Π2PCATH

GTÜ CSE 495&496

BLOCKCHAIN BASED SECURE MESSAGING APPLICATION

Muhammed Bedir ULUCAY

Project Consultant:
Prof. Dr. Ibrahim SOGUKPINAR

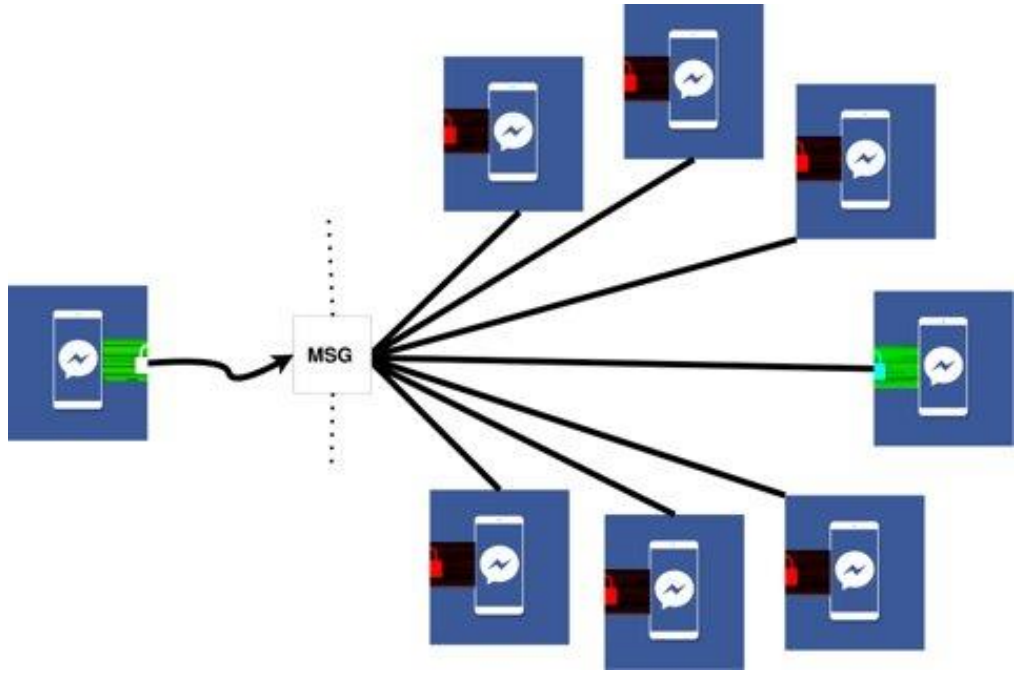
Jan 20223

GEBZE TEKNİK ÜNİVERSİTESİ

CONTENTS

• SCHEME AND DESCRIPTION OF THE PROJECT

- **An application where people can securely communicate with each other as a peer to peer. To create a reliable and unchangeable communication channel between users using blockchain and cryptology. In this way, users can be absolutely sure that their data cannot be accessed by third parties or malicious people and from the recipient side.**



• IMPLEMENTATIONS

- We made two different implementation for the project.
- 1-) Ethereum Network and tools usage
- 2-) Implementation own local blockchain network

- The first implementation was carried out with the use and integration of many already developed tools.
- Tools : Etherscan, Hardhat, Infura, Metamask, Remix

- The second implementation is implemented from scratch in go programming language.
- A node can do the following:
  1. Create wallet address
  2. Send message
  3. Search message
  4. Mine own transaction
  5. It could be a miner for other's transaction
  6. Print the whole blockchain

• ETHEREUM NETWORK - DEPLOY

```
mbulucay@mbulucay:~/Blockchain/deploy/p2pChat$ npx hardhat clean; npx hardhat compile
Compiled 2 Solidity files successfully
mbulucay@mbulucay:~/Blockchain/deploy/p2pChat$ npx hardhat run ./scripts/deploy.js --network goerli
Lock with 1 ETH and unlock timestamp 1705345107 deployed to 0xd4CF6711d2b034DA31C95a8D96b29e6af1C96CEf
mbulucay@mbulucay:~/Blockchain/deploy/p2pChat$
```

