

Claims

1. A method, comprising:

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;

receiving a piece of electronic evidence from a party of a legal action as target electronic evidence;

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

determining whether the target electronic evidence is stored by at least one candidate blockchain ledger platform;

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 the 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;

adopting the target electronic evidence in the legal action based on the authenticity reference score of the target electronic evidence; 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 legal action,

wherein the determining whether the target electronic evidence is 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

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.

2. The method according to claim 1, wherein the determining whether the target electronic evidence is 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 ledger platform, determining electronic evidence stored by the transaction as target electronic evidence, and determining that the target electronic evidence has been stored by the candidate blockchain ledger platform; and

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.

3. 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:

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 transactions recorded by the candidate blockchain ledger platform:

determining whether electronic evidence stored by the transaction is the 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 the electronic evidence stored by the target 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 there is no transaction whose transaction hash is 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.

4. The method according to claim 1, comprising:
determining, from the plurality of score intervals corresponding to the target category, the score interval into which the authenticity reference score corresponding to the target electronic evidence belongs to 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.

5. The method according to claim 4, further comprising 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;

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

in response to 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.

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

7. 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.

8. A non-transitory storage medium that stores computer-executable instructions, which when executed by a processor enable the processor to implement acts comprising:

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;

receiving a piece of electronic evidence from a party of a legal action as target electronic evidence;

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

determining whether the target electronic evidence is stored by at least one candidate blockchain ledger platform;

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 the determining module determines that the target electronic evidence is 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 the authenticity reference score corresponding to the target electronic evidence based on the scoring rule corresponding to the target category and in response to that the determining module determines 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;

adopting the target electronic evidence in the legal action based on the authenticity reference score of the target electronic evidence; 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 legal action,

wherein the determining whether the target electronic evidence is stored by 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

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.

9. The non-transitory storage medium according to claim 8, wherein the determining whether the target electronic evidence is stored by 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 ledger platform:

determining electronic evidence stored by the target transaction as 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 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.

10. The non-transitory storage medium according to claim 8, wherein the determining whether the target electronic evidence is stored by 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 target transaction is the same as the target electronic evidence;

in response to that the electronic evidence stored by the target transaction is the same as the 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 target 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 a 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.

11. The non-transitory storage medium according to claim 8, wherein the acts further comprise:

determining the score interval that the authenticity reference score corresponding to the target electronic evidence belongs to 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.

12. The non-transitory storage medium according to claim 11, wherein the acts further comprise:

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;

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

in response to that a ratio between the identified electronic evidence and 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.

13. The non-transitory storage medium according to claim 8, wherein the determining the second score as the authenticity reference score corresponding to the target electronic evidence comprises:

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; and

in response to 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, the third score being greater than the second score and less than the first score.

14. The non-transitory storage medium according to claim 8, wherein the determining the second score as the authenticity reference score corresponding to the target electronic evidence comprises:

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.

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

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;

receiving a piece of electronic evidence from a party of a legal action as target electronic evidence;

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

determining whether the target electronic evidence is stored by at least one candidate blockchain ledger platform;

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 the 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;

adopting the target electronic evidence in the legal action based on the authenticity reference score of the target electronic evidence; 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 legal action,

wherein the determining whether the target electronic evidence is stored by a candidate blockchain ledger platform of the at least one candidate blockchain ledger platform includes determining whether a hash corresponding to the target electronic evidence is included in a transaction stored by the candidate blockchain ledger platform.

16. The computer device according to claim 15, wherein the determining the second score as the authenticity reference score corresponding to the target electronic evidence specifically 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 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.

17. The computer device according to claim 15, 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.