International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 8 Issue 12 ǁ 2020 ǁ PP. 26-30

Secure Messaging Platform Using Blockchain Technology

Suman Kumar Das
[*1]*Software Engineer, Zenlabs, Zensar Technologies, Pune, India*
Corresponding Author:itsmesuman999@gmail.com

Abstract
This work aims to study the feasibility and advantages of blockchain technology in chat applications and propose a blockchain-based system for the messaging system. The existing Messaging System is based on centralized computing system architecture, but on a broader level replicas of such servers are distributed over several regions or zones. Secondly, the issue with the existing chat system is privacy, confidentiality, and trust. As every chat and related data is processed via centralized systems which are prone to various Cyber attacks like MITM, EFAIL, and others. This work proposed a blockchain-based system to counter and address such issues that exist in messaging systems and to help the user to exchange message and information securely.
Keywords: *Decentralized, Blockchain, Ethereum, Whisper Protocol, Security, Privacy and Confidentiality.*

Date of Submission: 08-12-2020 Date of acceptance: 24-12-2020

I. INTRODUCTION

In today's generation chatting over messaging platforms are a part of an individual's lifestyle. Today's most of the communication happens over social media platforms. All these platforms also provide users the option to share multimedia attachments leveraging their communication protocols over sockets. All these chat or messaging platforms are processed through centralized servers. All the user's message or information (maybe confidential) is being processed by the central server before transmitting the same to intended recipients. The issue with these kinds of system is that all the information are visible at processing servers even if the messages or information transmitted are claimed to be end to end encrypted. The author has created a messaging or rather say a simple chat application and has explained experimentally shown how the transmitted messages are visible at processing servers. Nevertheless, the system of the centralized system has scalability issues when compared to decentralized computing systems. In this work, the author has proposed a blockchain[1] based solution based on ethereum platform[2] using Whisper Protocol[3] to the issues that exist in traditional messaging or chat applications. In this section, the author has explained the background key concepts.

1.1. Deep Dive into the Problem Statement

Problem Statement- "In existing or traditional messaging platform or chat application, processing of information (message or information) happens through central computing servers. This can cause the private conversation between users visible at the server, even if they are claimed to be end to end protected". The author has shown how exchanged messages and information are visible at the Server end. Author has created a simple chat application and have shown the visibility of exchanged message or information in the central server.

Figure 1. shows the illustration of the Chat System between two users and Figure 2 shows the visibility of the message at server or web socket running on port 3000.

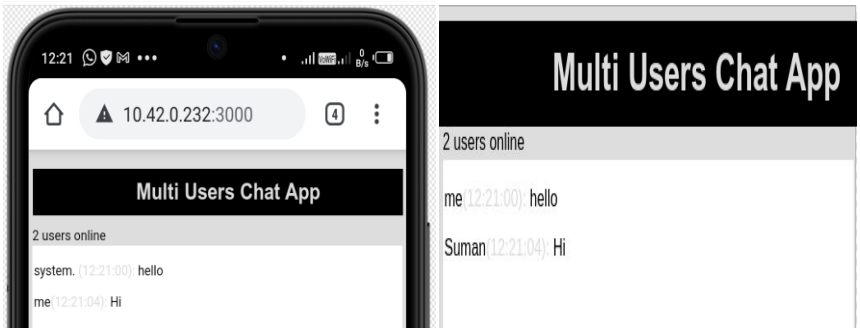

Figure 1. Chat between two users over a messaging platform.

```
debug - broadcasting packet
debug - websocket writing 5:::{"name":"newMsg","args":["system. ","hello \n","#000000"]}
debug - emitting heartbeat for client elOW6YT6HdM3HXfNmC9O
debug - websocket writing 2::
debug - set heartbeat timeout for client elOW6YT6HdM3HXfNmC9O
debug - broadcasting packet
debug - websocket writing 5:::{"name":"newMsg","args":["Suman","Hi","#000000"]}
debug - got heartbeat packet
```

Figure 2. Chat between two users visible at Messaging Platform.