Contract 0xd4CF6711d2b034DA31C95a8D96b29e6af1C96CEf

Contract Overview

Balance: 0 Ether

More Info More

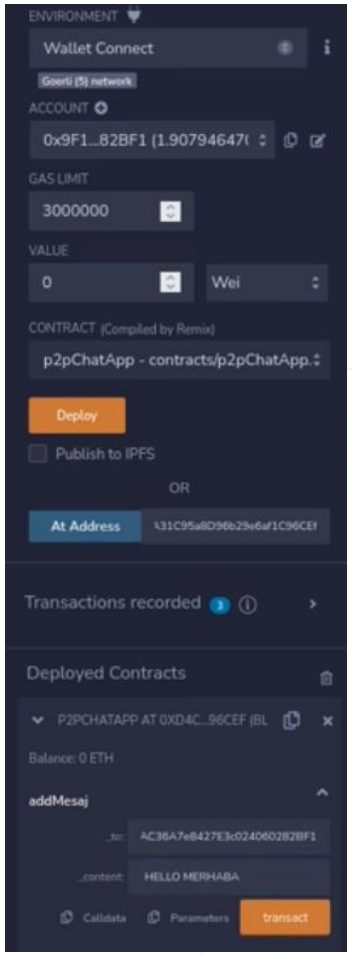
My Name Tag: Not Available

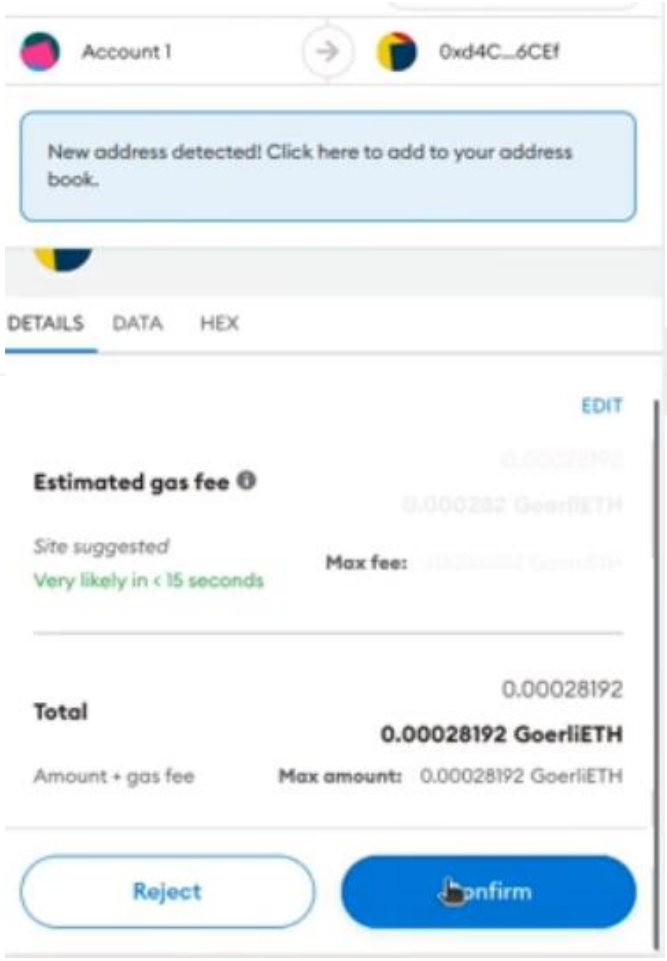
Contract Creator: 0x9f1fb796a96214ac36a... at txn 0x892d091a6e6a527c72...

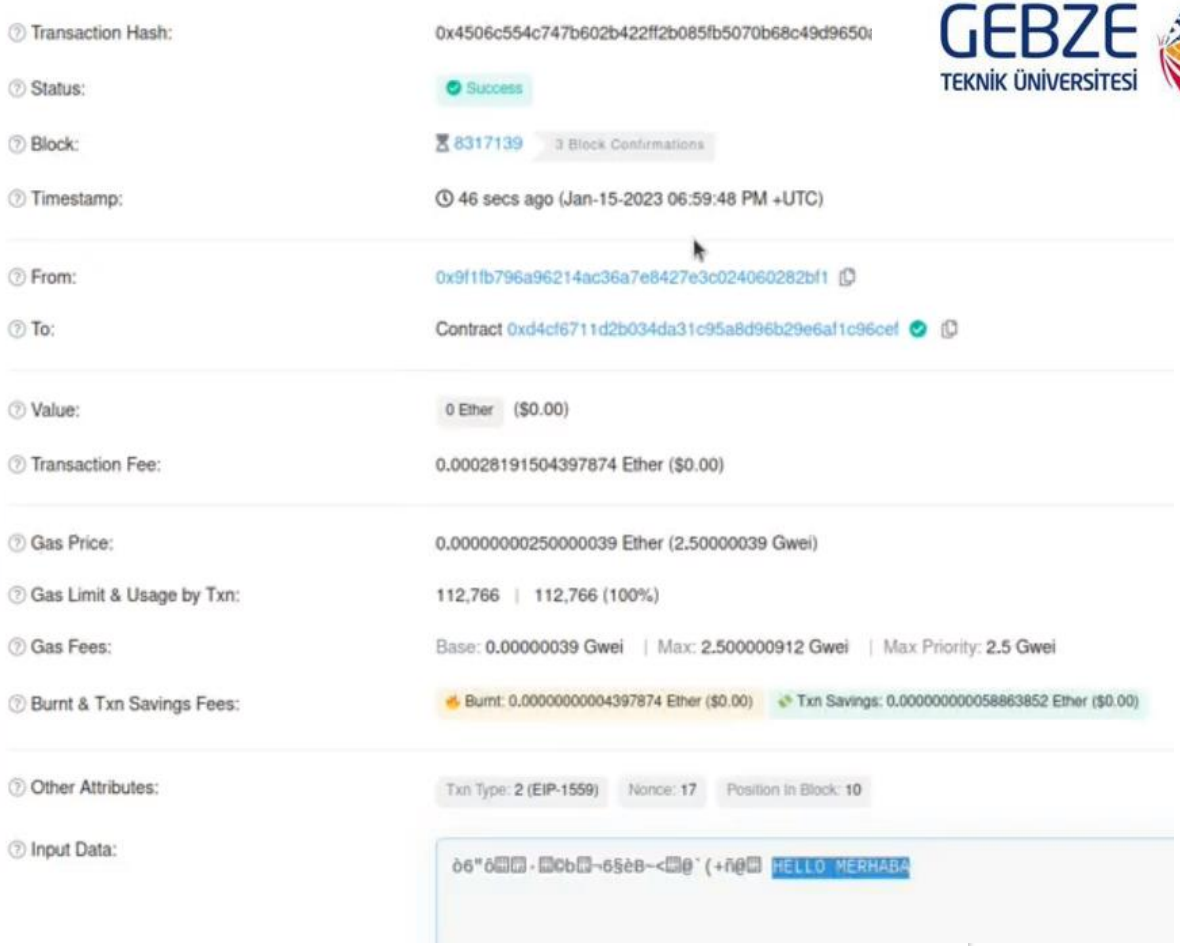
Transactions | Erc20 Token Txns | Contract | Events

