**E-Commerce Assignment**

| **Name** | **Roll No** | **Email** | **Address** | **Image** |
| --- | --- | --- | --- | --- |
| Sufiyan Irfan | SE-19037 | [irfan4202381@cloud.neduet.edu.pk](mailto:irfan4202381@cloud.neduet.edu.pk) | A-97 Block C North Nazimabad, Karachi |  |
| Wajahat Ahmed | SE-19038 | [ahmed4202412@cloud.neduet.edu.pk](mailto:ahmed4202412@cloud.neduet.edu.pk) | House 299 Usmania Society, Nazimabad No.1 |  |

**Deploying Smart Contracts and Monitoring Transactions in Web 3.0 dApps using Blockchain Technology**

Sufiyan Irfan 1, Wajahat Ahmed 2

1,2Department of Software Engineering, NED University of Engineering & Technology, Karachi, Pakistan

***Abstract****-***The advent of Web 3.0 has revolutionized the internet, utilizing blockchain technology with features like decentralization of data, encryption, immutability, transparency, and distributed ledger to solve the issues related to trust. Additionally, it emphasizes enhancing user security and privacy. In Web 2.0, everything is centralized, users' data is not secure, and user privacy is at risk. To solve this issue, Web 3.0 came into existence, where all data is recorded in the form of blocks connected through chains. In this paper we have discussed how secured, trustless P2P (Peer-to-peer) transactions are done in Web 3.0 without any middleman. The study carries out empirical analysis by creating a basic prototype of an Ethereum decentralized application with integrated Web 3 monitoring to demonstrate how smart contracts are deployed on network chains and how we can interact with ethereum nodes and monitor performance of ethereum transactions on testnet. The proposed system consists of web3.js client library which will be interacting with dApp backend and solidity language is used to write smart contracts which are deployed on ethereum blockchain. The research outcomes from this paper would help developers and blockchain architects to create and deploy smart contracts on the blockchain, choosing the right testnet for testing smart contracts, and building highly scalable and secure decentralized applications (dApps).**

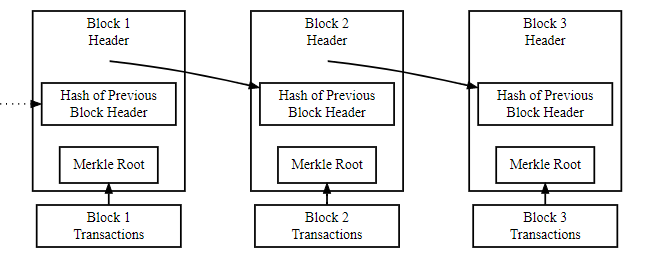
***Index Terms****-* Blockchain, dApps, Decentralized, Smart Contracts, Web 3.0

1. INTRODUCTION

When Web 1.0 arrived, the internet was treated like a newspaper (such as wikipedia), people could only read the content from the website with no interactivity. Then came Web 2.0 which is the “read-write” web, where users can both read and write data to a website. Web 2.0 is considered as the age of targeted advertising and lack of privacy. All data is centralized [1]. Companies that have centralized data own everything, like Google, Facebook, etc. They are [invading users' privacy](https://theconversation.com/online-privacy-must-improve-after-the-facebook-data-uproar-94435) and misusing their data. The third generation of the web is the next evolution of the internet utilizing blockchain technology and the tools of decentralized distributed computing. In Web 3.0, users have full control over their personal data that has been largely at risk in Web 2.0. On top of it, decentralized applications protect user’s privacy as they do not ask for any identity details. Users have a unique wallet ID through which they can perform transactions. Web 3.0 Decentralized Applications (dApps) are censorship resistant and they never go offline since they run on blockchain. dapp is a combination of centralized front-end and decentralized back-end (smart contracts) Torrent and crypto currencies are good examples of it.

Web 3.0 seeks to establish a more equitable online ecosystem where everything will be decentralized. In Web 3.0, most of the applications are token driven. e.g, Brave browser alternative to Google gives users tokens while browsing having monetary value. Blockchain and distributed ledger technology will be the standard for self-sovereign identity and decentralized data storage, as well as the payment infrastructure for the semantic web [2]. AI will be in charge of analyzing and sorting online data to provide users with the finest options. The semantic web's interoperability layer, which connects the internet to smart devices, will be ensured by IoT. Some use cases of blockchain in Web 3 are DeFi, Metaverse, dApps, NFTs, DAOs