This condition is true even for most of the messaging platform which claims the messages between users are end to end encrypted, the central server (which is hosting the chat business rule for chat application) must have the key to decrypt the message. Hence the encrypted messages can be visible at server end. There is no transparency how the server is maintained. It is a major concern as there is no assurance for Privacy and Confidentiality. Users often transfer confidential information (confidential files to trusted users) through these platforms. So there must be some systems which should assure full privacy and confidentiality to exchanged messages between users. Blockchain can be the key technology to address the above mentioned issues.

1.2. Blockchain

Blockchain is one of the emerging and cutting edge technology in the recent era. Blockchain is a decentralized ledger instead of a central authority. In simple words, the term blockchain itself stating it is a chain of blocks. A block can be a data structure that contains data and some attributes. Blocks can be linked together to form a chain of blocks. Basic Components of blocks are:

A. Hash: Unique Identifier of the current block. (Always unique).
B. Timestamp value.
C. Previous Hash: Hash of the previous block.
D. Data: Based on the type of Blockchain.

A hash can be treated as a fingerprint to identify a block. Figure 3. shows the representation of a blockchain. The first block is often referred to as the genesis block in the blockchain world, and it has no reference to the previous block.

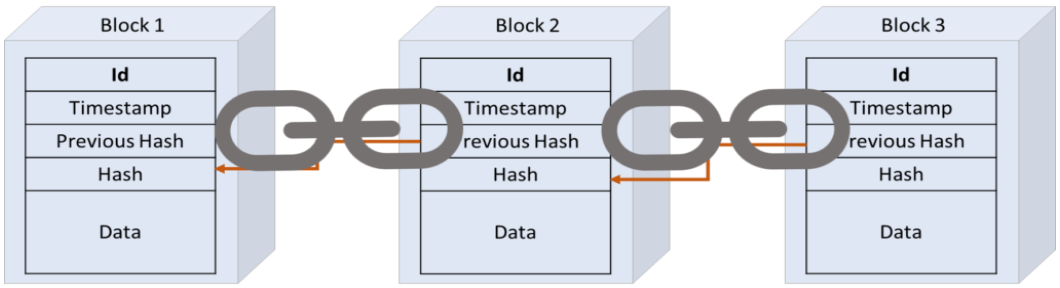

Figure 3. Representation of Blockchain

1.3. Ethereum

Ethereum is a public or permissionless Blockchain platform. Ethereum is one of the blockchain platforms to build decentralized applications. Ethereum Platform provides the flexibility to not only store transaction details on the block but also code snippets, which are termed as smart contracts[4]. The use of Smart Contracts makes the ethereum platform programmable. Ethereum follows WEB 3.0 Architecture which is illustrated in Figure 4.

