*Grenze International Journal of Engineering and Technology, Jan Issue*

# Ethereum Smart Contract Threats, Attacks and Solutions: A Survey

Mr.Sachin S. Lamkane[1] and Dr.Ajay U. Surwade[2]
[1]Department of Computer Science, Mudhoji College, Phaltan
Email: sslamkane2015@gmail.com
[2]Associate Professor, School of Computer Sciences, KBCNMU, Jalgaon
Email: ajaysurwade@gmail.com

***Abstract*—The importance and popularity of Ethereum smart contract has been continuously growing despite the availability of alternatives such as polkadot, Hyperledger Fabric and Stellar. Smart contracts are program that can be run on decentralized blockchain network with its most important property immutability. Due to this property, smart contract once deployed on the blockchain network, it cannot be modified or updated even for security enhancement purpose also. Hence it is necessary to develop strong secure contract program before deploying it on blockchain network and avoid potential exploitation and delay. Smart contracts are vulnerable to different typed of threats and attacks. To develop secure smart contracts is one of the most important challenges. In this paper we have analyzed different types of vulnerabilities on ethereum smart contract. We also review some available tools that detect these vulnerabilities. The main objective of this paper is to identify the research gap after carrying out literature survey of smart contract security and propose a model to improve security of smart contract.**

***Index Terms*— Blockchain, Ethereum, Smart Contract, Vulnerability.**

## I. INTRODUCTION

Ethereum is a decentralized blockchain platform establishes a peer-to-peer network that securely executes smart contracts. Ether is the transactional token that facilitates to perform operations on Ethereum network. Ether is the natal cryptocurrency of the ethereum platform. Ether is the second largest cryptocurrency amongst different cryptocurrencies. Now-a-days an ethereum smart contracts have boomed, it has become an integral part of the blockchain ecosystem. Actually the concept of smart contract is introduced by Nick Szabo in 1997 [1]. Smart contracts are programs that are hosted on decentralized blockchain network. The smart contract allows two or more parties to form an agreement and initiate transaction between these parties without an involvement of intermediary [2]. Ethereum is a blockchain platform which provides tools for developer to build decentralized application using Ethereum Virtual Machine (EVM). It enables involving parties to make an agreement in a transparent and secure way. However there exists some security vulnerabilities within these smart contracts and hence it causes huge financial loss. Vulnerability in smart contract cannot be fixed, due to the immutable property of blockchain. Hence smart contracts are targeted by different kinds of attacks. Most of the attacks on smart contract are exploited due to the poor smart contract code [3]. In fact, ethereum smart contract already faced several overwhelming attacks including Decentralized Autonomous Organization (DAO) attack, Parity

*Grenze ID: 01.GIJET.9.1.714*