compromise individual users. In the prior art system 100 of Figure 1, a multi-signature wallet 117 on device 115 submits a blockchain transaction request 125 upon receiving multiple approvals 127 from a given number of the multiple separate owners of the multi-signature wallet 117 (e.g., three approvals from three separate owners in the example illustrated in Figure 1). This technique requires that multiple ones of the separate owners of the multi-signature wallet 117 submit signed approvals. In addition, compromise of the device 115 could also result in compromising the conventional multi-signature wallet 117.

[005] It would be desirable to address these issues.

Summary

[005a] In an aspect, the present disclosure refers to 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.

[005b] In an aspect, the present disclosure refers to 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.

[005c] In an aspect, the present disclosure refers to 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.

[006] In an example, a robust technique using a multi-factor (“MFA”) smart contract wallet with enhanced security is provided. The MFA smart contract wallet enforces MFA rules for blockchain transactions utilizing multiple blockchain transaction requests from separate external resources for a single transaction. The MFA smart contract wallet provides additional security, by requiring that a user confirm the transaction by submitting the transaction’s recipient, call data, and value to the MFA smart contract wallet using multiple different externally owned accounts on multiple devices and/or applications. The enforcement of the MFA rules mitigates key compromise issues by preventing an attacker that has compromised less than a requisite number of the user’s externally owned account (EOA) keys from spending smart contract wallet funds.

[007] In one example, a proposed specific blockchain transaction request is transmitted to the MFA smart contract wallet from a proposing one of the user’s externally owned accounts. The transmitted proposed specific blockchain transaction request is received by the MFA smart contract wallet. The proposed specific blockchain transaction request has a transaction value, call data and a recipient address, and has been signed by a unique private key associated with the

proposing one of the user’s externally owned accounts. The MFA smart contract wallet can include an MFA rule requiring a given number m of the externally owned accounts out of the total number n of 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. In other words, the MFA smart contract wallet only executes an actual blockchain transaction when m of the n total externally owned accounts submit blockchain transaction requests including the requisite transaction information, with each blockchain transaction request from an externally owned account being signed by a unique private key associated with the corresponding externally owned account. In some implementations, m is at least two and n is equal to or greater than two. It is to be understood that m and n can have various values, e.g., m=3 and n=5, m=3 and n=3, m=4 and n=6, etc.

[008] In one example, the MFA smart contract wallet receives responsive blockchain transaction requests from m minus 1 of the n total externally owned accounts, in support of the proposed specific blockchain transaction request. (Note that the MFA smart contract wallet has already received the proposed blockchain transaction request from one of the externally owned accounts, so to make a total of m received transaction requests, it now needs to receive m-1 more). 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. In other examples, more, less, or different transaction data can be used.

[009] In some examples, the MFA smart contract wallet notifies other ones of the n externally owned accounts that it has received the proposed blockchain transaction request, for

example by utilizing a notification service to push out notifications concerning MFA smart contract wallet events.

[010] In some examples, responsive to satisfaction of the MFA rule requiring receipt of requests from a given number of the externally owned accounts, the MFA smart contract wallet transmits to the blockchain (e.g., executes) a multi-factor authenticated blockchain transaction request signed by its own unique private key, the multi-factor authenticated blockchain transaction request corresponding to the proposed specific blockchain transaction request.

[011] The features and advantages described in this summary and in the following detailed description are not all-inclusive, and particularly, many additional features and advantages may be apparent to one of ordinary skill in the relevant art in view of the drawings, specification, and claims hereof. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter, resort to the claims being necessary to determine such inventive subject matter.

Brief Description of the Drawings

[012] Figure 1 (prior art) is a block diagram illustrating a conventional multi-signature wallet.

[013] Figure 2 is a high-level block diagram illustrating a system enforcing MFA requirements for blockchain transactions utilizing multiple blockchain transaction requests from separate external resources for a single transaction, according to an implementation.

[014] Figure 3 is a more detailed block diagram illustrating a blockchain server for executing secured blockchain transactions by an MFA smart contract wallet using smart contract functionality, from the system of Figure 2, according to an implementation.