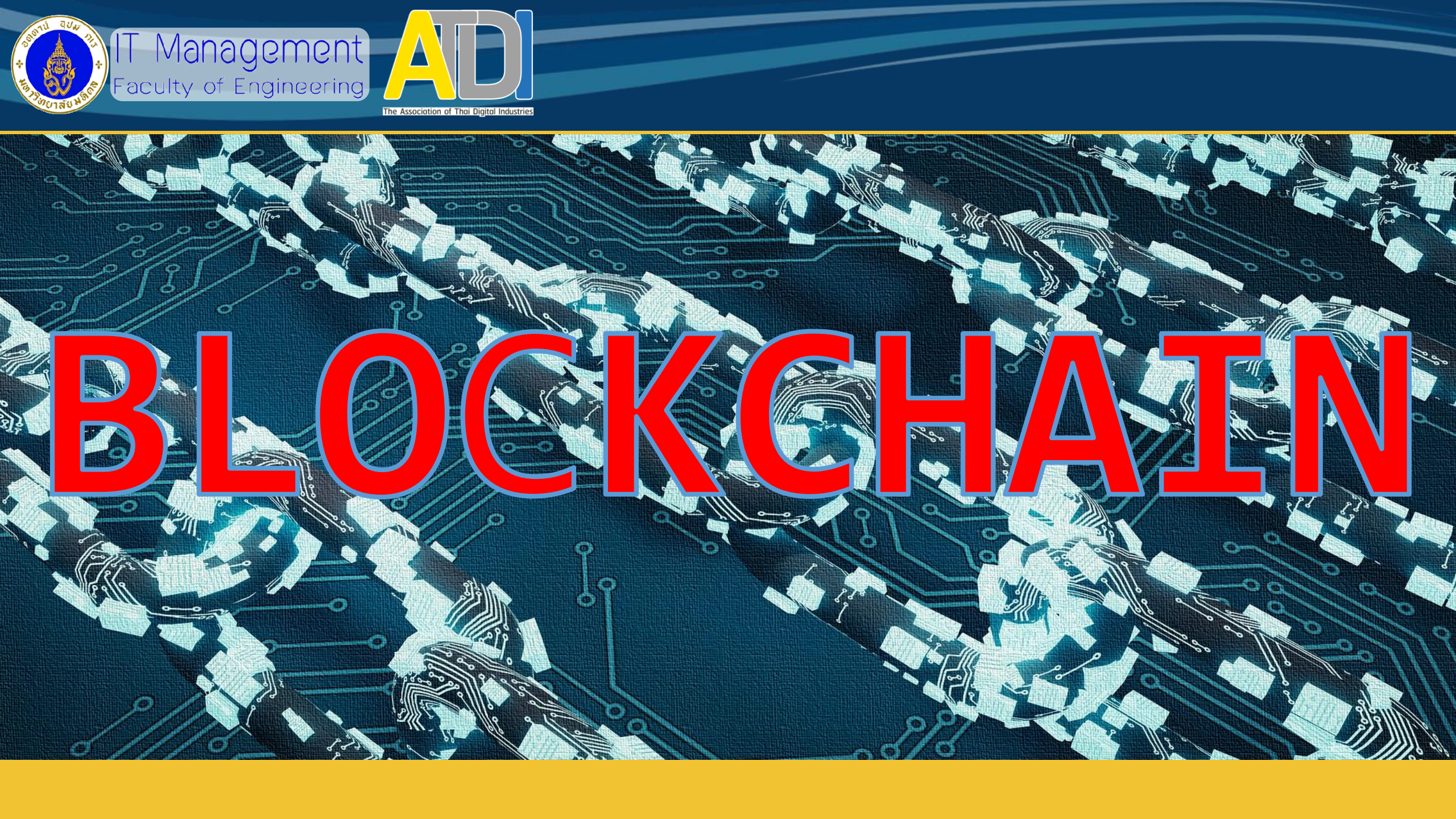

IT Management
Faculty of Engineering
ATDI
The Association of Thai Digital Industries
BLOCKCHAIN

Requirement

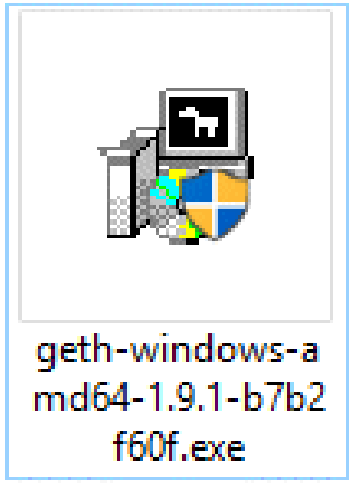
1. Geth (go Ethereum)
2. Node.js
3. Git
4. vscode
5. node-gyp
6. browserify
7. http-server
8. windows-build-tools
9. web3
10. ipfs
11. buffer

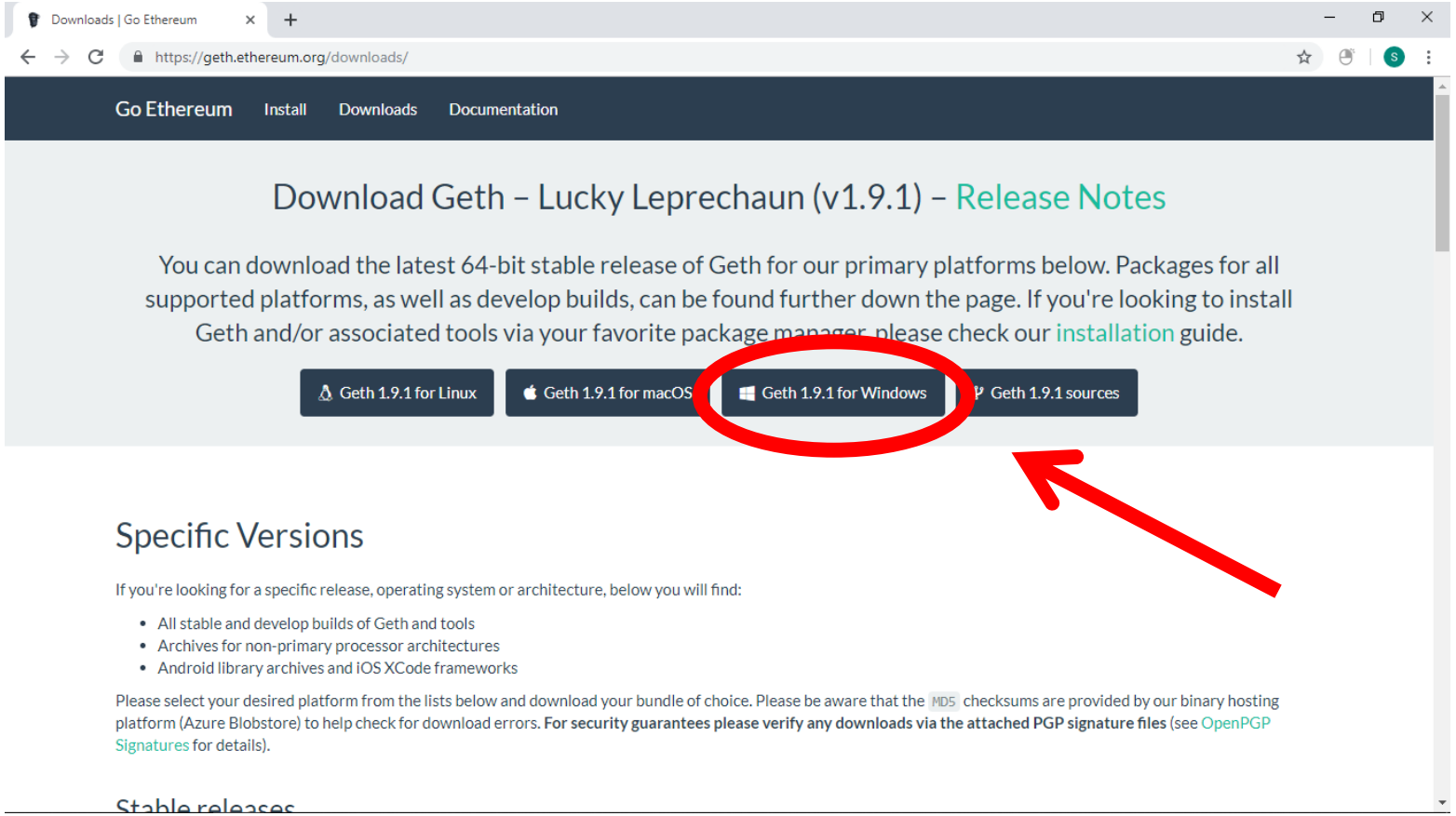
Geth

1. Download **geth** from

https://geth.ethereum.org/downloads/

2. Click installation file

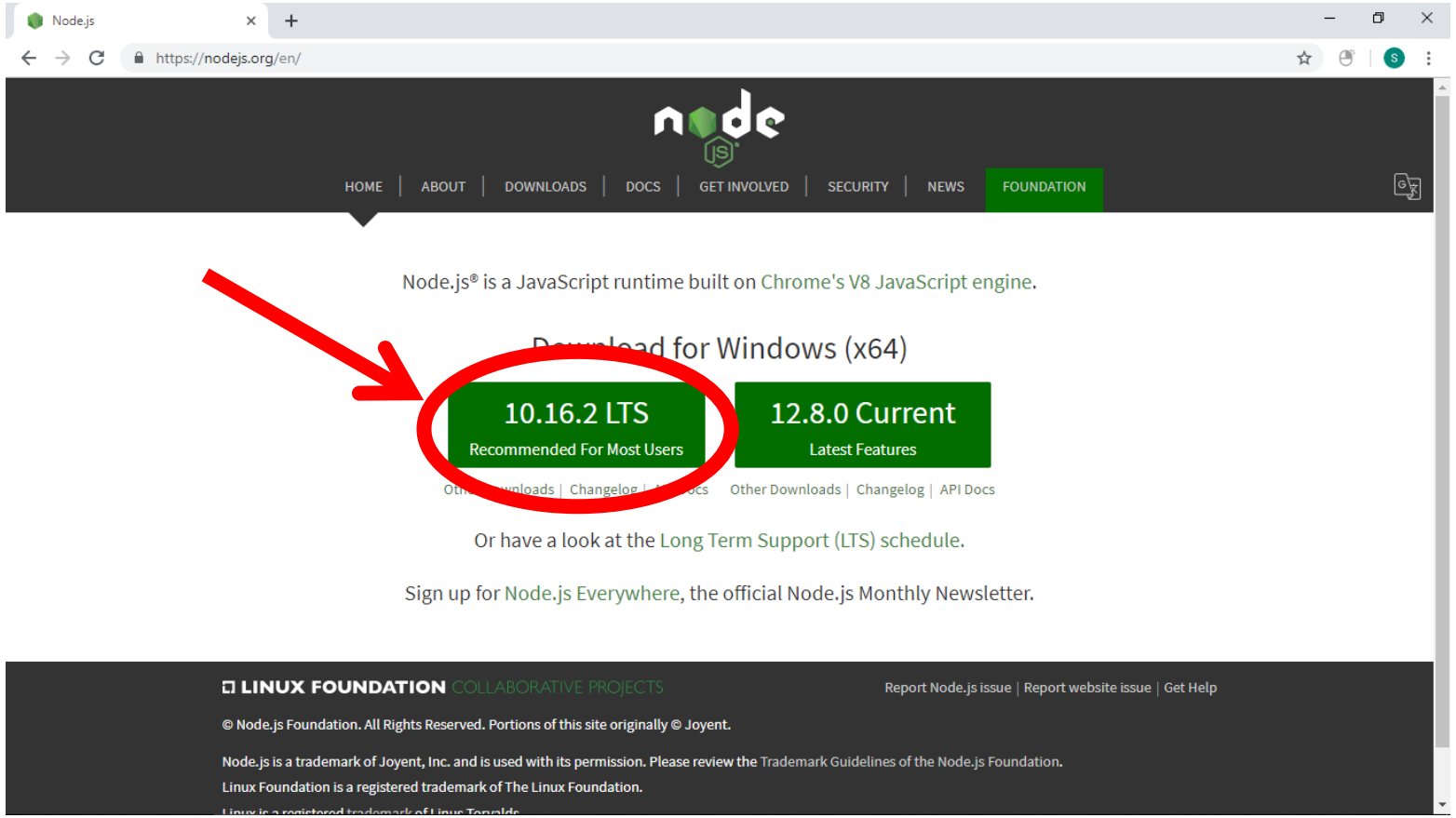




Nodejs

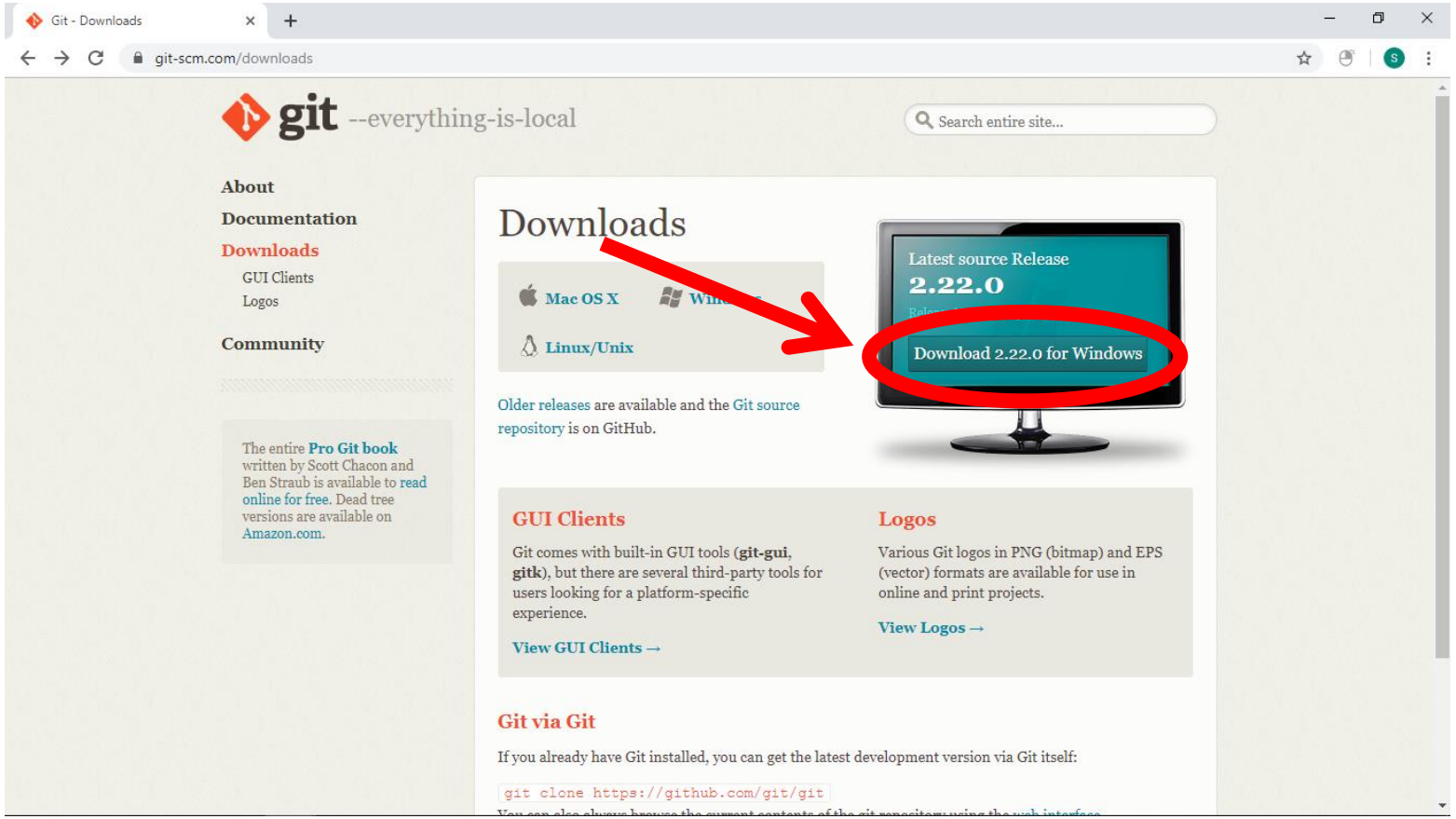
1. Download **Nodejs** from https://nodejs.org/en/

2. Click installation file



Git

1. Download **Git** from https://git-scm.com/downloads
2. Click installation file



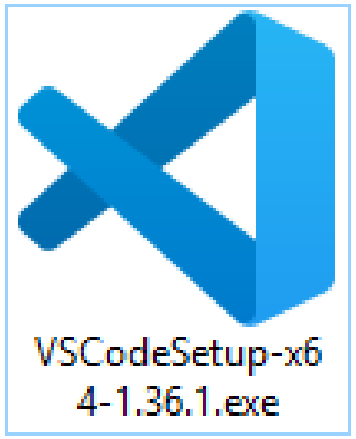
Virtual Studio Code

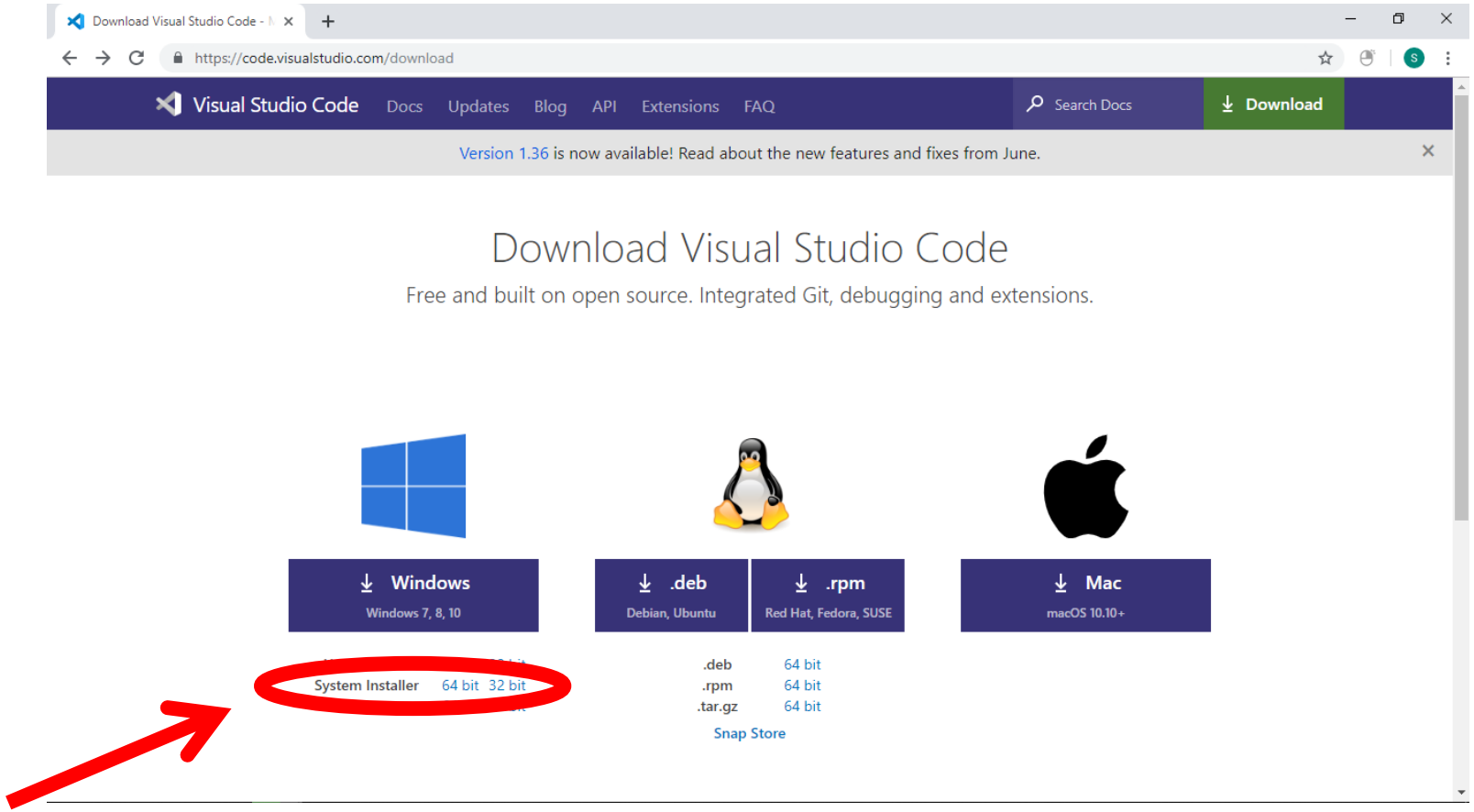
1. Download **vscode** from

https://code.visualstudio.com/download

1.1 select **System Installer**

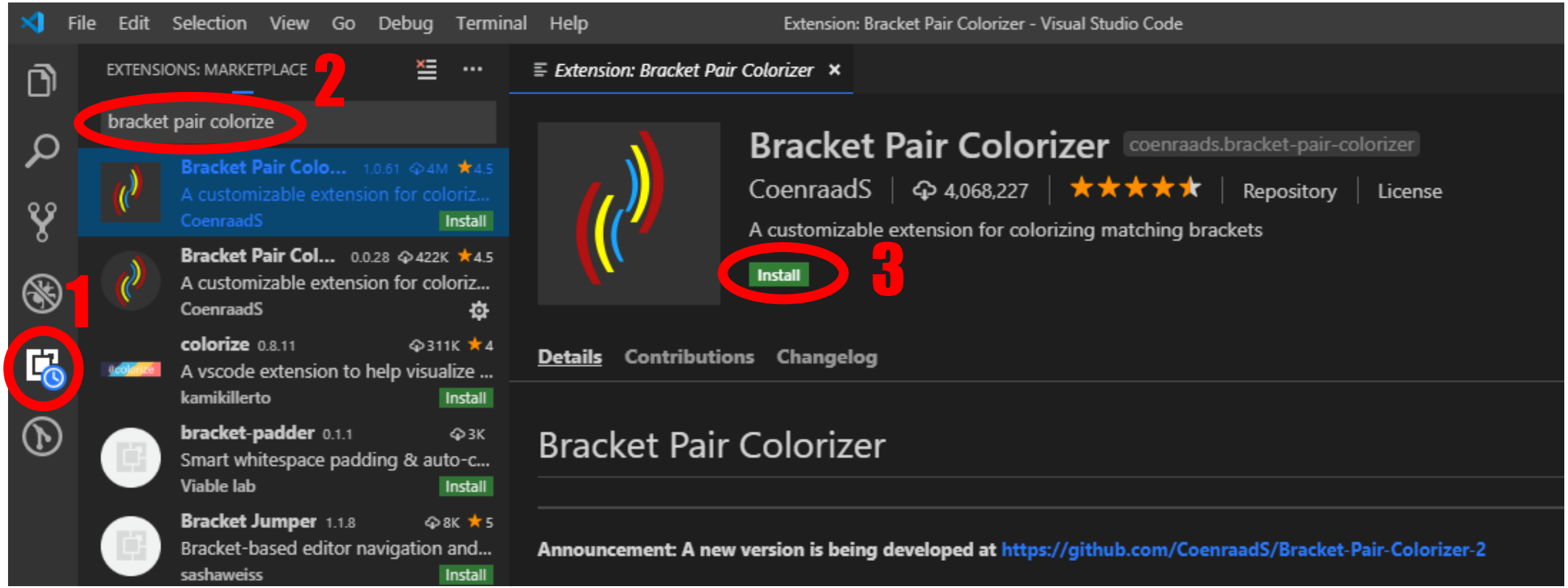
2. Click installation file





Setting vscode

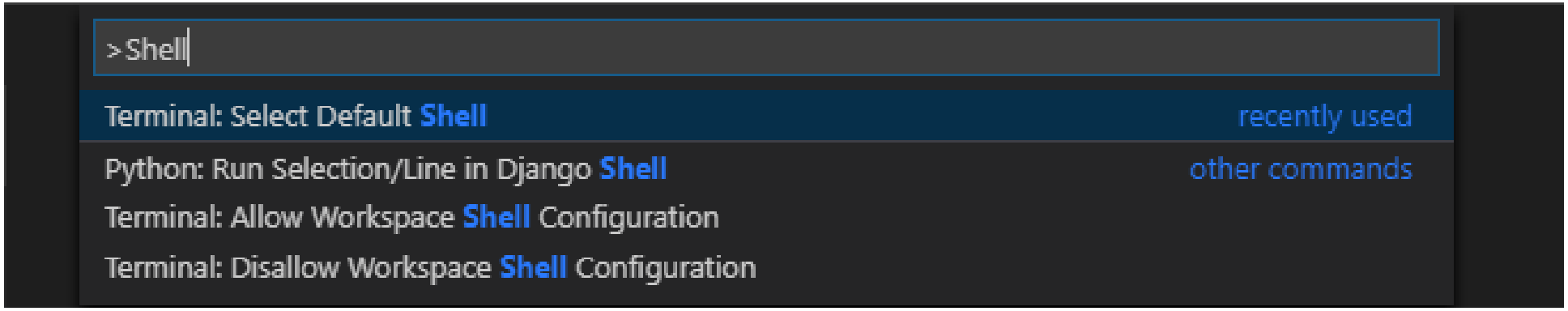
1. Download Bracket Pair Colorize Extension



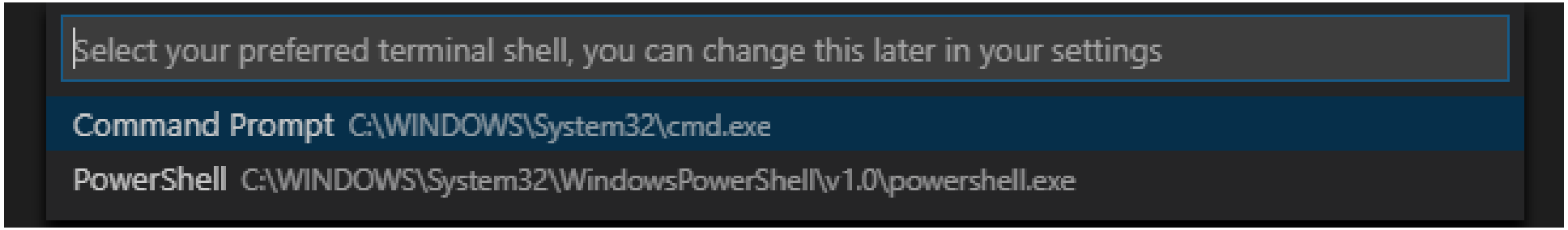
Setting vscode

2. Set default shell

    1. press **F1** or **Ctrl+Shift+P** and typing/selecting **Terminal Select Default Shell**

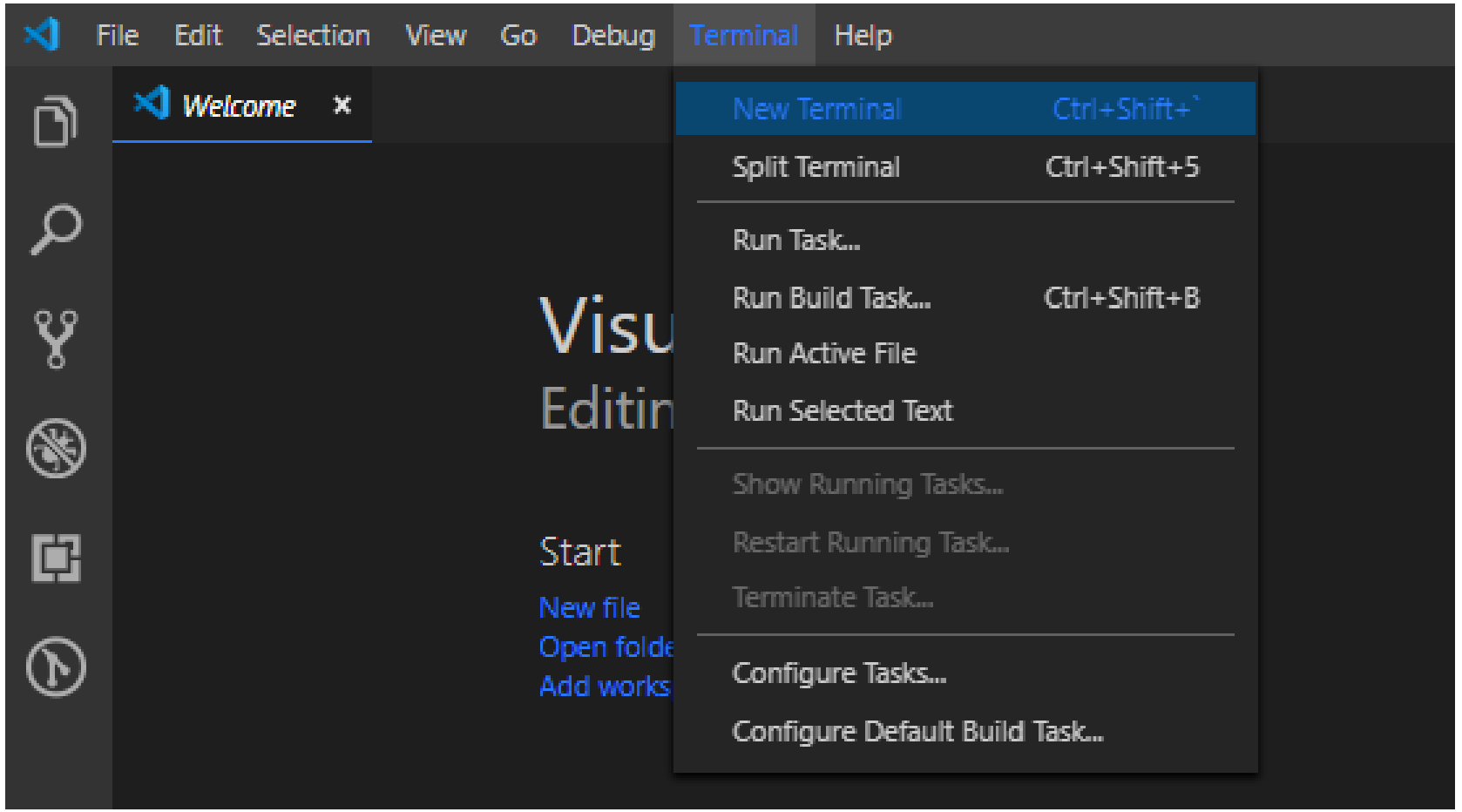


    2. Select **Command Prompt**



install node-gyp

1. Open Terminal



install node-gyp

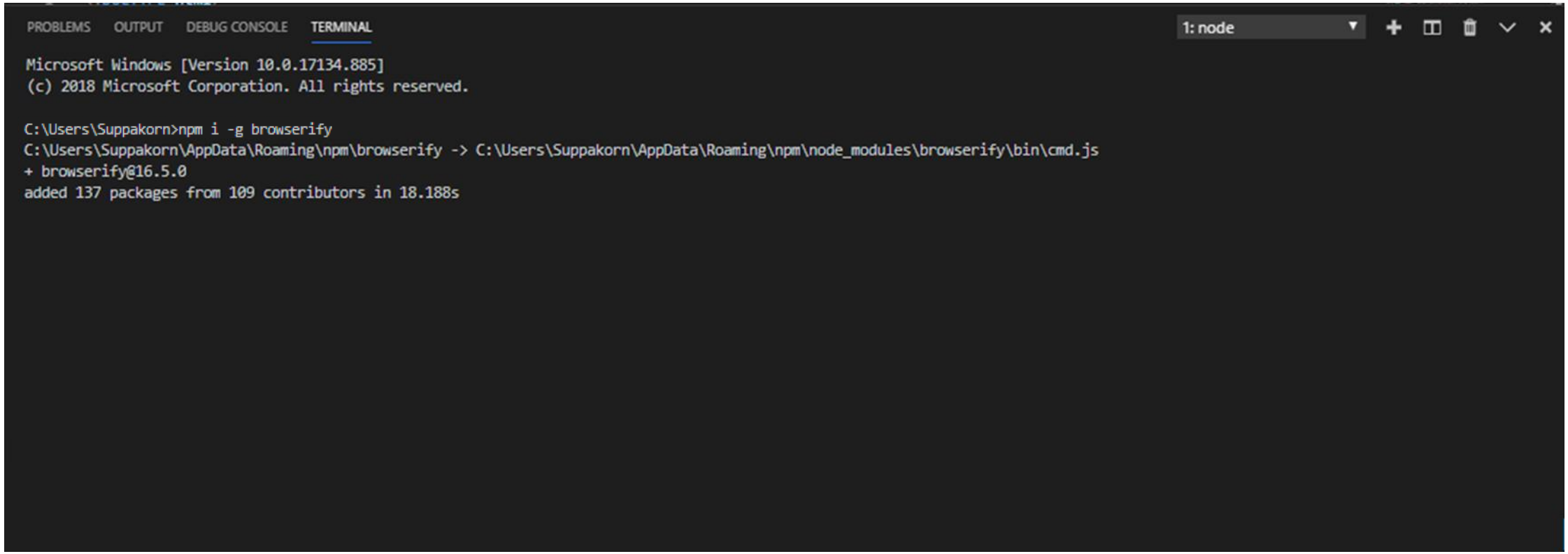
2. Run command

C:\User> npm i -g node-gyp

install browserify

1. Run command

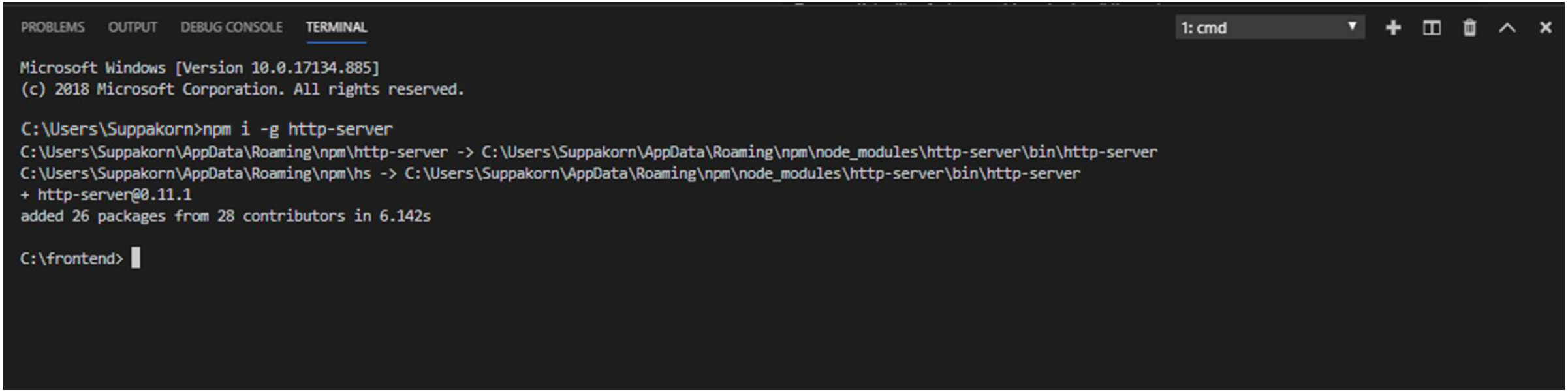
C:\User> npm i -g browserify



http-server

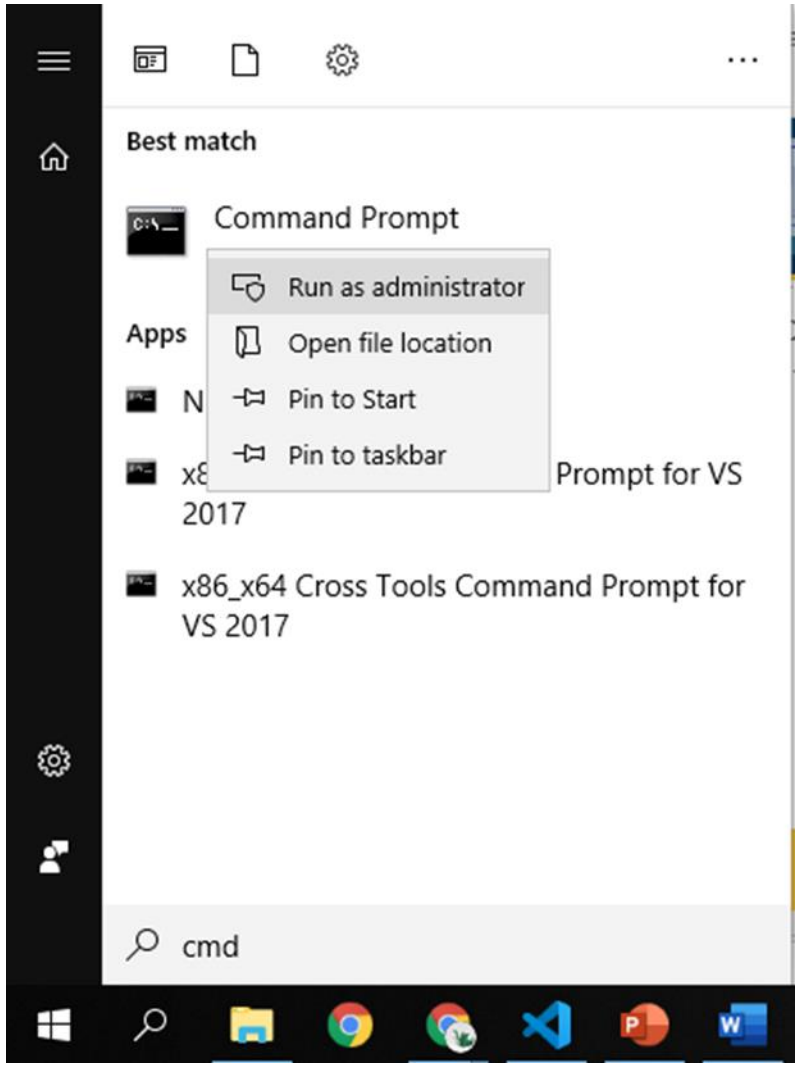
1. Run command

C:\User> npm i -g http-server



install windows-build-tools

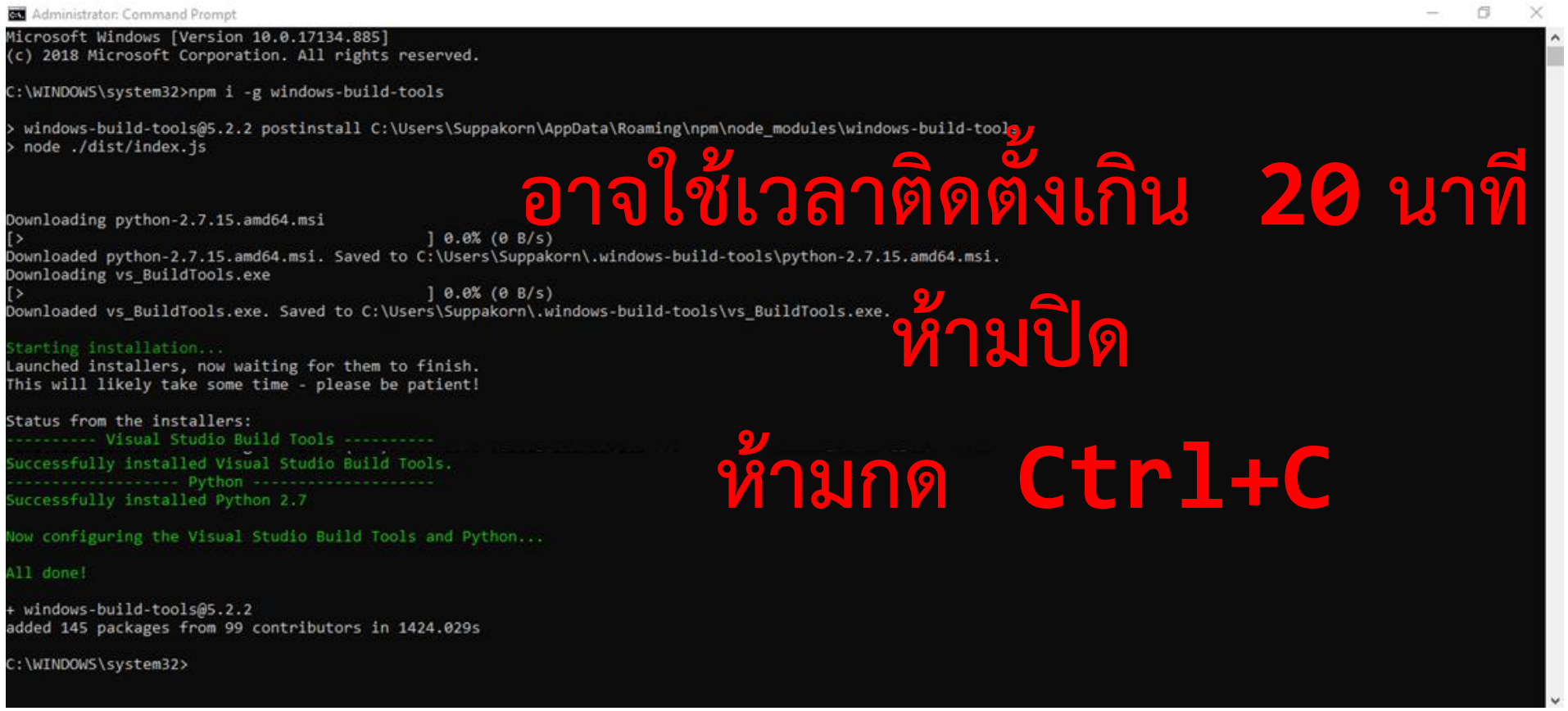
1. Open Command prompt as administrator



install windows-build-tools

2. Run command

C:\User>npm i -g windows-build-tools



workshop folder

1. make 2 folders

2. back to the Terminal
3. run command

C:\User> cd C:\frontend

```
C:\Users\Suppakorn>cd C:\frontend

C:\frontend>
```

install web3

1. run command

C:\frontend> npm init

```
C:\frontend>npm init
This utility will walk you through creating a package.json file.
It only covers the most common items, and tries to guess sensible defaults.

See `npm help json` for definitive documentation on these fields
and exactly what they do.

Use `npm install <pkg>` afterwards to install a package and
save it as a dependency in the package.json file.

Press ^C at any time to quit.
package name: (frontend)
version: (1.0.0)
description:
entry point: (index.js)
test command:
git repository:
keywords:
author:
license: (ISC)
About to write to C:\frontend\package.json:

{
  "name": "frontend",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC"
}


Is this OK? (yes)

C:\frontend>
```

install web3

2. Run command

C:\frontend>npm i web3

```
C:\frontend>npm i web3

> sha3@1.2.3 install C:\frontend\node_modules\sha3
> node-gyp rebuild


C:\frontend\node_modules\sha3>if not defined npm_config_node_gyp (node "C:\Program Files\nodejs\node_modules\npm\node_modules\npm-lifecycle\node-gyp-bin\\..\..\node_modules\node-gyp\bin\n
(node "C:\Program Files\nodejs\node_modules\npm\node_modules\node-gyp\bin\node-gyp.js" rebuild )
Building the projects in this solution one at a time. To enable parallel build, please add the "/m" switch.
  addon.cpp
  displayIntermediateValues.cpp
  KeccakF-1600-reference.cpp
  KeccakNISTInterface.cpp
  KeccakSponge.cpp
  win_delay_load_hook.cc
 c:\frontend\node_modules\websocket\src\validation.cc(133): warning C4996: 'v8::Value::ToObject': was declared deprecated [C:\frontend\node_modules\websocket\build\validation.vcxproj]
   c:\users\suppakorn\.node-gyp\10.16.2\include\node\v8.h(10046): note: see declaration of 'v8::Value::ToObject'
      Creating library C:\frontend\node_modules\websocket\build\Release\validation.lib and object C:\frontend\node_modules\websocket\build\Release\validation.exp
   Generating code
   All 121 functions were compiled because no usable IPDB/IOBJ from previous compilation was found.
   Finished generating code
   validation.vcxproj -> C:\frontend\node_modules\websocket\build\Release\\validation.node
 npm notice created a lockfile as package-lock.json. You should commit this file.
 npm WARN frontend@1.0.0 No description
 npm WARN frontend@1.0.0 No repository field.
 npm WARN optional SKIPPING OPTIONAL DEPENDENCY: fsevents@1.2.9 (node_modules\fsevents):
 npm WARN notsup SKIPPING OPTIONAL DEPENDENCY: Unsupported platform for fsevents@1.2.9: wanted {"os":"darwin","arch":"any"} (current: {"os":"win32","arch":"x64"})

 + web3@1.2.1
 added 623 packages from 406 contributors and audited 117991 packages in 122.727s
 found 1 low severity vulnerability
   run `npm audit fix` to fix them, or `npm audit` for details

 C:\frontend>
```

install IPFS

1. Run command

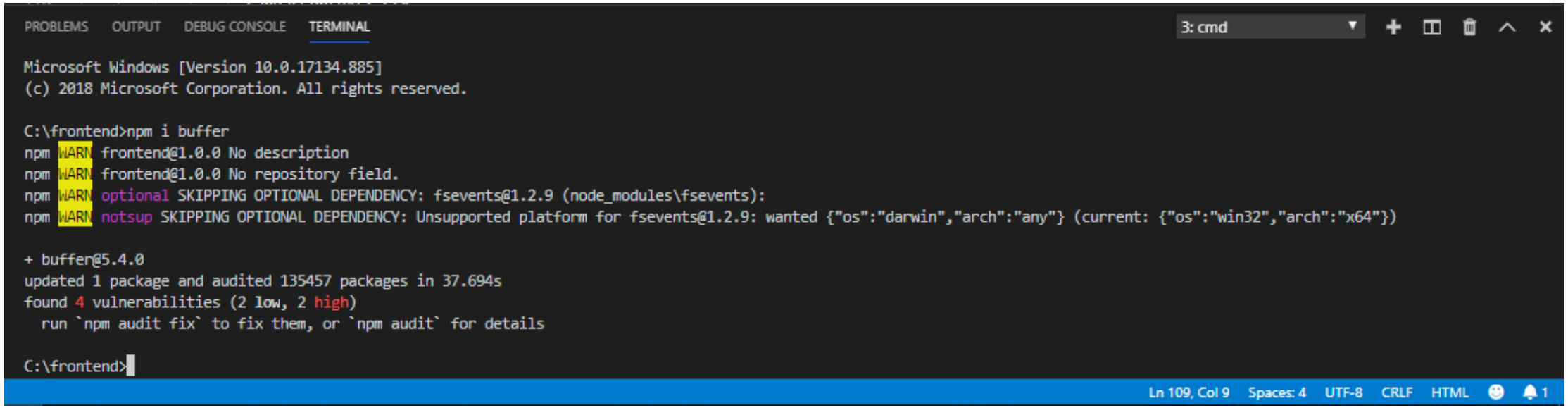
C:\frontend>npm i ipfs

```
C:\frontend>npm i ipfs

> gc-stats@1.4.0 install C:\frontend\node_modules\gc-stats
> node-pre-gyp install --fallback-to-build

node-pre-gyp WARN Using request for node-pre-gyp https download
[gc-stats] Success: "C:\frontend\node_modules\gc-stats\build\gcstats\v1.4.0\Release\node-v64-win32-x64\gcstats.node" is installed via remote

> keccak@1.4.0 install C:\frontend\node_modules\keccak
> npm run rebuild || echo "Keccak bindings compilation fail. Pure JS implementation will be used."


> keccak@1.4.0 rebuild C:\frontend\node_modules\keccak
> node-gyp rebuild

> assemblyscript@0.6.0 postinstall C:\frontend\node_modules\assemblyscript
> opencollective-postinstall || exit 0

Thank you for using assemblyscript!
If you rely on this package, please consider supporting our open collective:
> https://opencollective.com/assemblyscript/donate

npm WARN frontend@1.0.0 No description
npm WARN frontend@1.0.0 No repository field.
npm WARN optional SKIPPING OPTIONAL DEPENDENCY: fsevents@1.2.9 (node_modules\fsevents):
npm WARN notsup SKIPPING OPTIONAL DEPENDENCY: Unsupported platform for fsevents@1.2.9: wanted {"os":"darwin","arch":"any"} (current: {"os":"win32","arch":"x64"})

+ ipfs@0.37.0
added 782 packages from 683 contributors and audited 135454 packages in 237.214s
found 4 vulnerabilities (2 low, 2 high)
  run `npm audit fix` to fix them, or `npm audit` for details

C:\frontend>
```

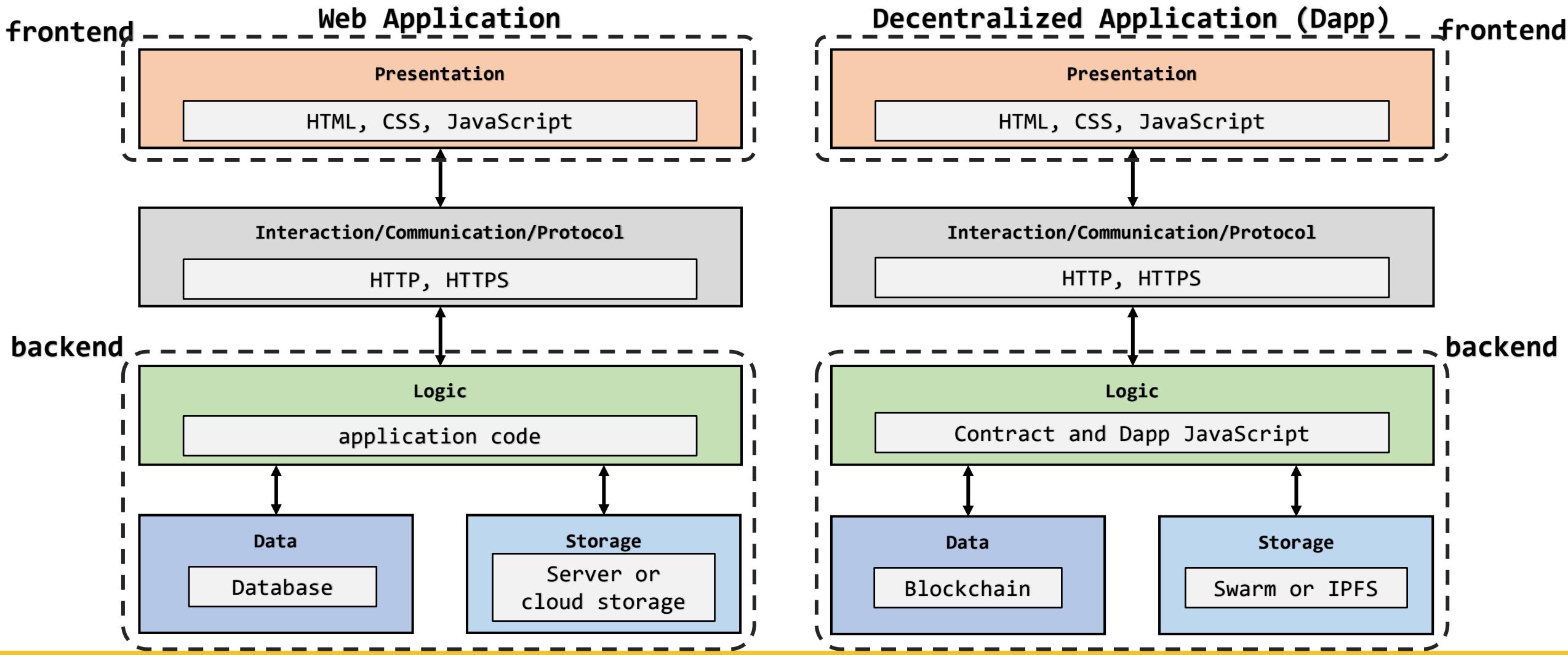
install buffer

1. Run command

C:\frontend>npm i buffer

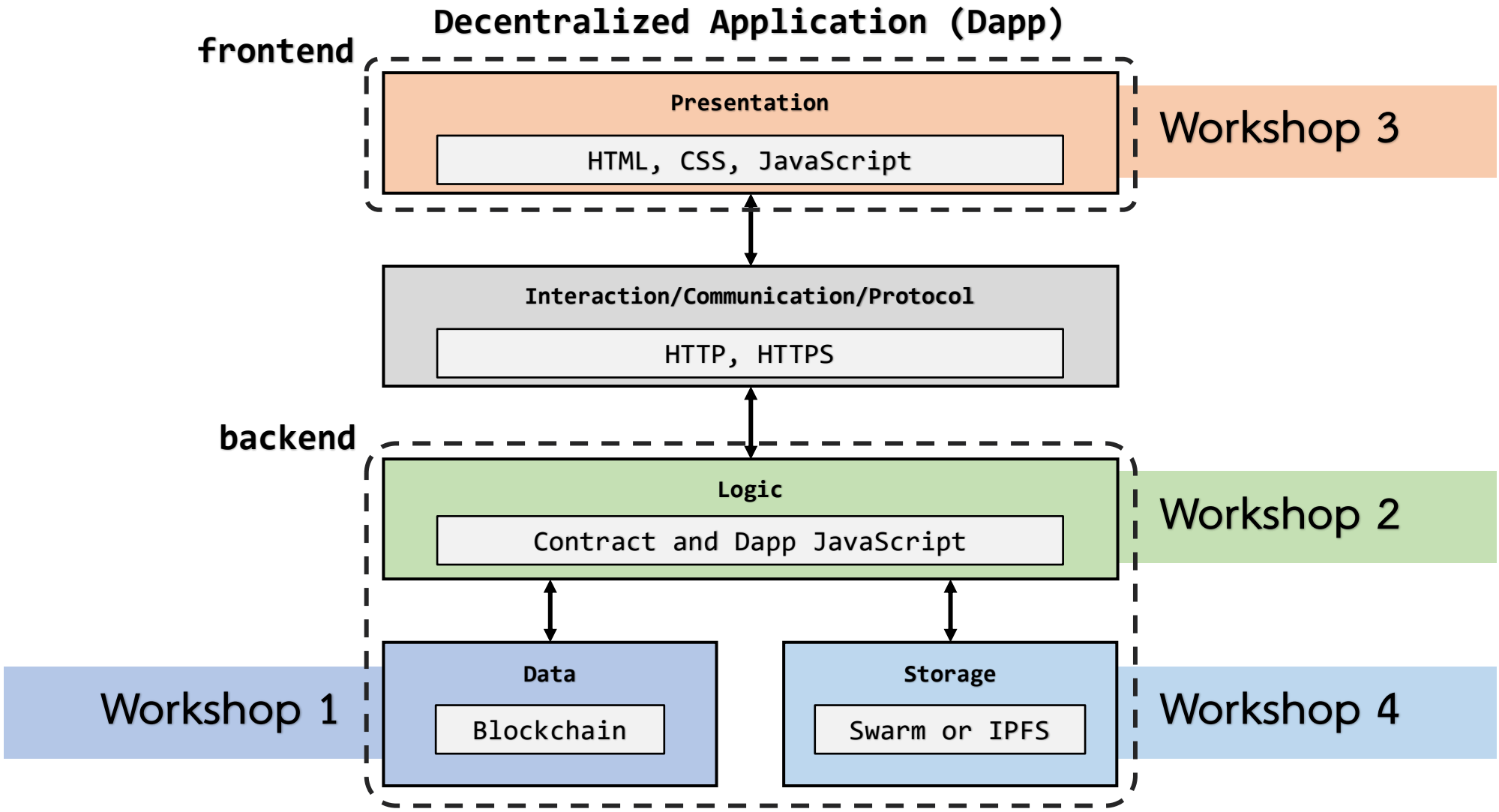


Overview



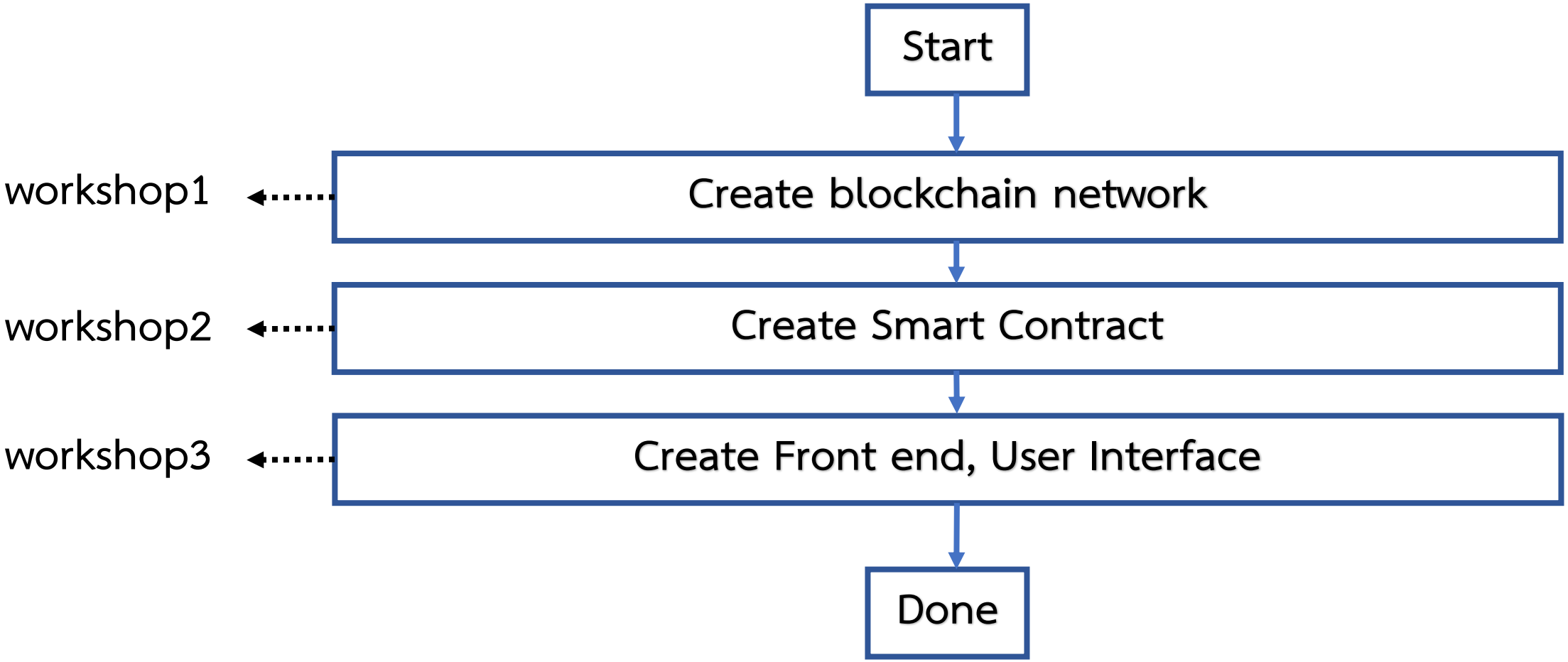
https://file.scirp.org/pdf/JSEA_2016102814012798.pdf

Overview



https://file.scirp.org/pdf/JSEA_20161028140127798.pdf

Course Outline

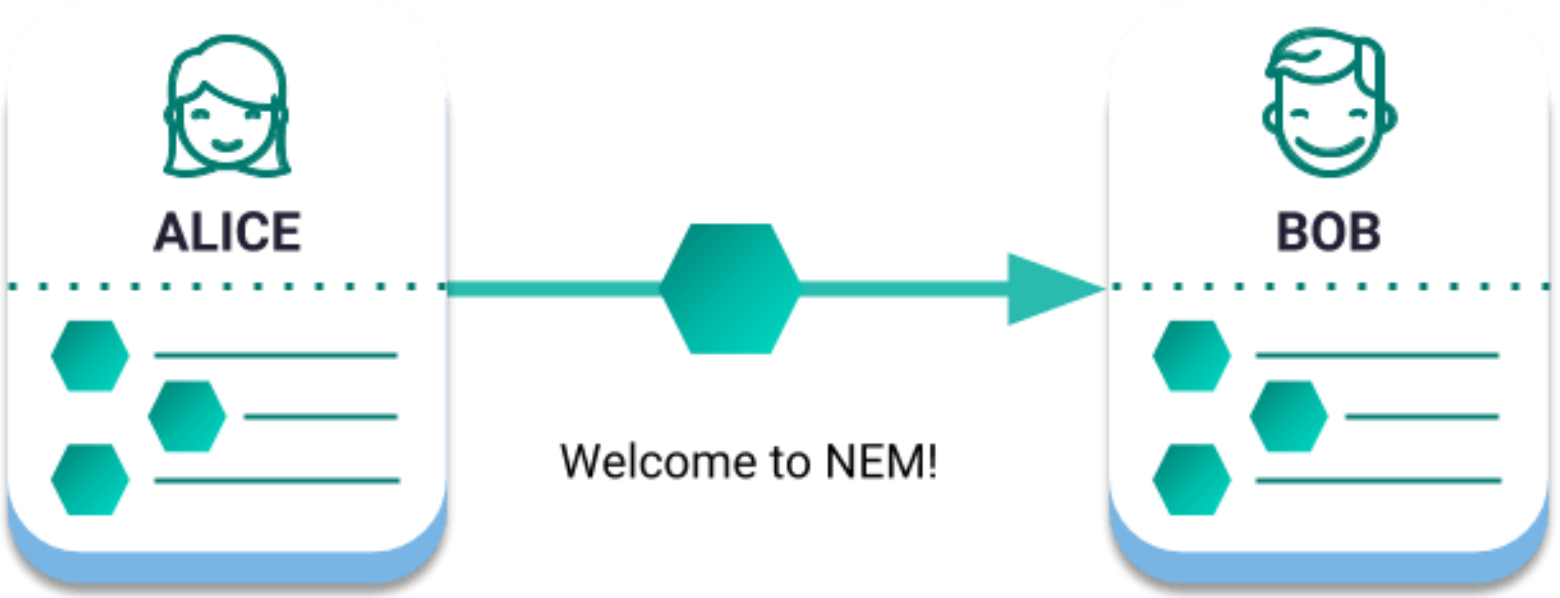


Topology

Transaction

Blockchain transaction can be defined as a small unit of task that is stored in public records.

