What is claimed is:

1. A computer-implemented method executed by a multi-factor authentication (MFA) smart contract wallet for securing blockchain transactions, by enforcing MFA rules requiring a number m of separate blockchain transaction requests from separate ones of a plurality consisting of a number n total externally owned accounts to authorize a corresponding single, specific blockchain transaction, the method comprising:

receiving, by the MFA smart contract wallet, from a proposing one of the n externally owned accounts, a proposed specific blockchain transaction request having a transaction value, call data and a recipient address, and being signed by a unique private key associated with the proposing one of the n externally owned accounts;

wherein the MFA smart contract wallet includes an MFA rule requiring the number m externally owned accounts out of the number n total externally owned accounts to each submit a blockchain transaction request to the MFA smart contract wallet, prior to execution of a corresponding single, specific blockchain transaction, wherein m is at least two and n is equal to or greater than two, and wherein each blockchain transaction request from an externally owned account is signed by a unique private key associated with the corresponding externally owned account;

receiving, by the MFA smart contract wallet, responsive blockchain transaction requests from the number m minus 1 of the number n total externally owned accounts, in support of the proposed specific blockchain transaction request, wherein the responsive blockchain transaction requests from the externally owned accounts each comprise the transaction value, the call data and the recipient address, each responsive transaction request being signed by a unique private key associated with a corresponding one of the externally owned accounts; and

executing, responsive to satisfaction of the MFA rule, a multi-factor authenticated blockchain transaction request signed by a unique private key of the MFA smart contract wallet, the multi-factor authenticated blockchain transaction request corresponding to the proposed specific blockchain transaction request.

2. The method of claim 1, wherein the transaction value, the call data and the recipient address are received at a device or an application corresponding to each one the one of the n externally owned accounts, prior to submitting the responsive blockchain transaction requests from the m approving ones of the externally owned accounts.

3. The method of claim 1, further comprising notifying other of the n externally owned accounts of the proposed blockchain transaction request received by the MFA smart contract wallet.

4. The method of claim 1, using a notification service to push notifications to each one of the n externally owned accounts, the pushed notifications concerning MFA smart contract wallet events, the events including proposed blockchain transaction requests received by the MFA smart contract wallet.

5. The method of claim 1, wherein there is a fixed period of time for the m approving ones of the externally owned accounts to submit the responsive blockchain transaction requests.

6. The method of claim 1, wherein the n total number of external accounts each having a unique private key are controlled by a single user.

7. The method of claim 1, wherein the n total number of external accounts each having a unique private key are controlled by a plurality of different users.

8. The method of claim 1, wherein the n total number of unique private keys are associated with externally owned accounts on different computing devices.

9. The method of claim 1, wherein the n total number of unique private keys are associated with different applications on one or more computing devices.

10. The method of claim 1, wherein the proposed blockchain transaction comprises sending cryptocurrency from the MFA smart contract wallet to a receiving wallet.

11. The method of claim 1, wherein at least one externally owned account comprises an application associated with at least a private key.

12. The method of claim 1, wherein at least one externally owned account comprises a wallet comprising at least a private key.

13. The method of claim 1, wherein the blockchain server is located remotely from the externally owned accounts.

14. The method of claim 1, wherein each externally owned account is hosted by a unique computing device.

15. At least one non-transitory computer-readable storage medium for securing blockchain transactions, by enforcing MFA rules requiring a number m of separate blockchain transaction requests from separate ones of a plurality consisting of a number n total externally owned accounts to authorize a corresponding single, specific blockchain transaction, the at least one non-transitory computer-readable storage medium storing computer executable instructions that, when loaded into computer memory and executed by at least one processor of a computing device, cause the computing device to perform the following steps:

receiving, by an MFA smart contract wallet, from a proposing one of the n externally owned accounts, a proposed specific blockchain transaction request having a transaction value, call data and a recipient address, and being signed by a unique private key associated with the proposing one of the n externally owned accounts;

wherein the MFA smart contract wallet includes an MFA rule requiring the number m externally owned accounts out of the number n total externally owned accounts to each submit a blockchain transaction request to the MFA smart contract wallet, prior to execution of a corresponding single, specific blockchain transaction, wherein m is at least two and n is equal to or greater than two, and wherein each blockchain transaction request from an externally owned account is signed by a unique private key associated with the corresponding externally owned account;

receiving, by the MFA smart contract wallet, responsive blockchain transaction requests from the number m minus 1 of the number n total externally owned accounts, in support of the proposed specific blockchain transaction request, wherein the responsive blockchain transaction requests from the externally owned accounts each comprise the transaction value, the call data and the recipient address, each responsive transaction request being signed by a unique private key associated with a corresponding one of the externally owned accounts; and

executing, responsive to satisfaction of the MFA rule, a multi-factor authenticated blockchain transaction request signed by a unique private key of the MFA smart contract wallet, the multi-factor authenticated blockchain transaction request corresponding to the proposed specific blockchain transaction request.

