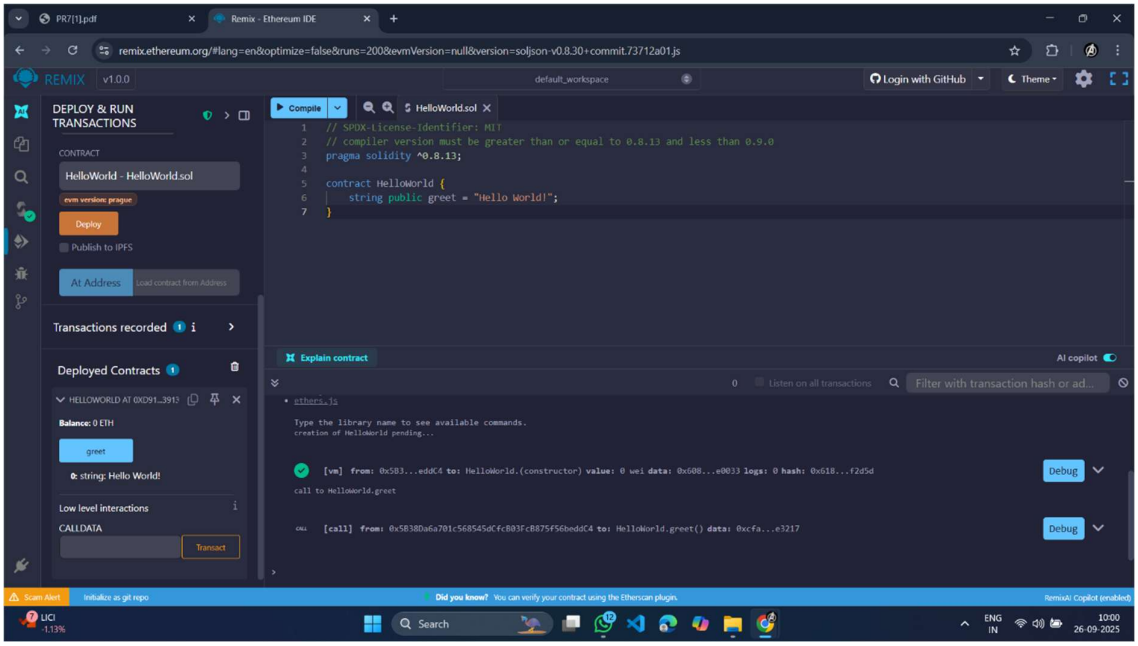
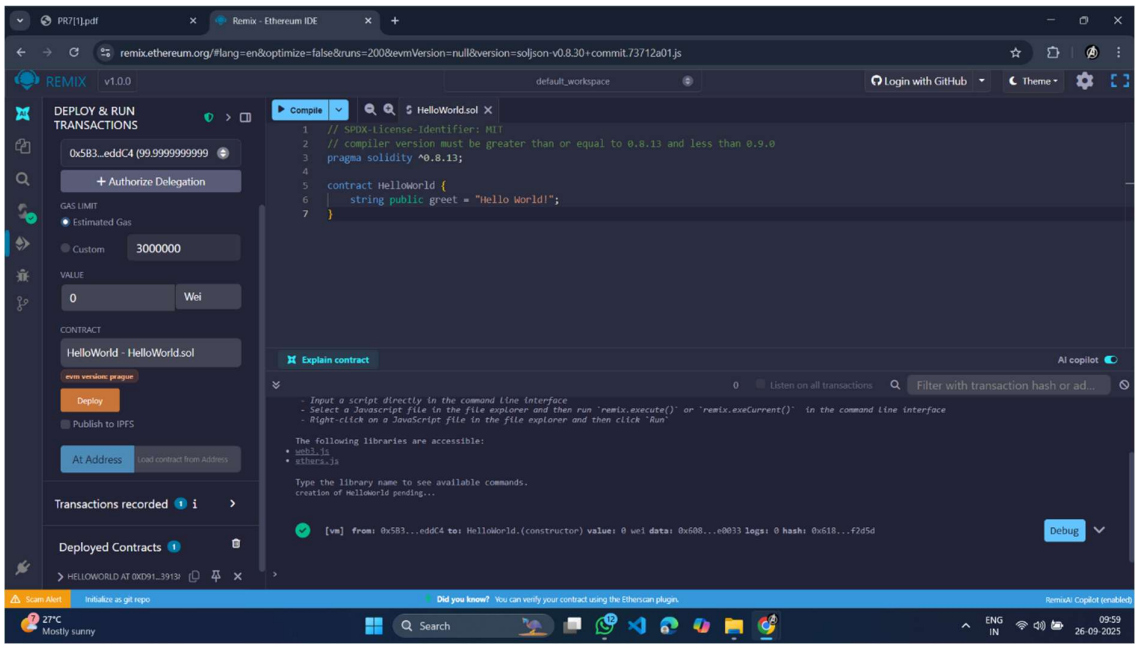
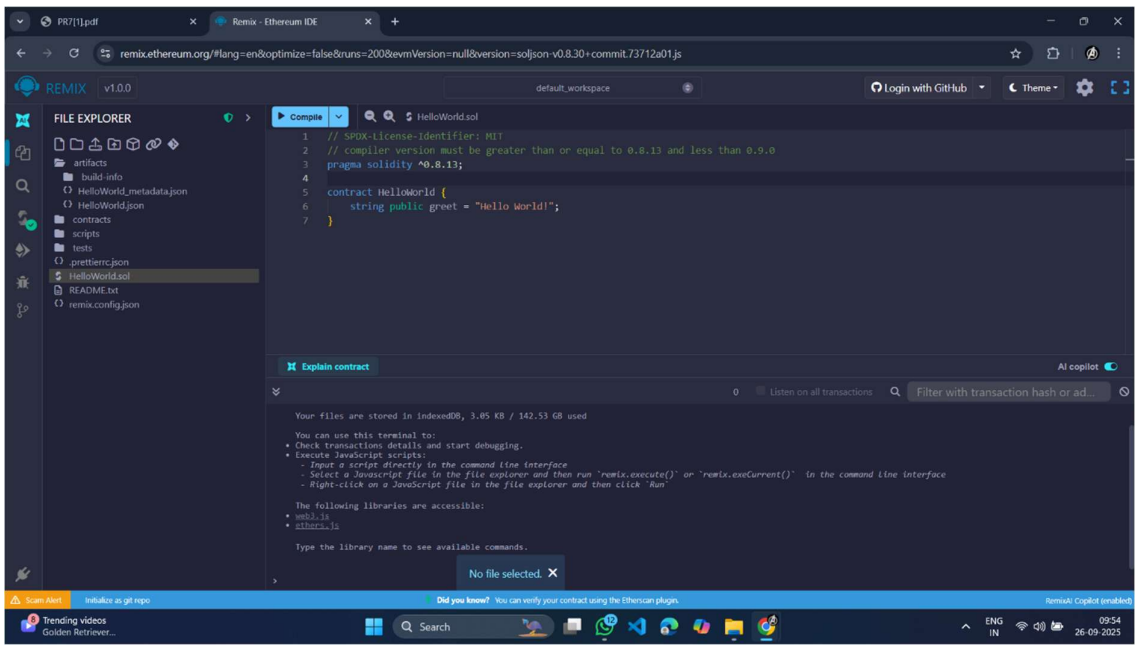
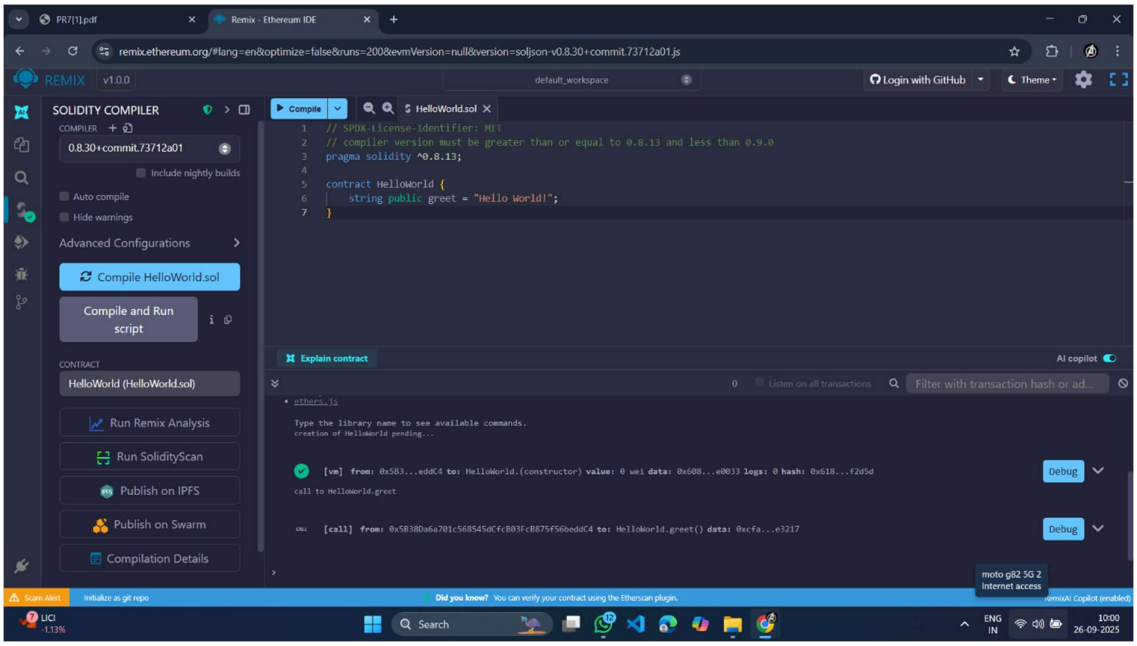

PR7[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
DEPLOY & RUN TRANSACTIONS
CONTRACT
HelloWorld - HelloWorld.sol
evm version: prague
Deploy
Publish to IPFS
At Address
Load contract from Address
Transactions recorded
Deployed Contracts
HELLOWORLD AT 0XD91...3913
Balance: 0 ETH
greet
0: string: Hello World!