- send transaction (โอนเหรียญ)
- send data
- query data
- edit data
- deploy smart contract



https://ethereum.github.io/yellowpaper/paper.pdf
https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

Block

Block header

1.the hash of this block

2.the hash of the previous block

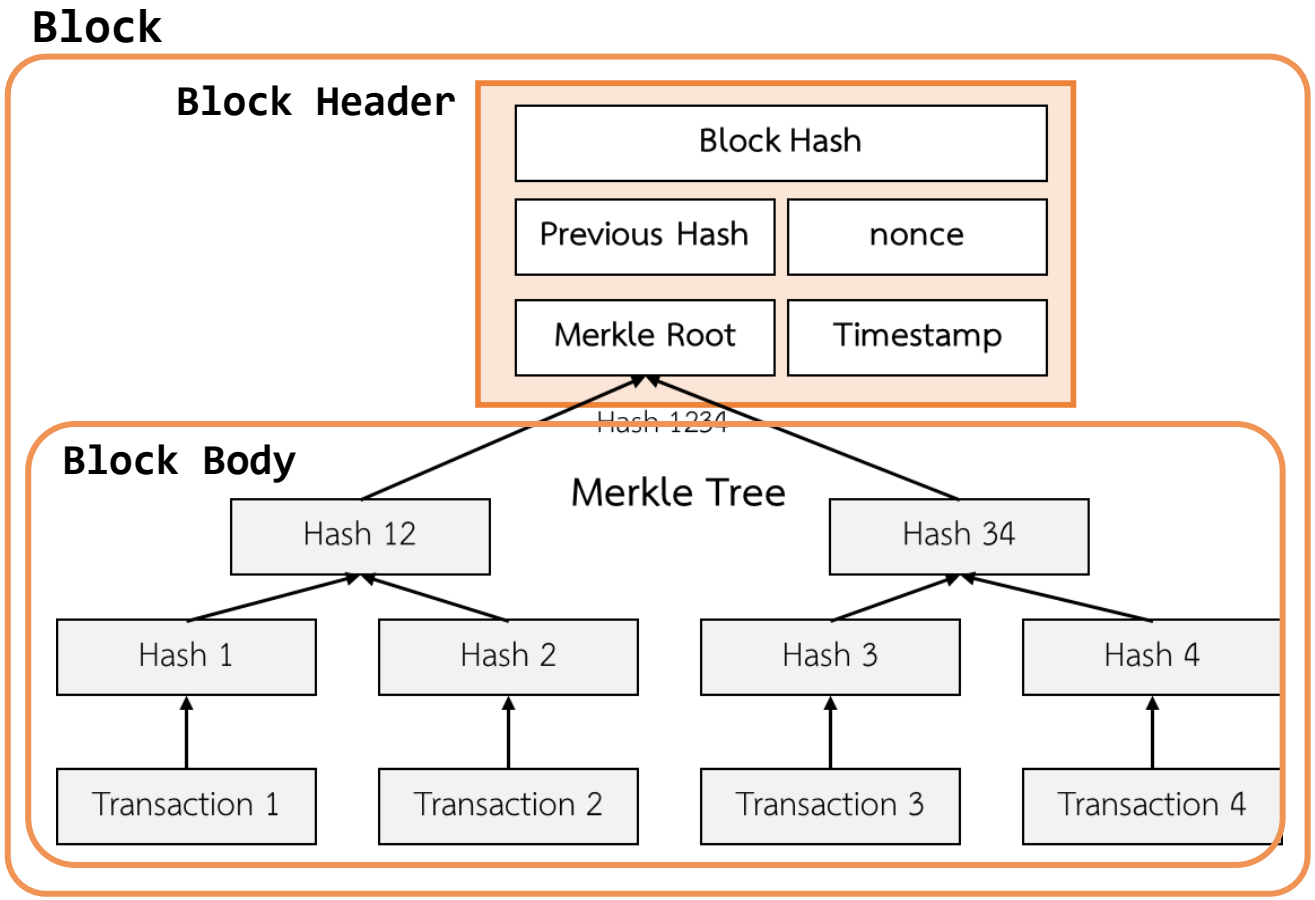
3.the root hash of the Merkle tree (Merkle Root)

4.the time in seconds since 1970–01–01 T00: 00 UTC

5.the nonce

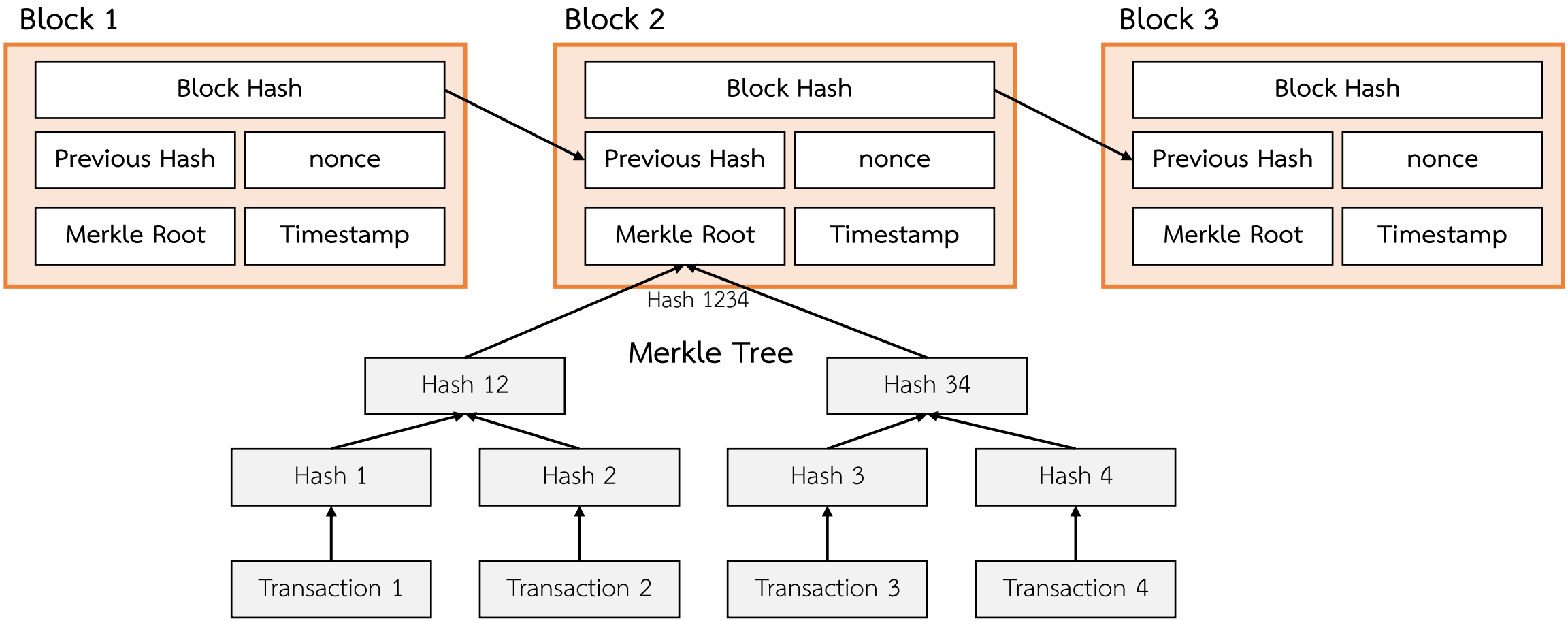
Block Body

The block body is conceivable as the loading space of a truck. It contains all transactions that are confirmed with the block. The transactions in a block are stored in Merkle Tree.



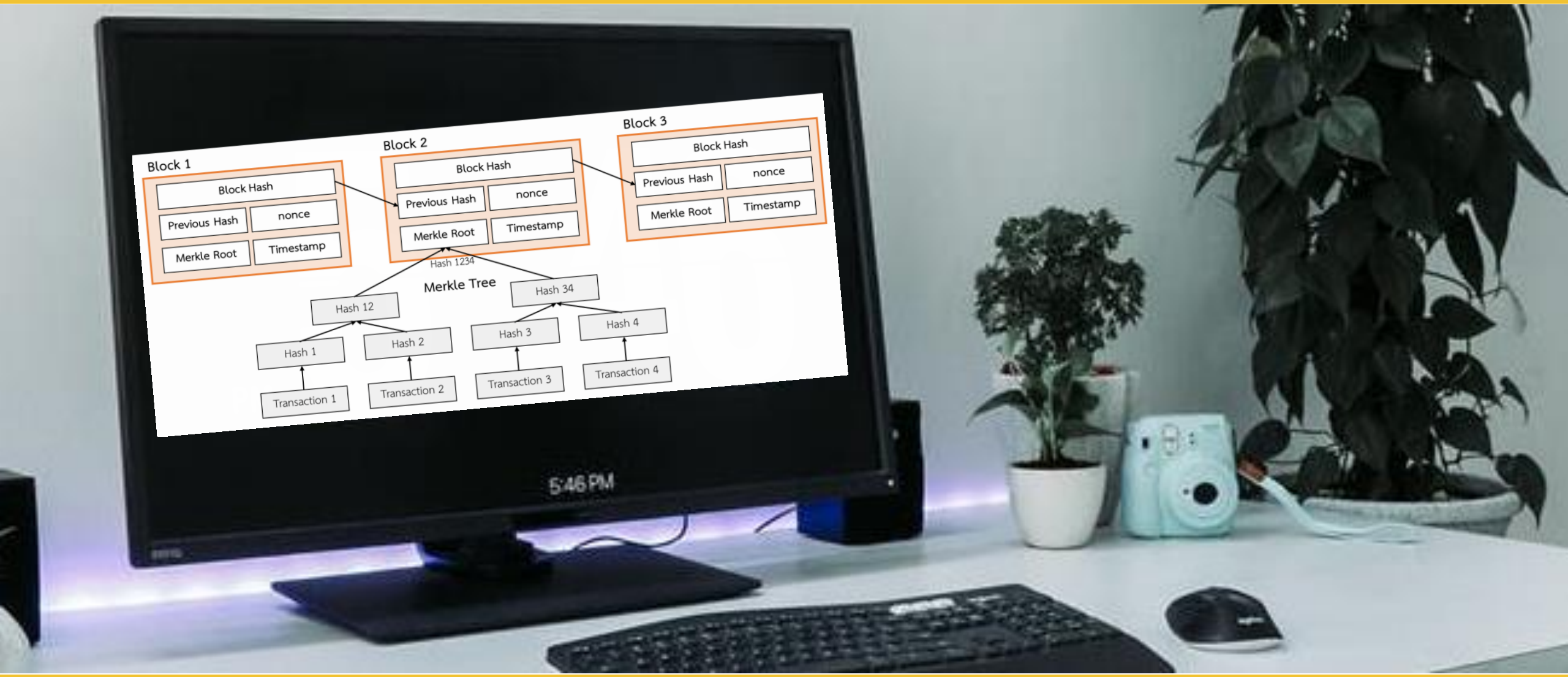
https://ethereum.github.io/yellowpaper/paper.pdf https://file.scirp.org/pdf/JSEA_20161028140127 98.pdf
https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

Blockchain

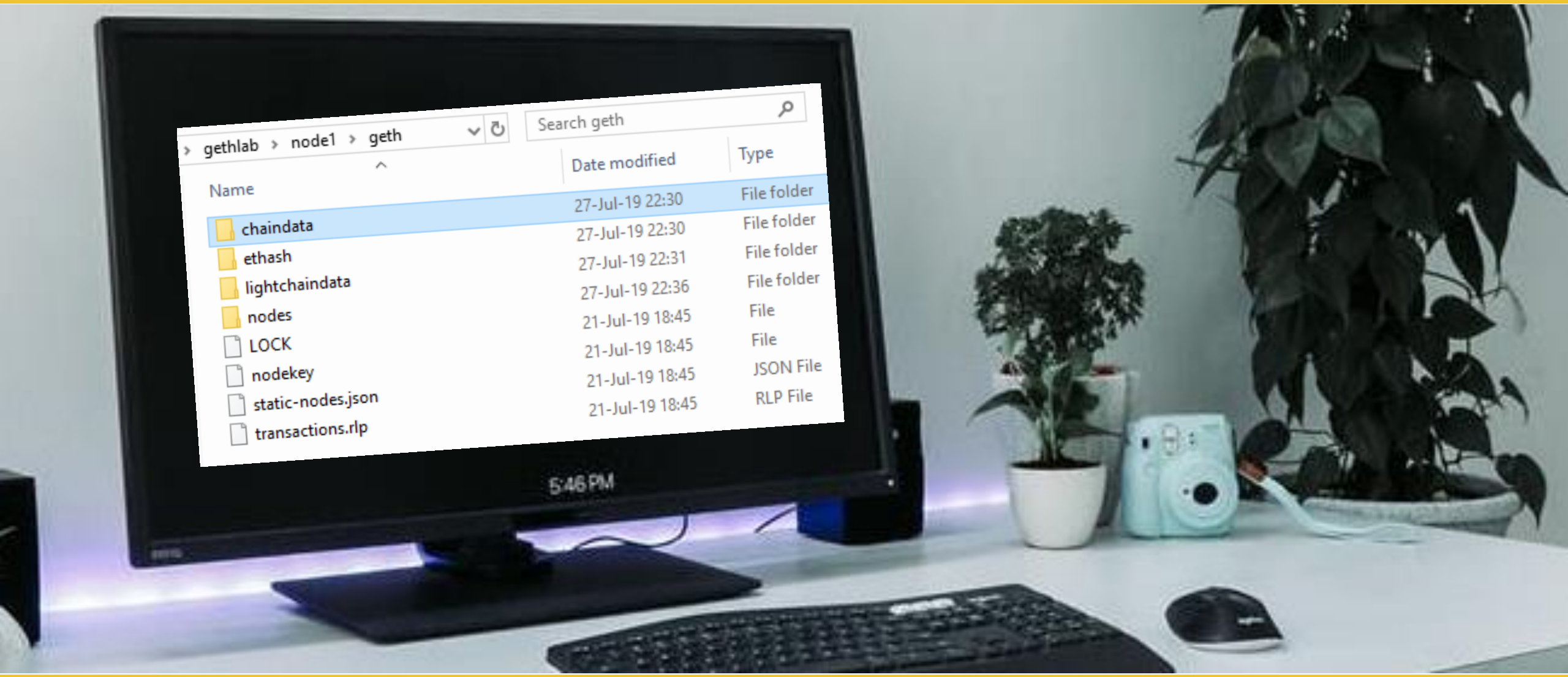


https://ethereum.github.io/yellowpaper/paper.pdf https://file.scirp.org/pdf/JSEA_20161028140127 98.pdf
https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

Node

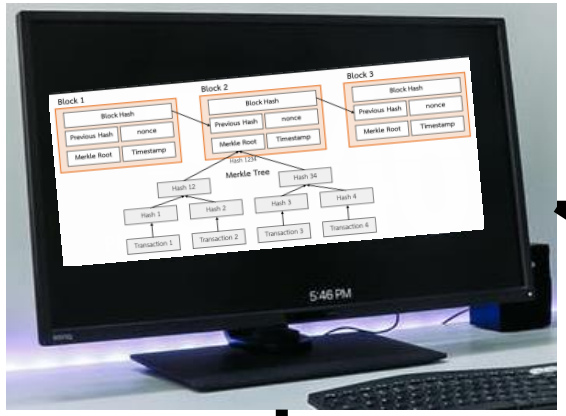

Block 1
Block Hash
Previous Hash
nonce
Merkle Root
Timestamp
Block 2
Block Hash
Previous Hash
nonce
Merkle Root
Timestamp
Block 3
Block Hash
Previous Hash
nonce
Merkle Root
Timestamp
Hash 1234
Merkle Tree
Hash 12
Hash 34
Hash 1
Hash 2
Hash 3
Hash 4
Transaction 1
Transaction 2
Transaction 3
Transaction 4
5:46 PM

Node

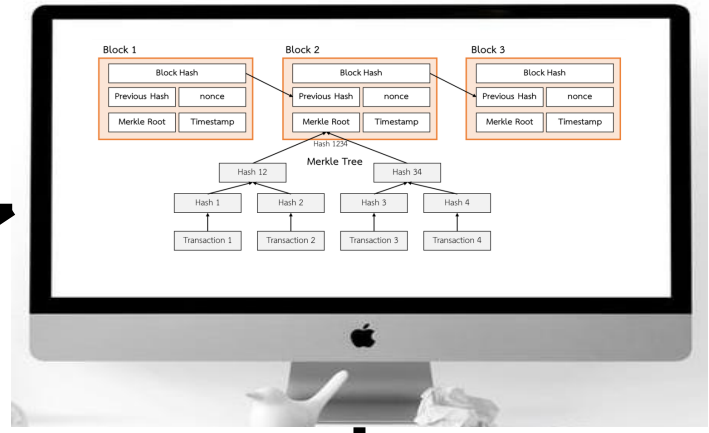

gethlab › node1 › geth
Search geth
Name
Date modified
Type
chaindata 27-Jul-19 22:30 File folder
ethash 27-Jul-19 22:30 File folder
lightchaindata 27-Jul-19 22:31 File folder
nodes 27-Jul-19 22:36 File folder
LOCK 21-Jul-19 18:45 File
nodekey 21-Jul-19 18:45 File
static-nodes.json 21-Jul-19 18:45 JSON File
transactions.rlp 21-Jul-19 18:45 RLP File
5:46 PM

Blockchain Network

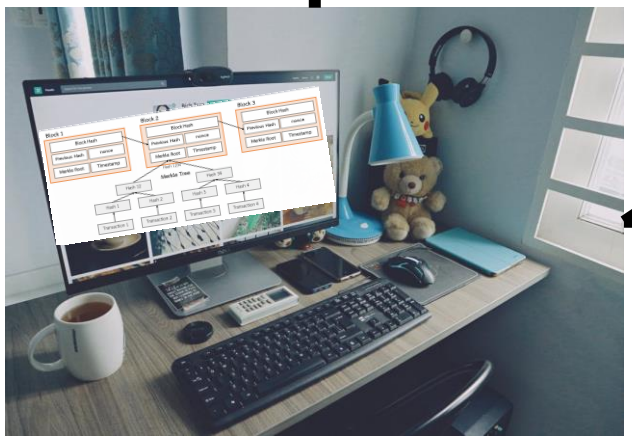
Node



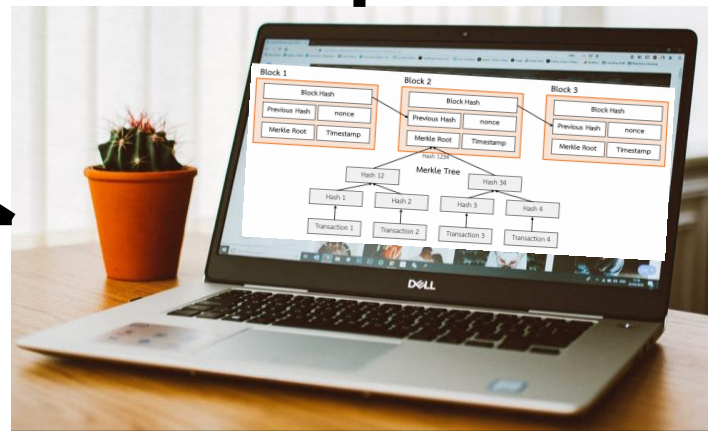
Node



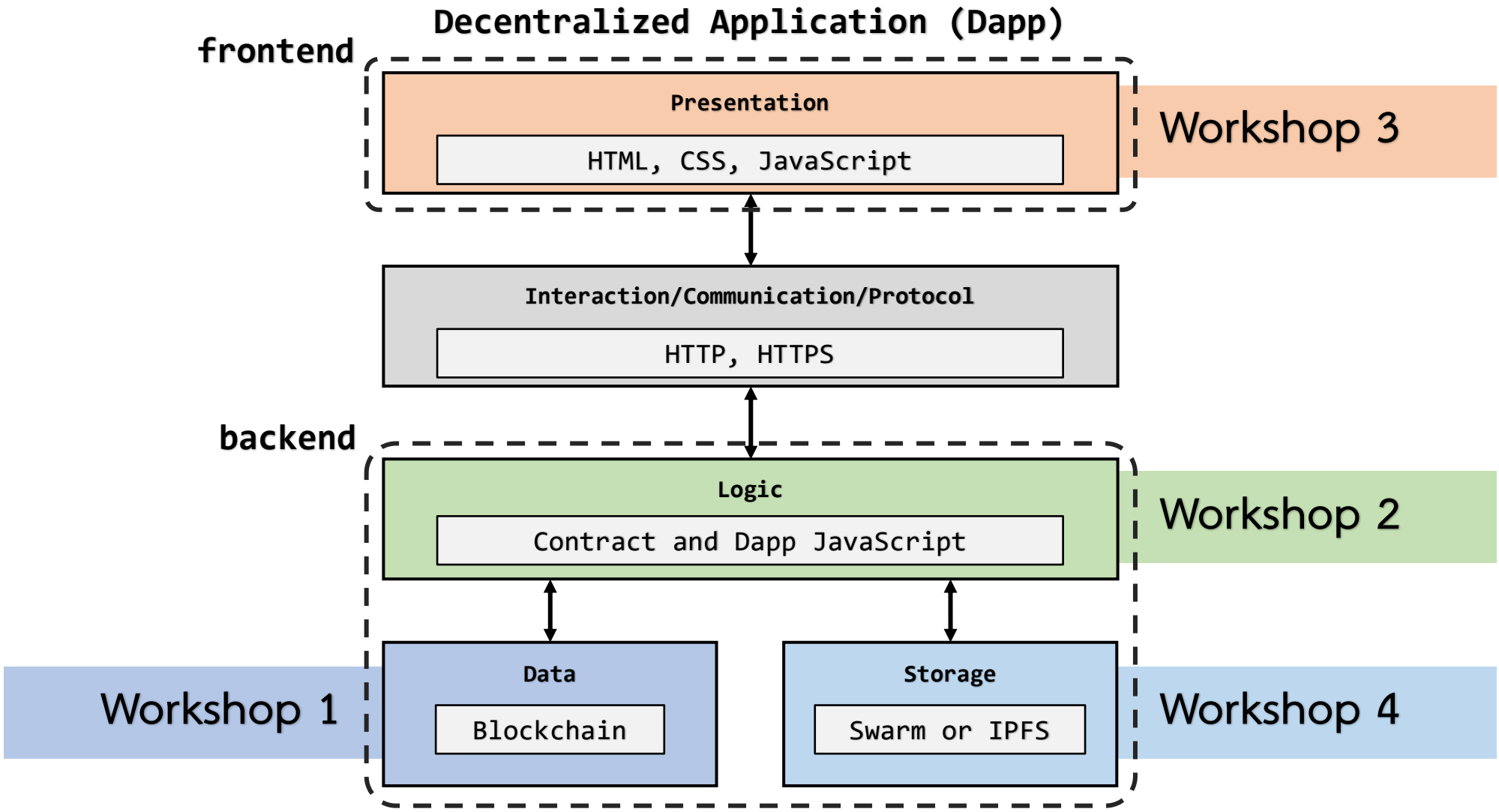
Node



Node



Overview



https://file.scirp.org/pdf/JSEA_20161028140127798.pdf

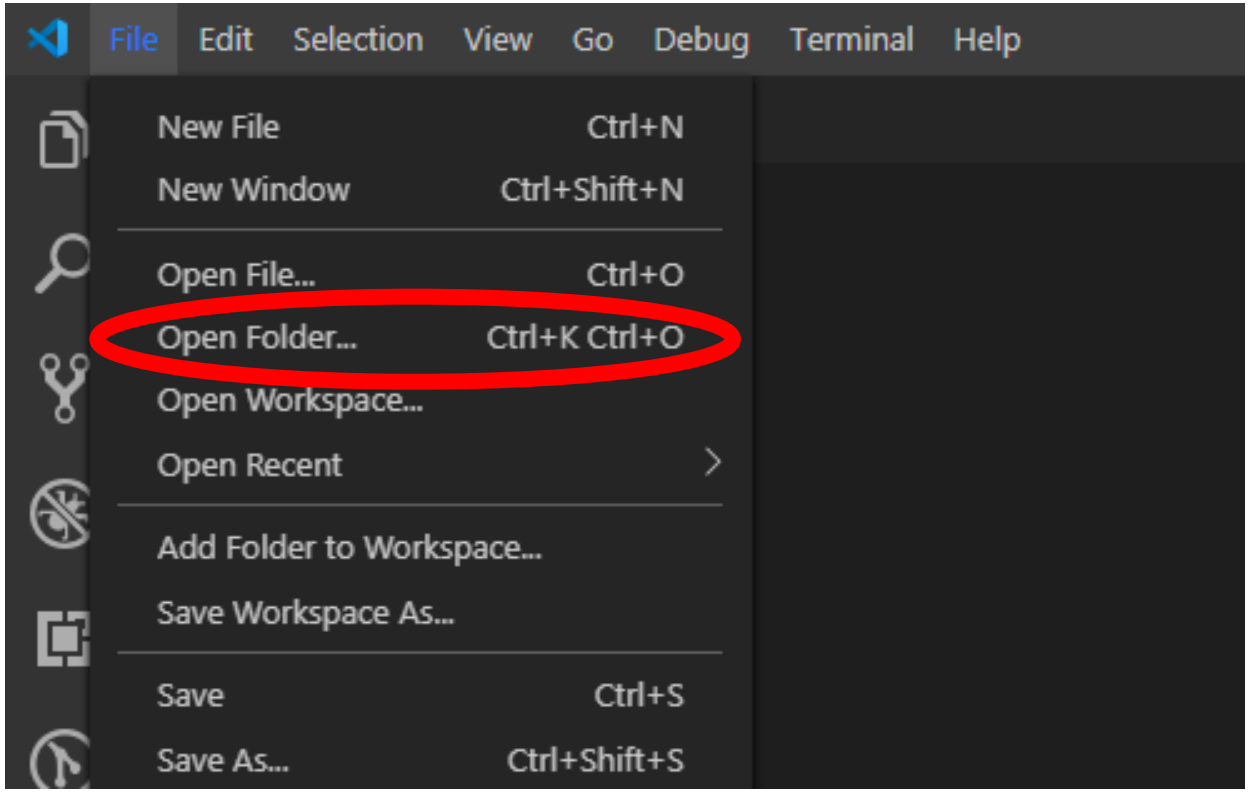
Workshop 1 Geth

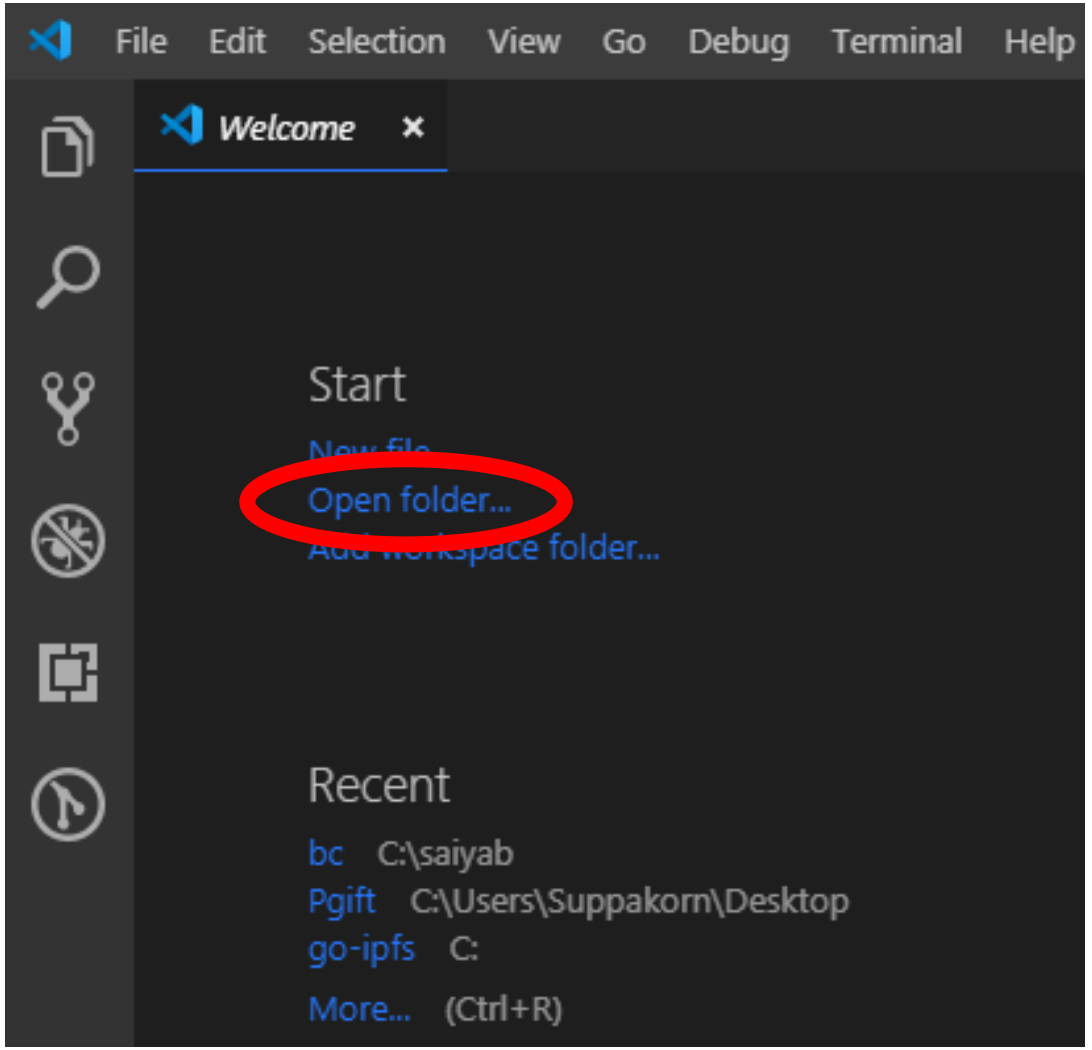
workshop นี้ทำอะไร

1. create new local blockchain network (1 node) on personal laptop using Geth (open source)
2. Blockchain ที่สร้างได้เป็น blockchain เปล่าๆ ไม่มีอะไรเลย
    - 2.1 เราจะมาเริ่มกันที่สร้างบัญชี 2 บัญชีภายใน 1 node โดยหมายเลขบัญชีจะเรียกว่า Wallet Address
    - 2.2 แล้วเราก็จะขุดเหรียญกัน เป็นเหรียญที่ไม่มีค่า แต่ผมอยากให้ทุกคนมองว่าเหรียญนี้คือข้อมูล
        - 2.2.1 ตอนขุดจะกินเวลาค่อนข้างนาน ผมจะใช้เวลาช่วงนี้อธิบายว่าการขุดคืออะไร และสัมพันธ์กับด้านsecurity ของblockchain ยังไง
3. พอมีบัญชี และมีเหรียญแล้ว เราก็จะมาโอนเหรียญ (ส่งข้อมูล) จากบัญชีที่หนึ่งไปยังบัญชีที่สอง
4. เราจะสร้าง node ขึ้นมาอีกหนึ่งอัน แล้วก็จะเอามันมาเชื่อมต่อกับโหนดแรก ก็จะได้ blockchain network(2 nodes)
5. แล้วเราจะโอนเหรียญ(ส่งข้อมูล)ข้ามโหนดกัน

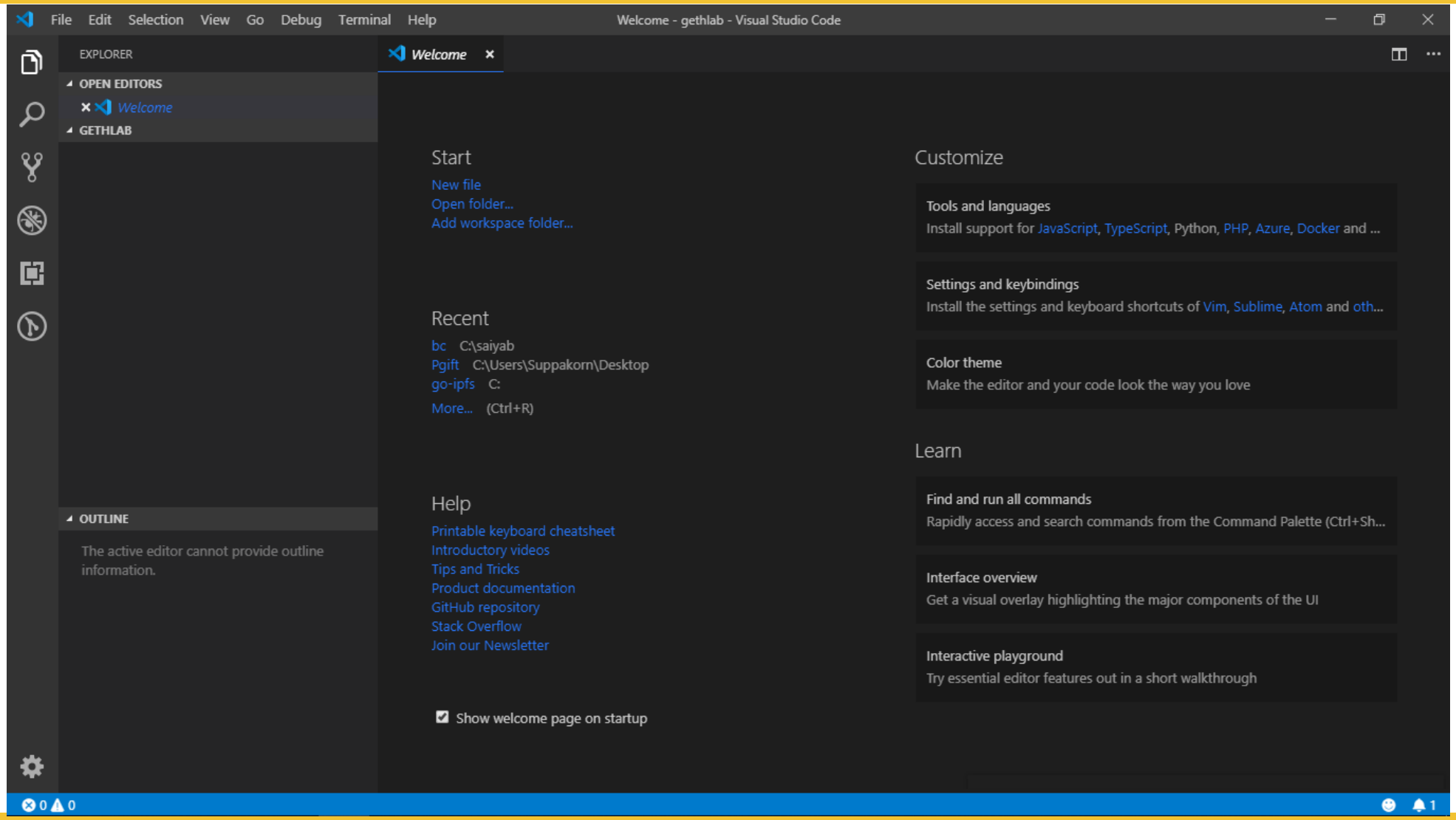
genesis.json

1. Open vscode > File > Open Folder > C:\gethlab





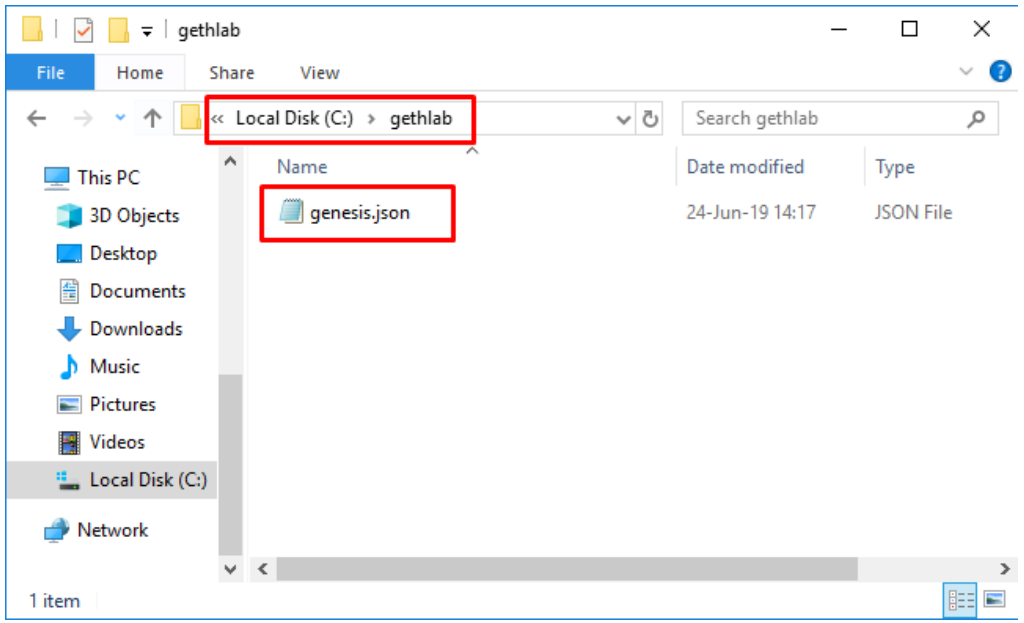
genesis.json



genesis.json

2. File > New File > paste code

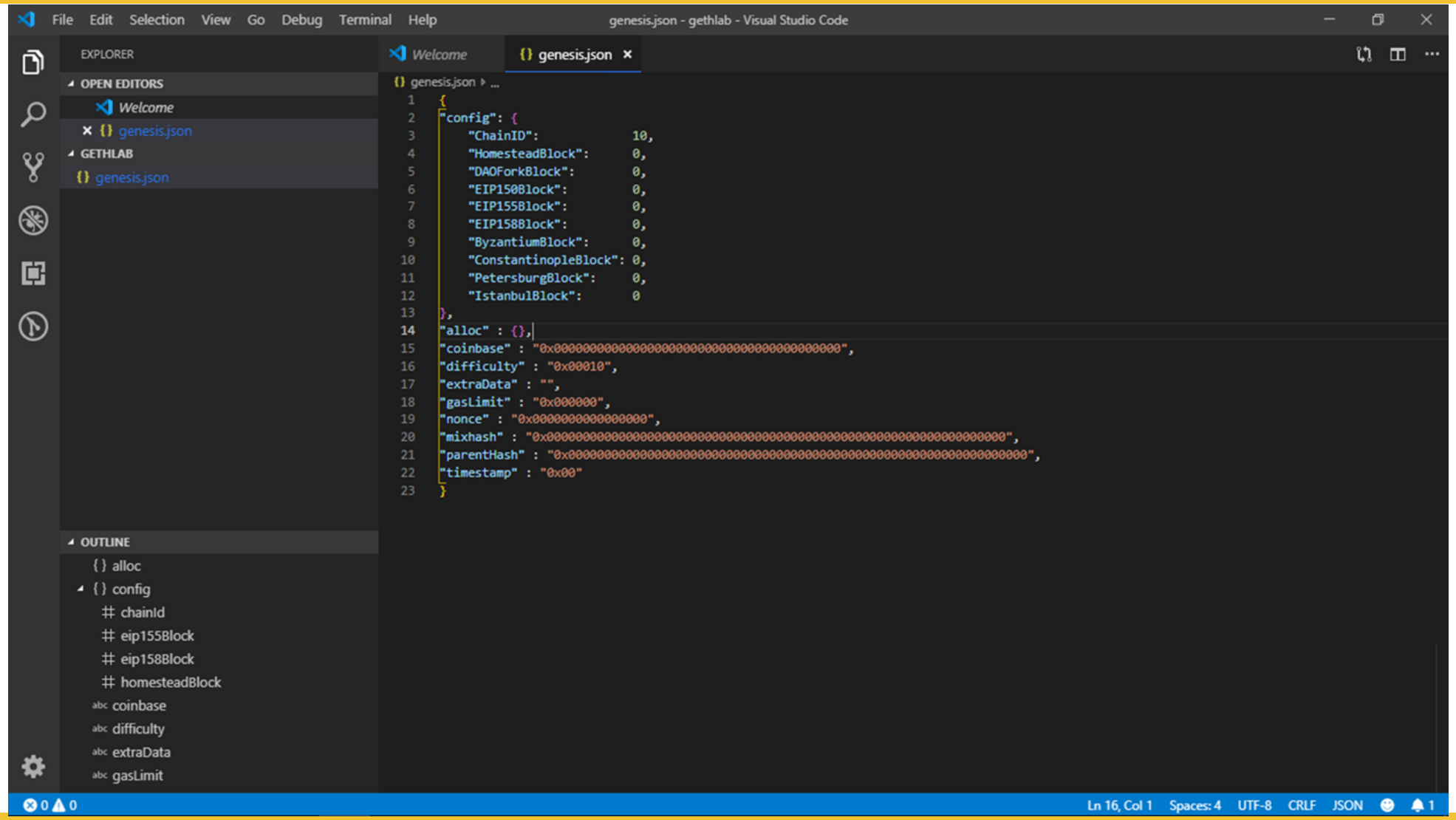
3. Save file as genesis.json in folder C:\gethlab




```
{
"config": {
    "ChainID":             10,
    "HomesteadBlock":      0,
    "DAOForkBlock":        0,
    "EIP150Block":         0,
    "EIP155Block":         0,
    "EIP158Block":         0,
    "ByzantiumBlock":      0,
    "ConstantinopleBlock": 0,
    "PetersburgBlock":     0,
    "IstanbulBlock":       0
},
"alloc" : {},
"coinbase" : "0x0000000000000000000000000000000000000000",
"difficulty" : "0x00010",
"extraData" : "",
"gasLimit" : "0x5F5E100",
"nonce" : "0x0000000000000000",
"mixhash" : "0x0000000000000000000000000000000000000000000000000000000000000000",
"parentHash" : "0x0000000000000000000000000000000000000000000000000000000000000000",
"timestamp" : "0x00"
}
```

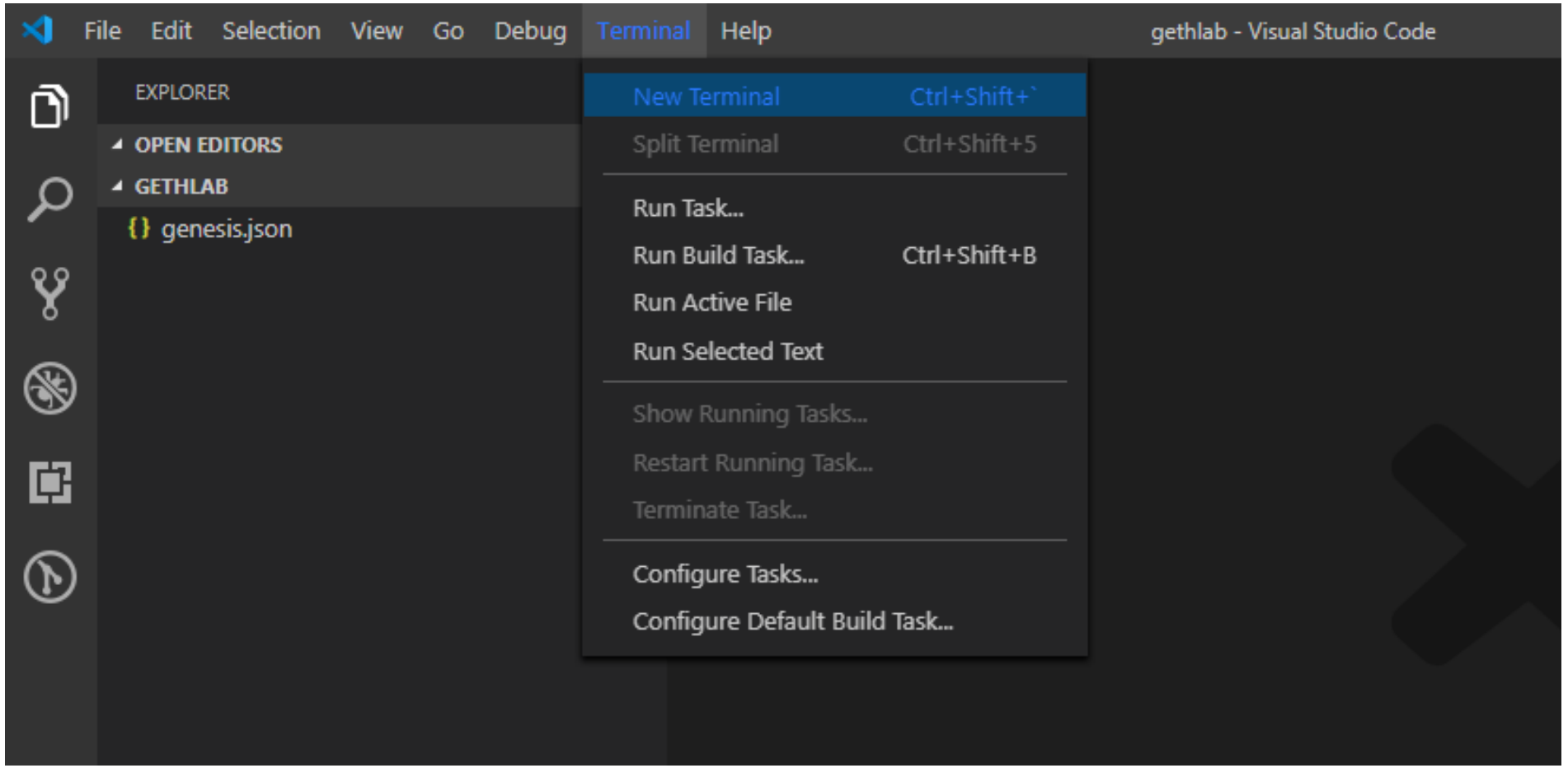
https://medium.com/coinmonks/ethereum-setting-up-a-private-blockchain-67bbb96cf4f1
https://github.com/ethereum/go-ethereum/blob/master/params/config.go

genesis.json



Create local node

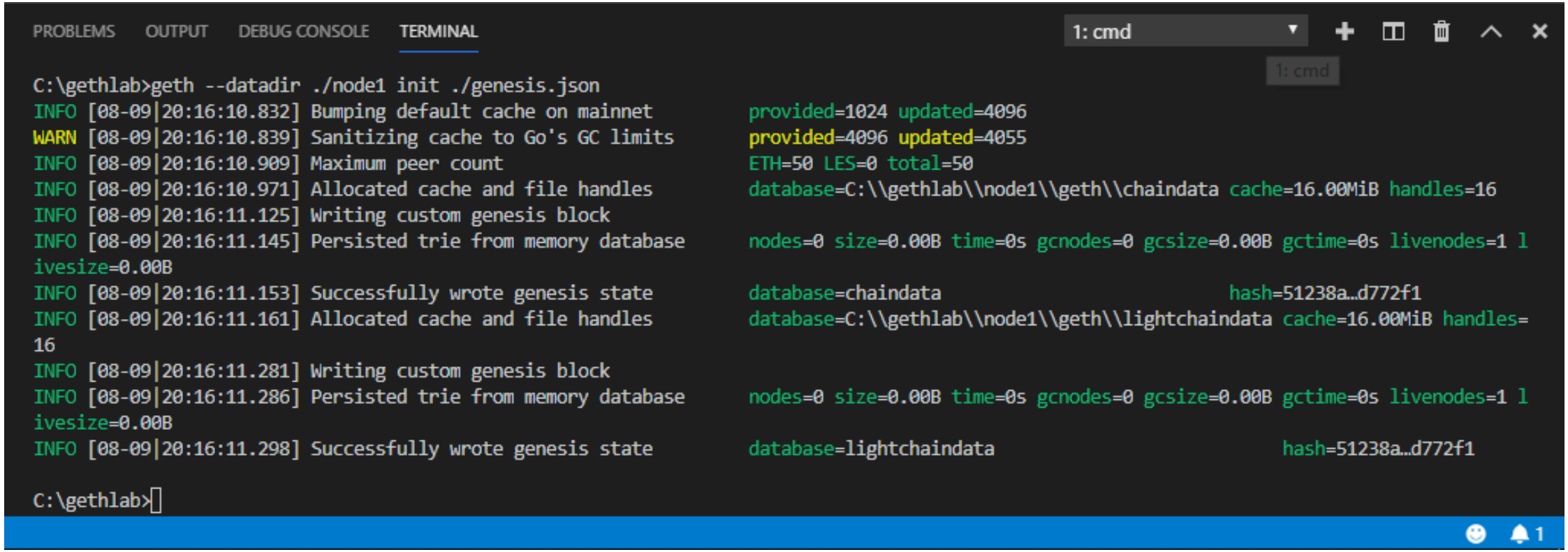
1. Open Command prompt



Create local node

2. Run command

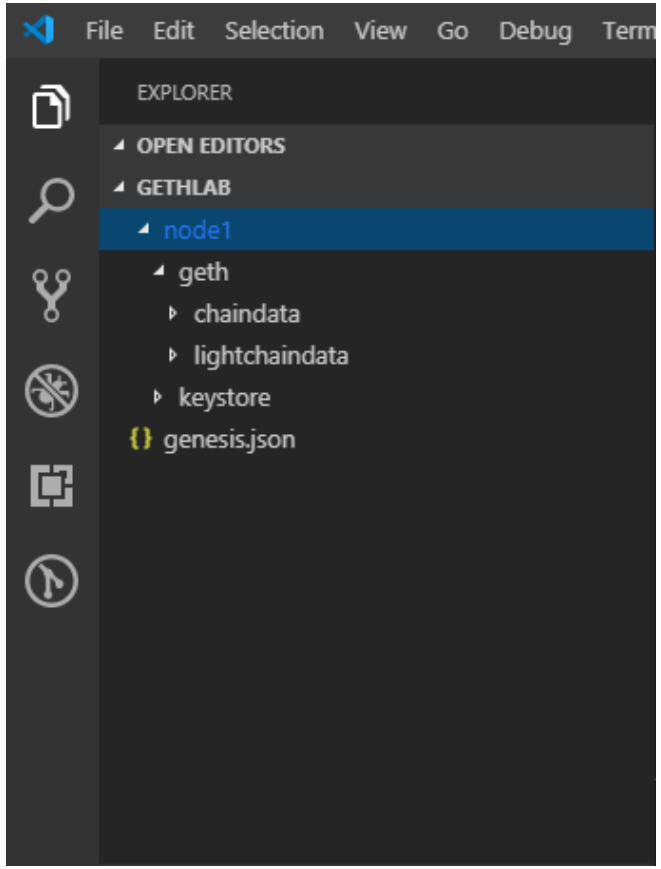
C:\gethlab>geth --datadir ./node1 init ./genesis.json

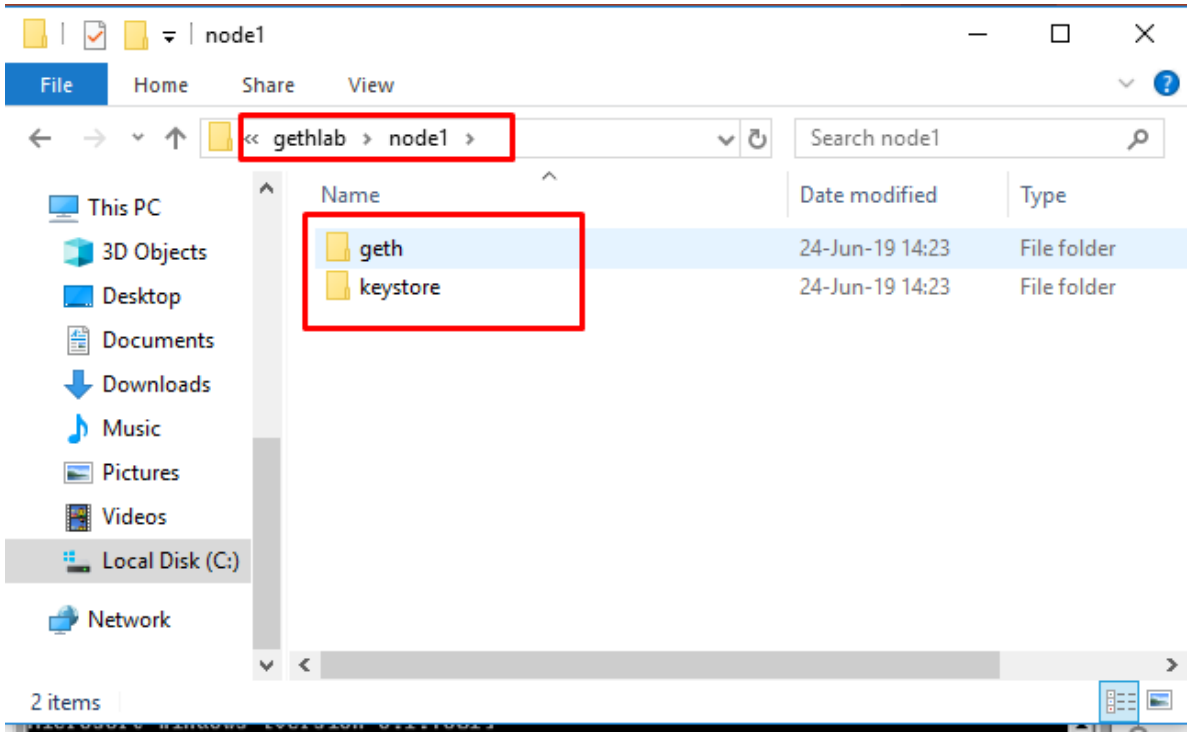


https://geth.ethereum.org/interface/Command-Line-Options

Create local node

3. Check your file and folder





https://geth.ethereum.org/interface/Command-Line-Options

Open Console

1. Run command

C:\gethlab>geth --datadir ./node1 --networkid 10 --verbosity 3 console 2>console.log

```
C:\gethlab>geth --datadir ./node1  --networkid 10 --verbosity 3 console
INFO [08-09|20:20:00.501] Maximum peer count                       ETH=50 LES=0 total=50
INFO [08-09|20:20:00.571] Starting peer-to-peer node               instance=Geth/v1.9.1-stable-b7b2f60f/windows-amd64/go1.12.7
INFO [08-09|20:20:00.578] Allocated trie memory caches             clean=256.00MiB dirty=256.00MiB
INFO [08-09|20:20:00.583] Allocated cache and file handles         database=C:\\gethlab\\node1\\geth\\chaindata cache=512.00MiB handles=8192

INFO [08-09|20:20:00.938] Regenerated local transaction journal    transactions=0 accounts=0
INFO [08-09|20:20:00.958] Allocated fast sync bloom                size=512.00MiB
INFO [08-09|20:20:00.963] Initialized fast sync bloom              items=0 errorrate=0.000 elapsed=0s
INFO [08-09|20:20:01.130] New local node record                    seq=19 id=e8d2f7018b518169 ip=127.0.0.1 udp=30303 tcp=30303
INFO [08-09|20:20:01.139] Started P2P networking                   self=enode://d66ed9d9ecfd36ea7630489cac8f664462f4a65659b727ab297ec179e34f
91092e15dc4106c83182be1f569ebcfe8d416393af3ae58ba7403351a40990ba8270@127.0.0.1:30303
INFO [08-09|20:20:01.142] IPC endpoint opened                      url=\\\\.\\pipe\\geth.ipc
WARN [08-09|20:20:01.291] Served eth_coinbase                      reqid=3 t=0s err="etherbase must be explicitly specified"
Welcome to the Geth JavaScript console!

instance: Geth/v1.9.1-stable-b7b2f60f/windows-amd64/go1.12.7
at block: 0 (Thu, 01 Jan 1970 07:00:00 +07)
 datadir: C:\gethlab\node1
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

>
```

https://geth.ethereum.org/interface/Command-Line-Options
https://skorks.com/2009/09/output-redirection-with-bash/ https://www.thaicert.or.th/papers/general/2011/pa2011ge006.html

geth	the go-ethereum command line interface
--datadir ./node1	Data directory for the databases and keystore
--port 30303	Network listening port (default: 30303)
--networkid 10	Network identifier (integer, 1=Frontier, 2=Morden(disused), 3=Ropsten, 4=Rinkeby, 5=Goerli) (default: 1)
--verbosity 3	Logging verbosity: 0=silent, 1=error, 2=warn, 3=info, 4=debug, 5=detail (default: 3)
console	Start an interactive JavaScript environment
2>console.log	write STDERR (standard error) to console.log (0=STDIN, 1=STDOUT, 2=STDERR)

https://geth.ethereum.org/interface/Command-Line-Options
https://skorks.com/2009/09/output-redirection-with-bash/ https://www.thaicert.or.th/papers/general/2011/pa2011ge006.html

personal.newAccount()

```
> personal.newAccount()
Passphrase:
Repeat passphrase:
INFO [08-10|11:30:27.045] Your new key was generated                address=0xF7b2CA8af32603fc2B1337690A6d3A5938013Bc3
WARN [08-10|11:30:27.050] Please backup your key file!              path=C:\\gethlab\\node1\\keystore\\UTC--2019-08-10T04-30-24.308487100Z--f
7b2ca8af32603fc2b1337690a6d3a5938013bc3
WARN [08-10|11:30:27.056] Please remember your password!
"0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3"
```

```
> personal.newAccount("1234")
INFO [08-10|11:30:53.351] Your new key was generated                address=0x70418C6EB01705AdaBadA1348d7E892Cc07BB741
WARN [08-10|11:30:53.356] Please backup your key file!              path=C:\\gethlab\\node1\\keystore\\UTC--2019-08-10T04-30-51.239425800Z--7
0418c6eb01705adabada1348d7e892cc07bb741
WARN [08-10|11:30:53.363] Please remember your password!
"0x70418c6eb01705adabada1348d7e892cc07bb741"
```

eth.accounts

```
> eth.accounts
["0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3", "0x70418c6eb01705adabada1348d7e892cc07bb741"]
> eth.accounts[0]
"0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3"
> eth.accounts[1]
"0x70418c6eb01705adabada1348d7e892cc07bb741"
> eth.accounts[2]
undefined
>
```

eth.coinbase

```
> eth.coinbase
INFO [08-10|11:33:22.171] Etherbase automatically configured
"0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3"
> eth.coinbase
"0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3"
>
```

miner.setEtherbase(account)

```
> miner.setEtherbase("0x70418c6eb01705adabada1348d7e892cc07bb741")
true
> eth.coinbase
"0x70418c6eb01705adabada1348d7e892cc07bb741"
> miner.setEtherbase(eth.accounts[0])
true
> eth.coinbase
"0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3"
>
```

miner.start(thread)

> miner.start(1)

