on the negative event data; and

adjusting, by at least one processor, the trust score for each node of the plurality of nodes connected to the third node by one of the plurality of edges,

wherein the negative event data comprises at least one of complaint data associated with a complaint, an indication associated with a fraudulent transaction, or any combination thereof.

18. A system, comprising:

at least one processor configured to:

authenticate a sponsor device associated with a sponsoring user;

communicate a first unique identifier to the authenticated sponsor device;

receive first image data associated with a first image of an enrolling user from the authenticated sponsor device, the first image data comprising the first unique identifier;

record the first image data and the first unique identifier in a ledger;

generate a first edge in a tree based on the first image data and the first unique identifier, the tree being stored in the ledger and comprising a plurality of nodes and a plurality of edges, each node of the plurality of nodes being connected to at least one other node of the plurality of nodes by a respective edge of the plurality of edges, the first edge connecting a first node of the plurality of nodes associated with the sponsoring user to a second node of the plurality of nodes associated with the enrolling user;

determine a second trust score for the second node based on a respective trust score of each of at least one node of the plurality of nodes connected to the second node by a respective edge of the plurality of edges, the at least one node of the plurality of nodes comprising the first node, the first node being associated with a first trust score;

receive second image data associated with a second image of a government identification document of the enrolling user; and

approve the enrolling user and/or the government identification document based on the second trust score.

19. A computer program product, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

authenticate a sponsor device associated with a sponsoring user;

communicate a first unique identifier to the authenticated sponsor device;

receive first image data associated with a first image of an enrolling user from the authenticated sponsor device, the first image data comprising the first unique identifier;

record the first image data and the first unique identifier in a ledger;

generate a first edge in a tree based on the first image data and the first unique identifier, the tree being stored in the ledger and comprising a plurality of nodes and a plurality of edges, each node of the plurality of nodes being connected to at least one other node of the plurality of nodes by a respective edge of the plurality of edges, the first edge connecting a first node of the plurality of nodes associated with the sponsoring user to a second node of the plurality of nodes associated with the enrolling user;

determine a second trust score for the second node based on a respective trust score of each of at least one node of the plurality of nodes connected to the second node by a respective edge of the plurality of edges, the at least one node of the plurality of nodes comprising the first node, the first node being associated with a first trust score;

receive second image data associated with a second image of a government identification document of the enrolling user; and

approve the enrolling user and/or the government identification document based on the second trust score.