

FIT5214: Blockchain

Assignment Project Exam Help

Lecture 3: Ethereum and Smart Contract

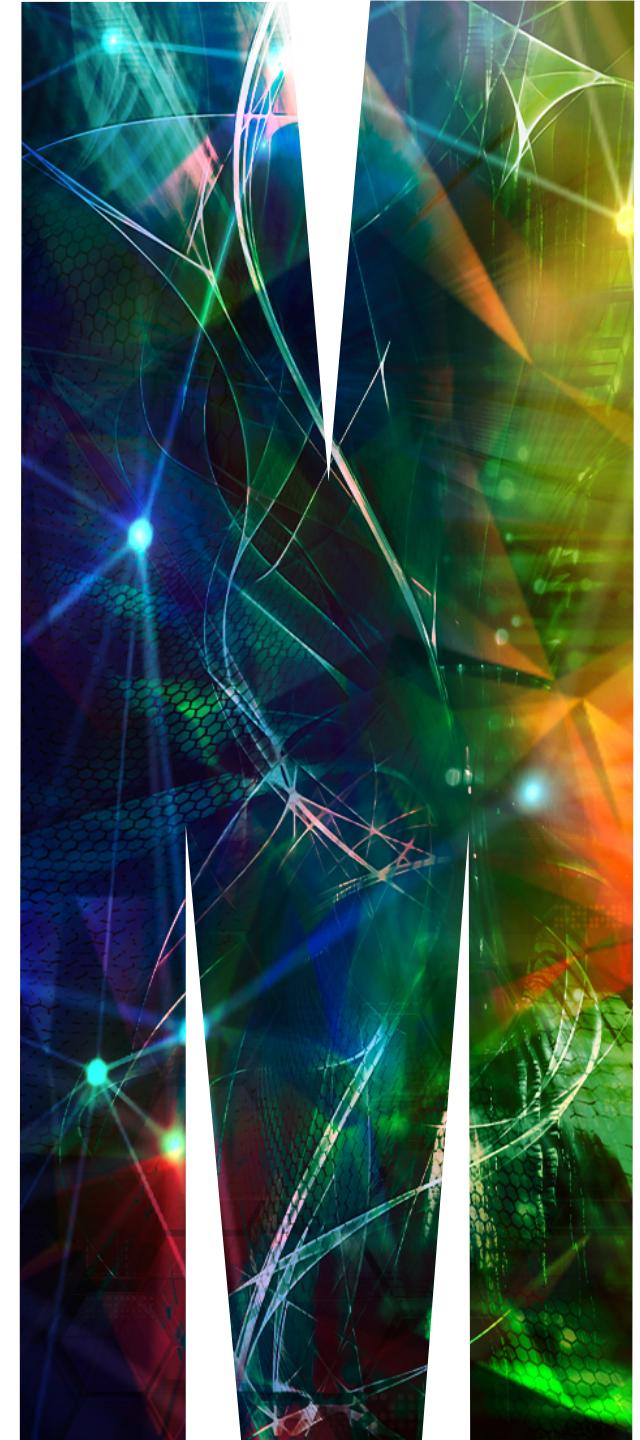
<https://powcoder.com>

Add WeChat powcoder

Lecturer: Rafael Dowsley

rafael.dowsley@monash.edu

<https://dowsley.net>



Unit Structure

- **Lecture 1: Introduction to Blockchain**
- **Lecture 2: Bitcoin**
- Lecture 3: Ethereum and Smart contracts
- Lecture 4: Proof-of-Work (PoW) **Assignment Project Exam Help**
- Lecture 5: Attacks on Blockchains **<https://powcoder.com>**
- Lecture 6: Class Test/Alternatives to PoW
- Lecture 7: Proof-of-Stake (PoS) **Add WeChat powcoder**
- Lecture 8: Privacy
- Lecture 9: Byzantine Agreement
- Lecture 10: Blockchain Network
- Lecture 11: Payment Channels
- Lecture 12: Guest Lecture

Unit Structure

- **Lecture 1: Introduction to Blockchain**
 - **Lecture 2: Bitcoin**
 - **Lecture 3: Ethereum and Smart contracts**
 - Lecture 4: Proof-of-Work (PoW)
 - Lecture 5: Attacks on Blockchains
 - Lecture 6: Class Test/Alternatives to PoW
 - Lecture 7: Proof-of-Stake (PoS)
 - Lecture 8: Privacy
 - Lecture 9: Byzantine Agreement
 - Lecture 10: Blockchain Network
 - Lecture 11: Payment Channels
 - Lecture 12: Guest Lecture
- Introduction to Ethereum and smart contract
→ Understand “DAO” and “DAO” attacks
→ Other key vulnerabilities
- Assignment Project Exam Help**
<https://powcoder.com>
Add WeChat powcoder

Digital currency and smart contract - A brief history

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Digital currency and smart contract - A brief history

The concept of e-Cash

- **1982** David Chaum

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Digital currency and smart contract - A brief history

The concept of e-Cash

- **1982** David Chaum
- **1990** DigiCash
(Founded by Chaum)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Digital currency and smart contract - A brief history

The concept of e-Cash

- **1982** David Chaum
- **1990** DigiCash
(Founded by Chaum)
 - **1994** First payment sent

The concept of PoW
preventing email spam

**The concept of
smart contract**

- **1997** Hashcash (pt. of Hash)
- **1997** Nick Szabo
<https://powcoder.com>
- **1998** b-money (Wei Dai)

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

Digital currency and smart contract - A brief history

The concept of e-Cash

- **1982** David Chaum
- **1990** DigiCash
(Founded by Chaum)
 - **1994** First payment sent

The concept of PoW
preventing email spam

**The concept of
smart contract**

Assignment Project Exam Help

1997 Nick Szabo
<https://powcoder.com>

- **1998** b-money (Wei Dai)
- **1998** Bit gold (never implemented)
by Nick Szabo

Add WeChat powcoder

Digital currency and smart contract - A brief history

The concept of e-Cash

- **1982** David Chaum
- **1990** DigiCash
(Founded by Chaum)
 - **1994** First payment sent

The concept of PoW
preventing email spam

**The concept of
smart contract**

- **1997** Hashcash (Proof of Cash)
- **1997** Nick Szabo
 - <https://powcoder.com>
- **1998** b-money (Wei Dai)
- **1998** Bit gold (never implemented)
by Nick Szabo
- **1998** PayPal

Digital currency and smart contract - A brief history

The concept of e-Cash

- **1982** David Chaum
- **1990** DigiCash
(Founded by Chaum)
 - **1994** First payment sent

The concept of PoW
preventing email spam

**The concept of
smart contract**

Assignment Project Exam Help

- **1997** Nick Szabo
 - <https://powcoder.com>
- **1998** b-money (Wei Dai)
- **1998** Bit gold (never implemented)
by Nick Szabo
- **1998** PayPal
- **2008** Bitcoin (**Satoshi Nakamoto**)

Add WeChat powcoder

Digital currency and smart contract - A brief history

The concept of e-Cash

- **1982** David Chaum
- **1990** DigiCash
(Founded by Chaum)
 - **1994** First payment sent
- **1997** Hashcash (proto-cash)
- **1997** Nick Szabo
 - https://powcoder.com**
- **1998** b-money (Wei Dai)
- **1998** Bit gold (never implemented) by Nick Szabo
- **1998** PayPal
- **2008** Bitcoin (**Satoshi Nakamoto**)
- **2009** Bitcoin software released
- **2014** Ethereum (**Vitalik Buterin**)

The concept of PoW preventing email spam

The concept of smart contract

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Smart Contract

The concept of smart contract was first proposed by Nick Szabo in 1997.

