

CLAIMS

1. A method, comprising:

receiving case event information of a first party of a case and first party evidence, the first party evidence being electronic evidence presented by the first party to support the case event information;

determining a first authenticity reference score corresponding to the first party evidence through a target procedure;

sending the case event information and the first party evidence to a second party of the case; and

in response to that it is determined that there is second party evidence, determining a second authenticity reference score corresponding to the second party evidence through the target procedure, the second party evidence being electronic evidence presented by the second party to falsify the case event information;

wherein the target procedure includes:

determining a plurality of categories of evidence, and configuring a scoring rule corresponding to a category of the plurality of categories, the plurality of categories of evidence including a first category and a second category, a first scoring rule corresponding to the first category being different from a second scoring rule corresponding to the second category;

determining a category of the plurality of categories that the target electronic evidence belongs to as a target category;

determining whether target electronic evidence has been stored by at least one candidate blockchain ledger platform, the target electronic evidence being the first party evidence or the second party evidence;

determining a first score as an authenticity reference score corresponding to the target electronic evidence based on a scoring rule corresponding to the target category and in response to that it is determined that the target electronic evidence has been stored by the at least one candidate blockchain ledger platform, the scoring rule including a plurality of score intervals each corresponding to an authenticity reference level, the authenticity reference score belonging to a score interval of the plurality of score intervals;

determining a second score as an authenticity reference score corresponding to the target electronic evidence based on the scoring rule corresponding to the target category and in response to that it is determined that the target electronic evidence is not stored by the at least one candidate blockchain ledger platform, the first score being
5 greater than the second score; and

adjusting one or more of the scoring rule or the plurality of score intervals of the scoring rule based on an authenticity confidence level of the target electronic evidence determined in a judicial procedure of the case.

2. The method according to claim 1, wherein the determining whether the
10 target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

obtaining the target electronic evidence uploaded by a user;

calculating an evidence hash of the target electronic evidence based on the target electronic evidence;

15 querying a candidate blockchain ledger platform based on the evidence hash to determine whether the evidence hash is included in a transaction stored by the candidate blockchain ledger platform;

in response to that the evidence hash is included in the transaction stored by the candidate blockchain ledger platform, determining that the target electronic evidence has
20 been stored by the candidate blockchain ledger platform; and

in response to that the evidence hash is not included in the transaction stored by the candidate blockchain ledger platform, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform.

3. The method according to claim 1, wherein the determining whether the
25 target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

obtaining a target transaction hash uploaded by a user;

querying a candidate blockchain ledger platform based on the target transaction hash to determine, among transactions recorded by the candidate blockchain

ledger platform, whether there is a transaction whose transaction hash is a same as the target transaction hash;

in response to that there is a transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain

5 ledger platform, determining electronic evidence stored by the transaction as the target electronic evidence, and determining that the target electronic evidence has been stored by the candidate blockchain ledger platform; or

in response to that there is no transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain

10 ledger platform, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform.

4. The method according to claim 1, wherein the determining whether the target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

15 obtaining the target electronic evidence and a target transaction hash uploaded by a user;

querying a candidate blockchain ledger platform based on the target transaction hash to determine, among transactions recorded by the candidate blockchain ledger platform, whether there is a transaction whose transaction hash is a same as the target transaction hash;

20

in response to there is a transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain ledger platform,

determining whether electronic evidence stored by the transaction is a same as the target electronic evidence,

25

in response to that the electronic evidence stored by the target transaction is the same as the target electronic evidence, determining that the target electronic evidence has been stored by the candidate blockchain ledger platform, and

in response to that the electronic evidence stored by the transaction is not the same as the target electronic evidence, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform; and

5 in response to there is no transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain ledger platform, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform.

5. The method according to claim 1, comprising:

10 determining, from the plurality of score intervals corresponding to the target category, a score interval into which the authenticity reference score corresponding to the target electronic evidence falls as a target score interval; and

determining an authenticity reference level corresponding to the target score interval as an authenticity reference level corresponding to the target electronic evidence.