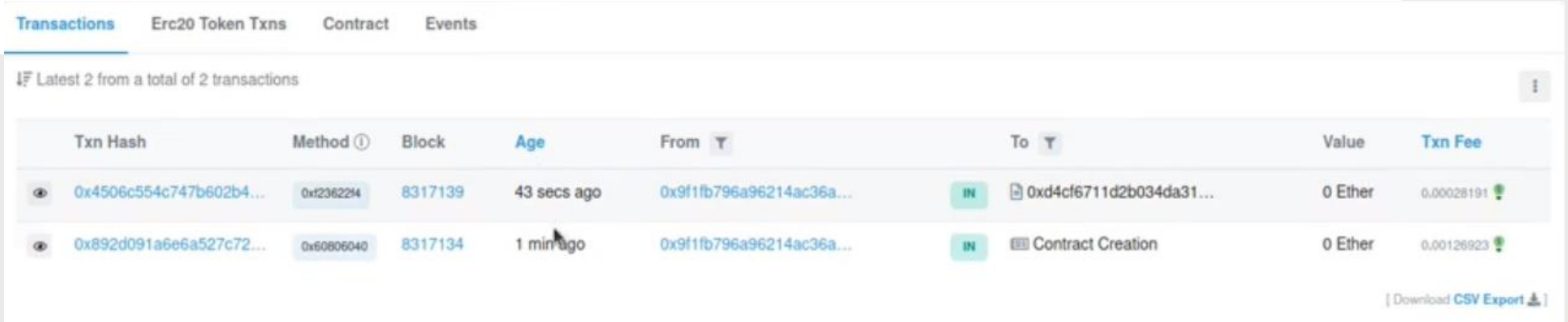
Latest 1 from a total of 1 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0x892d091a6e6a527c72...	0x60806040	8317134	32 secs ago	0x9f1fb796a96214ac36a...	IN	Contract Creation	0 Ether	0.00126923


ENVIRONMENT
Wallet Connect
Goerli (5) network
ACCOUNT
0x9F1...82BF1 (1.90794647(
GAS LIMIT
3000000
VALUE
0
Wei
CONTRACT (Compiled by Remix)
p2pChatApp - contracts/p2pChatApp.
Deploy
Publish to IPFS
OR
At Address
Transactions recorded
Deployed Contracts
P2PCHATAPP AT 0XD4C...96CEF (BL
Balance: 0 ETH
addMesaj
_to:
AC36A7e8427E3c024060282BF1
_content:
HELLO MERHABA
Calldata
Parameters
transact


Account 1
0xd4C...6CEf
New address detected! Click here to add to your address book.
DETAILS
DATA
HEX
EDIT
Estimated gas fee
Site suggested
Very likely in < 15 seconds
Max fee:
Total
0.00028192
0.00028192 GoerliETH
Amount + gas fee
Max amount: 0.00028192 GoerliETH
Reject
Confirm


Transaction Hash:
0x4506c554c747b602b422ff2b085fb5070b68c49d9650
Status:
Success
Block:
8317139
3 Block Confirmations
Timestamp:
46 secs ago (Jan-15-2023 06:59:48 PM +UTC)
From:
0x9f1fb796a96214ac36a7e8427e3c024060282bf1
To:
Contract 0xd4cf6711d2b034da31c95a8d96b29e6af1c96cef
Value:
0 Ether ($0.00)
Transaction Fee:
0.00028191504397874 Ether ($0.00)
Gas Price:
0.000000002500000039 Ether (2.50000039 Gwei)
Gas Limit & Usage by Txn:
112,766 | 112,766 (100%)
Gas Fees:
Base: 0.00000039 Gwei | Max: 2.500000912 Gwei | Max Priority: 2.5 Gwei
Burnt & Txn Savings Fees:
Burnt: 0.000000000004397874 Ether ($0.00)
Txn Savings: 0.000000000058863852 Ether ($0.00)
Other Attributes:
Txn Type: 2 (EIP-1559)
Nonce: 17
Position In Block: 10
Input Data:
HELLO MERHABA


Transactions
Erc20 Token Txns
Contract
Events
Latest 2 from a total of 2 transactions
Txn Hash
Method
Block
Age
From
To
Value
Txn Fee
0x4506c554c747b602b4...
0xf2362214
8317139
43 secs ago
0x9f1fb796a96214ac36a...
IN
0xd4cf6711d2b034da31...
0 Ether
0.00028191
0x892d091a6e6a527c72...
0x60806040
8317134
1 min ago
0x9f1fb796a96214ac36a...
IN
Contract Creation
0 Ether
0.00126923
[Download CSV Export]

