

Claims

1. An apparatus for cybersecurity, the apparatus comprising:

a processor being configured to execute instructions in a memory to control the apparatus to:

receive an input for a subject address in a target blockchain system;
obtain a list of addresses involved in a predefined number of hops of transactions upstream and/or downstream of the subject address in the target blockchain system;

identify suspicious transaction behaviour of addresses in the obtained list of addresses upstream and/or downstream of the subject address; and

calculate a risk score indicative of degree of cybersecurity threat for the subject address taking into consideration the suspicious transaction behaviour, wherein the apparatus is further controllable to:

identify an address from the obtained list of addresses that transacted directly with the subject address upstream of the subject address as immediate source address, and/or identify an address from the obtained list of addresses that transacted directly with the subject address downstream of the subject address as immediate destination address,

wherein each hop is defined as a transaction between two addresses that involves transfer of one or more tokens of a cryptocurrency of the target blockchain system;

classify each immediate source address and/or immediate destination address with an indicator of degree of cybersecurity threat based on the determined suspicious transaction behaviour and/or based on indicator of degree of cybersecurity threat pre-recorded for the immediate source address and/or immediate destination address;

assign to each of one or more tasks, a plurality of transactions occurring in a time period in the predefined number of hops of transactions upstream and/or downstream of the subject address, wherein the plurality of transactions comprises transactions between the subject address, the immediate source address and/or the immediate destination address;

classify each task with an indicator of degree of cybersecurity threat based on the classification of the immediate source address and/or immediate destination address involved in the task; and

calculate the risk score indicative of degree of cybersecurity threat for the subject address based on the classification of the one or more tasks.

2. The apparatus of claim 1, wherein the plurality of transactions assigned to the task comprises transactions starting from a first transaction between the subject address and a first immediate source address to a last transaction between the subject address and a last immediate destination address, wherein the last immediate destination address is an address that transacted with the subject address before a transaction between the subject address and an immediate source address,

wherein the risk score is calculated based on:

number of tasks classified with an indicator of a predetermined high degree of cybersecurity threat;

time duration of the subject address involving one or more transactions involving the one or more tasks classified with an indicator of a predetermined high degree of cybersecurity threat; and

amount of bad value of tokens in the one or more tasks that the subject address has transacted with and which is derived from addresses in the obtained list of addresses with an indicator of a predetermined high degree of cybersecurity threat.

3. The apparatus of claim 2, wherein the apparatus is controllable to:

calculate the amount of bad value of tokens considered for one task by:

calculating a total input token amount received in the task from one or more immediate source addresses;

calculating a total output token amount sent in the task to one or more immediate destination addresses, wherein a total absolute value of tokens transacted in the task equals to the total output token amount,

wherein

if a first condition that total bad value of tokens in the task from one or more immediate source addresses with an indicator of a predetermined high degree of cybersecurity threat is more than bad value of tokens sent to one or more immediate destination addresses in the task is satisfied,

5 and

if a second condition that total bad value of tokens in the task from one or more immediate source addresses with an indicator of a predetermined high degree of cybersecurity threat is less than or equal to the total absolute value of tokens transacted is satisfied,

10 the amount of bad value of tokens considered for the task is equal to total input bad value tokens is achieved,

however, if a third condition that total bad value of tokens in the task from one or more immediate source addresses with an indicator of a predetermined high degree of cybersecurity threat is more than the total absolute value of tokens transacted, the amount of bad value of tokens considered for the task is equal to the total absolute value of tokens transacted,

15 however, if a fourth condition that the total bad value of tokens in the task to the one or more immediate destination addresses with an indicator of a predetermined high degree of cybersecurity threat is greater than the bad value of tokens in the task from one or more immediate source addresses with an indicator of a predetermined high degree of cybersecurity threat, the amount of bad value of tokens considered for the task is equal to the total bad value of tokens in the task to the one or more immediate destination addresses with an indicator of a predetermined high degree of cybersecurity threat.

