International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

BLOCKCHAIN BASED SECURED IOT

Prema C[1], Venkataramanan C[2], Naveen J[3], Vinoth kumar S[4]

[1]Assistant Professor,Department of ECE, KGiSL Institute of Technology, Coimbatore, India
[2,3,4]UG Scholar,Department of ECE,KGiSL Instsitute of Technology, Coimbatore,India

***Abstract*—This paper is focused on mapping the current evolution of Internet of Things (IoT) and blockchain technologies to create an application used for assert tracking. The Supply chain of food plays and important role in our day to day life. The food we take every day travels many hands in between . By implementing the distributed ledger technology with IoT the food supply chain tracking would be very easy and highly secure.**

***Keywords*—IoT Cyber Risk, IoT risk analysis, Security, Devices, Network.**

I INTRODUCTION

Blockchain technology is now getting too much of attention from software scientists since it has been created. Actually, it has the ability t0 optimize and revolutionize the global infrastructure of the technologies connected with each other through internet. It has mainly two fields which are:

- By creating a decentralized system, there is no need of central servers and provides peer-to-peer connection.
- It can create a fully transparent database, which could bring transparency to the governance and elections.

Blockchain technology basically has 4 pillars, first Compelling security refers to integrating the digital and physical world, Competitive Fees refers that the blockchain platforms are preserved by their users, without the need for other users, Consistent Transparency refers to that the blockchain ledgers are open and cloud be looked by any person, so any system predicted on an open public blockchain platform is very translucent. Cyber security has been recognised as a essential national policy issue by several countries Economic impact of cyber risk and cyber security importance is growing because the integration of IoT connected devices into good producing and provide, cities, intelligent transport systems, smart grids and more aspects of modern life, including banking, finance, autonomous cars and personal medical devices. A essential question for presidency policy and for personal sector business ways for IoT connected product, platforms and services is the sufficiency of cyber security to minimize cyber risk that accompanies IoT deployments.

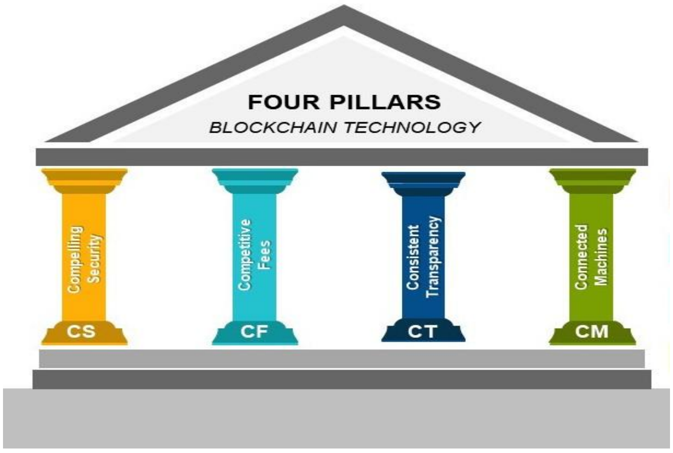

Fig. 1. Pillars of Blockchain Technology

Cyber security has been recognised as a critical national policy issue by many countries Economic impact of cyber risk and cyber security importance is growing as the integration of IoT connected devices into smart manufacturing and supply, cities, intelligent transport systems, smart grids and more aspects of modern life, including banking, finance, autonomous cars and personal medical devices. A critical question for government policy and for private sector business strategies for IoT connected products, platforms and services is the sufficiency of cyber security to minimize cyber risk that accompanies IoT deployments. Such analysis would complement the process of building frameworks and methodologies for mitigating the economic impact of cyber risk of commercial use of deployments of IoT connected products and services.The purpose of this research paper is to provide guidance for the use of blockchain technology, to make a more secure and trustable IoT nodes.

II. LITERATURE SURVEY

A. Digital infrastructure - key to Economic development

The United Kingdom has been ranked as the overall global super power according to the same report, the analysis of industry application of digital infrastructure in key sectors (Smart Grids, E-Health, E-Commerce. The uk drops a lot of lower to the fifth place and us on the third place of the index. It appears that the united kingdom and US ar powerfully protected to face up to digital infrastructure cyber-attacks, which is crucial in developing digital economy. But the united kingdom and U.S.A. appear to be insulation behind in terms of capabilities to capitalise on the new digital era. This insulating material behind within the harnessing of amount from digital infrastructure might be caused by the barriers to adoption of good producing technologies (such as cost), particularly for tiny enterprises. New infrastructure for smart manufacturing technology would create large savings for manufacturers.This could improve the harnessing of economic value from digital infrastructures.

B. Economic impacts of cyber crime in IoT

Cyber risk has not been clearly quantified through historical measures because of the risk environment is changing fast the main difficulties in calculating the economic impact of cyber risks are the lack of suitable data and the universal standardised framework to assess cyber risk. It also complicated because of the impact on brand reputation,cost of intellectual property loss, legal liability and many other variables.

C. Economic Impact of Cyber Risk from the Internet of Things

The world is experiencing the fourth industrial revolution, where the IoT real-time enabled platforms represents the foundation for digital industry. The Digital industry would be supported with more intelligence and interconnected systems. The integration of Artificial Intelligence (AI), machine learning, Deep learning, the cloud, and IoT will create systems of machines having the capability of interacting with humans to share the informations globally.

D. Economic impacts of IoT

IoT is essential for future economic competitiveness, but technological innovations are necessary for harnessing the economic values of a industry or a country. Maximising the economic impact of IoT should contain: extreme-yield of agriculture supported by energy-aware buildings and cities, physical critical infrastructure with preventive maintenance, and self- correcting cyber-physical systems . The electric power grid represents one of the largest complex interconnected networks, and under stressed conditions, even that the single failure can trigger complex cascading effects, creating wide-spread failure and blackouts.