Low level interactions
CALLDATA
Transact
Compile
HelloWorld.sol
// SPDX-License-Identifier: MIT
// compiler version must be greater than or equal to 0.8.13 and less than 0.9.0
pragma solidity ^0.8.13;
contract HelloWorld {
string public greet = "Hello World!";
}
Explain contract
AI copilot
Listen on all transactions
Filter with transaction hash or ad...
ethers.js
Type the library name to see available commands.
creation of HelloWorld pending...
[vm] from: 0x5B3...eddC4 to: HelloWorld.(constructor) value: 0 wei data: 0x608...e0033 logs: 0 hash: 0x618...f2d5d
Debug
call to HelloWorld.greet
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: HelloWorld.greet() data: 0xcfa...e3217
Debug
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Etherscan plugin.
RemixAI Copilot (enabled)
LICI -1.13%
Search
ENG IN
10:00 26-09-2025


PR7[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
DEPLOY & RUN TRANSACTIONS
0x5B3...eddC4 (99.9999999999
+ Authorize Delegation
GAS LIMIT
Estimated Gas
Custom
3000000
VALUE
0
Wei
CONTRACT
HelloWorld - HelloWorld.sol
evm version: prague
Deploy
Publish to IPFS
At Address
Load contract from Address
Transactions recorded
Deployed Contracts
HELLOWORLD AT 0XD91...3913
Compile
HelloWorld.sol
// SPDX-License-Identifier: MIT
// compiler version must be greater than or equal to 0.8.13 and less than 0.9.0
pragma solidity ^0.8.13;
contract HelloWorld {
string public greet = "Hello World!";
}
Explain contract
AI copilot
Listen on all transactions
Filter with transaction hash or ad...
- Input a script directly in the command line interface
- Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()` in the command line interface
- Right-click on a JavaScript file in the file explorer and then click `Run`
The following libraries are accessible:
web3.js
ethers.js
Type the library name to see available commands.
creation of HelloWorld pending...
[vm] from: 0x5B3...eddC4 to: HelloWorld.(constructor) value: 0 wei data: 0x608...e0033 logs: 0 hash: 0x618...f2d5d
Debug
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Etherscan plugin.
RemixAI Copilot (enabled)
27°C Mostly sunny
Search
ENG IN
09:59 26-09-2025


PR7[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
FILE EXPLORER
artifacts
build-info
HelloWorld_metadata.json
HelloWorld.json
contracts
scripts
tests
.prettierrc.json
HelloWorld.sol
README.txt
remix.config.json
Compile
HelloWorld.sol
// SPDX-License-Identifier: MIT
// compiler version must be greater than or equal to 0.8.13 and less than 0.9.0
pragma solidity ^0.8.13;
contract HelloWorld {
string public greet = "Hello World!";
}
Explain contract
AI copilot
Listen on all transactions
Filter with transaction hash or ad...
Your files are stored in indexedDB, 3.05 KB / 142.53 GB used
You can use this terminal to:
• Check transactions details and start debugging.
• Execute JavaScript scripts:
- Input a script directly in the command line interface
- Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()` in the command line interface
- Right-click on a JavaScript file in the file explorer and then click `Run`
The following libraries are accessible:
web3.js
ethers.js
Type the library name to see available commands.
No file selected.
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Etherscan plugin.
RemixAI Copilot (enabled)
Trending videos Golden Retriever...
Search
ENG IN
09:54 26-09-2025




```
RSA ENCRYPTOR/DECRYPTOR
**************************************************
PLEASE ENTER THE 'p' AND 'q' VALUES BELOW:
Enter a prime number for p: 3
Enter a prime number for q: 5
**************************************************
RSA Modulus(n) is: 15
Eulers Toitent(r) is: 8
**************************************************
The value of e is: 999
**************************************************
EUCLID'S ALGORITHM:
8 = 0*(999) + 8
999 = 124*(8) + 7
8 = 1*(7) + 1
END OF THE STEPS USED TO ACHIEVE EUCLID'S ALGORITHM.