Blockchain is a distributed, decentralized immutable ledger which is completely transparent and keeps the record of transactions occurring globally and makes it impossible to change the block without changing all blocks that came after it and obtaining the network node’s agreement. As a result transactions will be immutable, secured (because everything is hashed), and a trustless environment will be created because blockchain is decentralized means no one will hold the power on our data, instead everyone in blockchain network will have the copy of data so no one will worry about data lost and deceive from other person, as everything is recorded on every blockchain node and is immutable [3]-[5]. Blockchain enables the secure transfer of information, money and assets without the need of any centralized authority or middleman, such as tech companies, financial institutions, banks etc. Additionally, a blockchain can serve as the foundational architecture for smart contracts. It is a chain of blocks that contains transactions in the form of hash (containing data). Figure 1 will visualize the chain of blocks. Every block has a hash of the previous block and it generates the hash of transactions with the help of merkel root (it is a technique for generating a single hash of multiple transactions) and many other factors as well.



This paper specifically takes into consideration how secured and trustless transactions are done in Web 3.0 and how smart contracts can be deployed and tested on ethereum testnet. This research study is extremely helpful in cases where scaling and monitoring transactions on the blockchain network is the main goal.

The core contributions of this research study are as follows:

1. A detailed empirical analysis has been done by building a working prototype of a decentralized crypto wallet application on ethereum blockchain with monitoring of transactions through web3.js library.
2. To give an idea how smart contracts are deployed on local blockchain (ganache) and testnets.
3. Comparison analysis of performance of ethereum transactions on different testnets available.

The research paper has been organized in this way: Section II illustrates a summary of the current research work related to decentralization and emerging Web 3.0 technologies and existing efforts to study the significance of scaling decentralized applications and exploring Web 3 technologies. Section III depicts the brief explanation of tools and technologies used in the proposed system. Section IV presents an overview of our proposed designed architecture based upon blockchain technology. Implementation and execution of our dApp is presented in section V along with details of blockchain setup including tools used, the type of blockchain created as well as methods and techniques used to interact with frontend client application. Section VI details the experimentation conducted along with analyzing results of e[thereum transactions](https://www.researchgate.net/publication/341719725_Ethereum_Transaction_Performance_Evaluation_Using_Test-Nets) on testnet.

II. RELATED WORK

The key cause for research on this topic was that lack of prior research work was found in this area. Deployment of smart contracts and simultaneously monitoring its transactions in Web 3.0 dApps will require new challenges so after examining and searching in this domain we have done following literature reviews for understanding the previous work. These papers do not have a direct link to our research problem but we have gained knowledge with their research. Now in the research paper [1] they identify the problem of copyrights in the Web 3.0. Their research suggests that copyright holders embrace a decentralized Internet to get ahead of the issue. It will ultimately solve the issue of copyrights in Web 3.0.

Applications stack for different purposes in Web2.0 and Web 3.0 are discussed in [2]. Like in Web 2.0 for cloud file storage we have Amazon s3 bucket whereas in Web 3.0 we have IPFS or swarm. For browsing Google is used in Web 2.0 whereas Brave browser in Web 3.0. Similarly for payments credit cards/paypal and ethereum/bitcoin are used in Web 2.0 and Web 3.0 respectively.

Different applications of blockchain including cryptocurrencies, smart contracts, steem, and distributed cloud storage are explored in [3]. The authors also highlighted vulnerabilities and potential security flaws in platforms used to store assets and data. Further investigating in paper [4] a decentralized social network application is developed using smart contracts and IPFS storage deployed on ethereum private blockchain.

Since traditional finance is less secure and less private, people are moving towards decentralized finance (Defi). So in the paper [5] the state of Defi is enhanced, by doing an in-depth analysis of the security and privacy features of popular DeFi based applications. As a result, the privacy and security risks will decrease. Now in [6] public, private and consortium ethereum blockchains are compared and a detailed analysis has been done about how two sided client server architecture based applications based on Web 2.0 technology that are used in MIS (Management Information Systems) can be combined with Web 3 decentralized applications. Also, a framework is also discussed where on top of public Ethereum blockchain, a private blockchain system is developed.

In [7] it has been discussed how blockchain technology facilitates trustless permissionless complex transactions and co-ordination between two strangers knowing only each other's public wallet id. A decentralized messaging app is developed on ethereum blockchain to increase privacy and end-to-end encryption of sending and receiving messages [8]. End-to-end encryption of messages is done through web3.js library and ethereum wallet is integrated since sending messages cost some ether. To complete a transaction means successful sending of a message the system requires around 30 seconds so users have to wait for a long duration.