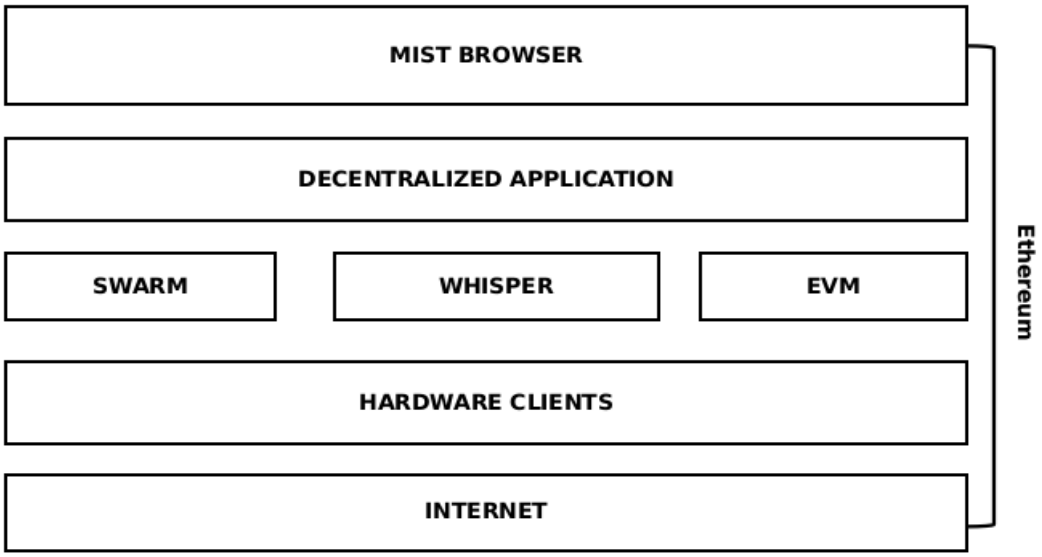

Figure 4. Web 3.0 Architecture - Representing Ethereum

The important layer related to this work is Layer 3. Swarm module only emphasizes on File Storage, an example is Inter Planetary File System (IPFS). EVM module emphasizes Consensus, this is something that networks must be agreeing upon some facts, Ethereum uses the Proof of Work[6] consensus algorithm. And Messaging layer is something that is used by Ethereum for communication using Peer to Peer Protocol, this protocol is known as Whisper Protocol. Whisper protocol happens over off-chain i.e. it has nothing to do with the smart contract execution of the blockchain. In a whisper, the protocol is an identity-based communication protocol, meaning each node or participant in the network is having some identity. Suppose, there are 5 nodes or participants in the network, A, B, C, D, and E respectively, if node A wants to send a message to node 2, then according to the whisper protocol, each node C, D, E, and B will receive the message, the message will only be decoded by intended recipient i.e. Node B in our case. Other nodes C, D, and E will simply discard or drop the message. The entire communication in whisper protocol is providing nodes to communicate in a secure environment. To make the entire communication more secure from external attacks Consensus algorithm Proof-of-Work is used. Whisper protocol is committed to achieving 100% darkness, however, there is some trade-off between the theoretical and practical value. Whisper protocol uses Asymmetric Key Encryption for communication.

1.4. Smart Contracts

Smart contracts are actually a business logic that is being developed as per requirements. It is used for automation and executes a specific task based on some events, i.e. Got automatically triggered when some events are executed. In the Ethereum platform Smart Contracts are written in “Solidity”, the Ethereum State Machine or (Ethereum Virtual Machine) converts the solidity code into low-level machinery language called Opcodes. Opcodes, often known as operational codes, is a set of instructions to execute a specific task. Initially, there were 140 Unique Opcodes. These opcodes together make the Ethereum machine a Turing complete. Figure 5 shows some of the most commonly used EVM opcodes and corresponding Gas consumption.

Operation	Gas	Description
ADD/SUB	3	Arithmetic operation
MUL/DIV	5	
ADDMOD/MULMOD	8	
AND/OR/XOR	3	Bitwise logic operation
LT/GT/SLT/SGT/EQ	3	Comparison operation
POP	2	Stack operation
PUSH/DUP/SWAP	3	
MLOAD/MSTORE	3	Memory operation
JUMP	8	Unconditional jump
JUMPI	10	Conditional jump
SLOAD	200	Storage operation
SSTORE	5,000/ 20,000	
BALANCE	400	Get balance of an account
CREATE	32,000	Create a new account using CREATE
CALL	25,000	Create a new account using CALL

Figure 5. Opcodes and Corresponding Gas Consumption

II. PROPOSED METHODOLOGY

Figure 6. shows the work flow of the proposed architecture.