**************************************************
EUCLID'S EXTENDED ALGORITHM:
1 = 8*(1) + (-1)*(7)
1 = 999*(-1) + (125)*(8)
s=-1. Since -1 is less than 0, s = s(modr), i.e., s=7.
END OF THE STEPS USED TO ACHIEVE THE VALUE OF 'd'.
The value of d is: 7
**************************************************
Private Key is: (7, 15)
Public Key is: (999, 15)
**************************************************
What would you like encrypted or decrypted?(Separate numbers with ',' for decryption):HELLO
Your message is: HELLO
Type '1' for encryption and '2' for decryption.1
Your encrypted message is: [13, 4, 11, 11, 14]
Thank you for using the RSA Encryptor. Goodbye!
```

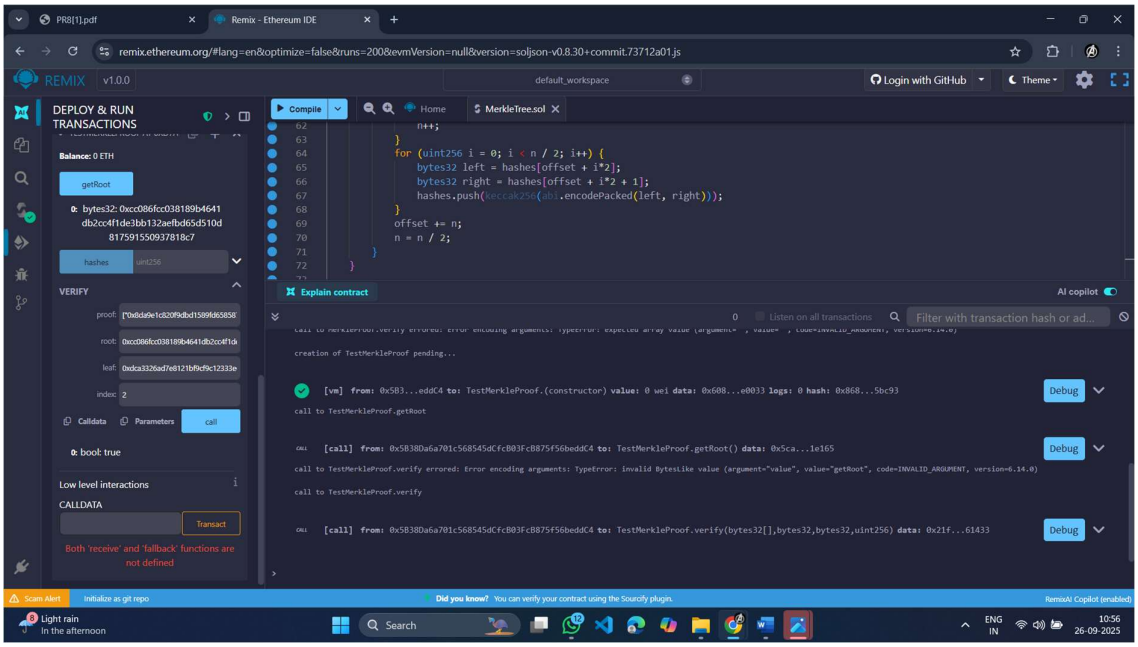
```
***Mining fccCoin about to start***
[0 - 0 - 0 - [] - 1758459286.5632427]
***Mining fccCoin has been successful***
[0 - 0 - 0 - [] - 1758459286.5632427, 1 - 88914 - f1a5e382305ba71af55814621533271ad8a564e585536cc50b46c300f3911c42 - [{'sender': 'Anuj Gite', 'recipient': 'CSE Department', 'quantity': 1}] - 1758459286.6857083]
```

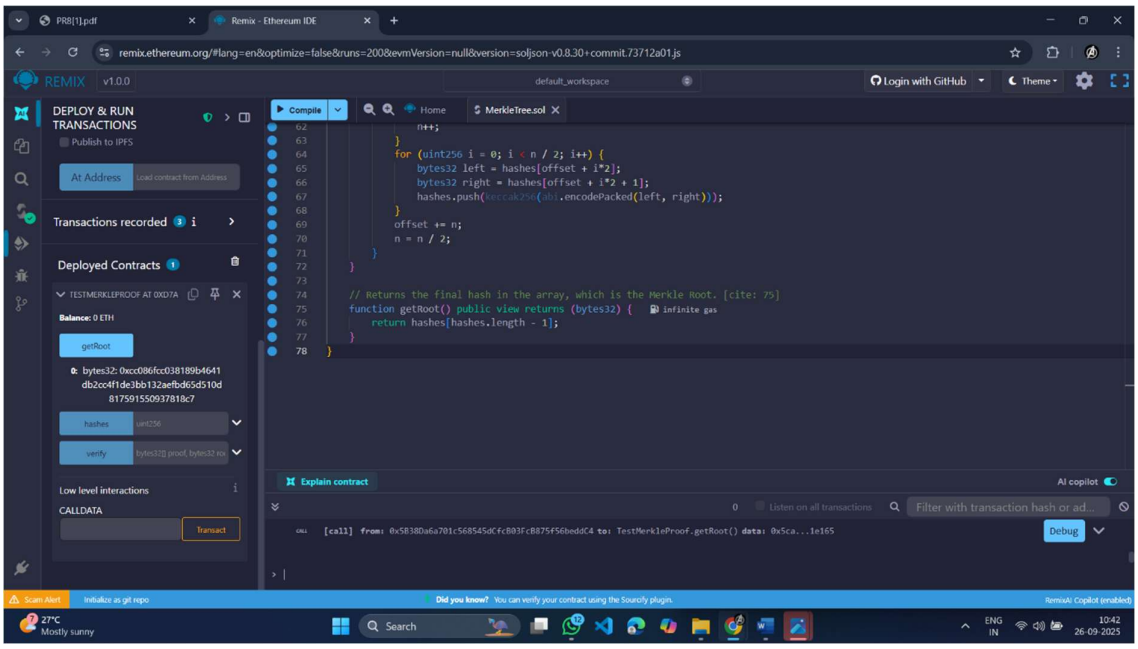
```
Validators in the network:
 - Alice (Stake: 50)
 - Bob (Stake: 30)
 - Charlie (Stake: 15)
 - Diana (Stake: 5)

--- Block Validation Rounds ---
Round 10: Block validated by Charlie
```

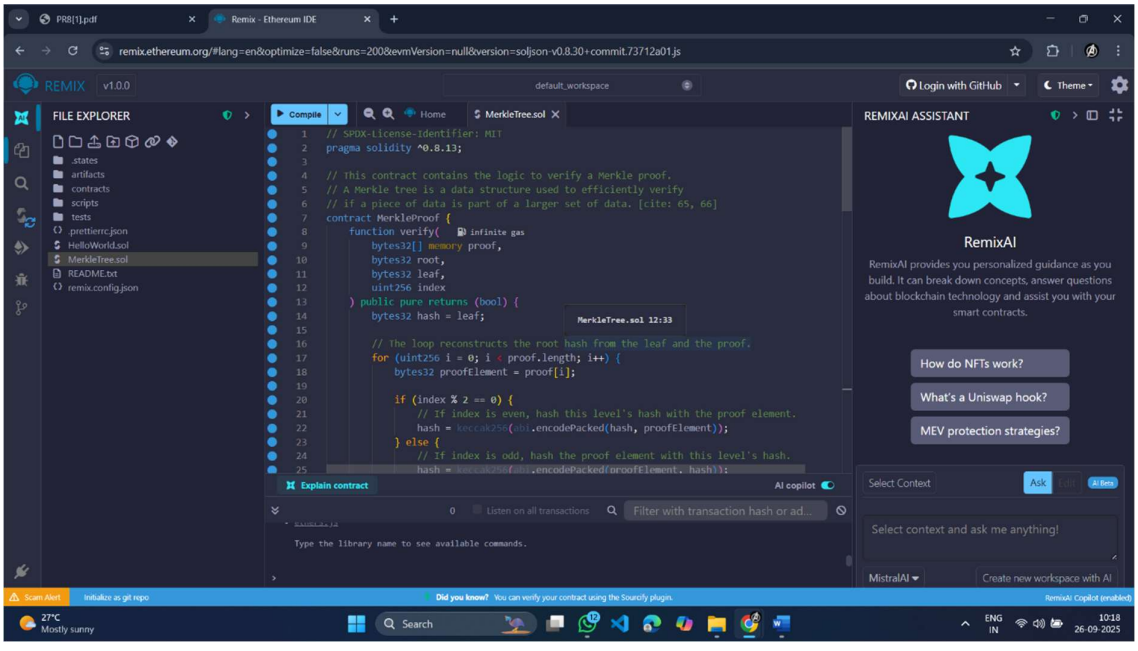
```
0