Szabo defines **smart contracts** as agreements that are derived from legal principles, but enforced by cryptographic protocols.

<https://powcoder.com>

Add WeChat powcoder

Smart Contract

The concept of smart contract was first proposed by Nick Szabo in 1997.

Szabo defines **smart contracts** as agreements that are derived from legal principles, but enforced by cryptographic protocols.

<https://powcoder.com>

Add WeChat powcoder

A **smart contract** is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

– Wikipedia

Smart Contract

So, a contract is “*smart*” if **Assignment Project Exam Help**

- it is run by a machine rather than a person;
- the assets in the contract are moved automatically.

Add WeChat powcoder

Smart Contract

User-defined programs running on top of a blockchain

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Smart Contract

User-defined programs running on top of a blockchain

Cryptocurrency



Assignment Project Exam Help

Transfer 5 coins from Address X to Address Y
<https://powcoder.com>

Add WeChat powcoder → ← ← ← ← ... ←

Distributed ledger, or “Blockchain”

Smart Contract

User-defined programs running on top of a blockchain

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Smart Contract

User-defined programs running on top of a blockchain

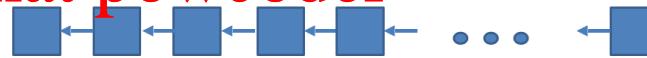
Smart Contract



Assignment Project Exam Help

If the 200th block contains more transactions than the 201th block,
then transfer 5 coins from Address X to Address Y

Add WeChat powcoder



Distributed ledger, or “Blockchain”

Group Discussion:

Does Bitcoin support smart contracts?
Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Answer:

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Answer:

Assignment Project Exam Help

Bitcoin supports smart contracts via a Turing-incomplete Script language, examples include *multi-signature accounts, payment channels, atomic cross-chain trading.*

<https://powcoder.com>

Add WeChat powcoder

Smart Contract Languages

Smart contracts on a blockchain can be written in different programming languages, such as

- Solidity (Ethereum)
- Golang/Java/JavaScript (Hyperledger Fabric)
- C++ (EOS)
- ...

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Decentralized Application (DApp)

- ❖ A DApp is a computer application that runs on a distributed system
- ❖ With Blockchain, a smart contract is a DApp – it runs on the distributed ledger.

<https://powcoder.com>

Add WeChat powcoder

Ethereum

Ethereum is an open source programmable blockchain platform.

- ❖ Nov. 2013. Ethereum was proposed by Vitalik Buterin.
- ❖ July - August 2014. Ethereum crowdsourcing campaign >\$18 million through initial coin offering (by selling Ether – the Ethereum coins/tokens).
- ❖ 30th July 2015. The first release.
- ❖ Mar. 2016. Official release.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Potential applications

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Potential applications

- ❖ Crowdfunding/initial coin offering (ICO)
- ❖ Gambling
- ❖ Supply-chain management
- ❖ Power trading and management
- ❖ Internet of Things
- ❖ Asset Issuance
- ❖ Marketplaces
- ❖ ...

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Ethereum Blockchain

Different from Bitcoin:

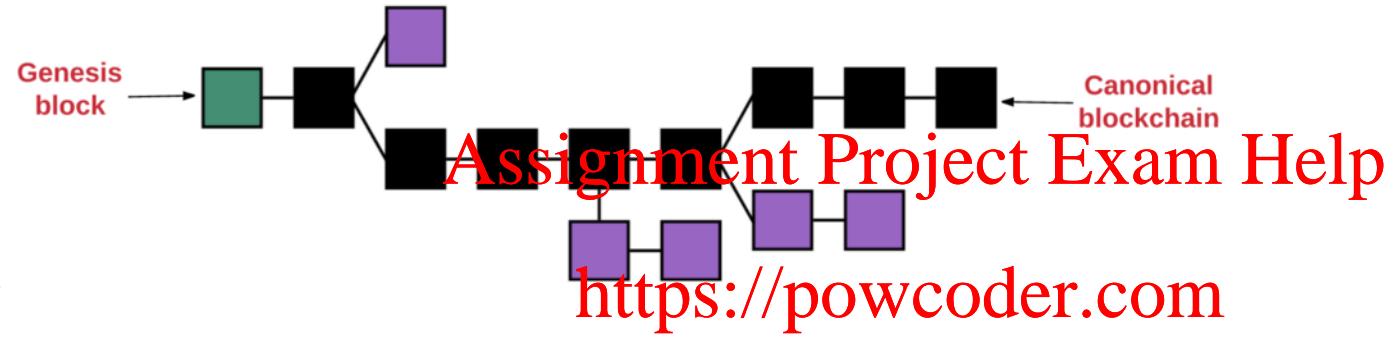
- ❖ Block generation: on average one block every 12 seconds through PoW
- ❖ Mining algorithm: Ethash
 - ❖ Memory bound
 - ❖ Helps mitigate ASIC and GPU advantages
- ❖ Difficulty is adjusted every block
- ❖ Hash algorithm:
 - ❖ SHA3_256 (a.k.a. Keccak-256) and
 - ❖ SHA3_512 (a.k.a. Keccak-512)

Assignment Project Exam Help

<https://powcoder.com>

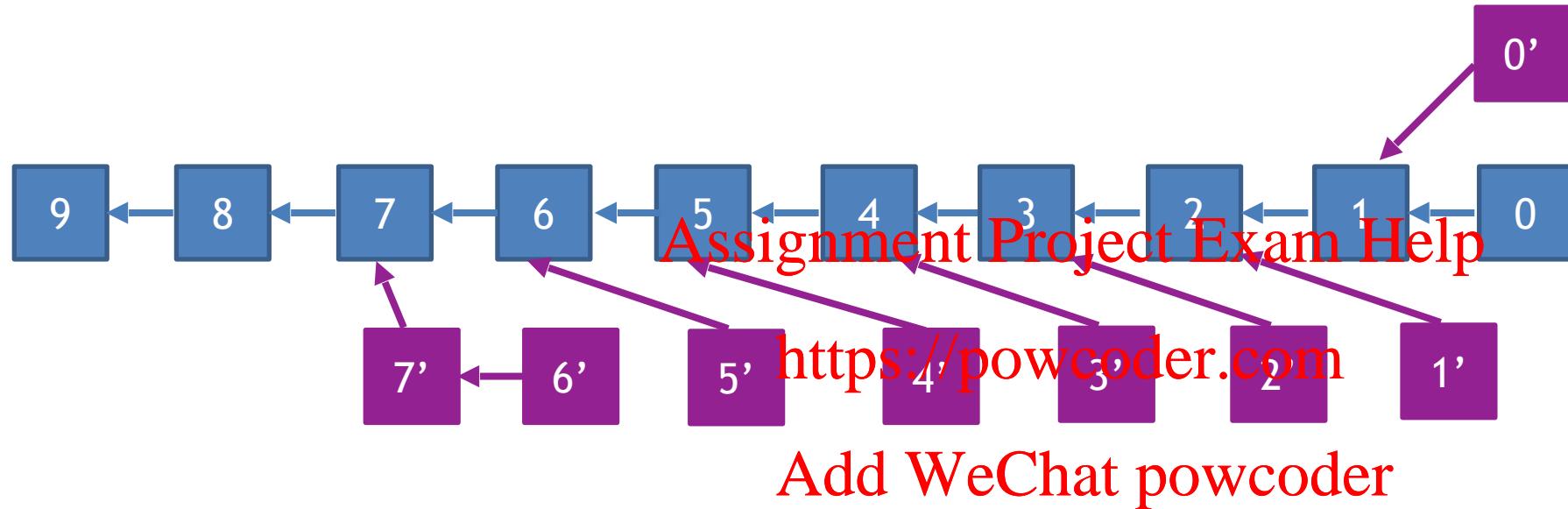
Add WeChat powcoder

Simplified GHOST (Greedy Heaviest Observed Subtree)



Add WeChat powcoder
Choose the path that has the most computation done

Uncle blocks



Uncles are orphan blocks, i.e., with parents that are ancestors (max 6 blocks back) of a block in the canonical blockchain.