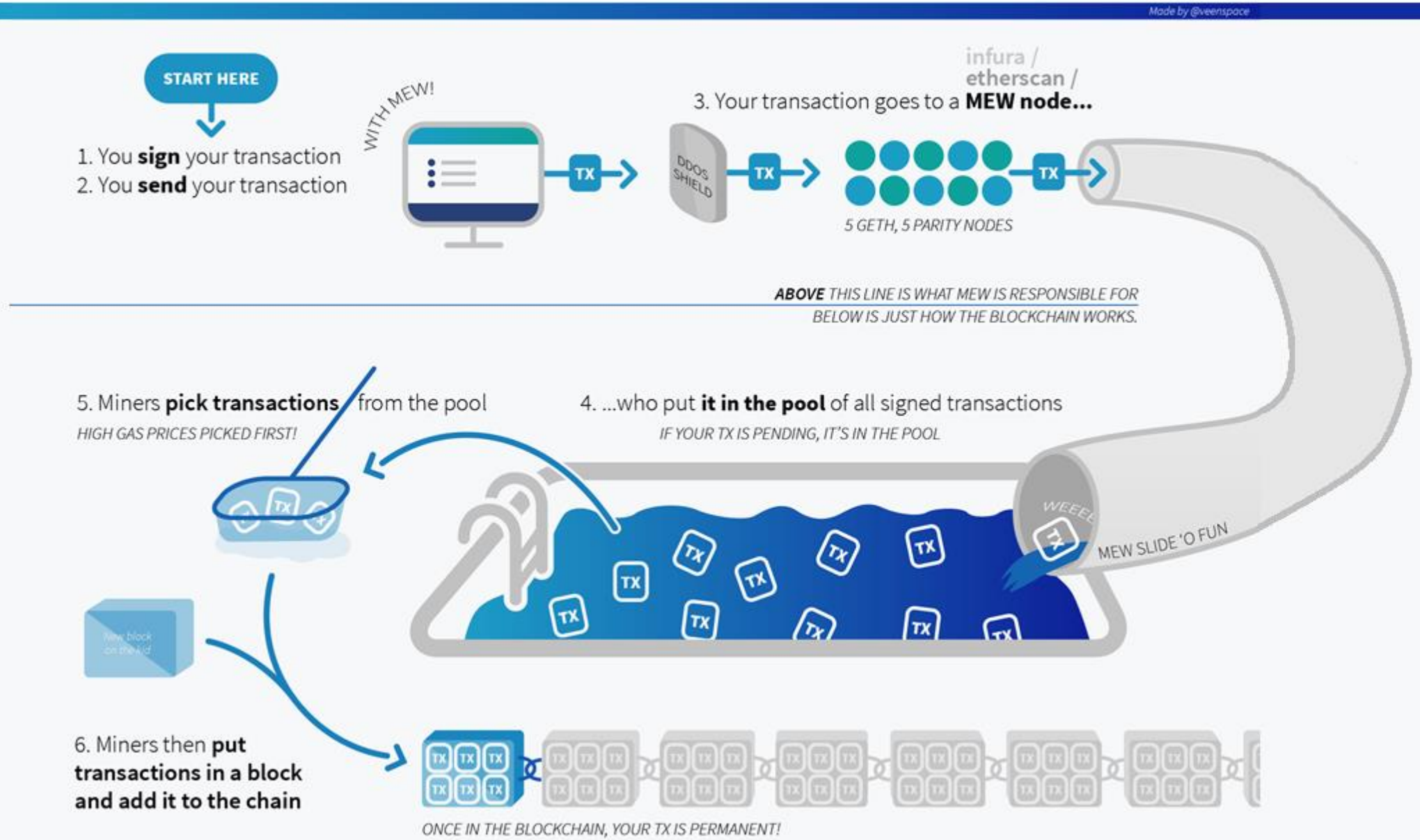
```
> miner.start(1)
INFO [08-10|11:36:38.681] Updated mining threads                   threads=1
INFO [08-10|11:36:38.705] Transaction pool price threshold updated price=1000000000
null
> INFO [08-10|11:36:38.747] Commit new mining work                   number=1 sealhash=5b9512…a9b6e7 uncles=0 txs=0 gas=0 fees=0 elapsed=36.
623ms
```

```
INFO [08-10|12:29:46.035] Successfully sealed new block           number=967 sealhash=3a0ae4…0bb26f hash=b2a06c…b0315e elapsed=4.722s
INFO [08-10|12:29:46.040] 🔗block reached canonical chain         number=960 hash=32df66…8cecc6
INFO [08-10|12:29:46.045] 🔨mined potential block                 number=967 hash=b2a06c…b0315e
INFO [08-10|12:29:46.049] Commit new mining work                  number=968 sealhash=52ad76…6b4418 uncles=0 txs=0 gas=0 fees=0 elapsed=8.9
```

miner.stop()

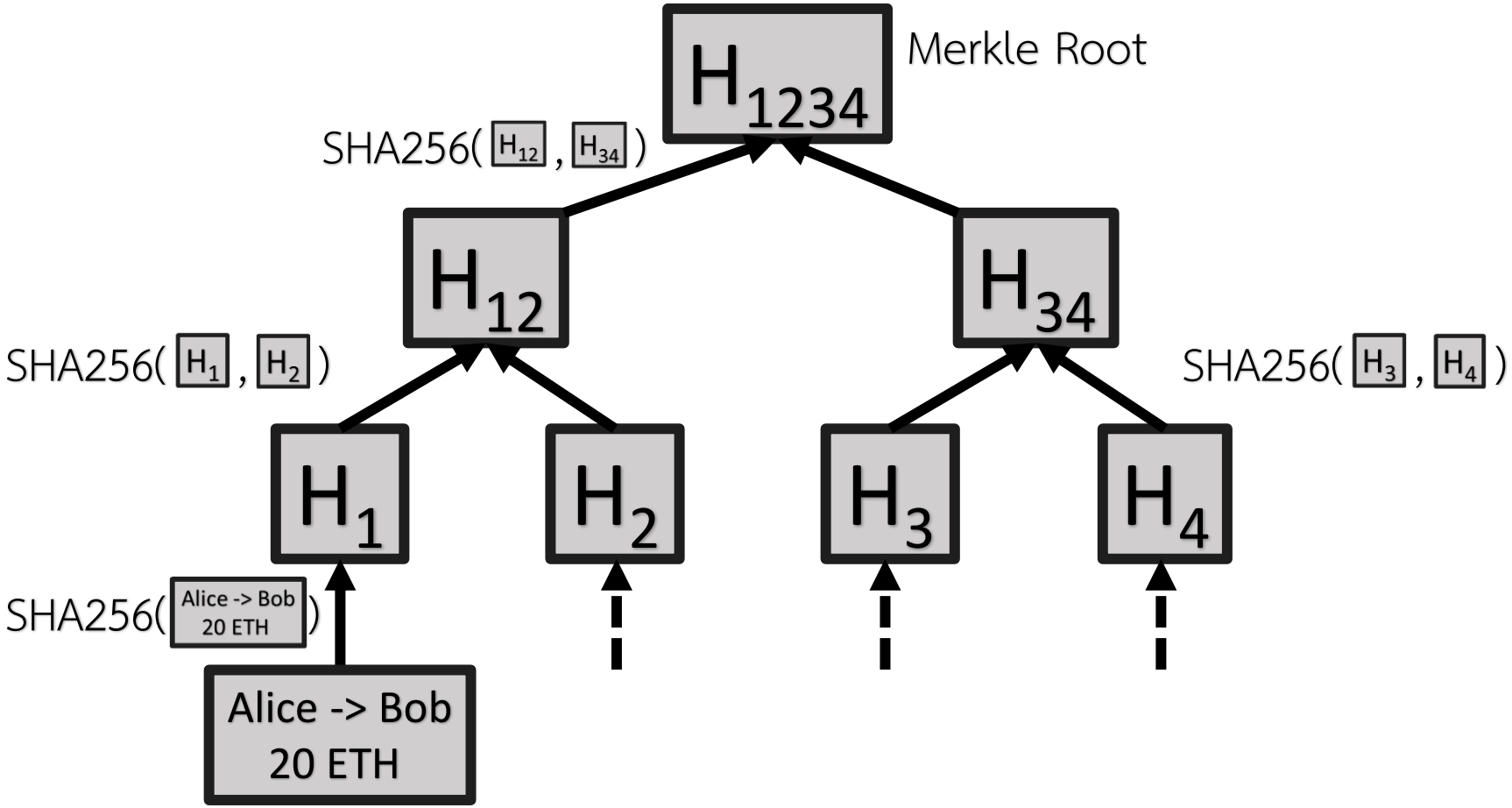
```
> miner.stop()
null
```

MyEtherWallet Behind-The-Scenes

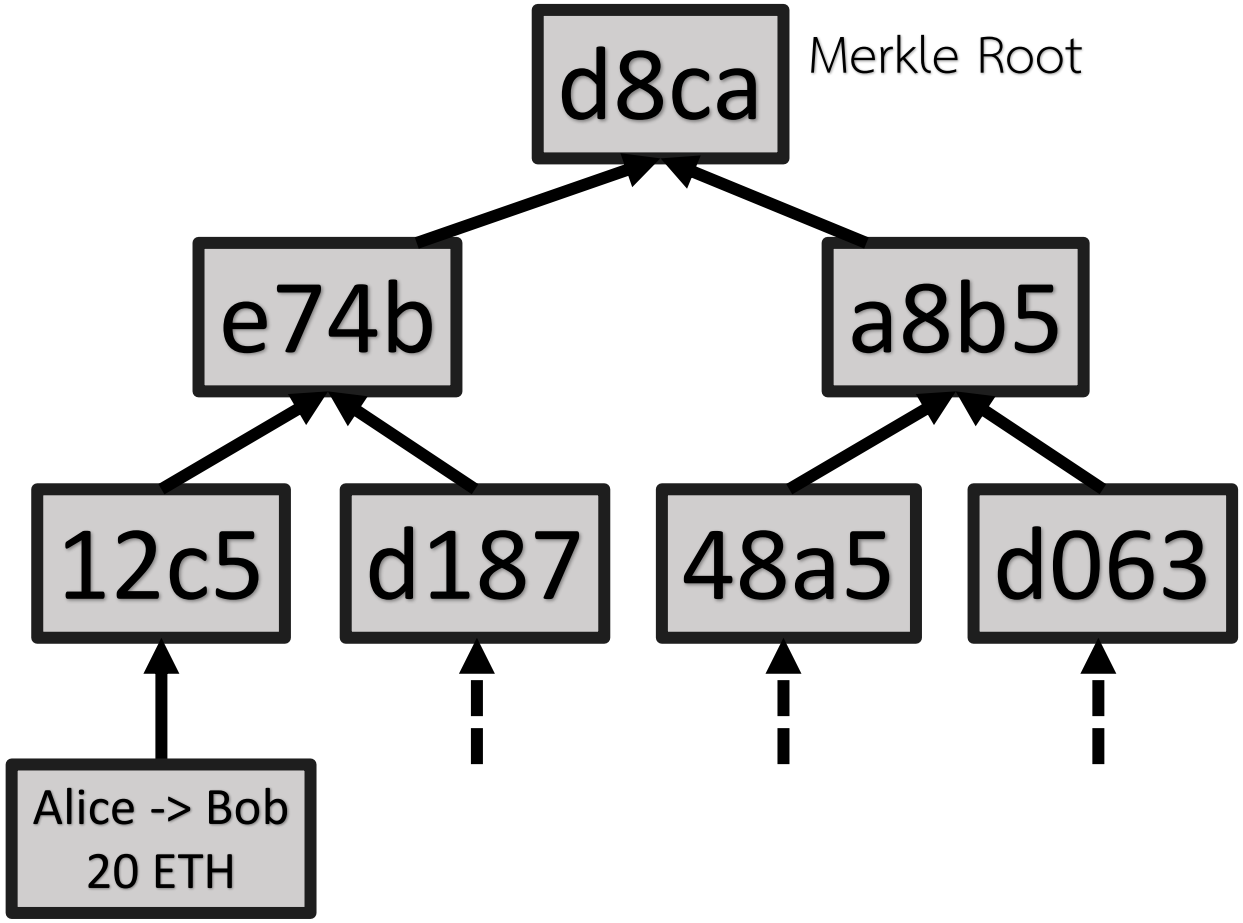


https://kb.myetherwallet.com/en/transactions/transaction-not-found-or-pending-forever/

Merkle Tree


H1234
Merkle Root
SHA256(H12 , H34)
H12
H34
SHA256(H1 , H2)
SHA256(H3 , H4)
H1
H2
H3
H4
SHA256(Alice -> Bob 20 ETH)
Alice -> Bob
20 ETH

Merkle Tree

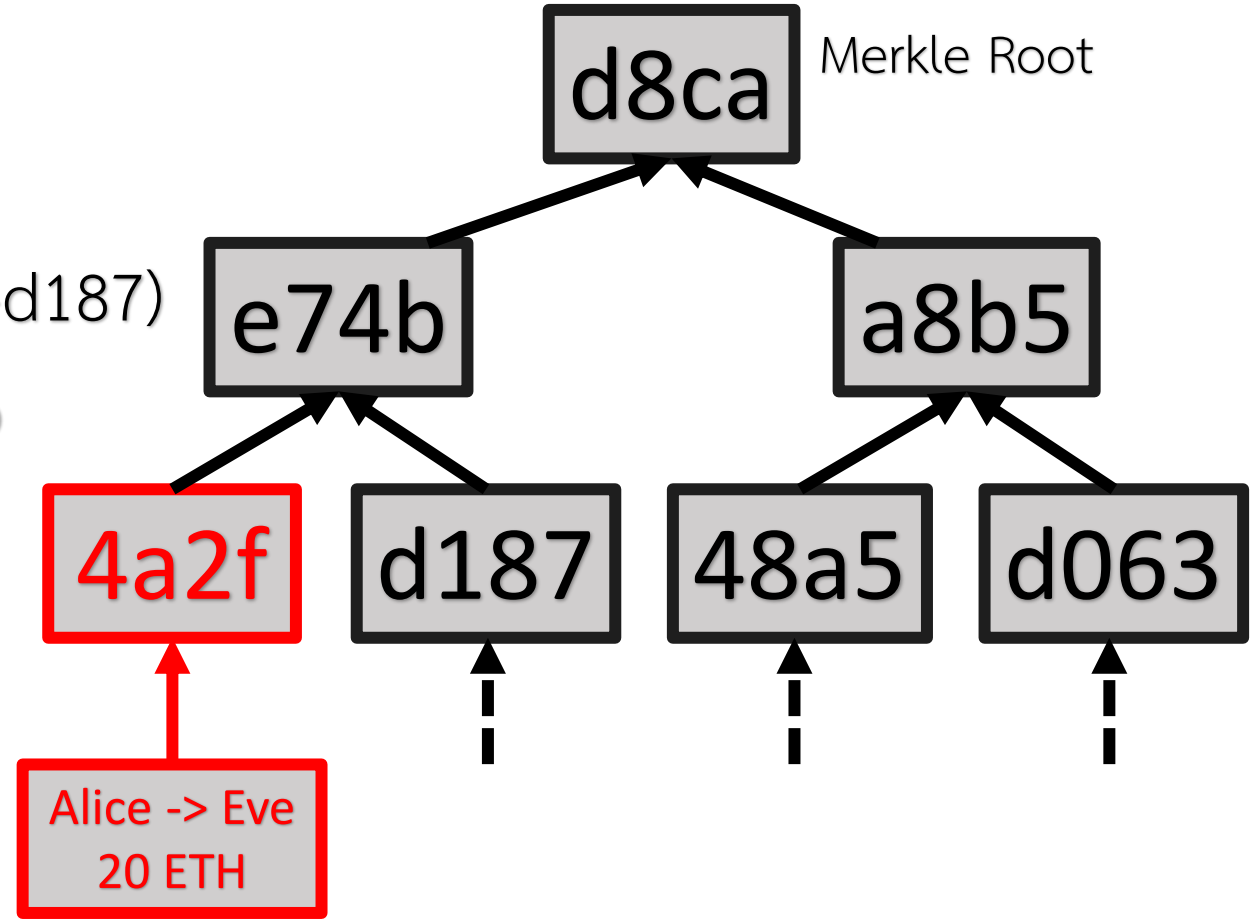

d8ca
Merkle Root
e74b
a8b5
12c5
d187
48a5
d063
Alice -> Bob
20 ETH

Merkle Tree

ERROR:

SHA256(4a2f+d187)

!= e74b

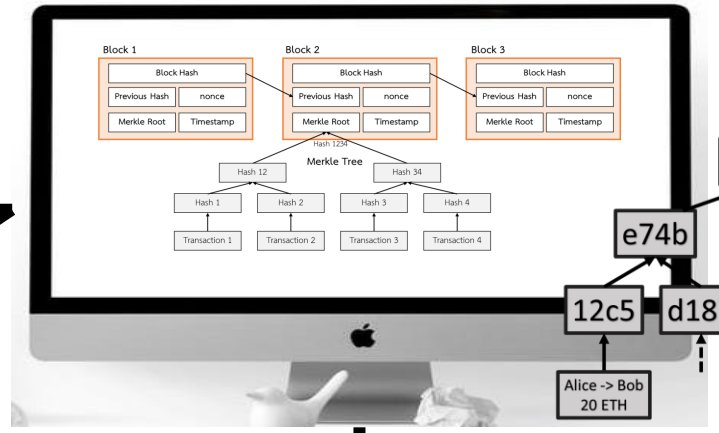


Attack Transaction

Node1

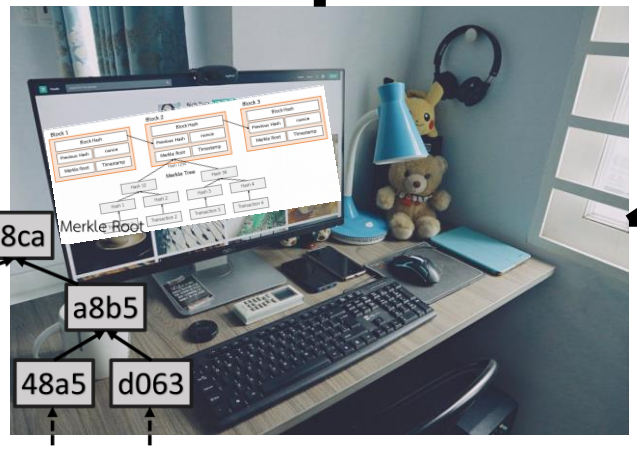
d8ca
e74b
a8b5
4a2f
d187
48a5
d063
Alice -> Eve
20 ETH

Node2



Merkle Root
d8ca
e74b
a8b5
12c5
d187
48a5
d063
Alice -> Bob
20 ETH

Node3



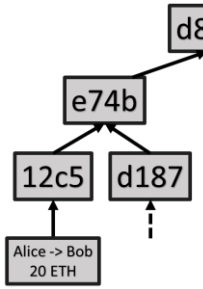
Merkle Root
d8ca
e74b
a8b5
12c5
d187
48a5
d063
Alice -> Bob
20 ETH

Node4

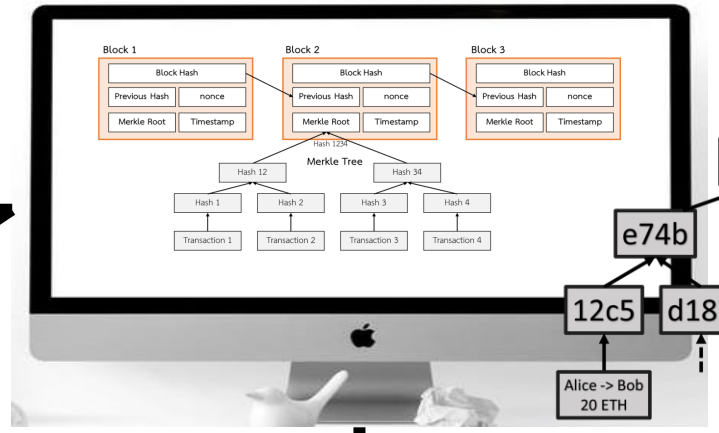
Merkle Root
d8ca
e74b
a8b5
12c5
d187
48a5
d063
Alice -> Bob
20 ETH

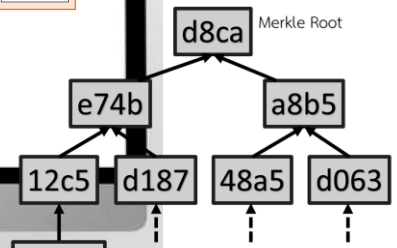
Attack Transaction

Node1

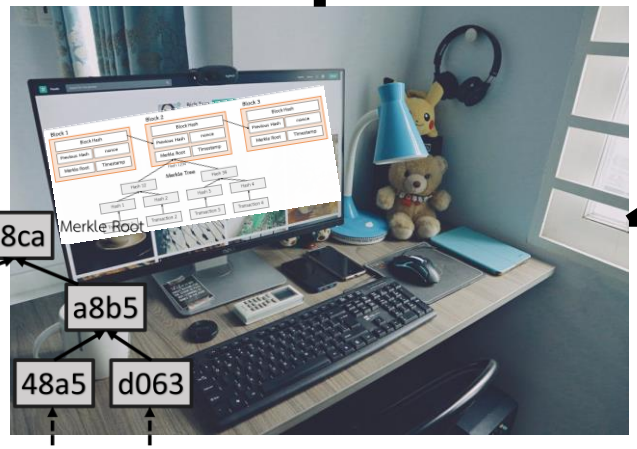


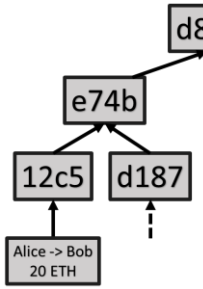
Node2



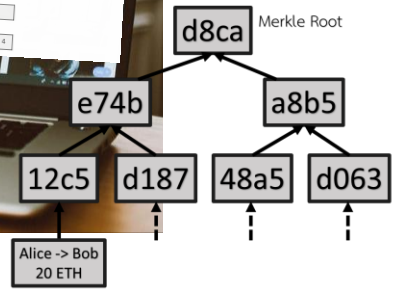


Node3



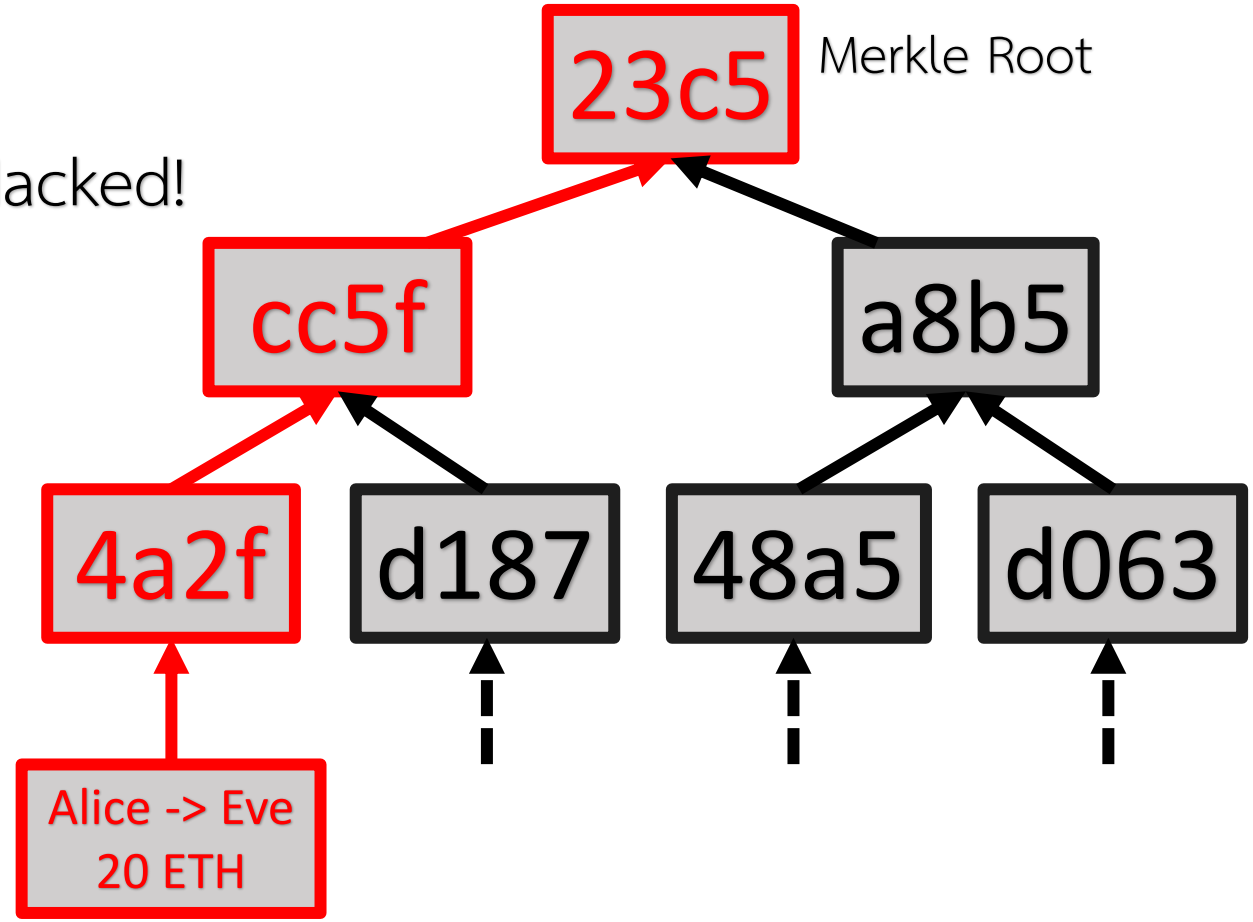


Node4



Merkle Tree

Merkle Tree Hacked!



Proof of Work

SHA256(SHA256(*All hashes in block header* +nonce)) ≤ target

target =$(10^{60})_{16}$ = 2^240

nonce	hashในบล็อค+nonce	SHA256(SHA256(ข้อมูลในบล็อค +nonce)) [เลขฐาน 16]	[เลขฐาน 10]
0	"5a3b1a0"	1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64	2^252.253458683
1	"5a3b1a1"	e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8	2^255.868431117
2	"5a3b1a2"	ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7	2^255.444730341
…	…	…	…
4248	"5a3b1a4248"	6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965	2^254.782233115
4249	"5a3b1a4249"	c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6	2^255.585082774
4250	"5a3b1a4250"	0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9	2^239.61238653

Proof of Work

$$\text{Target} = \frac{0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF}{difficulty}$$

why 10 minutes? -> moore's law

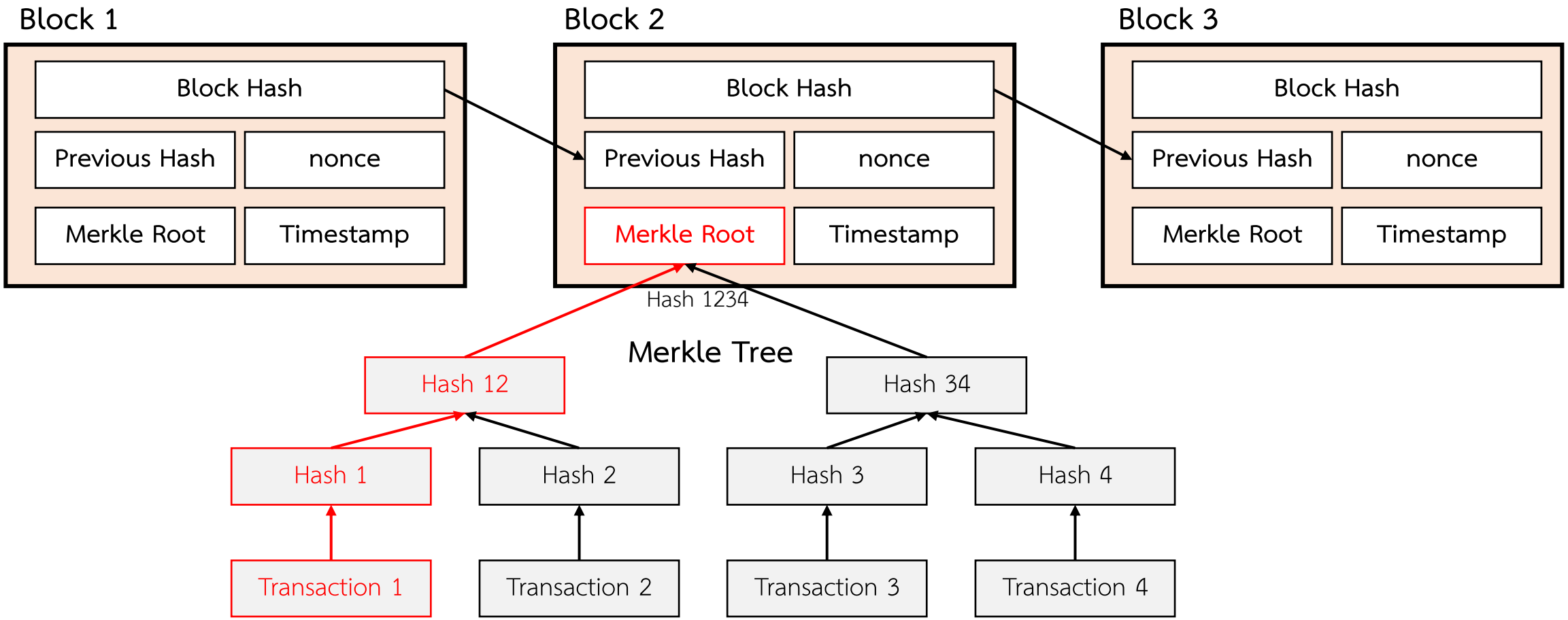
> A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

Update every 2 weeks (2016 blocks)

$$2\ weeks \times \frac{7\ days}{1\ week} \times \frac{24\ hours}{1\ day} \times \frac{60\ mins}{1\ hour} \times \frac{1\ blocks}{10\ mins} = 2016\ blocks$$

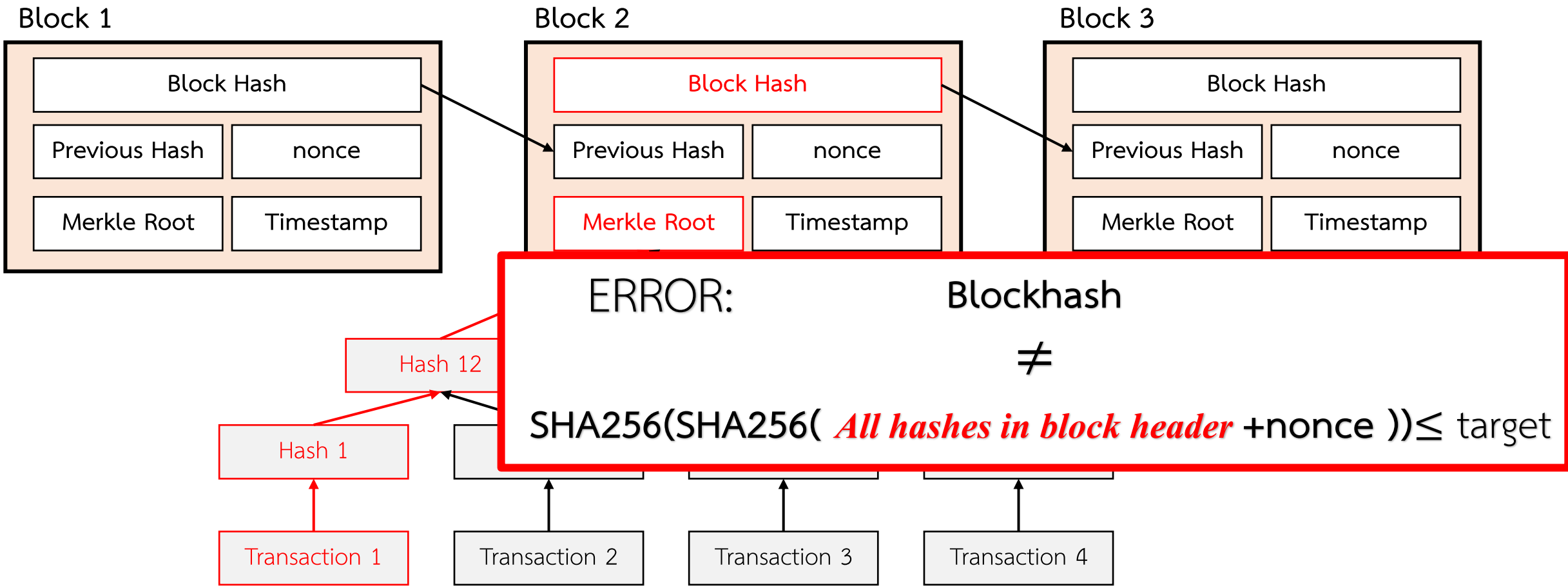
https://bitcoin.org/bitcoin.pdf https://etherscan.io/chart/blocksize
https://github.com/ethereum/wiki/wiki/White-Paper#mining

Attack Node



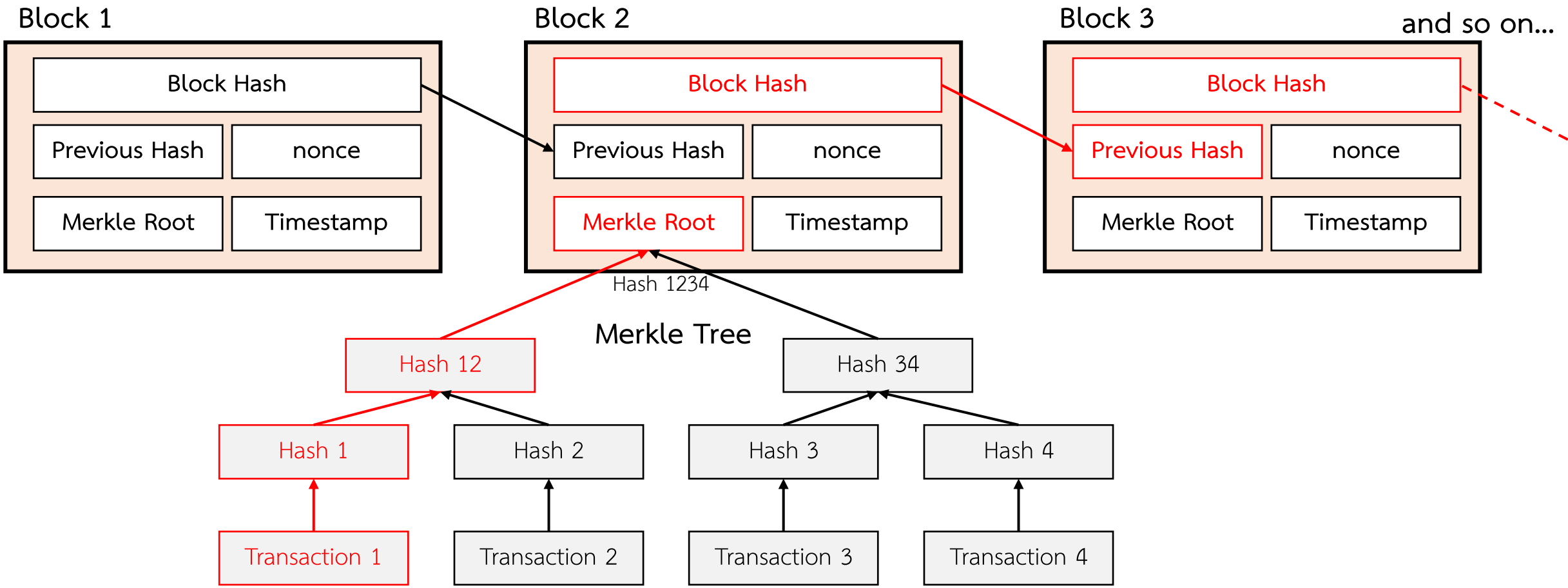
https://ethereum.github.io/yellowpaper/paper.pdf https://file.scirp.org/pdf/JSEA_20161028140127 98.pdf
https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

Attack Node



https://ethereum.github.io/yellowpaper/paper.pdf https://file.scirp.org/pdf/JSEA_20161028140127 98.pdf
https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

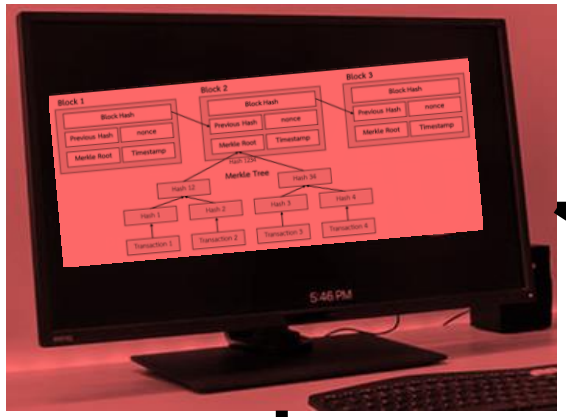
Attack Node



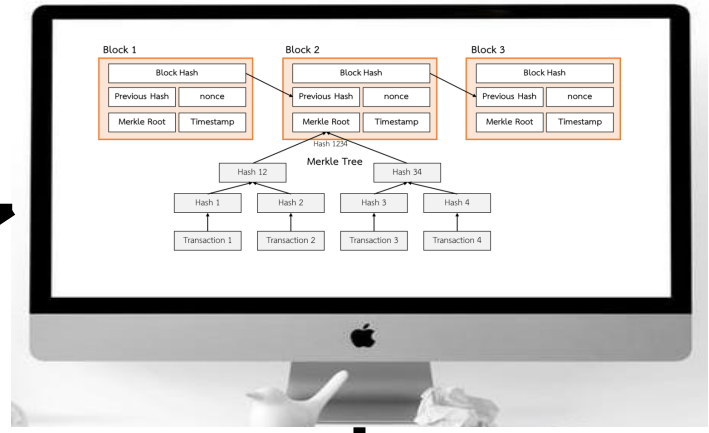
https://ethereum.github.io/yellowpaper/paper.pdf https://file.scirp.org/pdf/JSEA_20161028140127 98.pdf
https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

Attack Node < 50%

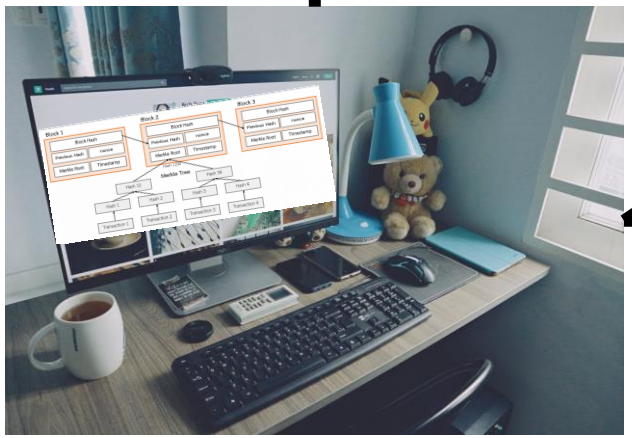
Node1



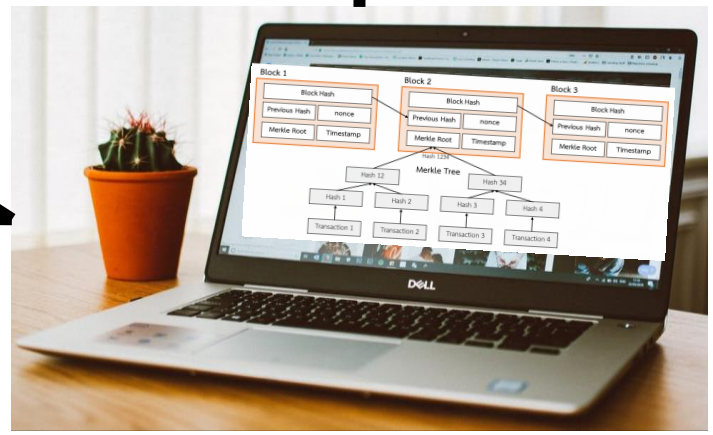
Node2



Node3

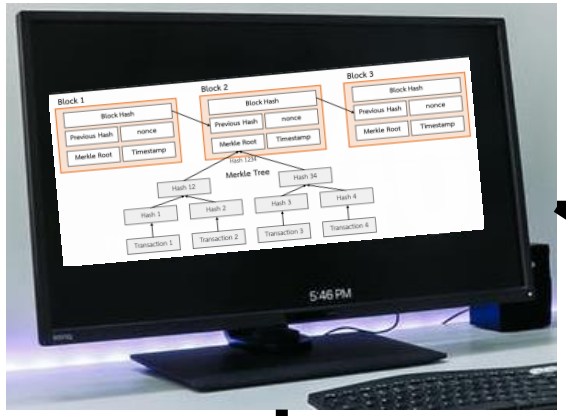


Node4

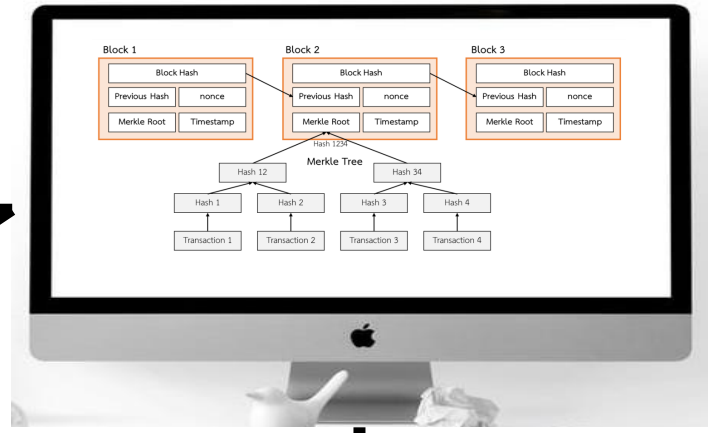


Attack Node < 50%

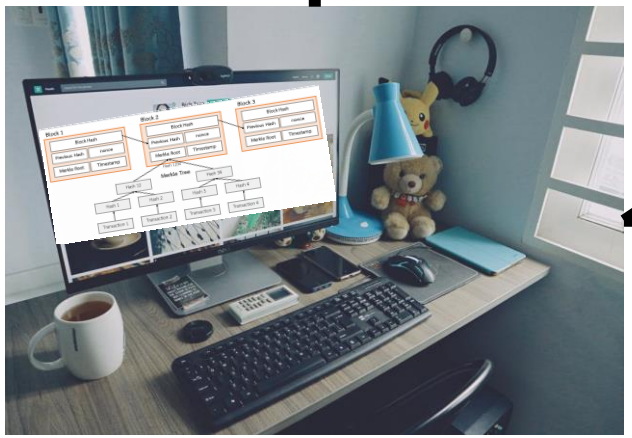
Node1



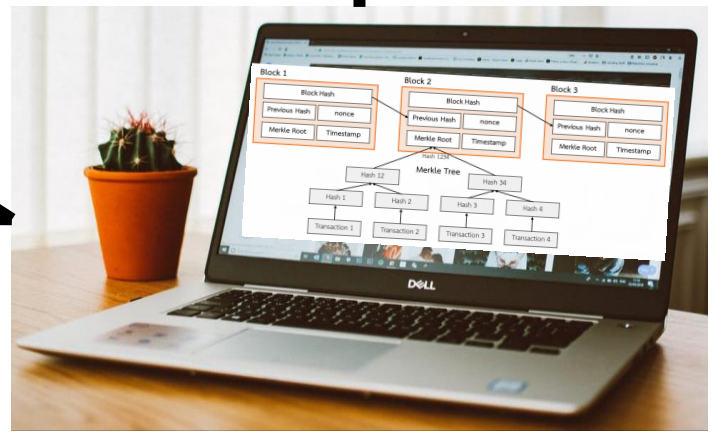
Node2



Node3

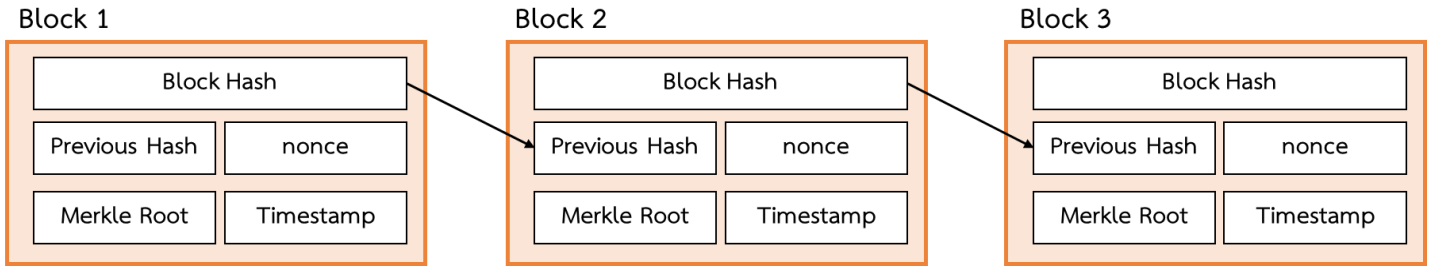


Node4



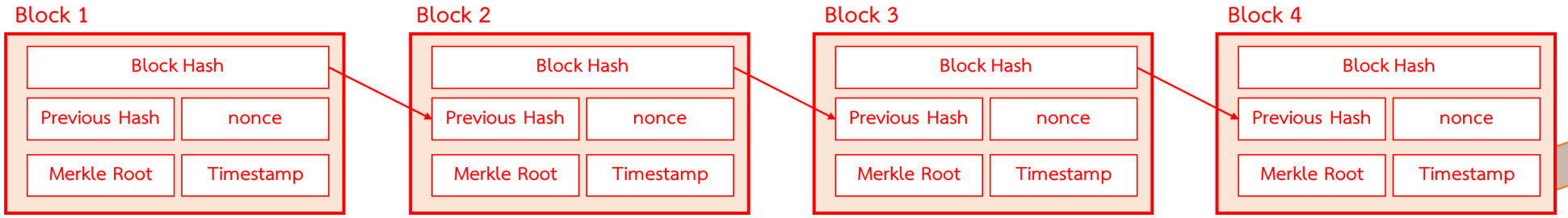
มีโอกาสเกิดกับ public blockchain ที่เปิดให้บุคคลภายนอก join node เข้ามาได้เท่านั้น

Node 1 3 blocks



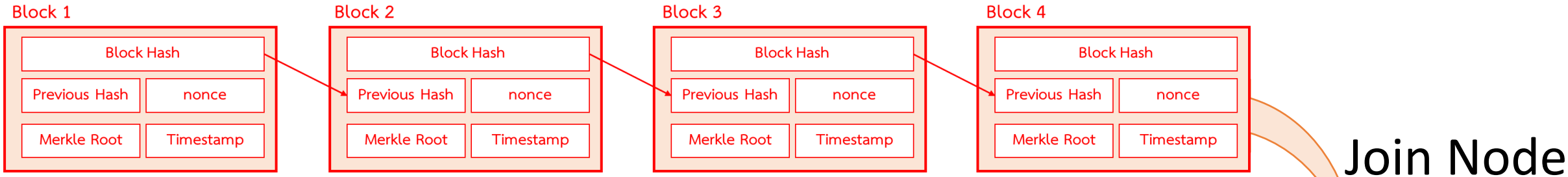
Join Node

Node 2 Attacker 4 blocks

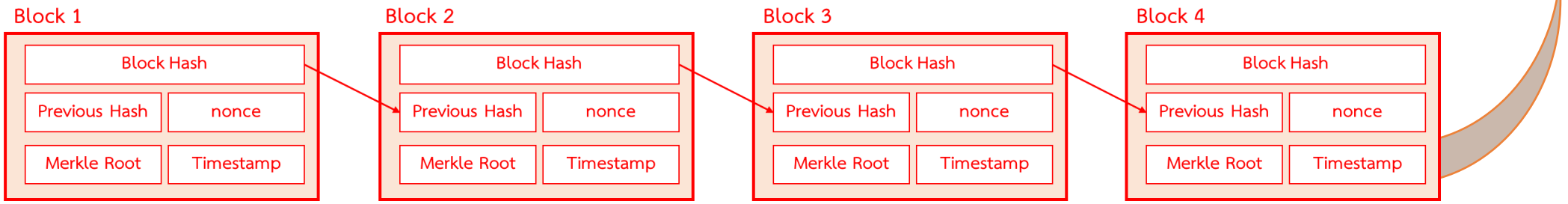


มีโอกาสเกิดกับ public blockchain ที่เปิดให้บุคคลภายนอก join node เข้ามาได้เท่านั้น

Node 1 4 blocks



Node 2 Attacker 4 blocks



eth.blockNumber

```
> eth.blockNumber
2028
```

eth.getBlock(number)

>eth.getBlock(1)

```
> eth.getBlock(1)
{
  difficulty: 131072,
  extraData: "0xda83010901846765746888676f312e31322e378777696e646f7773",
  gasLimit: 4716988,
  gasUsed: 0,
  hash: "0x3fcf47a9d7b76518a6a46012a828d1e261538c21800b8a02d39727e6df067605",
  logsBloom: "0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000",
  miner: "0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3",
  mixHash: "0x74503c50a8d8d5ff12767efb7313b4691ecbc1b5fa192067e4adb2c97f249fc1",
  nonce: "0x32f56c6644f1bc57",
  number: 1,
  parentHash: "0x51238aa1ec08fc8e7ac48c8bf29cdb4043a2a34a830de0ebdf5168ec0cd772f1",
  receiptsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  size: 538,
  stateRoot: "0x55d4a7dc1b0d73e71e7fa8ef535e50e84929a78847581588f227b84c13b2ebc5",
  timestamp: 1565411864,
  totalDifficulty: 131088,
  transactions: [],
  transactionsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  uncles: []
}
>
```

>eth.getBlock(2028)

```
> eth.getBlock(2028)
{
  difficulty: 319075,
  extraData: "0xda83010901846765746888676f312e31322e378777696e646f7773",
  gasLimit: 8000000,
  gasUsed: 0,
  hash: "0x1955d16b60f1261d41f22ee6c58a356ea725e45e6414cb14a152837b93bee896",
  logsBloom: "0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000",
  miner: "0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3",
  mixHash: "0x73d386d9fb4b310f015b3d598ead38be77233092150cd1b1c262411473c10359",
  nonce: "0x474382e27e996524",
  number: 2028,
  parentHash: "0xacc48cbc9be86ece25a1cbde02c3f161d1bd62a1cd71bd1f1d1d373b47f22efd
  receiptsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b4
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
  size: 540,
  stateRoot: "0x6e1f172c5ac95288b46ad075b2cd0e11ee6762383a6ad2e35b547ccf3f0bf25d"
  timestamp: 1565420051,
  totalDifficulty: 435961351,
  transactions: [],
  transactionsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e3
  uncles: []
}
>
```

eth.getBalance(account)

```
> eth.getBalance("0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3")
1.014e+22
> eth.getBalance(eth.accounts[0])
1.014e+22
> eth.getBalance(eth.coinbase)
1.014e+22
>
```

personal.unlockAccount(account)

```
> personal.unlockAccount("0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3")
Unlock account 0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3
Passphrase:
true
> personal.unlockAccount(eth.accounts[0])
Unlock account 0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3
Passphrase:
true
```

```
> personal.unlockAccount("0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3")
Unlock account 0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3
Passphrase:
WARN [08-10|14:31:08.496] Failed account unlock attempt            addr
 key with given passphrase"
WARN [08-10|14:31:08.505] Served personal_unlockAccount            reqi
Error: could not decrypt key with given passphrase
>
```

eth.sendTransaction({from:sender to:receiver value:amount})

eth.sendTransaction({from: "0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3" to: "0x70418c6eb01705adabada1348d7e892cc07bb741"value: 2e+18})

$2e+18 = 2 \times 10^{18}$

```
> eth.sendTransaction({from: "0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3" to: "0x70418c6eb01705adabada1348d7e892cc07bb741"value: 2e+18})
INFO [08-10|14:33:36.079] Submitted transaction                    fullhash=0x6fbce8ef88cb30919a44f340a3c9a8df611da80b4ae247d0f571b6c97dfa20
be recipient=0x70418C6EB01705AdaBadA1348d7E892Cc07BB741
"0x6fbce8ef88cb30919a44f340a3c9a8df611da80b4ae247d0f571b6c97dfa20be"
```

eth.sendTransaction({from: eth.accounts[0] to: eth.accounts[1] value: 2e+18})

```
> eth.sendTransaction({from: eth.accounts[0] to: eth.accounts[1] value: 2e+18})
INFO [08-10|14:33:40.395] Submitted transaction                    fullhash=0xf47bd9e197587849fd394138ef9f6abb57c52a8498bc7ad7ae886324f1572b
e3 recipient=0x70418C6EB01705AdaBadA1348d7E892Cc07BB741
"0xf47bd9e197587849fd394138ef9f6abb57c52a8498bc7ad7ae886324f1572be3"
```

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

Add Peer/ Join Node

1.สร้างโหนดขึ้นมาอีกอัน

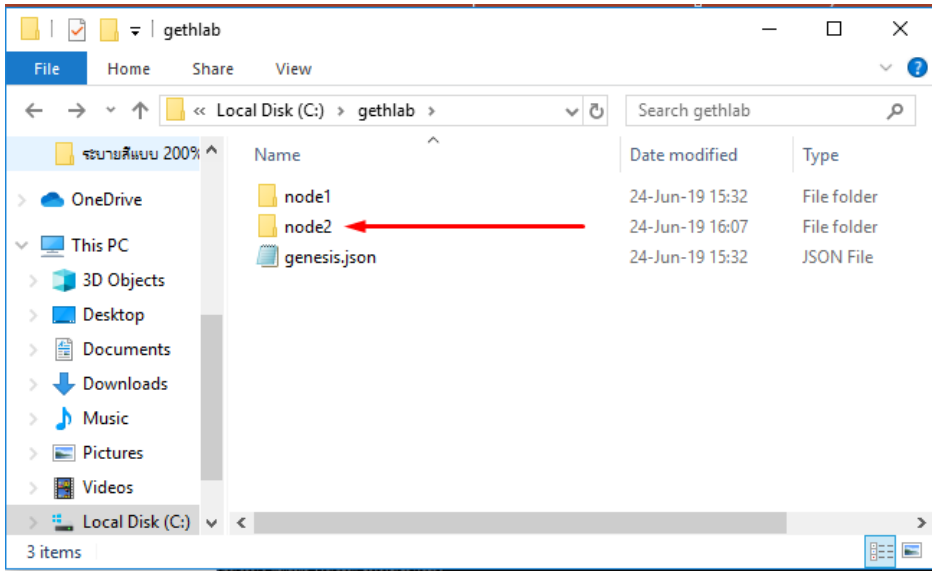
1.1 เปิด command prompt อีกหนึ่งอัน

1.2 สร้างโหนดสอง run command

C:\gethlab>geth --datadir ./node2 init ./genesis.json

1.3 เข้าคอนโซลของโหนดสอง run command

C:\gethlab>geth --datadir ./node2 --port 30304 --networkid 10 --ipcdisable console 2>console2.log




```
C:\gethlab>geth --datadir ./node2 init ./genesis.json
INFO [08-10|14:36:03.708] Bumping default cache on mainnet         provided=1024 updated=4096
WARN [08-10|14:36:03.718] Sanitizing cache to Go's GC limits       provided=4096 updated=4055
INFO [08-10|14:36:03.839] Maximum peer count                       ETH=50 LES=0 total=50
INFO [08-10|14:36:03.907] Allocated cache and file handles         database=C:\\gethlab\\node2\\geth\\
INFO [08-10|14:36:04.022] Writing custom genesis block
INFO [08-10|14:36:04.039] Persisted trie from memory database      nodes=0 size=0.00B time=0s gcnodes=
ivesize=0.00B
INFO [08-10|14:36:04.047] Successfully wrote genesis state         database=chaindata
INFO [08-10|14:36:04.053] Allocated cache and file handles         database=C:\\gethlab\\node2\\geth\\
16
INFO [08-10|14:36:04.189] Writing custom genesis block
INFO [08-10|14:36:04.194] Persisted trie from memory database      nodes=0 size=0.00B time=0s gcnodes=
ivesize=0.00B
INFO [08-10|14:36:04.202] Successfully wrote genesis state         database=lightchaindata

C:\gethlab>
```

Add Peer/ Join Node

****ขอเรียกคอนโซลแรกว่า cmd#1 และ คอนโซลของโหนดที่สร้างใหม่ว่า cmd#2****

2. Get Enode

cmd#2

2.1 run command

>admin.nodeInfo

2.2 File > New File

2.3 paste enode

COPY

```
> admin.nodeInfo
{
  enode: "enode://edbf10f2cae81f0ff19e4003c85b4fc2734d298a5c61ad
fdaf59@49.229.210.152:30304",
  enr: "enr:-Je4QPGRIxZsMV4Hco5UEe42qxFeLTmcl8-RgYQqGl9lN9_GYX4E
c2VjcDI1NmsxoQPtvxDyyugfD_GeQAPIW0_Cc00pilxhreg0cHaUjVUVRIN0Y3CC
  id: "9e0db447c3e3375f6430daf4fca3ab9741bfdba388641f9ba9579146b
  ip: "49.229.210.152",
  listenAddr: "[::]:30304",
  name: "Geth/v1.9.1-stable-b7b2f60f/windows-amd64/go1.12.7",
  ports: {
    discovery: 30304,
    listener: 30304
  },
```

Untitled-1

```
1  "enode://edbf10f2cae81f0ff19e4003c85b4fc2734d298a5c61ade8347076948d5515449f6e7ca3309ca0a5714256e450da8347d8c2db0978eb9bf5ad686641c4fdaf59@49.229.210.152:30304"
```

Add Peer/ Join Node

3. get IPv4 address

    3.1 เปิด command prompt อีกหนึ่งอัน (cmd#3)

    3.2 run command

        C:\gethlab>ipconfig

    3.3 แก้ไข ip ใน enode ให้เป็น IPv4

```
C:\gethlab>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5cf7:23d:9698:b566%15
   IPv4 Address. . . . . . . . . . . : 10.226.160.128
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.226.160.1
```

Change to IPv4

Untitled-1

```
1  "enode://edbf10f2cae81f0ff19e4003c85b4fc2734d298a5c61ade8347076948d5515449f6e7ca3309ca0a5714256e450da8347d8c2db0978eb9bf5ad686641c4fdaf59@49.229.210.152:30304"
```

Untitled-1

```
1  "enode://edbf10f2cae81f0ff19e4003c85b4fc2734d298a5c61ade8347076948d5515449f6e7ca3309ca0a5714256e450da8347d8c2db0978eb9bf5ad686641c4fdaf59@10.226.160.128:30304"
```

admin.addPeer(enode)

4. addPeer

cmd#1

4.1 run command format: admin.addPeer(enode) // อย่าลืมใส่ " "

>admin.addPeer("enode://edbf10f2cae81f0ff19e4003c85b4fc2734d298a5c61ade8347076948d5515449f6e7ca3309ca0a5714256e450da8347d8c2db0978eb9bf5ad686641c4fdaf59@10.226.160.128:30304")

```
> admin.addPeer("enode://edbf10f2cae81f0ff19e4003c85b4fc2734d298a5c61ade8347076948d5515449f
86641c4fdaf59@10.226.160.128:30304")
true
```

admin.peers

5. Check peers info

5.1 run command

>admin.peers

ถ้ารันใน node1 จะเห็นข้อมูลของ node2

ถ้ารันใน node2 ก็จะเห็นข้อมูลของ node1

node1

```
> admin.peers
[{
    caps: ["eth/63"],
    enode: "enode://edbf10f2cae81f0ff19e4003c85b4fc2734d298a5c61ade8347076948d5515449f
c4fdaf59@10.226.160.128:30304",
    id: "9e0db447c3e3375f6430daf4fca3ab9741bfdba388641f9ba9579146bde44dfc",
    name: "Geth/v1.9.1-stable-b7b2f60f/windows-amd64/go1.12.7",
    network: {
      inbound: false,
      localAddress: "10.226.160.128:55053",
      remoteAddress: "10.226.160.128:30304",
      static: true,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 16,
        head: "0x51238aa1ec08fc8e7ac48c8bf29cdb4043a2a34a830de0ebdf5168ec0cd772f1",
        version: 63
      }
    }
}]
```

node2

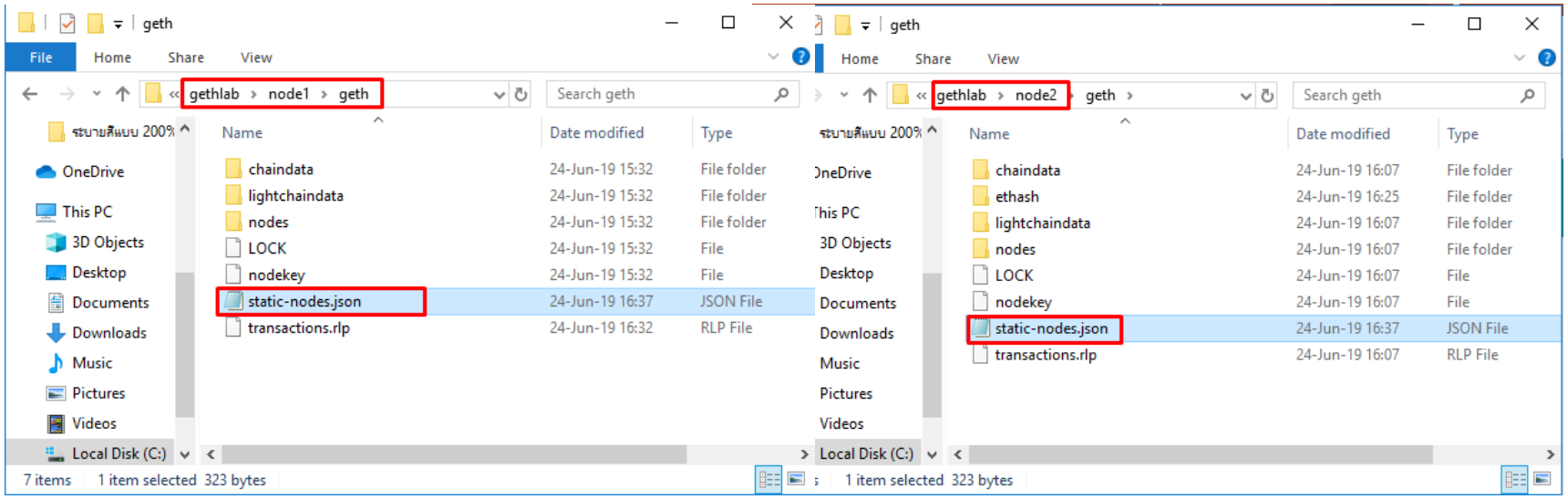
```
> admin.peers
[{
    caps: ["eth/63"],
    enode: "enode://d66ed9d9ecfd36ea7630489cac8f664462f4a65659b727ab297ec179e34f91092
90ba8270@10.226.160.128:55053",
    id: "e8d2f7018b518169989e9d375b626e00f71004c631bddf42a6936496370175c3",
    name: "Geth/v1.9.1-stable-b7b2f60f/windows-amd64/go1.12.7",
    network: {
      inbound: true,
      localAddress: "10.226.160.128:30304",
      remoteAddress: "10.226.160.128:55053",
      static: false,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 435961351,
        head: "0x1955d16b60f1261d41f22ee6c58a356ea725e45e6414cb14a152837b93bee896",
        version: 63
      }
    }
}]
```

static-nodes.json

1. File > New File > paste code
2. Save file as static-nodes.json
3. Copy file to Data folder C:\gethlab\node1\geth และ C:\gethlab\node2\geth

static-nodes.json format

```
[
 "enode://pubkey@ip:port“,
 "enode://pubkey@ip:port“
]
```



static-nodes.json

```
[
    "enode://d66ed9d9ecfd36ea7630489cac8f664462f4a92e15dc4106c83182be1f569ebcfe8d416393af3ae58ba7403351a40990ba8270@49.229.210.152:30303",
    "enode://edbf10f2cae81f0ff19e4003c85b4fc2734d249f6e7ca3309ca0a5714256e450da8347d8c2db0978eb9bf5ad686641c4fdaf59@10.226.160.128:30304"
]
```

Explorer

explorer.html

File | C:/saiyab/bc/bc1%20รุ่น%206/gethlab/explorer.html

Number	Tx#	Size	Timestamp
2027	0	540	1565420050
2026	0	540	1565420049
2025	0	540	1565420047
2024	0	540	1565420029
2023	0	540	1565420028
2022	0	540	1565420026
2021	0	540	1565420025
2020	0	540	1565420023
2019	0	540	1565420020
2018	0	540	1565420019
2017	0	540	1565420018
2016	0	540	1565420017
2015	0	540	1565420014
2014	0	540	1565420003
2013	0	540	1565420000
2012	0	540	1565419996
2011	0	540	1565419992

enable rpc port

1. exit console (Ctrl+D or type exit in console)
2. enter console with command

C:\gethlab>geth --datadir ./node1 --networkid 10 --verbosity 3 --rpc --rpcapi "eth,web3,personal,net,db" --rpccorsdomain "*" console 2>console.log

```
C:\gethlab>geth --datadir ./node1  --networkid 10 --verbosity 3 --rpc --rpcapi "eth,web3,personal,net,db" --rpccorsdomain "*" console 2>console.log
Welcome to the Geth JavaScript console!

instance: Geth/v1.9.1-stable-b7b2f60f/windows-amd64/go1.12.7
coinbase: 0x10effd5845381002f566e10e9371ff00d8767f41
at block: 725 (Thu, 15 Aug 2019 00:28:49 +07)
 datadir: C:\gethlab\node1
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

>
```

https://geth.ethereum.org/interface/Command-Line-Options

geth 1.9.x update!

accounts, cmd, internal: disable unlock account as default #17037

Merged karalabe merged 4 commits into `ethereum:master` from `rjl493456442:disable_unlock_account_asdefault` on Apr 4

holiman commented on Mar 29 — Contributor

As it now works, I think it's fine.

