SYSTEMS AND METHODS FOR INTERCEPTION OF SMART CONTRACTS

CROSS REFERENCE TO RELATED APPLICATIONS

[01] This application claims priority to U.S. Provisional Patent Application No. 62/396,293, filed on September 19, 2016, and U.S. Patent Application No. 15/707,571, filed on September 18, 2017, each of which are hereby incorporated by reference herein in their entireties.

BACKGROUND INFORMATION

[02] Distributed ledger systems provide a platform for the execution of smart contracts. Smart contracts typically include program instructions that may be executed in response to a transaction in the distributed ledger system addressed to the contract. Smart contracts may also represent legal contracts between users, with program functions of the smart contracts implementing terms, conditions, etc. of the legal contract.

[03] Properties of distributed ledger systems provide improved immutability of data, such as transactions and smart contracts of such systems, ensuring that such data may be written to the system but not tampered with. Implementing legal contracts and other functionality using smart contracts thus provides a highly reliable way to implement such functions.

[04] Unfortunately, problems exist with the execution of smart contracts in distributed ledger systems. For example, a legal contract represented by the smart contract may represent an illegal transaction in some jurisdictions. Additionally, the smart contract may include logical errors that cause it to execute a transaction different from that agreed to by parties to the legal contract. However, the immutability of the transactions, contracts, etc. provided by the distributed ledger system may be a barrier to actions to stop execution of such a contract.

[05] Thus, a need exists for systems and methods to provide improved intervention in the operation of smart contracts in a distributed ledger system.

SUMMARY

[05a] According to a first aspect of the present invention, there is provided a method of intervening in the operation of a smart contract in a distributed ledger system, the method comprising: launching, by a processor of a distributed node of the distributed ledger system, execution of program instructions of the smart contract, the program instructions being stored in a ledger structure of the distributed ledger system; upon launching execution of the smart contract, executing by the processor a judgment checking function of the program

instructions of the smart contract to determine whether a judgment against the smart contract exists in a judgment database, wherein the judgement is that the smart contract is illegal or contains a logical error, and wherein the program instructions of the judgment checking function invoke execution of a second smart contract by the processor of the distributed node, the program instructions of the second smart contract being stored in a ledger structure of the distributed ledger system, the execution of the program instructions of the second smart contract performing a read of a data structure in which the second smart contract has stored the judgment database in the distributed ledger system, the invoking of the second smart contract by the program instructions of the smart contract including communicating by the smart contract an input to the second smart contract including an identifier of the smart contract, and receiving by the smart contract an output from the second smart contract indicating whether the judgment against the smart contract exists in the judgment database; in response to a judgment against the smart contract existing in the judgment database, intervening by the program instructions of the smart contract in the operation of the smart contract to prevent further execution of the smart contract by the distributed node, the intervening including executing a first set of the program instructions of the smart contract, the first set of the program instructions including at least one of: (i) a throw function, or (ii) a self destruct function that deletes data of the smart contract from the distributed ledger system; and in response to no judgment against the smart contract existing in the judgment database, continuing execution of the smart contract by the distributed node, the continuing executing including executing a second set of the program instructions of the smart contract, the second set being different than the first set.

[05b] As disclosed, there is provided a method of intervening in the operation of a smart contract in a distributed ledger system, the method comprising: determining, by a server system, a judgment of a validity of a complaint against the smart contract based on input received from one or more judge systems; in response to the judgment upholding the validity of the complaint against the smart contract, recording the judgment in a judgment database; receiving a request, from a judgment checking function, to determine whether the judgment against the smart contract exists in the judgment database in response to launching execution of the smart contract; and transmitting a response to the request indicating whether the judgment exists in the judgment database.

[05c] According to a second aspect of the present invention, there is provided a system for intervening in the operation of a smart contract in a distributed ledger system, the system

configured to: launch execution of program instructions of the smart contract, the program instructions being stored in a ledger structure of the distributed ledger system; upon launching execution of the smart contract, execute a judgment checking function of the program instructions of the smart contract to determine whether a judgment against the smart contract exists in a judgment database, wherein the judgement is that the smart contract is illegal or contains a logical error, and wherein the program instructions of the judgment checking function invoke execution of a second smart contract by the processor of the distributed node, the program instructions of the second smart contract being stored in a ledger structure of the distributed ledger system, the execution of the program instructions of the second smart contract performing a read of a data structure in which the second smart contract has stored the judgment database in the distributed ledger system, the invoking of the second smart contract by the program instructions of the smart contract including communicating by the smart contract an input to the second smart contract including an identifier of the smart contract, and receiving by the smart contract an output from the second smart contract indicating whether the judgment against the smart contract exists in the judgment database; in response to a judgment against the smart contract existing in the judgment database, intervene by the program instructions of the smart contract in the operation of the smart contract to prevent further execution of the smart contract, the intervening including executing a first set of the program instructions of the smart contract, the first set of the program instructions including at least one of: (i) a throw function, or (ii) a self destruct function that deletes data of the smart contract from the distributed ledger system; and in response to no judgment against the smart contract existing in the judgment database, continue execution of the smart contract, the continuing executing including executing a second set of the program instructions of the smart contract, the second set being different than the first set.