Ethereum mining reward

A successful PoW miner receives:

- ❖ A static block reward of X Ether
 - ❖ Before Block 4369999 (16-Oct-2017)
X=5
 - ❖ Block 4,370,000 – Block 7,279,999 (16-Oct-2017 – 28-Feb-2019)
X=3
 - ❖ Since Block 7,280,000 (28-Feb-2019 – present)
X=2
- ❖ Transaction fees (all the gas consumed, explained later)
- ❖ An extra of 1/32 of 2 Ether for including Uncles as part of the block. (Can include up to two Uncles)
 - ❖ Uncles receive 7/8 of the static block reward, an uncle can only be included by one valid block.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

EVM and Solidity

EVM

Solidity

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

EVM and Solidity

EVM	Solidity
❖ EVM is a virtual machine for Ethereum, it can run smart contracts.	❖ Solidity is a language for writing smart contracts supported by EVM.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

EVM and Solidity

EVM	Solidity
❖ EVM is a virtual machine for Ethereum, it can run smart contracts.	❖ Solidity is a language for writing smart contracts supported by EVM.
❖ EVM “understands” EVM bytecode	❖ Solidity (High-level language) is deterministically compiled into EVM bytecode. https://powcoder.com

Assignment Project Exam Help

Add WeChat powcoder

EVM and Solidity

EVM	Solidity
<ul style="list-style-type: none">❖ EVM is a virtual machine for Ethereum, it can run smart contracts.	<ul style="list-style-type: none">❖ Solidity is a language for writing smart contracts supported by EVM.
<p style="text-align: center;">Assignment Project Exam Help</p> <p style="text-align: center;">https://powcoder.com</p>	
<ul style="list-style-type: none">❖ All Ethereum nodes need to have EVM to run all smart contracts to verify the transactions, like in BTC. Thus, they all share the same EVM states.	<ul style="list-style-type: none">❖ Solidity (High-level language) is deterministically compiled into EVM bytecode.❖ Solidity programs are capable of expressing all tasks accomplishable by computers, making them theoretically Turing complete. <p>(C, C++, C#, Java, Python.. are all Turing complete.)</p>

Smart contract in Ethereum

- ❖ Smart contract is written in Solidity;
- ❖ Solidity is deterministically compiled into EVM bytecode
- ❖ Each smart contract (bytecode) is contained in a transaction, just like BTC, and will be recorded in the blockchain;
<https://powcoder.com>
- ❖ When one user uploads a smart contract through their Ethereum node, it is included in one block and propagated around the network, where it is stored on every other node in the network.
- ❖ Since smart contract needs to be run and verified on every full node, it needs to be guaranteed to execute, and the result is deterministic (for verification).

Ether and Gas

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Ether and Gas

- ❖ Ether is the currency

Similar to Bitcoin, in Ethereum miners are paid “ether” for mining.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Ether and Gas

- ❖ Ether is the currency
Similar to Bitcoin, in Ethereum miners are paid “ether” for mining.
- ❖ Gas is a unit of work measuring the computational cost of an operation in EVM. Users can buy gas by using Ether
 - ➡ Ethereum Gas is the “fuel” for running smart contract
Just like the fuel for cars :-)
 - ➡ Gas guarantees that all “works” to process a smart contract or a transaction is properly priced.
 - ➡ Complicated contracts require more gas to operate – this prevents DoS attacks.

Assignment Project Exam Help

<https://powcoder.com>
Add WeChat powcoder

Ether and Gas

- ❖ Ether is the currency
Similar to Bitcoin, in Ethereum miners are paid “ether” for mining.
- ❖ Gas is a unit of work measuring the computational cost of an operation in EVM. Users can buy gas by using Ether
 - ➔ Ethereum Gas is the “fuel” for running smart contract
Just like the fuel for cars :-)
 - ➔ Gas guarantees that all “works” to process a smart contract or a transaction is properly priced.
 - ➔ Complicated contracts require more gas to operate – this prevents DoS attacks.
- ❖ Miners are paid “gas” for running smart contracts on the network
Use Ether to buy Gas, and use Gas as “transaction fees” to store and run the smart contract

Assignment Project Exam Help

<https://powcoder.com>
Add WeChat powcoder

Denominations of ether

Unit	Wei Value	Wei
wei	1 wei	Assignment Project Exam Help
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

Ether

The screenshot shows the Ethereum page on CoinMarketCap. The main header displays "Ethereum" with a diamond icon, "ETH", and a "Share" button. Below it, the rank is listed as "Rank #2" and the coin type as "Coin". A note indicates "On 2,871,055 watchlists". On the left sidebar, there are links for "Website", "Explorers", "Community", "Chat", "Source code", "Whitepaper", and sections for "Contracts" (BNB Smart Chain) and "Audits" (Fairyproof). The main content area shows the current price of Ethereum at \$1,752.91, down 1.06% from the previous day. It also shows the low price of \$1,752.52 and the high price of \$1,806.89 over the last 24 hours. The market cap is listed as \$213,664,806,045, down 1.05%. The fully diluted market cap is \$213,664,806,045. The volume for the last 24 hours is \$15,558,905,711, up 23.59%. The circulating supply is 121,891,144.19 ETH. The total supply is 121,891,144. Red text overlays on the page include "Assignment Project Exam Help", the URL "https://powcoder.com", and the instruction "Add WeChat powcoder".

Ethereum Price (ETH)

\$1,752.91 ▾1.06%

Low:\$1,752.52 High:\$1,806.89 24h

Market Cap ⓘ \$213,664,806,045 ▾1.05%

Fully Diluted Market Cap ⓘ \$213,664,806,045

Volume 24h ⓘ \$15,558,905,711 ▲23.59%

Circulating Supply ⓘ 121,891,144.19 ETH

Max Supply ⓘ --

Total Supply ⓘ 121,891,144

Ethereum

ETH

Share

Rank #2 Coin On 2,871,055 watchlists

Website Explorers Community Chat

Source code Whitepaper

Contracts: BNB Smart Chain (BEP20): 0x2170...9f933f8 More

Audits: Fairyproof

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

<https://coinmarketcap.com/currencies/ethereum/>

Ether

Ethereum to USD Chart



Gas cost

Each operation (Opcode) in the EVM was assigned a number of how much gas it consumes.