- If you call `unlock` via CLI, it fails the unlock if `ws` or `rpc` is enabled,
- If you call `personal.unlock` via rpc, it fails it if `ws` or http-`rpc` is enanbled

It is still possible to shoot yourself in the foot if you really try hard, via

```
> build/bin/geth --unlock 0 --password password.txt --nodiscover --maxpeers 0 console
[...]
> admin.startRPC()
INFO [03-29|11:32:57.269] HTTP endpoint opened                     url=http://localhost:8545
true
```

https://github.com/ethereum/go-ethereum/pull/17037

How to Unlock

1. with **allow-insecure-unlock** option

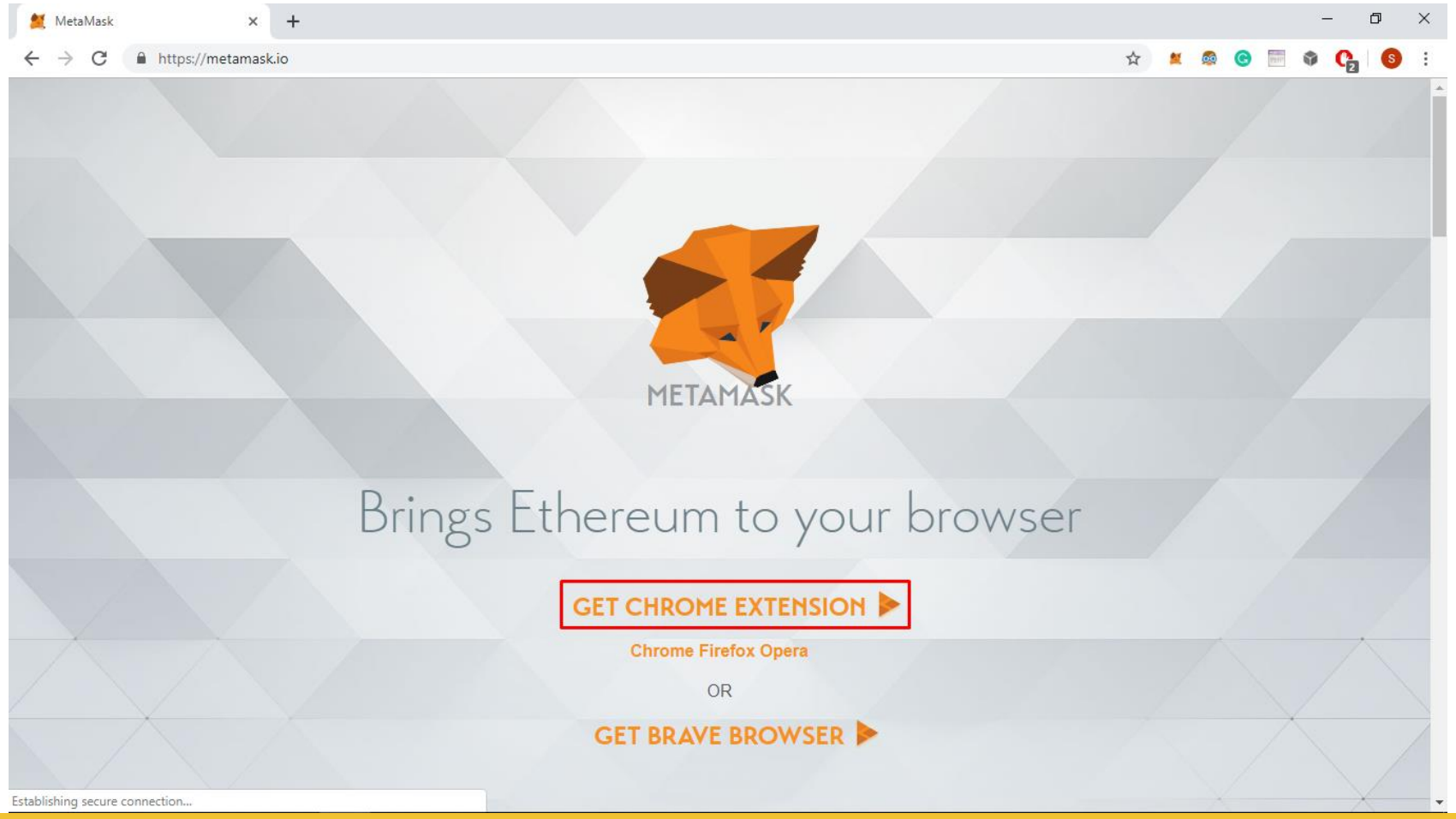
C:\gethlab>geth --datadir ./node1 --networkid 10 --verbosity 3 --rpc --rpcapi "eth,web3,personal,net,db" --rpccorsdomain "*" --allow-insecure-unlock --unlock 0 --password password.txt console 2>console.log

```
C:\gethlab>geth --datadir ./node1  --networkid 10 --verbosity 3 --rpc --rpcapi "eth,web3,personal,net,db" --rpccorsdomain "*" --allow-insecure-unlock --unlock 0 --password passwo
rd.txt console 2>console.log
Welcome to the Geth JavaScript console!

instance: Geth/v1.9.1-stable-b7b2f60f/windows-amd64/go1.12.7
coinbase: 0xf7b2ca8af32603fc2b1337690a6d3a5938013bc3
at block: 2028 (Sat, 10 Aug 2019 13:54:11 +07)
 datadir: C:\gethlab\node1
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

>
```

https://geth.ethereum.org/interface/Command-Line-Options

How to Unlock

2. with **metamask**



Geth Console

Command	Description
personal.newAccount()	Create new account
eth.accounts	View all accounts in the node
eth.coinbase	View coinbase
miner.setEtherbase(account)	Change coinbase to account
miner.start(thread)	Start mining with thread thread(s)
miner.stop()	Stop mining
eth.getBalance(account)	Get balance of that account

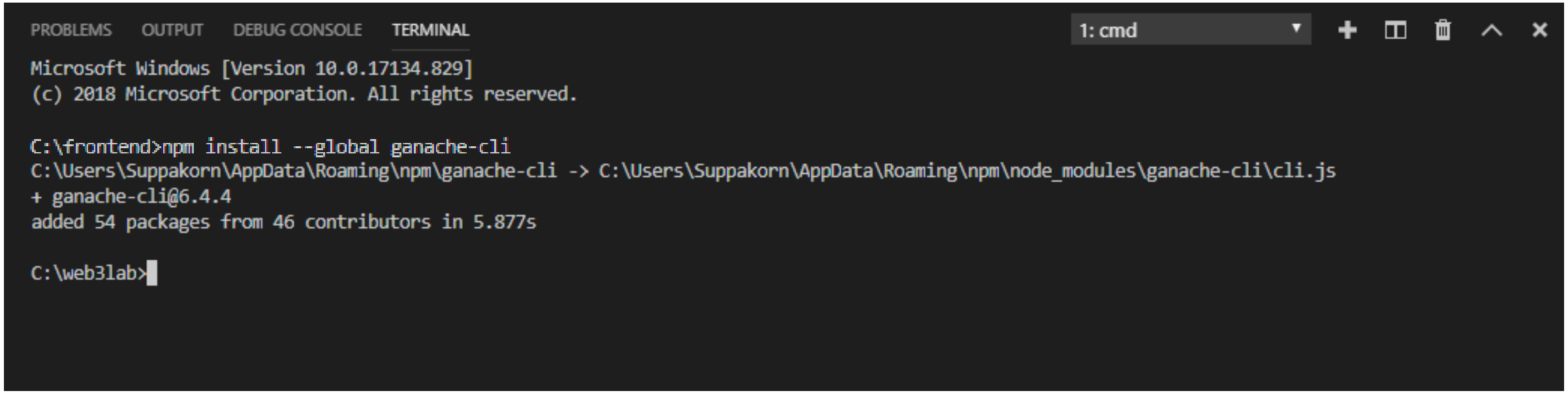
Geth Console

Command	Description
eth.blockNumber	View current block high
eth.getBlock(number)	Data of blok at that number
personal.unlockAccount(account)	Unlock the account
eth.sendtransaction({from:sender to:receiver value:amount})	Send amount wei(s) from sender to receiever
admin.nodeInfo	View node's info
admin.addPeer(enode_URL)	adding Peer using enode_URL
admin.peers	View peers' info

Install Ganache-cli

1. Open Terminal
2. Run command

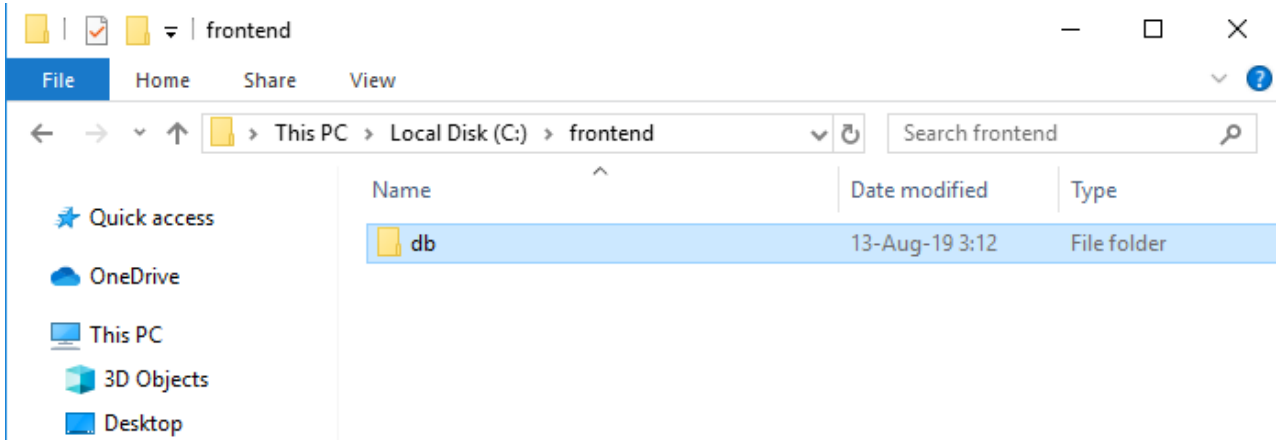
C:\web3lab>npm i -g ganache-cli



https://github.com/trufflesuite/ganache-cli

Start Ganache-cli

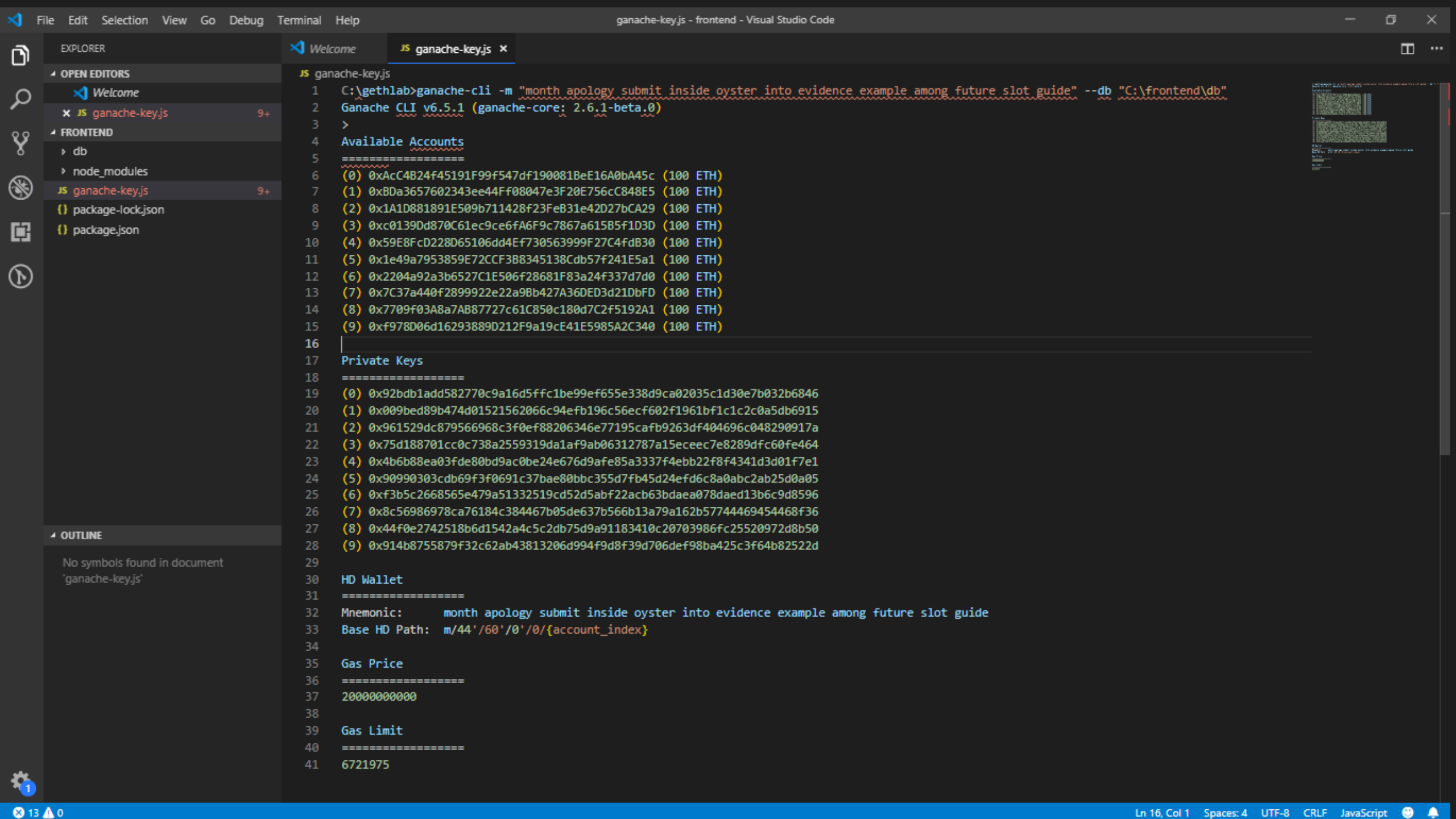
1. make folder C:\frontend\db



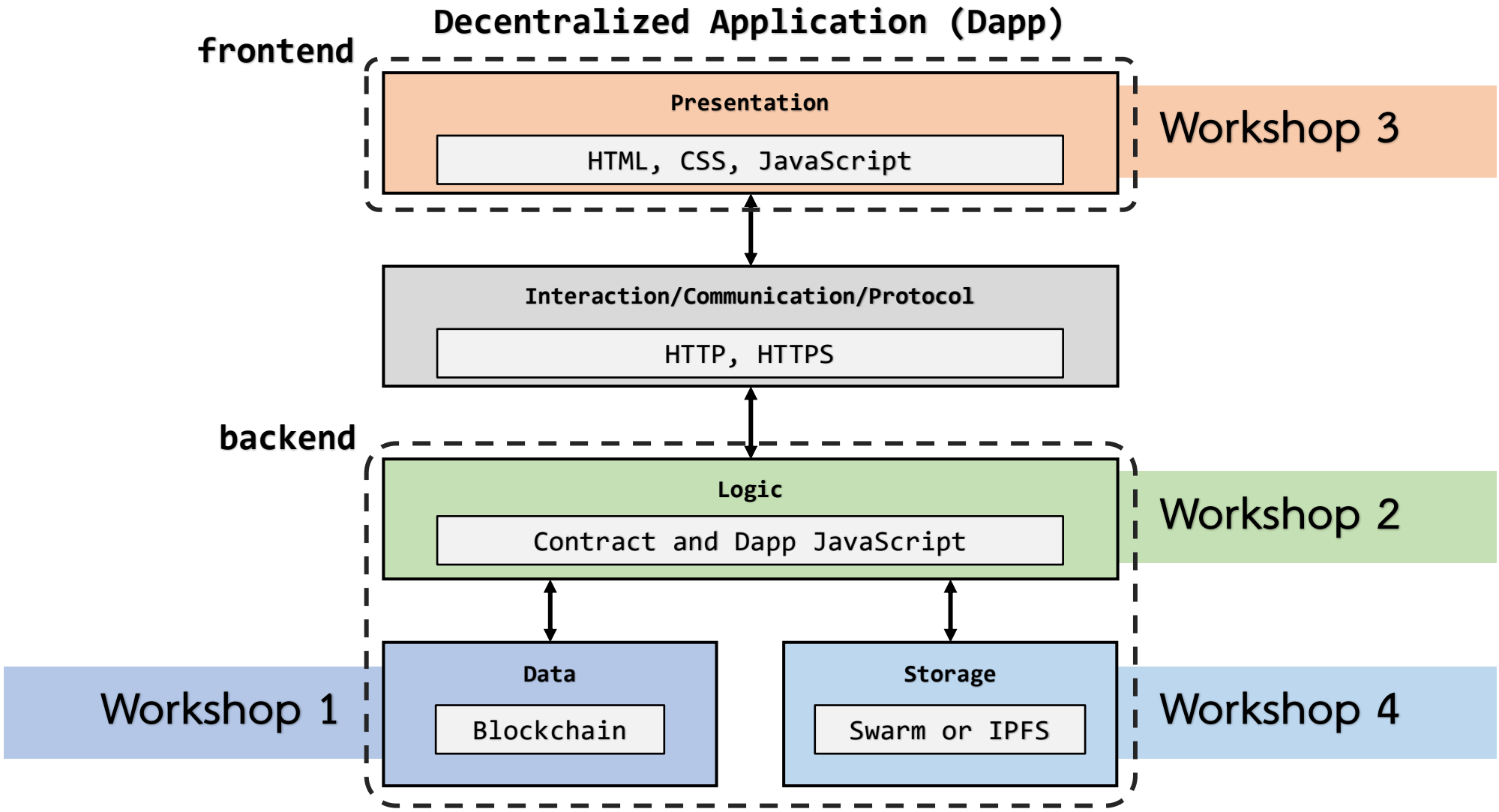
2. Run command

C:\frontend>ganache-cli -m "month apology submit inside oyster into evidence example among future slot guide" --db "C:\frontend\db"

```
(0) 0xAcC4B24f45191F99f547df190081BeE16A0bA45c (100 ETH)
(1) 0xBDa3657602343ee44Ff08047e3F20E756cC848E5 (100 ETH)
(2) 0x1A1D881891E509b711428f23FeB31e42D27bCA29 (100 ETH)
(3) 0xc0139Dd870C61ec9ce6fA6F9c7867a615B5f1D3D (100 ETH)
(4) 0x59E8FcD228D65106dd4Ef730563999F27C4fdB30 (100 ETH)
(5) 0x1e49a7953859E72CCF3B8345138Cdb57f241E5a1 (100 ETH)
(6) 0x2204a92a3b6527C1E506f28681F83a24f337d7d0 (100 ETH)
(7) 0x7C37a440f2899922e22a9Bb427A36DED3d21DbFD (100 ETH)
(8) 0x7709f03A8a7AB87727c61C850c180d7C2f5192A1 (100 ETH)
(9) 0xf978D06d16293889D212F9a19cE41E5985A2C340 (100 ETH)

Private Keys
==================
(0) 0x92bdb1add582770c9a16d5ffc1be99ef655e338d9ca02035c1d30e7b032b6846
(1) 0x009bed89b474d01521562066c94efb196c56ecf602f1961bf1c1c2c0a5db6915
(2) 0x961529dc879566968c3f0ef88206346e77195cafb9263df404696c048290917a
(3) 0x75d188701cc0c738a2559319da1af9ab06312787a15eceec7e8289dfc60fe464
(4) 0x4b6b88ea03fde80bd9ac0be24e676d9afe85a3337f4ebb22f8f4341d3d01f7e1
(5) 0x90990303cdb69f3f0691c37bae80bbc355d7fb45d24efd6c8a0abc2ab25d0a05
(6) 0xf3b5c2668565e479a51332519cd52d5abf22acb63bdaea078daed13b6c9d8596
(7) 0x8c56986978ca76184c384467b05de637b566b13a79a162b57744469454468f36
(8) 0x44f0e2742518b6d1542a4c5c2db75d9a91183410c20703986fc25520972d8b50
(9) 0x914b8755879f32c62ab43813206d994f9d8f39d706def98ba425c3f64b82522d

HD Wallet
==================
Mnemonic:      month apology submit inside oyster into evidence example among future slot guide
Base HD Path:  m/44'/60'/0'/0/{account_index}

Gas Price
==================
20000000000

Gas Limit
==================
6721975

Listening on 127.0.0.1:8545
eth_blockNumber
eth_blockNumber
eth_getBlockByNumber
```


File Edit Selection View Go Debug Terminal Help
ganache-key.js - frontend - Visual Studio Code
EXPLORER
OPEN EDITORS
Welcome
ganache-key.js 9+
FRONTEND
db
node_modules
ganache-key.js 9+
package-lock.json
package.json
OUTLINE
No symbols found in document 'ganache-key.js'
Welcome
ganache-key.js
ganache-key.js
C:\gethlab>ganache-cli -m "month apology submit inside oyster into evidence example among future slot guide" --db "C:\frontend\db"
Ganache CLI v6.5.1 (ganache-core: 2.6.1-beta.0)
>
Available Accounts
==================
(0) 0xAcC4B24f45191F99f547df190081BeE16A0bA45c (100 ETH)
(1) 0xBDa3657602343ee44Ff08047e3F20E756cC848E5 (100 ETH)
(2) 0x1A1D881891E509b711428f23FeB31e42D27bCA29 (100 ETH)
(3) 0xc0139Dd870C61ec9ce6fA6F9c7867a615B5f1D3D (100 ETH)
(4) 0x59E8FcD228D65106dd4Ef730563999F27C4fdB30 (100 ETH)
(5) 0x1e49a7953859E72CCF3B8345138Cdb57f241E5a1 (100 ETH)
(6) 0x2204a92a3b6527C1E506f28681F83a24f337d7d0 (100 ETH)
(7) 0x7C37a440f2899922e22a9Bb427A36DED3d21DbFD (100 ETH)
(8) 0x7709f03A8a7AB87727c61C850c180d7C2f5192A1 (100 ETH)
(9) 0xf978D06d16293889D212F9a19cE41E5985A2C340 (100 ETH)
Private Keys
==================
(0) 0x92bdb1add582770c9a16d5ffc1be99ef655e338d9ca02035c1d30e7b032b6846
(1) 0x009bed89b474d01521562066c94efb196c56ecf602f1961bf1c1c2c0a5db6915
(2) 0x961529dc879566968c3f0ef88206346e77195cafb9263df404696c048290917a
(3) 0x75d188701cc0c738a2559319da1af9ab06312787a15eceec7e8289dfc60fe464
(4) 0x4b6b88ea03fde80bd9ac0be24e676d9afe85a3337f4ebb22f8f4341d3d01f7e1
(5) 0x90990303cdb69f3f0691c37bae80bbc355d7fb45d24efd6c8a0abc2ab25d0a05
(6) 0xf3b5c2668565e479a51332519cd52d5abf22acb63bdaea078daed13b6c9d8596
(7) 0x8c56986978ca76184c384467b05de637b566b13a79a162b57744469454468f36
(8) 0x44f0e2742518b6d1542a4c5c2db75d9a91183410c20703986fc25520972d8b50
(9) 0x914b8755879f32c62ab43813206d994f9d8f39d706def98ba425c3f64b82522d
HD Wallet
==================
Mnemonic: month apology submit inside oyster into evidence example among future slot guide
Base HD Path: m/44'/60'/0'/0/{account_index}
Gas Price
==================
20000000000
Gas Limit
==================
6721975
13 0
Ln 16, Col 1 Spaces: 4 UTF-8 CRLF JavaScript

Overview



https://file.scirp.org/pdf/JSEA_20161028140127798.pdf

Workshop 2 Solidity

workshop นี้ทำอะไร

1. เราจะเริ่มจากเรียน smart contract structure กันก่อน
2. แล้วจากนั้นเราจะเรียน solidity value type, function and constructor, special function and variable ผ่านตัวอย่าง lottery contract
3. เราจะเก็บตก trick & tip ต่างๆในการเขียน solidity

Smart Contract Structure

```
pragma solidity ^0.5.11;

contract Storage {

    uint256 public data;

    function setData(uint256 _data) public{
        data = _data;
    }
}
```

Pragma

```
pragma solidity ^0.5.11;

contract Storage {

    uint256 public data;

    function setData(uint256 _data) public{
        data = _data;
    }
}
```

Contract

```
pragma solidity ^0.5.11;

contract Storage {

    uint256 public data;

    function setData(uint256 _data) public{
        data = _data;
    }
}
```

Contract

Variable

```
pragma solidity ^0.5.11;

contract Storage {

    uint256 public data;

    function setData(uint256 _data) public{
        data = _data;
    }
}
```

State Variable

Function

```
pragma solidity ^0.5.11;

contract Storage {

    uint256 public data;

    function setData(uint256 _data) public{
        data = _data;
    }
}
```

Function

Smart Contract Structure

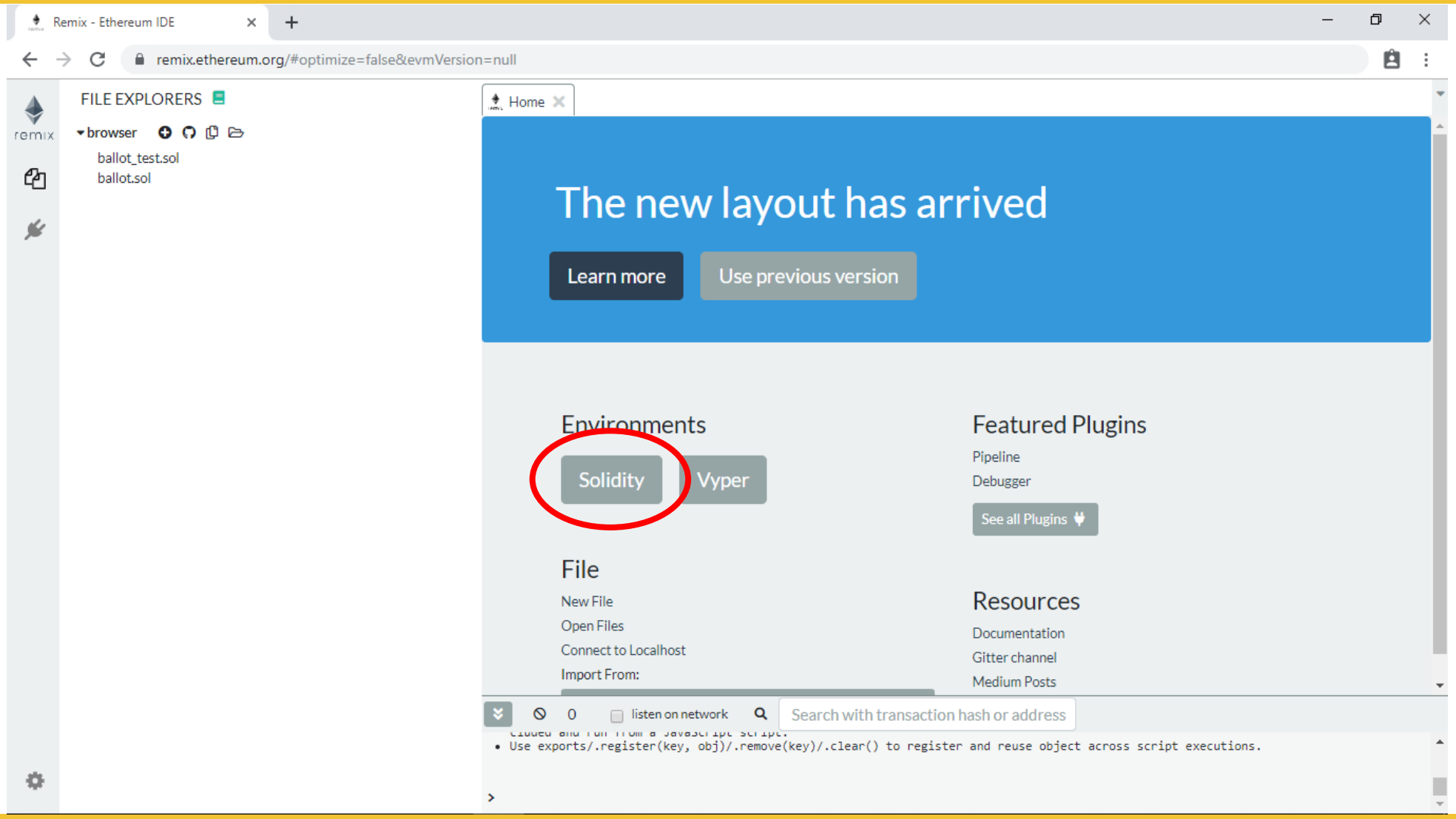
```
pragma solidity ^0.5.11;
```
Pragma

```
contract Storage {

    uint256 public data;

    function setData(uint256 _data) public{
        data = _data;
    }
}
```
Contract

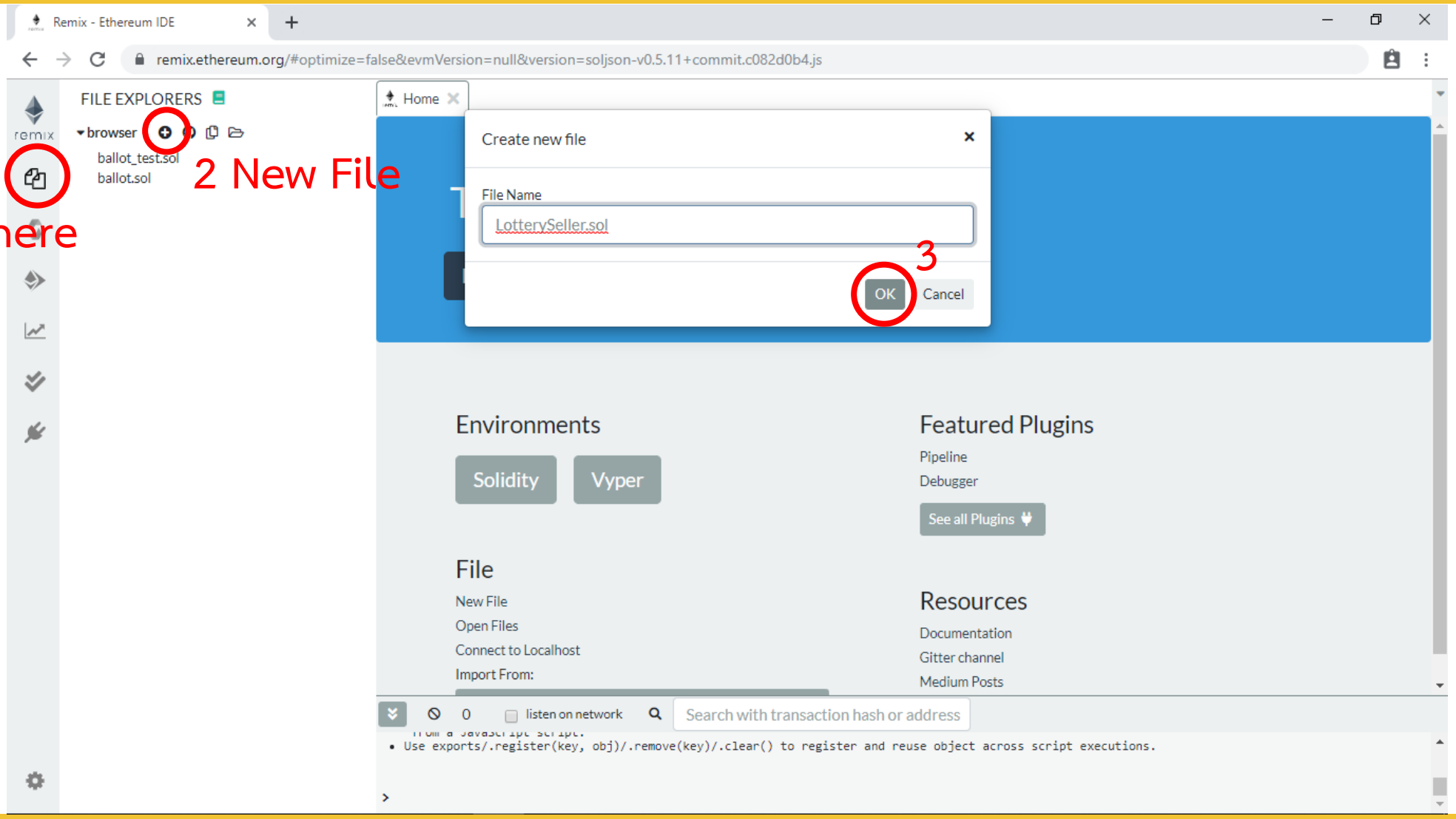
State Variable

Function

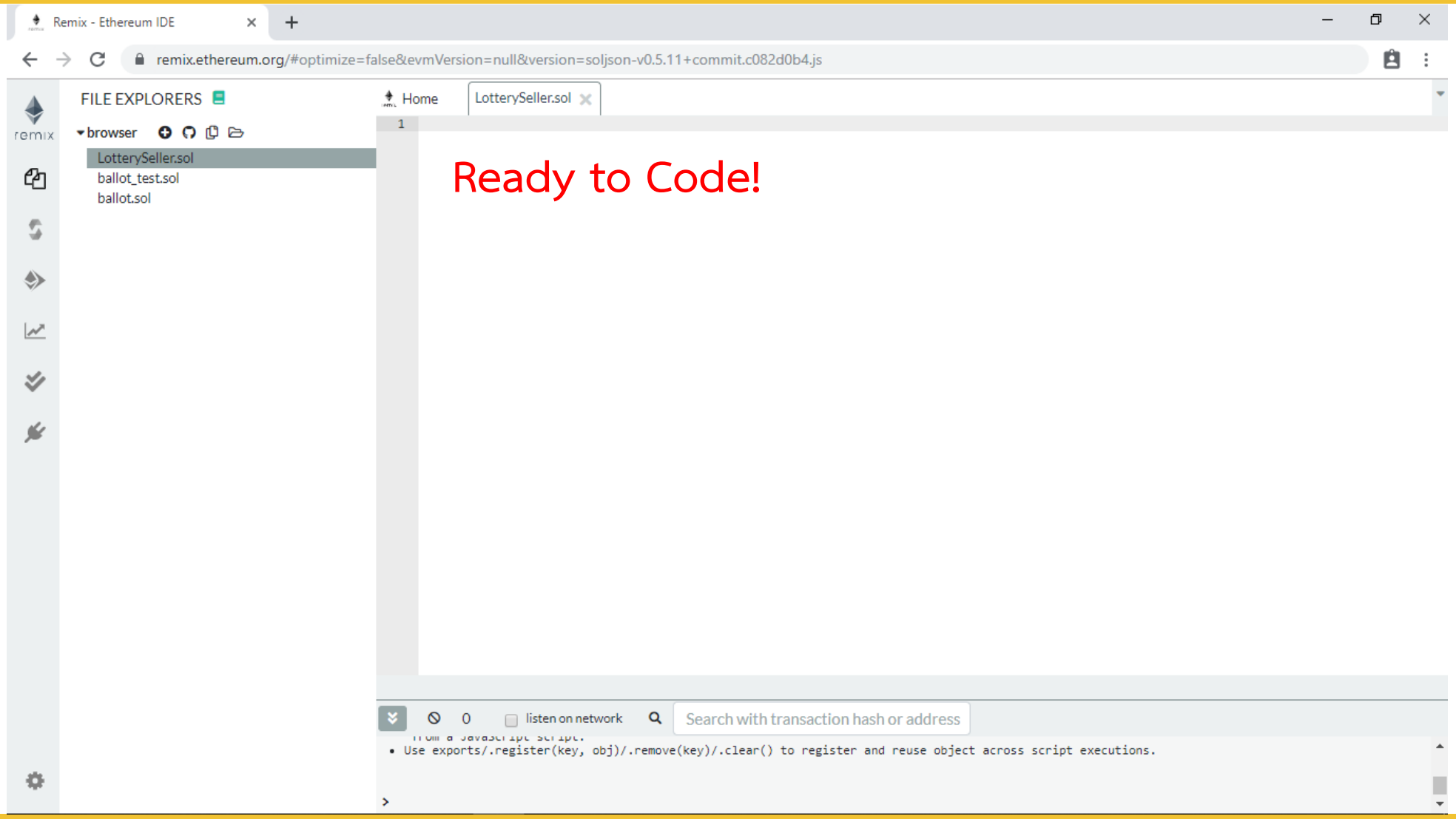
Editor: Remix-Ethereum



Editor: Remix-Ethereum



Editor: Remix-Ethereum



Learn By Example

https://solidity.readthedocs.io/en/v0.5.10/solidity-by-example.html

Smart Contract Outline

State Variable

- chairman
- price
- copy
- lottery
  - owner
  - sellCount

Function

- buy lottery
- how many left?
- check lottery owner
- check state
  - contract owner
  - price
  - copy

Smart Contract Outline

State Variable

- chairman **address**
- price **uint**
- copy **uint**
- lottery
  - owner
  - sellCount

} **Struct**

Function

- buy lottery
- how many left?
- check lottery owner
- check state
  - contract owner
  - price
  - copy

State Variable

```
pragma solidity ^0.5.11;
contract LotteryShop{
    struct Lottery{
        address[] lotteryOwner;
        uint sellCount ;
    }

    Lottery[1000000] public lottery;
    uint public copy;
    uint public price;
    address public contractOwner;

}
```

Variable Type

Type Visibility Variable Name

```
uint256 public price;
```

Type Visibility Variable Name

```
address[1000000] public lottery;
```

Variable Type

Type	Example
bool	bool isTrue = true;
int_size	int number = -100;
uint_size	uint number = 100;
string	string message = “Hello, World!”;
address	address wallet = 0xca35b7d915458ef540ade6068dfe2f44e8fa733c;
bytes_size	bytes code = 0x4beef;

https://solidity.readthedocs.io/en/v0.5.10/types.html

Variable Type

Type	Example
enum ★★	enum state{Created, Locked, Inactive};
ArrayType[_size]	uint[] set_of_Numbers;
struct _name{ _type _name; _type _name; }	struct Student{ string name; uint age; }
mapping(_key=>_value) ★★	mapping(address=>uint) wallet;

https://solidity.readthedocs.io/en/v0.5.10/types.html

Smart Contract Outline

State Variable

- chairman — **address**
- price — **uint**
- copy — **uint**
- lottery — **Struct**
  - owner
  - sellCount

Function

- buy lottery
- how many left?
- check lottery owner
- check state
  - contract owner
  - price
  - copy

constructor

```
pragma solidity ^0.5.11;
contract LotteryShop {
 //state variables done!

 constructor(uint _copy,uint _price) public{
        copy = _copy;
        price = _price;
        contractOwner = msg.sender;
    }
}
```

Constructor

```
constructor (<arguments>) public  {}
```

A constructor is a special method that is used to initialize a newly created object.

After the constructor has executed, the final code of the contract is deployed to the blockchain.

getOwner

```
pragma solidity ^0.5.11;

contract LotteryShop {
 //state variables done!
 //constructor done!

 function getOwner(uint _number)public view returns(address[] memory){
        return lottery[_number].lotteryOwner;
    }
}
```

Function

```
function _name(<input_arguments>)
      {visibility}
      {state mutability}
      {modifier}★★
      returns(<return_parameter>){}
```

public - all can access

private - can be accessed only from this contract

internal - can be accessed only from this contract and its subclasses

external - can be accessed only from other contracts

https://solidity.readthedocs.io/en/v0.5.10/contracts.html#view-functions

state mutability

Mutability	Read	Modify	note	Use Case
-none-	yes	yes	-	setter
payable	yes	yes	can received ETH!	deposit, purchase
view	yes	no	Free!	getter
pure	no	no	Free!	helper

https://solidity.readthedocs.io/en/v0.5.10/contracts.html#view-functions

Smart Contract Outline

State Variable

- chairman **address**
- price **uint**
- copy **uint**
- lottery **Struct**
  - owner
  - sellCount

Function

- buy lottery **payable**
- how many left? **view**
- check lottery owner **view**
- check state
  - contract owner
  - price
  - copy

howManyLeft

```
pragma solidity ^0.5.11;
contract LotteryShop {
 //...

 function howManyLeft(uint _number)public view returns(uint){
        require(_number<1000000,"we do not have the number");
        return copy-lottery[_number].sellCount;
    }
}
```

Require

require(bool condition, string memory message)

-if condition is false, abort the execution, revert state changes and return all the remaining gas to the sender. Also provides an error message

msg.sender - sender of the message (current call)

msg.value - number of wei sent with the message

https://solidity.readthedocs.io/en/v0.5.10/units-and-global-variables.html

Smart Contract Outline

State Variable

- chairman — **address**
- price — **uint**
- copy — **uint**
- lottery — **Struct**
  - owner
  - sellCount

Function

- buy lottery — **payable**
- how many left? — **view**
- check lottery owner — **view**
- check state
  - contract owner
  - price
  - copy

buyLottery

```
pragma solidity ^0.5.11;
contract LotteryShop {
 //...

 function buyLottery(uint _number)public payable{
        require(msg.sender != address(0),"address(0) is not allowed");
        require(msg.value == price,"payment must be equal to price");
        require(lottery[_number].sellCount < copy,"soldout");
        require(_number<1000000,"we do not have the number");
        lottery[_number].lotteryOwner.push(msg.sender);
        lottery[_number].sellCount ++;
    }

}
```

Smart Contract Outline

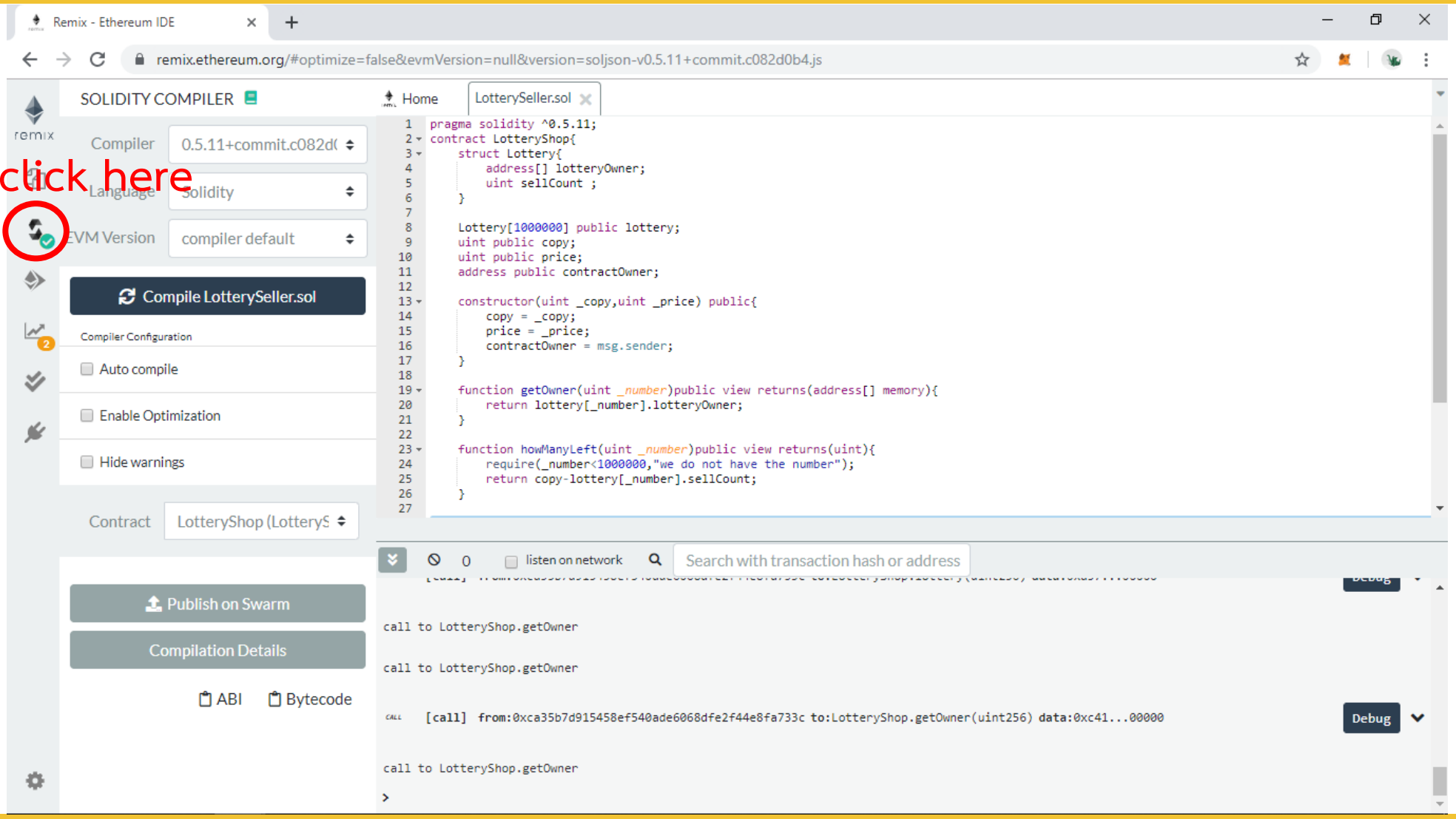
State Variable

- chairman — **address**
- price — **uint**
- copy — **uint**
- lottery — **Struct**
  - owner
  - sellCount

Function

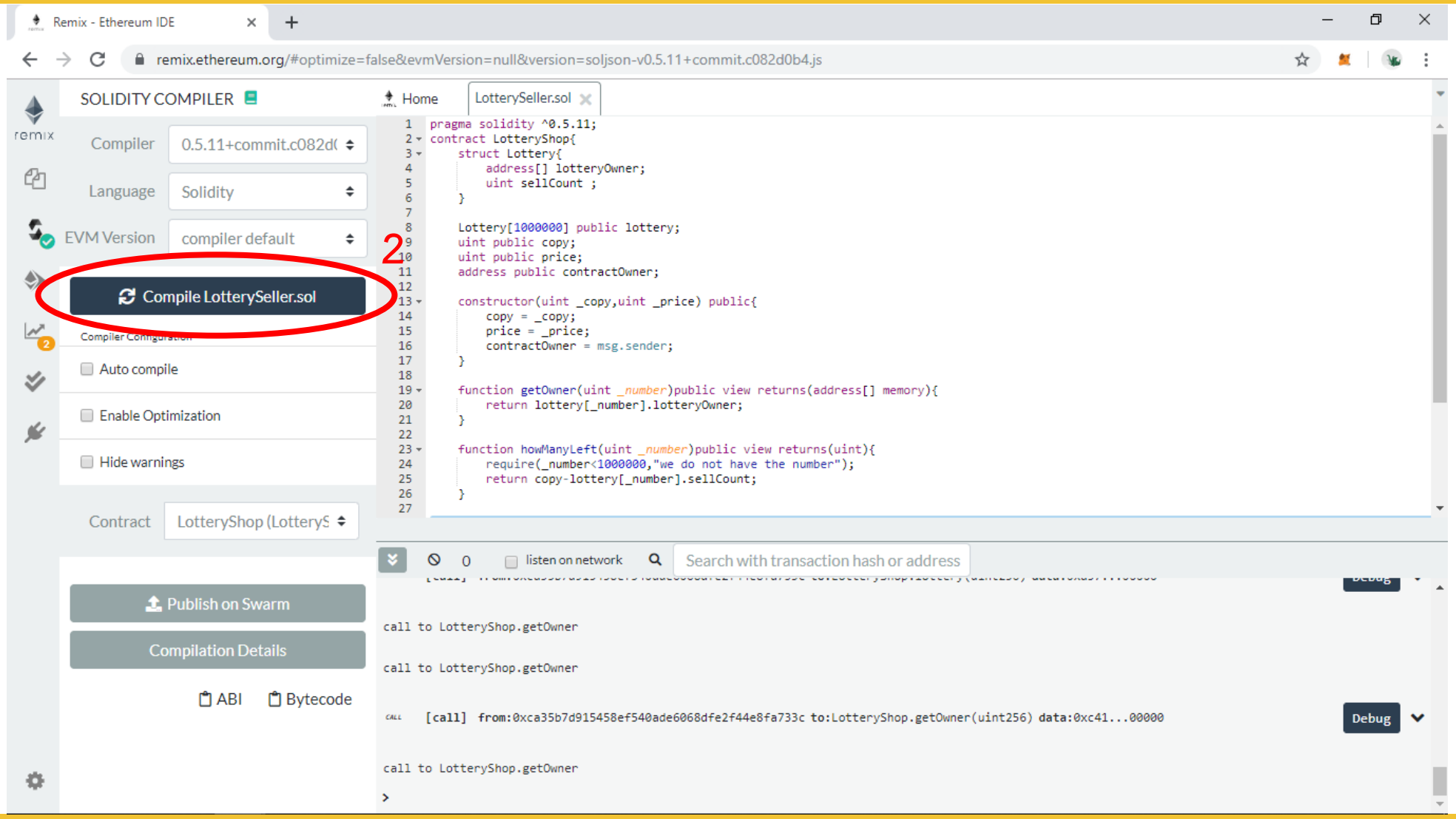
- buy lottery — **payable**
- how many left? — **view**
- check lottery owner — **view**
- check state
  - contract owner
  - price
  - copy

Compile

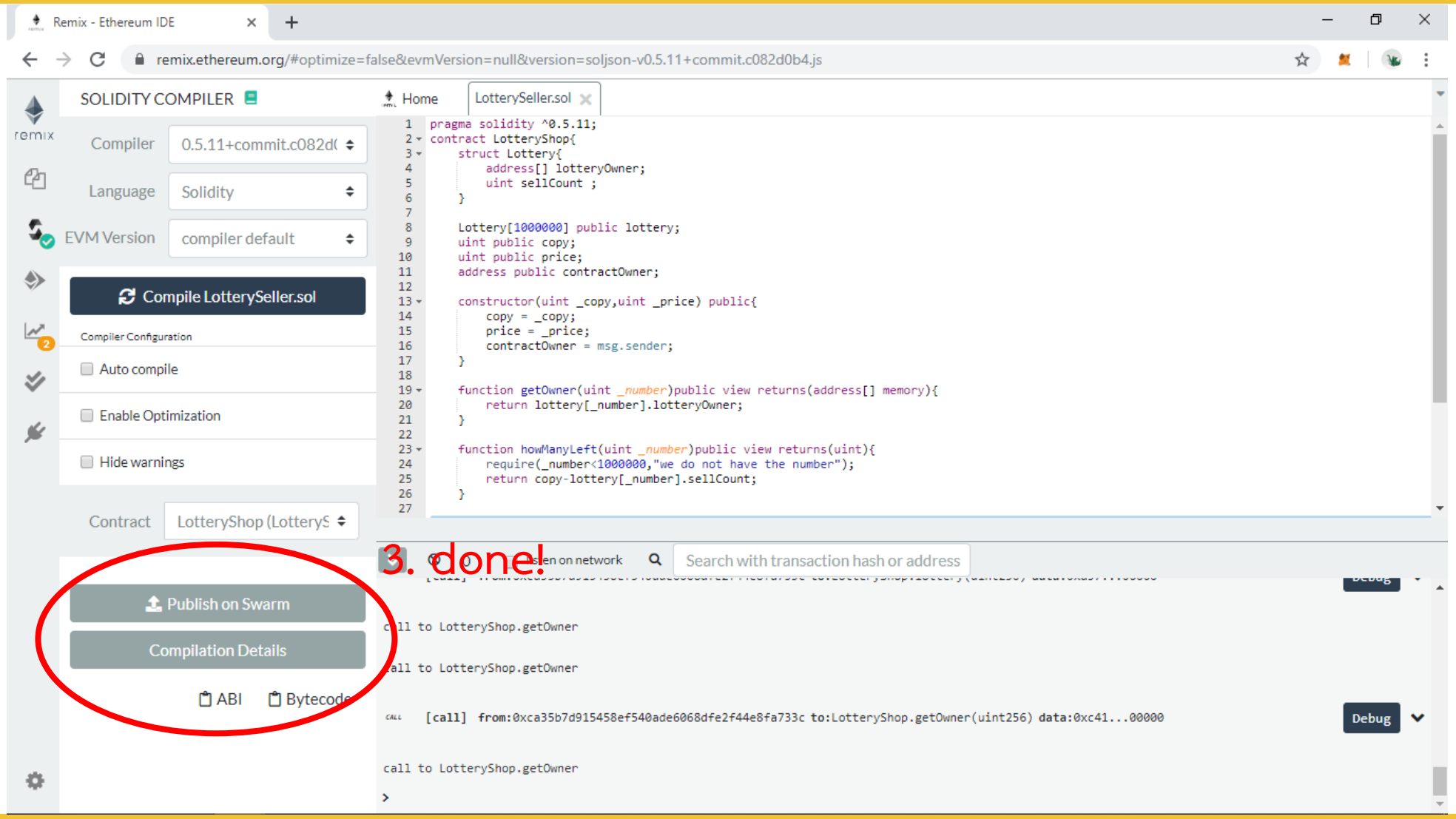


1.click here

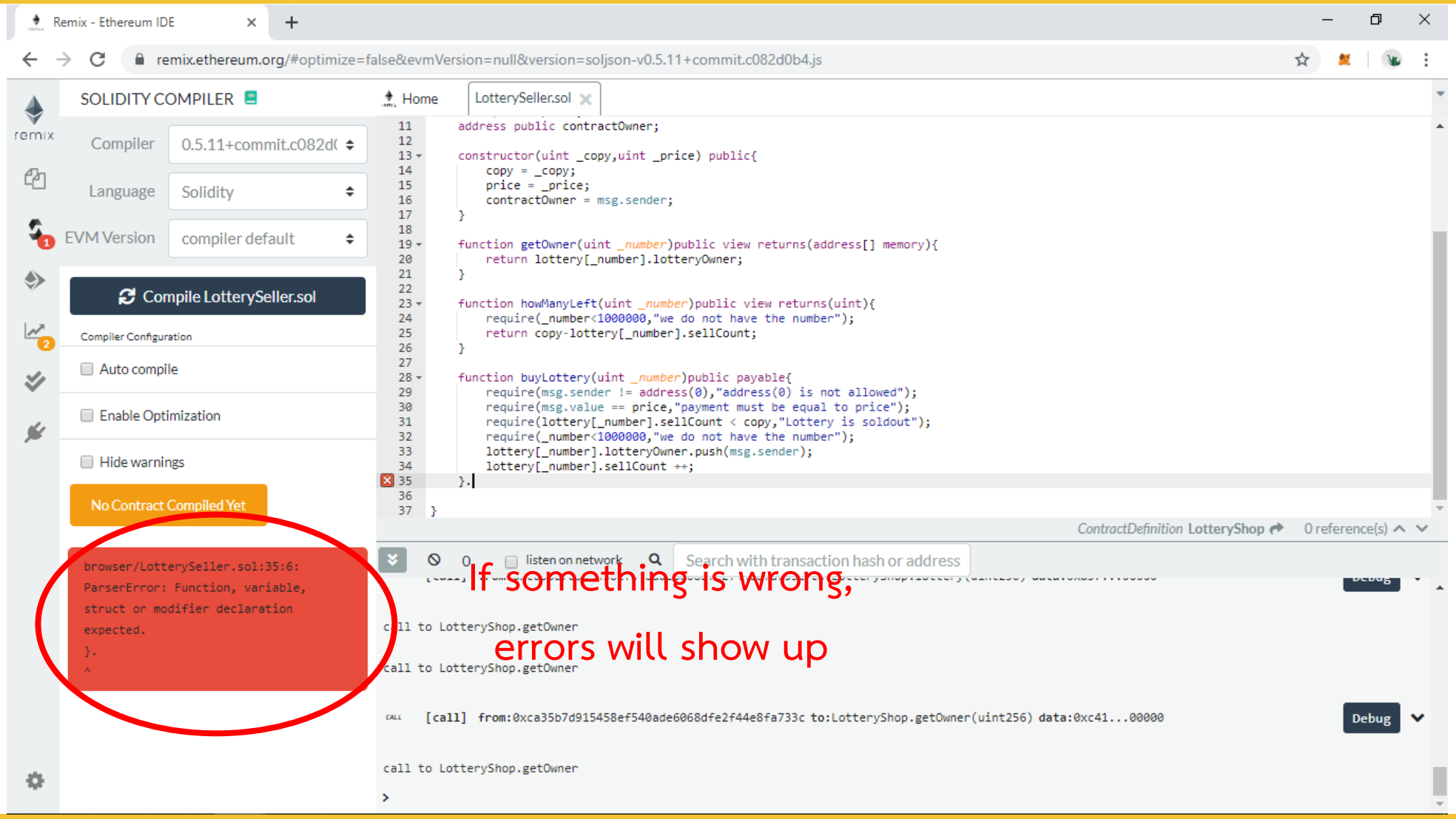
Compile


Remix - Ethereum IDE
remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.5.11+commit.c082d0b4.js
SOLIDITY COMPILER
Compiler
0.5.11+commit.c082d(
Language
Solidity
EVM Version
compiler default
2
Compile LotterySeller.sol
Compiler Configuration
Auto compile
Enable Optimization
Hide warnings
Contract
LotteryShop (LotteryS
Publish on Swarm
Compilation Details
ABI
Bytecode
Home
LotterySeller.sol
pragma solidity ^0.5.11;
contract LotteryShop{
struct Lottery{
address[] lotteryOwner;
uint sellCount ;
}
Lottery[1000000] public lottery;
uint public copy;
uint public price;
address public contractOwner;
constructor(uint _copy,uint _price) public{
copy = _copy;
price = _price;
contractOwner = msg.sender;
}
function getOwner(uint _number)public view returns(address[] memory){
return lottery[_number].lotteryOwner;
}
function howManyLeft(uint _number)public view returns(uint){
require(_number<1000000,"we do not have the number");
return copy-lottery[_number].sellCount;
}
}
0
listen on network
Search with transaction hash or address
call to LotteryShop.getOwner
call to LotteryShop.getOwner
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:LotteryShop.getOwner(uint256) data:0xc41...00000
Debug
call to LotteryShop.getOwner
>

