

PREVENTING AN ERRONEOUS TRANSMISSION OF A COPY OF A RECORD OF DATA TO A DISTRIBUTED LEDGER SYTEM

BACKGROUND

[0001] A blockchain can be a database that can be used to ensure an authenticity of a record of data. The blockchain can be organized as a sequence of blocks. A block can be added to the blockchain after a discrete duration of time has elapsed since a previous block was added to the blockchain. A block can include one or more records of data received by an electronic ledger system within the discrete duration of time since the previous block was added to the blockchain. A current block can include a hash of the previous block, a timestamp, and the one or more records of data that are a subject of the current block. The hash of the previous block can be a cryptographic hash. Another hash can represent the one or more records of data that are the subject of the current block. The other hash can be, for example, a merkle tree root hash. Because a subsequent block can include a hash of the current block, etc., an alteration of a record of data included in the blockchain can be determined by reference to hashes included in subsequent blocks.

SUMMARY

[0001a] According to an aspect of the present disclosure, there is provided a method for preventing an erroneous transmission of a copy of a record of data to a distributed ledger system, the method comprising:

performing, by a processor, a first operation on a first copy of the record of data, wherein the first operation confirms that a format of a content within the first copy of the record of data is correct;

performing, by the processor, a second operation on a set of information, wherein the second operation confirms that a format of a first element of the set of information and a format of a second element of the set of information are correct, the set of information being about an authorization of the record of data, the authorization being used to cause a second copy of the record of data to be communicated via the distributed ledger system;

performing, by the processor, a third operation on the first element and the second element, wherein the third operation confirms that a subject matter referenced by the first element is a same as a subject matter referenced by the second element and is a same as a subject matter of the record of data;

performing, by the processor, a fourth operation, wherein the fourth operation retrieves, from a memory, a first credential and a second credential, the first credential being associated with an entity that produced the first element, the second credential being associated with an entity that produced the second element;

performing, by the processor and using the first credential and the second credential, a fifth operation, wherein the fifth operation confirms that the entity that produced the first element was authorized to produce the first element and that the entity that produced the second element was authorized to produce the second element;

performing, by the processor, a sixth operation on the set of information, wherein the sixth operation confirms that the set of information is sufficient to authorize causing the second copy of the record of data to be communicated via the distributed ledger system;

causing, by the processor and in response to a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, and the sixth operation, a first signal to be sent, the first signal providing an indication that requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system, such that the first signal causes the second copy of the record of data to be recorded in the distributed ledger system; and

preventing, by the processor and in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation, the first signal from being sent, such that erroneous transmission of a copy of the record of data to the distributed ledger system is prevented,

causing, by the processor and in response to the completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, and the sixth operation, a second signal to be sent, the second signal sent to a hardware security module, the second signal providing the indication that the requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system; and

performing, by the hardware security module and in response to a receipt of the second signal, additional operations to confirm that the requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system;

wherein the causing the first signal to be sent further comprises causing in response to a completion of the additional operations; and

wherein the preventing in response to the lack of the completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation comprises preventing in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, the sixth operation, or any of the additional operations.

[0001b] There is disclosed a non-transitory computer-readable medium storing computer code for controlling a processor to cause the processor to prevent an erroneous transmission of a copy of a record of data to a distributed ledger system, the computer code including instructions to cause the processor to:

perform a first operation on a first copy of the record of data, wherein the first operation confirms that a format of a content within the first copy of the record of data is correct;

perform a second operation on a set of information, wherein the second operation confirms that a format of a first element of the set of information and a format of a second element of the set of information are correct, the set of information being about an authorization of the record of data, the authorization being used to cause a second copy of the record of data to be communicated via the distributed ledger system;

perform a third operation on the first element and the second element, wherein the third operation confirms that a subject matter referenced by the first element is a same as a subject matter referenced by the second element and is a same as a subject matter of the record of data;

perform a fourth operation, wherein the fourth operation retrieves, from a memory, a first credential and a second credential, the first credential being associated with an entity that produced the first element, the second credential being associated with an entity that produced the second element;

perform, using the first credential and the second credential, a fifth operation, wherein the fifth operation confirms that the entity that produced the first element was authorized to produce the first element and that the entity that produced the second element was authorized to produce the second element;

perform a sixth operation on the set of information, wherein the sixth operation confirms that the set of information is sufficient to authorize causing the second copy of the record of data to be communicated via the distributed ledger system;

cause, in response to a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, and the sixth operation, a signal to be sent, the signal providing an indication that requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system; and

prevent, in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation, the signal from being sent.