In the research paper [9] Industries have decided to add the internet in their machines to make life easier as a result machines can make their own decisions. The result is that industrialists and business owners will be more attracted towards smart machines because block chain has enhanced their functionality more. While in the paper [10] Web 3.0 transforms the way public administrations give cutting-edge and innovative services to citizens, which helps the e-government sector to interact with its people. In this paper, they demonstrate how Blockchain 3.0 and AI improve reliable, safe, scalable, and genuine provenance solutions. When discussing the authentication, In the research paper [11] OAuth 2.0-based authentication is currently the most widely used authentication solution. So in OAuth2.0 there are many privacy and security concerns. The paper examines blockchain and its use cases and proposes DAuth, so safety and privacy is retained.

In [12] the architecture is proposed in which it has been discussed how scalable dApps can be built using IPFS, smart contracts and ethereum to create a secure mechanism to initiate transactions and mechanisms of proxy re-encryption to improve the security and privacy of the network nodes. In the research paper [13] authors basically discussed the limitations in Web 2.0. With the help of block chain, the internet will be a peer to peer network, not all the data will be centralized in the giant companies, and security of users will be guaranteed with the help of cryptographic algorithms. Impact will be that the user will have a trustless environment.

In [14] two aspects are discussed for decentralization of the internet. First one are different consensus algorithms such as Proof-of-search (PoS), Proof-of-work (PoW), Paxos, Proof-of-property (PoP), which are highly scalable and second blockchain's compatibility with numerous cutting-edge internet technologies ( IOT, Cloud Computing, GraphChain ) and how those technologies are affected by Blockchain. In the research paper [15] the author's definition is not only about understanding Web 3.0 but also to learn the basics and characteristics of Web 3.0. They present a design for a third enabler called Hyper Service to check its scalability, practicality, usability. Their research ultimately adds another feature in Web 3.0

In the research paper [16] this research seeks to address the issue of duplicate submissions and improve paper security in journals. They developed a prototype and the effectiveness of the system was confirmed after testing the functionality and performance of the prototype. This technique improves journals' ability to publish and safeguards authors' intellectual property. In the research paper [17] [18] they talked about the ideas behind Web 3.0 and how it differs from Web 2.0 in various ways, such as Web 3.0 is decentralized since it is built on block chains and permits peer-to-peer connections without the use of middleware at minimal cost while Web 2.0 is totally centralized.

In the paper [19] they explained why there is the need for blockchain,smart contracts and stable coin. They gave both qualitative and quantitative analysis and reviews on them like which stable coin is better for which business and so on.Their research results that block chain future is very bright, it will benefit the society especially in financial sector, but it has also some problems also like scalability issue on global scale, its complexity etc. In the research paper [20] they say that there is not a complete definition of Web 3.0 which meets a certain standard criteria. To fill this gap, they clarified the term Web 3.0. They clearly explained the architecture of Web 3.0 dApp and its protocols and done evaluation analysis from the view of block chain which will result in proper guidance towards development of Web 3.0 services and applications.

III. TOOLS AND TECHNOLOGIES

Truffle: It is like an integrated development environment in which we can easily develop decentralized applications (dApps), deploy smart contracts and run tests. Mainly used for large projects.

Ganache: It is a local ethereum blockchain in which we can develop, deploy and test our decentralized application or smart contracts. In ganache time to block a mine in the blockchain is 0 because there is a special option called automine that is activated by default and with this option everytime ganache receives a transaction a new block is instantly mine. Block time is the average time that it takes for a block to be mine in the blockchain

Infura: They provide a suite of APIs and developer tools that give us access to the ethereum network. It interacts with the ethereum blockchain and runs nodes on behalf of its users, thereby making it easy for the developers.

Metamask: It is a browser plugin that serves as an ethereum cryptocurrency wallet that can be used to interact with decentralized applications where users can store ethers and other ERC-20 tokens.

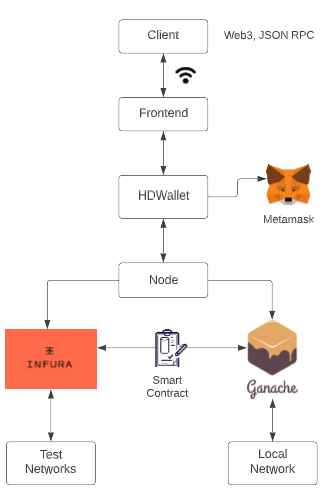
Smart contracts: Smart contracts are programs that are hosted and executed on a blockchain network. They allow users to perform transactions in a secured manner without any third party involvement

Solidity: It is a programming language designed for writing smart contracts that run on ethereum networks.