• OWN IMPLEMENTATION

- Build the own blockchain network using go programming language.
- Creating a Wallet

```
mbulucay@mbulucay:~/Blockchain/p2pChatApp$ export NODE_ID=6000
mbulucay@mbulucay:~/Blockchain/p2pChatApp$ go run main.go createwallet
New address is: 1PcywwMP955nUXyUnrztKX61iMZLavG8r9
mbulucay@mbulucay:~/Blockchain/p2pChatApp$
```

- See Wallet Address

```
mbulucay@mbulucay:~/Blockchain/p2pChatApp$ go run main.go listaddresses
1PcywwMP955nUXyUnrztKX61iMZLavG8r9
mbulucay@mbulucay:~/Blockchain/p2pChatApp$
```

- Genesis & Blockchain Creation

```
mbulucay@mbulucay:~/Blockchain/p2pChatApp$ go run main.go create
blockchain -address 14URJq5kz9irH9SbheDKGi1j2tsnz6GKmg
2023/01/15 22:06:10 Replaying from value pointer: {Fid:0 Len:0 O
ffset:0}
2023/01/15 22:06:10 Iterating file id: 0
2023/01/15 22:06:10 Iteration took: 9.28µs
0008d88722fd957e67c4d9b774d67cebce9920703922615f3579a7632e86d56d
Genesis created
Finished!
mbulucay@mbulucay:~/Blockchain/p2pChatApp$
```

- Key Generate

```
mbulucay@mbulucay:~/Blockchain/p2pChatApp/keyGenerator$ go run generate.go
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxq9BweR1N3XAWQ/28Q4kMdalhNQmIKehB8YtCzEnd/uuFACn
bpIz0rlf61/6Sac0ULXR+vtH2LK8aouGULALxSVYLde1F2v2CnZHdZrGWnHFynO1
yFCKhOcWwU7i3WGVpgGHcMf4y2BhEh41dj9EFD8gVekRY81AndXKZEk2680jYVsH
tyOglhPPsrsMT0MIyIU3jB8CPfm/0wfH7YIRKA3w++dnvrU9u4m6wv7fpB3y/vNm
riR6Ls72p1BL7YBEEOn3UURKozFtaKQmZvcj+jj5GjZ1OnPoQMt0tWg/9HdhE6wM
```

- Sending Message with key

```
mbulucay@mbulucay:~/Blockchain/p2pChatApp$ go run main.go send -
from 14URJq5kz9irH9SbheDKGi1j2tsnz6GKmg -to 1CP2zcQ5bntsskdSYFeN
r3s76ri3HzcCoM -message "BU BIR MESAJDIR" -mine -publickey ./use
rKeys/user_2/pubkey.pem
2023/01/15 22:08:18 Replaying from value pointer: {Fid:0 Len:42
Offset:1039}
2023/01/15 22:08:18 Iterating file id: 0
2023/01/15 22:08:18 Iteration took: 9.801µs
000ce366169205398eda0da737a70af55ce3d0f29719f9c187d311aa69672e8a
Success!
mbulucay@mbulucay:~/Blockchain/p2pChatApp$
```

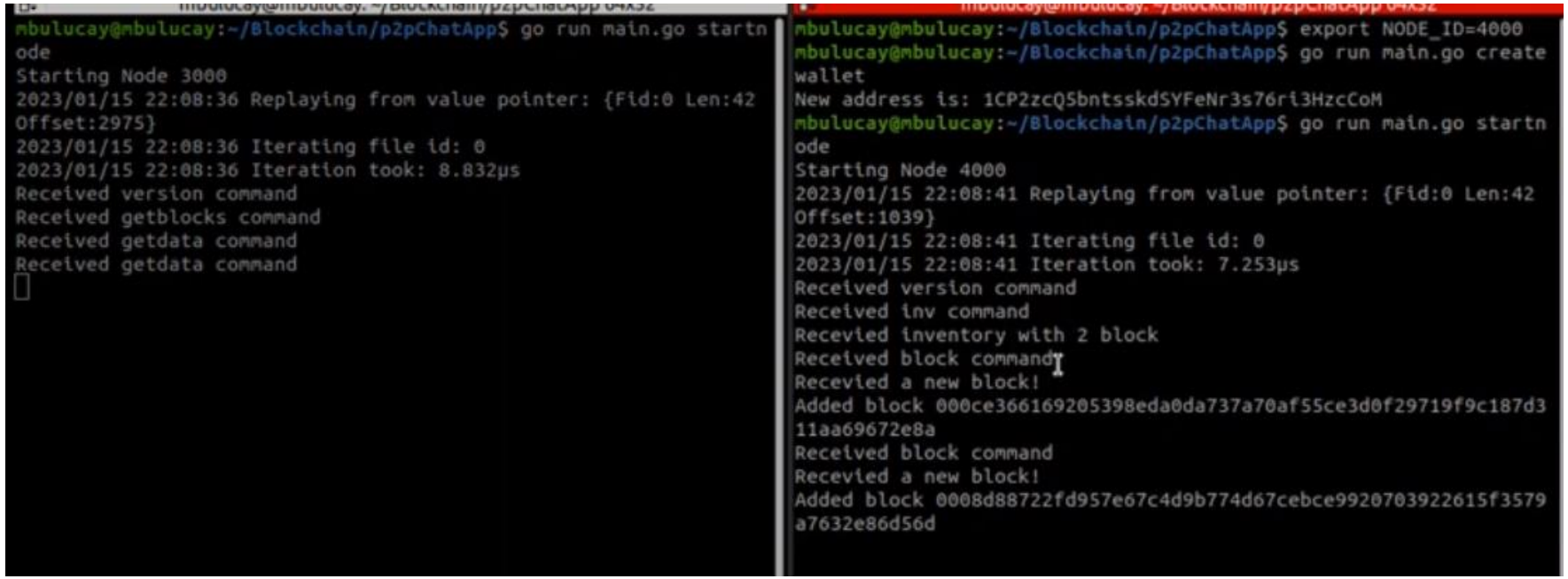
- Print Blockchain

```
mbulucay@mbulucay:~/Blockchain/p2pChatApp$ go run main.go printchain
2023/01/17 15:07:50 Replaying from value pointer: {Fid:0 Len:43 Offset:9945}
2023/01/17 15:07:50 Iterating file id: 0
2023/01/17 15:07:50 Iteration took: 148.605µs
```

