

CLAIMS

What is claimed is:

1. A vulnerability management system for blockchain digital assets comprising:
 - a sandbox engine configured to scan digital assets for vulnerabilities;
 - a knowledge base engine including artificial intelligence, the knowledge base engine configured to acquire information related to new vulnerabilities and threat intelligence;
 - a risk scoring engine including machine learning, the risk scoring engine configured to analyze sandbox engine outcomes and assign a risk score to each vulnerable asset; and
 - a security control system configured to take an action on an identified vulnerable asset based on the risk score assigned to the identified vulnerable asset.
2. The vulnerability management system of claim 1, wherein the sandbox engine includes:
 - a static analysis unit configured to perform static code scanning;
 - a dynamic analysis unit configured to generate compiled code and execute the compiled code in a virtual machine;
 - a statistical analysis unit comprising a database of global statistics for the digital assets and configured to:
 - receive the risk score of each vulnerable asset from the risk scoring engine;
 - identify similar digital assets from the database of global statistics; and
 - generate statistical vulnerability data representing each digital asset's standing within a population of similar digital assets with respect to each digital asset's vulnerabilities; and
 - an audit report generation unit configured to generate a heatmap based on the statistical vulnerability data of the statistical analysis unit.
3. The vulnerability management system of claim 2, wherein the heatmap comprises a graph displaying the risk score as a function of the number of lines of code.
4. The vulnerability management system of claim 1, wherein the risk scoring engine includes:
 - a regression model including a machine learning algorithm;
 - access to at least one database of digital assets, the at least one database of digital assets including:
 - known vulnerabilities of the digital assets;

- known vulnerable digital assets; and
 - known legitimate digital assets;
 - an offline training engine configured to estimate parameters of the machine learning algorithm and provided training data; and
 - an online prediction engine comprising the risk scoring engine.
5. The vulnerability management system of claim 4, wherein the provided training data includes feature vectors from known legitimate digital assets and feature vectors from known vulnerable digital assets.
6. The vulnerability management system of claim 1, wherein the security control system includes:
- logic to identify digital assets;
 - logic to scan digital assets for vulnerabilities and identify those digital assets as vulnerable digital assets;
 - logic to protect digital assets including the ability to suspend trading of vulnerable digital assets on a digital asset trading exchange; and
 - logic to respond to a trade on the digital asset trading exchange, the trade including vulnerable digital assets and legitimate digital assets, wherein the vulnerable digital assets are suspended and the legitimate digital assets are allowed to proceed.
7. The vulnerability management system of claim 1, wherein the knowledge base engine updates the information upon receiving threat intelligence to include a reentrancy vulnerability pattern.
8. The vulnerability management system of claim 7, wherein the reentrancy vulnerability pattern is detected by the dynamic analysis unit of the sandbox engine.
9. The vulnerability management system of claim 7, wherein the reentrancy vulnerability pattern is described as key-value pairs.
10. A method of protecting digital assets, the method comprising:
- scanning digital assets for vulnerabilities using a sandbox engine;
 - acquiring information related to new vulnerabilities and threat intelligence using a knowledge base engine including artificial intelligence;

analyzing sandbox engine outcomes and assigning a risk score to each vulnerable asset using a risk scoring engine including machine learning; and

taking an action on an identified vulnerable asset based on the risk score assigned to the identified vulnerable asset using a security control system.

11. The method of claim 10, wherein the sandbox engine includes:

a static analysis unit configured to perform static code scanning;

a dynamic analysis unit configured to generate compiled code and execute the compiled code in a virtual machine;

a statistical analysis unit comprising a database of global statistics for the digital assets and configured to:

receive the risk score of each vulnerable asset from the risk scoring engine;

identify similar digital assets from the database of global statistics; and

generate statistical vulnerability data representing each digital asset's standing within a population of similar digital assets with respect to each digital asset's vulnerabilities; and

an audit report generation unit configured to generate a heatmap based on the statistical vulnerability data of the statistical analysis unit.

12. The method of claim 11, wherein the heatmap comprises a graph displaying the risk score as a function of the number of lines of code.

13. The method of claim 10, where in the risk scoring engine includes:

a regression model including a machine learning algorithm;

access to at least one database of digital assets, the at least one database of digital assets including:

known vulnerabilities of the digital assets;

known vulnerable digital assets; and

known legitimate digital assets;

an offline training engine configured to estimate parameters of the machine learning algorithm and provided training data; and

an online prediction engine comprising the risk scoring engine.

14. The method of claim 13, wherein the provided training data includes feature vectors from known legitimate digital assets and feature vectors from known vulnerable digital assets.

15. The method of claim 10, wherein the security control system includes:

- logic to identify digital assets;
- logic to scan digital assets for vulnerabilities and identify those digital assets as vulnerable digital assets;
- logic to protect digital assets including the ability to suspend trading of vulnerable digital assets on a digital asset trading exchange; and
- logic to respond to a trade on the digital asset trading exchange, the trade including vulnerable digital assets and legitimate digital assets, wherein the vulnerable digital assets are suspended and the legitimate digital assets are allowed to proceed.

16. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a computer, cause the computer to:

- scan digital assets for vulnerabilities using a sandbox engine;
- acquire information related to new vulnerabilities and threat intelligence using a knowledge base engine including artificial intelligence;
- analyze sandbox engine outcomes and assign a risk score to each vulnerable asset using a risk scoring engine including machine learning; and
- take an action on an identified vulnerable asset based on the risk score assigned to the identified vulnerable asset using a security control system.

17. The non-transitory computer-readable storage medium of claim 16, wherein the sandbox engine includes:

- a static analysis unit configured to perform static code scanning;
- a dynamic analysis unit configured to generate compiled code and execute the compiled code in a virtual machine;
- a statistical analysis unit comprising a database of global statistics for the digital assets and configured to:
 - receive the risk score of each vulnerable asset from the risk scoring engine;
 - identify similar digital assets from the database of global statistics; and

generate statistical vulnerability data representing each digital asset's standing within a population of similar digital assets with respect to each digital asset's vulnerabilities; and

an audit report generation unit configured to generate a heatmap based on the statistical vulnerability data of the statistical analysis unit.

18. The non-transitory computer-readable storage medium of claim 16, wherein the security control system includes:

logic to identify digital assets;

logic to scan digital assets for vulnerabilities and identify those digital assets as vulnerable digital assets;

logic to protect digital assets including the ability to suspend trading of vulnerable digital assets on a digital asset trading exchange; and

logic to respond to a trade on the digital asset trading exchange, the trade including vulnerable digital assets and legitimate digital assets, wherein the vulnerable digital assets are suspended and the legitimate digital assets are allowed to proceed.

19. The non-transitory computer-readable storage medium of claim 16, wherein the knowledge base engine updates the information upon receiving threat intelligence to include a reentrancy vulnerability pattern.

20. The non-transitory computer-readable storage medium of claim 19, wherein the reentrancy vulnerability pattern is detected by the dynamic analysis unit of the sandbox engine.