International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Blockchain based Smart Contracts: Vulnerability and Future Trends

Umer Parvez Fakih , Prof. Mahesh Mahajan

ASM'S INSTITUTE OF MANAGEMENT AND COMPUTER STUDIES

Abstract

A smart contract is an agreement between two people in the form of computer code. They run on the blockchain, so they are stored on a public database and cannot be changed. The transactions that happen in a smart contract are processed by the blockchain, which means they can be sent automatically without a third party. In conventional method, which is centrally managed, the third party i.e. banks, insurance company, government agencies, controls business dealing between customers and providers.

Unfortunately, many security issues in smart contracts have been reported in the media, often leading to substantial financial losses such as the Contract code. Attacks such as the Decentralized Autonomous Organization (DAO) attack and the Parity Wallet hack have cost millions of dollars simply as a consequence of naïve bugs in the smart contract code.

Purpose of this research is to give review over security problems and future implementation trends with the help of some articles and research papers.

Keywords:

- ✓ Smart contract ,
- ✓ Blockchain,
- ✓ Vulnerability,
- ✓ future trends.

Introduction

A blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without a need for a central clearing authority. Potential applications can include fund transfers, settling trades, voting, and many other issues. A smart contract is a type of Ethereum Account that runs on a blockchain-based platform known as Ethereum blockchain An Ethereum Account consists of ether (ETH)as a balance Users accounts can communicate with a smart contract and access the data by

submitting a transaction this transaction executes a predefined function on the smart contract which gives the user access to the data present in a smart contract

Smart contract is an emerging technology and would be accepted in future as its used in Dapp(Decentralized Application).

A live incident stood up recently Coffee company Farmer Connect announced today that it would partner with Smucker's Folgers brand coffee to use the IBM IBM +2.1% blockchain platform connecting producers to customers. A QR code will allow consumers who buy 1850 Coffee to see how it was grown and brought to the shelf

Smart Contract Vulnerability

Today, smart contracts are becoming the forefront of Blockchain technology. They are catering to almost every industry segment with a variety of applications and transaction use cases. From Finance and IoT to the Supply Chain and Music industry, the implementation of smart contracts applies everywhere in our daily life.

If you think about the transparency of a smart contract implementation, it becomes visible for all the users of a said blockchain. However, there can be a situation where the security loopholes and vulnerabilities also become visible. And these potential security weaknesses can be exploited by hackers or cyber criminals to further damage an organization's smart contract, which can ultimately result in loss of revenues and customer data exposure.

- In 2016, a DAO called Genesis DAO was compromised by a hacker(s) exploiting a security loophole in the system. Here, hackers stole $50 million worth of ETH from Genesis DAO's crowdfunding investors.
- In August 2021, one of the biggest cryptocurrency heists happened. Hackers stole $613 million worth of digital currency from a company named Poly Network. They exploited a vulnerability in the digital contracts Poly Network uses.

Some group of people find some mistake in smart contract and then they Stole millions of ether on Ethereum network

Therefore, to prevent such situations, it is important to understand how smart contract security functions, and learn about its proper implementation and other aspects of securing a smart contract-based platform against cyberattacks and hacking attempts.

Best Practices

Developer needs a best practice to write a smart contract any mistake or wrong condition could make you a loss of millions of dollars

Do a static analysis of your code to identify style inconsistency and vulnerable code.

Perform security analysis for your smart contract using trusted tools like Mythril, MythX, Echidna, Oyente, Manticore, ERC20 Verifier.

Test for all the vulnerabilities mentioned in the SWC Registry.

Organise a bug bounty program during testing. Use a testnet like Rinkeby.io or Kovan.

Do the penetration testing in-house if you have an experienced security team available in your organization.

Generate a detailed report on identified vulnerabilities in your system and recommendations for fixing those vulnerabilities.

If your internal security team isn't capable of conducting a security audit or pentesting for your smart contract then get the external security auditors that can do the job for you.