[0001c] There is disclosed a system for preventing an erroneous transmission of a copy of a record of data to a distributed ledger system, the system comprising:

a memory configured to store a first copy of the record of data, a first credential, and a second credential; and

a processor configured to:

perform a first operation on the first copy of the record of data, wherein the first operation confirms that a format of a content within the first copy of the record of data is correct;

perform a second operation on a set of information, wherein the second operation confirms that a format of a first element of the set of information and a format of a second element of the set of information are correct, the set of information being about an authorization of the record of data, the authorization being used to cause a second copy of the record of data to be communicated via the distributed ledger system;

perform a third operation on the first element and the second element, wherein the third operation confirms that a subject matter referenced by the first element is a

same as a subject matter referenced by the second element and is a same as a subject matter of the record of data;

perform a fourth operation, wherein the fourth operation retrieves, from the memory, the first credential and the second credential, the first credential being associated with an entity that produced the first element, the second credential being associated with an entity that produced the second element;

perform, using the first credential and the second credential, a fifth operation, wherein the fifth operation confirms that the entity that produced the first element was authorized to produce the first element and that the entity that produced the second element was authorized to produce the second element;

perform a sixth operation on the set of information, wherein the sixth operation confirms that the set of information is sufficient to authorize causing the second copy of the record of data to be communicated via the distributed ledger system;

cause, in response to a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, and the sixth operation, a signal to be sent, the signal providing an indication that requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system; and

prevent, in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation, the signal from being sent.

[0001d] There is disclosed a method for preventing an erroneous transmission of a copy of a record of data to a distributed ledger system, the method comprising:

receiving, by a processor, a first signal, the first signal providing a first indication that requirements have been met for the copy of the record of data to be transmitted to the distributed ledger system;

receiving, by the processor, a second signal, the second signal providing a second indication that the requirements have been met for the copy of the record of data to be transmitted to the distributed ledger system;

causing, by the processor and in response to a reception of the first signal and a reception of the second signal, the copy of the record of data to be transmitted to the distributed ledger system; and

preventing, by the processor and in response to a lack of the reception of the first signal or a lack of the reception of the second signal, the copy of the record of data from being transmitted to the distributed ledger system.

[0001e] There is disclosed a non-transitory computer-readable medium storing computer code for controlling a processor to cause the processor to prevent an erroneous transmission of a copy of a record of data to a distributed ledger system, the computer code including instructions to cause the processor to:

receive a first signal, the first signal providing a first indication that requirements have been met for the copy of the record of data to be transmitted to the distributed ledger system;

receive a second signal, the second signal providing a second indication that the requirements have been met for the copy of the record of data to be transmitted to the distributed ledger system;

cause, in response to a reception of the first signal and a reception of the second signal, the copy of the record of data to be transmitted to the distributed ledger system; and

prevent, in response to a lack of the reception of the first signal or the reception of the second signal, the copy of the record of data from being transmitted to the distributed ledger system.

[0001f] There is disclosed a system for preventing an erroneous transmission of a copy of a record of data to a distributed ledger system, the system comprising:

a memory configured to store the copy of the record of data, a first signal, and a second signal; and

a processor configured to:

receive the first signal, the first signal providing a first indication that requirements have been met for the copy of the record of data to be transmitted to the distributed ledger system;

receive the second signal, the second signal providing a second indication that the requirements have been met for the copy of the record of data to be transmitted to the distributed ledger system;

cause, in response to a reception of the first signal and a reception of the second signal, the copy of the record of data to be transmitted to the distributed ledger system; and

prevent, in response to a lack of the reception of the first signal or the reception of the second signal, the copy of the record of data from being transmitted to the distributed ledger system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The accompanying drawings, which are included to provide a further understanding of the disclosed technologies, are incorporated in and constitute a part of this specification. The drawings also illustrate implementations of the disclosed technologies and together with the detailed description serve to explain the principles of implementation of the disclosed technologies. No attempt is made to show structural details in more detail than may be necessary for a fundamental understanding of the disclosed technologies and the various ways in which it can be practiced.