16. The at least one non-transitory computer-readable storage medium of claim 15, wherein the transaction value, the call data and the recipient address are received at a device or an application corresponding to each one the one of the n externally owned accounts, prior to submitting the responsive blockchain transaction requests from the m approving ones of the externally owned accounts.

17. The at least one non-transitory computer-readable storage medium of claim 15, further comprising notifying other of the n externally owned accounts of the proposed blockchain transaction request received by the MFA smart contract wallet.

18. The at least one non-transitory computer-readable storage medium of claim 15, using a notification service to push notifications to each one of the n externally owned accounts, the pushed notifications concerning MFA smart contract wallet events, the events including proposed blockchain transaction requests received by the MFA smart contract wallet.

19. The at least one non-transitory computer-readable storage medium of claim 15, wherein there is a fixed period of time for the m approving ones of the externally owned accounts to submit the responsive blockchain transaction requests.

20. The at least one non-transitory computer-readable storage medium of claim 15, wherein the n total number of external accounts each having a unique private key are controlled by a single user.

21. The at least one non-transitory computer-readable storage medium of claim 15, wherein the n total number of external accounts each having a unique private key are controlled by a plurality of different users.

22. The at least one non-transitory computer-readable storage medium of claim 15, wherein the n total number of unique private keys are associated with externally owned accounts on different computing devices.

23. The at least one non-transitory computer-readable storage medium of claim 15, wherein the n total number of unique private keys are associated with different applications on one or more computing devices.

24. The at least one non-transitory computer-readable storage medium of claim 15, wherein the proposed blockchain transaction comprises sending cryptocurrency from the MFA smart contract wallet to a receiving wallet.

25. The at least one non-transitory computer-readable storage medium of claim 15, wherein at least one externally owned account comprises an application associated with at least a private key.

26. The at least one non-transitory computer-readable storage medium of claim 15, wherein at least one externally owned account comprises a wallet comprising at least a private key.

27. The at least one non-transitory computer-readable storage medium of claim 15, wherein the blockchain server is located remotely from the externally owned accounts.

28. The at least one non-transitory computer-readable storage medium of claim 15, wherein each externally owned account is hosted by a unique computing device.

29. A computer system for securing blockchain transactions, by enforcing MFA rules requiring a number m of separate blockchain transaction requests from separate ones of a plurality consisting of a number n total externally owned accounts to authorize a corresponding single, specific blockchain transaction, the computer system comprising:

at least one processor;

a network interface, communicatively coupled to the at least one processor and to an external data communication network;

a memory, communicatively coupled to the at least one processor;

an MFA smart contract wallet residing in the memory and comprising:

a proposed specific blockchain transaction request receiving module configured to receive, from a proposing one of the n externally owned accounts, a proposed specific blockchain transaction request having a transaction value, call data and a recipient address, and being signed by a unique private key associated with the proposing one of the n externally owned accounts;

wherein the MFA smart contract wallet includes an MFA rule requiring the number m externally owned accounts out of the number n total externally owned accounts to each submit a blockchain transaction request to the MFA smart contract wallet, prior to execution of a corresponding single, specific blockchain transaction, wherein m is at least two and n is equal to or greater than two, and wherein each blockchain transaction request from an externally owned account is signed by a unique private key associated with the corresponding externally owned account;

a responsive blockchain transaction requests receiving module configured to receive responsive blockchain transaction requests from the number m minus 1 of the number n total externally owned accounts, in support of the proposed specific blockchain transaction request, wherein the responsive blockchain transaction requests from the externally owned accounts each comprise the transaction value, the call data and the recipient address, each responsive transaction request being signed by a unique private key associated with a corresponding one of the externally owned accounts; and a multi-factor authenticated blockchain transaction request executing module configured to execute, responsive to satisfaction of the MFA rule, a multi-factor authenticated blockchain transaction request signed by a unique private key of the MFA smart contract wallet, the multi-factor authenticated blockchain transaction request corresponding to the proposed specific blockchain transaction request.