IV. PROPOSED ARCHITECTURE

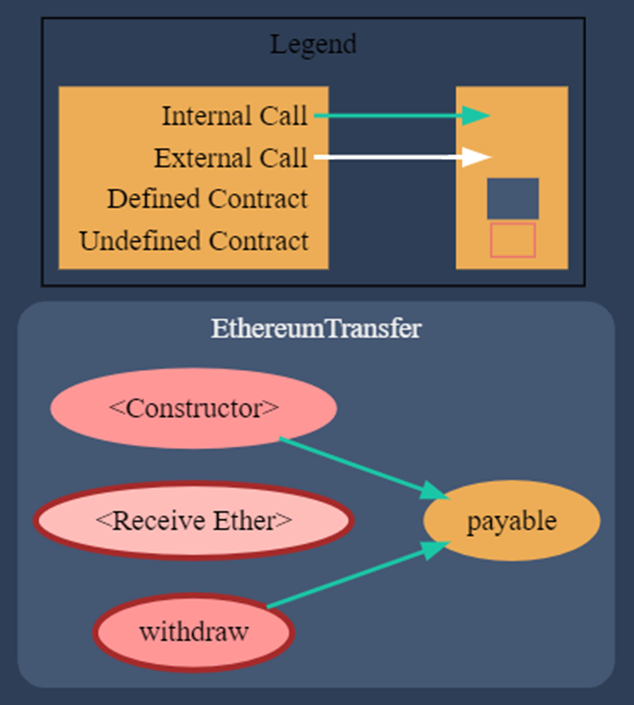
**A. Architecture Design:**

Figure 1 shows the architecture design of our decentralized application (dApp). On the client side, react is used for designing the frontend and web3.js library is used to interact with the ethereum blockchain and transfer ether from one account to another. Metamask serves as an ethereum wallet where ethers will be stored and transaction confirmation would be ensured. The smart contract used in our proposed dApp is deployed on two nodes one is Infura and second one is Ganache. Infura node connects with the ethereum test network like Ropsten, Rinkeby, Kovan etc whereas Ganache acts as a local blockchain and connects with the local network.

 Figure 1 Architecture Design

**B. Smart Contract Design:**

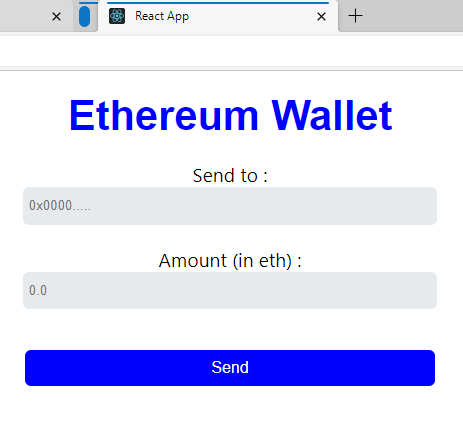
Solidity Visual Developer, a vscode extension was used to visualize the solidity smart contract as shown in Figure 2.

Figure 2 Smart Contract Visualization

The Ethereum Transfer smart contract includes functions like ReceiveEther() and withdraw(). The withdraw() function deducts the specified ether amount from the sender wallet address and the ReceiveEther() function with the payable modifier is used to receive ethers in a solidity smart contract or to some other defined wallet address.

**C. UI Design:**

We have used React to create the frontend of our ethereum wallet dApp which will be calling Web3 API to interact with the ethereum network and send eth from one account to another. Our dApp prototype includes two input fields: receiver address and the amount (in eth) to transfer. We have used both local blockchain (ganache) and test networks (using infura). Ganache doesn't require metamask window popup confirmation since it is locally connected with web3.js using JSON RPC protocol. For the test network we have used infura node integrated with metamask window popup for transaction confirmation. After transaction confirmation ethers would be transferred to the provided receiver address and a unique hash would be generated and will be shown in the alert box. Figure 3 illustrates the frontend design of our ethereum wallet.

Figure 3 Frontend UI Design

IV. IMPLEMENTATION AND SETUP

Inorder to run the ethereum wallet decentralized application as shown in Figure 1 we have setup local blockchain (ganache) and ethereum testnet. For deploying and testing the contract, mainnet (production ethereum) is not prefered since with each

transaction there is a real gas fee associated.

**A. Setting up Local Blockchain (Ganache):**

Figure 4 depicts the setup of ganache blockchain in a truffle development environment. Ganache provides 10 different wallet addresses with 100 ethers on each account.

