

CLAIMS

1. A system comprising:
 - an application layer comprising at least one blockchain-based application program configured to perform a plurality of steps to provide a service; and
 - a trusted service layer comprising a trusted timing module, a trusted identity module, and a trusted computing module;wherein for each step of at least some of the plurality of steps,
 - the application program is configured to perform, at least one of obtaining a verified time stamp from the trusted timing module, obtaining a verified identity from the trusted identity module, or obtaining a computation result based on a processing of blockchain data using the trusted computing module, and
 - the trusted computing module is configured to record information about the corresponding step that is performed by the application program and at least one of the verified time stamp, the verified identity, or the computation result in a blockchain.
2. The system of claim 1, wherein the trusted computing module is configured to, in response to a request for a verified record associated with the service, provide the verified record of the plurality of steps performed by the application program and the at least one of the verified time stamp, the verified identity, or the computation result associated with each step of the plurality of steps.
3. The system of claim 1, wherein the trusted computing module comprises one or more data processors having a trusted execution environment (TEE) that is isolated from the one or more data processors' operating system and configured to provide enhanced confidentiality and integrity of code executing, and data loaded within, the one or more data processors.
4. The system of claim 3, wherein the blockchain based application program comprises a trusted component that is configured to be executed in the trusted execution environment and record the plurality of steps performed by the application program and the at least one of

the verified time stamp, the verified identity, or the computation result associated with each step of the plurality of steps.

5. The system of claim 4, wherein the trusted component comprises a hash computation component that is configured to generate hash values of data representing the steps performed by the application program based on a hash algorithm.

6. The system of claim 1, wherein the blockchain based application program is configured to invoke functions of the trusted timing module, the trusted identity module, or the trusted computing module through a corresponding application programming interface (API) associated with the trusted timing module, the trusted identity module, or the trusted computing module.

7. The system of claim 1, wherein the trusted timing module is configured to generate time stamps based on at least one of (i) national standard timing information, or (ii) timing information obtained from a global positioning system.

8. The system of claim 1, wherein the trusted timing module is configured to generate time stamps associated with a first user using a first standard time recognized by a first court system associated with the first user, and to generate time stamps associated with a second user using a second standard time recognized by a second court system associated with the second user, in which the first and second users reside in different regions having different court systems.

9. The system of claim 1, wherein the trusted identity module is configured to verify an identity of a user based on one or more of identifiers associated with the user, the identifiers including at least one of (i) a mobile phone number, (ii) a credit card number, (iii) a user ID associated with an online payment system, (iv) a user ID associated with an online shopping account, (v) a user ID associated with a music streaming or downloading account, (vi) a user ID associated with a movie streaming or downloading account, (vii) a user ID associated with a messaging or chat account, (viii) a user ID associated with an online banking account, (ix) a user ID associated with a ride hailing service, (x) a user ID associated with an online

food ordering service, (xi) a social security number, (xii) a driver's license number, (xiii) a passport number, (xiv) a user ID associated with an online gaming service, (xv) an ID issued by a government entity, (xvi) one or more fingerprints, (xvii) one or more voice prints, or (xviii) iris information.

10. The system of claim 1, wherein the trusted identity module is configured to verify the identity of a first user using at least one of a first set of identifiers recognized by a first court system associated with the first user, and to verify the identity of a second user using at least one of a second set of identifiers recognized by a second court system associated with the second user, in which the first and second users reside in different regions having different court systems.

11. The system of claim 1, wherein the trusted computing module is configured to record information associated with the user in compliance with privacy laws.

12. The system of claim 1, wherein the blockchain based application program provides a shopping service to enable the user to search for information about a product provided by a seller and place an order for the product,

wherein the application program is configured to invoke the trusted identity module to verify an identity of the user and an identity of the seller, and invoke the trusted timing module to verify a timing of placement of the order by the user.

