CLAIMS

1. A system comprising:

a blockchain-based service of process tool configured to perform a plurality of steps to serve a notice from a first party to a second party in compliance with legal requirements for service of process; and

a trusted service layer comprising a trusted timing module, a trusted identity module, and a trusted computing module;

wherein the blockchain-based service of process tool is configured to:

for each step of at least some of the plurality of steps, perform, based on a processing of blockchain data using the trusted computing module, 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;

record data associated with a corresponding step that is performed by the blockchain-based service of process tool and at least one of the verified time stamp, the verified identity, or the computation result associated with the corresponding step;

identify one or more manners of delivering the notice based on available communication methods included in registration information of the first party and registration information of the second party that are recorded on a blockchain;

deliver the notice to the second party based on at least one of the one or more manners;

receive, from an account associated with the second party, an acknowledgement for accepting the notice from the first party;

record a time the acknowledgement is received on the blockchain; and

deliver the acknowledgement to the first party based on the available communication methods included in the registration information of the first party.

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 serving of the notice to the second party, providing the verified record of the plurality of steps performed by the blockchain-based

service of process tool 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 an 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 service of process tool comprises a trusted component that is configured to be executed in the trusted execution environment and record the plurality of steps performed by the blockchain-based service of process tool 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 plurality of steps performed by the blockchain-based service of process tool based on a hash algorithm.

6. The system of claim 1, wherein the blockchain-based service of process tool 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 identifiers associated with the user, the one or more 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, or (xv) an ID issued by a government entity.

10. The system of claim 1, wherein the trusted identity module is configured to verify an 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 an 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 a user in compliance with privacy laws.

12. The system of claim 1, wherein the blockchain-based service of process tool is configured to, upon receiving a request from the first party to serve notice to the second party, invoke the trusted identity module to verify an identity of the first party and an identity of the second party, invoke the trusted timing module to verify a timing of placement of an order by a user, and invoke the trusted computing module to update a blockchain that includes data representing activities associated with service of process.

13. The system of claim 12, wherein the blockchain-based service of process tool is configured to, upon completing serving the notice to the second party, invoke the trusted identity module to verify that the second party is a party who actually received the notice, invoke the trusted timing module to verify a timing of receipt of the notice by the second party, and invoke the trusted computing module to update the blockchain that includes data representing activities associated with the service of process.

14. The system of claim 12, wherein the blockchain-based service of process tool is configured to determine a method for serving the notice to the second party based on one or more communication methods associated with one or more accounts of the second party registered on the system.

15. A computer-implemented method for facilitating blockchain-based service of process performed by a blockchain node, the method comprising:

receiving a request generated based on a blockchain-based application for delivering a notice associated with a legal action from a serving party to a party to be served, wherein the request comprises an identity associated with the serving party and an identity associated with the party to be served;

determining that the serving party is a registered user of the blockchain-based application based on matching the identity of the serving party with an identity included in registration information of the serving party recorded on a blockchain;

recording a time that the request is received on the blockchain;

determining whether the party to be served is a registered user of the blockchain-based application based on the identity associated with the party to be served;

in response to determining that the party to be served is a registered user, identifying one or more manners of delivering the notice based on available communication methods included in the registration information of the serving party and registration information of the party to be served;

delivering the notice to the party to be served based on at least one of the one or more manners;

receiving, from an account associated with the party to be served, an acknowledgement for accepting the notice from a serving party;

recording a time the acknowledgement is received on the blockchain; and

delivering the acknowledgement to the serving party based on the available communication methods included in the registration information of the serving party.

16. The method of claim 15, further comprising:

in response to determining that the party to be served is not a registered user of the blockchain-based application, sending a notification to an account associated with the serving party.

17. The method of any of claims 15 and 16, further comprising:

determining whether the party to be served is logged on to an account registered with the blockchain-based application after delivering the notice to the party to be served; and

in response to determining that the party to be served is logged on to the account registered with the blockchain-based application, sending a notification to an account associated with the serving party to notify that the notice is delivered.

18. The method of claim 17, further comprising:

in response to determining that the party to be served is not logged on to the account registered with the blockchain-based application, sending a notification to the account associated with the serving party to notify that the serving party is offline.

19. The method of any of claims 15 to 18, further comprising:

adding the time that the request is received on the blockchain, and a digital signature generated based on the time to the notice before delivering the notice to the party to be served.

20. The method of any of claims 15 to 19, wherein the available communication methods comprise at least one of: e-mail, telephone call, or instant messaging.

21. An apparatus for blockchain-based information processing, the apparatus comprising a plurality of modules for performing the method of any of claims 15 to 20.