[05d] According to a third aspect of the present invention, there is provided at least one non-transitory, machine-readable storage medium having program instructions, which when executed by at least one processor cause a method for intervening in the operation of a smart contract in a distributed ledger system to be performed, the method including: launching, by a processor of a distributed node of the distributed ledger system, execution of program instructions of the smart contract, the program instructions being stored in a ledger structure of the distributed ledger system; upon launching execution of the smart contract, executing by the processor a judgment checking function of the program instructions of the smart contract

to determine whether a judgment against the smart contract exists in a judgment database, wherein the judgement is that the smart contract is illegal or contains a logical error, and wherein the program instructions of the judgment checking function invoke execution of a second smart contract by the processor of the distributed node, the program instructions of the second smart contract being stored in a ledger structure of the distributed ledger system, the execution of the program instructions of the second smart contract performing a read of a data structure in which the second smart contract has stored the judgment database in the distributed ledger system, the invoking of the second smart contract by the program instructions of the smart contract including communicating by the smart contract an input to the second smart contract including an identifier of the smart contract, and receiving by the smart contract an output from the second smart contract indicating whether the judgment against the smart contract exists in the judgment database; in response to a judgment against the smart contract existing in the judgment database, intervening by the program instructions of the smart contract in the operation of the smart contract to prevent further execution of the smart contract by the distributed node, the intervening including executing a first set of the program instructions of the smart contract, the first set of the program instructions including at least one of: (i) a throw function, or (ii) a self destruct function that deletes data of the smart contract from the distributed ledger system; and in response to no judgment against the smart contract existing in the judgment database, continuing execution of the smart contract by the distributed node, the continuing executing including executing a second set of the program instructions of the smart contract, the second set being different than the first set.

BRIEF DESCRIPTION OF THE DRAWINGS

[06] So that the features of the present invention can be understood, a number of drawings are described below. However, the appended drawings illustrate only particular embodiments of the invention and are therefore not to be considered limiting of its scope, for the invention may encompass other equally effective embodiments.

WHAT IS CLAIMED IS:

1. A method of intervening in the operation of a smart contract in a distributed ledger system, the method comprising:

launching, by a processor of a distributed node of the distributed ledger system, execution of program instructions of the smart contract, the program instructions being stored in a ledger structure of the distributed ledger system;

upon launching execution of the smart contract, executing by the processor a judgment checking function of the program instructions of the smart contract to determine whether a judgment against the smart contract exists in a judgment database, wherein the judgement is that the smart contract is illegal or contains a logical error, and wherein the program instructions of the judgment checking function invoke execution of a second smart contract by the processor of the distributed node, the program instructions of the second smart contract being stored in a ledger structure of the distributed ledger system, the execution of the program instructions of the second smart contract performing a read of a data structure in which the second smart contract has stored the judgment database in the distributed ledger system, the invoking of the second smart contract by the program instructions of the smart contract including communicating by the smart contract an input to the second smart contract including an identifier of the smart contract, and receiving by the smart contract an output from the second smart contract indicating whether the judgment against the smart contract exists in the judgment database;

in response to a judgment against the smart contract existing in the judgment database, intervening by the program instructions of the smart contract in the operation of the smart contract to prevent further execution of the smart contract by the distributed node, the intervening including executing a first set of the program instructions of the smart contract, the first set of the program instructions including at least one of: (i) a throw function, or (ii) a self destruct function that deletes data of the smart contract from the distributed ledger system; and

in response to no judgment against the smart contract existing in the judgment database, continuing execution of the smart contract by the distributed node, the continuing executing including executing a second set of the program instructions of the smart contract, the second set being different than the first set.

2. The method of claim 1, wherein continuing execution of the smart contract by the distributed node includes at least one of: completing a financial transaction by the smart contract, or identifying an individual by the smart contract.

3. The method of claim 1, further comprising:

determining the judgment of a validity of a complaint against the smart contract based on input received from one or more judge systems;

in response to the judgment upholding the validity of the complaint against the smart contract, recording the judgment in the judgment database.

4. The method of claim 3, wherein recording the judgment in the judgment database includes generating a transaction addressed to the second smart contract of the distributed ledger system, the transaction containing an instruction to write the judgment and an identifier of the smart contract to the data structure of the second smart contract, and transmitting the transaction to a distributed node of the distributed ledger system.

5. The method of claim 3, further comprising receiving, by the server system from a complainant system, the complaint regarding the smart contract.