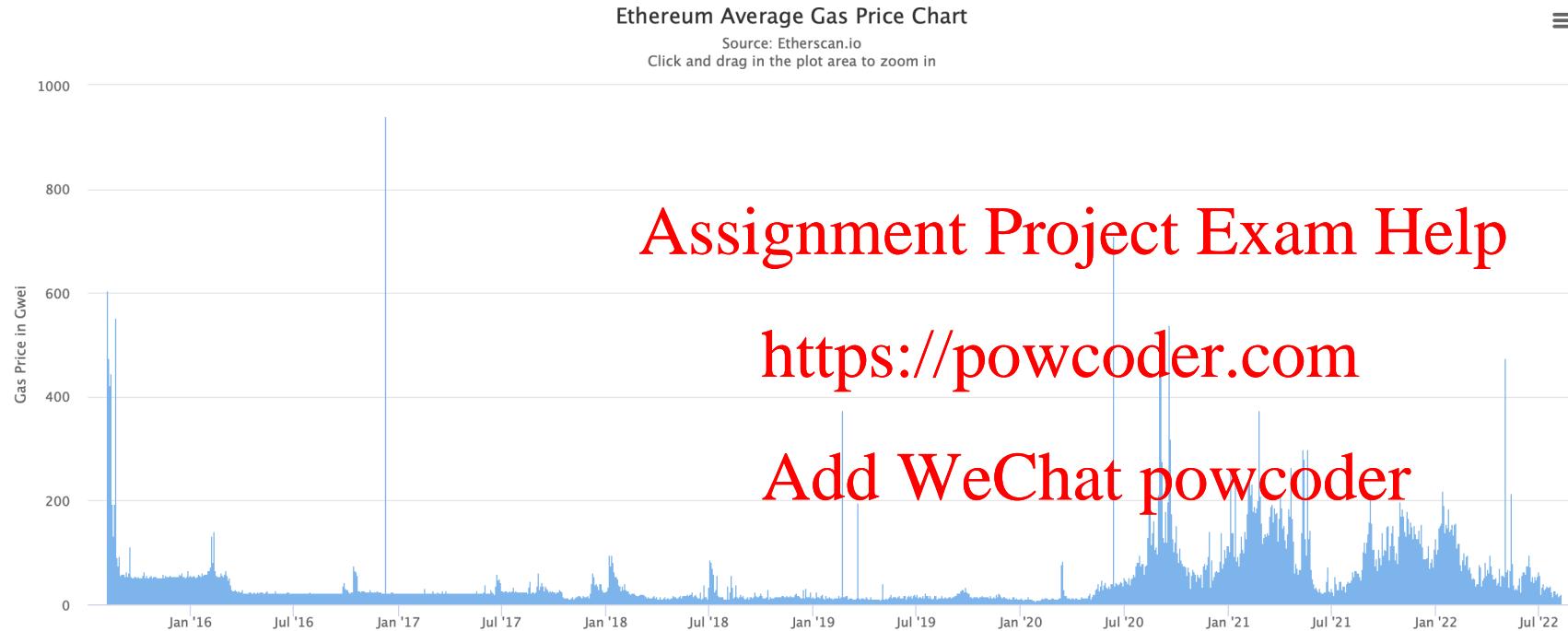
Operation Name	Gas Cost	Remark
step	1	default amount per execution cycle
stop	0	free
suicide	0	free
sha3	20	
sload	20	get from permanent storage
sstore	100	put into permanent storage
balance	20	
create	100	contract creation
call	20	initiating a read-only call
memory	1	every additional word when expanding memory
txdata	5	every byte of data or code for a transaction
transaction	500	base fee transaction
contract creation	53000	changed in homestead from 21000

Assignment Project Exam Help

<https://powcoder.com>

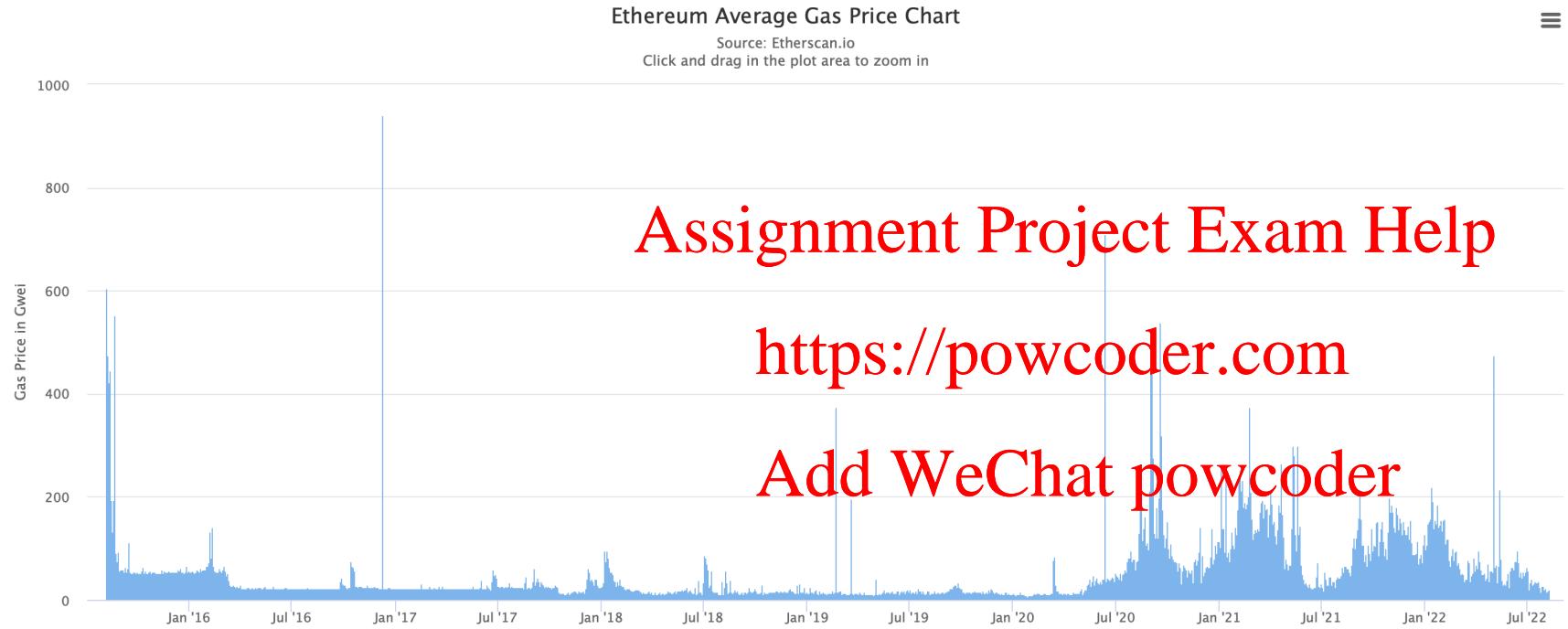
Add WeChat powcoder

Gas



<https://etherscan.io/chart/gasprice>

Gas



<https://etherscan.io/chart/gasprice>

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

Gas Price

Gas Price: the price of a unit of gas the creator is willing to pay.

Like transaction fees, the higher the Gas price is, the faster the transaction will be chosen by a miner.