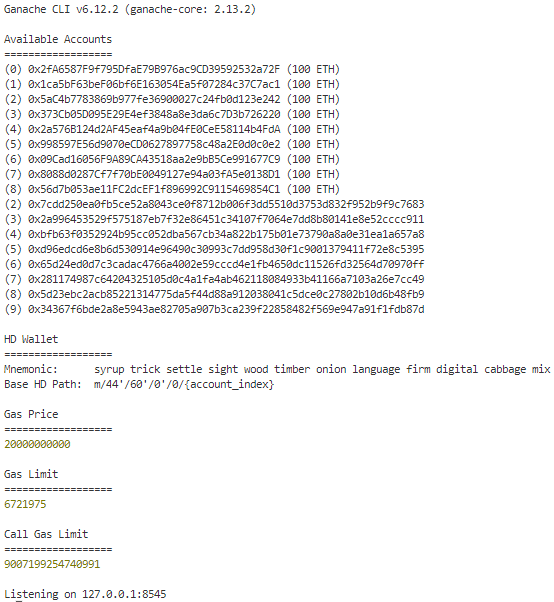


Figure 4 Local Blockchain (Ganache)

**B. Setting up Metamask Wallet and Infura for Testnets:**

We have downloaded metamask chrome extension and created two accounts one will be sending ethers and the other one would be receiving it. On the sending end Ropsten network is used. However in section V comparison analysis is performed of different testnets available and which one is better to use. Testnets are replicas of the mainnet. Testnets are used by developers to test smart contracts and tokens and to see whether the decentralized application built is performing well or not before deploying it to mainnet because every transaction done on ethereum blockchain costs some ether and gas fees. The more complicated the smart contracts with complex functions the more gas fee is required to deploy that contract. To get free ethers on testnets there are faucets available like Ropsten, Rinkeby and Kovan which provide free test ETH but with a limitation of 0.1 - 1 ETH per day. Figure 5 shows the metamask wallet used for performing transactions.

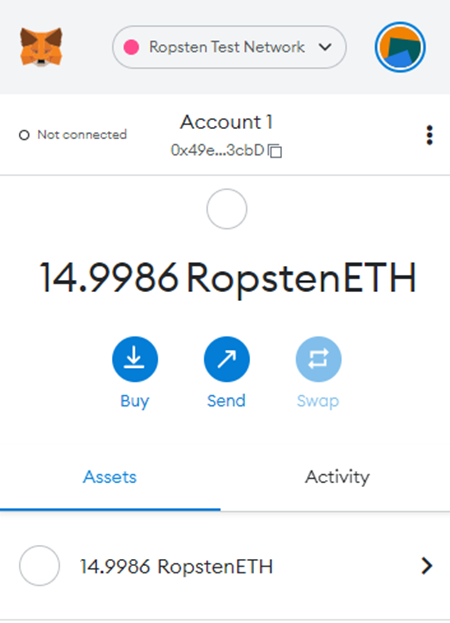
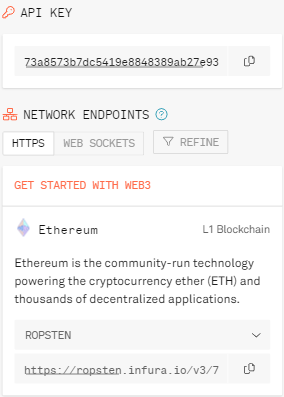


Figure 5 Metamask Wallet

Figure 6 shows the configuration of Infura to gain access to the ethereum network. For the dApp Ropsten network endpoint is used since it mimics the behavior of the mainnet environment.

Figure 6 Infura Configuration

**C. Smart Contract:**

The smart contract deployed and used in the decentralized application is shown in Figure 7