6. The method according to claim 5, further comprising:

15 for a category of the plurality of categories,

obtaining an authenticity confidence level corresponding to each electronic evidence belonging to the category, the authenticity confidence level corresponding to the electronic evidence being confirmed by a judicial procedure;

20 selecting, among the electronic evidence belonging to the category, electronic evidence whose authenticity reference level and authenticity confidence level are inconsistent as identified electronic evidence; and

25 in response to that a ratio between an amount of the identified electronic evidence and an amount of the electronic evidence belonging to the category is greater than a threshold ratio, adjusting one or more of a scoring rule and a score interval corresponding to the category based on the authenticity confidence level corresponding to each identified electronic evidence.

7. The method according to claim 1, wherein the determining the second score as the authenticity reference score corresponding to the target electronic evidence includes:

determining whether the target electronic evidence is stored by a non-candidate blockchain ledger platform specified by a user;

in response to that the target electronic evidence is stored by the non-candidate blockchain ledger platform specified by the user, determining a third score corresponding to the target electronic evidence as the authenticity reference score corresponding to the target electronic evidence, the third score being greater than the second score and less than the first score; and

in response to that the target electronic evidence is not stored by the non-candidate blockchain ledger platform specified by the user, determining the second score as the authenticity reference score corresponding to the target electronic evidence.

8. The method according to claim 1, wherein the determining the second score includes:

determining electronic evidence most similar to the target electronic evidence among electronic evidence stored by a candidate blockchain ledger platform as similar electronic evidence corresponding to the target electronic evidence;

calculating a similarity score between the target electronic evidence and the similar electronic evidence as a similarity score corresponding to the target electronic evidence;

selecting a similarity score that is greatest among similarity scores corresponding to the target electronic evidence as a greatest similarity score;

in response to that the greatest similarity score does not meet a threshold similarity score, assigning a first score value as the second score; and

in response to that the greatest similarity score meets the threshold similarity score, determining a second score value as the second score, the second score value greater than the first score value.

9. The method according to claim 1, further comprising:
in response to it is determined that there is no second party evidence,
increasing the first authenticity reference score of the first party evidence.

10. The method according to claim 1, further comprising:
5 in response to that the second authenticity reference score corresponding to the
second party evidence meets a threshold, adjusting the first authenticity reference score
corresponding to the first party evidence.

11. The method according to claim 10, wherein the adjusting the first
authenticity reference score corresponding to the first party evidence includes:

10 in response to that the second authenticity reference score corresponding to the
second party evidence is greater than a first threshold score, decreasing the first authenticity
reference score corresponding to the first party evidence; and

in response to that the second authenticity reference score corresponding to the
second party evidence is less than a second threshold score, increasing the first authenticity
15 reference score corresponding to the first party evidence;

wherein the first threshold score is greater than the second threshold score.

12. An apparatus, comprising:

a receiving module, configured to receive case event information of a first
party of a case and first party evidence, the first party evidence being electronic evidence
20 presented by the first party to support the case event information;

an accusation evidence identification module, configured to determine a first
authenticity reference score corresponding to first party evidence through a target procedure;

a sending module, configured to send the case event information and the first
party evidence to a second party of the case; and

25 a responding evidence identification module, configured to, in response to that
it is determined that there is second party evidence, determine a second authenticity reference
score corresponding to the second party evidence through the target procedure, the second

party evidence being electronic evidence presented by the second party to falsify the case event information;

wherein the target procedure includes:

- 5 determining a plurality of categories of evidence, and configuring a scoring rule corresponding to a category of the plurality of categories, the plurality of categories of evidence including a first category and a second category, a first scoring rule corresponding to the first category being different from a second scoring rule corresponding to the second category;
- 10 determining a category of the plurality of categories that the target electronic evidence belongs to as a target category;
- determining whether target electronic evidence has been stored by at least one candidate blockchain ledger platform, the target electronic evidence being the first party evidence or the second party evidence;
- 15 determining a first score as an authenticity reference score corresponding to the target electronic evidence based on a scoring rule corresponding to the target category and in response to that it is determined that the target electronic evidence has been stored by the at least one candidate blockchain ledger platform, the scoring rule including a plurality of score intervals each corresponding to an authenticity reference level, the authenticity reference score belonging to a score interval of the plurality of score
- 20 intervals;
- determining a second score as an authenticity reference score corresponding to the target electronic evidence based on the scoring rule corresponding to the target category and in response to that it is determined that the target electronic evidence is not stored by the at least one candidate blockchain ledger platform, the first score being
- 25 greater than the second score; and
- adjusting one or more of the scoring rule or the plurality of score intervals of the scoring rule based on an authenticity confidence level of the target electronic evidence determined in a judicial procedure of the case.