20 4. The apparatus of claim 3, wherein the risk score is calculated based on a first equation as follow:

Risk Score = average (normalized malicious token + normalized malicious tasks + normalized malicious days),

30 wherein normalized malicious value of each of the *normalized malicious token, normalized malicious tasks and normalized malicious days* is calculated by a second equation:

normalized malicious value = (normalized absolute bad value + % of bad value without normalization)/2,

35 wherein the normalized absolute bad value of each metric comprising tokens, tasks and days, is calculated by a third equation:

40 normalized absolute bad value = [(absolute bad value of metric) * (% of bad value of metric)]/(maximum absolute bad value of metric * normalizer),

wherein the maximum absolute bad value of each metric comprising tokens, tasks and days is learnt by machine learning,

45 wherein the normalizer is a predetermined value to normalise the absolute bad value of each metric comprising tokens, tasks and days based on the % of bad value of each metric comprising tokens, tasks and days.

5. The apparatus of claim 4, wherein the apparatus is further controllable to

50 classify each task with normal, suspicious, highly suspicious or malicious as the indicator of degree of cybersecurity threat based on characteristics that comprise at least one of the following:

a) immediate spending of all tokens from all immediate source addresses to immediate destination addresses with a balance of 0 token and token hold time by all immediate source addresses is less than or equal to 1 day; and/or

55 b) spending of all tokens from all immediate source addresses after considerable hold time with a balance of 0 token and token hold time greater than or equal to 10 days.

6. The apparatus of claim 5, wherein the suspicious transaction behaviour is identified based on

whether the one or more transactions upstream and/or downstream of the subject address has a predetermined number of hops, and/or

5 after each address in the list of addresses is determined as a low transaction address or a medium transaction address based on one or more predetermined transaction volume thresholds, whether one or more addresses that are determined as low transaction address or a medium transaction address in the predetermined number of hops is involved in a transaction with a predetermined factor of aggregation or splitting of tokens, and/or

10 whether one or more addresses in the list of addresses are involved in a transaction with a predetermined factor of aggregation or splitting of tokens.

7. The apparatus of claim 6, wherein the suspicious transaction behaviour to identify comprises:

15 at least 5 hops of transactions, from an immediate source or destination address upstream or downstream of the subject address that directly transacted with the subject address, of direct relaying of tokens without aggregation or splitting of tokens;

20 at least 4 hops of transactions, from an immediate source or destination address upstream or downstream of the subject address that directly transacted with the subject address, of relaying of tokens with at least 4 factors of splitting or aggregation of tokens by a low transaction address;

at least 4 hops of transactions, from an immediate source or destination address upstream or downstream of the subject address that directly transacted with the subject address, of relaying of tokens with at least 8 factors of splitting or aggregation of tokens by a medium transaction address;

25 at least 3 hops of transactions, from an immediate source or destination address upstream or downstream of the subject address that directly transacted with the subject address, of relaying of tokens with at least 2 factors of aggregation or splitting of tokens that involves a minimum of 2 addresses; and/or

30 a single transaction with at least 10 factors of aggregation or splitting of tokens that involves a minimum of 2 addresses and occurring just before or after an exchange address.

8. The apparatus of claim 7, wherein the predefined number of hops of transactions upstream or downstream from the subject address is 5 or 6.

35 9. The apparatus of claim 8, wherein the suspicious transaction behaviour of one or more address upstream and/or downstream of the subject address is determined using a trained artificial intelligence system that had undergone machine learning.

40 10. The apparatus of claim 9, wherein the apparatus is further controllable to generate a virtualization diagram to show

a marker for each address in the list of addresses involved in the predefined number of hops of transactions upstream and/or downstream of the subject address, direction of token flow between the shown markers, and amount of token transacted between the shown markers.

45 11. The apparatus of claim 10, wherein the apparatus is further controllable to generate the virtualization diagram based on user inputs, wherein the user inputs include one or more of the following:

50 source depth to select a number of hops of transactions downstream of the subject address to show in the virtualization diagram;

distribution depth to select a number of hops of transactions upstream of the subject address to show in the virtualization diagram;

transaction limit to enter an amount of token to exclude showing of addresses that have transacted beyond the entered amount of token in the virtualization diagram;

55 date range to enter a start date and an end date to show addresses with transactions occurring between the start date and end date in the virtualization diagram; and/or

disablement of showing of each address that has more than a predetermined number of token flow paths into or from said address.