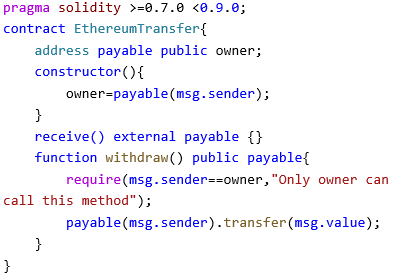
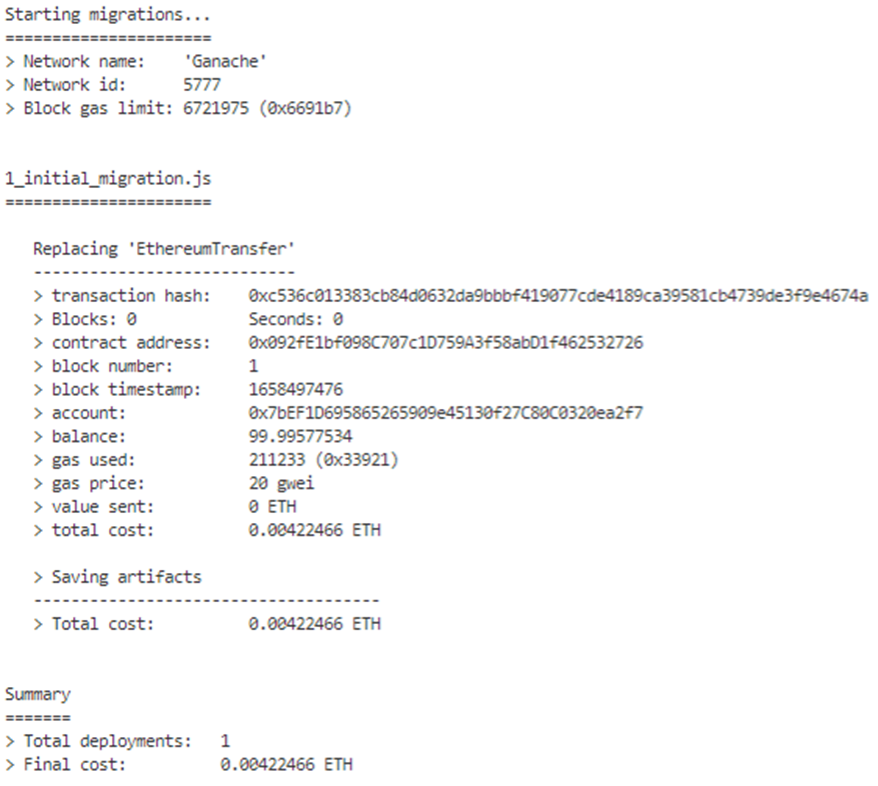


Figure 7 Ethereum Wallet Smart Contract

There are three methods through which we can transfer ether from one account to another from a contract address. Analysis of these methods is shown in Table 1

| **Function** | **Gas Limit** | **Exception Transmission** | **Issues** |
| --- | --- | --- | --- |
| Transfer() | 2300 | Reverts the state on failure | Gas limit and amount of forwarding gas very low |
| Send() | 2300 | Returns false on failure | Gas limit and amount of forwarding gas very low |
| Call() | Remaining  gas | Returns false on failure | If forwarding gas not specified transfer all gas to receiving contract |

Table 1



Since the smart contract code and functions developed are simple involving less gas, we have used transfer() method and it is also considered safe against reentrancy. However for complex smart contracts it is recommended to use call() function as there would be no problem of exceeding gas limit but when using this method gas should be specified otherwise all gas would be transferred to the receiving contract.Inorder to send ether to a smart contract payable keyword should be used with the function, It specifies that function can access some ether and without payable keyword function will reject incoming transaction.

V. EXPERIMENTAL RESULTS AND ANALYSIS

**A. Deploying Smart Contract on Ganache:**

Smart contract deployed on Ganache blockchain is shown in Figure 8. Similarly Figure 9 shows the deployed contract on Ganache GUI.