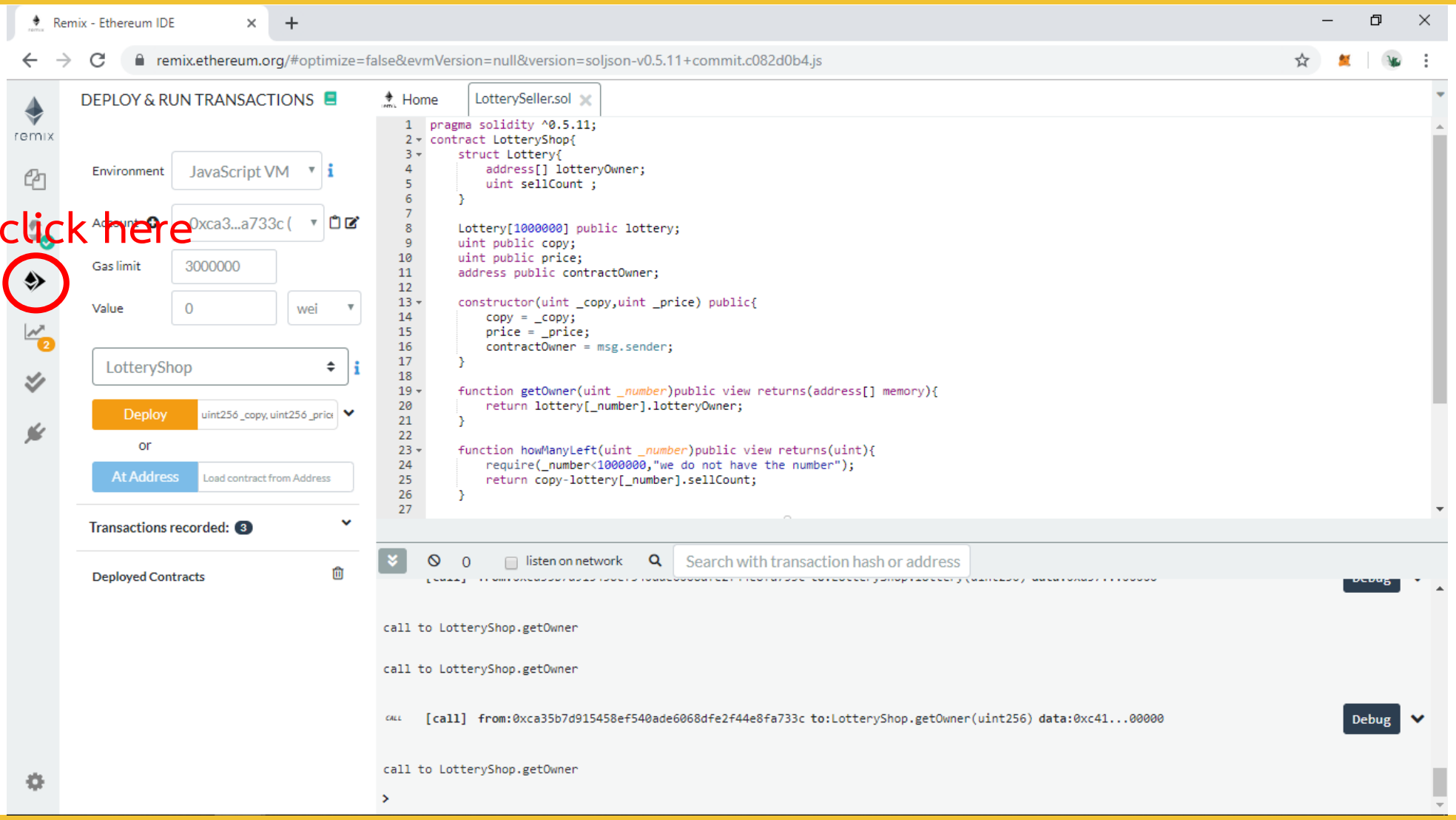
Compile


Remix - Ethereum IDE
remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.5.11+commit.c082d0b4.js
SOLIDITY COMPILER
Compiler
0.5.11+commit.c082d(
Language
Solidity
EVM Version
compiler default
Compile LotterySeller.sol
Compiler Configuration
Auto compile
Enable Optimization
Hide warnings
Contract
LotteryShop (LotteryS
Publish on Swarm
Compilation Details
ABI
Bytecode
Home
LotterySeller.sol
pragma solidity ^0.5.11;
contract LotteryShop{
struct Lottery{
address[] lotteryOwner;
uint sellCount ;
}
Lottery[1000000] public lottery;
uint public copy;
uint public price;
address public contractOwner;
constructor(uint _copy,uint _price) public{
copy = _copy;
price = _price;
contractOwner = msg.sender;
}
function getOwner(uint _number)public view returns(address[] memory){
return lottery[_number].lotteryOwner;
}
function howManyLeft(uint _number)public view returns(uint){
require(_number<1000000,"we do not have the number");
return copy-lottery[_number].sellCount;
}
}
3. done!
Search with transaction hash or address
call to LotteryShop.getOwner
call to LotteryShop.getOwner
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:LotteryShop.getOwner(uint256) data:0xc41...00000
Debug
call to LotteryShop.getOwner

Compile

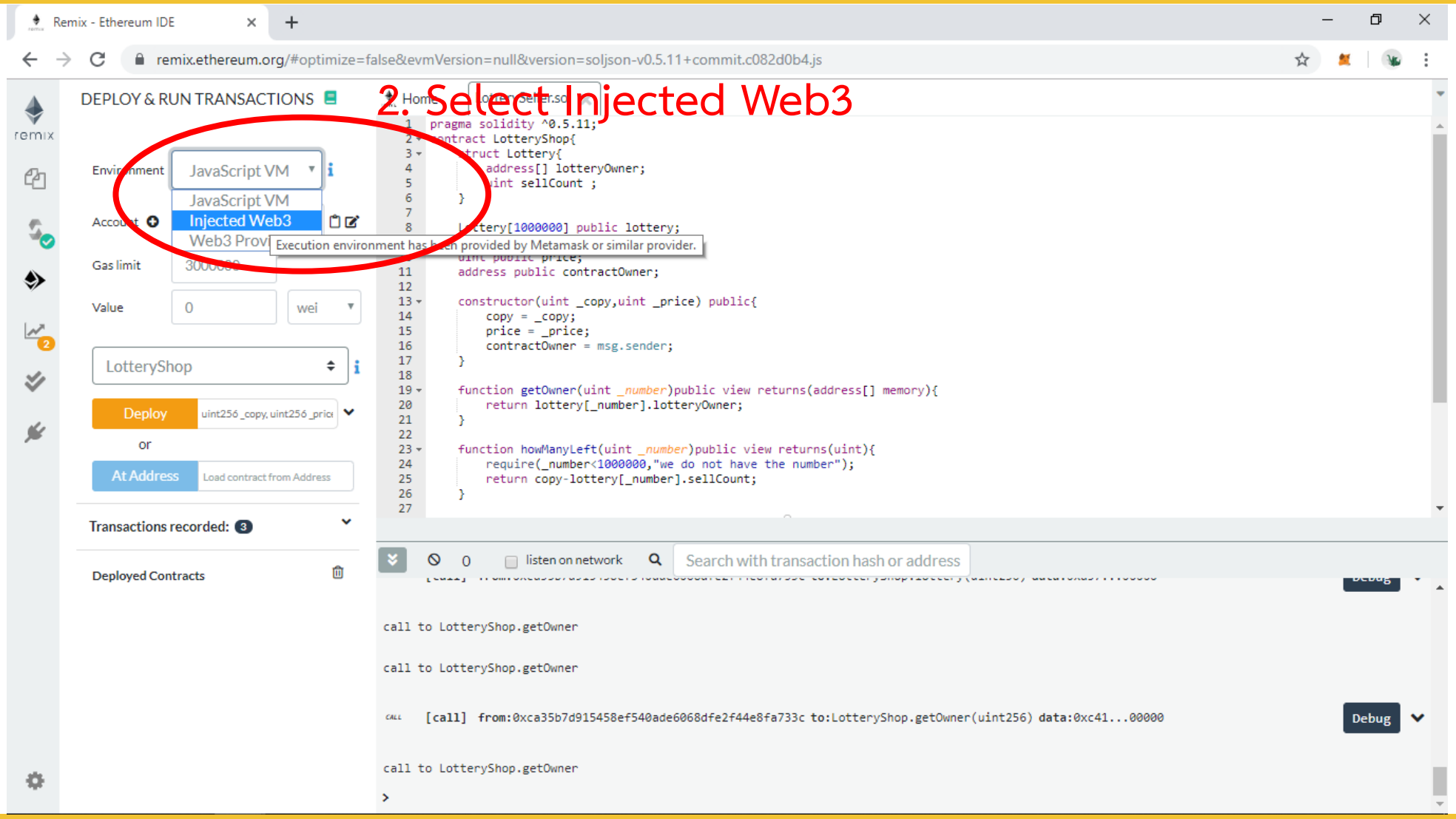

Remix - Ethereum IDE
remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.5.11+commit.c082d0b4.js
SOLIDITY COMPILER
Compiler
0.5.11+commit.c082d(
Language
Solidity
EVM Version
compiler default
Compile LotterySeller.sol
Compiler Configuration
Auto compile
Enable Optimization
Hide warnings
No Contract Compiled Yet
browser/LotterySeller.sol:35:6:
ParserError: Function, variable,
struct or modifier declaration
expected.
}.
^
Home
LotterySeller.sol
address public contractOwner;
constructor(uint _copy,uint _price) public{
copy = _copy;
price = _price;
contractOwner = msg.sender;
}
function getOwner(uint _number)public view returns(address[] memory){
return lottery[_number].lotteryOwner;
}
function howManyLeft(uint _number)public view returns(uint){
require(_number<1000000,"we do not have the number");
return copy-lottery[_number].sellCount;
}
function buyLottery(uint _number)public payable{
require(msg.sender != address(0),"address(0) is not allowed");
require(msg.value == price,"payment must be equal to price");
require(lottery[_number].sellCount < copy,"Lottery is soldout");
require(_number<1000000,"we do not have the number");
lottery[_number].lotteryOwner.push(msg.sender);
lottery[_number].sellCount ++;
}.
}
ContractDefinition LotteryShop
0 reference(s)
listen on network
Search with transaction hash or address
If something is wrong,
errors will show up
call to LotteryShop.getOwner
call to LotteryShop.getOwner
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:LotteryShop.getOwner(uint256) data:0xc41...00000
Debug
call to LotteryShop.getOwner

Deploy

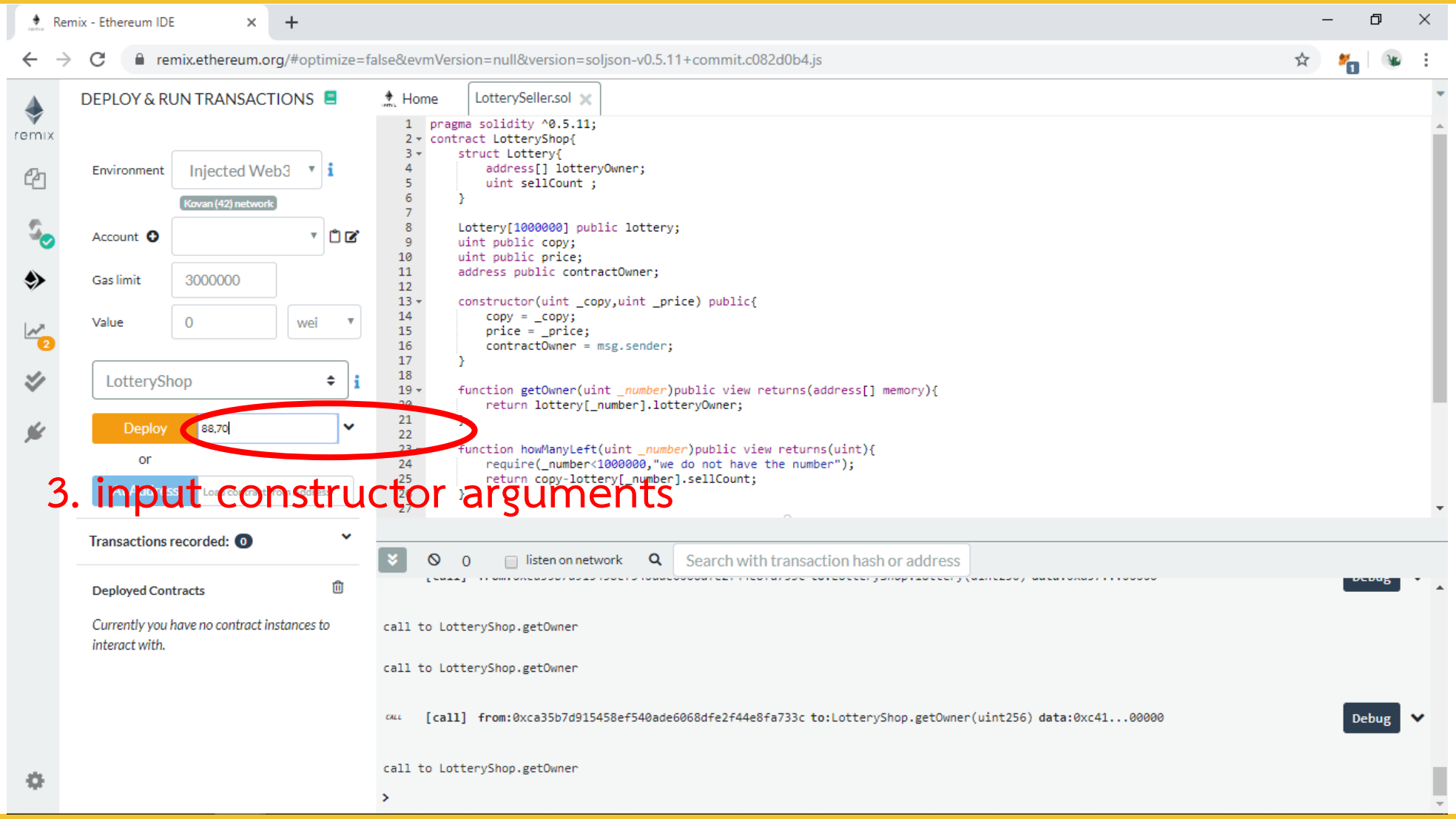


1.click here

Deploy

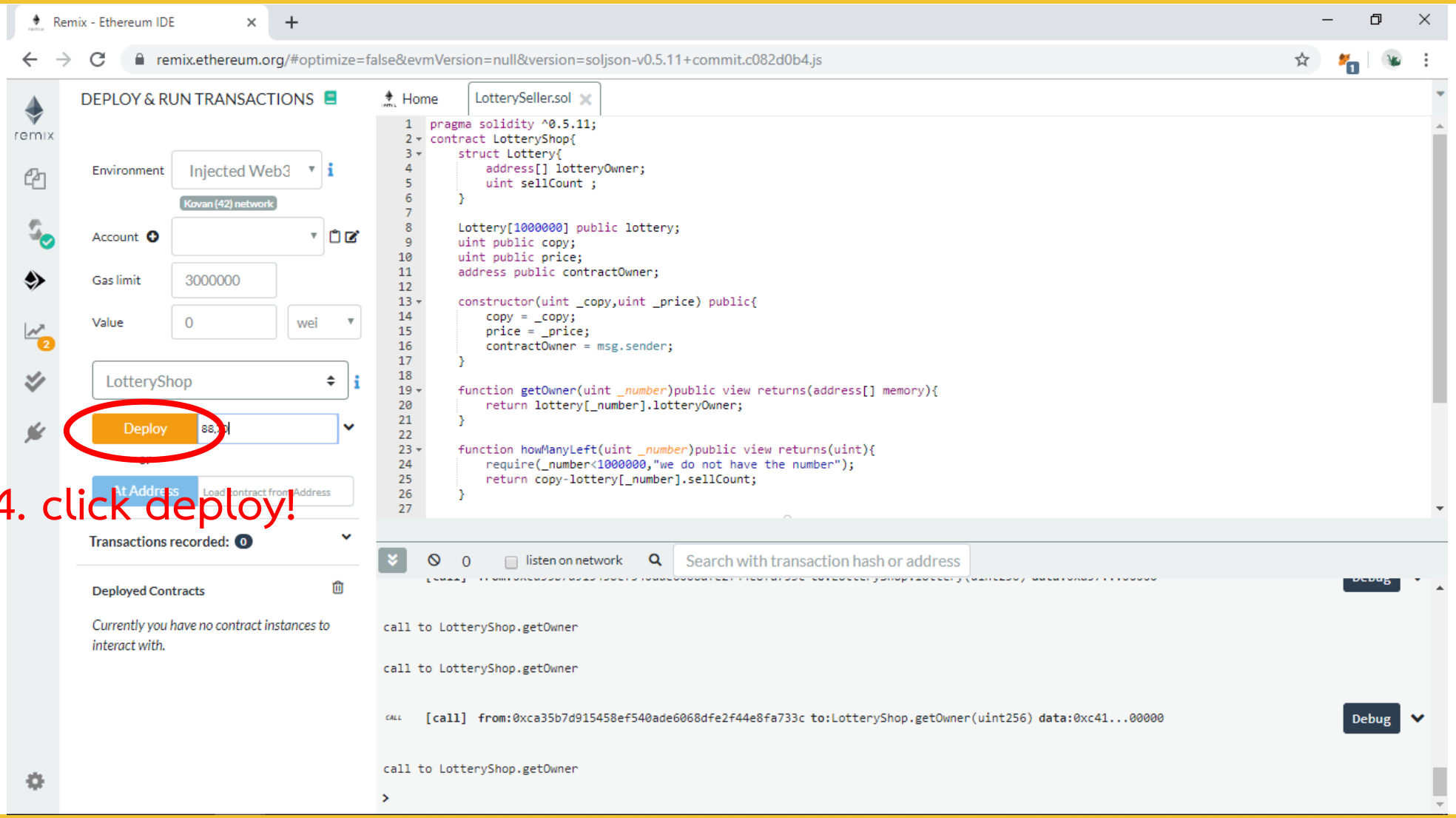

Remix - Ethereum IDE
remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.5.11+commit.c082d0b4.js
DEPLOY & RUN TRANSACTIONS
2. Select Injected Web3
Environment
JavaScript VM
JavaScript VM
Injected Web3
Web3 Provider
Execution environment has been provided by Metamask or similar provider.
Account
Gas limit
Value
0
wei
LotteryShop
Deploy
uint256 _copy, uint256 _price
or
At Address
Load contract from Address
Transactions recorded: 3
Deployed Contracts
pragma solidity ^0.5.11;
contract LotteryShop{
struct Lottery{
address[] lotteryOwner;
uint sellCount ;
}
Lottery[1000000] public lottery;
uint public price;
address public contractOwner;
constructor(uint _copy,uint _price) public{
copy = _copy;
price = _price;
contractOwner = msg.sender;
}
function getOwner(uint _number)public view returns(address[] memory){
return lottery[_number].lotteryOwner;
}
function howManyLeft(uint _number)public view returns(uint){
require(_number<1000000,"we do not have the number");
return copy-lottery[_number].sellCount;
}
0
listen on network
Search with transaction hash or address
call to LotteryShop.getOwner
call to LotteryShop.getOwner
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:LotteryShop.getOwner(uint256) data:0xc41...00000
Debug
call to LotteryShop.getOwner

Deploy



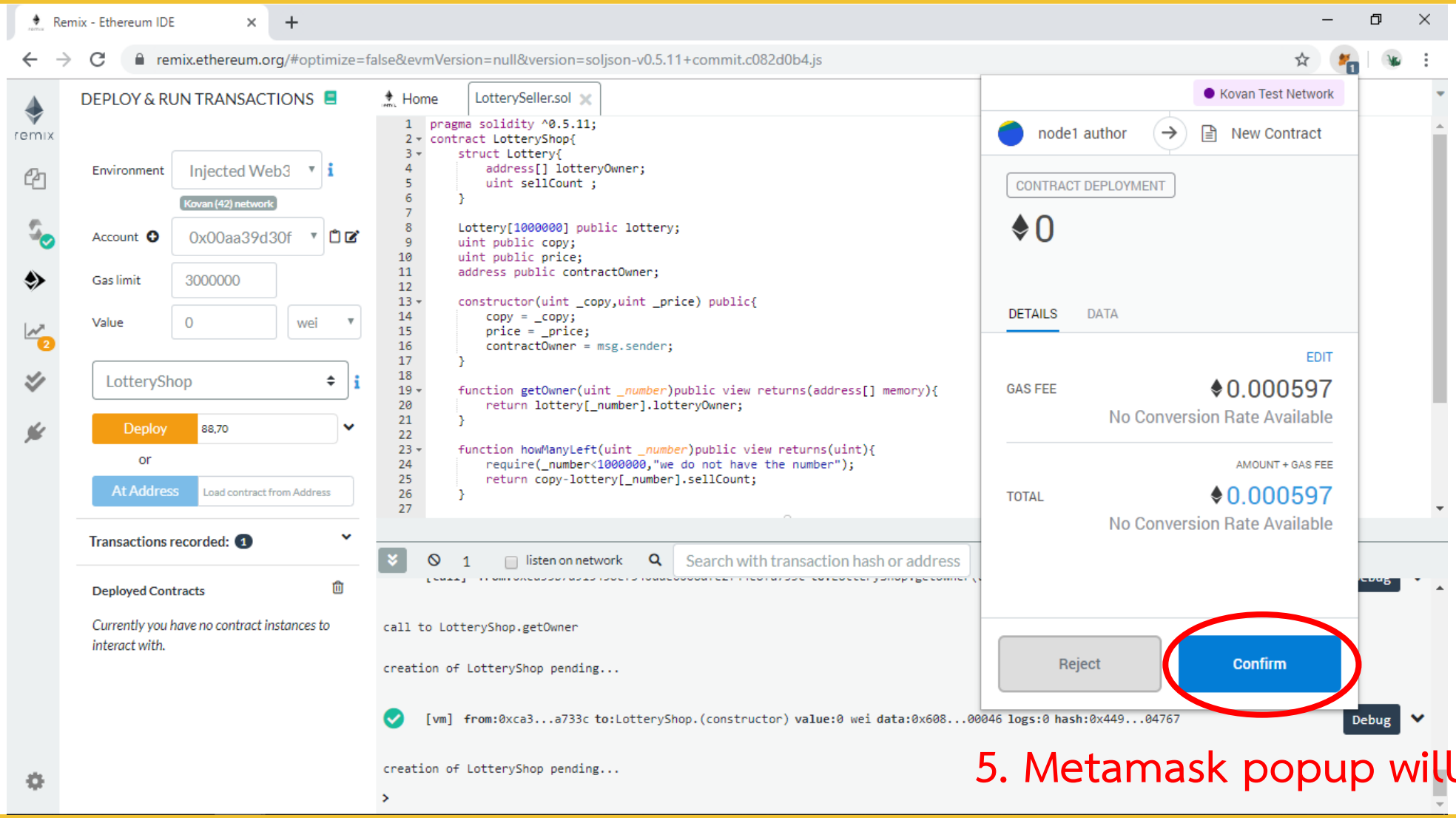
3. input constructor arguments

Deploy



4. click deploy!

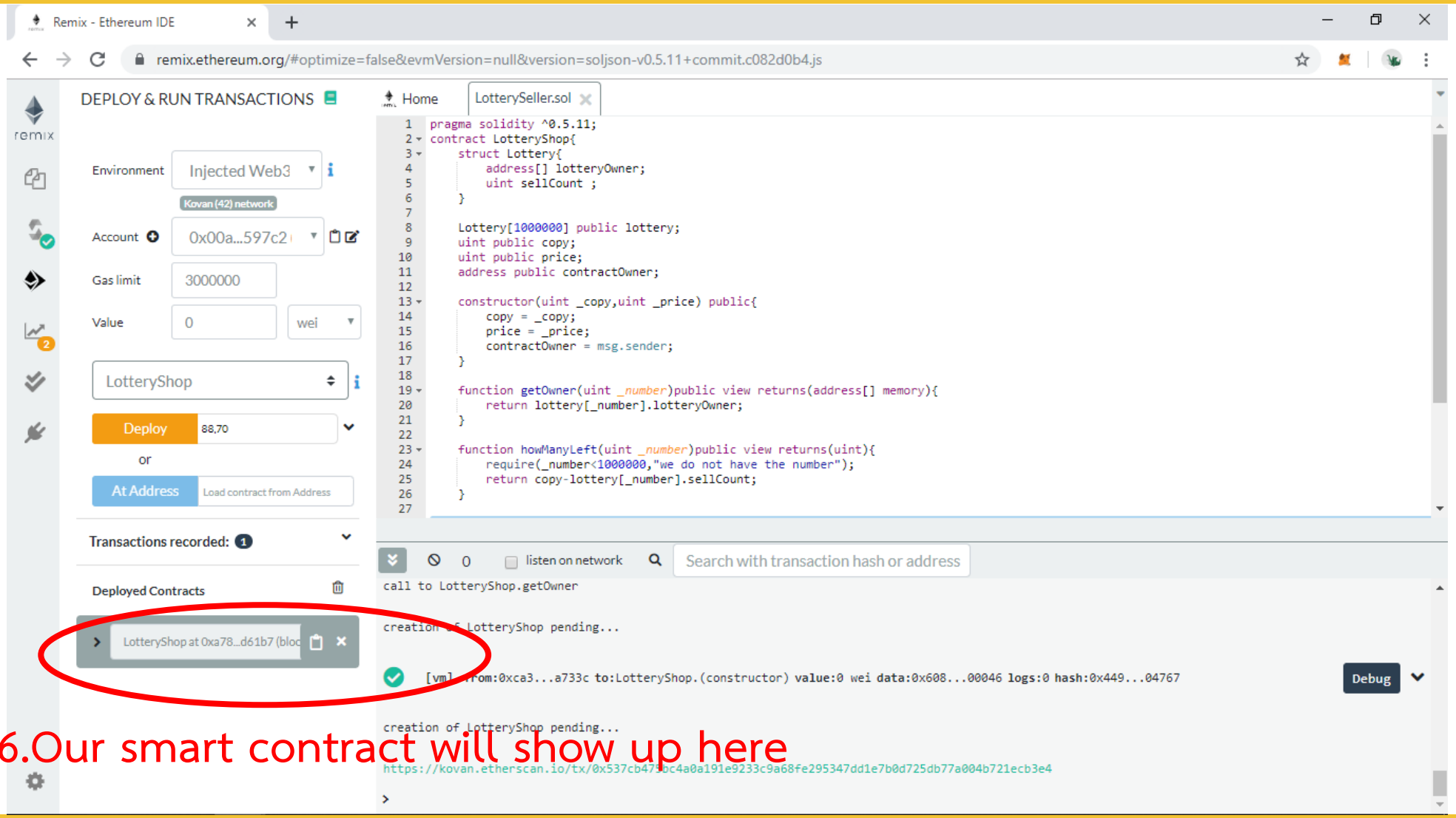
Deploy



5. Metamask popup will show up

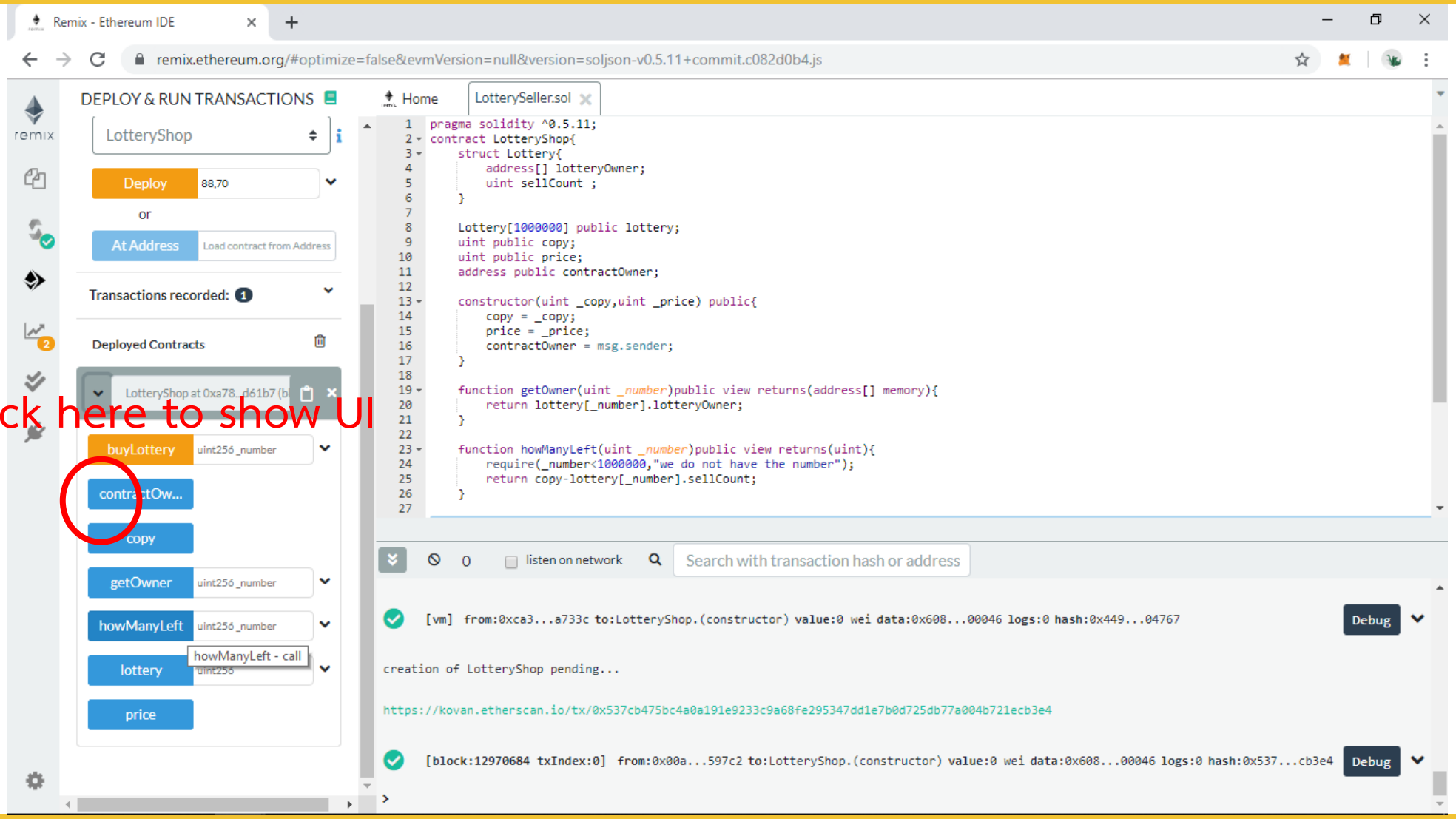
click Confirm to continue

Deploy



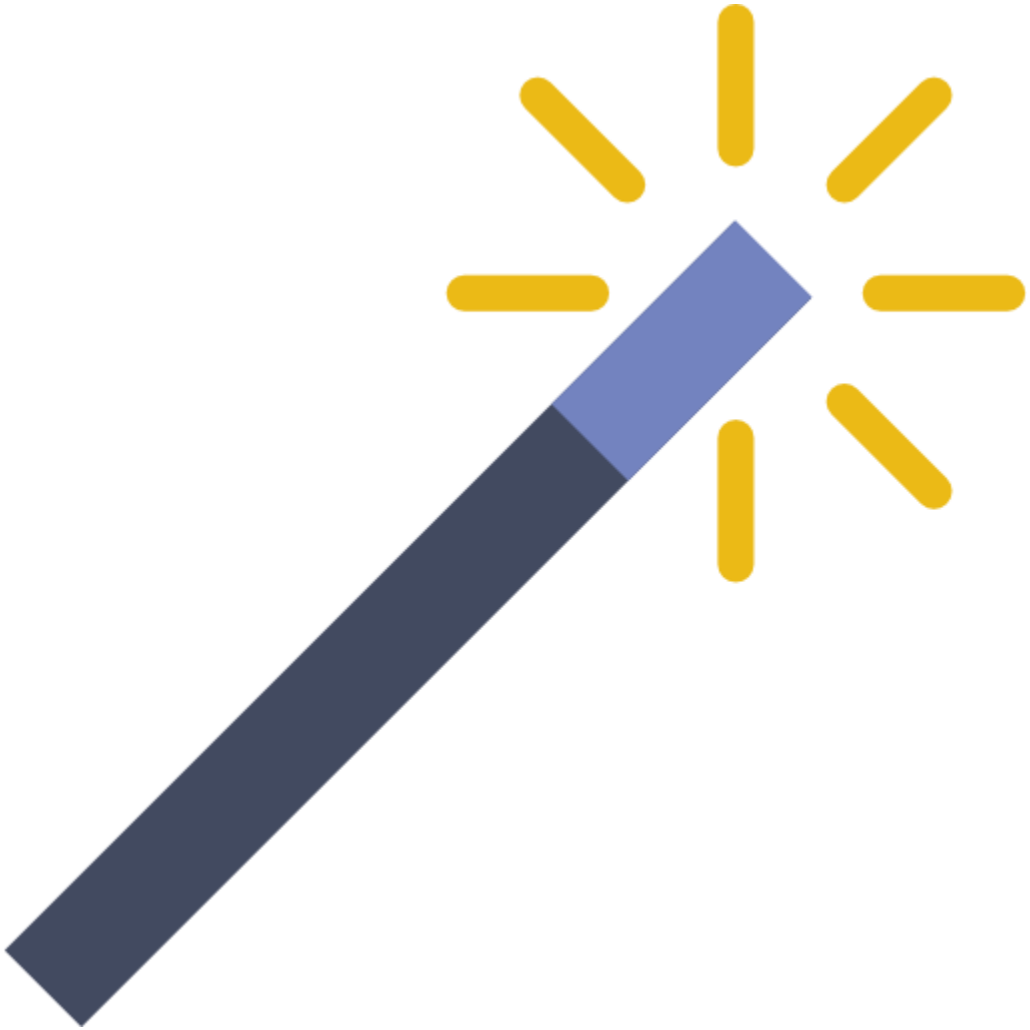
6.Our smart contract will show up here

Deploy



7. click here to show UI

Tip & Tricks



Mapping

value Type key Variable Name Variable Name key value

```
address[5] wallet;        wallet[4]= 0xaA;
```

key value Type Variable Name

```
mapping(uint => address) wallet;
```

Mapping

```
mapping(string => string) dictionary;

dictionary["ant"]="a small insect";
```

Mapping

key value Type Variable Name

```
mapping(string => string) dictionary;
```

Variable Name key value

```
dictionary["ant"]="a small insect";
```

Mapping

key value Type Variable Name

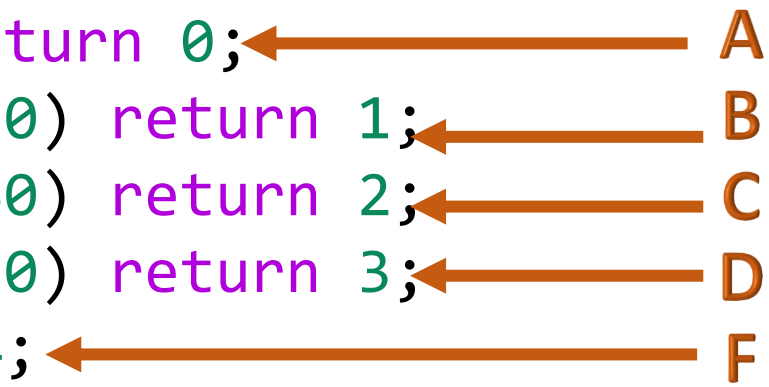
```
mapping(address => uint) score;
```

Variable Name key value

```
score[0x045ad]= 99;
```

Enum

```
pragma solidity ^0.5.11;
contract test{
    mapping(address => uint) score;


   function getGrade(address student)public view returns (uint){
       uint a = score[student];
       if(a > 80) return 0;
       else if(a > 70) return 1;
       else if(a > 60) return 2;
       else if(a > 50) return 3;
       else return 4;
   }
}
```



Enum

```
pragma solidity ^0.5.11;
contract test{
    mapping(address => uint) score;
    enum grade {A,B,C,D,F}

   function getGrade(address student)public view returns (grade){
       uint a = score[student];
       if(a > 80) return grade.A;
       else if(a > 70) return grade.B;
       else if(a > 60) return grade.C;
       else if(a > 50) return grade.D;
       else return grade.F;
   }
}
```

Modifer

```
contract test{
    address owner;
    constructor()public{
        owner = msg.sender;
    }
    function superPower1()public{
        require(msg.sender == owner);
        //...
    }
    function superPower2()public{
        require(msg.sender == owner);
        //...
    }
}
```

Modifer

```
contract test{
    address owner;
    constructor()public{
        owner = msg.sender;
    }
    modifier onlyOwner{
        require(msg.sender==owner);
        _;
    }
    function superPower1()public onlyOwner{
        //...
    }
    function superPower2()public onlyOwner{
        //...
    }
}
```

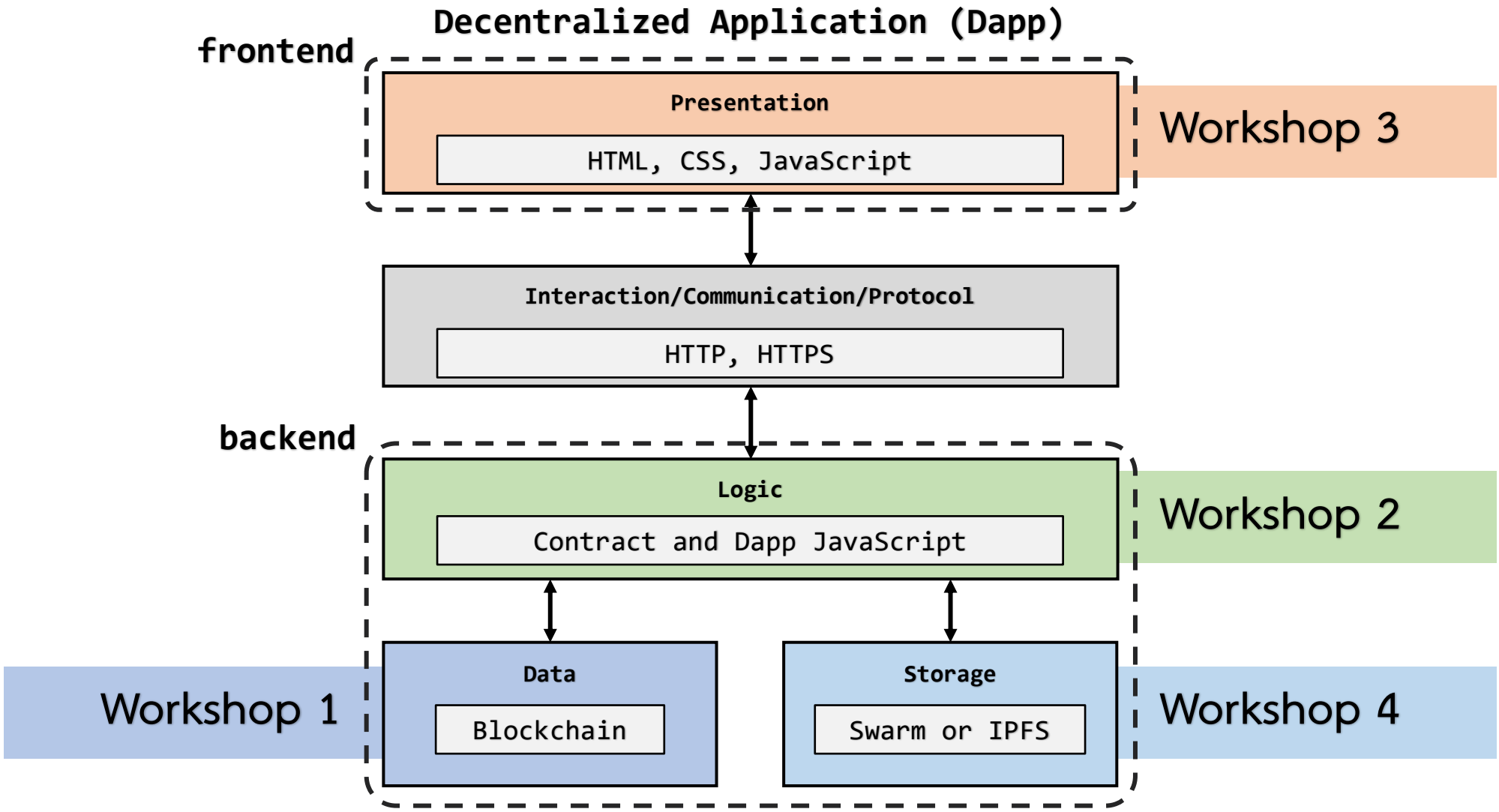
ERC20

browser/erc20.sol

```
1   pragma solidity ^0.5.0;
2   library SafeMath {...}
20  // ----------------------------------------------------------------------------
21  // ERC Token Standard #20 Interface
22  // https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md
23  // ----------------------------------------------------------------------------
24  contract ERC20Interface {
25      function totalSupply() public view returns (uint);
26      function balanceOf(address tokenOwner) public view returns (uint balance);
27      function allowance(address tokenOwner, address spender) public view returns (uint remaining);
28      function transfer(address to, uint tokens) public returns (bool success);
29      function approve(address spender, uint tokens) public returns (bool success);
30      function transferFrom(address from, address to, uint tokens) public returns (bool success);
31
32      event Transfer(address indexed from, address indexed to, uint tokens);
33      event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
34  }
35  contract ApproveAndCallFallBack {...}
38  contract Owned {...}
63  // ----------------------------------------------------------------------------
64  // ERC20 Token, with the addition of symbol, name and decimals and a
65  // fixed supply
66  // ----------------------------------------------------------------------------
67  contract FixedSupplyToken is ERC20Interface, Owned {
68      using SafeMath for uint;
69
70      string public symbol;
71      string public  name;
72      uint8 public decimals;
73      uint _totalSupply;
```

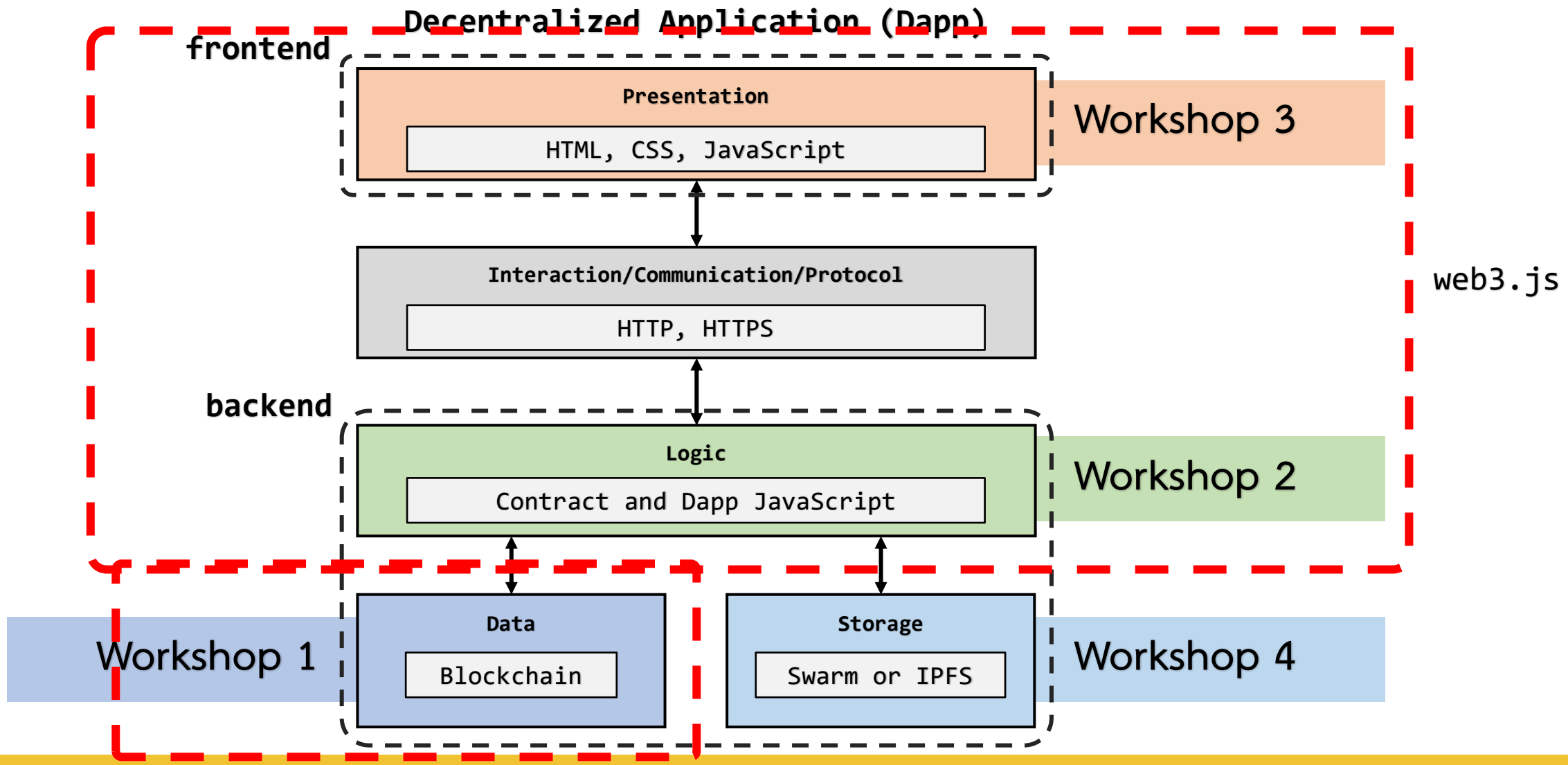
https://theethereum.wiki/w/index.php/ERC20_Token_Standard

Overview



https://file.scirp.org/pdf/JSEA_20161028140127798.pdf

Overview



https://file.scirp.org/pdf/JSEA_20161028140127798.pdf

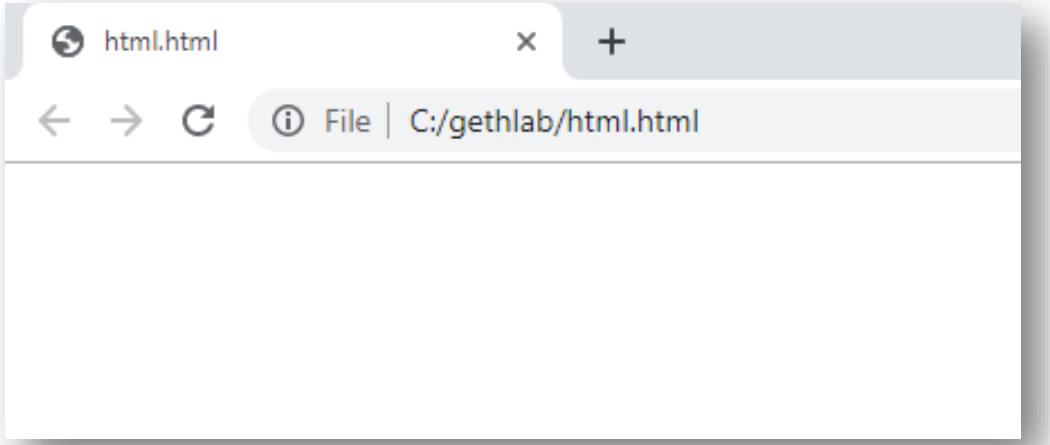
Workshop 3 Front End

workshop นี้ทำอะไร

1. เราจะสร้าง Web Application กัน ดังนั้นสิ่งที่ต้องรู้ก็คือภาษาที่ใช้เขียนเว็บได้แก่
    1.1 HTML (div, input, button)
    1.2 JavaScript (document.innerHTML, document.value)
    1.3 JavaScript [, callback], Promise, Async/Await
2. เราจะใช้ web3.js module เป็น open source ที่ใช้ในการติดต่อกับ Ethereum blockchain
    2.1 web3.js script

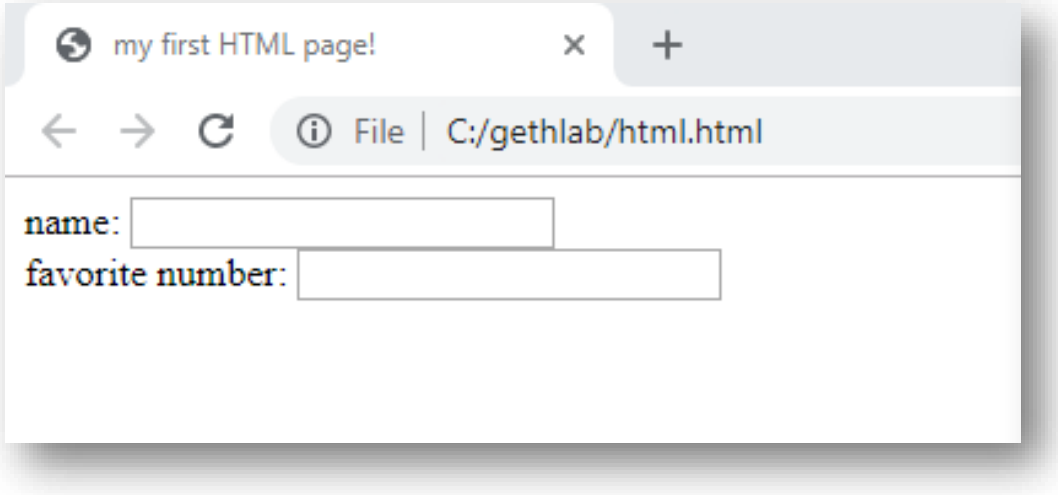
HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>my first HTML page!</title>
</head>
<body>

</body>
</html>
```



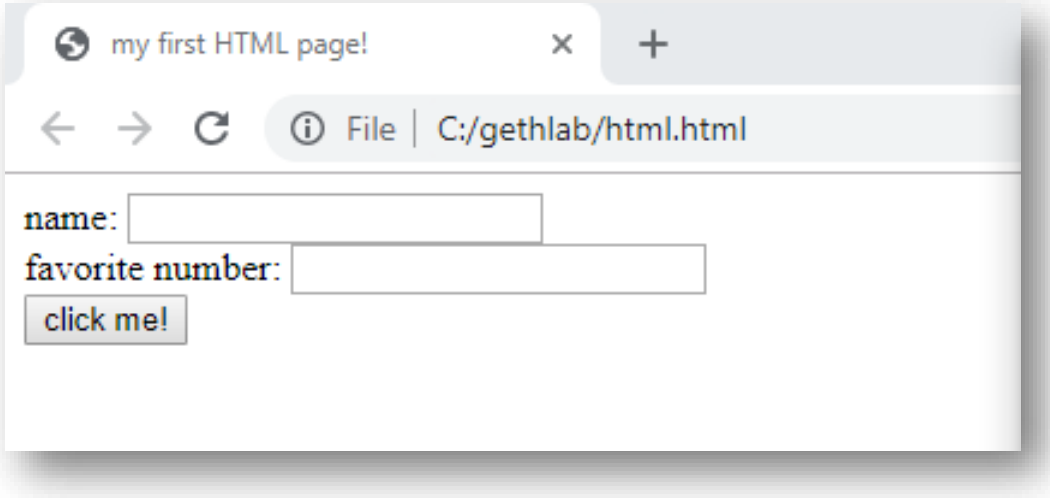
Input-HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    name:  <input type="text" id="name"></br>
    favorite number:  <input type="number" id="fav_num""><br>
</body>
</html>
```



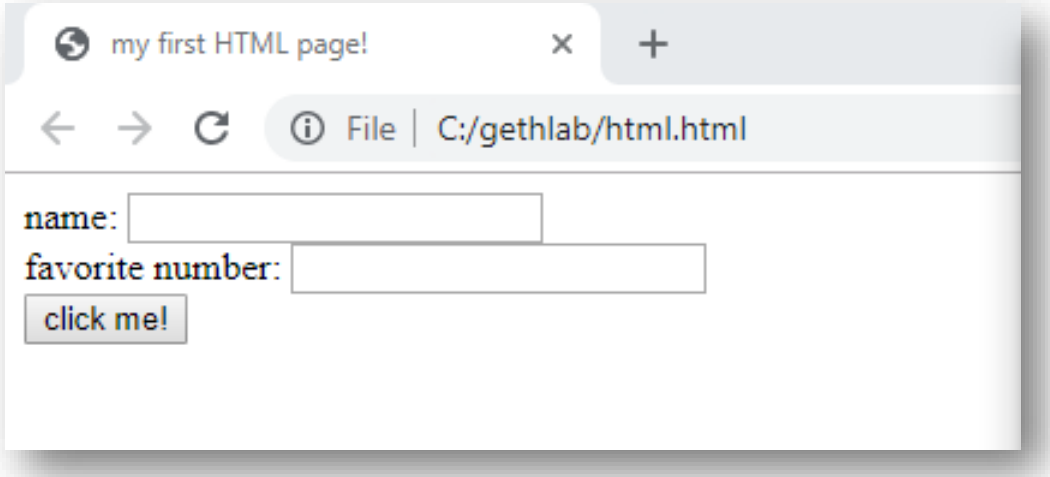
Button

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    <!--input-HTML done!-->
    <button onclick="myFunction()">click me!</button>
</body>
</html>
```



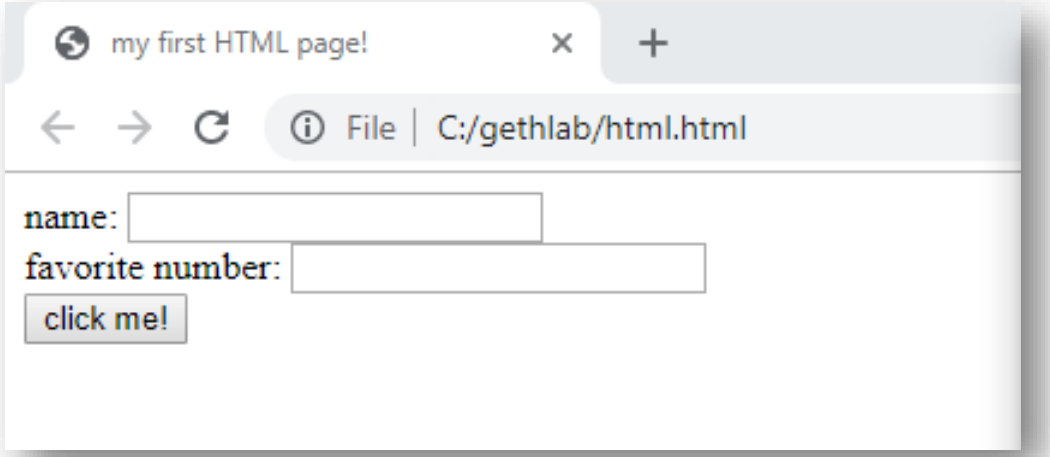
Output-HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    <!--input-HTML done!-->
    <!--button done!-->
    <div id="placeholder"></div>
</body>
</html>
```



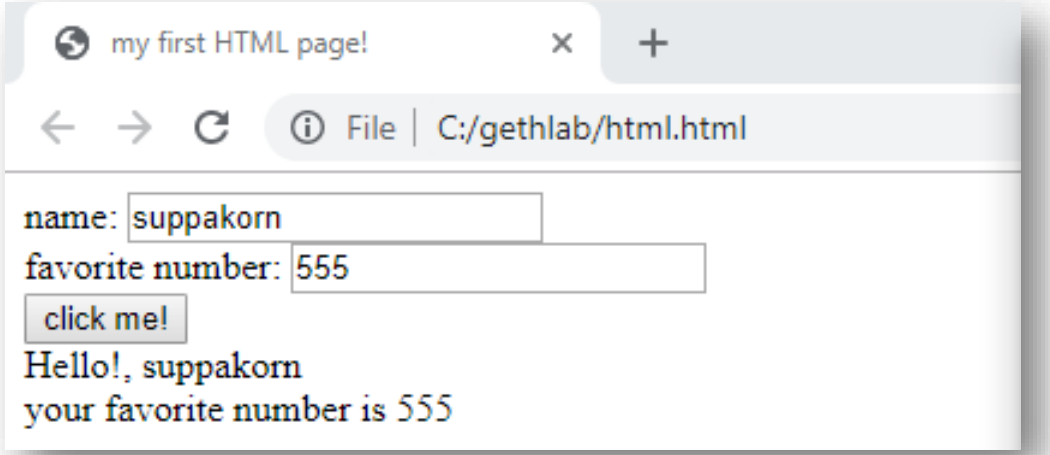
Input-JS

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    <!--input-HTML done!-->
    <!--button done!-->
    <!--output-HTML done!-->
    <script>
        function myFunction(){
            let name = document.getElementById("name").value
            let fav_num = document.getElementById("fav_num").value
        }
    </script>
</body>
</html>
```



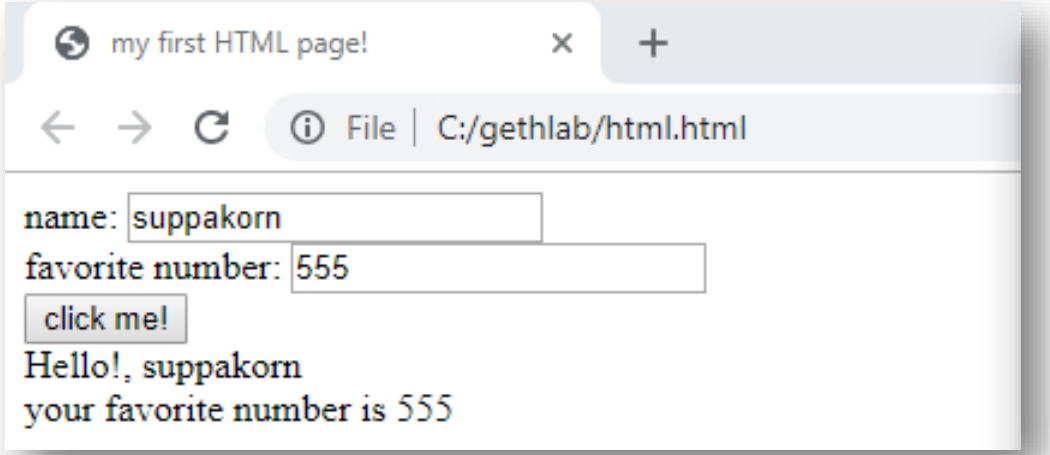
Output-JS

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    <!--input-HTML done!-->
    <!--button done!-->
    <!--output-HTML done!-->
    <script>
        function myFunction(){
            //input-JS done!
            document.getElementById("placeholder").innerHTML = "Hello!, "+name+"<br>
            your favorite number is "+fav_num
        }
    </script>
</body>
</html>
```



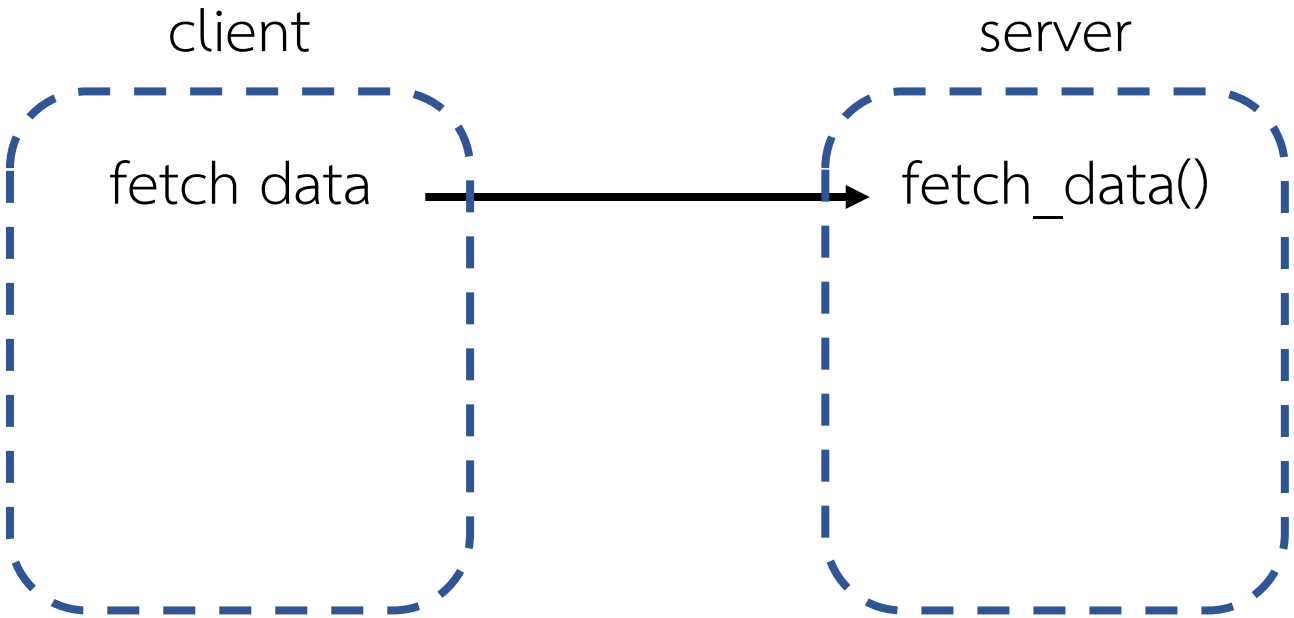
Full Code

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>my first HTML page!</title>
</head>
<body>
    name:  <input type="text" id="name"></input><br>
    favorite number:  <input type="number" id="fav_num""></input><br>
    <script>
        let name = document.getElementById("name").value;
        let fav_num = document.getElementById("fav_num").value;
    </script>
    <button onclick="myFunction()">click me!</button>
    <div id="placeholder"></div>
    <script>
        function myFunction(){
            let name = document.getElementById("name").value;
            let fav_num = document.getElementById("fav_num").value;
            document.getElementById("placeholder").innerHTML = "Hello!, "+name+"<br> your favorite number is "+fav_num;
        }
    </script>
</body>
</html>
```



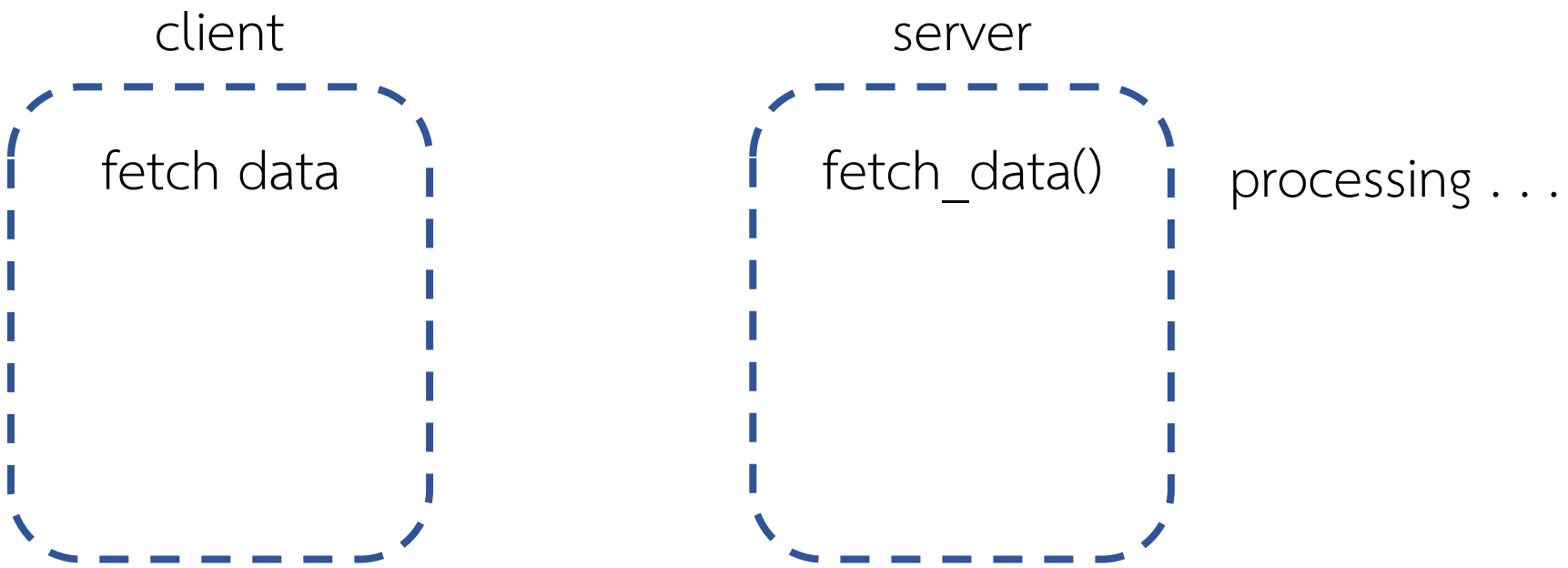
[, callback]