13. The apparatus according to claim 12, wherein the determining whether the target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

obtaining the target electronic evidence uploaded by a user;

5 calculating an evidence hash of the target electronic evidence based on the target electronic evidence;

querying a candidate blockchain ledger platform based on the evidence hash to determine whether the evidence hash is included in a transaction stored by the candidate blockchain ledger platform;

10 in response to that the evidence hash is included in the transaction stored by the candidate blockchain ledger platform, determining that the target electronic evidence has been stored by the candidate blockchain ledger platform; or

in response to that the evidence hash is not included in the transaction stored by the candidate blockchain ledger platform, determining that the target electronic evidence
15 is not stored by the candidate blockchain ledger platform.

14. The apparatus according to claim 12, wherein the determining whether the target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

obtaining a target transaction hash uploaded by a user;

20 querying a candidate blockchain ledger platform based on the target transaction hash to determine, among transactions recorded by the candidate blockchain ledger platform, whether there is a transaction whose transaction hash is a same as the target transaction hash;

in response to that there is a transaction whose transaction hash is the same as
25 the target transaction hash among the transactions recorded by the candidate blockchain ledger platform, determining electronic evidence stored by the transaction as the target electronic evidence, and determining that the target electronic evidence has been stored by the candidate blockchain ledger platform; and

in response to that there is no transaction whose transaction hash is the same
30 as the target transaction hash among the transactions recorded by the candidate blockchain

ledger platform, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform.

15. The apparatus according to claim 12, wherein the determining whether the target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

obtaining the target electronic evidence and a target transaction hash uploaded by a user;

querying a candidate blockchain ledger platform based on the target transaction hash to determine, among transactions recorded by the candidate blockchain ledger platform, whether there is a transaction whose transaction hash is a same as the target transaction hash;

in response to that there is a transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain ledger platform,

determining whether electronic evidence stored by the transaction is a same as the target electronic evidence,

in response to that the electronic evidence stored by the target transaction is the same as the target electronic evidence, determining that the target electronic evidence has been stored by the candidate blockchain ledger platform, and

in response to that the electronic evidence stored by the transaction is not the same as the target electronic evidence, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform; and

in response to that there is no transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain ledger platform, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform.

16. The apparatus according to claim 12, wherein the target procedure includes:

determining, as a target score interval from the score intervals corresponding to the target category, a score interval into which the authenticity reference score corresponding to the target electronic evidence falls; and

5 determining an authenticity reference level corresponding to the target score interval as an authenticity reference level corresponding to the target electronic evidence.

17. The apparatus according to claim 16, wherein the target procedure further includes:

10 for a category of the plurality of categories, obtaining an authenticity confidence level corresponding to each electronic evidence belonging to the category, the authenticity confidence level corresponding to the electronic evidence being confirmed by a judicial procedure;

15 selecting, among the electronic evidence belonging to the category, electronic evidence whose authenticity reference level and authenticity confidence level are inconsistent as identified electronic evidence; and

20 in response to that a ratio between an amount of the identified electronic evidence and an amount of the electronic evidence belonging to the category is greater than a threshold ratio, adjusting one or more of a scoring rule and a score interval corresponding to the category based on the authenticity confidence level corresponding to each identified electronic evidence.

18. The apparatus according to claim 12, wherein the determining the second score as the authenticity reference score corresponding to the target electronic evidence includes:

25 determining whether the target electronic evidence is stored by a non-candidate blockchain ledger platform specified by a user;

in response to that the target electronic evidence is stored by the non-candidate blockchain ledger platform specified by the user, determining a third score corresponding to the target electronic evidence as the authenticity reference score corresponding to the target

electronic evidence, the third score being greater than the second score and less than the first score; and

in response to that the target electronic evidence is not stored by the non-candidate blockchain ledger platform specified by the user, determining the second score as the authenticity reference score corresponding to the target electronic evidence.

19. The apparatus according to claim 12, wherein the determining the second score includes:

determining electronic evidence most similar to the target electronic evidence among electronic evidence stored by a candidate blockchain ledger platform as similar electronic evidence corresponding to the target electronic evidence;

calculating a similarity score between the target electronic evidence and the similar electronic evidence as a similarity score corresponding to the target electronic evidence;

selecting a similarity score that is greatest among similarity scores corresponding to the target electronic evidence as a greatest similarity score;

in response to that the greatest similarity score does not meet a threshold similarity score, determining a first score value as the second score; and

in response to that the greatest similarity score meets the threshold similarity score, determining a second score value as the second score, the second score value greater than the first score value.