 ----> Mining New Block -->


 ----> New Block mined successfully -->

-----Block 0 ---------
 timestamp = Wed Sep 24 05:43:02 2025
 data = genesisBlock
 previousHash = 00000
 hash = e0a1c9c7cfedbc9c8ffe9b5ff870a3be0ebd54faa726f382d23ede93e8585058

-----Block 1 ---------
 timestamp = Wed Sep 24 05:43:08 2025
 data = 0
 previousHash = e0a1c9c7cfedbc9c8ffe9b5ff870a3be0ebd54faa726f382d23ede93e8585058
 hash = b700a32623f33d70e0fd6644f7f1a5e69cb0965b9a963ae816f5830d32b9bc37
```

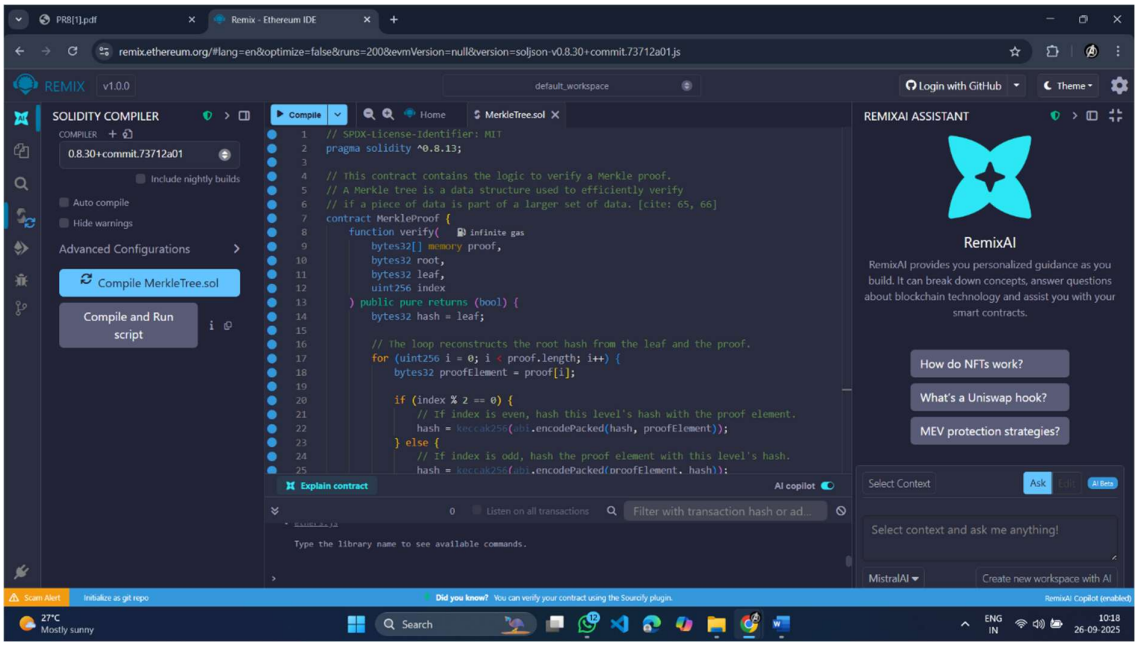
```
The hexadecimal equivalent of SHA256 is :
634f59cdba42b5cccca655b810218fe26e8cfdb72b779f237b4decb53915e0d0

The hexadecimal equivalent of SHA384 is :
f89937f9ceda541dbafedd197f3a68a8671bffb26a763c7dae462860e7409fbd690b86da144c64d6c69c389c6323a81f

The hexadecimal equivalent of SHA224 is :
9bb2114762931d2ab557444a3c0b53e86663eac827fff9cbd68870f7

The hexadecimal equivalent of SHA512 is :
5e1a20d8fe80c7bb10ec1852581d73a3bbab31ed4109372b3194be4dd8a1b921366d4c46b516a8cf88d5c07db9777fc52ff55286610c7e9ae520c424047592ae

The hexadecimal equivalent of SHA1 is :
64525125ed05dd32b7b78a4856d1745e497c40ad
```

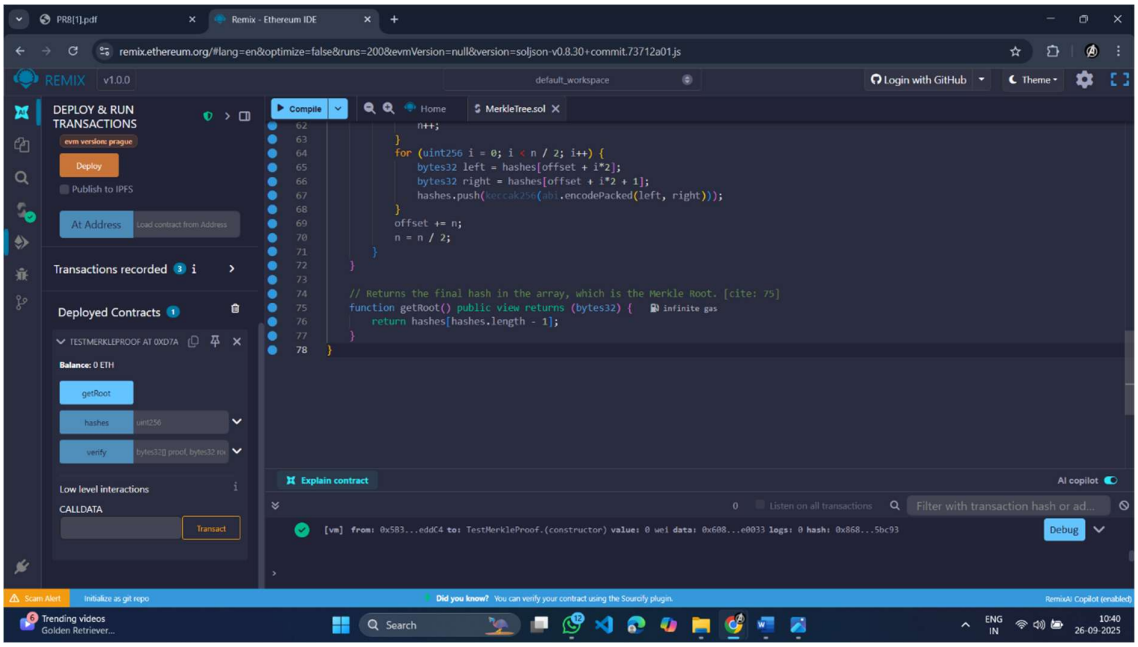
```
The Value of P is :23
The Value of G is :9
The Private Key a for Alice is :4
The Private Key b for Bob is :3
Secret key for the Alice is : 9
Secret Key for the Bob is : 9
```