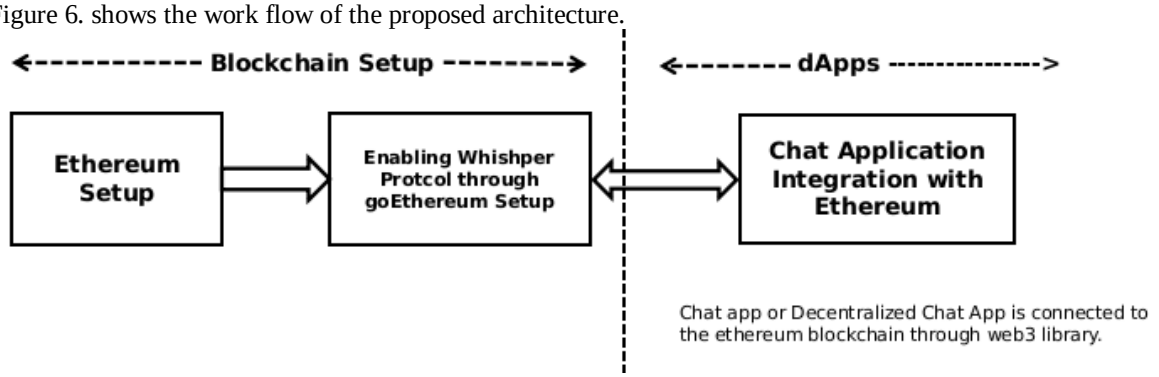

Figure 6. Proposed Architecture.

In the first step author have setup the ethereum platform and have enabled the whishper protocol for communication. Post deploying the ethereum network author have integrated the chat application with blockchain network through "web3.js" library. The chat will happens over peer to peer protocol, the no server is involved in between.

III. RESULT AND DISCUSSION

Figure 7. shows the illustration of setting up the ethereum network and enabling whisper protocol and Figure 8, depicts the working of decentralized application.

```
root@mail:/home/sd51481# geth --syncmode fast --cache=1024 --shh --datadir $DATADIR/private --rpcaddr 0.0.0.0 --rpc --rpcport 8545 --r
pccorsdomain="*" --networkid 12345 --rpcapi eth,net,web3,personal,shh --nodiscover
INFO [12-18|22:35:55.584] Maximum peer count                       ETH=50 LES=0 total=50
WARN [12-18|22:35:55.584] The flag --rpc is deprecated and will be removed in the future, please use --http
WARN [12-18|22:35:55.585] The flag --rpcaddr is deprecated and will be removed in the future, please use --http.addr
WARN [12-18|22:35:55.585] The flag --rpcport is deprecated and will be removed in the future, please use --http.port
WARN [12-18|22:35:55.585] The flag --rpccorsdomain is deprecated and will be removed in the future, please use --http.corsdomain
WARN [12-18|22:35:55.585] The flag --rpcapi is deprecated and will be removed in the future, please use --http.api
INFO [12-18|22:35:55.585] Smartcard socket not found, disabling    err="stat /run/pcscd/pcscd.comm: no such file or directory"
INFO [12-18|22:35:55.588] Set global gas cap                       cap=25000000
WARN [12-18|22:35:55.588] Whisper support has been deprecated and the code has been moved to github.com/ethereum/whisper
INFO [12-18|22:35:55.588] Allocated trie memory caches             clean=255.00MiB dirty=256.00MiB
INFO [12-18|22:35:55.588] Allocated cache and file handles         database=/private/geth/chaindata cache=512.00MiB handles=524288
INFO [12-18|22:35:55.834] Opened ancient database                  database=/private/geth/chaindata/ancient
INFO [12-18|22:35:55.837] Initialised chain configuration          config="{ChainID: 1 Homestead: 1150000 DAO: 1920000 DAOSupport: tru
e EIP150: 2463000 EIP155: 2675000 EIP158: 2675000 Byzantium: 4370000 Constantinople: 7280000 Petersburg: 7280000 Istanbul: 9069000, Mu
ir Glacier: 9200000, YOLO v1: <nil>, Engine: ethash}"
```