Assignment Project Exam Help

Category	Value
Cheapest Gas Price (gwei)	18.50654929
Highest Gas Price (gwei)	815
Median Gas Price (gwei)	35
Cheapest Transfer Fee	\$1.4162
Highest Transfer Fee	\$50.18
Total Transactions	8939
% Empty Blocks	0
% Full Blocks	28

<https://powcoder.com>

Add WeChat powcoder



<https://ethgasstation.info>

DeFi

ETH25 LEADERBOARD

Last 30 Days

RANK	NAME	ETH SPENT	AVE. GWEI	USD VALUE
1	Uniswap	1.50K	112	\$2.00M
2	Tether USD	1.24K	133	\$1.65M
3	1inch Exchange	292	125	\$390K
4	USDC	195	133	\$260K
5	0x0000000000000007...e9f56	179	176	\$239K
6	SushiSwap	149	56	\$374K
7	Aave	114	135	\$152K
8	Metamask Swap	100	119	\$134K
9	0x	94.4	122	\$126K
10	0x00c7a37b03690...75446	92.3	145	\$123K
11	0xa57bd00134b28...dd6cf	92.2	308	\$123K
12	0xf570deefff684...f7419	84.3	155	\$112K
13	ChainLink	78.6	140	\$105K
14	0x860bd2dba9cd4...78f66	78.4	158	\$105K
15	0x78a55b9b3bbef...c55e8	71.9	207	\$95.8K
16	0x00000063f648c...ff184	71.8	167	\$95.8K
17	Bitstamp	67.2	172	\$89.5K
18	0x03f34be1bf910...59659	63.2	131	\$84.3K

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Why using gas rather than Ether?

- ❖ Ether is a cryptocurrency, and the price of one ether is ever changing.
- ❖ If using ether, the price of running the same operation/contract can be very different.
- ❖ So, Ethereum uses Gas, where users can define the gas price!

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Error: Out of Gas

If gas is not enough to complete all operations of a transaction, then:

Assignment Project Exam Help

1. the contract is terminated and transaction is cancelled.
2. the miner still gets the transaction fees.
3. the contract creator loses the transaction fees, but not the coin to be transferred.

<https://powcoder.com>

Add WeChat powcoder

Error: Out of Gas

Etherscan

All Filters Search by Address / Txn Hash / Block / Token / Ens

Eth: \$212.59 (+1.10%)

Home Blockchain Tokens Resources More Sign In

Transaction Details

Sponsored: AMFEIX - The World's First Smart Contract Trading Fund - Averaging 20% Compounded Returns Per Month since January.

Overview State Changes New Comments

⑦ Transaction Hash: 0xda8c0b80d8e240a83c8f5b017c9550a9eb73e3e0ee1fd4992a101232f1235c

⑦ Block: 3840222 4493918 Block Confirmations

⑦ Timestamp: 794 days 16 hrs ago (Jun-08-2017 02:02:51 UTC)

⑦ From: 0xec5765dff3b6a36ee32b9c4051d3eaec30f3f483

⑦ To: Contract 0xace62f87abe9f4ee9fd6e115d91548df24ca0243 (Monaco: Token Sale) ▾
Warning! Error encountered during contract execution [Call to great()]

⑦ Value: 0.1 Ether (\$21.26) - [CANCELLED] i

⑦ Transaction Fee: 0.625 Ether (\$132.87)

⑦ Gas Limit: 25,000

⑦ Gas Used by Transaction: 25,000 (100%)

⑦ Gas Price: 0.000025 Ether (25,000 Gwei)

⑦ Nonce Position 0

⑦ Input Data:

```
Function: buyWithCustomerId(uint128 customerId)
MethodID: 0x99e9376c
[0]: 0000000000000000000000000000000050b59b35ebc043df811dba62d371efd9
```

View Input As DecodeInput Data

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

How it works - basics

The high-level idea is the same as Bitcoin

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

How it works - basics

The high-level idea is the same as Bitcoin

Step 1. The very first block, called genesis block, is hardcoded to initialise the system.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

How it works - basics

The high-level idea is the same as Bitcoin

Step 1. The very first block, called genesis block, is hardcoded to initialise the system.

Step 2. New blocks are created through the PoW-based mining process.

- The mining algorithm is Ethash rather than SHA-256 in Bitcoin
- A block is generated every 12 seconds
- Ethereum plans to move to Proof-of-Stake.

<https://powcoder.com>

Add WeChat powcoder

How it works - basics

The high-level idea is the same as Bitcoin

Step 1. The very first block, called genesis block, is hardcoded to initialise the system.

Step 2. New blocks are created through the PoW-based mining process.

- The mining algorithm is Ethash rather than SHA-256 in Bitcoin
- A block is generated every 12 seconds
- Ethereum plans to move to Proof-of-Stake.

<https://powcoder.com>

Step 3. Miners get reward

- The mining reward is static
- Transaction fees go to the miner as well
- An extra of 1/32 of 2 Ether for including Uncles as part of the block.
(Can include up to two Uncles)

[Add WeChat powcoder](#)

How it works - basics

The high-level idea is the same as Bitcoin

Step 1. The very first block, called genesis block, is hardcoded to initialise the system.

Step 2. New blocks are created through the PoW-based mining process.

- The mining algorithm is Ethash rather than SHA-256 in Bitcoin
- A block is generated every 12 seconds
- *Ethereum plans to move to Proof-of-Stake.*

<https://powcoder.com>

Step 3. Miners get reward

- The mining reward is static
- Transaction fees go to the miner as well
- An extra of 1/32 of 2 Ether for including Uncles as part of the block.
(Can include up to two Uncles)

[Add WeChat powcoder](#)

Step 4. Block creators gain the new coins as reward, and spend them through transactions.

How it works - basics

The high-level idea is the same as Bitcoin

Step 1. The very first block, called genesis block, is hardcoded to initialise the system.

Step 2. New blocks are created through the PoW-based mining process.

- The mining algorithm is Ethash rather than SHA-256 in Bitcoin
- A block is generated every 12 seconds
- *Ethereum plans to move to Proof-of-Stake.*

<https://powcoder.com>

Step 3. Miners get reward

- The mining reward is static
- Transaction fees go to the miner as well
- An extra of 1/32 of 2 Ether for including Uncles as part of the block.
(Can include up to two Uncles)

[Add WeChat powcoder](#)

Step 4. Block creators gain the new coins as reward, and spend them through transactions.

Step 5. Transactions are included in blocks through Step 2.

How it works - basics

Smart contract:

Assignment Project Exam Help

<https://powcoder.com>

1. Create a contract (Solidity)
2. Create a transaction containing the contract (EVM bytecode)
3. Submit the transaction to the blockchain

Add WeChat powcoder

Account and wallet

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Account and wallet

Two types of accounts:

- Externally-Owned Account
- Contract Account

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Account and wallet

Two types of accounts:

- Externally-Owned Account
- Contract Account

Wallets:

- A set of one or more external accounts
- Used to store/transfer Ether

<https://powcoder.com>

Add WeChat powcoder

Externally-Owned Account (EOA)

Externally-Owned Account:

- the bank account for a user
- it keeps money (Ether) for the user
- it can send transactions
- controlled by the private key
- no code!

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Contract Account

Contract Account:

- the account for a deployed contract
- it keeps money (Ether) to support the contract
- hold contract code in the memory
- can be triggered by other contracts
- no owner once released

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Transaction

A transaction is a request to modify the state of the blockchain

- It can run code/contracts to change the global state of the blockchain

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Transaction

A transaction is a request to modify the state of the blockchain

- It can run code/contracts to change the global state of the blockchain

Assignment Project Exam Help

Types of transactions: <https://powcoder.com>

- **Value Transaction:**

Fund transfer between EOAs

[Add WeChat powcoder](#)

- **Creation Transaction:**

Deploy a contract on Ethereum network

- **Invocation Transaction:**

Invoke code (functions) on a Deployed Contract

Transaction

Main fields:

- **From:** Fund sender, an EOA
- **To:** Fund receiver, an EOA
- **Value:** amount
(wei is the unit)
- **Gas Limit:** the total amount of gas.
(The default amount for a standard ETH transfer is 21,000 gas)
- **Gas Price:** the price of a unit of gas the creator is willing to pay
(Gwei is the unit).