Do a static analysis of your code to identify style inconsistency and vulnerable code.

Perform security analysis for your smart contract using trusted tools like Mythril, MythX, Echidna, Oyente, Manticore, ERC20 Verifier.
Test for all the vulnerabilities mentioned in the SWC Registry.
Organise a bug bounty program during testing. Use a testnet like Rinkeby.io or Kovan.
Do the penetration testing in-house if you have an experienced security team available in your organization.
Generate a detailed report on identified vulnerabilities in your system and recommendations for fixing those vulnerabilities.
If your internal security team isn't capable of conducting a security audit or pentesting for your smart contract then get the external security auditors that can do the job for you.

Future Trends

1. **Government voting system**

Smart contracts provide a secure environment making the voting system less susceptible to manipulation. Votes using smart contracts would be ledger-protected, which is extremely difficult to decode.

Moreover, smart contracts could increase the turnover of voters, which is historically low due to the inefficient system that requires voters to line up, show identity, and complete forms. Voting, when transferred online using smart contracts, can increase the number of participants in a voting system Voters can vote while sitting at their home.

2.Healthcare

Blockchain can store the encoded health records of patients with a private key. Only specific individuals would be granted access to the records for privacy concerns. Similarly, research can be conducted confidentially and securely using smart contracts.

All hospital receipts of patients can be stored on the blockchain and automatically shared with insurance companies as proof of service. Moreover, the ledger can be used for different activities, such as managing supplies, supervising drugs, and regulation compliance.

3. Supply chain

Traditionally, supply chains suffer due to paper-based systems where forms pass through multiple channels to get approvals. The laborious process increases the risk of fraud and loss.

Blockchain can nullify such risks by delivering an accessible and secure digital version to parties involved in the chain. Smart contracts can be used for inventory management and the automation of payments and tasks.

2.1Crowdfunding

Crowdfunding is a method of connecting between
entrepreneurs and investors to invest in small amounts with
an internet-based platform
In crowdfunding, entrepreneurs, crowdfunding platforms and
investors are the main criteria. The main stakeholders have
their respective roles and interests. The first flow starts with
entrepreneurs (businesses or startups) proposing ideas,
funding requests through crowdfunding platforms and then
promising returns to investors. Backers (investors) will look

at investment opportunities offered by entrepreneurs and
then give their commitment to fund or give advice. to bring
together investors and supporters, a platform that acts as an
intermediary is needed.

Conclusion

Blockchain technology is widely acknowledged and highly evaluated due to its decentralized nature and peer-to- peer characteristics.

The main purpose of this research

paper is to gather information on Blockchain based Smart Contracts,

Vulnerability and Future trends

Moreover, this paper discussed the various security issues, susceptible, and threats that slowdown the increased adoption of smart contract while exploring these challenges in a variety of aspects.

We also suggested some remarkable brains for creation of specific contracts.Given practices may not be the best solution for the problem but can be used in such situations.

References

- ✓ https://www.getastra.com/blog/security-audit/smart-contract-security/#:~:text=A%20smart%20contract%20is%20a%20type%20of%20Ethereum%20Account%20that,data%20by%20submitting%20a%20transaction.
- ✓ https://www.ibm.com/in-en/topics/smart-contracts
- ✓ https://www.forbes.com/sites/robertanzalone/2020/07/15/big-coffee-
- ✓ sellers-use-blockchain-to-connect-farmers-and-customers/#:~:text=Farmer%20Connect%20announced%20today%20that,and%20brought%20to%20the%20shelf.
- ✓ https://link.springer.com/article/10.1007/s12083-021-01127-0
- ✓ https://lenderkit.com/blog/how-smart-contracts-in-crowdfunding-work/https://blog.coinbase.com/top-ten-smart-contract-security-risks-47ecbe8af15d
- ✓ https://www.youtube.com/c/DappUniversity
- ✓ https://corporatefinanceinstitute.com/resources/knowledge/deals/smart-contracts/