[0003] FIG. 1 is a diagram illustrating an example of an environment for preventing an erroneous transmission of a copy of a record of data to an electronic network, according to the disclosed technologies.

CLAIMS

1. A method for preventing an erroneous transmission of a copy of a record of data to a distributed ledger system, the method comprising:

performing, by a processor, a first operation on a first copy of the record of data, wherein the first operation confirms that a format of a content within the first copy of the record of data is correct;

performing, by the processor, a second operation on a set of information, wherein the second operation confirms that a format of a first element of the set of information and a format of a second element of the set of information are correct, the set of information being about an authorization of the record of data, the authorization being used to cause a second copy of the record of data to be communicated via the distributed ledger system;

performing, by the processor, a third operation on the first element and the second element, wherein the third operation confirms that a subject matter referenced by the first element is a same as a subject matter referenced by the second element and is a same as a subject matter of the record of data;

performing, by the processor, a fourth operation, wherein the fourth operation retrieves, from a memory, a first credential and a second credential, the first credential being associated with an entity that produced the first element, the second credential being associated with an entity that produced the second element;

performing, by the processor and using the first credential and the second credential, a fifth operation, wherein the fifth operation confirms that the entity that produced the first element was authorized to produce the first element and that the entity that produced the second element was authorized to produce the second element;

performing, by the processor, a sixth operation on the set of information, wherein the sixth operation confirms that the set of information is sufficient to authorize causing the second copy of the record of data to be communicated via the distributed ledger system;

causing, by the processor and in response to a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, and the sixth operation, a first signal to be sent, the first signal providing an indication that requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system, such that the first signal causes the second copy of the record of data to be recorded in the distributed ledger system; and

preventing, by the processor and in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation, the first signal from being sent, such that erroneous transmission of a copy of the record of data to the distributed ledger system is prevented,

causing, by the processor and in response to the completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, and the sixth operation, a second signal to be sent, the second signal sent to a hardware security module, the second signal providing the indication that the requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system; and

performing, by the hardware security module and in response to a receipt of the second signal, additional operations to confirm that the requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system;

wherein the causing the first signal to be sent further comprises causing in response to a completion of the additional operations; and

wherein the preventing in response to the lack of the completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation comprises preventing in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, the sixth operation, or any of the additional operations.

2. The method of claim 1, wherein the record of data is associated with a transaction.

3. The method of claim 1, wherein at least one of the first element or the second element comprises a digital signature.

4. The method of claim 1, further comprising:

performing, by the processor, a seventh operation, wherein the seventh operation retrieves, from the memory, a third credential, the third credential being associated with an entity that produced the record of data; and performing, by the processor and using the third credential, an eighth operation, wherein the eighth operation confirms that the entity that produced the record of data was authorized to produce the record of data.

5. The method of claim 1, further comprising causing, by the processor and in response to the lack of the completion of the first operation, the second operation, the third operation, the fourth

operation, the fifth operation, or the sixth operation, a second signal to be sent, the second signal providing an indication that the requirements have not been met for the second copy of the record of data to be communicated via the distributed ledger system.

6. The method of claim 1, further comprising:

performing, by the processor and in response to the completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, and the sixth operation, a seventh operation, wherein the seventh operation retrieves, from the memory, a third credential and performing, by the processor and in response to a retrieval of the third credential, an eighth operation, wherein the eighth operation produces the first signal, the first signal including the third credential,

wherein the causing the first signal to be sent further comprises causing in response to a completion of the seventh operation and the eighth operation and wherein the preventing in response to the lack of the completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation comprises preventing in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, the sixth operation, the seventh operation, or the eighth operation.