The total cost of a transaction (the “transaction fee”) is:
the Gas Limit * Gas Price

Transaction

Transaction Details

Etherscan - Sponsored slots available. [Book your slot here!](#)

Overview	State Changes	New	Comments
⑦ Transaction Hash:	0x86d70d9c9ec0873d8a0c8e4c48af426394090ea7eab3e5f5c10ac6db4260e35c		
⑦ Status:	Success		
⑦ Block:	8083074	2 Block Confirmations	
⑦ Timestamp:	⌚ 14 secs ago (Jul-04-2019 05:51:14 AM UTC)		
⑦ From:	0x4332ae6a251d3200bbe08432c00bcc2d0e4100dd		
⑦ To:	0x8803c1abd5b229bbf94da201908ef011df33d		
⑦ Value:	13 Ether (\$3,828.89)		
⑦ Transaction Fee:	0.000168 Ether (\$0.05)		
⑦ Gas Limit:	21,000		
⑦ Gas Used by Transaction:	21,000 (100%)		
⑦ Gas Price:	0.000000008 Ether (8 Gwei)		
⑦ Nonce	Position	24	145
⑦ Input Data:	0x		

<https://etherscan.io>

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Transaction

Transaction Details

Etherscan - Sponsored slots available. [Book your slot here!](#)

[Overview](#) [State Changes](#) [New](#) [Comments](#)

⑦ Transaction Hash: [0x86d70d9c9ec0873d8a0c8e4c48af426394090ea7eab3e5f5c10ac6db4260e35c](#)

⑦ Status: Success

⑦ Block: [8083074](#) 2 Block Confirmations

⑦ Timestamp: ⌚ 14 secs ago (Jul-04-2019 05:51:14 AM +UTC)

⑦ From: [0x4332ae6a251d3200bbe08432c00bcc2d0e4100dd](#)

⑦ To: [0x8803c1abd5b229bbf94da20908ef011df33d](#)

⑦ Value: 13 Ether (\$3,828.89)

⑦ Transaction Fee: 0.000168 Ether (\$0.05)

Gas price*gas limit = transaction fee
0.00000008 Ether * 21000 = 0.000168 Ether

⑦ Gas Limit: 21,000

⑦ Gas Used by Transaction: 21,000 (100%)

⑦ Gas Price: 0.00000008 Ether (8 Gwei)

⑦ Nonce 24 145

⑦ Input Data: 0x

[https://etherscan.io](#)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Transaction

Transaction Details

Etherscan - Sponsored slots available. [Book your slot here!](#)

[Overview](#) [State Changes](#) [New](#) [Comments](#)

⑦ Transaction Hash: [0x86d70d9c9ec0873d8a0c8e4c48af426394090ea7eab3e5f5c10ac6db4260e35c](#)

⑦ Status: Success

⑦ Block: [8083074](#) 2 Block Confirmations

⑦ Timestamp: ○ 14 secs ago (Jul-04-2019 05:51:14 AM +UTC)

⑦ From: [0x4332ae6a251d3200bbe08432c00bcc2d0e4100dd](#)

⑦ To: [0x8803c1abd5b229bbf94da20908ef011df33d](#)

⑦ Value: 13 Ether (\$3,828.89)

⑦ Transaction Fee: 0.000168 Ether (\$0.05) Gas price*gas limit = transaction fee
0.00000008 Ether * 21000 = 0.000168 Ether

⑦ Gas Limit: 21,000

⑦ Gas Used by Transaction: 21,000 (100%)

⑦ Gas Price: 0.00000008 Ether (8 Gwei)

⑦ Nonce 24 145

⑦ Input Data: 0x No data for smart contract, so this is only for transferring money (13 Ether)

[https://etherscan.io](#)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Transaction

Transaction Details

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

gas limit = 98,415 > 21.000

Bytecode of a contract



Transaction

- ❖ Given a smart contract source code (Solidity), it is easy to verify the bytecode.

You need to trust Etherscan using the service. If you don't, you still need to trust EVM.

- ❖ It is very hard to decompile from bytecode to Solidity, but you can publish the verified smart contract source code at Etherscan.

<https://powcoder.com>
Add WeChat powcoder

Transaction

- ❖ Given the by

You ne
still n

- ❖ It is v
publis

Verify & Publish Contract Source Code

COMPLIER TYPE AND VERSION SELECTION

Source code verification provides transparency for users interacting with smart contracts. By uploading the source code, Etherscan will match the compiled code with that on the blockchain. Just like contracts, a "smart contract" should always do what it says it does. Verification on the blockchain allows anyone to audit the code to independently verify that it actually does what it is supposed to do.

Please enter the Contract Address you would like to verify

Please select Compiler Type

Solidity (Single file)

Please select Compiler Version

[Please Select]

Un-Check to show all nightly Commits also

I agree to the [terms of service](#)

[Continue](#) [Reset](#)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

<https://etherscan.io>

Transaction

Verify & Publish Contract Source Code
Compiler Type: SINGLE FILE / CONCATENATED METHOD

Info: A simple and structured interface for verifying smart contracts that fit in a single file

Contract Source Code

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

1. If the contract compiles correctly at REMIX, it should also compile correctly here.
2. We have limited support for verifying contracts created by another contract and there is a timeout of up to 45 seconds for each contract compiled.
3. For programmatic contract verification, check out the [Contract API Endpoint](#)

