CLAIMS

1. A system for assessing future execution of a smart contract based on previous executions on a blockchain-based platform, comprising:

   A blockchain computer system that hosts an original smart contract and stores and maintains a blockchain ledger; and

   An off-chain computer system that is not part of the blockchain system and does not store or maintain the blockchain ledger, the off-chain system is configured to automatically perform an off-chain comparison between the behavior of the original smart contract and a new smart contract;

   Wherein the off-chain computer system having at least one application that is configured to retrieve transaction data together with the original smart contract from the blockchain ledger of the blockchain computer system, to identify at least one base path of the original smart contract, wherein the base path are flows through the code of the smart contract that indicate how the system worked in the past, and accordingly to create a base path that includes an initial state of an original transaction of the identified base path, to simulate a transaction using the initial state of the original transaction of the identified base path, but with instructions of the new smart contract, to decide whether the behavior of the original and new smart contracts are identical or differ, and accordingly to generate an insight.

2. The system according to claim 1, in which the off-chain computer system is implemented by using one or more processors, a memory and

one or more persistent storage devices that allow the off-chain computer system to store data and host one or more applications and communicate with the blockchain computer system over a communications path and interact with the blockchain ledger in order to reproduce a transaction's execution by the off-chain computer system.

3. A method for assessing future execution of a smart contract based on previous executions on a blockchain-based platform, comprising:

providing a blockchain computer system that hosts an original smart contract and stores and maintains a blockchain ledger;

providing an off-chain computer system that is not part of the blockchain system and does not store or maintain the blockchain ledger, the off-chain system having at least one an application that is configured to perform a comparison between the behavior of the original smart contract and a new smart contract; and

retrieving, by the off-chain computer system, data from the blockchain computer system, wherein said data comprising actual data inputs provided to the smart contract, the smart contract's code, and data relative to fetch state of the blockchain system when a transaction was executed, in order to reproduce a transaction's execution by the off-chain system, thereby evaluating a new version of a smart contract based on the actual behavior of a previous version of a smart contract that was used before in the blockchain computer system.

4. The method according to claim 3, wherein the comparison comprising:

retrieving, by the off-chain computer system, transaction data together with the original smart contract from the blockchain ledger of the blockchain computer system;

identifying, by the off-chain computer system, at least one base path of the original smart contract, wherein the base path are flows through the code of the smart contract that indicate how the system worked in the past, and accordingly creating a base path that includes an initial state of an original transaction of the identified base path;

simulating, by the off-chain computer system, a transaction using the initial state of the original transaction of the identified base path, but with instructions of the new smart contract; and

deciding, by the off-chain computer system, whether the original smart contact and the new smart contract are identical or differ in their behavior, and accordingly generating an insight.

5. The method according to claim 3, wherein the off-chain computer system fetches the state of the blockchain computer system by utilizing capabilities of blockchain implementations to read the state of the blockchain computer system at a given address at a given time, thereby enabling the off-chain computer system to reproduce the state of the blockchain computer system when a desired transaction was executed.

6. The method according to claim 4, further comprising handling new reads in case the new smart contract performs memory reads from a memory address that the off-chain computer system does not have in

the created base path, the off-chain computer system indicating the two contracts are different in the context of this specific transaction, ending the simulation, and concluding the transactions are 'very' different.

7. The method according to claim 4, further comprising handling new reads in case the new smart contract performs memory reads from a memory address that the off-chain computer system does not have in the created base path, the off-chain computer system: attempting to calculate the value at said memory address when the transaction executed originally.

8. The method according to claim 3, further comprising comparing the behaviors of two smart contracts over a plurality of transactions, wherein for each transaction, the off-chain computer system determines how different the behaviors of the two contracts were in the context of that transaction, and accordingly classifying the smart contracts into categories that is used to describe how different the contracts are under the specific context of that transaction.

9. The method according to claim 3, wherein using the results of a plurality of transactions, the off-chain computer system determines how different the smart contracts are in a wider context of many transactions.

10. A non-transitory computer-readable medium comprising instructions which when executed by at least one processor causes the processor to perform the method of claim 3.