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain is a kind of decentralized database, which keeps record of every transaction made on a network. Rather than having a traditional central database like that of banks or governments. This network can be public, like the internet, which is accessible to any person in the world with accessibility given to only persons of an organization.Blockchains are decentralized cryptographic models allows users to trust each other and make a peer-to-peer transactions, and eliminating the need of intermediaries. This technology is become a futuristic for the secured IoT nodes in the world. The four main components of blockchain ecosystem are as follows:

1. node application
2. shared ledger
3. Consensus Algorithm
4. Virtual Algorithm

1. Node Application:-

Each Internet-connected laptop has to install and run a laptop application specific to the scheme they need to participate in.Using the case of Bitcoin as associate degree example scheme, every laptop should be running the Bitcoin use case application.

2. *Shared Ledger:-*

This is a logical component. The distributed ledger may be a system managed within the node application. Once you have the node application running, you can view the respective ledger contents for that ecosystem. The shared ledger provides there is no central administrator and centralized data storage.

3. Consensus Algorithm:-

This is a logical component of the ecosystem. The consensus algorithm is implemented as part of the node application, providing the rules for how the ecosystem will arrive at a single view of the ledger. During the computations this often requires some data values to perform the process.

4. Virtual Machine:-

The virtual machine is that the final logical element enforced as a part of the node application that each participant within the system runs. To understand the capabilities further to AN system by together with a virtual machine let's take a fast cross-check what a virtual machine.

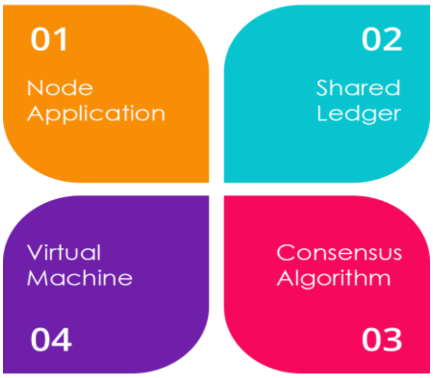

Fig. 2 Components of Blockchain

IV . WORKING

An assert tracking network has been designed and implemented using blockchain. The blockchain network consist of participants , trascations , assets and events. The participant used in our blockchain network are

- Grower
- Importer
- Shipper

The assets used in our blockchain are,

- Contract
- Shipment

The events used in our blockchain are,

- Temperature threshold event.
- Shipment received event.

Transactions used in our blockchain are,

- Temperature reading
- Gps reading
- Shipment received

Step1:

- The grower is a participant who produces shipments(fruits,vegetables,grains etc).
- The grower send shipment to the importer .

Step2:

- Importer is a participant who imports goods from the grower.
- The importer also pays the grower for the received shipment.

Step3:

- The shipper is a participant who ships the shipment from grower to the importer.

Step4:

- The contract of shipment is declared between the grower and the importer.
- The shipment consist of vegetables , fruits etc should be maintained in an temperature range of 0 - 10° C .
- If the temperature is above or below the threshold a penalty will be applied.
- An raspberry pi is used to log the temperature to the blockchain network.

Step5:

- The live location of the shipment would also recorded in the blockchain .
- The live location is taken by using the gps integrated with raspberry pi.

V . CONCLUSION

The fourth industrial revolution paved a way for rapid iot deployments all over the world. The IoT applications without security is an greatest vulnerability for the present day technology. Hence by integration the blockchain with iot the applications , it become safe and reliable to the mass.

REFERENCES

1. Madhusudan Singh, Abhiraj Singh, Shiho Kim, ”Blockchain: A game changer for securing IoT data”, 2018 IEEE 4th World Forum on Internet of Things (WF-IoT).

2. Humayed Abdulmalik, *Cyber-Physical Systems Security-A Survey*, 2017.

3. Dhananjay Singh,Gaurav Tripathi,Antonio J. Jara, “A survey of Internet-of-Things: Future vision, architecture, challenges and services”, 2014 IEEE World Forum on Internet of Things (WF-IoT).

4. C. Aggarwal, N. Ashish, and A. Sheth. The Internet of Things: A Survey from The Data-Centric Perspective, Book Chapter in "Managing and Mining Sensor Data", Springer, 2013.

5. I. Miladinovic, S. Schefer-Wenzl, "Highly Scalable IoT Architecture through Network Function Virtualization", *Open Journal of Internet of Things (OJIOT)*, vol. 3, no. 1, 2017.

6. Uden, Lorna, and Wu He, "How the Internet of Things can help knowledge management: a case study from the automotive domain," Journal of Knowledge Management 21.1 (2017).

7. C. Decker and R. Wattenhofer, “A fast and scalable payment network with bitcoin duplex micropayment channels,” In Stabilization, Safety, and Security of Distributed Systems pages 3–18. Springer, 2015.

8. A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," Information Systems Frontiers, vol. 17, pp. 261-274, 2015.

9. A. Kumar, V. Srivastava, M. K. Singh, and G. P. Hancke, "Current Status of the IEEE 1451 Standard-Based Sensor Applications," IEEE Sensors Journal, vol. 15, pp. 2505-2513, 2015.

10. P. Pyykonen, J. Laitinen, J. Viitanen, P. Eloranta, and T. Korhonen, "IoT for intelligent traffic system," IEEE 9th International Conference on Intelligent Computer Communication and Processing, ICCP 2013, pp. 175-179, 2013.