Contract Address: 0xd70b0C09890A5b2a3957af2D3B340b7618989Fa

Compiler: v0.6.1-nightly|2019.3.1+commit.470fe8a

Optimization: No

Enter the Solidity Contract Code below *

Fetch from Gist

<https://etherscan.io>

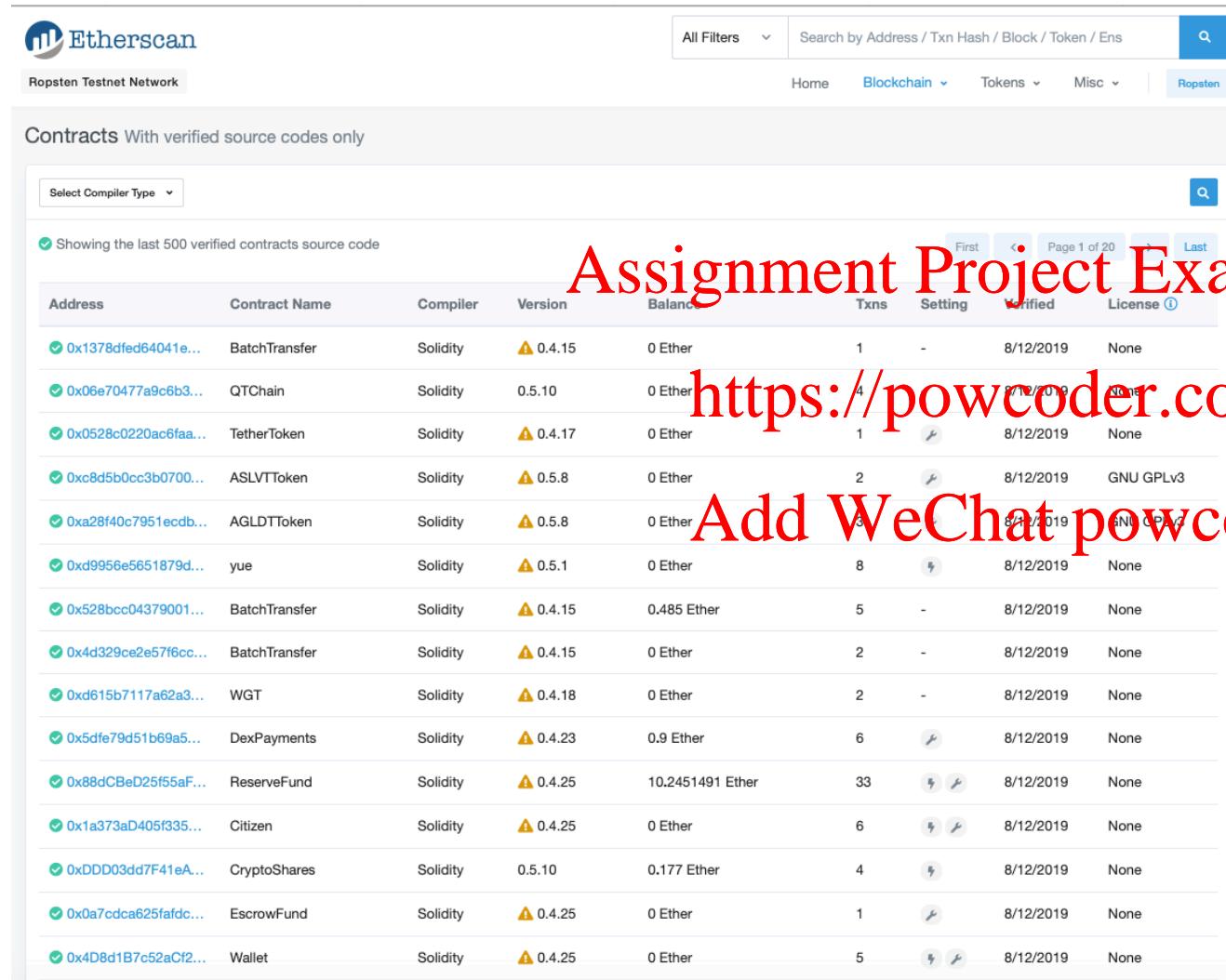
Contracts With verified source codes

The screenshot shows the Etherscan interface for the Ropsten Testnet Network. The main heading is "Contracts With verified source codes only". A red watermark "Assignment Project Exam Help" is overlaid across the middle of the page. Below it, a large red watermark URL "https://powcoder.com" and a red watermark text "Add WeChat powcoder" are displayed. At the bottom left, another red watermark URL "https://ropsten.etherscan.io/contractsVerified" is shown. The table lists 15 contracts from the last 500, with columns for Address, Contract Name, Compiler, Version, Balance, Txns, Setting, Verified, and License.

Address	Contract Name	Compiler	Version	Balance	Txns	Setting	Verified	License
0x1378dfed64041e...	BatchTransfer	Solidity	0.4.15	0 Ether	1	-	8/12/2019	None
0x06e70477a9c6b3...	QTChain	Solidity	0.5.10	0 Ether	4	-	8/12/2019	None
0x0528c0220ac6faa...	TetherToken	Solidity	0.4.17	0 Ether	1		8/12/2019	None
0xc8d5b0cc3b0700...	ASLVTToken	Solidity	0.5.8	0 Ether	2		8/12/2019	GNU GPLv3
0xa28f40c7951ecdb...	AGLDTToken	Solidity	0.5.8	0 Ether	3		8/12/2019	GNU GPLv3
0xd9956e5651879d...	yue	Solidity	0.5.1	0 Ether	8		8/12/2019	None
0x528bcc04379001...	BatchTransfer	Solidity	0.4.15	0.485 Ether	5	-	8/12/2019	None
0x4d329ce2e57f6cc...	BatchTransfer	Solidity	0.4.15	0 Ether	2	-	8/12/2019	None
0xd615b7117a62a3...	WGT	Solidity	0.4.18	0 Ether	2	-	8/12/2019	None
0x5dfe79d51b69a5...	DexPayments	Solidity	0.4.23	0.9 Ether	6		8/12/2019	None
0x88dCBeD25f55aF...	ReserveFund	Solidity	0.4.25	10.2451491 Ether	33		8/12/2019	None
0x1a373aD405f335...	Citizen	Solidity	0.4.25	0 Ether	6		8/12/2019	None
0xDDD03dd7F41eA...	CryptoShares	Solidity	0.5.10	0.177 Ether	4		8/12/2019	None
0xa07cdca625fafdc...	EscrowFund	Solidity	0.4.25	0 Ether	1		8/12/2019	None
0x4D8d1B7c52aCf2...	Wallet	Solidity	0.4.25	0 Ether	5		8/12/2019	None

<https://ropsten.etherscan.io/contractsVerified>

Contracts With verified source codes



The screenshot shows the Etherscan interface for the Ropsten Testnet Network. The main heading is "Contracts With verified source codes only". A red watermark "Assignment Project Exam Help" is overlaid across the middle of the page. Below it, a large red URL "https://powcoder.com" and a red text "Add WeChat powcoder" are displayed. The table lists 15 contracts from the last 500, with columns for Address, Contract Name, Compiler, Version, Balance, Txns, Setting, Verified, and License.

Address	Contract Name	Compiler	Version	Balance	Txns	Setting	Verified	License
0x1378dfed64041e...	BatchTransfer	Solidity	0.4.15	0 Ether	1	-	8/12/2019	None
0x06e70477a9c6b3...	QTChain	Solidity	0.5.10	0 Ether	4	-	8/12/2019	None
0x0528c0220ac6faa...	TetherToken	Solidity	0.4.17	0 Ether	1		8/12/2019	None
0xc8d5b0cc3b0700...	ASLVTToken	Solidity	0.5.8	0 Ether	2		8/12/2019	GNU GPLv3
0xa28f40c7951ecdb...	AGLDTToken	Solidity	0.5.8	0 Ether	3		8/12/2019	GNU GPLv3
0xd9956e5651879d...	yue	Solidity	0.5.1	0 Ether	8		8/12/2019	None
0x528bcc04379001...	BatchTransfer	Solidity	0.4.15	0.485 Ether	5	-	8/12/2019	None
0x4d329ce2e57f6cc...	BatchTransfer	Solidity	0.4.15	0 Ether	2	-	8/12/2019	None
0xd615b7117a62a3...	WGT	Solidity	0.4.18	0 Ether	2	-	8/12/2019	None
0x5dfe79d51b69a5...	DexPayments	Solidity	0.4.23	0.9 Ether	6		8/12/2019	None
0x88dCBeD25f55aF...	ReserveFund	Solidity	0.4.25	10.2451491 Ether	33		8/12/2019	None
0x1a373aD405f335...	Citizen	Solidity	0.4.25	0 Ether	6		8/12/2019	None
0xDDD03dd7F41eA...	CryptoShares	Solidity	0.5.10	0.177 Ether	4		8/12/2019	None
0xa07cdca625fafdc...	EscrowFund	Solidity	0.4.25	0 Ether	1		8/12/2019	None
0x4D8d1B7c52aCf2...	Wallet	Solidity	0.4.25	0 Ether	5		8/12/2019	None

<https://ropsten.etherscan.io/contractsVerified>

Again, you need to trust Etherscan if using the service

Running a transaction

All full nodes do:

- Verification:
The sender.balance should have at least $\text{Value} + \text{Gas Limit} * \text{Gas price}$