PR8[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
DEPLOY & RUN TRANSACTIONS
Balance: 0 ETH
getRoot
0: bytes32: 0xcc086fcc038189b4641db2cc4f1de3bb132aefbd65d510d817591550937818c7
hashes uint256
VERIFY
proof: ["0x8da9e1c820f9dbd1589fd6585
root: 0xcc086fcc038189b4641db2cc4f1di
leaf: 0xdca3326ad7e8121bf9cf9c12333e
index: 2
Calldata Parameters call
0: bool: true
Low level interactions
CALLDATA
Transact
Both 'receive' and 'fallback' functions are not defined
Compile
Home
MerkleTree.sol
Explain contract
AI copilot
Listen on all transactions
Filter with transaction hash or ad...
creation of TestMerkleProof pending...
[vm] from: 0x583...eddC4 to: TestMerkleProof.(constructor) value: 0 wei data: 0x608...e0033 logs: 0 hash: 0x868...5bc93
Debug
call to TestMerkleProof.getRoot
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: TestMerkleProof.getRoot() data: 0x5ca...1e165
call to TestMerkleProof.verify errored: Error encoding arguments: TypeError: invalid Bytes-like value (argument="value", value="getRoot", code=INVALID_ARGUMENT, version=6.14.0)
call to TestMerkleProof.verify
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: TestMerkleProof.verify(bytes32[],bytes32,bytes32,uint256) data: 0x21f...61433
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Sourcify plugin.
RemixAI Copilot (enabled)
Light rain In the afternoon