```
<script>
        function myFunction(){
            let name = fetch_data_from_blockchain()
            document.getElementById("placeholder").innerHTML = name
        }
</script>
```



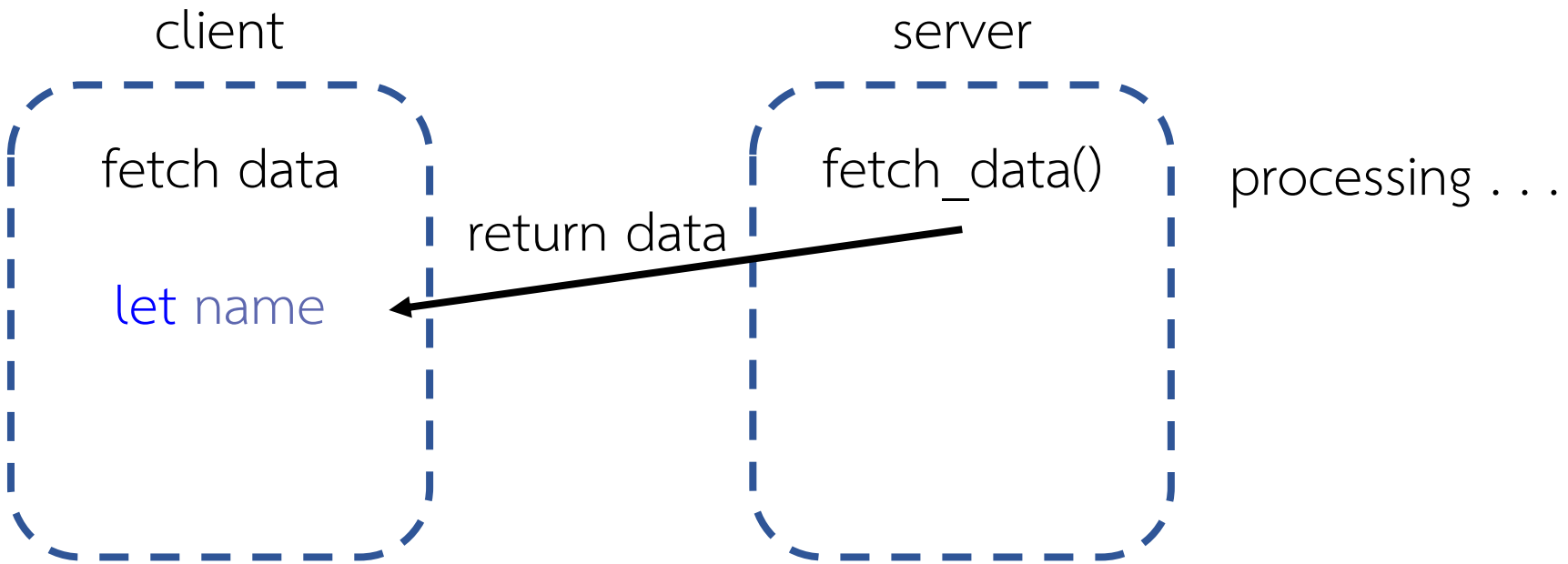
[, callback]

```
<script>
        function myFunction(){
            let name = fetch_data_from_blockchain()
            document.getElementById("placeholder").innerHTML = name
        }
</script>
```



[, callback]

```
<script>
        function myFunction(){
            let name = fetch_data_from_blockchain()
            document.getElementById("placeholder").innerHTML = name
        }
</script>
```

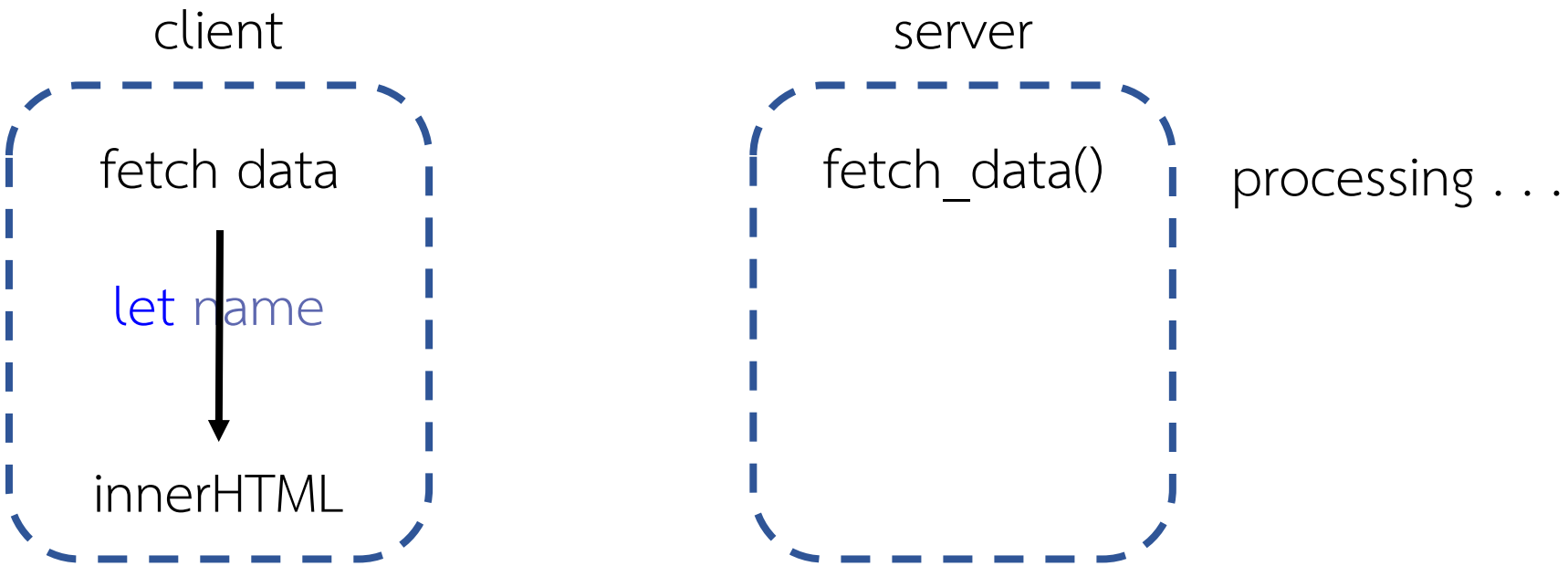


[, callback]

```
<script>
        function myFunction(){
            let name = fetch_data_from_blockchain()
            document.getElementById("placeholder").innerHTML = name
        }
</script>
```

[, callback]

```
<script>
        function myFunction(){
            let name = fetch_data_from_blockchain()
            document.getElementById("placeholder").innerHTML = name
        }
</script>
```



[, callback]

```
function myFunction(){
        let name = fetch_data_from_blockchain(
            ,function(error,data){
             if(error){
                 console.log(error)
             }else{
                 name = data;
                 document.getElementById("placeholder").innerHTML = name
             }
         });
    }
```

[, callback]

```
dataBase.verifyUser(username, password, (error, userInfo) => {
                        if (error) {
                            console.log(error)
                        }else{
                            dataBase.getRoles(username, (error, roles) => {
                                if (error){
                                    console.log(error)
                                }else {
                                    dataBase.logAccess(username, (error) => {
                                        if (error){
                                            console.log(error)
                                        }else{
                                            User.Update(userInfo, roles)
                                        }
                                    })
                                }
                            })
                        }
                    });
```

https://blog.hellojs.org/asynchronous-javascript-from-callback-hell-to-async-and-await-9b9ceb63c8e8

Promise

```
database.verifyUser(username, password)
  .then(userInfo => dataBase.getRoles(userInfo))
  .then(rolesInfo => dataBase.logAccess(rolesInfo))
  .then(finalResult => {
      User.Update(userInfo, roles)
  })
  .catch((err) => {
      console.log(err)
  })
```

https://blog.hellojs.org/asynchronous-javascript-from-callback-hell-to-async-and-await-9b9ceb63c8e8

Async/Await

```
async function(username, password){
      try {
          const userInfo = await dataBase.verifyUser(username, password);
          const rolesInfo = await dataBase.getRoles(userInfo);
          const logStatus = await dataBase.logAccess(userInfo);
          User.Update(userInfo,rolesInfo);
      }catch (e){
          console.log(e);
      }
 };
```

https://blog.hellojs.org/asynchronous-javascript-from-callback-hell-to-async-and-await-9b9ceb63c8e8

Key Note

- <input>
- <button>
-
- document.getElementById(“ ”). innerHTML
- document.getElementById(“ ”).value
- Async/Await

http-server

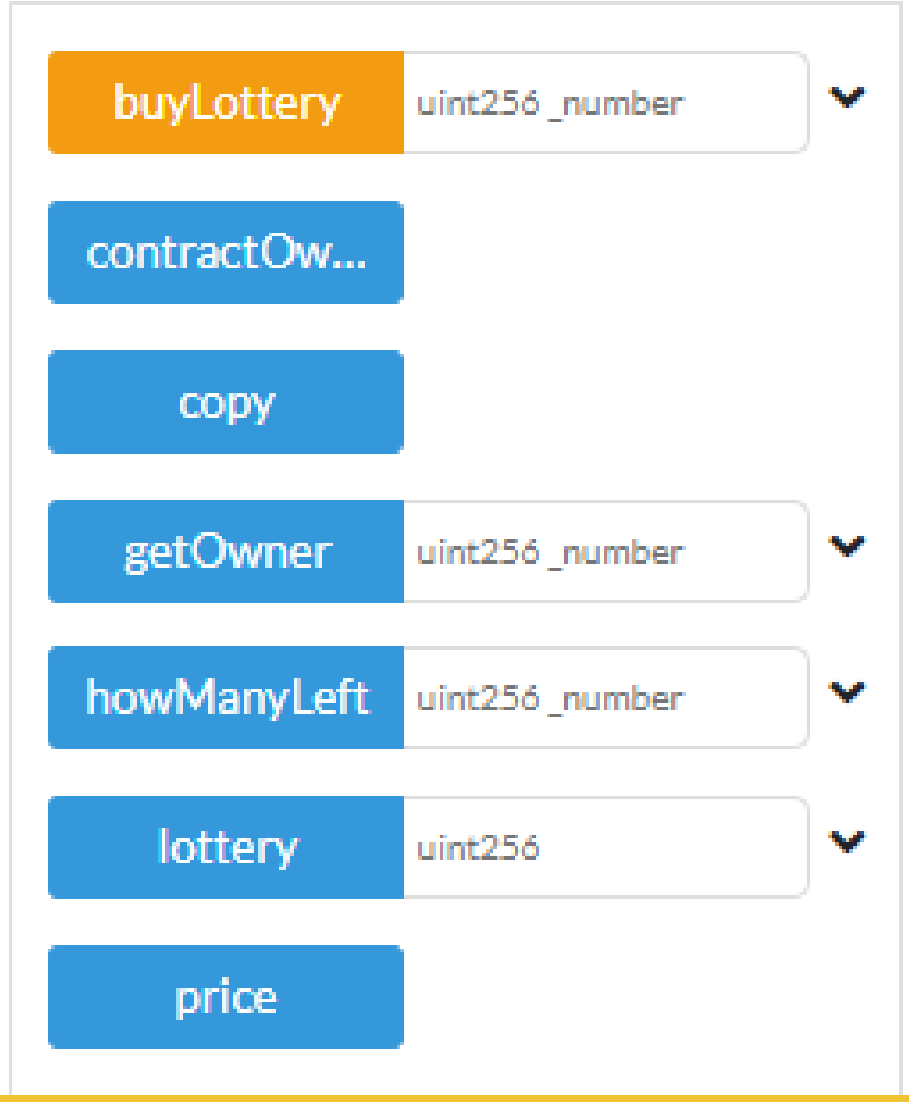
1. Run command

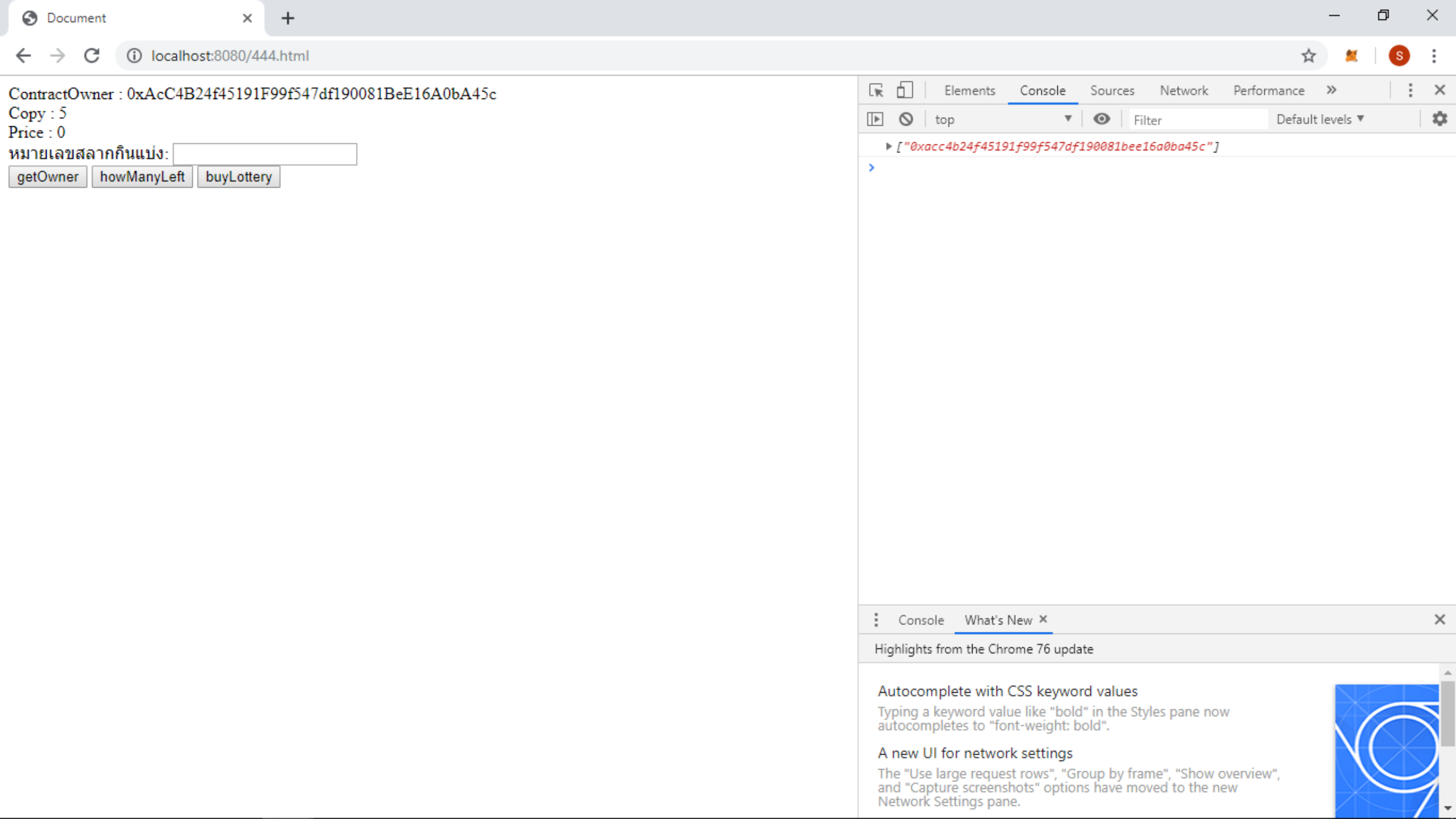
C:\frontend>http-server

สร้างไฟล์ index.html

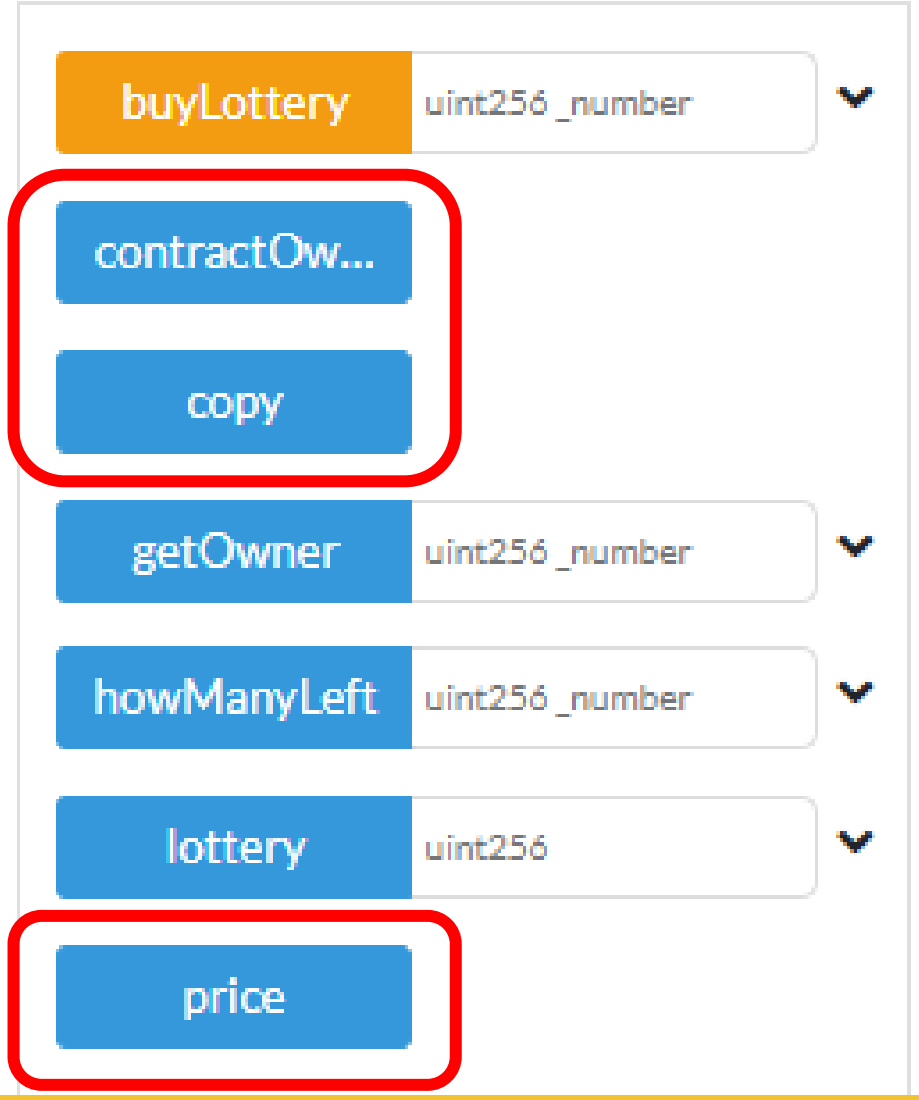
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title>
</head>
<body>
    hello

</body>
</html>
```

frontend

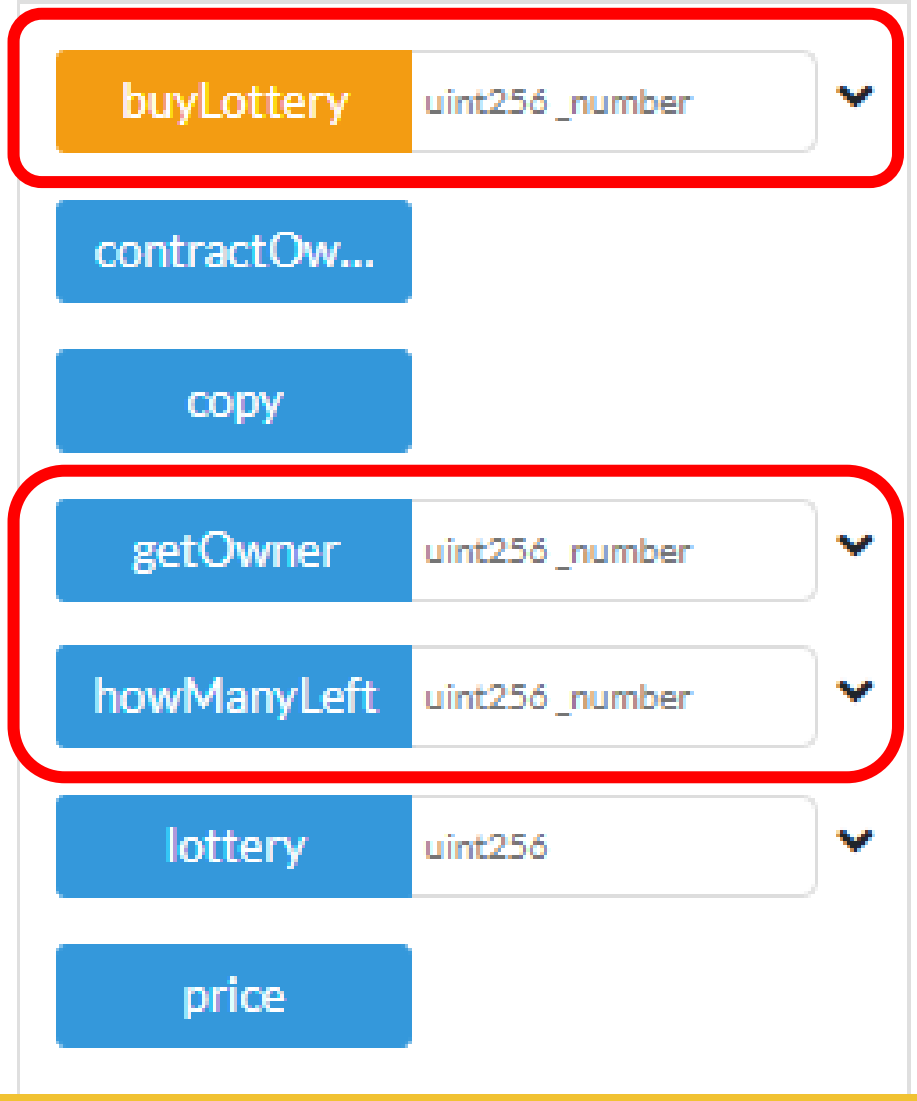

buyLottery
uint256 _number
contractOw...
copy
getOwner
uint256 _number
howManyLeft
uint256 _number
lottery
uint256
price


Document
localhost:8080/444.html
ContractOwner : 0xAcC4B24f45191F99f547df190081BeE16A0bA45c
Copy : 5
Price : 0
หมายเลขสลากกินแบ่ง:
getOwner
howManyLeft
buyLottery
Elements
Console
Sources
Network
Performance
top
Filter
Default levels
["0xacc4b24f45191f99f547df190081bee16a0ba45c"]
Console
What's New
Highlights from the Chrome 76 update
Autocomplete with CSS keyword values
Typing a keyword value like "bold" in the Styles pane now autocompletes to "font-weight: bold".
A new UI for network settings
The "Use large request rows", "Group by frame", "Show overview", and "Capture screenshots" options have moved to the new Network Settings pane.

frontend


buyLottery
uint256 _number
contractOw...
copy
getOwner
uint256 _number
howManyLeft
uint256 _number
lottery
uint256
price

frontend


buyLottery
uint256 _number
contractOw...
copy
getOwner
uint256 _number
howManyLeft
uint256 _number
lottery
uint256
price

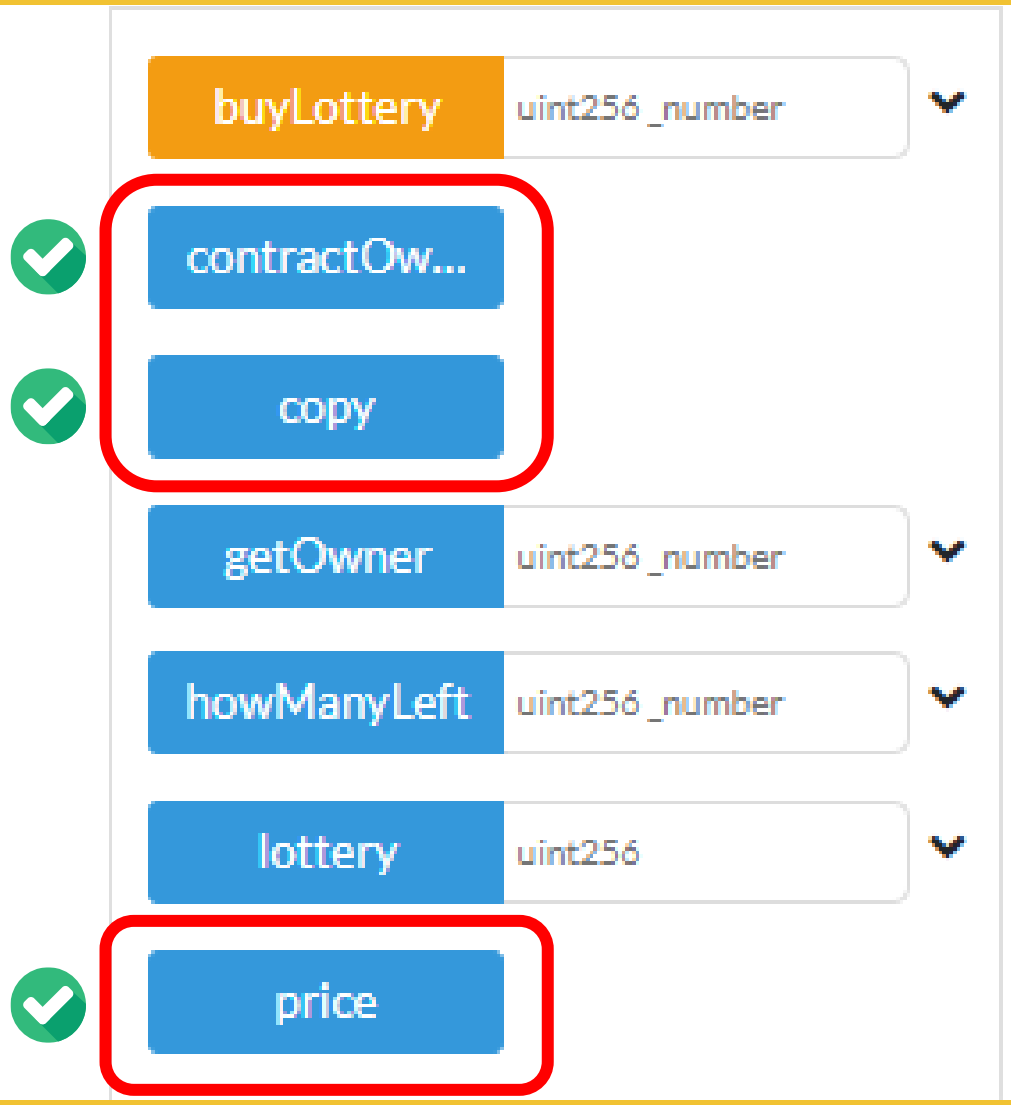
dashboard

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    <div id="showContractOwner"></div>
    <div id="showCopy"></div>
    <div id="showPrice"></div>
</body>
</html>
```

frontend

HTML

JavaScript

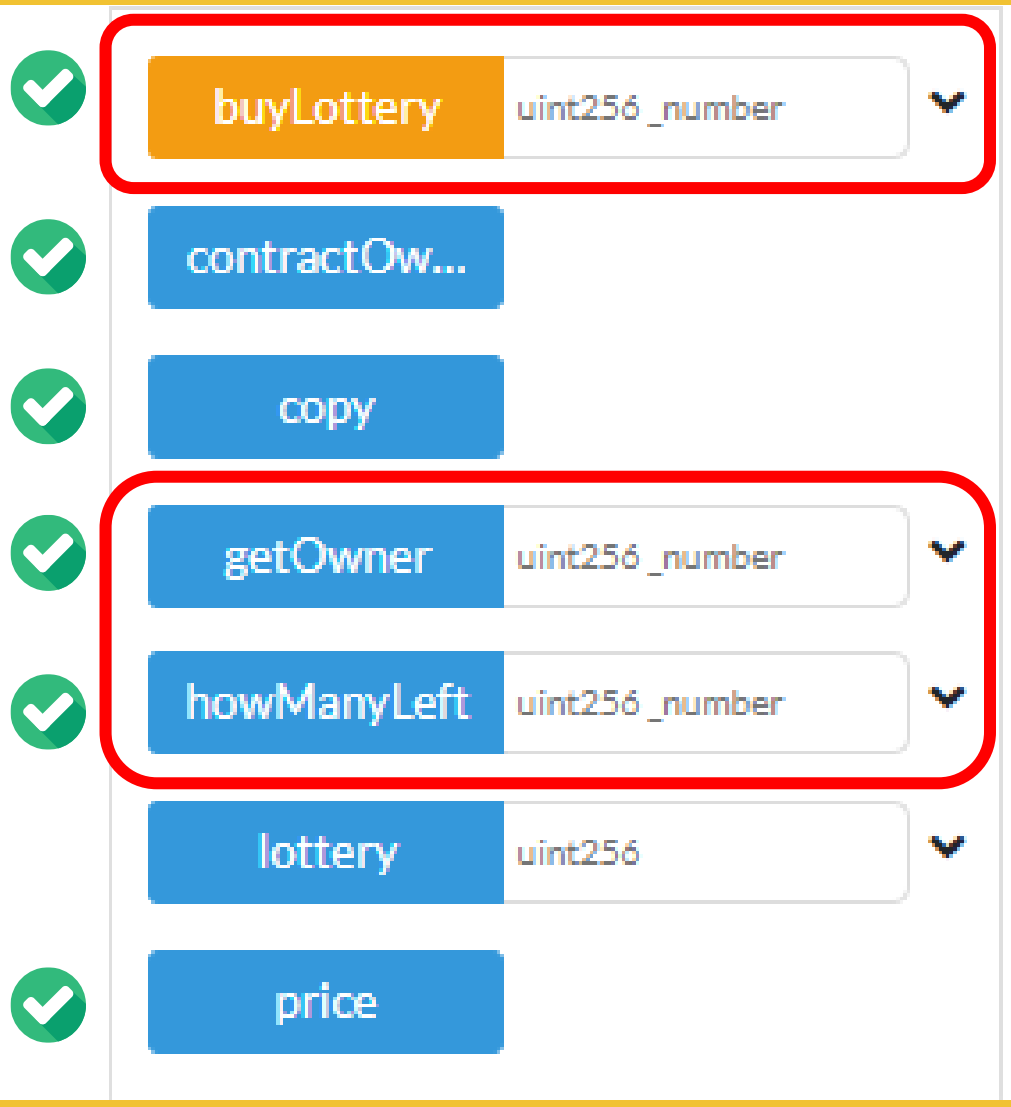


input

```
<body>
    <!--dashboard done!-->
    หมายเลขสลากกินแบ่ง: <input type="number" id="lottery"><br>
    <button onclick="getOwner()">getOwner</button>
    <button onclick="howManyLeft()">howManyLeft</button>
    <button onclick="buyLottery()">buyLottery</button>
    <div id="showGetOwner"></div>
    <div id="showHowManyLeft"></div>
    <div id="showBuyLottery"></div>
</body>
```

frontend

HTML



JavaScript

browserify

1. Run command

C:\frontend>browserify –r web3 > bundle.js

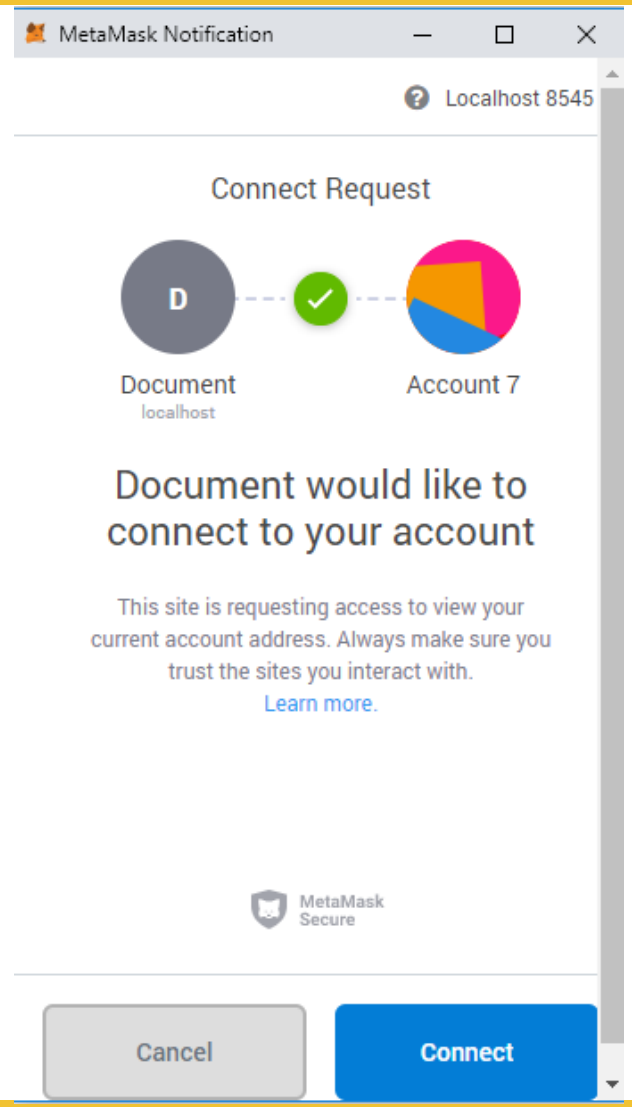
1. Run command

C:\frontend>browserify -r web3 -r ipfs -r buffer > bundle.js

bundle.js

```
require=(function(){function r(e,n,t){function o(i,f){if(!n[i]){if(!e[i]){var c="function"==typeof require&&require;if(!f&&c)return c(i,!0);
var asn1 = exports;

asn1.bignum = require('bn.js');

asn1.define = require('./asn1/api').define;
asn1.base = require('./asn1/base');
asn1.constants = require('./asn1/constants');
asn1.decoders = require('./asn1/decoders');
asn1.encoders = require('./asn1/encoders');

},{"./asn1/api":2,"./asn1/base":4,"./asn1/constants":8,"./asn1/decoders":10,"./asn1/encoders":13,"bn.js":16}],2:[function(require,module,expo
var asn1 = require('../asn1');
var inherits = require('inherits');

var api = exports;

api.define = function define(name, body) {
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--...-->
    <script src="./bundle.js"></script>
    <script>
        ethereum.enable()
        const Web3 = require('web3')
        const web3 = new Web3(Web3.givenProvider)
    </script>
</head>
<body>
    <!--UI done!-->
</body>
</html>
```



https://web3js.readthedocs.io/en/v1.2.1/getting-started.html

web3

The web3.eth is for the ethereum blockchain and smart contracts

The web3.shh is for the whisper protocol to communicate p2p and broadcast

The web3.bzz is for the swarm protocol, the decentralized file storage

The web3.utils contains useful helper functions for Dapp developers.

https://www.jsdelivr.com/package/npm/web3-eth https://www.jsdelivr.com/package/npm/web3-shh
https://www.jsdelivr.com/package/npm/web3-bzz https://www.jsdelivr.com/package/npm/web3-utils

web3

The web3.eth is for the ethereum blockchain and smart contracts

The web3.shh is for the whisper protocol to communicate p2p and broadcast

The web3.bzz is for the swarm protocol, the decentralized file storage

The web3.utils contains useful helper functions for Dapp developers.

https://www.jsdelivr.com/package/npm/web3-eth https://www.jsdelivr.com/package/npm/web3-shh
https://www.jsdelivr.com/package/npm/web3-bzz https://www.jsdelivr.com/package/npm/web3-utils

contract instance

```
<head>
    <!--...-->
 <script>
   //web3 done!
   const abi =
   const contractAddress = ""
   const lotteryContract = new web3.eth.Contract(abi,contractAddress)
 </script>
</head>
```

https://web3js.readthedocs.io/en/v1.2.1/getting-started.html

contract instance

contract instance

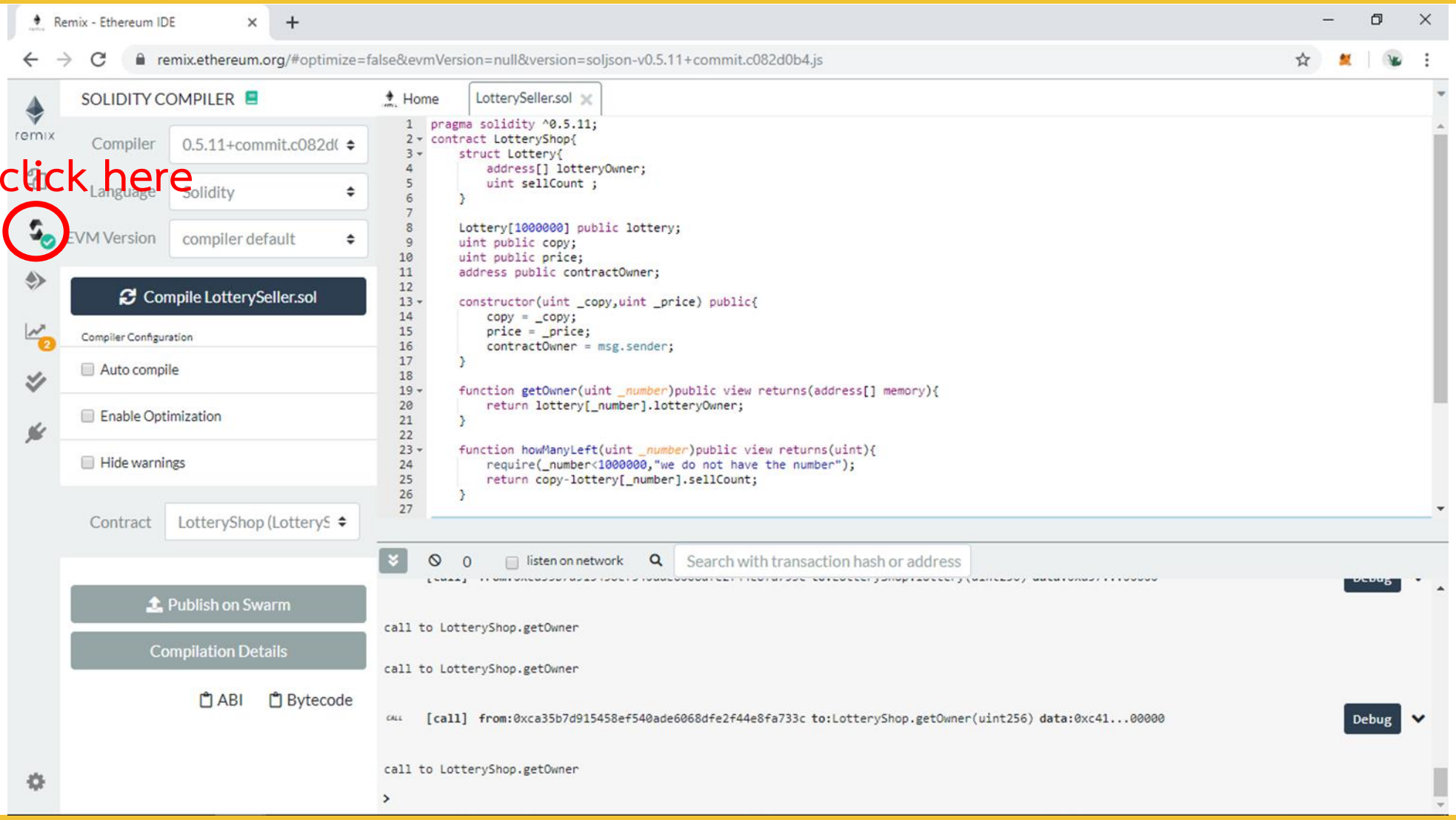
Application Binary Interface

```
const lotteryContract = new web3.eth.Contract(abi,contractAddress)
```

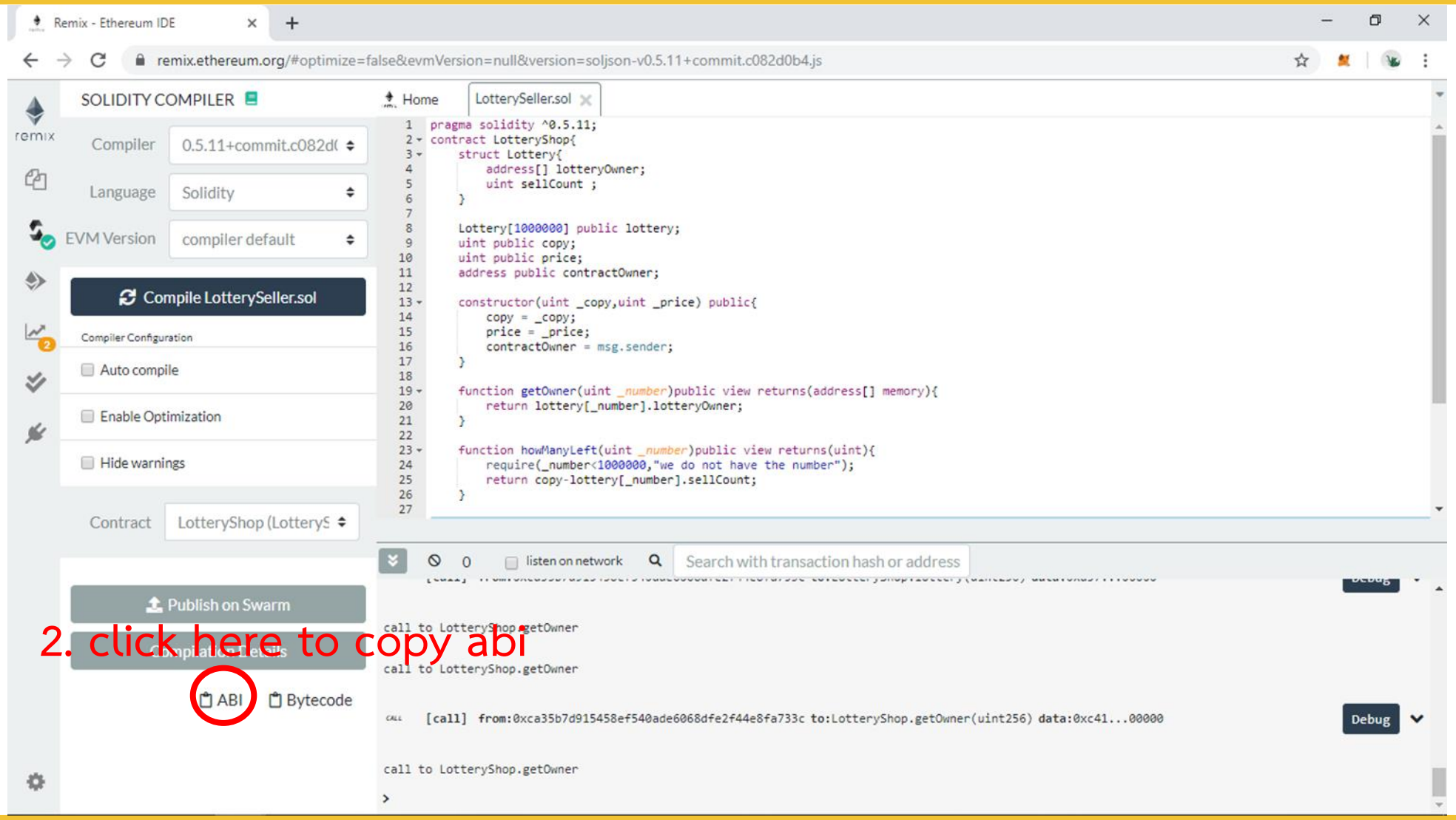
a web3 methods

location of our contract

Application Binary Interface



Application Binary Interface



2. click here to copy abi

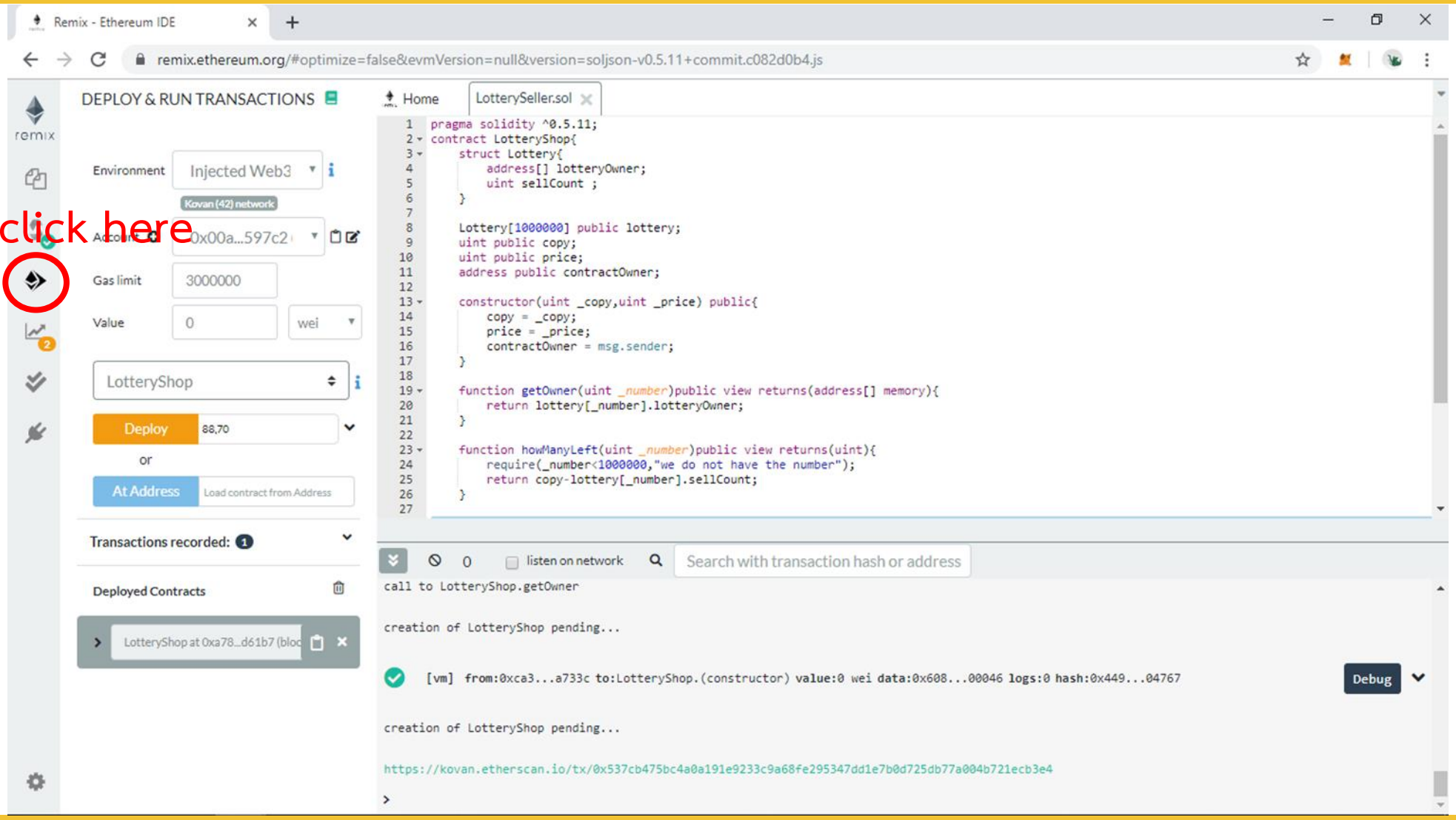
Application Binary Interface

[{ "constant": true, "inputs": [], "name": "copy", "outputs": [{ "internalType": "uint256", "name": "", "type": "uint256" }], "payable": false, "stateMutability": "view", "type": "function" }, { "constant": true, "inputs": [{ "internalType": "uint256", "name": "_number", "type": "uint256" }], "name": "howManyLeft", "outputs": [{ "internalType": "uint256", "name": "", "type": "uint256" }], "payable": false, "stateMutability": "view", "type": "function" }, { "constant": true, "inputs": [], "name": "price", "outputs": [{ "internalType": "uint256", "name": "", "type": "uint256" }], "payable": false, "stateMutability": "view", "type": "function" }, { "constant": true, "inputs": [{ "internalType": "uint256", "name": "", "type": "uint256" }], "name": "lottery", "outputs": [{ "internalType": "uint256", "name": "sellCount", "type": "uint256" }], "payable": false, "stateMutability": "view", "type": "function" }, { "constant": true, "inputs": [{ "internalType": "uint256", "name": "_number", "type": "uint256" }], "name": "getOwner", "outputs": [{ "internalType": "address[]", "name": "", "type": "address[]" }], "payable": false, "stateMutability": "view", "type": "function" }, { "constant": true, "inputs": [], "name": "contractOwner", "outputs": [{ "internalType": "address", "name": "", "type": "address" }], "payable": false, "stateMutability": "view", "type": "function" }, { "constant": false, "inputs": [{ "internalType": "uint256", "name": "_number",

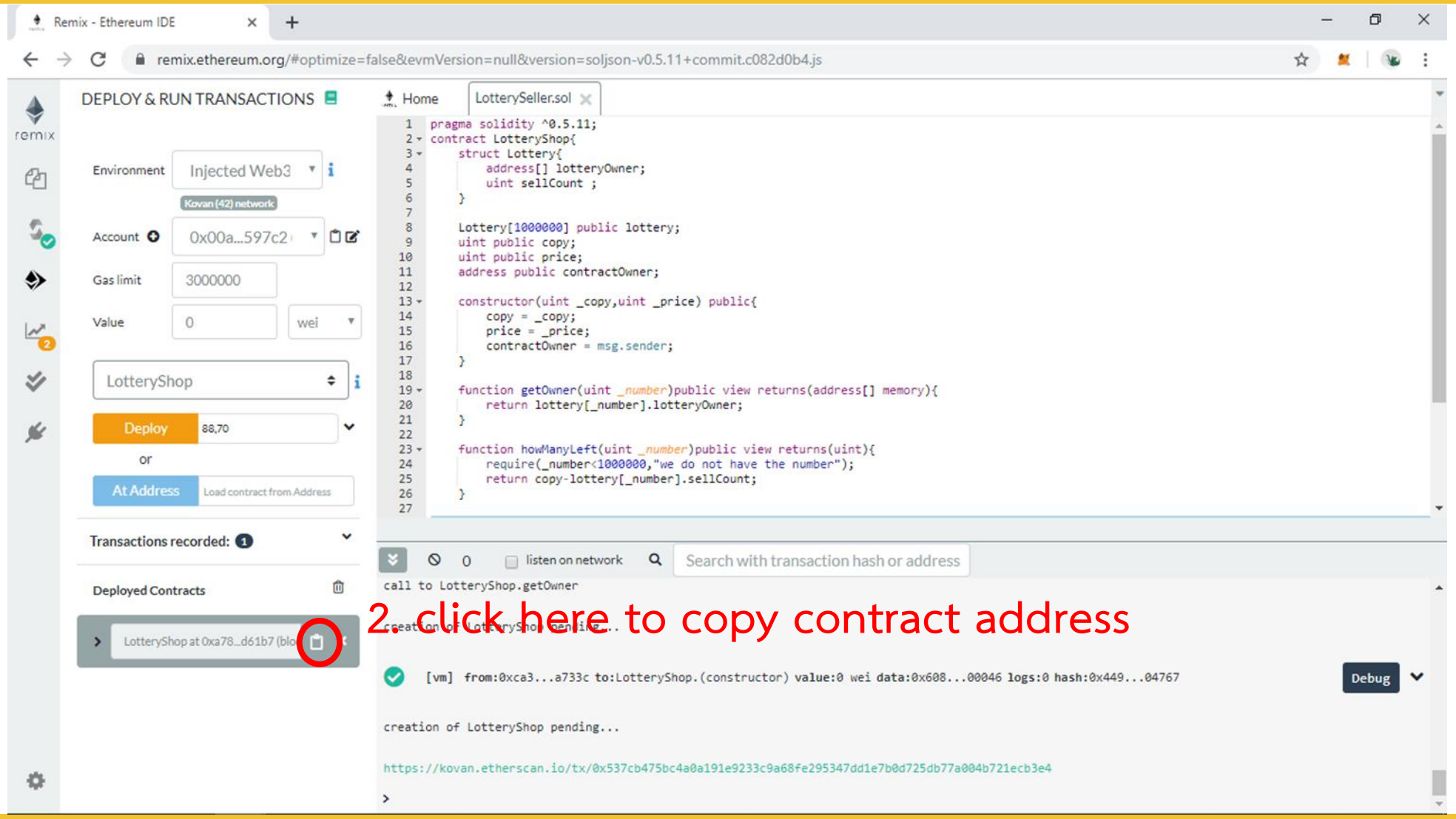
Application Binary Interface

```
<head>
    <!--...-->
 <script>
   //web3 done!
   const abi = <paste your abi here>
   const contractAddress = ""
   const lotteryContract = new web3.eth.Contract(abi,contractAddress)
 </script>
</head>
```

contract address



contract address



contract address

```
<head>
    <!--...-->
 <script>
   //web3 done!
   const abi = <paste your abi here>
   const contractAddress = "0x5d4e134aef2f88a2dedd35757c5fb9e72dfbfe97"
   const lotteryContract = new web3.eth.Contract(abi,contractAddress)
 </script>
</head>
```

DOMContentLoaded

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--...-->
    <script>
        //web3 and contract done!
        window.addEventListener('DOMContentLoaded', (event) => {
            //DOM fully loaded and parsed
        })
    </script>
</head>
<body>
    <!--UI done!-->
</body>
</html>
```

https://web3js.readthedocs.io/en/v1.2.1/getting-started.html

dashboard

```
window.addEventListener('DOMContentLoaded', async function(event) {
    let contractOwner = await lotteryContract.methods.contractOwner().call()
    document.getElementById("showContractOwner").innerHTML =
        "ContractOwner : "+ contractOwner
})
```

dashboard

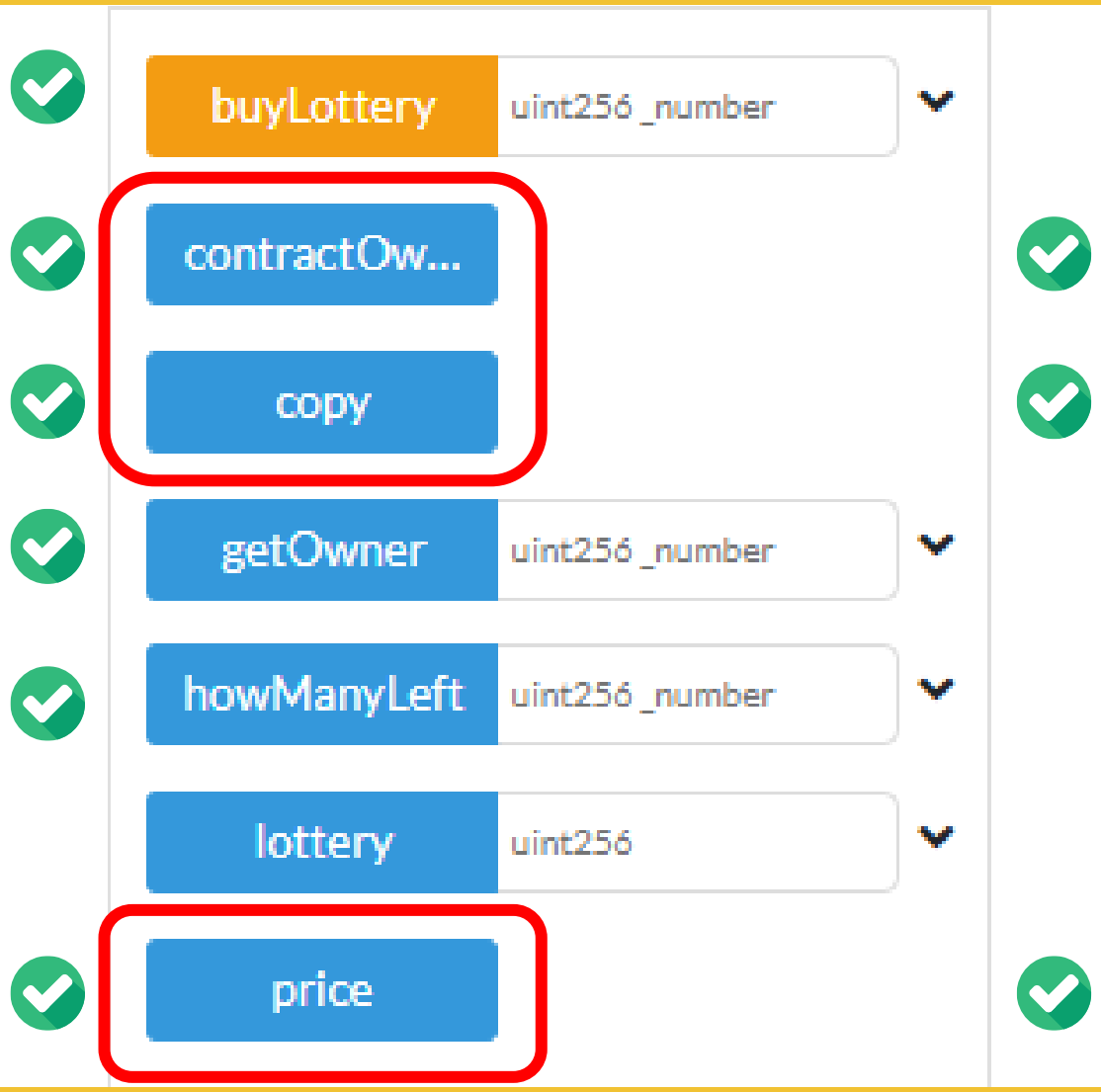
```
window.addEventListener('DOMContentLoaded', async function(event) {
    let contractOwner = await lotteryContract.methods.contractOwner().call()
    document.getElementById("showContractOwner").innerHTML =
        "ContractOwner : "+ contractOwner

    let copy = await lotteryContract.methods.copy().call()
    document.getElementById("showCopy").innerHTML = "Copy : "+copy

})
```

dashboard

```
window.addEventListener('DOMContentLoaded', async function(event) {
    let contractOwner = await lotteryContract.methods.contractOwner().call()
    document.getElementById("showContractOwner").innerHTML =
        "ContractOwner : "+ contractOwner

    let copy = await lotteryContract.methods.copy().call()
    document.getElementById("showCopy").innerHTML = "Copy : "+copy

    let price = await lotteryContract.methods.price().call()
    document.getElementById("showPrice").innerHTML = "Price : "+price

})
```

frontend

HTML

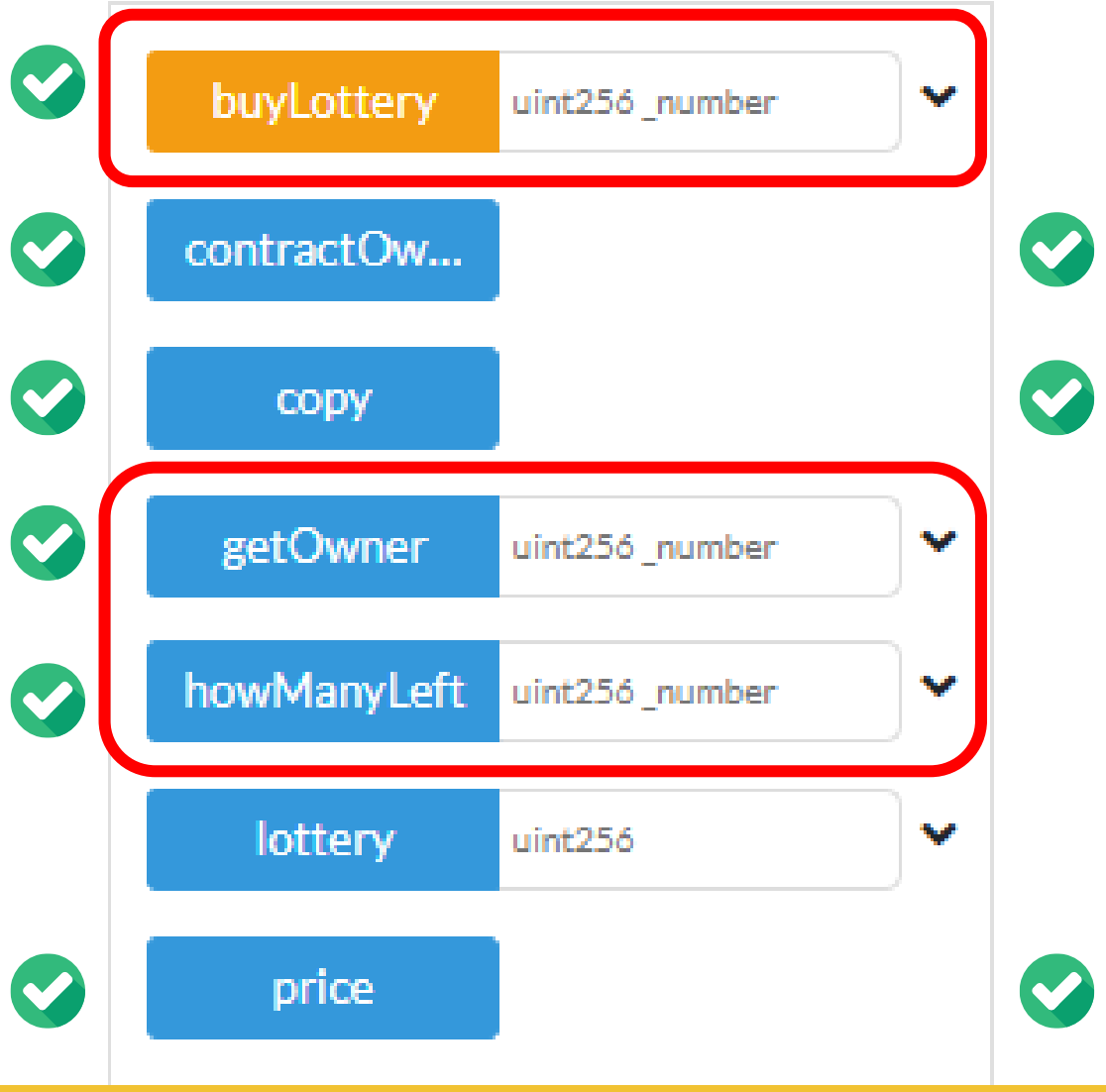


JavaScript

frontend

HTML

JavaScript



function

```
<head>
    <script>
    //web3 and contract
    window.addEventListener('DOMContentLoaded', async function(event){
        //done
    })
    async function getOwner(){}
    async function howManyLeft(){}
    async function buyLottery(){}
    </script>
</head>
```

