

CLAIMS

What is claimed is:

1. A computer-implemented method for blockchain-based loan management, comprising:

receiving, by a blockchain node associated with a blockchain, a first blockchain transaction comprising an encrypted unit loan amount associated with a loan request, wherein the loan request is associated with a total loan amount that equals the unit loan amount multiplied by a total number of units;

receiving, by the blockchain node, a plurality of second blockchain transactions, each of the second blockchain transactions comprising an encrypted number of units;

receiving, by the blockchain node, a third blockchain transaction specifying a subset of the second blockchain transactions; and

executing, by the blockchain node, a blockchain contract associated with the blockchain to determine and store an encrypted loan amount corresponding to each second blockchain transaction of the subset based on the encrypted unit loan amount and the encrypted number of units in the second blockchain transaction;

wherein the encrypted unit loan amount, the encrypted number of units, and the encrypted loan amount are generated based on a homomorphic encryption scheme.

2. The method of claim 1, further comprising:

receiving, by the blockchain node, a fourth blockchain transaction comprising an encrypted unit repayment amount; and

executing, by the blockchain node, the blockchain contract to update the encrypted loan amount corresponding to each second blockchain transaction of the subset based on the encrypted unit repayment amount and the encrypted number of units in the second blockchain transaction

3. The method of claim 2, wherein the executing the blockchain contract to update the encrypted loan amount corresponding to each second blockchain transaction of the subset comprises, for each second blockchain transaction of the subset, executing, by the blockchain node, the blockchain contract to:

determine an encrypted difference between the encrypted unit loan amount and the encrypted unit repayment amount; and

update the encrypted loan amount as a product of the encrypted difference and the encrypted number of units in the second blockchain transaction.

4. The method of claim 1, further comprising:

executing, by the blockchain node, the blockchain contract to determine and store an encrypted debt amount corresponding to the first blockchain transaction, the encrypted debt amount comprising a sum of the encrypted loan amount corresponding to each second blockchain transaction of the subset.

5. The method of claim 4, further comprising:

receiving, by the blockchain node, a fourth blockchain transaction comprising an encrypted unit repayment amount; and

executing, by the blockchain node, the blockchain contract to update the encrypted debt amount corresponding to the first blockchain transaction based on the encrypted unit repayment amount and the encrypted number of units in each second blockchain transaction of the subset.

6. The method of claim 1, further comprising:

sending, by a first computing system associated with the first blockchain transaction, the unit loan amount to one or more second computing systems associated with the plurality of second blockchain transactions via an off-blockchain channel.

7. The method of claim 1, further comprising:

receiving, by the blockchain node, a range claimed to encompass the unit loan amount and a zero-knowledge range proof that the unit loan amount falls within the claimed range.

8. The method of claim 1, wherein:

the homomorphic encryption scheme is a Somewhat Homomorphic Encryption (SWHE) scheme based on a public key associated with the first blockchain transaction.

9. The method of claim 1, wherein:

the first blockchain transaction further comprises a first unique identifier; and

each of the plurality of second blockchain transactions further comprises the first unique identifier of the first blockchain transaction and a second unique identifier.

10. The method of claim 9, wherein:

the third blockchain transaction comprises a plurality of the second unique identifiers respectively corresponding to the subset of the second blockchain transactions.

11. The method of claim 9, wherein:

the plurality of second blockchain transactions are sorted in a chronological order, and

the third blockchain transaction comprises a number K indicating that first K of the plurality of second blockchain transactions are to be included in the subset of the second blockchain transactions.

12. The method of claim 1, wherein:

the third blockchain transaction further comprises an encrypted residual number of units for one of the subset of the second blockchain transactions, wherein the encrypted residual number of units is smaller than the encrypted number of units corresponding to the one of the subset of the second blockchain transactions.

13. The method of claim 1, wherein the encrypted loan amount corresponding to each second blockchain transaction of the subset comprises a product of the encrypted unit loan amount and the encrypted number of units associated with the second blockchain transaction.

14. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform the method of any one of the claims 1-13.

15. An apparatus for blockchain-based loan management comprising a plurality of modules for performing the method of any one of the claims 1-13.

16. A system for blockchain-based loan management comprising one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

receiving a first blockchain transaction comprising an encrypted unit loan amount associated with a loan request, wherein the loan request is associated with a total loan amount that equals the unit loan amount multiplied by a total number of units;

receiving a plurality of second blockchain transactions, each of the second blockchain transactions comprising an encrypted number of units;

receiving a third blockchain transaction specifying a subset of the second blockchain transactions; and

executing a blockchain contract associated with the blockchain to determine and store an encrypted loan amount corresponding to each second blockchain transaction of the subset based on the encrypted unit loan amount and the encrypted number of units in the second blockchain transaction;

wherein the encrypted unit loan amount, the encrypted number of units, and the encrypted loan amount are generated based on a homomorphic encryption scheme.

17. The system of claim 16, wherein the operations further comprise:

receiving a fourth blockchain transaction comprising an encrypted unit repayment amount; and

executing the blockchain contract to update the encrypted loan amount corresponding to each second blockchain transaction of the subset based on the encrypted unit repayment amount and the encrypted number of units in the second blockchain transaction.

18. The system of claim 16, wherein the operations further comprise:

executing the blockchain contract to determine and store an encrypted debt amount corresponding to the first blockchain transaction, the encrypted debt amount comprising a sum of the encrypted loan amount corresponding to each second blockchain transaction of the subset.

19. The system of claim 18, wherein the operations further comprise:

receiving a fourth blockchain transaction comprising an encrypted unit repayment amount; and

executing the blockchain contract to update the encrypted debt amount corresponding to the first blockchain transaction based on the encrypted unit repayment amount and the encrypted number of units in each second blockchain transaction of the subset.

20. The system of claim 16, further comprising:

receiving a range claimed to encompass the unit loan amount and a zero-knowledge range proof that the unit loan amount falls within the claimed range.