20. The apparatus according to claim 12, further comprising:

a first correction module, configured to, in response to that it is determined that there is no second party evidence, increase the first authenticity reference score corresponding to the first party evidence.

21. The apparatus according to claim 12, further comprising:

a second correction module, configured to, in response to that the second authenticity reference score corresponding to the second evidence meets a threshold, adjust the first authenticity reference score corresponding to the first party evidence.

22. The apparatus according to claim 21, wherein the second correction module is configured to:

in response to that the second authenticity reference score corresponding to the second party evidence is greater than a first threshold score, decrease the first authenticity reference score corresponding to the first party evidence; and

in response to that the second authenticity reference score corresponding to the second party evidence is less than a second threshold score, increase the first authenticity reference score corresponding to the first party evidence,

wherein the first threshold score is greater than the second threshold score.

23. A computer device, comprising a memory, a processor, and executable instructions stored in the memory, which when executed by the processor, configure the processor to implement acts including:

receiving case event information of a first party of a case and first party evidence, the first party evidence being electronic evidence presented by the first party to support the case event information;

determining a first authenticity reference score corresponding to the first party evidence through a target procedure;

sending the case event information and the first party evidence to a second party of the case; and

in response to that it is determined that there is second party evidence, determining a second authenticity reference score corresponding to the second party evidence through the target procedure, the second party evidence being electronic evidence presented by the second party to falsify the case event information;

wherein the target procedure includes:

determining a plurality of categories of evidence, and configuring a scoring rule corresponding to a category of the plurality of categories, the plurality of categories of evidence including a first category and a second category, a first scoring rule corresponding to the first category being different from a second scoring rule corresponding to the second category;

determining a category of the plurality of categories that the target electronic evidence belongs to as a target category;

determining whether target electronic evidence has been stored by at least one candidate blockchain ledger platform, the target electronic evidence being the first party evidence or the second party evidence;

determining a first score as an authenticity reference score corresponding to the target electronic evidence based on a scoring rule corresponding to the target category and in response to that it is determined that the target electronic evidence has been stored by the at least one candidate blockchain ledger platform, the scoring rule including a plurality of score intervals each corresponding to an authenticity reference level, the authenticity reference score belonging to a score interval of the plurality of score intervals;

determining a second score as an authenticity reference score corresponding to the target electronic evidence based on the scoring rule corresponding to the target category and in response to that it is determined that the target electronic evidence is not stored by the at least one candidate blockchain ledger platform, the first score being greater than the second score; and

adjusting one or more of the scoring rule or the plurality of score intervals of the scoring rule based on an authenticity confidence level of the target electronic evidence determined in a judicial procedure of the case.

24. The computing device according to claim 23, wherein the determining whether the target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

obtaining the target electronic evidence uploaded by a user;

calculating an evidence hash of the target electronic evidence based on the target electronic evidence;

querying a candidate blockchain ledger platform based on the evidence hash to determine whether the evidence hash is included in a transaction stored by the candidate blockchain ledger platform;

in response to that the evidence hash is included in the transaction stored by the candidate blockchain ledger platform, determining that the target electronic evidence has been stored by the candidate blockchain ledger platform; and

5 in response to that the evidence hash is not included in the transaction stored by the candidate blockchain ledger platform, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform.

25. The computing device according to claim 23, wherein the determining whether the target electronic evidence has been stored by the at least one candidate blockchain ledger platform includes:

10 obtaining a target transaction hash uploaded by a user;
querying a candidate blockchain ledger platform based on the target transaction hash to determine, among transactions recorded by the candidate blockchain ledger platform, whether there is a transaction whose transaction hash is a same as the target transaction hash;

15 in response to that there is a transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain ledger platform, determining electronic evidence stored by the transaction as the target electronic evidence, and determining that the target electronic evidence has been stored by the candidate blockchain ledger platform; or

20 in response to that there is no transaction whose transaction hash is the same as the target transaction hash among the transactions recorded by the candidate blockchain ledger platform, determining that the target electronic evidence is not stored by the candidate blockchain ledger platform.