Search
ENG IN
10:56
26-09-2025


PR8[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
DEPLOY & RUN TRANSACTIONS
Publish to IPFS
At Address Load contract from Address
Transactions recorded 3
Deployed Contracts 1
TESTMERKLEPROOF AT 0XD7A
Balance: 0 ETH
getRoot
0: bytes32: 0xcc086fcc038189b4641db2cc4f1de3bb132aefbd65d510d817591550937818c7
hashes uint256
verify bytes32[] proof, bytes32 roo
Low level interactions
CALLDATA
Transact
Compile
Home
MerkleTree.sol
// Returns the final hash in the array, which is the Merkle Root. [cite: 75]
function getRoot() public view returns (bytes32) {
infinite gas
return hashes[hashes.length - 1];
Explain contract
AI copilot
Listen on all transactions
Filter with transaction hash or ad...
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: TestMerkleProof.getRoot() data: 0x5ca...1e165
Debug
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Sourcify plugin.
RemixAI Copilot (enabled)
27°C Mostly sunny
Search
ENG IN
10:42
26-09-2025


PR8[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
FILE EXPLORER
.states
artifacts
contracts
scripts
tests
.prettierrc.json
HelloWorld.sol
MerkleTree.sol
README.txt
remix.config.json
Compile
Home
MerkleTree.sol
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.13;
// This contract contains the logic to verify a Merkle proof.