12. The apparatus of claim 11, wherein the apparatus is part of a cybersecurity blockchain system that comprises:

5 a threat reputation database comprising cybersecurity threat data collected by users, security experts and/or artificial intelligence machines deployed to detect cybersecurity threat, wherein the apparatus is further controllable to update the threat reputation database with the risk score indicative of degree of cybersecurity threat for the subject address when the
10 apparatus is used to calculate the risk score for the subject address,

wherein one or more nodes of the cybersecurity blockchain system is configured to allow a user to report a case in which cybersecurity is compromised and involves one or more addresses of the target blockchain system, and such report is sent to one or more nodes in the cybersecurity blockchain accessible to one or more designated security experts to validate,

15 wherein, after validation, record or records of one or more addresses along with an assigned degree of cybersecurity threat, if assigned, are saved as a data block of the cybersecurity blockchain system in the threat reputation database.

13. The apparatus of claim 12, wherein each address shown in the visualization diagram is shown with a category after referring to records in the threat reputation database, wherein the category is one of the following: Blacklist; Whitelist; Exchange; Decentralised exchange; Involved in a Scam; Involved with Phishing; Associated with a Smart contract; Annotated with information in the threat reputation database; and Not falling in any of the above categories.

14. The apparatus of claim 13, wherein the apparatus is further controllable to:
periodically query the target blockchain system to
update the threat reputation database with a newly found address in the target
blockchain system and to assign the newly found address with one of the following types:
exchange wallet, user wallet, or relay wallet used by an exchange; and/or

30 update an existing address stored in the threat reputation database with newly acquired information from the target blockchain system that is queried.

15. The apparatus of claim 14, wherein the target blockchain system is queried by
requesting for a list of addresses that transacted with a specific inputted address,
35 requesting for number of transactions performed by each address in the requested list of addresses, and
requesting for a balance token amount of each address in the requested list of addresses.

16. The apparatus of claim 15, wherein the apparatus is further controllable to:
assign the newly found address or update assignment of the existing address to be an
exchange wallet

45 if it is known that the specific inputted address is a user wallet associated with an exchange and the specified inputted address had transacted with an exchange wallet and the newly found address or the existing address and if the newly found address or the existing address is found to transact with 10 other user wallets issued by the same exchange of the specified inputted address; or

50 assign the newly found address or update assignment of the existing address to be a user wallet

if found from the query to the target blockchain that token or tokens are transferred directly from the newly found address or the existing address to one or more known exchange wallet or one or more known relay wallet used by an exchange, or

55 if found from the query to the target blockchain that a wallet creator had created the newly found address or the existing address and the wallet creator is known to be used by an exchange; or

assign the newly found address or update assignment of the existing address to be a relay wallet used by an exchange

if found from the query to the target blockchain that the newly found address or the existing address is involved in one inward token transaction and one outward token transaction that result in a balance of 0 token for the newly found address or the existing address, or

if found from the query to the target blockchain that token withdrawal took place for the newly found address or the existing address and after the token withdrawal, any balance tokens of the newly found address or the existing address is transferred to more than one wallet.

17. The apparatus of claim 16, wherein the apparatus is further controllable to detect an impersonator twitter account or a malicious tweet.

18. The apparatus of claim 17, wherein the apparatus is further controllable to:

authenticate identity of a subject twitter account by

detecting anomaly in use of space between a twitter handle of the subject twitter account and a profile name of the subject twitter account;

detecting similarity between a known profile name of an authentic twitter account and the profile name of the subject twitter account;

detecting a similarity between a known twitter handle of an authentic twitter account and the twitter handle of the subject twitter account, and/or

detecting an anomaly in number of Cyrillic characters used in the profile name and the twitter handle of the subject twitter account; and

display a badge proximate to the profile name of the subject twitter account that is indicative of the authenticity of the identity of the subject twitter account.

19. The apparatus of claim 18, wherein the apparatus is further controllable to:

poll for new tweets in an authentic twitter account; and

flag each of the retrieved new tweets as a potentially malicious or malicious tweet if at least one of the following conditions is satisfied:

(i) the retrieved new tweet is determined to contain at least one pre-defined keyword indicative of malicious content and a wallet address;

(ii) the retrieved new tweet is determined to contain at least one pre-defined keyword indicative of malicious content and a Uniform Resource Locator (URL);

(iii) the retrieved new tweet is determined to contain at least one URL and after accessing the URL, the URL is determined to comprise pre-defined HTML source code indicative of malicious content; or

(iv) the retrieved new tweet is determined to contain a wallet address or a URL that is pre-determined to be blacklisted; and

display a visual indicator to indicate the retrieved new tweet is potentially malicious or malicious tweet.