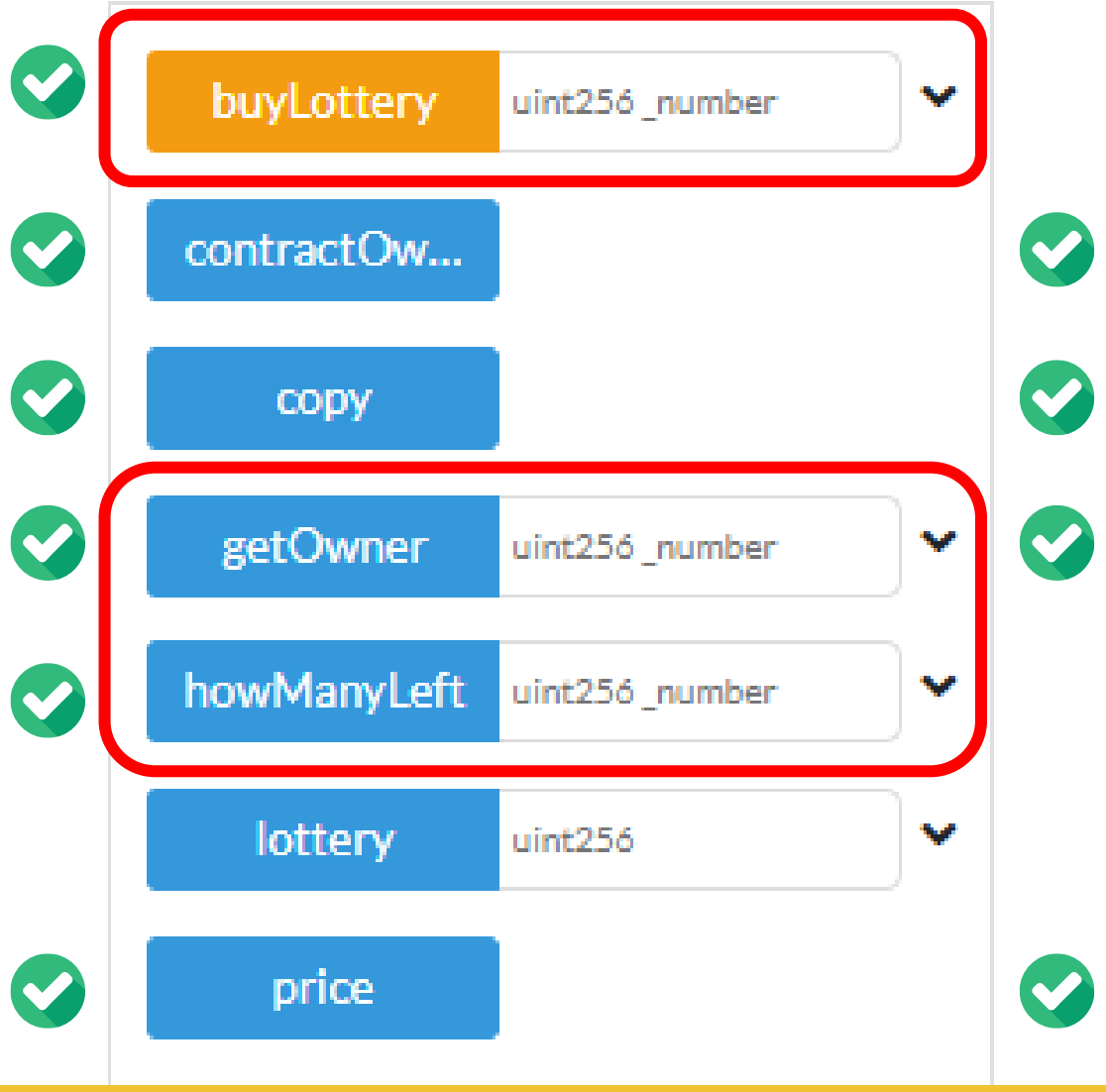
function

```
async function getOwner(){
    let _number = document.getElementById("lottery").value
    let owner = await lotteryContract.methods.getOwner(_number).call()
    document.getElementById("showGetOwner").innerHTML = "Owner : "+owner
}
```

frontend

HTML

JavaScript



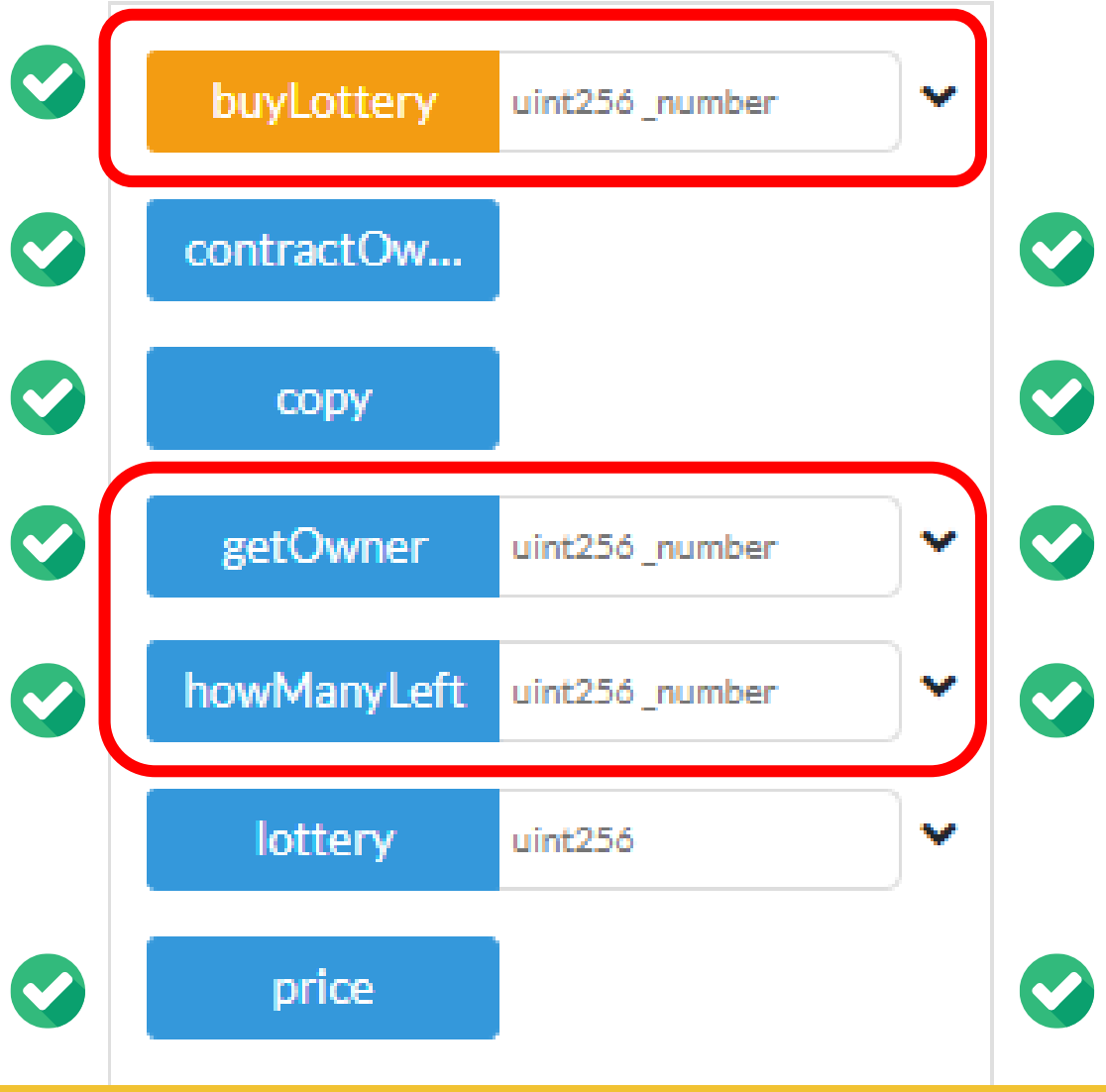
function

```
async function howManyLeft(){
    let _number = document.getElementById("lottery").value
    let left = await lotteryContract.methods.howManyLeft(_number).call()
    document.getElementById("showHowManyLeft").innerHTML = "left : "+left
}
```

frontend

HTML

JavaScript



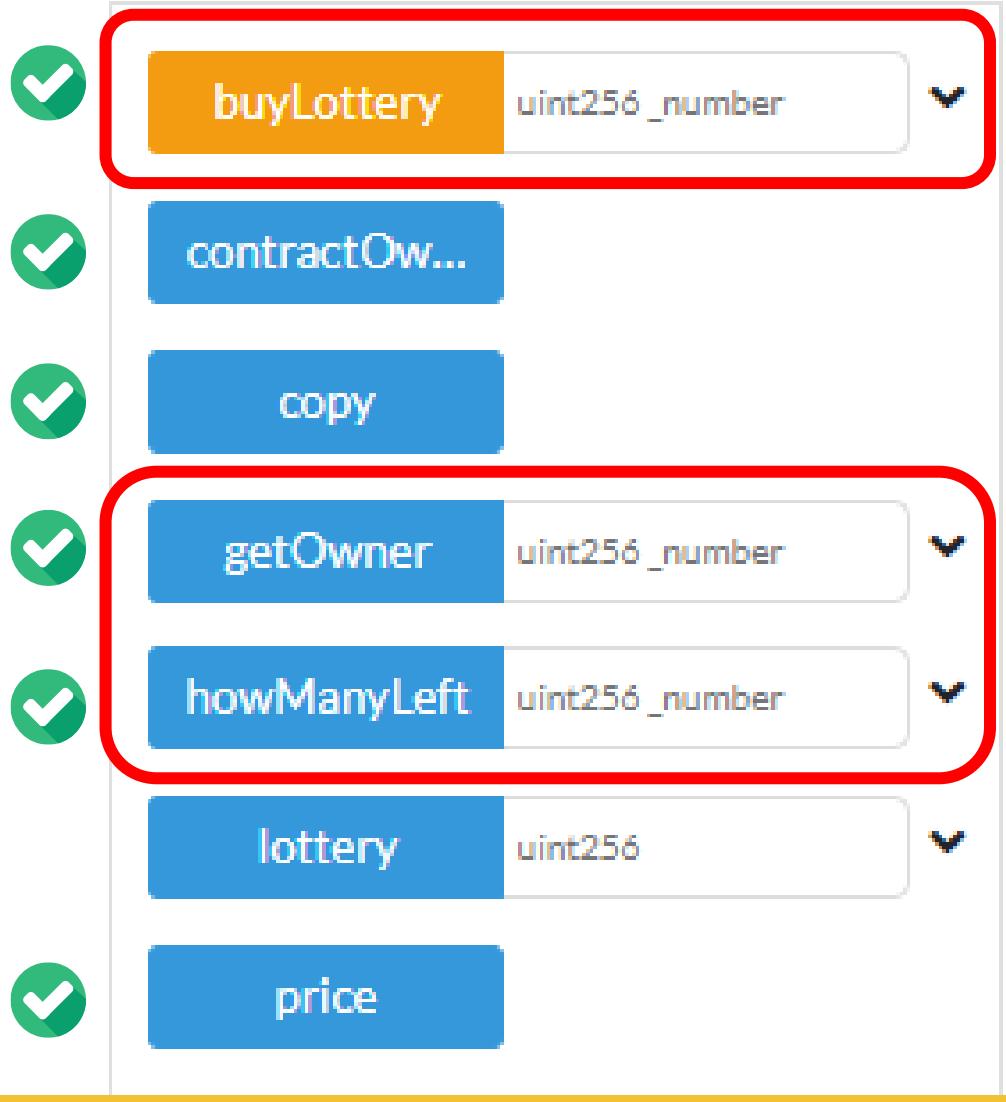
function

```
async function buyLottery(){
    let _number = document.getElementById("lottery").value
    let price = await lotteryContract.methods.price().call()
    let wallet = await web3.eth.getAccounts()
    lotteryContract.methods.buyLottery(_number).send({from: wallet[0], value: price})
    .on('receipt', function(receipt){
      console.log('receipt')
      document.getElementById("showBuyLottery").innerHTML = "คุณได้ซื้อสลากหมายเลข"+ _number+
                                                            " เรียบร้อยแล้ว"

    })
    .on('error', function(error){
        console.log(error)
        document.getElementById("showBuyLottery").innerHTML = error
    })
}
```

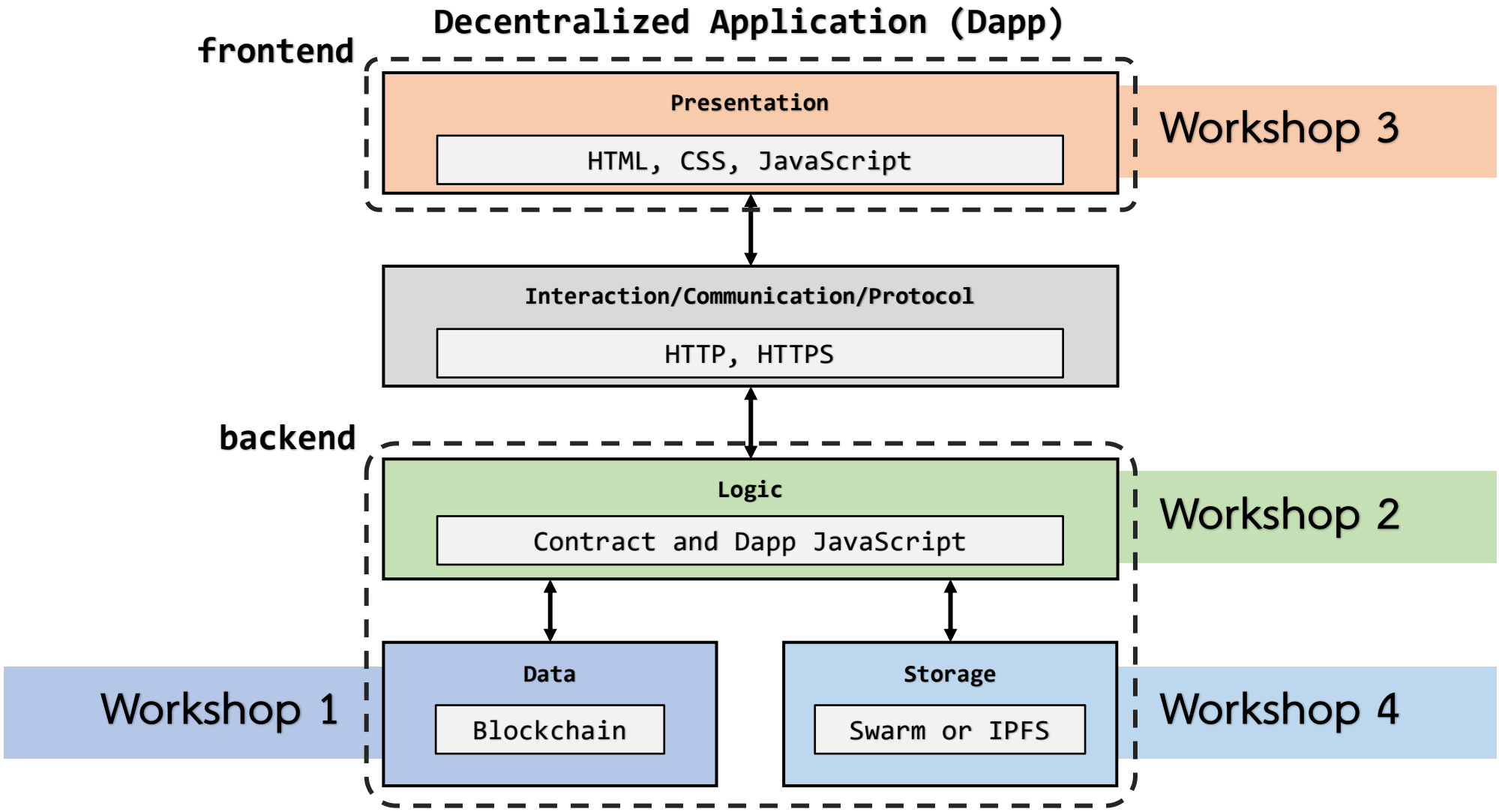
frontend

HTML

JavaScript



Overview



https://file.scirp.org/pdf/JSEA_20161028140127798.pdf

Workshop 4 Storage

workshop นี้ทำอะไร

1. จากที่เราตะลุยมา 3 Workshops เราพบว่าจุดอ่อนของ smart contract คือมันเก็บได้แต่ตัวแปร ดังนั้นใน workshop นี้ เราจะมาเก็บไฟล์กัน โดยมีจะใช้วิธีได้แก่

    1.1 IPFS ที่ใช้เก็บไฟล์ประเทศกูมีที่เป็นกระแสอยู่พักนึงนั่นเอง

    1.2 แปลงไฟล์ให้เป็น data (byte) แล้วเก็บในตัวแปร bytes ของ smart contract

IPFS

A peer-to-peer hypermedia protocol

to make the web faster, safer, and more open.

https://ipfs.io/

What is IPFS?

IPFS is a distributed system for

storing and accessing files, websites, applications, and data.

https://docs.ipfs.io/introduction/overview/

How IPFS works?

Each file and all of the **blocks within it** are given a **unique fingerprint** called a **cryptographic hash.**

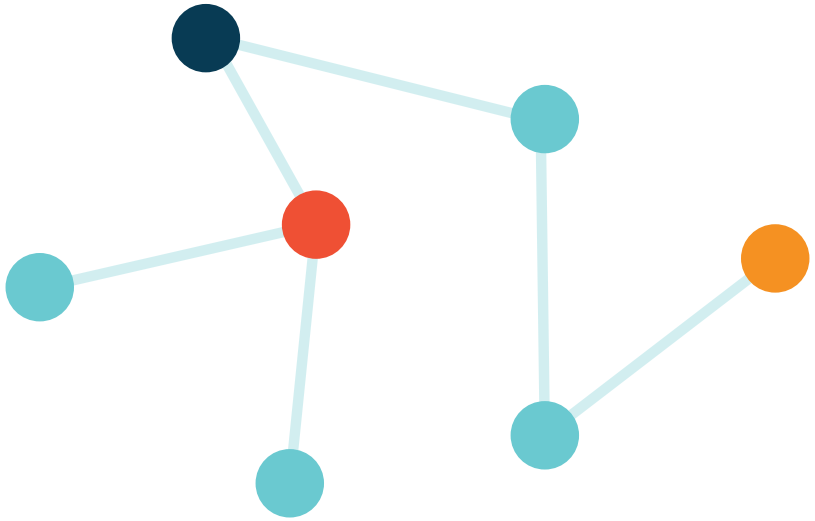
https://ipfs.io/#how

How IPFS works?

IPFS **removes duplications** across the network.

https://ipfs.io/#how

How IPFS works?



Each **network node** stores only content it is interested in, and some indexing information that helps figure out who is storing what.

https://ipfs.io/#how

How IPFS works?

When **looking up files**, you're asking the network to find nodes storing the content behind a unique hash.

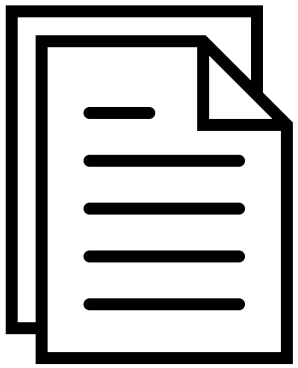
https://ipfs.io/#how

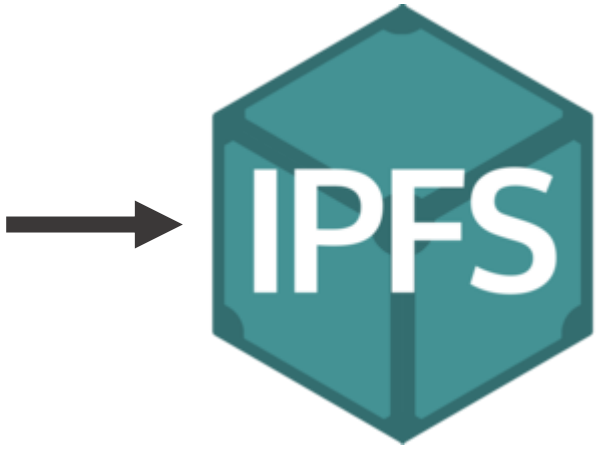
How IPFS works?

Every file can be found by **human-readable names** using a decentralized naming system called **IPNS**.

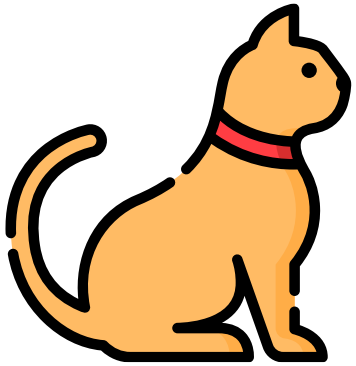
https://ipfs.io/#how

TL;DR





QmXcUvn9ow9Zx6KN1578AU2JjaT8gRfGog89wdJ9CS6To1

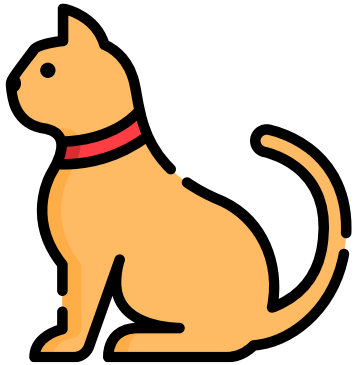


สมชาย

TL;DR

QmXcUvn9ow9Zx6KN1578AU2JjaT8gRfGog89wdJ9CS6To1 → IPFS →

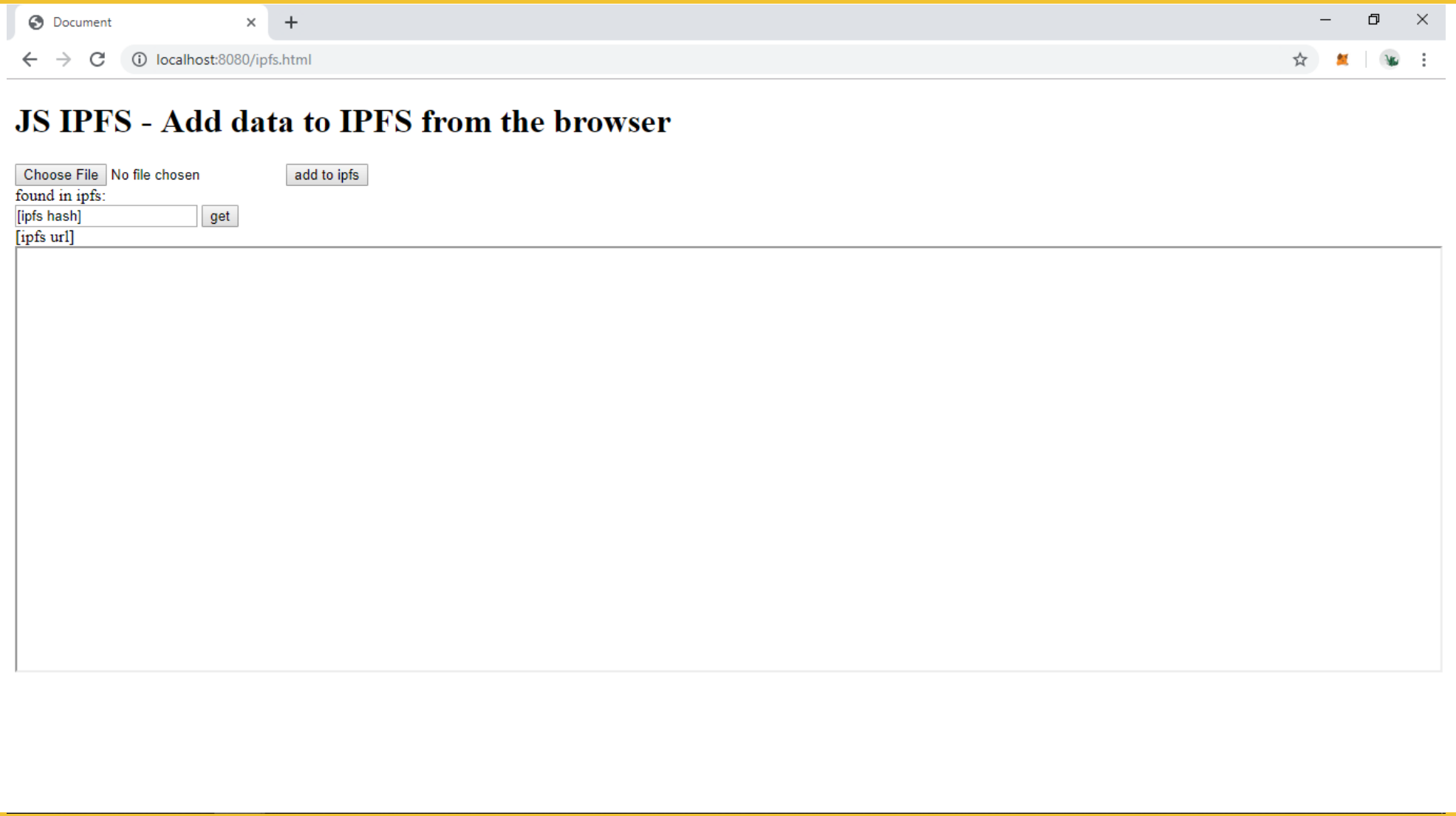
สมหมาย



สร้างไฟล์ ipfs.html

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title>
</head>
<body>
    hello

</body>
</html>
```

1. UI


Document
localhost:8080/ipfs.html
JS IPFS - Add data to IPFS from the browser
Choose File
No file chosen
add to ipfs
found in ipfs:
[ipfs hash]
get
[ipfs url]

1. UI

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    <h1>JS IPFS - Add data to IPFS from the browser</h1>
    <input type="file" id="source"></input>
    <button onclick="store()">add to ipfs</button>
    <div>found in ipfs:</div>
    <input type="text" id="hash" value="[ipfs hash]">
    <button onclick="show()">show</button><br>
    <a id="url">[ipfs url]</a>
    <iframe id="content" width="100%" height="400">[ipfs content]</iframe>
</body>

</html>
```

1. UI


Document
localhost:8080/ipfs.html
JS IPFS - Add data to IPFS from the browser
Choose File
pic.png
add to ipfs
found in ipfs:
QmXcUvn9ow9Zx6KN1578A
show
https://ipfs.io/ipfs/QmXcUvn9ow9Zx6KN1578AU2JjaT8gRfGog89wdJ9CS6To1
PIC

2. require('ipfs')

1. Run command

C:\frontend>browserify -r web3 -r ipfs -r buffer > bundle.js

bundle.js

```
require=(function(){function r(e,n,t){function o(i,f){if(!n[i]){if(!e[i]){var c="function"==typeof require&&require;if(!f&&c)return c(i,!0);
var asn1 = exports;

asn1.bignum = require('bn.js');

asn1.define = require('./asn1/api').define;
asn1.base = require('./asn1/base');
asn1.constants = require('./asn1/constants');
asn1.decoders = require('./asn1/decoders');
asn1.encoders = require('./asn1/encoders');

},{"./asn1/api":2,"./asn1/base":4,"./asn1/constants":8,"./asn1/decoders":10,"./asn1/encoders":13,"bn.js":16}],2:[function(require,module,expo
var asn1 = require('../asn1');
var inherits = require('inherits');

var api = exports;

api.define = function define(name, body) {
```

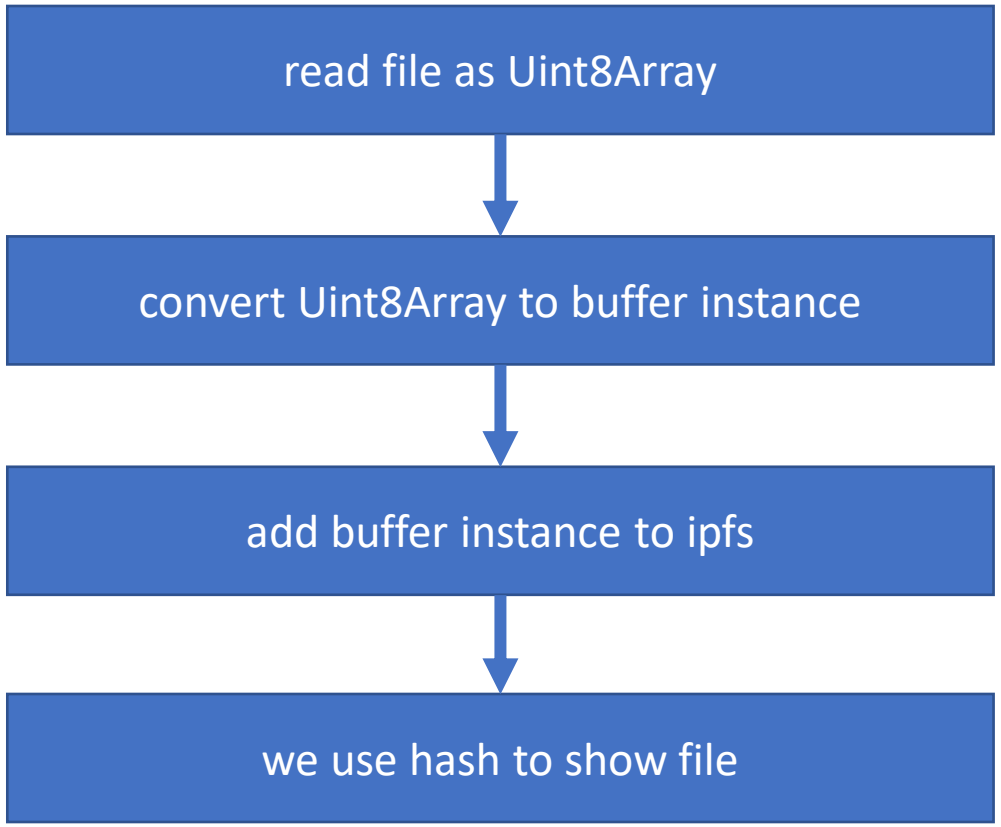
2. require('ipfs')

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
    <script src="bundle.js"></script>
    <script>
        const IPFS = require('ipfs')
        const Buffer = require('buffer') </script>
</head>
<body>
    <!--UI done!-->
</body>
</html>
```

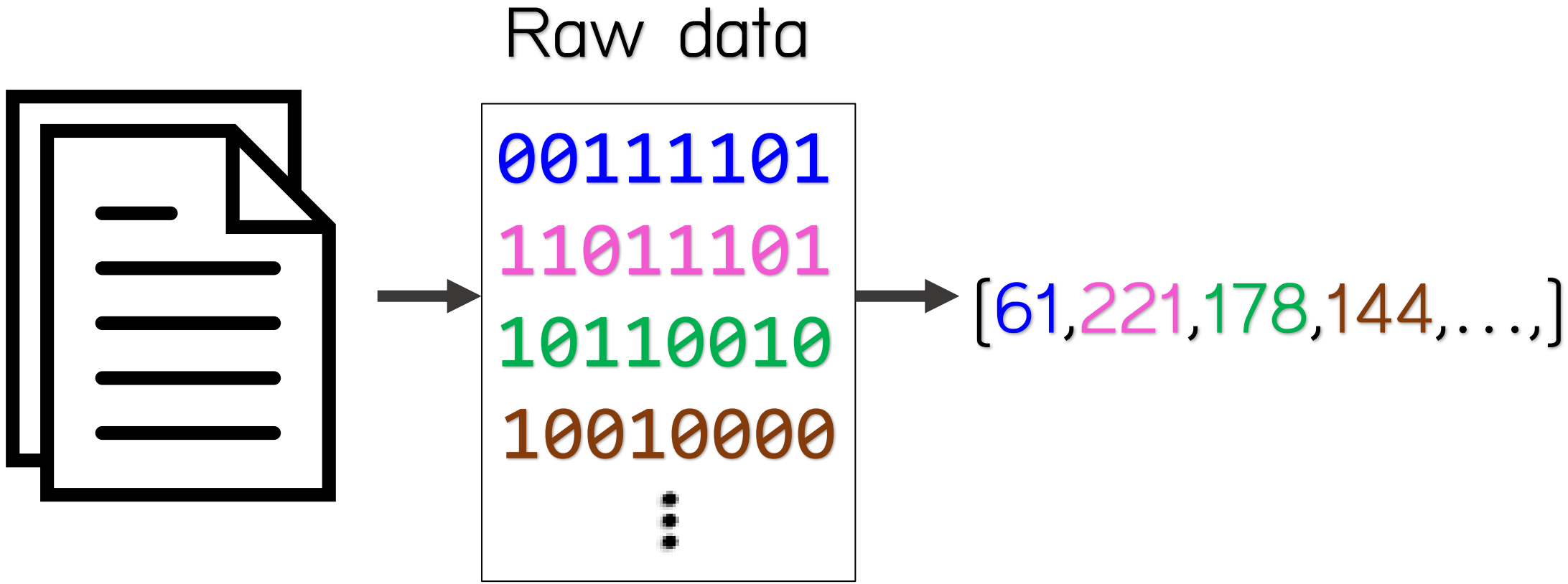
3. node instance

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
    <!--require done!-->
    <script>
        let node
        IPFS.create().then((res)=>{
        node =res
        })
        console.log('IPFS node is ready')
    </script>
</head>
<body>
    <!--UI done!-->
</body>
</html>
```

4. store()


read file as Uint8Array
convert Uint8Array to buffer instance
add buffer instance to ipfs
we use hash to show file

4.1 file to Uint8Array



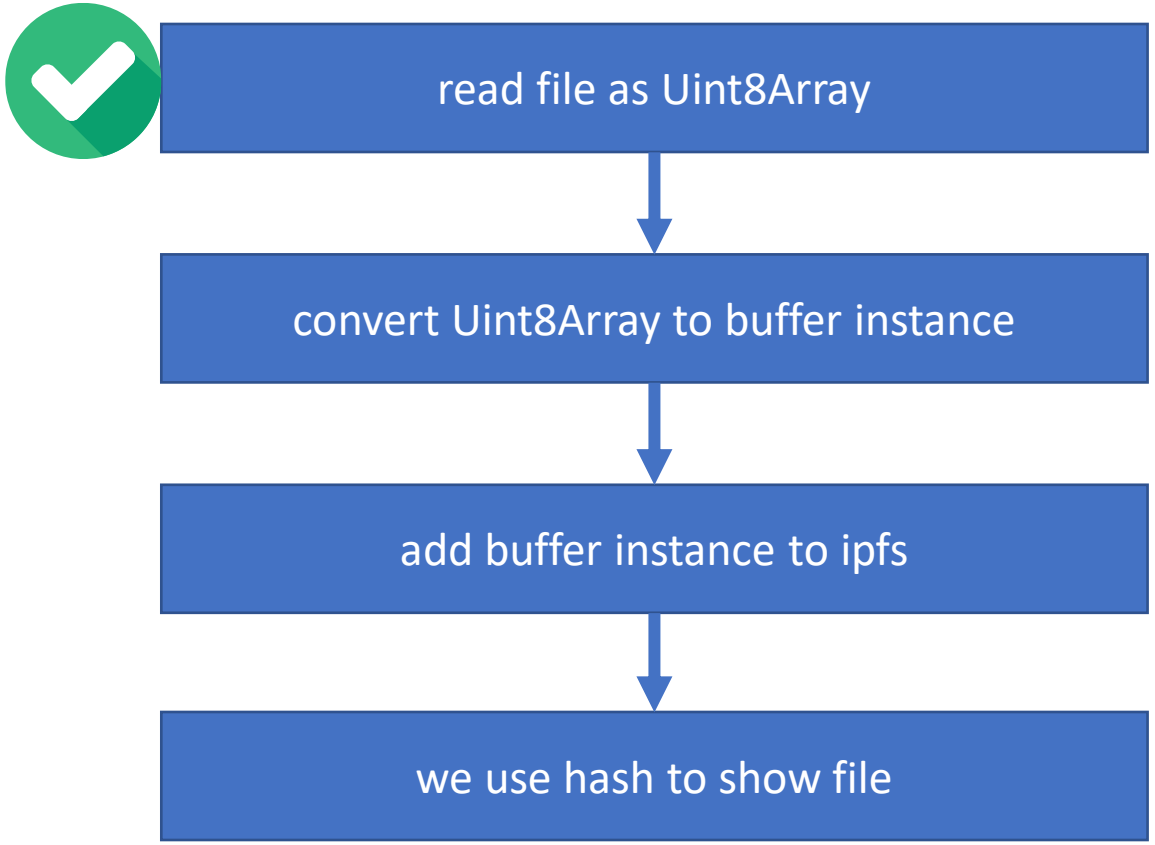
https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/ArrayBuffer#Properties

4.1 file to Uint8Array

```
async function store(){
        let selectedFile = document.getElementById("source").files
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0]
            let fileReader = new FileReader()

            fileReader.onloadend = async function(fileLoadedEvent) {
                let uint8Array = fileLoadedEvent.target.result
                 //uint8Array is stored in variable uint8Array
            };

            await fileReader.readAsArrayBuffer(fileToLoad)//read data as uint8Array
        }
    }
```

https://developer.mozilla.org/en-US/docs/Web/API/FileReader
https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/ArrayBuffer#Properties

4.1 file to Uint8Array



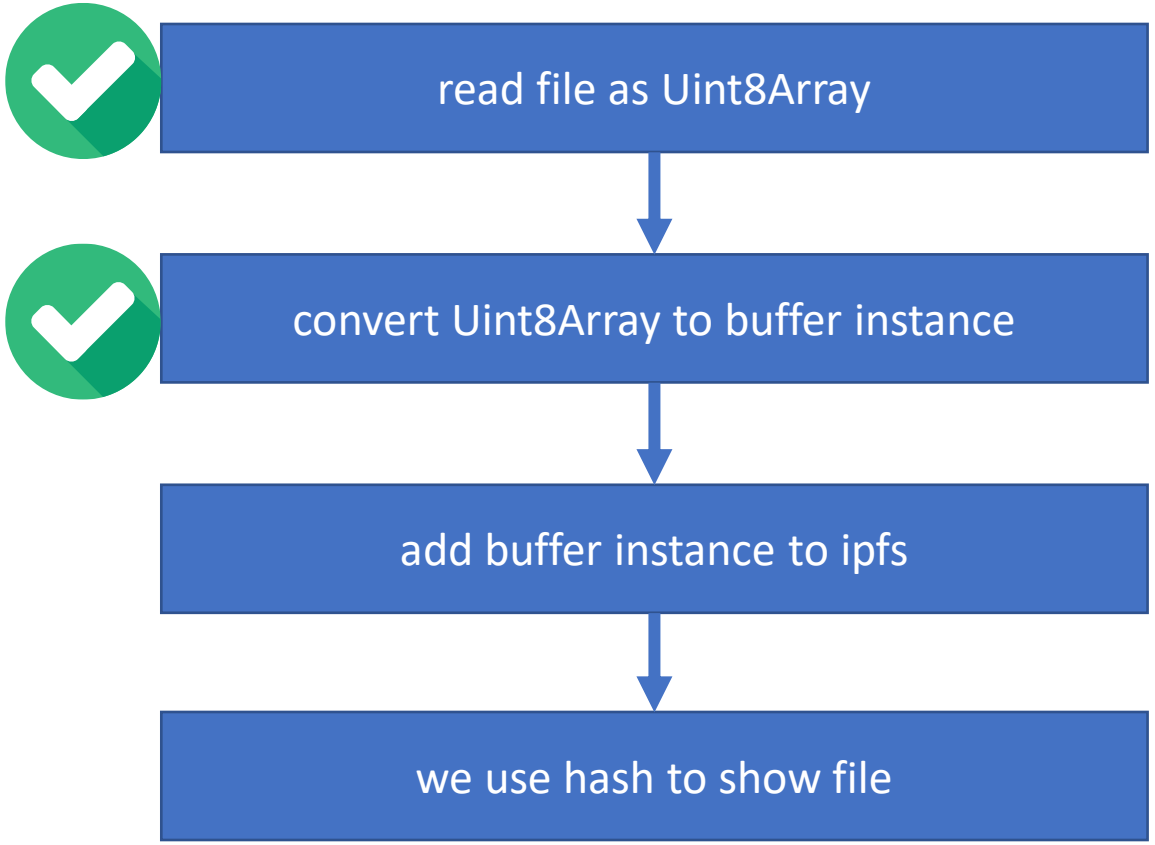

```
read file=                                                    ipfs.html:28
▼ ArrayBuffer(266289) {}
  ▶ [[Int8Array]]: Int8Array(266289) [37, 80, 68, 70, 45, 49, 4…
  ▶ [[Uint8Array]]: Uint8Array(266289) [37, 80, 68, 70, 45, 49,…
    byteLength: (...)
  ▶ __proto__: ArrayBuffer
```

4.2 buffer instance

```
async function store(){
        let selectedFile = document.getElementById("source").files
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0]
            let fileReader = new FileReader()

            fileReader.onloadend = async function(fileLoadedEvent) {
                let uint8Array = fileLoadedEvent.target.result;
                let buff = Buffer.Buffer(fileLoadedEvent.target.result)
                //convert uint8Array buffer to a buffer instance
            };

            await fileReader.readAsArrayBuffer(fileToLoad)//read data as uint8Array
        }
    }
```

https://www.npmjs.com/package/buffer

4.2 buffer instance



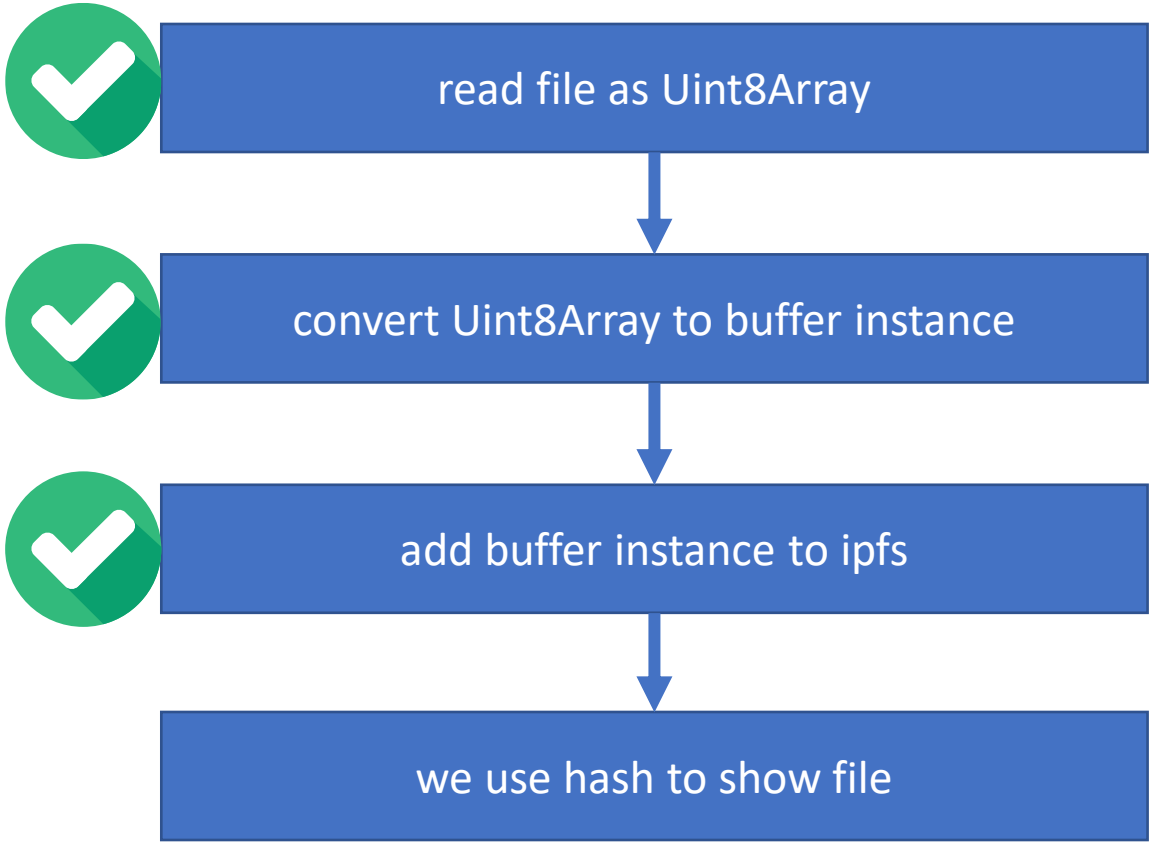

```
buff=                                                    ipfs.html:30
  Uint8Array(266289) [37, 80, 68, 70, 45, 49, 46, 55, 13, 10, 37
  , 181, 181, 181, 181, 13, 10, 49, 32, 48, 32, 111, 98, 106, 13
  , 10, 60, 60, 47, 84, 121, 112, 101, 47, 67, 97, 116, 97, 108,
  111, 103, 47, 80, 97, 103, 101, 115, 32, 50, 32, 48, 32, 82, 4
  7, 76, 97, 110, 103, 40, 101, 110, 45, 85, 83, 41, 32, 47, 83,
  116, 114, 117, 99, 116, 84, 114, 101, 101, 82, 111, 111, 116,
  32, 51, 48, 32, 48, 32, 82, 47, 77, 97, 114, 107, 73, 110, 102
  , 111, 60, 60, 47, …]
```

4.3 add to ipfs

```
async function store(){
        let selectedFile = document.getElementById("source").files
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0]
            let fileReader = new FileReader()

            fileReader.onloadend = async function(fileLoadedEvent) {
                let uint8Array = fileLoadedEvent.target.result
                let buff = Buffer.Buffer(fileLoadedEvent.target.result)
                const res = await node.add(buff)//add buffer to ipfs
            };

            await fileReader.readAsArrayBuffer(fileToLoad)//read data as uint8Array
        }
    }
```

https://github.com/ipfs/js-ipfs

4.3 add to ipfs

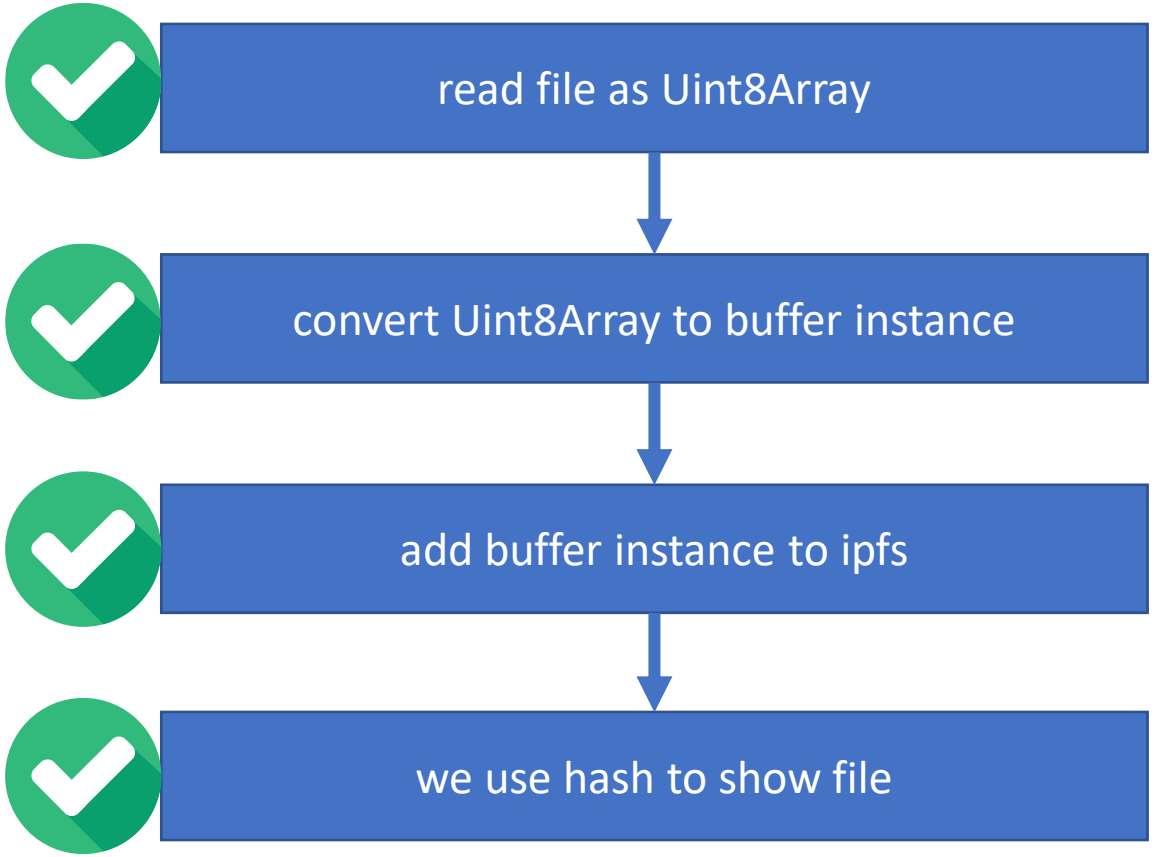



```
res=                                                    ipfs.html:32
▼[{…}] t
  ▼0:
      hash: "QmYgXPUvjwWsa2JFAy3HjoXshYK7n3ZQScFSKtXToAgZGc"
      path: "QmYgXPUvjwWsa2JFAy3HjoXshYK7n3ZQScFSKtXToAgZGc"
      size: 266416
    ▶__proto__: Object
    length: 1
  ▶__proto__: Array(0)
```

4.3 add to ipfs

```
function store(){
    let selectedFile = document.getElementById("source").files
    if (selectedFile.length > 0) {
        let fileToLoad = selectedFile[0]
        let fileReader = new FileReader()

        fileReader.onloadend = async function(fileLoadedEvent) {
            let uint8Array = fileLoadedEvent.target.result
            let buff = Buffer.Buffer(fileLoadedEvent.target.result)
            const res = await node.add(buff)
            hash = res[0].hash
            let url = 'https://ipfs.io/ipfs/'+hash
            console.log('url =',url)
            document.getElementById('hash').value = hash
            document.getElementById('url').innerHTML = url
            document.getElementById('url').href = url
            document.getElementById('content').src= url

            let data = await node.cat(hash)
            console.log("data = ",data)
        }
        await fileReader.readAsArrayBuffer(fileToLoad);//read data as uint8Array
    }
}
```

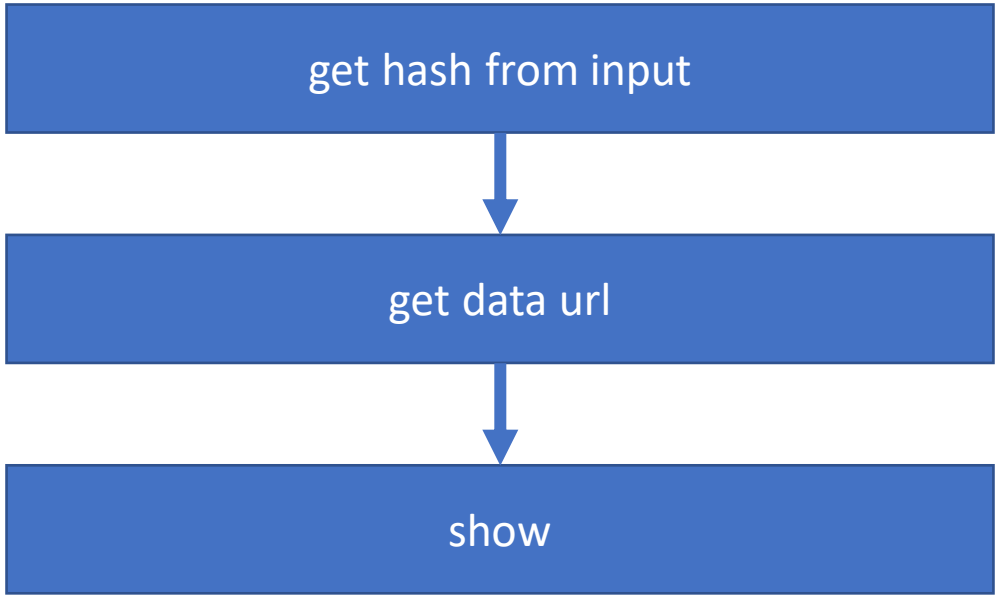
4. store()


read file as Uint8Array
convert Uint8Array to buffer instance
add buffer instance to ipfs
we use hash to show file

4. store()

```
async function store(){
        let selectedFile = document.getElementById("source").files
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0]
            let fileReader = new FileReader()
            fileReader.onloadend = async function(fileLoadedEvent) {
                let uint8Array = fileLoadedEvent.target.result
                let buff = Buffer.Buffer(fileLoadedEvent.target.result)
                const res = await node.add(buff)
                hash = res[0].hash
                let url = 'https://ipfs.io/ipfs/'+hash
                console.log('url =',url)
                document.getElementById('hash').value = hash
                document.getElementById('url').innerHTML = url
                document.getElementById('url').href = url
                document.getElementById('content').src= url

                let data = await node.cat(hash)
                console.log("data = ",data)
            }
            await fileReader.readAsArrayBuffer(fileToLoad);//read data as uint8Array
        }
    }
```

5. show()



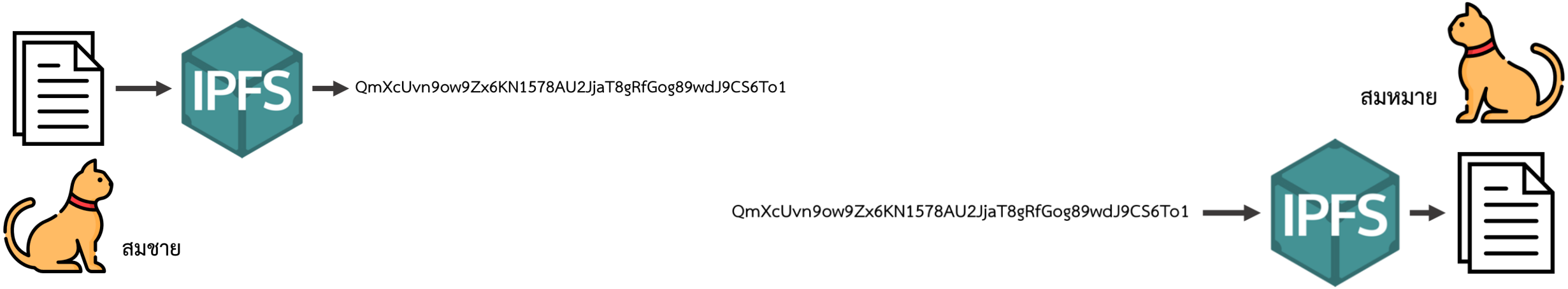
5. show()

```
async function show(){
        let hash = document.getElementById('hash').value
        let data = await node.cat(hash)
        let url = 'https://ipfs.io/ipfs/'+hash
        document.getElementById('url').innerHTML = url
        document.getElementById('url').href = url
        document.getElementById('content').src= url
        data = await node.cat(hash)
        console.log("data = ",data)
    }
```

full code

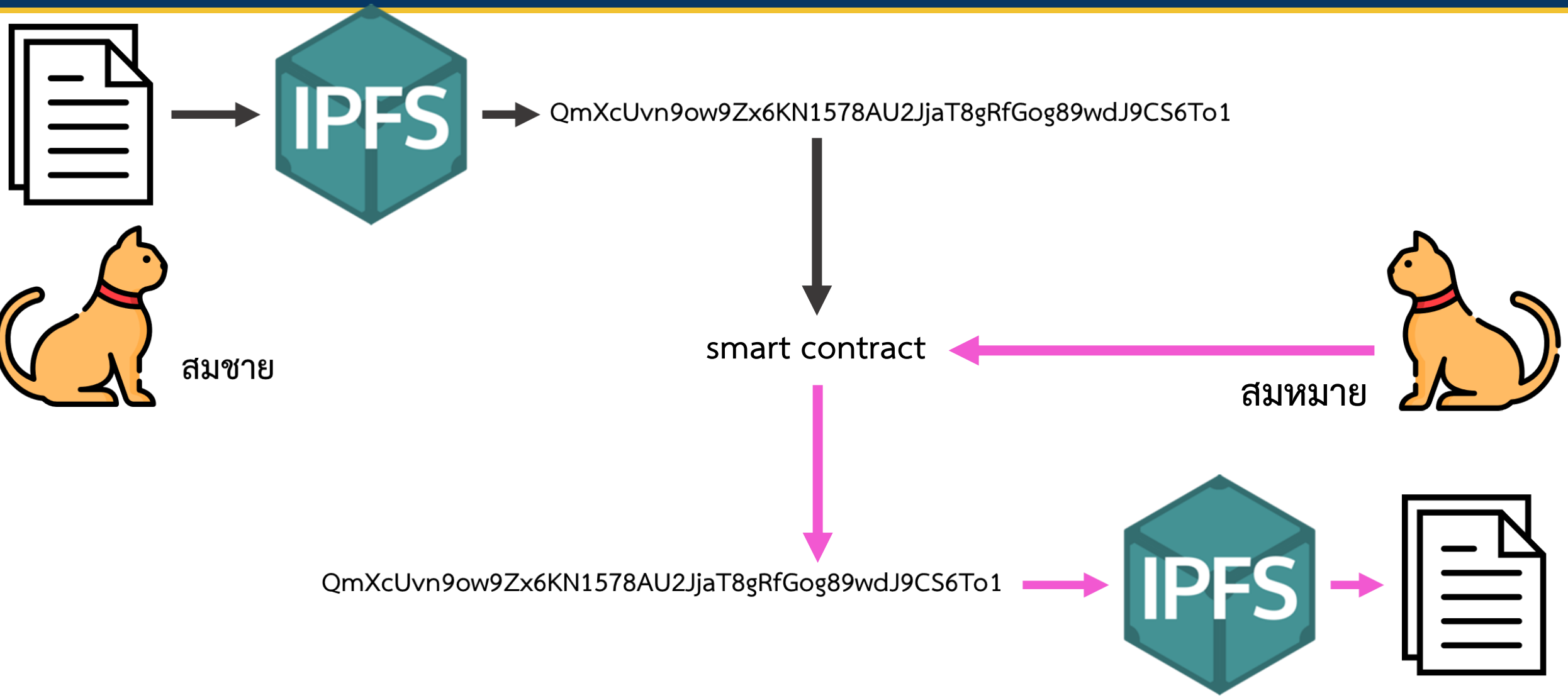
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title><!DOCTYPE html>
    <script src="bundle.js"></script>
    <script>
        const IPFS = require('ipfs')
        const Buffer = require('buffer')
        let node
        IPFS.create({ repo: String(Math.random() + Date.now()) }).then((res)=>{
        node =res;
        })
        console.log('IPFS node is ready')

        async function store(){
        let selectedFile = document.getElementById("source").files;
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0];
            let fileReader = new FileReader();
            fileReader.onloadend = async function(fileLoadedEvent) {
                buff = Buffer.Buffer(fileLoadedEvent.target.result)//convert array buffer to buffer
                const res = await node.add(buff)//add buffer to ipfs
                hash = res[0].hash
                let url = 'https://ipfs.io/ipfs/'+hash
                console.log('url =',url);
                document.getElementById('hash').value = hash
                document.getElementById('url').innerHTML = url
                document.getElementById('url').href = url
                document.getElementById('content').src= url

                data = await node.cat(hash)
                console.log("data = ",data)
            };

            await fileReader.readAsArrayBuffer(fileToLoad);//read data as array buffer
        }
    }

    async function show(){
        let hash = document.getElementById('hash').value
        let data = await node.cat(hash)
        let url = 'https://ipfs.io/ipfs/'+hash
        document.getElementById('url').innerHTML = url
        document.getElementById('url').href = url
        document.getElementById('content').src= url
        data = await node.cat(hash)
        console.log("data = ",data)
    }
    </script>
</head>
<body>
    <h1>JS IPFS - Add data to IPFS from the browser</h1>
    <input type="file" id="source"></input>
    <button onclick="store()">add to ipfs</button>
    <div>found in ipfs:</div>
    <input type="text" id="hash" value="[ipfs hash]">
    <button onclick="show()">show</button><br>
    <a id="url">[ipfs url]</a>
    <iframe id="content" width="100%" height="400">[ipfs content]</iframe>
</body>
</html>
```

ipfs + blockchain!??



Where is blockchain include!??

flowchart!


IPFS
QmXcUvn9ow9Zx6KN1578AU2JjaT8gRfGog89wdJ9CS6To1
สมชาย
smart contract
สมหมาย
QmXcUvn9ow9Zx6KN1578AU2JjaT8gRfGog89wdJ9CS6To1
IPFS

set contract()

