

[0004] Due to the data structure that needs to be maintained, blockchain systems may have relatively low transaction rates. For example, public blockchain systems, such as Bitcoin and Ethereum, may only process around a dozen transactions per second. While consortium blockchain systems may support higher transaction rates, many are still limited to a few thousand transactions per second. Therefore, a relatively moderate increase in network traffic may cause data congestions, which may lead to breakdown of systems in certain circumstances. Consequently, blockchain systems may be prone to denial-of-service (DoS) attacks, including distributed denial-of-service (DDoS) attacks, which are malicious attempts to interrupt network traffic to target destinations, networks, or servers, by overwhelming the targets with massive amounts of fraudulent traffic from numerous source locations. Furthermore, blockchain systems often have multiple distributed nodes for receiving transactions, making blockchain systems more vulnerable to DDoS attacks.

SUMMARY

[0005] In one aspect, a computer-implemented method for preventing denial-of-service attacks on a blockchain system includes: retrieving a decryption key D_K from a k -th block of a blockchain; determining whether an encrypted transaction to be included in a block subsequent to the k -th block is valid based on the decryption key D_K ; in response to a determination that the encrypted transaction to be included in the block subsequent to the k -th block is invalid, rejecting the encrypted transaction; generating an encryption key E_{K+1} , generating a decryption key D_{K+1} based on the encryption key E_{K+1} ; generating a non-machine-readable representation of the encryption key E_{K+1} , the non-machine-readable representation

comprising a distorted image representing the encryption key E_{K+1} , and storing the decryption key D_{K+1} and the non-machine-readable representation of the encryption key E_{K+1} in the block subsequent to the k-th block.

[0006] In another aspect, a device for preventing denial-of-service attacks on a blockchain system includes: one or more processors; and one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to: retrieve a decryption key D_K from a k-th block of a blockchain; determine whether an encrypted transaction to be included in a block subsequent to the k-th block is valid based on the decryption key D_K ; in response to a determination that the encrypted transaction to be included in the block subsequent to the k-th block is invalid, reject the encrypted transaction; generating an encryption key E_{K+1} , generating a decryption key D_{K+1} based on the encryption key E_{K+1} ; generating a non-machine-readable representation of the encryption key E_{K+1} , the non-machine-readable representation comprising a distorted image representing the encryption key E_{K+1} , and storing the decryption key D_{K+1} and the non-machine-readable representation of the encryption key E_{K+1} in the block subsequent to the k-th block.

[0007] In still another aspect, a non-transitory computer-readable medium have stored therein instructions that, when executed by a processor of a device, cause the device to perform a method for preventing denial-of-service attacks on a blockchain system. The method includes: retrieving a decryption key D_K from a k-th block of a blockchain; determining whether an encrypted transaction to be included in a block subsequent to the k-th block is valid based on the decryption key D_K ; in response to a determination that the encrypted transaction to be included in the block subsequent to the k-th block is invalid, rejecting the encrypted transaction;

generating an encryption key E_{k+1} , generating a decryption key D_{k+1} based on the encryption key E_{k+1} ; generating a non-machine-readable representation of the encryption key E_{k+1} , the non-machine-readable representation comprising a distorted image representing the encryption key E_{k+1} , and storing the decryption key D_{k+1} and the non-machine-readable representation of the encryption key E_{k+1} in the block subsequent to the k-th block.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments. In the following description, which refers to the drawings, the same numbers in different drawings represent the same or similar elements unless otherwise represented.

[0009] FIG. 1 is a schematic diagram of a blockchain system, according to an embodiment.

[0010] FIG. 2 is a schematic diagram of a computing device for implementing a node in a blockchain system, according to an embodiment.

What Is Claimed Is:

1. A computer-implemented method for preventing denial-of-service attacks on a blockchain system, the method comprising:
 - retrieving a decryption key D_K from a k-th block of a blockchain;
 - determining whether an encrypted transaction to be included in a block subsequent to the k-th block is valid based on the decryption key D_K ;
 - in response to a determination that the encrypted transaction to be included in the block subsequent to the k-th block is invalid, rejecting the encrypted transaction;
 - generating an encryption key E_{K+1} ;
 - generating a decryption key D_{K+1} based on the encryption key E_{K+1} ;
 - generating a non-machine-readable representation of the encryption key E_{K+1} , the non-machine-readable representation comprising a distorted image representing the encryption key E_{K+1} ; and
 - storing the decryption key D_{K+1} and the non-machine-readable representation of the encryption key E_{K+1} in the block subsequent to the k-th block.
2. The method of claim 1, wherein the encryption key E_{K+1} is generated based on a data structure utilized to store transactions recorded on the blockchain.
3. The method of claim 2, wherein the encryption key E_{K+1} is generated based on a hash value of the data structure.
4. The method of claim 2 or 3, wherein rejecting the encrypted transaction further comprises:

preventing the encrypted transaction from being packaged into the block subsequent to the k-th block.

5. The method of any one of claims 2 to 4, wherein rejecting the encrypted transaction further comprises:

refusing to accept the block subsequent to the k-th block as a new block of the blockchain.

6. The method of claim 5, wherein refusing to accept the block subsequent to the k-th block as a new block of the blockchain further comprises:

determining a number of invalid encrypted transactions contained in the block subsequent to the k-th block; and

refusing to accept the block subsequent to the k-th block as a new block of the blockchain when the number of invalid encrypted transactions exceeds a threshold.

7. A device for preventing denial-of-service attacks on a blockchain system, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 6.

8. An apparatus for preventing denial-of-service attacks on a blockchain system, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 6.

9. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 6.