SMART CONTRACT AUDIT FOR INDUSTRIES USING BLOCKCHAIN

Kavi Balaji, Praneet, Karthikeyan, Chandraprabha

KAVI BALAJI E,COMPUTER SCIENCE AND ENGINEERING,BIT,TAMIL NADU,INDIA
PRANEET S,COMPUTER SCIENCE AND ENGINEERING,BIT,TAMIL NADU,INDIA
[3] KARTHIKEYAN A,INFORMATION TECHNOLOGY ,BIT,TAMIL NADU,INDIA
CHANDRAPRABHA K, INFORMATION TECHNOLOGY ,BIT,TAMIL NADU,INDIA

ABSTRACT

Smart contracts, a groundbreaking innovation powered by blockchain technology, have emerged as a transformative force across various industries. This abstract provides an overview of the significance and applications of smart contracts in the industrial sector, highlighting their potential to revolutionize operations, enhance efficiency, and foster trust in business processes.Blockchain technology forms the foundation of smart contracts, offering immutable, decentralized, and tamper-resistant ledgers in which we use metamask for transactions and as repository. These characteristics of metamask are particularly advantageous in industries where transparency, security, and accountability are paramount. Smart contracts are self-executing agreements with predefined rules and conditions encoded in computer code in several platforms ,we use Ethereum blockchain in which we write computer code in remix Ethereum browser. They automate and enforce contract terms without the need for intermediaries, reducing the risk of disputes and costly delays.In the industrial sector, smart contracts are being deployed across a range of applications. In which we specifically added a admin part which can be government in land registry process or in contracts as legalised vendors. Supply chain management benefits from enhanced traceability, real-time monitoring, and automated payments. Manufacturers can streamline procurement processes, automate quality control, and reduce lead times. Energy companies use smart contracts to optimize energy trading, automate billing, and enable peer-to-peer energy sharing.Furthermore, smart contracts improve asset management by providing an auditable record of ownership, maintenance, and transfer. In the context of intellectual property, these contracts facilitate royalty payments and enforce licensing agreements automatically.This abstract also explores the challenges and considerations involved in implementing smart contracts in industries. Scalability, legal recognition, and data privacy are among the key issues that need to be addressed to unlock the full potential of smart contracts. Industry-specific standards and best practices are emerging to guide organizations in adopting this innovative technology securely and effectively.In this we have used test network for transaction for instead of Ethereum coin.

1. INTRODUCTION

With the appearance of blockchain innovation, brilliant agreements have become quite possibly of the most sought after innovation . Shrewd agreement is another innovation that can naturally arrange, satisfy, and uphold the provisions of an understanding in a blockchain climate Contrasted and customary agreements, brilliant agreements have the promotion vantages of reducing risk, reducing down organization and administration expenses, and working on the proficiency of business processes .All the more significantly, shrewd agreements have the ability to make trust between parties in what we termnotrust contracting conditions
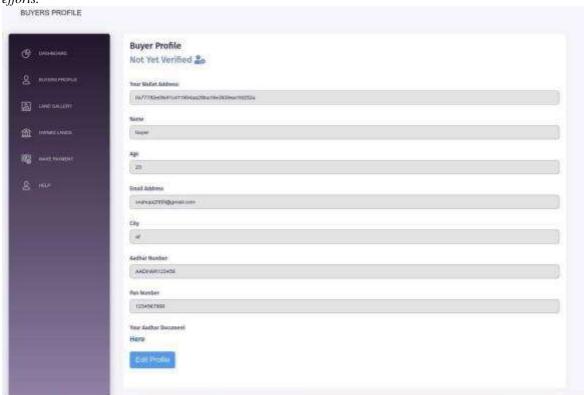
In such manner, it will reshape business cycles and, surprisingly, customary practices These days, in view of the computerized innovation, obtainment has started to change from conventional acquirement framework to an electronic obtainment approach, which can be portrayed as a thorough ICT interaction to lay out arrangements for the procurement of items or administrations (contracting) or buy items or administrations in return for installment (buying).

This electronic acquisition approach will change the manner in which organizations or people buy. It could defeat specific weaknesses of the conventional obtainment framework, like low exchange security, absence of trust, monotonous confirmation, and installment delays. The improvement of blockchain and brilliant agreements gives additional opportunities to acquisition. Blockchain, particularly savvy contracts, is undermining the

conventional acquisition model.

Notwithstanding, to whom much is given, much will be expected. Blemishes or weaknesses in brilliant agreements can prompt obliterating results, including monetary misfortunes, information breaks, and reputational harm. This is where brilliant agreement reviews become an integral factor .

A shrewd agreement review includes an intensive assessment of the agreement's code, usefulness, and safety efforts.

directing these reviews, organizations can relieve chances, guarantee administrativeconsistence, and improve the general security and effectiveness of their blockchain-fueled frameworks.