Figure 8 Smart Contract Deployment on Ganache

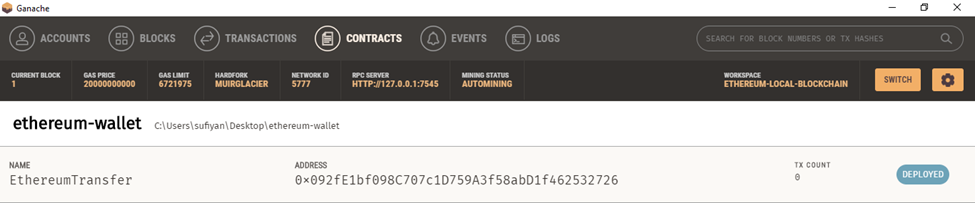
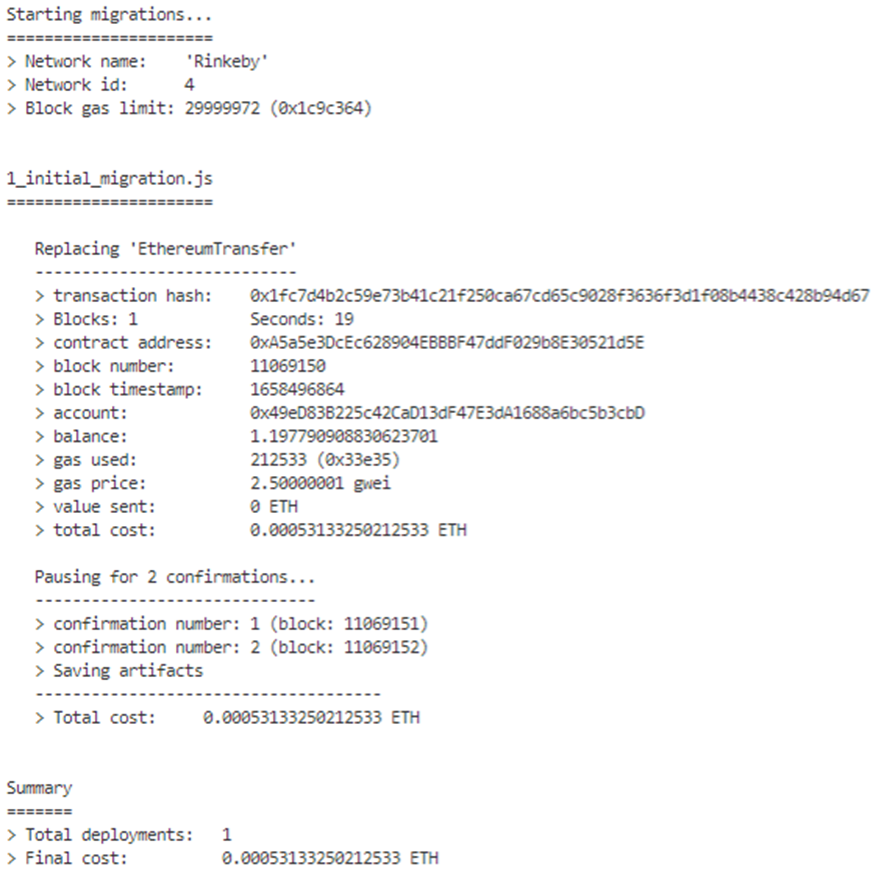


Figure 9 Deployed Smart Contract on Ganache GUI

When using ganache for deploying and testing smart contracts the block time is 0 since the block is automined so it is faster than a testnet. It is preferred only for quick smart contract testing and deployment. Since ganache is a local blockchain running on our system, it does not replicate the behavior of actual ethereum blockchain (mainnet).

**B. Deploying Smart Contract on Testnet:**

The smart contract was deployed on four different ethereum testnets ropsten, rinkeby, kovan and goerli. Figure 10 shows the deployed smart contract on the ropsten network. Comparison analysis of the time taken by different testnets to add a block is shown in Figure 11.

Figure 10 Deployed Smart Contract on Ropsten testnet

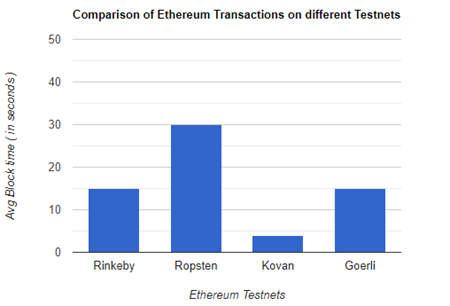


Figure 11

Table 2 shows the comparison of different ethereum testnets available considering different parameters and which one is better to use for deploying and testing purposes.

| **Ethereum Testnet** | **Average Block time** | **Network Id** | **Consensus Mechanism** |
| --- | --- | --- | --- |
| Rinkeby | 15s | 4 | PoA |
| Ropsten | 30s | 3 | PoW |
| Kovan | 4s | 42 | PoA |
| Goerli | 15s | 5 | PoA |

Table 2

For most use cases, Ropsten is the best and most popular Ethereum testnet faucet. The key benefit of Ropsten is that it is the only Proof of Work testnet that mimics how the actual Ethereum blockchain behaves in practice. As Proof of Authority networks like Rinkeby, Kovan, and Goerli might not be as accurate as Ropsten in simulating the actual Ethereum production environment so it is preferred to use Ropsten.

REFERENCES

**[1]** Vogel, Nick, The Great Decentralization: How Web 3.0 Will Weaken Copyrights (December 1, 2015). John Marshall Review of Intellectual Property Law, Vol. 15, No. 1, 2016, Available at SSRN: <https://ssrn.com/abstract=2738357>

**[2]** F. A. Alabdulwahhab, "Web 3.0: The Decentralized Web Blockchain networks and Protocol Innovation," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018, pp. 1-4, doi: 10.1109/CAIS.2018.8441990.

**[3]** R. Patel, A. Sethia and S. Patil, "Blockchain – Future of Decentralized Systems," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 369-374, doi: 10.1109/GUCON.2018.8675091.