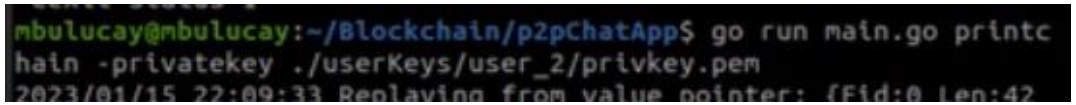
```
Hash: 0008d88722fd957e67c4d9b774d67cebce9920703922615f3579a7632e
86d56d
Prev. hash:
PoW: true
--- Transaction 3c2c038f523b98b65c797da4166913c8bf023c91a3466aa1
8d98aa190c28e6c1:
     Input 0:
     TXID []:
     Out -1:
     Signature :
     PubKey 4669727374205472616e73616374696f6e2066726f6d2047656e
65736973:
        Output 0
        Value  Thank you for your services 14URJq5kz9irH9SbheDK
Gi1j2tsnz6GKmg
        Script: &◆,;◆OS◆*◆◆◆◆◆Fv◆◆
```

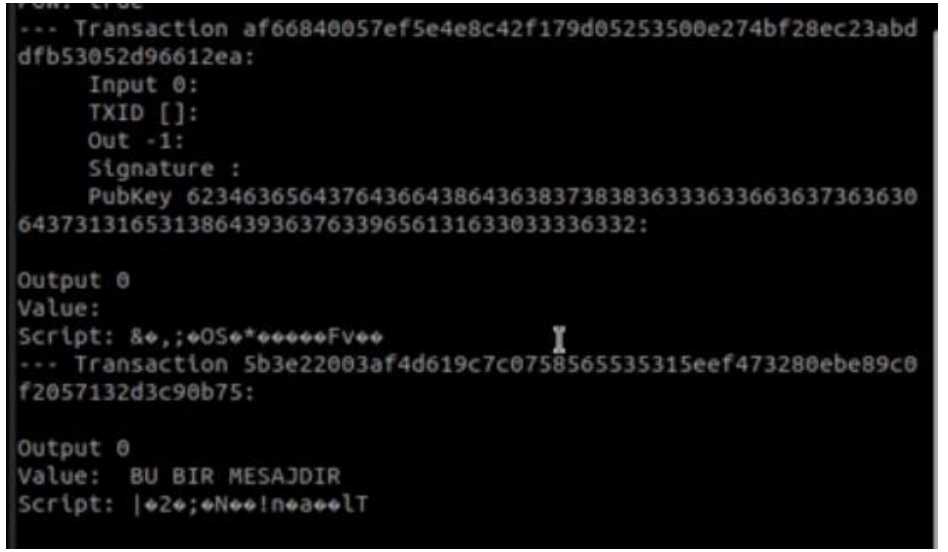
```
2023/01/15 22:08:22 Replaying from value pointer: {Fid:0 Len:42
Offset:2975}
2023/01/15 22:08:22 Iterating file id: 0
2023/01/15 22:08:22 Iteration took: 8.974µs
Hash: 000ce366169205398eda0da737a70af55ce3d0f29719f9c187d311aa69
672e8a
Prev. hash: 0008d88722fd957e67c4d9b774d67cebce9920703922615f3579
a7632e86d56d
PoW: true
--- Transaction af66840057ef5e4e8c42f179d05253500e274bf28ec23abd
dfb53052d96612ea:
     Input 0:
     TXID []:
     Out -1:
     Signature :
     PubKey 6234636564376436643864363837383836333633663637363630
643731316531386439363763396561316330333336332:
        Output 0
        Value  Thank you for your services 14URJq5kz9irH9SbheDK
Gi1j2tsnz6GKmg
        Script: &◆,;◆OS◆*◆◆◆◆◆Fv◆◆
--- Transaction 5b3e22003af4d619c7c0758565535315eef473280ebe89c0
f2057132d3c90b75:
        Output 0
        Value  c◆◆E◆◆KL◆E◆@◆◆<b◆◆◆◆*"◆◆◆'◆◆t◆&*x◆'◆◆Ek◆◆)aP}◆◆[
◆8◆◆◆◆@◆◆◆C◆◆{◆,◆L+◆◆Z◆,◆◆◆=◆X◆◆◆tZG5◆Pv◆◆◆+◆◆◆◆◆3◆◆U◆x8M5◆◆9◆◆
S◆_\"◆◆◆r◆OR◆◆/◆◆U◆◆◆g◆◆kt◆U k= ◆u◆◆◆z◆◆)
◆◆◆
   ◆◆H◆'df◆◆◆*◆j<◆u◆?◆0.)◆W◆◆mP&◆;S◆◆l◆%◆9◆Y◆◆WXw◆◆◆k◆<◆◆Q◆8◆m◆◆
◆a90
        Script: |◆2◆;◆N◆◆!n◆a◆◆lT
```