13. The system of claim 12, wherein the blockchain based application program is configured to invoke the trusted computing module to update the blockchain, and the blockchain is configured to include data representing online activities of the user associated with the placement of the order of the product.

14. The system of claim 13, wherein the blockchain based application program is configured to invoke the trusted computing module to update the blockchain to include data representing information shown to the user and each piece of information provided by the user to the seller after the user initiates a checkout process, an identity of the user, an identity of the seller, and a timing of the placement of the order.

15. The system of claim 14, wherein the information shown to the user after the user initiates the checkout process includes a description of the product that is being ordered, a price of the product, an identifier of the seller, a name of an entity to receive the product, a shipping address, and a message asking the user to confirm placement of the order.

16. The system of claim 1, wherein the blockchain based application program comprises a web browser configured to enable the user to view web pages on a network and save contents of one or more of the web pages in a storage,

wherein the application program is configured to invoke the trusted identity module to verify an identity of the user, and invoke the trusted timing module to verify a timing that a web page has been viewed and/or saved by the user.

17. The system of claim 16, wherein the blockchain based application program is configured to invoke the trusted computing module to update the blockchain, and the blockchain is configured to include data representing contents of web pages viewed and/or saved by the user, URLs of the web pages, an identity of the user, and time stamps showing when the web pages were viewed and/or saved by the user.

18. The system of claim 1, wherein the blockchain based application program provides an online agreement signing service to enable two or more parties to enter into an agreement online,

wherein the application program is configured to invoke the trusted identity module to verify identities of parties to the agreement, and invoke the trusted timing module to verify a timing of signing the agreement by each of the parties.

19. The system of claim 18, wherein the blockchain based application program invokes the trusted computing module to update the blockchain, and the blockchain is configured to include data representing online activities of the parties associated with the signing of the agreement.

20. The system of claim 18, wherein the blockchain based application program invokes the trusted computing module to update the blockchain to include data representing (i) contents of the agreement signed by each party, (ii) modifications, if any, made to the agreement by each party, (iii) identity of each party signing the agreement, and (iv) time stamps shown when the agreement was signed by each party.

21. A method comprising:
at a blockchain-based trusted platform, providing a service to a user in a plurality of steps;

for each step of the plurality of steps, performing at least one of obtaining a verified time stamp from a trusted timing module of the trusted platform, obtaining a verified identity from a trusted identity module of the trusted platform, or obtaining a computation result from a trusted computing module of the trusted platform, and

recording data associated with the service provided to the user and at least one of the verified time stamp, the verified identity, or the computation result associated with the step in a blockchain.

22. The method of claim 21, comprising in response to a request for a verified record associated with the service, providing the verified record of the plurality of steps performed by an application program and the at least one of the verified time stamp, the verified identity, or the computation result associated with each step of the plurality of steps.

23. The method of claim 21, comprising using the trusted computing module to process blockchain data of the blockchain using one or more data processors having a trusted execution environment (TEE) that is isolated from the one or more data processors' operating system and configured to provide enhanced confidentiality and integrity of code executing, and data loaded within, the one or more data processors.

24. The method of claim 23, comprising executing a trusted component associated with provisioning of the service in the TEE and recording the plurality of steps of the service

provided to the user and the at least one of the verified time stamp, the verified identity, or the computation result associated with each step of the plurality of steps in the blockchain.

25. The method of claim 24, wherein executing the trusted component comprises calculating hash values of data associated with the steps of the services provided to the user based on a hash algorithm.

26. The method of claim 21, comprising, at a blockchain based application program of the trusted platform configured to provide the service to the user, invoking functions of the trusted timing module, the trusted identity module, or the trusted computing module through a corresponding application programming interface (API) associated with the trusted timing module, the trusted identity module, or the trusted computing module.

27. The method of claim 21, comprising at the trusted timing module, generating time stamps based on at least one of (i) national standard timing information, or (ii) timing information obtained from a global positioning system.