Figure 7. Ethereum Network set up and enabling Whisper Protocol using shh flag

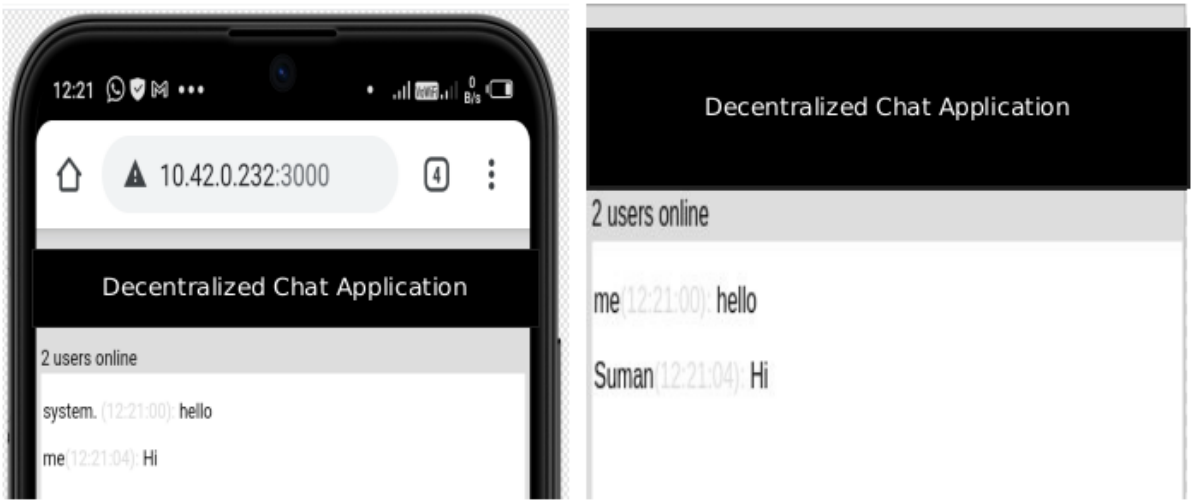

Figure 8. Decentralized Chat Application.

As the communication is happening over a blockchain platform leveraging whisper protocol in peer to peer mode, the communication does not rely on the central server. All the message that is happening between recipients is secure, private, and confidential. Also, these kinds of decentralized chat system perform better as compared to Centralized Chat Application in terms of throughput, scalability, and uptime.

IV. CONCLUSION

From the above discussion, we conclude that the blockchain platform can be a key technology that can solve privacy and confidentiality related issues that exist in the Traditional or existing messaging system. Also, a decentralized-based messaging system performs better than a centralized messaging platform in terms of scalability, throughput, processing, and uptime. This author has practically shown how confidential and private messages are visible at the processing or computing end of the chat server. Authors have also explained and shown how blockchain-based chat application will help users to exchange information securely, leveraging whisper protocol in peer to peer mode.

REFERENCES

[1]. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[2]. Vujicic, Dejan & Jagodic, Dijana & Ranđić, Siniša. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. 1-6. 10.1109/INFOTEH.2018.8345547.

[3]. Eberhardt, Jacob & Tai, Stefan. (2017). On or Off the Blockchain? Insights on Off-Chaining Computation and Data. 3-15. 10.1007/978-3-319-67262-5_1.

[4]. Alharby, Maher & van Moorsel, Aad. (2017). Blockchain Based Smart Contracts : A Systematic Mapping Study. 125-140. 10.5121/csit.2017.71011.

[5]. EVM Opcodes Imagehttps://labs.imaginea.com/optimizing-smart-contracts-for-cost/

[6]. Gervais, Arthur & Karame, Ghassan & Wüst, Karl & Glykantzis, Vasileios & Ritzdorf, Hubert & Capkun, Srdjan. (2016). On the Security and Performance of Proof of Work Blockchains. 3-16. 10.1145/2976749.2978341.