- Start Node Pull Transaction

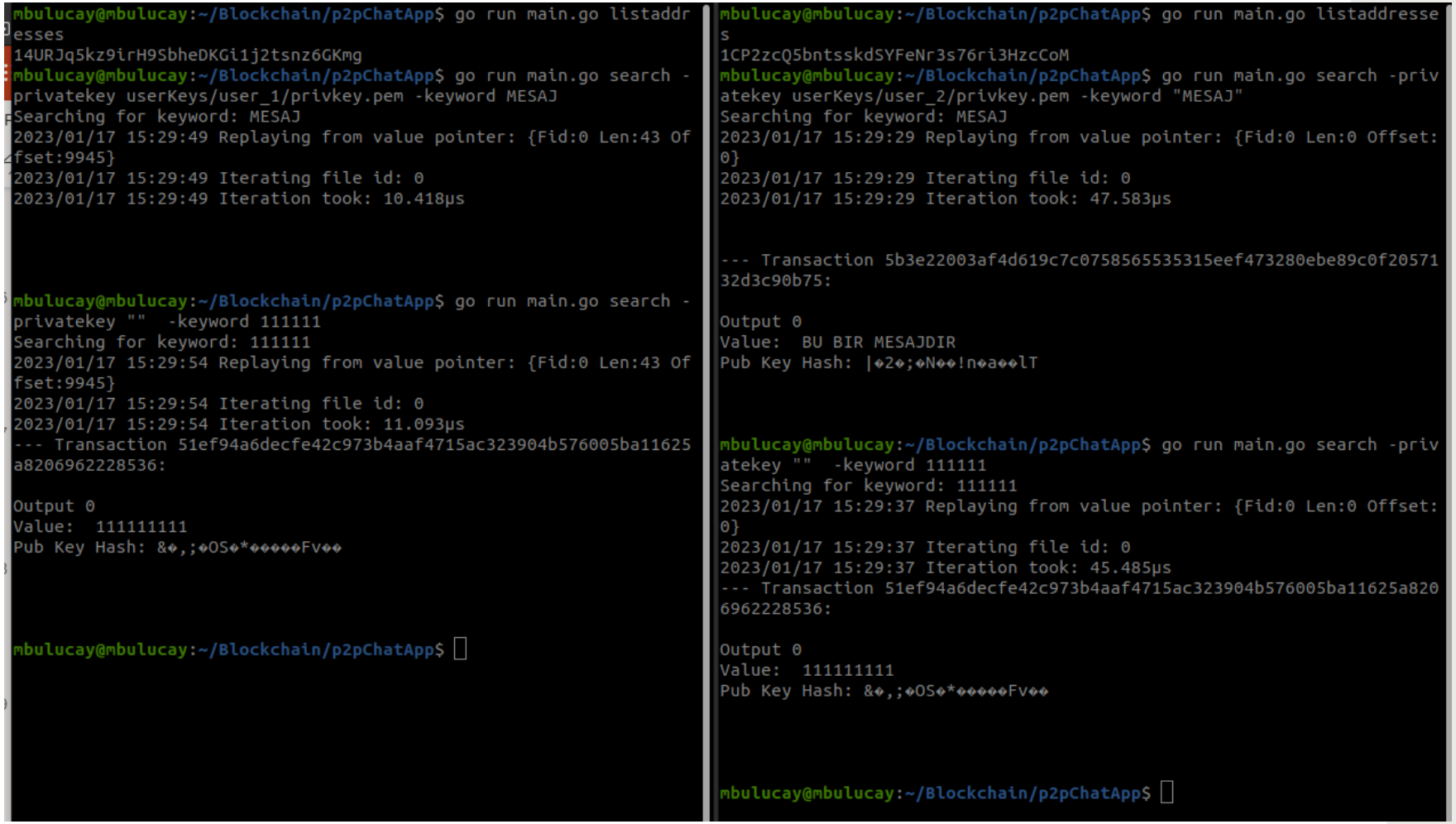


- Encrypt Message

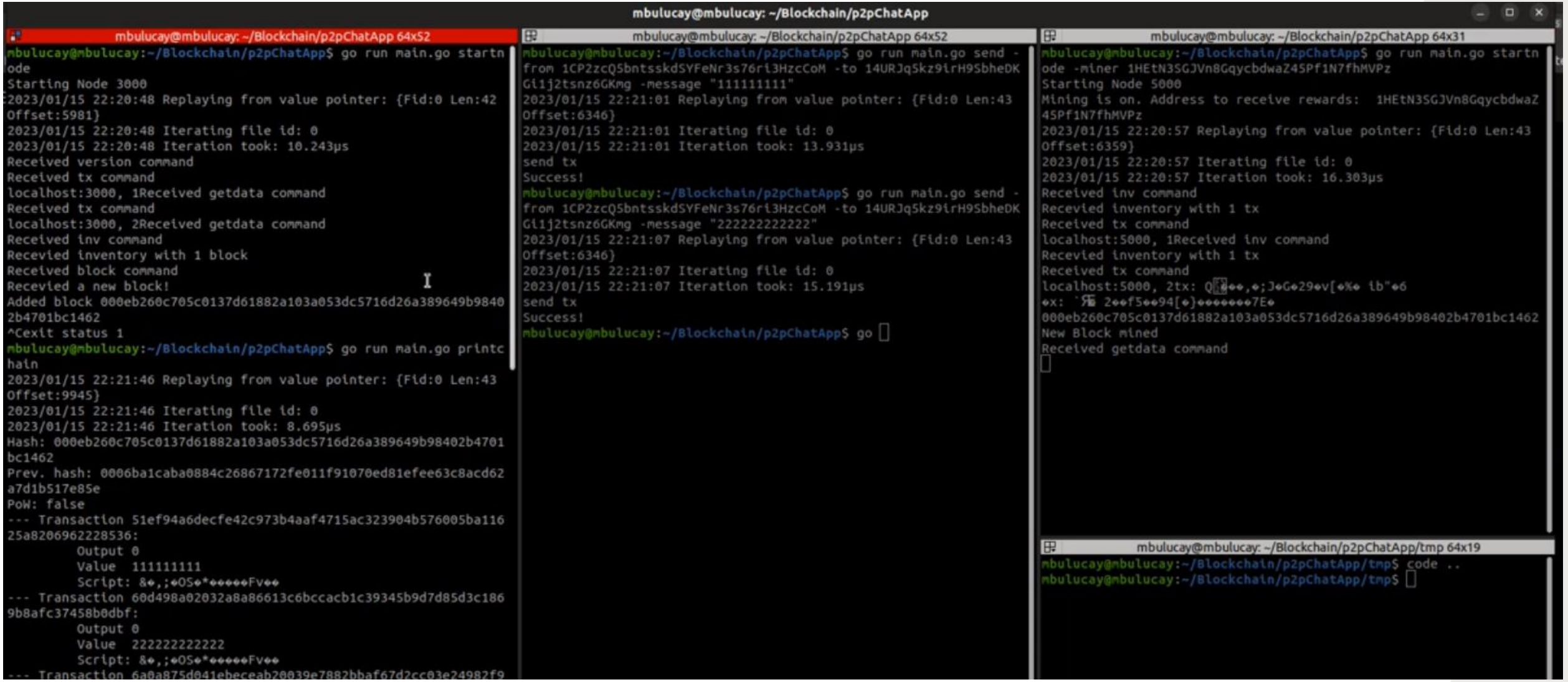




- Searching A Word



- Being A Miner Node



PROJECT DEVELOPMENT STAGES

- **First Presentation:**