7. The method of claim 1, wherein the additional operations comprise:

performing, by the hardware security module, a seventh operation on the first copy of the record of data, wherein the seventh operation confirms that the format of the content within the first copy of the record of data is correct;

performing, by the hardware security module, an eighth operation on the set of information, wherein the eighth operation confirms that the format of the first element of the set of information and the format of the second element of the set of information are correct;

performing, by the hardware security module, a ninth operation on the first element and the second element, wherein the ninth operation confirms that the subject matter referenced by the first element is the same as the subject matter referenced by the second element and is the same as the subject matter of the record of data;

performing, by the hardware security module, a tenth operation, wherein the tenth operation retrieves the first credential and the second credential;

performing, by the hardware security module and using the first credential and the second credential, an eleventh operation, wherein the eleventh operation confirms that the entity that

produced the first element was authorized to produce the first element and that the entity that produced the second element was authorized to produce the second element;

performing, by the hardware security module, a twelfth operation on the set of information, wherein the twelfth operation confirms that the set of information is sufficient to authorize causing the second copy of the record of data to be communicated via the distributed ledger system;

performing, by the hardware security module and in response to a completion of the seventh operation, the eighth operation, the ninth operation, the tenth operation, the eleventh operation, and the twelfth operation, a thirteenth operation, wherein the thirteenth operation retrieves a third credential; and

causing, by the hardware security module and in response to a retrieval of the third credential, a third signal to be sent, the third signal sent to the processor, the third signal providing an indication of a confirmation that the requirements have been met for the second copy of the record of data to be communicated via the distributed ledger system, the third signal including the third credential;

wherein the causing the first signal to be sent further comprises causing in response to a receipt of the third signal; and

wherein the preventing in response to the lack of the completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, the sixth operation, or the additional operations comprises preventing in response to a lack of a completion of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, the sixth operation, the any of the additional operations, or the receipt of the third signal.

8. The method of claim 1, wherein the processor is a component of a system for preventing the erroneous transmission of the copy of the record of data to the distributed ledger system, and further comprising receiving, by the processor and from another processor of the system for preventing the erroneous transmission of the copy of the record of data to the distributed ledger system, the first copy of the record of data.

9. The method of claim 1, further comprising receiving, by the processor and from a device outside of a system for preventing the erroneous transmission of the copy of the record of data to the distributed ledger system, the first copy of the record of data.

10. The method of claim 1, wherein the causing the first signal to be sent comprises causing the first signal to be sent to another processor of a system for preventing the erroneous transmission of the copy of the record of data to the distributed ledger system

11. The method of claim 1, wherein the causing the first signal to be sent comprises causing the first signal to be sent to a device outside of a system for preventing the erroneous transmission of the copy of the record of data to the distributed ledger system.

12. The method of claim 1, further comprising:

- performing, by the processor, a seventh operation on an instruction, wherein the seventh operation confirms that a format of the instruction is correct, the instruction being about a modification to a requirement associated with at least one of the first operation, the second operation, the third operation, the fourth operation, the fifth operation, or the sixth operation;

- performing, by the processor, an eighth operation, wherein the eighth operation retrieves, from the memory, a third credential, the third credential being associated with an entity that produced the instruction;

- performing, by the processor and using the third credential, a ninth operation, the ninth operation confirms that the entity that produced the instruction was authorized to produce the instruction; and

- causing, by the processor and in response to a completion of the seventh operation, the eighth operation, and the ninth operation, the instruction to be implemented.

13. A non-transitory computer-readable medium storing computer code for controlling a processor to cause the processor to prevent an erroneous transmission of a copy of a record of data to a distributed ledger system, the computer code including instructions to cause the processor to perform the method of any preceding claim.

14. A system for preventing an erroneous transmission of a copy of a record of data to a distributed ledger system, the system comprising:

- a memory configured to store the copy of the record of data, a first signal, and a second signal; and

- a processor configured to perform the method of any one of claims 1 to 12.