**[4]** Q. Xu, Z. Song, R. S. Mong Goh and Y. Li, "Building an Ethereum and IPFS-Based Decentralized Social Network System," 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 2018, pp. 1-6, doi: 10.1109/PADSW.2018.8645058.

**[5]** Philipp Winter, Anna Harbluk Lorimer, Peter Snyder, Benjamin Livshits, “What’s in Your Wallet? Privacy and Security Issues in Web 3.0”

**[6]** K. C. Chan, X. Zhou, R. Gururajan, X. Zhou, M. Ally and M. Gardiner, "Integration of Blockchains with Management Information Systems," 2019 International Conference on Mechatronics, Robotics and Systems Engineering (MoRSE), 2019, pp. 157-162, doi: 10.1109/MoRSE48060.2019.8998694.

**[7]** Mally Anderson, “Exploring Decentralization: Blockchain Technology and Complex Coordination” 2019 Journal of Design and Science

**[8]** Mahzad Stearns, “A Decentralized Approach to Messaging Using Blockchain Technology” 2019 CALIFORNIA STATE UNIVERSITY, NORTHRIDGE

**[9]** A. G. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz and T. M. Alam, "A journey of WEB and Blockchain towards the Industry 4.0: An Overview," 2019 International Conference on Innovative Computing (ICIC), 2019, pp. 1-7, doi: 10.1109/ICIC48496.2019.8966700.

# **[10]** [Sofia Terzi](https://arxiv.org/search/cs?searchtype=author&query=Terzi%2C+S), [Konstantinos Votis](https://arxiv.org/search/cs?searchtype=author&query=Votis%2C+K), [Dimitrios Tzovaras](https://arxiv.org/search/cs?searchtype=author&query=Tzovaras%2C+D), [Ioannis Stamelos](https://arxiv.org/search/cs?searchtype=author&query=Stamelos%2C+I), [Kelly Cooper](https://arxiv.org/search/cs?searchtype=author&query=Cooper%2C+K), “Blockchain 3.0 Smart Contracts in E-Government 3.0 Applications”

**[11]** S. Patel, A. Sahoo, B. K. Mohanta, S. S. Panda and D. Jena, "DAuth: A Decentralized Web Authentication System using Ethereum based Blockchain," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019, pp. 1-5, doi: 10.1109/ViTECoN.2019.8899393.

**[12]** K. B. Muthe, T. S. T. Vemuru, K. Sharma and N. S. Mohammad, "Decentranet - An Ethereum, Proxy Re-Encryption and IPFS Based Decentralized Internet," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225483.

**[13]** Gaurish Korpal and Drew Scott, “Decentralization and web3 technologies” The University of Arizona Tucson, Arizona 85721

**[14]** Zarrin, J., Wen Phang, H., Babu Saheer, L. et al. Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Comput 24, 2841–2866 (2021).<https://doi.org/10.1007/s10586-021-03301-8>

**[15]** Z. Liu et al., "Make Web3.0 Connected," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2021.3079315.

**[16]** LIN Qinghua, WANG Keyuan, “A blockchain-based scheme to handle duplicate submission and paper authentication and the prototype system” [Chinese Journal of Scientific and Technical Periodicals](https://www.cjstp.cn/) ›› [2021](https://www.cjstp.cn/EN/archive/2021), [Vol. 32](https://www.cjstp.cn/EN/archive/2021) ›› [Issue (9)](https://www.cjstp.cn/EN/Y2021/V32/I9): 1105-1110. doi: [10.11946/cjstp.202102250175](https://doi.org/10.11946/cjstp.202102250175)

**[17]** Alex Murray, Dennie Kim, Jordan Combs, The promise of a decentralized Internet: What is web 3.0 and HOW can firms prepare?, Business Horizons, 2022, ISSN 0007-6813,<https://doi.org/10.1016/j.bushor.2022.06.002>. (<https://www.sciencedirect.com/science/article/pii/S0007681322000714>)

**[18]** Murray, Alex and Kim, Dennie and Combs, Jordan, The Promise of a Better Internet: What Is Web 3.0 and What Are We Building? (April 12, 2022). Available at SSRN: <https://ssrn.com/abstract=4082462> or [http://dx.doi.org/10.2139/ssrn.4082462](https://dx.doi.org/10.2139/ssrn.4082462)

**[19]** Bergquist Mcneil, L. (2022). Blockchains, smart contracts, and stablecoins as a global payment system : The rise of web 3.0 (Dissertation). Retrieved from<http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-114247>

**[20]** Qin Wang, Rujia Li, Qi Wang, Shiping Chen, Mark Ryan, Thomas Hardjono, “Exploring Web3 From the View of Blockchain”