Most of the time until my first presentation was spent doing literature research and researching similar projects.

- **Second Presentation:**

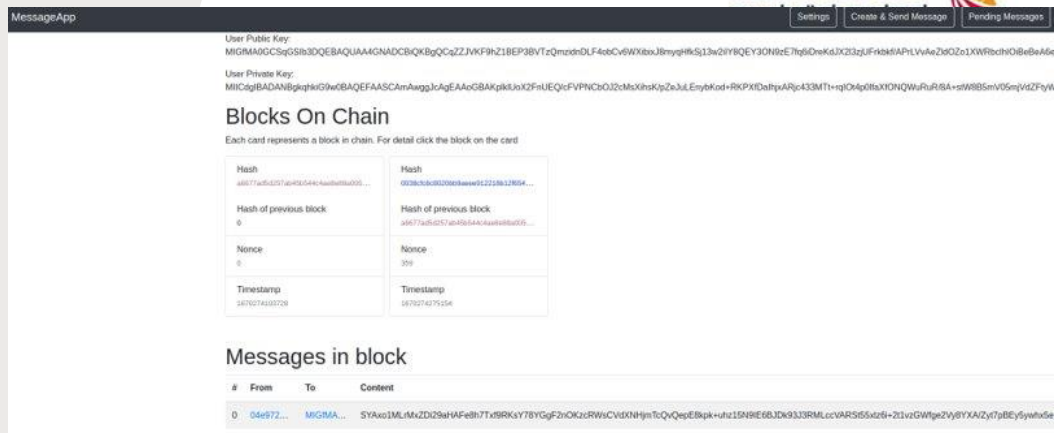
I prepared a simple blockchain structure and passed with data sending and receiving operations on it.