6. A system for intervening in the operation of a smart contract in a distributed ledger system, the system configured to:

launch execution of program instructions of the smart contract, the program instructions being stored in a ledger structure of the distributed ledger system;

upon launching execution of the smart contract, execute a judgment checking function of the program instructions of the smart contract to determine whether a judgment against the smart contract exists in a judgment database, wherein the judgement is that the smart contract is illegal or contains a logical error, and wherein the program instructions of the judgment checking function invoke execution of a second smart contract by the processor of the distributed node, the program instructions of the second smart contract being stored in a ledger structure of the distributed ledger system, the execution of the program instructions of the second smart contract performing a read of a data structure in which the second smart contract has stored the judgment

database in the distributed ledger system, the invoking of the second smart contract by the program instructions of the smart contract including communicating by the smart contract an input to the second smart contract including an identifier of the smart contract, and receiving by the smart contract an output from the second smart contract indicating whether the judgment against the smart contract exists in the judgment database;

in response to a judgment against the smart contract existing in the judgment database, intervene by the program instructions of the smart contract in the operation of the smart contract to prevent further execution of the smart contract, the intervening including executing a first set of the program instructions of the smart contract, the first set of the program instructions including at least one of: (i) a throw function, or (ii) a self destruct function that deletes data of the smart contract from the distributed ledger system; and

in response to no judgment against the smart contract existing in the judgment database, continue execution of the smart contract, the continuing executing including executing a second set of the program instructions of the smart contract, the second set being different than the first set.

7. The system of claim 6, wherein continuing execution of the smart contract by the distributed node includes at least one of: completing a financial transaction by the smart contract, or identifying an individual by the smart contract.

8. The system of claim 6, further configured to:

determine the judgment of the validity of a complaint against the smart contract based on input received from one or more judge systems; and

in response to the judgment upholding the validity of the complaint against the smart contract, record the judgment in the judgment database.

9. The system of claim 8, wherein recording the judgment in the judgment database includes generating a transaction addressed to the second smart contract of the distributed ledger system, the transaction containing an instruction to write the judgment and an identifier of the smart

contract to the data structure of the second smart contract, and transmitting the transaction to a distributed node of the distributed ledger system.

10. The system of claim 8, further comprising receiving, by the server system from a complainant system, the complaint regarding the smart contract.

11. At least one non-transitory, machine-readable storage medium having program instructions, which when executed by at least one processor cause a method for intervening in the operation of a smart contract in a distributed ledger system to be performed, the method including:

launching, by a processor of a distributed node of the distributed ledger system, execution of program instructions of the smart contract, the program instructions being stored in a ledger structure of the distributed ledger system;

upon launching execution of the smart contract, executing by the processor a judgment checking function of the program instructions of the smart contract to determine whether a judgment against the smart contract exists in a judgment database, wherein the judgement is that the smart contract is illegal or contains a logical error, and wherein the program instructions of the judgment checking function invoke execution of a second smart contract by the processor of the distributed node, the program instructions of the second smart contract being stored in a ledger structure of the distributed ledger system, the execution of the program instructions of the second smart contract performing a read of a data structure in which the second smart contract has stored the judgment database in the distributed ledger system, the invoking of the second smart contract by the program instructions of the smart contract including communicating by the smart contract an input to the second smart contract including an identifier of the smart contract, and receiving by the smart contract an output from the second smart contract indicating whether the judgment against the smart contract exists in the judgment database;

in response to a judgment against the smart contract existing in the judgment database, intervening by the program instructions of the smart contract in the operation of the smart contract to prevent further execution of the smart contract by the distributed node, the intervening including executing a first set of the program instructions of the smart contract, the

first set of the program instructions including at least one of: (i) a throw function, or (ii) a self destruct function that deletes data of the smart contract from the distributed ledger system; and

in response to no judgment against the smart contract existing in the judgment database, continuing execution of the smart contract by the distributed node, the continuing executing including executing a second set of the program instructions of the smart contract, the second set being different than the first set.

12. The non-transitory machine-readable storage medium of claim 11, wherein continuing execution of the smart contract by the distributed node includes at least one of: completing a financial transaction by the smart contract, or identifying an individual by the smart contract.

13. The non-transitory machine-readable storage medium of claim 11, further configured to:

determine the judgment of the validity of a complaint against the smart contract based on input received from one or more judge systems; and

in response to the judgment upholding the validity of the complaint against the smart contract, record the judgment in the judgment database.

14. The non-transitory machine-readable storage medium of claim 13, wherein recording the judgment in the judgment database includes generating a transaction addressed to the second smart contract of the distributed ledger system, the transaction containing an instruction to write the judgment and an identifier of the smart contract to the data structure of the second smart contract, and transmitting the transaction to a distributed node of the distributed ledger system.

15. The non-transitory machine-readable storage medium of claim 13, further comprising receiving, by the server system from a complainant system, the complaint regarding the smart contract.