Our group of master reviewers is focused on assisting ventures with exploring the intricacies of blockchain innovation and enabling them to securely bridle its extraordinary potential.
Together, we can fabricate a safer and versatile future for blockchainpoweredbusinesses.

1.1 BACKGROUND

1.1.1 Ethereum:

Ethereum is regularly utilized for shrewd agreement reviews in ventures utilizing blockchain in light of multiple factors. Ethereum was presented in the blockchain space with its presence in 2015, Vitalik Buterin, a Canadian-Russian developer, has delivered new decentralized applications (dApps). Notwithstanding, Ethereum's prosperity is essentially credited to the execution of shrewd agreements .Many individuals accept that savvy contracts are another idea and were imagined with the Ethereum Blockchain Stage. Be that as it may, brilliant agreements date back to 1996 when PC researcher Scratch Szabo authored the expression "savvy contracts" and made sense of them as:I refer to these new agreements as "shrewd", on the grounds that they are undeniably more utilitarian than their lifeless paper-based progenitors. No utilization of man-made brainpower is suggested. A brilliant agreement is a bunch of commitments determined in computerized structure, including conventions inside which the gatherings perform on these commitments.

1.1.2 SOLIDITY:

Strength is a flawless programming language made by Ethereum which is the second largest market of computerized cash by capitalization, conveyed in the year 2015 . A couple of basic features of heartiness are recorded underneath: Strength is a highlevel programming language expected for doing shrewd agreements.It is a statically created object-oriented(contract-arranged) language.

Strength is particularly affected by Python, c++ , and JavaScript which run on the Ethereum Virtual Machine(EVM). Power maintains complex client described programming, libraries, and heritage. Power is the fundamental language for blockchains running stages. Strength can be used to make contracts like vote based, blind closeouts, crowdfunding, multisignature wallets, etc.

METAMASK:

MetaMask acts both as an Ethereum program and a wallet. It licenses you to communicate with canny arrangements and Apps on the web without downloading the blockchain or presenting any item. You simply need to add MetaMask as a Chrome Development, make a wallet and submit Ether .But MetaMask is at present open for Google Chrome program, it is ordinary to ship off for Firefox excessively sooner rather than later. Download MetaMask chrome extension before you start forming canny agreements . Whenever it is downloaded and added as a Chrome development, you can either import a by and large made wallet or make another wallet. You ought to have an ethers in your Ethereum wallet to convey Ethereum canny settlement on the association

1.2 HOW DOES SMART CONTRACT WORK:

Here's an overview of the typical steps involved in a smart contract audit:

Requirement Gathering: *The inspecting system starts with understanding the particular prerequisites and goals of the brilliant agreement being evaluated. Thisincorporates recognizing the agreement's expected usefulness, its collaboration with other brilliant agreements or outside frameworks, and the potential dangers related with its execution.*

Code Review: *Inspectors lead a careful survey of the savvy agreement's codebase. They examine the code to recognize possible weaknesses, bugs, or sensible mistakes that could be taken advantage of by aggressors. This step includes static code investigation and manual survey to guarantee exhaustive inclusion.*

REFERENCE

[1] ***Security Assessment:*** *The agreement's safety efforts, for example, access controls, verification components, and information taking care of practices, are surveyed for possible shortcomings. Inspectors search for conceivable as* Asgaonkar A, Krishnamachari B (2019) Solving the buyer and seller's dilemma: "A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator". In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

[2] Atzei N, Bartoletti M, Cimoli T (2017) "A survey of attacks on ethereum smart contracts (sok)." In: International Conference on Principles of Security and Trust, Springer, pp 164–186

[3] Bader L, Bürger JC, Matzutt R, Wehrle K (2018) "Smart contract-based car insurance policies. In: 2018 IEEE Globecom workshops" (GC wkshps), pp 1–7

sault vectors like reentrancy, flood/sub-current, and inappropriate info approval.

Compliance Check: *The savvy contract is considered in contrast to industry best works on, coding principles, and any significant administrative prerequisites. This guarantees that the agreement complies with laid out standards and rules, diminishing the probability of consistence related issues.*

Functionality Testing: *Reviewers check whether the brilliant agreement capabilities as planned and whether all expressed elements work accurately. This step guarantees that the agreement acts typically under different situations.*

External Dependency Review: *In the event that the brilliant agreement depends on outer parts, for example, other shrewd agreements or APIs, reviewers evaluate their security and expected influence on the general framework.*

Report Generation: *In the wake of finishing the review, the discoveries and suggestions are ordered into an extensive report. This report features any weaknesses or issues found during the review and gives direction on the best way to address to them.*