

## WHAT IS CLAIMED IS

1. An apparatus comprising:  
  
a processor configured to generate a blockchain request which comprises data for a blockchain, create a tag value which identifies whether the blockchain request is a noisy request that comprises fake data or a non-noisy request that comprises non-noisy data, and store the tag value within the blockchain request; and  
  
a network interface configured to transmit the blockchain request to one or more blockchain peers.
2. The apparatus of claim 1, wherein the processor is configured to generate a noisy blockchain request that comprises fake data for the blockchain, and create a tag value which identifies the blockchain request as noisy.
3. The apparatus of claim 2, wherein the fake data comprises fake key-values for the blockchain ledger, and the tag value comprises a hash value previously agreed to by creators of the blockchain request.
4. The apparatus of claim 2, wherein the processor is further configured to receive signatures and read-write sets with respect to the noisy blockchain request from endorser peers of the blockchain, and store the signatures and the read-write sets in the noisy blockchain request.
5. The apparatus of claim 1, wherein the processor is configured to generate a noisy blockchain request based on a historical pattern of behavior of multiple clients on the blockchain.

6. The apparatus of claim 1, wherein the processor is further configured to obscure the tag value based on a secret key prior to transmission of the blockchain request.

7. The apparatus of claim 6, wherein the secret key comprises a public key of a symmetric public and private key pair, and the private key is shared by blockchain clients within a blockchain network that created the noisy blockchain request but not shared by other blockchain clients within the blockchain network.

8. An apparatus comprising:  
a network interface configured to receive a blockchain request that comprises a tag value which identifies whether the blockchain request is a noisy request that comprises fake data or a non-noisy request that comprises non-noisy data; and  
a processor configured to verify that the blockchain request has been endorsed by enough blockchain peers to satisfy a predetermined policy, and in response to successful verification, store the blockchain request which includes the tag value within a data block among a hash-linked chain of data blocks.

9. The apparatus of claim 8, wherein the blockchain request is a noisy blockchain request that comprises fake data for a blockchain, and the tag value identifies the blockchain request as noisy.

10. The apparatus of claim 9, wherein the fake data comprises fake key-values for the blockchain, and the tag value comprises a hash value previously agreed to by creators of the noisy blockchain request.

11. The apparatus of claim 9, wherein the processor is configured to verify signatures and read-write sets with respect to the noisy blockchain request from endorser peers of the noisy blockchain request, and store the signatures and the read-write sets within the data block.

12. The apparatus of claim 8, wherein the tag value comprises an obscured tag value that has been obscured based on a secret key.

13. The apparatus of claim 12, wherein the secret key comprises a public key of a symmetric public and private key pair, and the private key is shared by blockchain clients within a blockchain network that created the noisy blockchain request but not shared by other blockchain clients within the blockchain network.

14. The apparatus of claim 8, wherein the blockchain request is a non-noisy blockchain request that comprises live data for the blockchain, and the tag value identifies that the blockchain request is not noise.

15. A method comprising  
generating a blockchain request which comprises data for a blockchain;  
creating a tag value which identifies whether the blockchain request is a noisy request that comprises fake data or a non-noisy request that comprises non-noisy data;  
storing the tag value within the blockchain request; and  
transmitting the blockchain request to one or more blockchain peers.

16. The method of claim 15, wherein the generating comprises generating a noisy blockchain request that comprises fake data for the blockchain, and the tag value identifies the blockchain request as noisy.

17. The method of claim 16, wherein the fake data comprises fake key-values for the blockchain, and the tag value comprises a hash value previously agreed to by creators of the noisy blockchain request.

18. The method of claim 16, wherein the method further comprises receiving signatures and read-write sets with respect to the noisy blockchain request from endorser peers of the blockchain, and storing the signatures and the read-write sets in the noisy blockchain request.

19. The method of claim 15, wherein the generating comprises generating a noisy blockchain request based on a historical pattern of behavior of multiple clients on the blockchain.

20. The method of claim 15, wherein the creating further comprises obscuring the tag value with a secret key prior to transmitting the blockchain request.

21. A computer program comprising program code adapted to perform the method steps of any of claims 15 to 20 when said program is run on a computer.