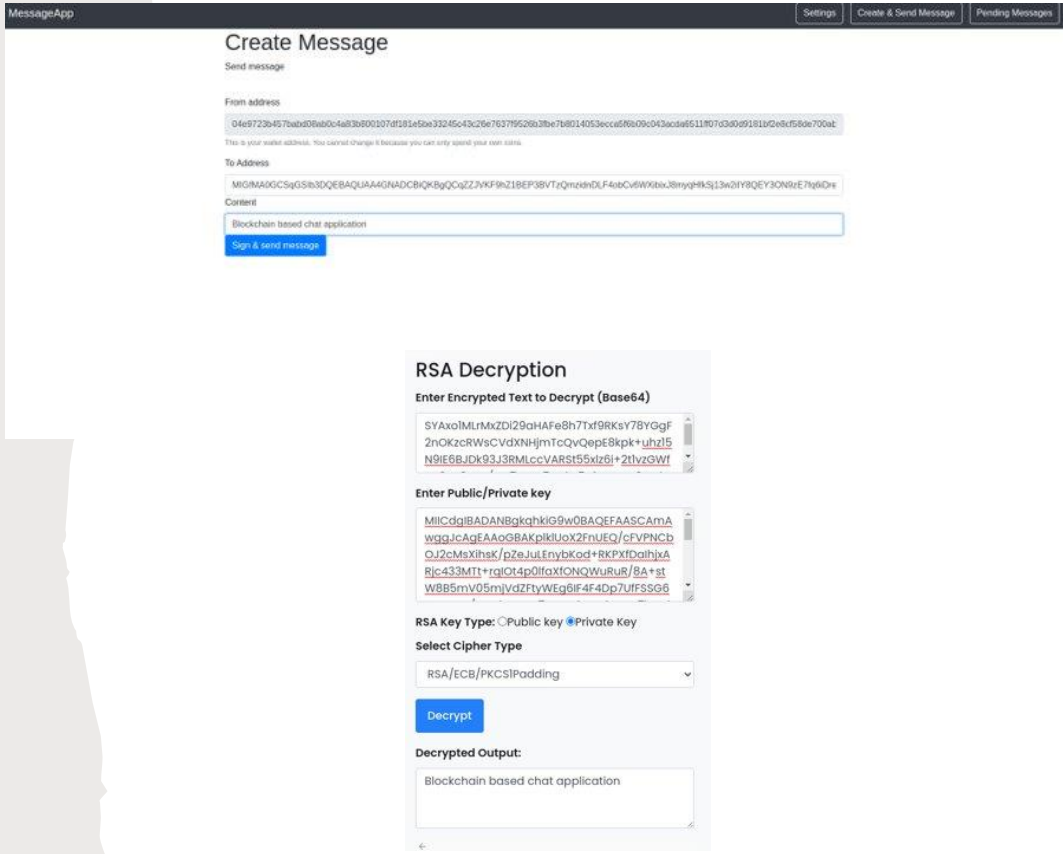
I did research on asymmetric encryption.

The design of the project became more specific.

I did research and experiments about the technologies I use.

I made transactions on the simple blockchain that I designed with a simple interface.





- **Final Presentation:**

Made an application about how to deploy the blockchain application on the Ethereum Network and send and receive data there.

Designed a blockchain network within my own local network.

Stored the data under different folders on this network using message exchange and badger database.

For the nodes, I defined the features related to sending data, reading data, calculating transactions and creating records.

• RESULT

- We have developed a system using a peer to peer blockchain based database where users can communicate with each other after creating a wallet address and 2 keys, one public and the other private.
- Users can do basic features such as sending messages and encryption within the application.
- It is also resistant to any point attacks or single point failure as the data is stored in different parts.
- Regarding the computational issues of messaging, the requesting node can directly calculate its own message, while other willing nodes can volunteer to compute the messages of others. While creating the block,

thank you message will be defined to their address :D:D

• SUCCESS CRITERIA

- Making message transaction below 4 second (human psychological) (Successful)

- Usage and signing of the program after installation in 10 minute.
  The project requirements slightly changed after second representation sign in in the program is just one command for own implementation.
  Ethereum Network implementation is just installing the meta mask on your browser.
  (Requirements has changed for new approach Successful)

- Loading message transactions from blockchain under 2 minute. (Successful)

Depend On The Size

When a text search is requested, all messages containing the text written in less than 2 minute can be displayed to the user. (Successful)

Depend On The Size

REFERENCES

- https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends
- https://www.irjet.net/archives/V7/i5/IRJET-V7I5531.pdf
- https://github.com/machinomy/awesome-non-financial-blockchain#readme
- https://scholarworks.calstate.edu/concern/theses/qj72pb04f?locale=en
- https://bitcoin.org/bitcoin.pdf
- https://github.com/TristanBilot/blockchain-chat-app
- https://www.youtube.com/watch?v=hYip_Vuv8J0&t=261s
- https://www.youtube.com/watch?v=bBC-nXj3Ng4&t=1065s
- https://www.youtube.com/watch?v=ZEApLtE8KkE&list=PLxz5ldaTYSOUmhECFNN-WfGeJrzlnXn_a
- https://www.blockchain.com/tr/explorer
- https://www.youtube.com/watch?v=yubzJw0uiE4&t=261s

- https://medium.com/adamant-im/how-decentralized-blockchain-messenger-works-b9932834a639
- https://medium.com/@BeFastTV/top-blockchain-messaging-apps-crypto-messengers-28893e5f908f
- https://hal.archives-ouvertes.fr/hal-02180329/document/
- https://docs.soliditylang.org/en/v0.8.17/introduction-to-smart-contracts.html
- https://remix.ethereum.org
- https://www.researchgate.net/publication/328160285_Survey_of_Consensus_Protocols
- https://blog.harmony.one/peer-discovery-in-harmony-network/
- https://rejolut.com/blog/creating-your-own-blockchain-network/
- https://docs.infura.io/infura/networks/ethereum
- https://hardhat.org/hardhat-runner/docs/getting-started#overview
- https://go.dev/doc/