```
pragma solidity ^0.5.11;

contract hashStorage {
    string public ipfsHash;
    address public owner;

    constructor()public{
        owner = msg.sender;
    }

    function addHash(string memory _ipfsHash)public {
        require(msg.sender == owner);
        ipfsHash=_ipfsHash;
    }
}
```

html change

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title><!DOCTYPE html>
    <script src="bundle.js"></script>
    <script>
        const IPFS = require('ipfs')
        const Buffer = require('buffer')
        const Web3 = require('web3')
        ethereum.enable().then(x=>{console.log(x)})
        const web3 = new Web3(Web3.givenProvider || new Web3.providers.HttpProvider('http://localhost:8545'))

        const contractABI=[ ···

        const contractAddress="0x5e050bde777039933d646ddb6ce1de104f6565dc"
        const ipfsContract = new web3.eth.Contract(contractABI,contractAddress)


        let node
        IPFS.create({ repo: String(Math.random() + Date.now()) }).then((res)=>{
        node =res;
        })
        console.log('IPFS node is ready')
```

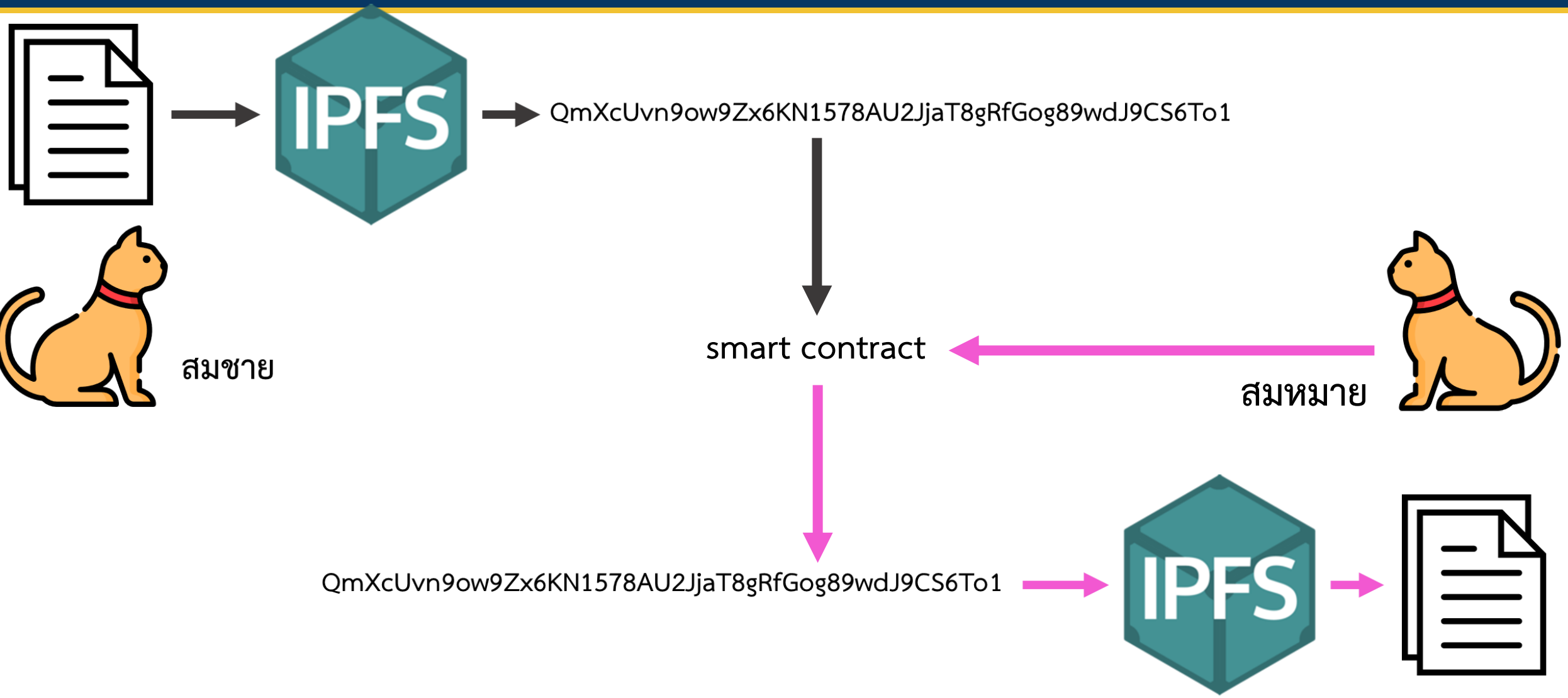
html change

```
async function store(){
let selectedFile = document.getElementById("source").files;
if (selectedFile.length > 0) {
    let fileToLoad = selectedFile[0];
    let fileReader = new FileReader();
    fileReader.onloadend = async function(fileLoadedEvent) {
        buff = Buffer.Buffer(fileLoadedEvent.target.result)//convert array buffer to buffer
        const res = await node.add(buff)//add buffer to ipfs
        hash = res[0].hash
        let url = 'https://ipfs.io/ipfs/'+hash
        console.log('url =',url);
        document.getElementById('hash').value = hash
        document.getElementById('url').innerHTML = url
        document.getElementById('url').href = url
        document.getElementById('content').src= url

        data = await node.cat(hash)
        console.log("data = ",data)

        let wallet = await web3.eth.getAccounts()
        let result = await ipfsContract.methods.addHash(hash).send({from: wallet[0]})
        console.log(result)
    };

    await fileReader.readAsArrayBuffer(fileToLoad);//read data as array buffer
}
}
```

html change

```
async function show_eth(){
        let hash = await ipfsContract.methods.ipfsHash().call();
        document.getElementById('hash').value = hash
        let data = await node.cat(hash)
        let url = 'https://ipfs.io/ipfs/'+hash
        document.getElementById('url').innerHTML = url
        document.getElementById('url').href = url
        document.getElementById('content').src= url
    }
```

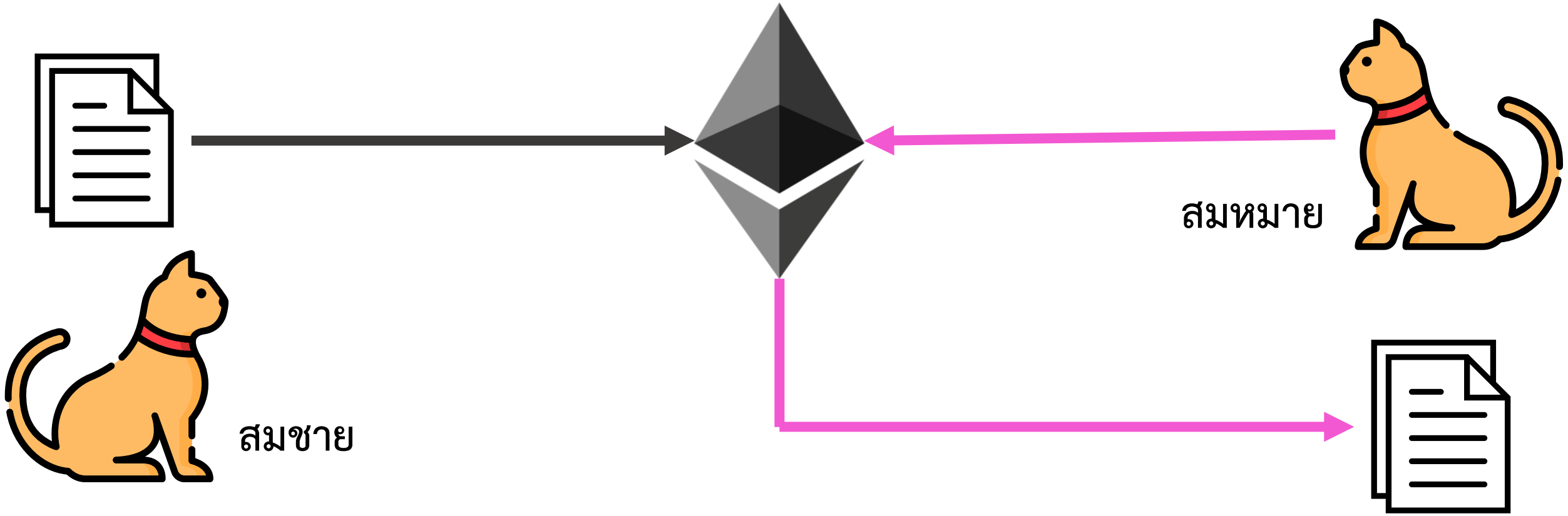
flowchart!


IPFS
QmXcUvn9ow9Zx6KN1578AU2JjaT8gRfGog89wdJ9CS6To1
สมชาย
smart contract
สมหมาย
QmXcUvn9ow9Zx6KN1578AU2JjaT8gRfGog89wdJ9CS6To1
IPFS

ประเทศกูมี

QmXFf5QLQi3DhbwyrgR7qH8tHAZcGyWtWtsBy6iij4B7aL

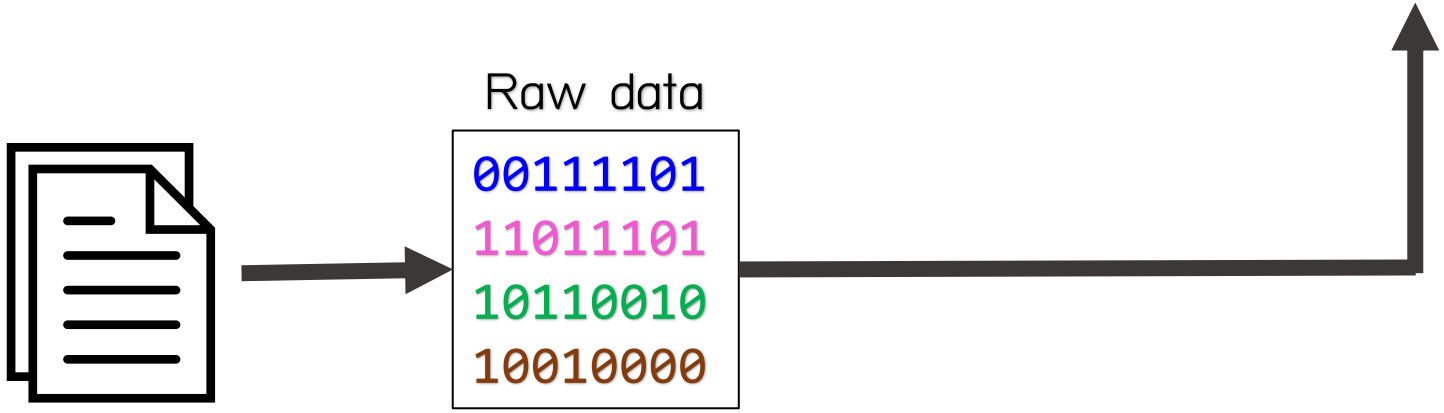
Byte



dataURL

```
data:[<mediatype>][;base64],<data>
```

```
data:application/pdf;base64,3dddb290…
```



https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Data_URIs

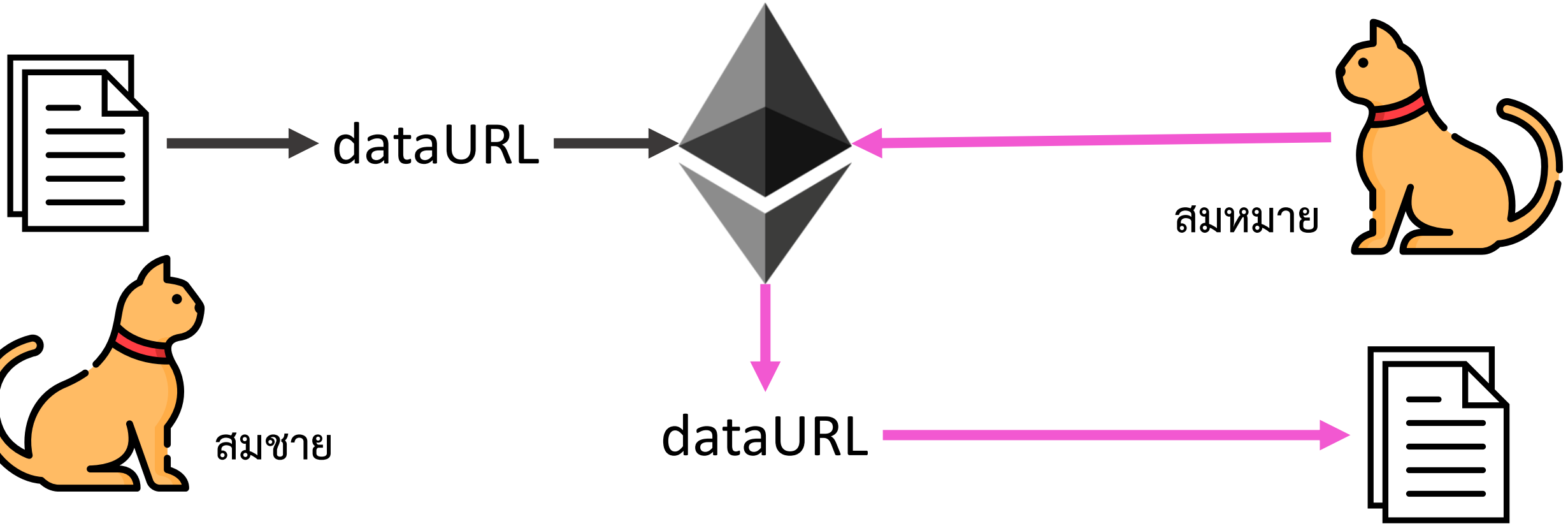
dataURL

```
data:text/plain;base64,<data>
<data>
data:video/mp4;base64,<data>
```

More Info ...

https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types

flowChart



contract

```
pragma solidity ^0.5.11;
contract Storage{
    string public dataURL;

    function set(string memory _dataURL)public{
        dataURL = _dataURL;
    }
}
```

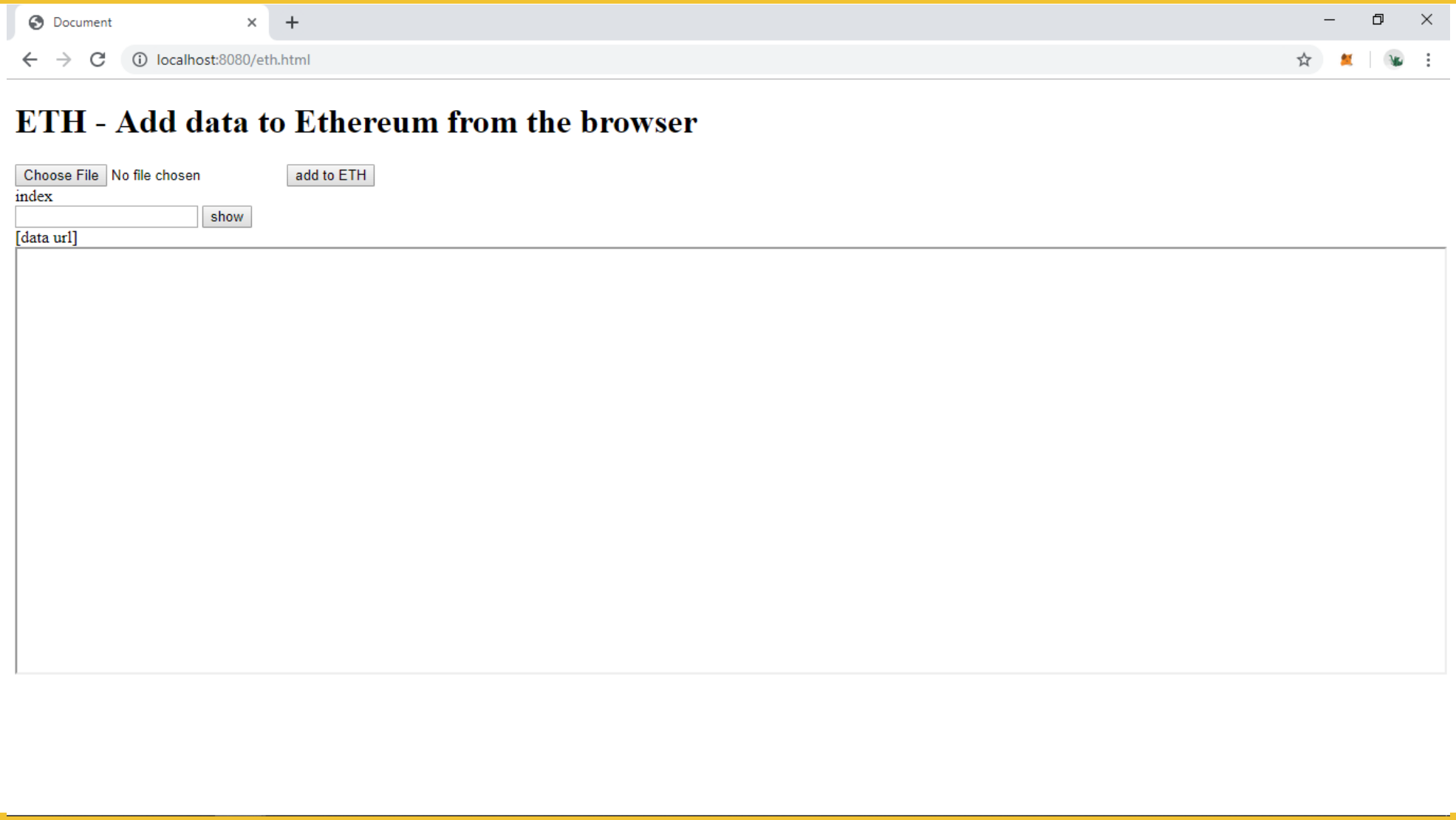
error!

```
c615932526c5a6d646f6157707a64485632643368356 56f4f45685961486949
6d4b6b704f556c5a61586d4a6d616f714f6b7061616e714b6d7173724f30746
26133754c6d3677735045786362487 94d6e4b3074505531646258324e6e6134
654c6a354f586d352b6a7036764879382f5431397666342b66722f784141664
151414441514542415145424151454241414141414141414151494442415547
4277674a4367762f7841433145514143415149454241 4d45427755454241414
2416e6341415149444551514649544547456b4652423246784579479675167
5551704768736345 4a497a4e5338425669637445 4b4669513034535878467 86
75a4769596e4b436b714e5459334f446b3651305246526b6449535570545646
56575631685a576d4a6b5a575a6e61476c7165555 2916 46e6346558714367 3
45346 86f6549695971536b3553566c70 Show more (1.4 MB) Copy
{code: -32603, message: "Error: Error: [ethjs-rpc] rpc error w
ith payload {…":"eth_sendRawTransaction"} Error: oversized dat
a"} i
  code: -32603
  message: "Error: Error: [ethjs-rpc] rpc error with payload {
  __proto__: Object
```

contract

```
pragma solidity ^0.5.11;
contract Storage{
    bytes public dataURL;
    bytes public a;

    function set(string memory _dataURL)public{
        a = bytes(_dataURL);
        for(uint i=0;i<a.length;i++){
            dataURL.push(a[i]);
        }
    }

    function clear()public{
        dataURL = "";
    }
}
```

1. UI


Document
localhost:8080/eth.html
ETH - Add data to Ethereum from the browser
Choose File
No file chosen
add to ETH
index
show
[data url]

1. UI

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
</head>
<body>
    <h1>ETH - Add data to Ethereum from the browser</h1>
    <input type="file" id="source"></input>
    <button onclick="store()">add to ETH</button>
    <div>index</div>
    <input type="number" id="index" value="">
    <button onclick="show()">show</button><br>
    <a id="url">[data url]</a>
    <iframe id="content" width="100%" height="400">[data content]</iframe>
 </body>
</html>
```

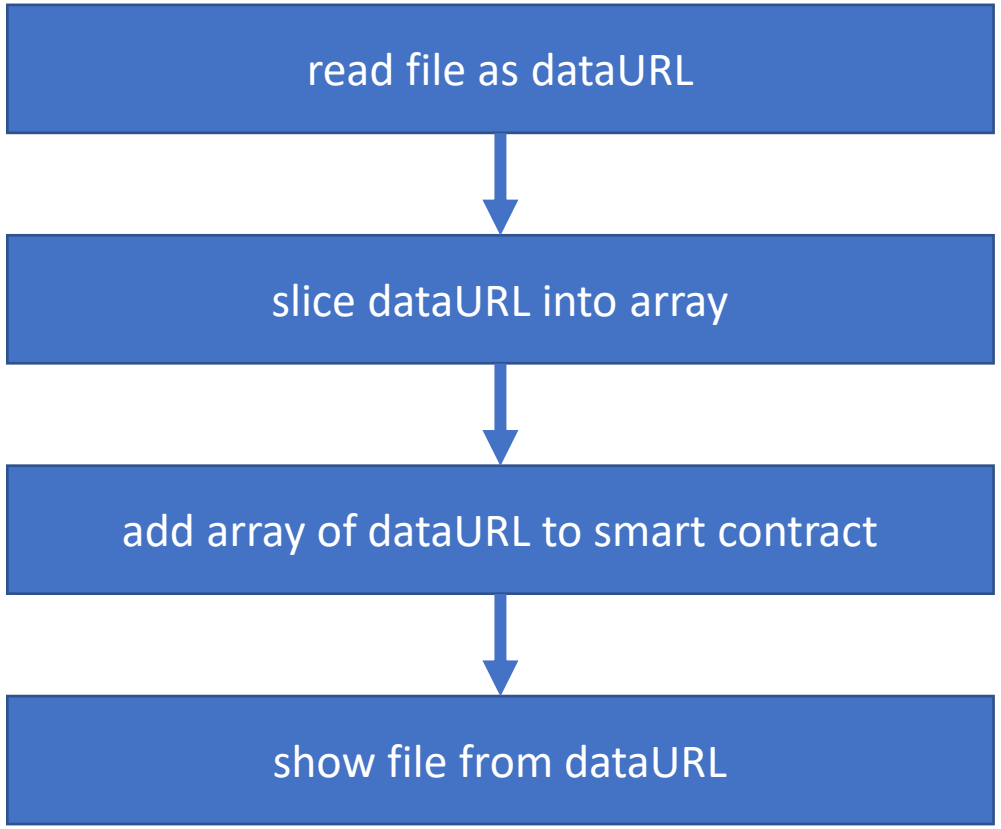
2. connect to contract

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
    <script src="bundle.js"></script>
    <script>
        const Web3 = require('web3')
        //ethereum.enable().then(x=>{console.log(x)})
        const web3 = new Web3(Web3.givenProvider)

        const contractABI = [ ... ]
        const contractAddress="0xbd2627f94b55c42525da8374814287f13b63ce56"
        const byteContract = new web3.eth.Contract(contractABI,contractAddress)
    </script>
</head>
<body>
    <!--UI done!-->
 </body>
</html>
```

2. connect to contract

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!--meta and title done!-->
    <script src="bundle.js"></script>
    <script>
        const Web3 = require('web3')
        //ethereum.enable().then(x=>{console.log(x)})
        const web3 = new Web3(Web3.givenProvider)

        const contractABI = [ ... ]
        const contractAddress="0xbd2627f94b55c42525da8374814287f13b63ce56"
        const byteContract = new web3.eth.Contract(contractABI,contractAddress)
    </script>
</head>
<body>
    <!--UI done!-->
 </body>
</html>
```

3. store()

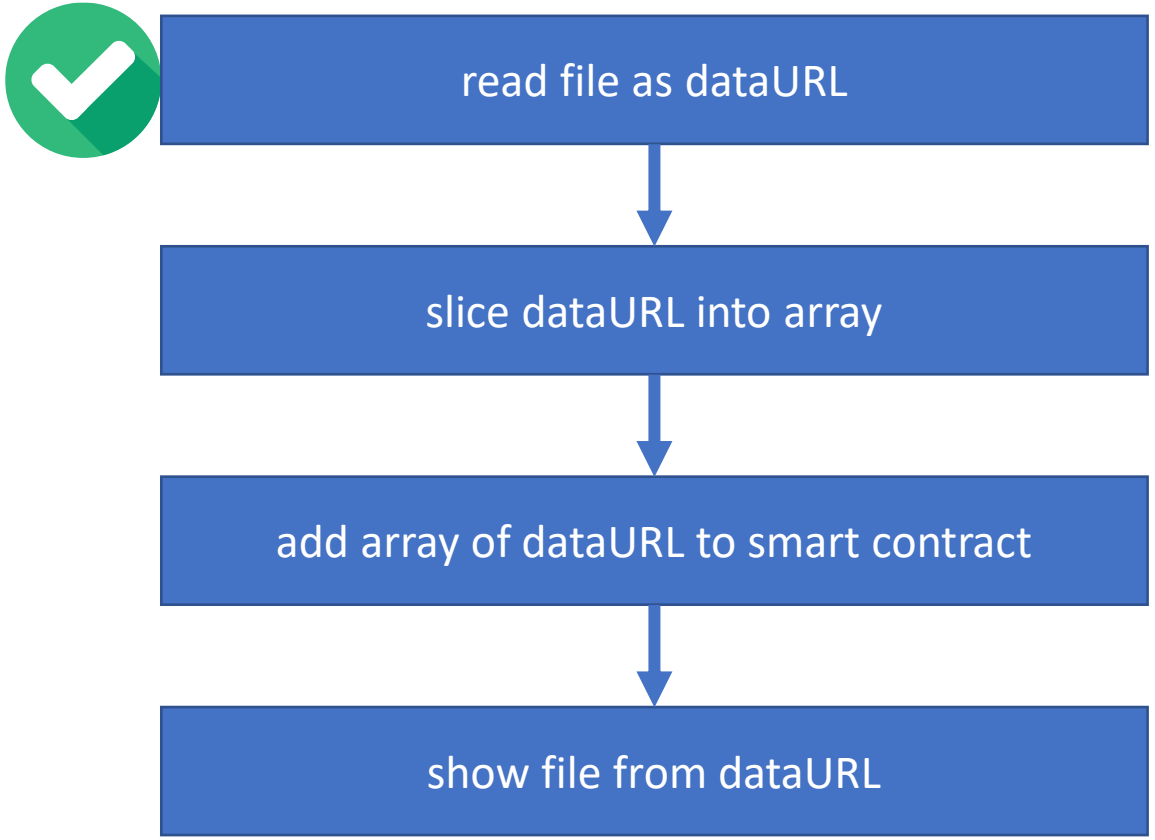

read file as dataURL
slice dataURL into array
add array of dataURL to smart contract
show file from dataURL

3.1 file to dataURL

```
async function store(){
        let selectedFile = document.getElementById("source").files
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0]
            let fileReader = new FileReader()

            fileReader.onloadend = async function(fileLoadedEvent) {
                let dataURL = fileLoadedEvent.target.result
                 // dataURL is stored in variable dataURL
            };

            fileReader.readAsDataURL(fileToLoad)//read data as dataURL
        }
    }
```

https://developer.mozilla.org/en-US/docs/Web/API/FileReader

3.1 file to dataURL



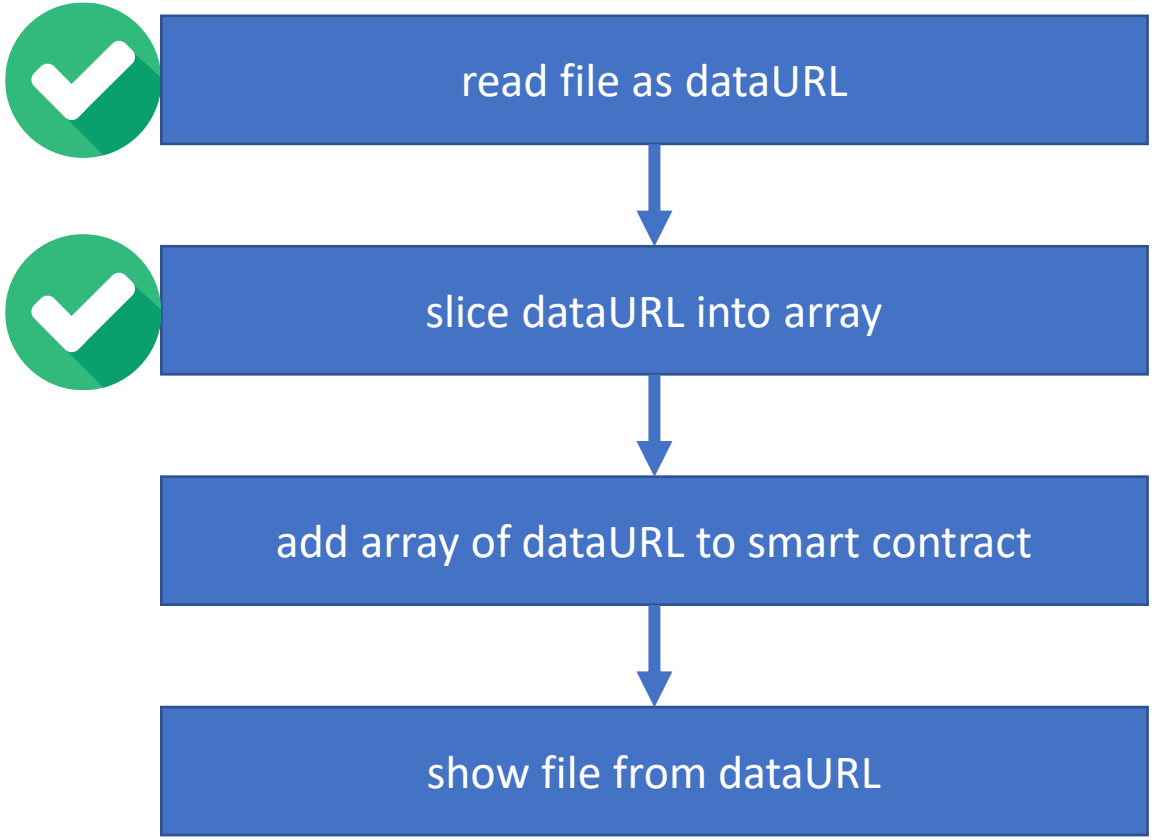
dataURL= eth.html:25
Rw0KGgoAAAANSUhEUgAAAXwAAADPCAIAAAB5rP3yAAAAAXNS
R…VEBygl0kAp0QFKiQ5QSnSAUqIDlBIdoJToAKVEByj0+/f/
AI0GLsLHE0+wAAAAAElFTkSuQmCC

3.2 slice into array

```
async function store(){
        let selectedFile = document.getElementById("source").files
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0]
            let fileReader = new FileReader()

            fileReader.onloadend = async function(fileLoadedEvent) {
                let dataURL = fileLoadedEvent.target.result
                let dataURLSlice = dataURL.match(/.{1,500}/g)
                 // each elements contain 500 characters
                for(let i=0;i<dataURLSlice.length;i++){
                 // TODO
                }
            };

            fileReader.readAsDataURL(fileToLoad)
        }
    }
```

https://developer.mozilla.org/en-US/docs/Web/API/FileReader

3.2 file to dataURL




```
dataURLSlice=                                                    eth.html:83
▼ 0: "…
  1: "CnRKed/IbbfMs3NzefP39+8+ZNDuvv4u+cnZ1dX1/nI+E+rTfm79+/j1fzq1evctUBGN9…
  2: "q67fLksEqic+c8muJQoEV0wp2TLPNtgbEZ5Kqtik0rvvJ4iqHPLk8OaPfRWT2kCopDjS7…
  3: "h20ZlXkaI+uarQeOqQy0vIEWxjDA6saKhddJY6oTOMpw65vIQcwcZjuL6+dmBFQ72iE4c…
  4: "zyNOYh5PKa8sGiQ1ddXprOIk9jHkIurykfLDp01eWl6SzyNOYh5PKa8sGiQ1ddXprOIk9…
  5: "kJuWoDl5eXR0dH+eX+L+Z8pzs+sZO1elJpVVQv/xIHafnoOLa615iTkMsbuzc9W9nxib5…
  6: "SAUqIDlBIdoJToAKVEByglOkAp0QFKiQ5QSnSAUqIDlBIdoJToAKVEByglOkAp0QFKiQ5…
  length: 7
▶ __proto__: Array(0)
```

3.3 add to contract

1. `tx` - `Object` : **The transaction object as follows:**
    - `nonce` - `String` : (optional) The nonce to use when signing this transaction. Default will use web3.eth.getTransactionCount().
    - `chainId` - `String` : (optional) The chain id to use when signing this transaction. Default will use web3.eth.net.getId().
    - `to` - `String` : (optional) The recevier of the transaction, can be empty when deploying a contract.
    - `data` - `String` : (optional) The call data of the transaction, can be empty for simple value transfers.
    - `value` - `String` : (optional) The value of the transaction in wei.
    - `gasPrice` - `String` : (optional) The gas price set by this transaction, if empty, it will use web3.eth.gasPrice()
    - `gas` - `String` : The gas provided by the transaction.

https://web3js.readthedocs.io/en/v1.2.1/web3-eth-accounts.html?highlight=rawtransaction#signtransaction

3.3 add to contract

```
for(let i=0;i<dataURLSlice.length;i++){
    let tx = {
        nonce: ,
        gasPrice: ,
        gas: ,
        to: ,
        value: "",
        data:
    }
}
```

https://web3js.readthedocs.io/en/v1.2.1/web3-eth-accounts.html?highlight=rawtransaction#signtransaction

3.3.1 nonce

```
for(let i=0;i<dataURLSlice.length;i++){
    let wallet = await web3.eth.getAccounts()
    let latestNonce = await web3.eth.getTransactionCount(wallet[0])
    let tx = {
        nonce: latestNonce,
        gasPrice: ,
        gas: ,
        to: ,
        value: "",
        data:
    }
}
```

3.3.2 gasPrice and gasUsed

```
for(let i=0;i<dataURLSlice.length;i++){
    let wallet = await web3.eth.getAccounts()
    let latestNonce = await web3.eth.getTransactionCount(wallet[0]);
    let estimateGas = await byteContract.methods.set(dataURLSlice[i]).estimateGas({from: wallet[0]})
    let tx = {
        nonce: latestNonce,
        gasPrice: web3.utils.toHex(web3.utils.toWei('1', 'gwei')),
        gas: web3.utils.toHex((estimateGas + 1000)),
        to: ,
        value: "",
        data:
    }
}
```

3.3.3 to

```
for(let i=0;i<dataURLSlice.length;i++){
    let wallet = await web3.eth.getAccounts()
    let latestNonce = await web3.eth.getTransactionCount(wallet[0]);
    let estimateGas = await byteContract.methods.set(dataURLSlice[i]).estimateGas({from: wallet[0]})
    let tx = {
        nonce: latestNonce,
        gasPrice: web3.utils.toHex(web3.utils.toWei('1', 'gwei')),
        gas: web3.utils.toHex((estimateGas + 1000)),
        to: contractAddress,
        value: "",
        data:
    }
}
```

3.3.4 data

```
for(let i=0;i<dataURLSlice.length;i++){
    let wallet = await web3.eth.getAccounts()
    let latestNonce = await web3.eth.getTransactionCount(wallet[0]);
    let estimateGas = await byteContract.methods.set(dataURLSlice[i]).estimateGas({from: wallet[0]})
    let tx = {
        nonce: latestNonce,
        gasPrice: web3.utils.toHex(web3.utils.toWei('1', 'gwei')),
        gas: web3.utils.toHex((estimateGas + 1000)),
        to: contractAddress,
        value: "",
        data: byteContract.methods.set(dataURLSlice[i]).encodeABI()
    }
}
```

```
eth.html:97
{gasPrice: "10000000000", gas: "0x65fa93", to: "0xaae9eedf707340af01f01e6
▶ 6a13dca0dbc9f6542", value: "", data: "0x4ed3885e000000000000000000000000
000000000000000…833326c4f69306b392b77364c000000000000000000000000"}
```

3.3.5 signTransaction

```
for(let i=0;i<dataURLSlice.length;i++){
    let wallet = await web3.eth.getAccounts()
    let latestNonce = await web3.eth.getTransactionCount(wallet[0]);
    let estimateGas = await byteContract.methods.set(dataURLSlice[i]).estimateGas({from: wallet[0]})
    let tx = {
        nonce: latestNonce,
        gasPrice: web3.utils.toHex(web3.utils.toWei('1', 'gwei')),
        gas: web3.utils.toHex((estimateGas + 1000)),
        to: contractAddress,
        value: "",
        data: byteContract.methods.set(dataURLSlice[i]).encodeABI()
    }
    const privateKey = "0x262CA48C689471E77309BFD778628170F03B12C3C745670DEFF9D53B5E40066A"
    let signedTx = await web3.eth.accounts.signTransaction(tx,privateKey)
}
```

eth.html:100

```
{messageHash: "0x33fff2b0eb01f307a7c6f6784db97cee6bb306ee0de4f69bc806556d
2e66b0d1", v: "0x77", r: "0x89e0989ff9409dbb536f43e574fc028d27c036743387e
59644466f33a0630322", s: "0x6ca0a9b02c141788830a79e71b7bfb379953099669424
d7de22d7dd0867d6bb9", rawTransaction: "0xf902ab1b8502540be4008365fa9394aa
e9eedf707340af01…8830a79e71b7bfb379953099669424d7de22d7dd0867d6bb9"}
```

https://web3js.readthedocs.io/en/v1.2.0/web3-eth-accounts.html#signtransaction

3.3.6 sendTransaction

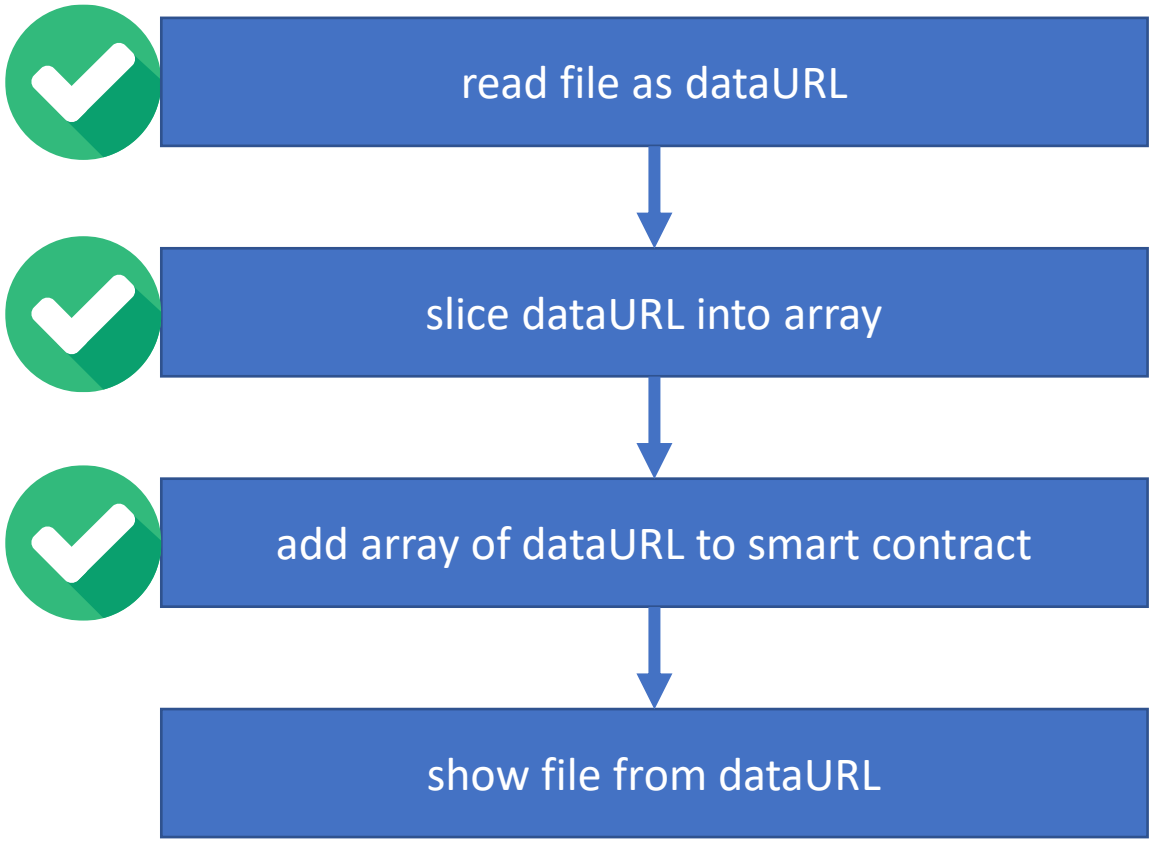
```
for(let i=0;i<dataURLSlice.length;i++){
    let wallet = await web3.eth.getAccounts()
    let latestNonce = await web3.eth.getTransactionCount(wallet[0]);
    let estimateGas = await byteContract.methods.set(dataURLSlice[i]).estimateGas({from: wallet[0]})
    let tx = {
        nonce: latestNonce,
        gasPrice: web3.utils.toHex(web3.utils.toWei('1', 'gwei')),
        gas: web3.utils.toHex((estimateGas + 1000)),
        to: contractAddress,
        value: "",
        data: byteContract.methods.set(dataURLSlice[i]).encodeABI()
    }
    const privateKey = "0x262CA48C689471E77309BFD778628170F03B12C3C745670DEFF9D53B5E40066A";
    let signedTx = await web3.eth.accounts.signTransaction(tx,privateKey)
    let res = await web3.eth.sendSignedTransaction(signedTx.rawTransaction)
    console.log(res)
}
```

eth.html:102

```
{blockHash: "0x3c2a8f249ec7e135d537642f1ee645648e6ebef2f5f193bc41be124f443f0b0c", blockNumber: 12867071, contractAddress: null, cumulativeGasUsed: 6424605, from: "0x00aa39d30f0d20ff03a22ccfc30b7efbfca597c2", …}
```

https://web3js.readthedocs.io/en/v1.2.0/web3-eth.html#sendsignedtransaction

3.3 add to contract

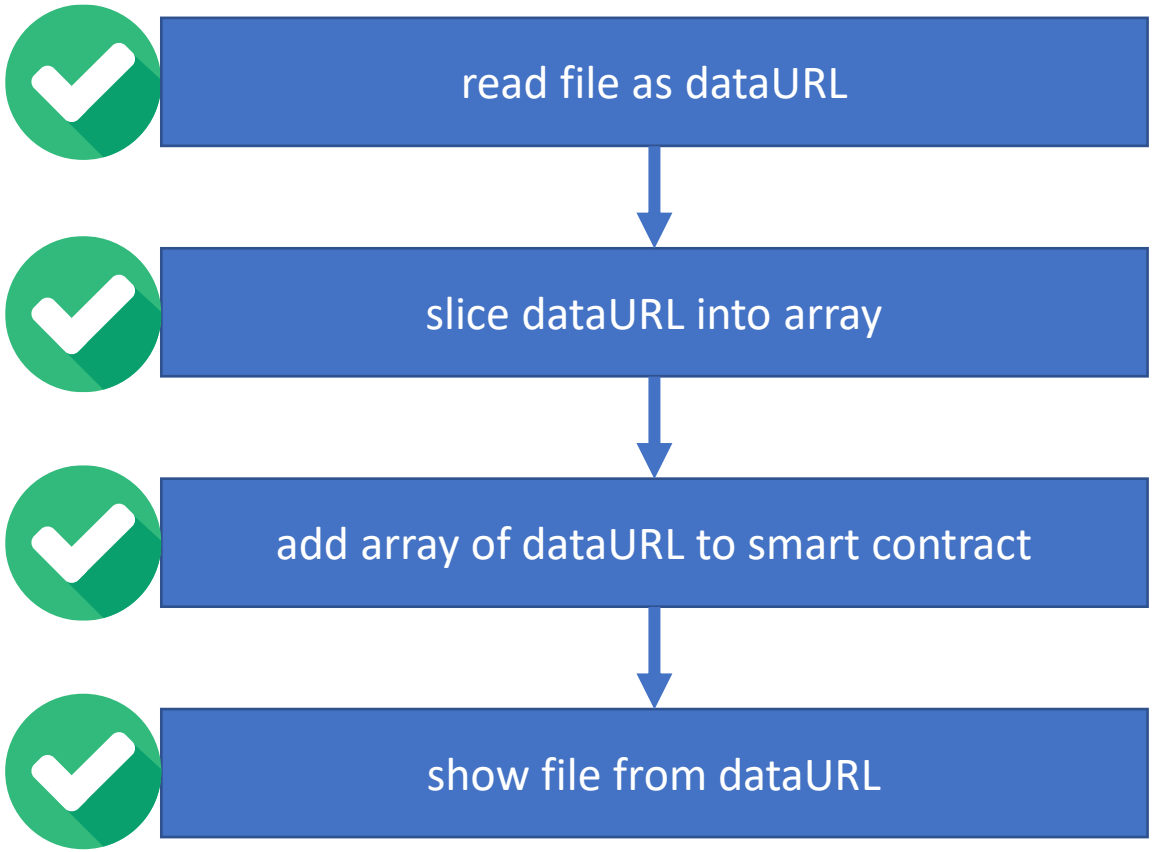



```
gas= 6683283                                                    eth.html:89

                                                                eth.html:97
  {gasPrice: "10000000000", gas: "0x65fa93", to: "0xaae9eedf707340af01f01e6
▶ 6a13dca0dbc9f6542", value: "", data: "0x4ed3885e000000000000000000000000000
  00000000000000…833326c4f69306b392b77364c000000000000000000000000"}

                                                                eth.html:100
  {messageHash: "0x33fff2b0eb01f307a7c6f6784db97cee6bb306ee0de4f69bc806556d
  2e66b0d1", v: "0x77", r: "0x89e0989ff9409dbb536f43e574fc028d27c036743387e
▶ 59644466f33a0630322", s: "0x6ca0a9b02c141788830a79e71b7bfb379953099669424
  d7de22d7dd0867d6bb9", rawTransaction: "0xf902ab1b8502540be4008365fa9394aa
  e9eedf707340af01…8830a79e71b7bfb379953099669424d7de22d7dd0867d6bb9"}

                                                                eth.html:102
  {blockHash: "0x0b9b635b1284e6f36005af15715f5bd7a8b6ab219ed289331ba0a8f5ce
▶ 8bf49c", blockNumber: 12867066, contractAddress: null, cumulativeGasUsed:
  6682283, from: "0x00aa39d30f0d20ff03a22ccfc30b7efbfca597c2", …}

gas= 6425605                                                    eth.html:89

                                                                eth.html:97
  {gasPrice: "10000000000", gas: "0x620c05", to: "0xaae9eedf707340af01f01e6
▶ 6a13dca0dbc9f6542", value: "", data: "0x4ed3885e000000000000000000000000000
  00000000000000…f473362392b4f4e6476795a330000000000000000000000000"}

                                                                eth.html:100
  {messageHash: "0x84858708060d88c96c4baa5dae8ed66bafc952c4f88210974942323d
  c05cafba", v: "0x78", r: "0x4bdb2d38b50e85b4c85963189fea24221c9a8a389a2f6
▶ 28f8eb7a4631dba34a", s: "0x63c71c1a2ec04b3133a2d3b25cd31bf6459d76ccf84a35
  a544173e2d1629397f", rawTransaction: "0xf902ab1c8502540be40083620c0594aae
  9eedf707340af01…133a2d3b25cd31bf6459d76ccf84a35a544173e2d1629397f"}

                                                                eth.html:102
  {blockHash: "0x3c2a8f249ec7e135d537642f1ee645648e6ebef2f5f193bc41be124f44
▶ 3f0b0c", blockNumber: 12867071, contractAddress: null, cumulativeGasUsed:
  6424605, from: "0x00aa39d30f0d20ff03a22ccfc30b7efbfca597c2", …}
```

3.4 show data

```
async function store() {
        let selectedFile = document.getElementById("source").files
        if (selectedFile.length > 0) {
            let fileToLoad = selectedFile[0]
            let fileReader = new FileReader()
            fileReader.onload = async function(fileLoadedEvent) {
                //dataURLSlice done!
                for(let i=0;i<dataURLSlice.length;i++){
                    //sendRawTransaction done!
                }
                let dataURLFromBlockchain = await byteContract.methods.dataURL().call()
                let hexURL = dataURLFromBlockchain.slice(2,dataURLFromBlockchain.length)// remove 0x
                let url = ""
                for (let i = 0; i < hexURL.length; i += 2) {
                    url += String.fromCharCode(parseInt(hexURL.substr(i, 2), 16));
                }
                console.log('url =',url)
                document.getElementById('url').innerHTML = url
                document.getElementById('url').href = url
                document.getElementById('content').src= url
            }
            fileReader.readAsDataURL(fileToLoad)
        }
    }
```

3.4 show data

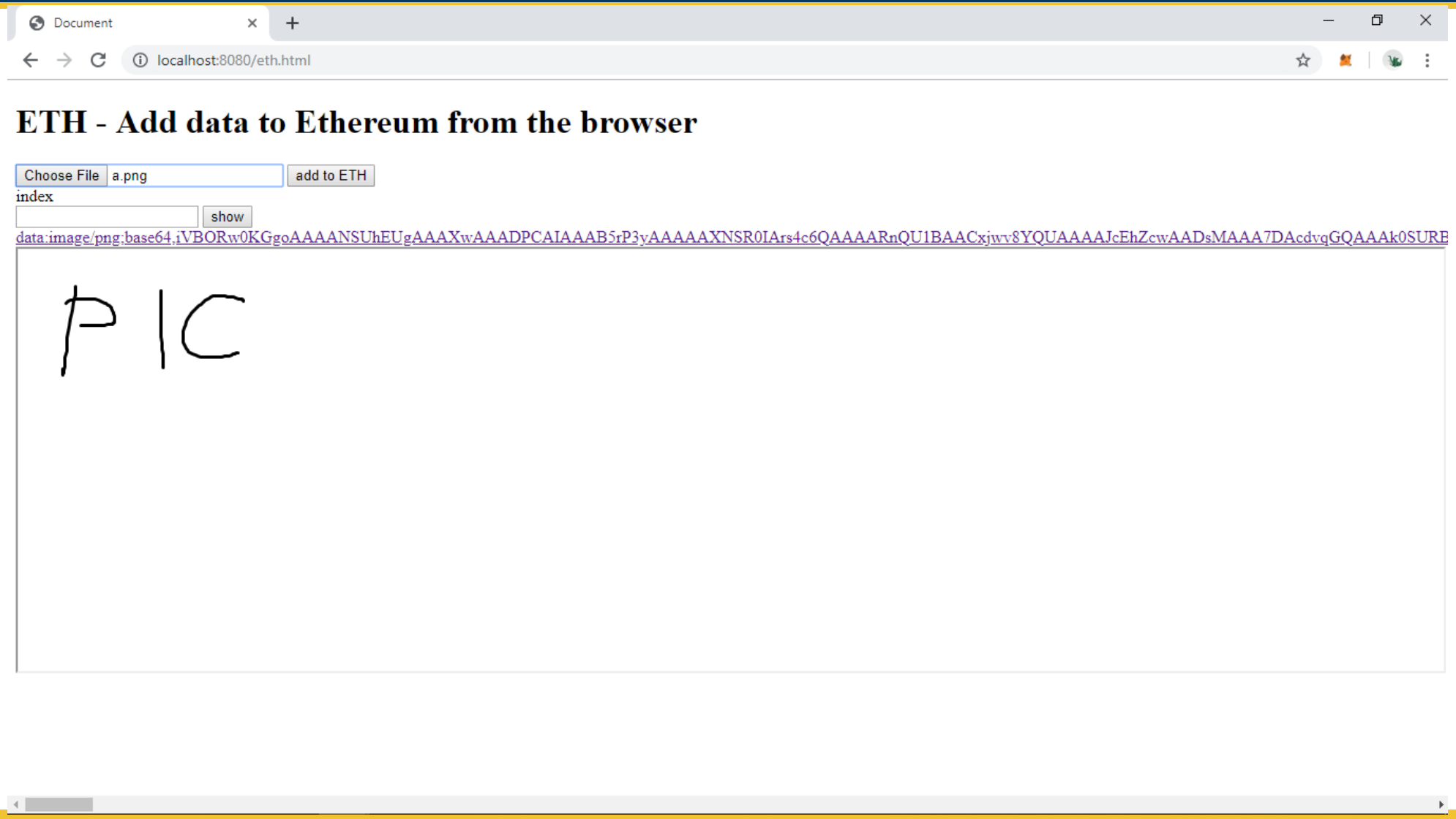



```
dataURLSlice=                                                    eth.html:83
▼ 0: "…
  1: "CnRKed/IbbfMs3NzefP39+8+ZNDuvv4u+cnZ1dX1/nI+E+rTfm79+/j1fzq1evctUBGN9…
  2: "q67fLksEqic+c8muJQoEV0wp2TLPNtgbEZ5Kqtik0rvvJ4iqHPLk8OaPfRWT2kCopDjS7…
  3: "h20ZlXkaI+uarQeOqQy0vIEWxjDA6saKhddJY6oTOMpw65vIQcwcZjuL6+dmBFQ72iE4c…
  4: "zyNOYh5PKa8sGiQ1ddXprOIk9jHkIurykfLDp01eWl6SzyNOYh5PKa8sGiQ1ddXprOIk9…
  5: "kJuWoDl5eXR0dH+eX+L+Z8pzs+sZO1elJpVVQv/xIHafnoOLa615iTkMsbuzc9W9nxib5…
  6: "SAUqIDlBIdoJToAKVEByglOkAp0QFKiQ5QSnSAUqIDlBIdoJToAKVEByglOkAp0QFKiQ5…
  length: 7
▶ __proto__: Array(0)
```

4. show data

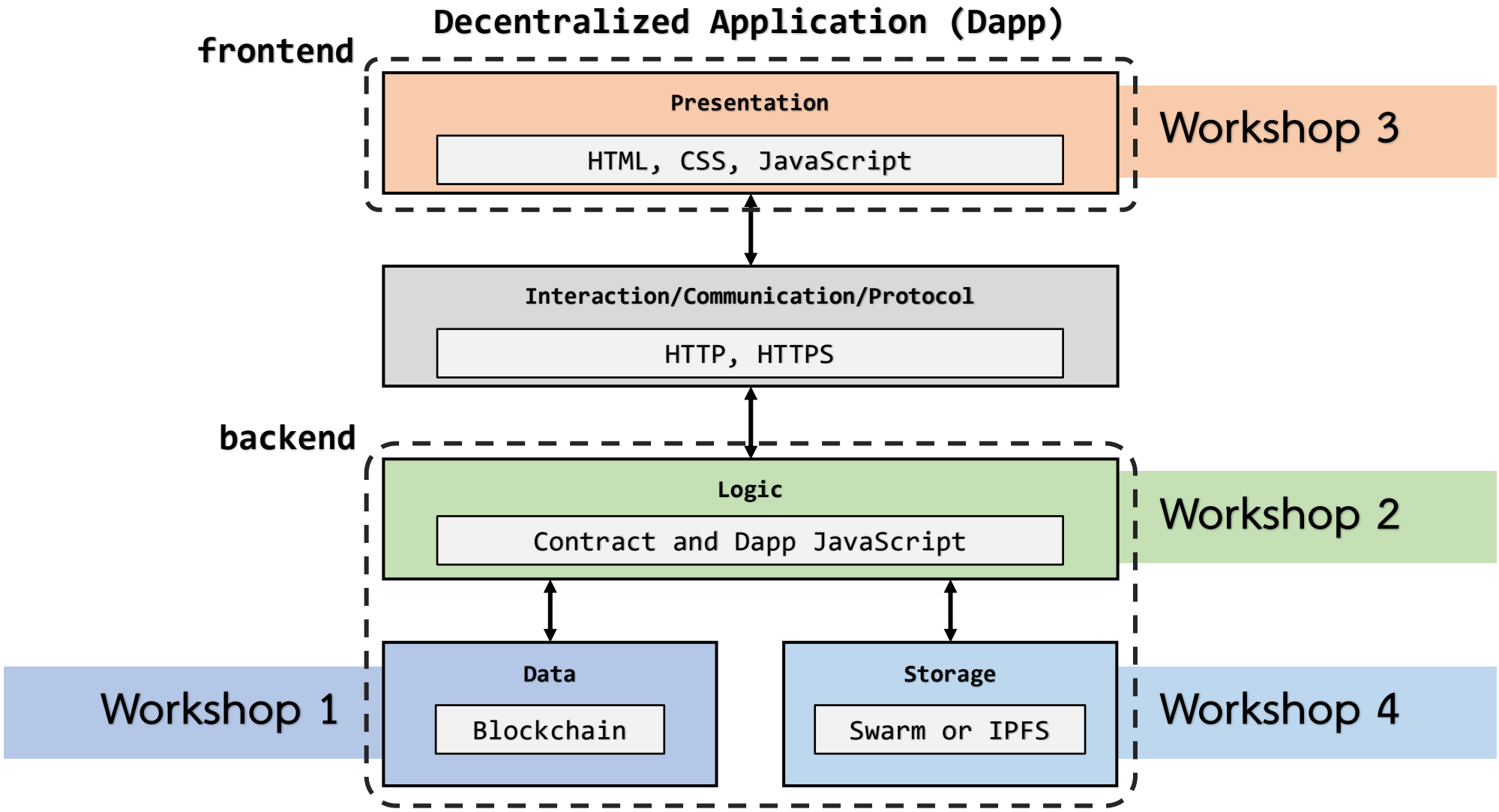
```
async function show(){
        let dataURLFromBlockchain = await byteContract.methods.dataURL().call()
        let hexURL = dataURLFromBlockchain.slice(2,dataURLFromBlockchain.length)// remove 0x
        let url = ""
        for (let i = 0; i < hexURL.length; i += 2) {
            url += String.fromCharCode(parseInt(hexURL.substr(i, 2), 16));
        }
        console.log('url =',url)
        document.getElementById('url').innerHTML = url
        document.getElementById('url').href = url
        document.getElementById('content').src= url
    }
```

4. show data


Document
localhost:8080/eth.html
ETH - Add data to Ethereum from the browser
Choose File
a.png
add to ETH
index
show

P IC

Overview



https://file.scirp.org/pdf/JSEA_20161028140127798.pdf

Blockchain Voting

1. เกิดอคติต่อกัน
2. เกิดการซื้อสิทธิ์ขายเสียงมากขึ้น

เพราะคนซื้อตรวจสอบได้ว่าโหวตตามที่สัญญาไว้หรือเปล่า

และคนขายก็ไม่กล้าเบี้ยว เพราะตรวจสอบได้

Use Cases

https://media.consensys.net/40-ethereum-apps-you-can-use-right-now-d643333769f7

THANK YOU! :3