// A Merkle tree is a data structure used to efficiently verify
// if a piece of data is part of a larger set of data. [cite: 65, 66]
contract MerkleProof {
function verify(
infinite gas
bytes32[] memory proof,
bytes32 root,
bytes32 leaf,
uint256 index
) public pure returns (bool) {
bytes32 hash = leaf;
MerkleTree.sol 12:33
// The loop reconstructs the root hash from the leaf and the proof.
for (uint256 i = 0; i < proof.length; i++) {
bytes32 proofElement = proof[i];
if (index % 2 == 0) {
// If index is even, hash this level's hash with the proof element.
hash = keccak256(abi.encodePacked(hash, proofElement));
} else {
// If index is odd, hash the proof element with this level's hash.
hash = keccak256(abi.encodePacked(proofElement, hash));
Explain contract
AI copilot
Listen on all transactions
Filter with transaction hash or ad...
Type the library name to see available commands.
REMIXAI ASSISTANT
RemixAI
RemixAI provides you personalized guidance as you build. It can break down concepts, answer questions about blockchain technology and assist you with your smart contracts.
How do NFTs work?
What's a Uniswap hook?
MEV protection strategies?
Select Context
Ask
Edit
AI Beta
Select context and ask me anything!
MistralAI
Create new workspace with AI
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Sourcify plugin.
RemixAI Copilot (enabled)
27°C Mostly sunny
Search
ENG IN
10:18
26-09-2025


PR8[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
SOLIDITY COMPILER
COMPILER
0.8.30+commit.73712a01
Include nightly builds
Auto compile
Hide warnings
Advanced Configurations
Compile MerkleTree.sol
Compile and Run script
Compile
Home
MerkleTree.sol
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.13;
// This contract contains the logic to verify a Merkle proof.
// A Merkle tree is a data structure used to efficiently verify
// if a piece of data is part of a larger set of data. [cite: 65, 66]
contract MerkleProof {
function verify(infinite gas
bytes32[] memory proof,
bytes32 root,
bytes32 leaf,
uint256 index
) public pure returns (bool) {
bytes32 hash = leaf;
// The loop reconstructs the root hash from the leaf and the proof.
for (uint256 i = 0; i < proof.length; i++) {
bytes32 proofElement = proof[i];
if (index % 2 == 0) {
// If index is even, hash this level's hash with the proof element.
hash = keccak256(abi.encodePacked(hash, proofElement));
} else {
// If index is odd, hash the proof element with this level's hash.
hash = keccak256(abi.encodePacked(proofElement, hash));
Explain contract
AI copilot
0
Listen on all transactions
Filter with transaction hash or ad...
Type the library name to see available commands.
REMIXAI ASSISTANT
RemixAI
RemixAI provides you personalized guidance as you build. It can break down concepts, answer questions about blockchain technology and assist you with your smart contracts.
How do NFTs work?
What's a Uniswap hook?
MEV protection strategies?
Select Context
Ask
Edit
AI Beta
Select context and ask me anything!
MistralAI
Create new workspace with AI
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Sourcify plugin.
RemixAI Copilot (enabled)
27°C
Mostly sunny
Search
ENG
IN
10:18
26-09-2025


PR8[1].pdf
Remix - Ethereum IDE
remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.30+commit.73712a01.js
REMIX v1.0.0
default_workspace
Login with GitHub
Theme
DEPLOY & RUN TRANSACTIONS
evm version: prague
Deploy
Publish to IPFS
At Address
Load contract from Address
Transactions recorded 3
Deployed Contracts 1
TESTMERKLEPROOF AT 0XD7A
Balance: 0 ETH
getRoot
hashes uint256
verify bytes32[] proof, bytes32 lea
Low level interactions
CALLDATA
Transact
Compile
Home
MerkleTree.sol
n++;
}
for (uint256 i = 0; i < n / 2; i++) {
bytes32 left = hashes[offset + i*2];
bytes32 right = hashes[offset + i*2 + 1];
hashes.push(keccak256(abi.encodePacked(left, right)));
}
offset += n;
n = n / 2;
}
}
// Returns the final hash in the array, which is the Merkle Root. [cite: 75]
function getRoot() public view returns (bytes32) { infinite gas
return hashes[hashes.length - 1];
}
}
Explain contract
AI copilot
0
Listen on all transactions
Filter with transaction hash or ad...
[vm] from: 0x583...eddC4 to: TestMerkleProof.(constructor) value: 0 wei data: 0x608...e0033 logs: 0 hash: 0x868...5bc93
Debug
Scam Alert
Initialize as git repo
Did you know? You can verify your contract using the Sourcify plugin.
RemixAI Copilot (enabled)
Trending videos
Golden Retriever...
Search
ENG
IN
10:40
26-09-2025