28. The method of claim 21, comprising at the trusted timing module, generating time stamps associated with a first user using a first standard time recognized by a first court system associated with the first user, and generating time stamps associated with a second user using a second standard time recognized by a second court system associated with the second user, in which the first and second users reside in different regions having different court systems.

29. The method of claim 21, comprising at the trusted identity module, verifying an identity of a user based on one or more of identifiers associated with the user, the identifiers including at least one of (i) a mobile phone number, (ii) a credit card number, (iii) a user ID associated with an online payment system, (iv) a user ID associated with an online shopping account, (v) a user ID associated with a music streaming or downloading account, (vi) a user ID associated with a movie streaming or downloading account, (vii) a user ID associated with a messaging or chat account, (viii) a user ID associated with an online banking account, (ix) a user ID associated with a ride hailing service, (x) a user ID associated with an online

food ordering service, (xi) a social security number, (xii) a driver's license number, (xiii) a passport number, (xiv) a user ID associated with an online gaming service, (xv) an ID issued by a government entity, (xvi) one or more fingerprints, (xvii) one or more voice prints, or (xviii) iris information.

30. The method of claim 21, comprising at the trusted identity module, verifying the identity of a first user using at least one of a first set of identifiers recognized by a first court system associated with the first user, and verifying the identity of a second user using at least one of a second set of identifiers recognized by a second court system associated with the second user, in which the first and second users reside in different regions having different court systems.

31. The method of claim 21, comprising at the trusted computing module, recording information associated with the user in compliance with privacy laws.

32. The method of claim 21, wherein providing the service comprises providing a shopping service to enable the user to search for information about a product provided by a seller and place an order for the product,

and the method comprises invoking the trusted identity module to verify an identity of the user and an identity of the seller, and invoking the trusted timing module to verify a timing of placement of the order by the user.

33. The method of claim 32, comprising invoking the trusted computing module to update the blockchain, in which the blockchain is configured to include data representing online activities of the user associated with the placement of the order of the product.

34. The method of claim 33, comprising invoking the trusted computing module to update the blockchain to include data representing information shown to the user and each piece of information provided by the user to the seller after the user initiates a checkout process, an identity of the user, an identity of the seller, and a timing of the placement of the order.

35. The method of claim 34, wherein the information shown to the user after the user initiates the checkout process includes a description of the product that is being ordered, a price of the product, an identifier of the seller, a name of an entity to receive the product, a shipping address, and a message asking the user to confirm placement of the order.

36. The method of claim 21, wherein providing the service comprises providing a web browser configured to enable the user to view web pages on a network and save contents of one or more of the web pages in a storage,

and the method comprises invoking the trusted identity module to verify an identity of the user, and invoking the trusted timing module to verify a timing that a web page has been viewed and/or saved by the user.

37. The method of claim 36, comprising invoking the trusted computing module to update the blockchain, in which the blockchain is configured to include data representing contents of web pages viewed and/or saved by the user, URLs of the web pages, an identity of the user, and time stamps showing when the web pages were viewed and/or saved by the user.

38. The method of claim 21, wherein providing the service comprises providing an online agreement signing service to enable two or more parties to enter into an agreement online,

and the method comprises invoking the trusted identity module to verify identities of parties to the agreement, and invoking the trusted timing module to verify a timing of signing the agreement by each of the parties.

39. The method of claim 38, wherein the blockchain based application program invokes the trusted computing module to update the blockchain, in which the blockchain is configured to include data representing online activities of the parties associated with the signing of the agreement.

40. The method of claim 38, comprising invoking the trusted computing module to update the blockchain to include data representing (i) contents of the agreement signed by

each party, (ii) modifications, if any, made to the agreement by each party, (iii) identity of each party signing the agreement, and (iv) time stamps shown when the agreement was signed by each party.

41. An apparatus for providing a service, the apparatus comprising a plurality of modules for performing the method of any of claims 21 to 40.