[Assignment](#) [Project](#) [Exam](#) [Help](#)

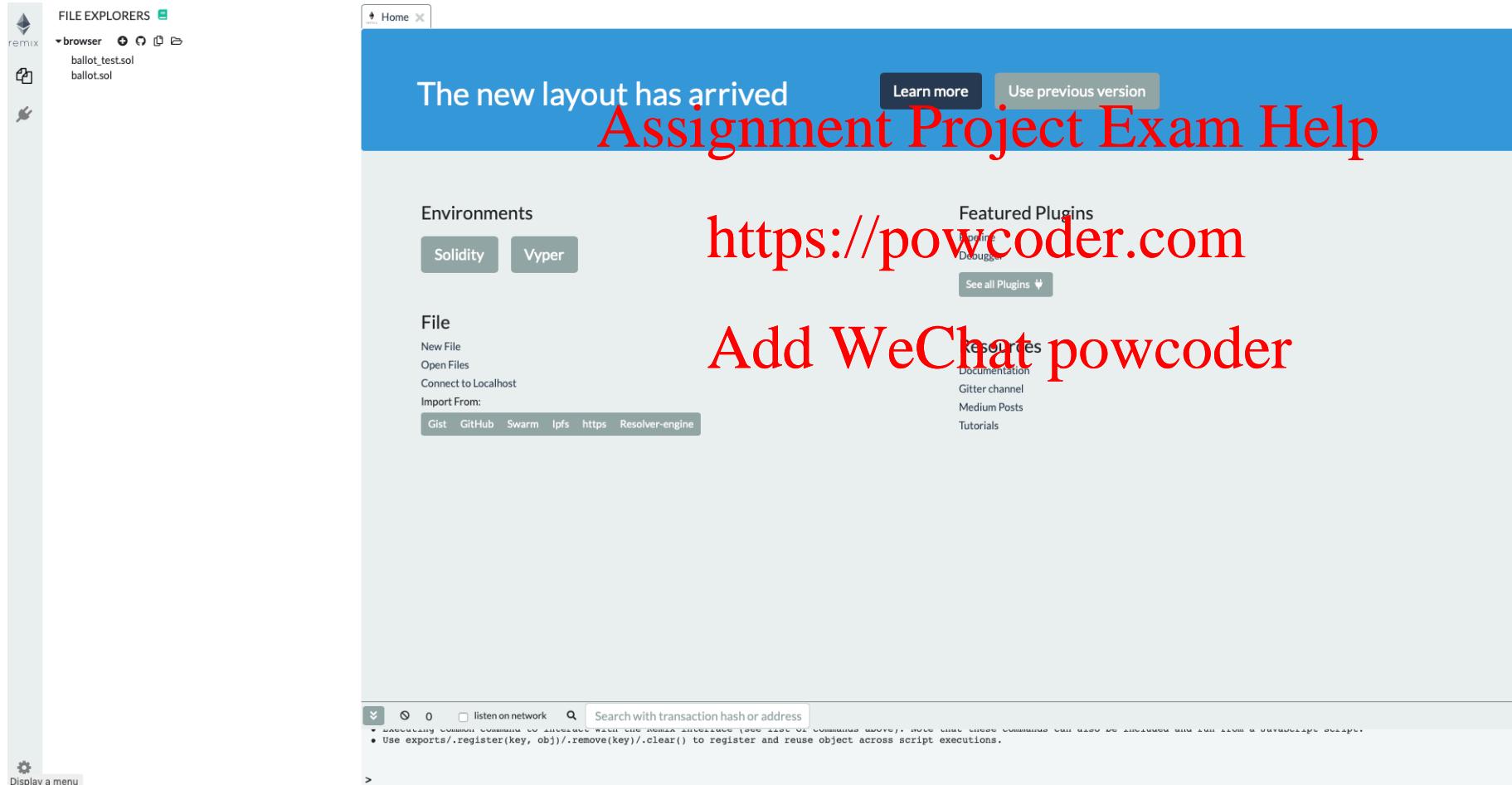
- Update account balance:
 - Recipient.balance += Value
 - Sender.balance -= Value + Gas Limit * Gas price
 - Sender.balance += The unused gas * Gas price

<https://powcoder.com>

Add WeChat powcoder

Remix

An IDE to write, deploy, and run smart contracts in Solidity or Vyper.
You can access Remix from a web browser!



The screenshot shows the Remix IDE interface. At the top, there's a blue header bar with the text "The new layout has arrived" and buttons for "Learn more" and "Use previous version". Below the header, the main menu bar features "Assignment Project Exam Help" in red text. On the left side, there's a sidebar titled "FILE EXPLORERS" with a "remix" icon. It lists a "browser" section containing "ballot_testsol" and "ballot.sol". Below this, there are icons for "File Explorer", "Terminal", and "Logs". The main workspace has several sections: "Environments" with "Solidity" and "Vyper" buttons; "File" with options like "New File", "Open Files", "Connect to Localhost", and "Import From:" with links to "Gist", "GitHub", "Swarm", "Ipfs", "Https", and "Resolver-engine". To the right, there's a "Featured Plugins" section with "See all Plugins" and a "RESOURCES" section with links to "Documentation", "Gitter channel", "Medium Posts", and "Tutorials". At the bottom, there's a search bar with "Search with transaction hash or address" and a note about executing common commands. A footer bar at the very bottom contains a gear icon and the text "Display a menu".

<https://remix.ethereum.org>

Decentralized Autonomous Organization (DAO)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Decentralized Autonomous Organization (DAO)

May 2016

DAO deployed a smart contract to raise 11.5 million Ether (\$150 million USD at the time) in a token sale for funding

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Decentralized Autonomous Organization (DAO)

May 2016 DAO deployed a smart contract to raise 11.5 million Ether (\$150 million USD at the time) in a token sale for funding

June 2016 Vulnerability is found in DAO code, and 3.6 million Ether (\$50 million USD at the time) was stolen.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Decentralized Autonomous Organization (DAO)

May 2016	DAO deployed a smart contract to raise 11.5 million Ether (\$150 million USD at the time) in a token sale for funding
June 2016	Vulnerability is found in DAO code, and 3.6 million Ether (\$50 million USD at the time) was stolen. Assignment Project Exam Help
20 July 2016	Ethereum community at large decided to hard fork the chain to restore the funds to their original wallets and patch the vulnerability Add WeChat powcoder <ul style="list-style-type: none">• Ethereum Classic (ETC): The continued original chain containing the vulnerability in DAO code• Ethereum (ETH): The hard forked chain with vulnerability of DAO code patched and stolen money returned to their owner. The majority of the community and the core developers continued working on this chain.

The DAO Attack (simplified)

A contract can have one unnamed function, called **fallback function**. This function does not take any arguments and it is triggered in three cases:

1. No functions of the call to a contract match any of the functions in the called contract.
[Assignment Project Exam Help
https://powcoder.com](https://powcoder.com)
2. No data was supplied.
3. The contract receives Ether without extra data.
[Add WeChat powcoder](#)

Reentrancy Attack on DAO

A simplified example of DAO:

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x());  
        balances[msg.sender] -= x;  
    }  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

A simplified example of DAO:

```
mapping (address => unit) public balances;
```

```
function withdraw(uint x) {
    if (balances[msg.sender] >= x) {
        msg.sender.call.value(x)();
        balances[msg.sender] -= x;
    }
}
```

It maps an **address** to a **value**, and stores the value in a public variable **balances**.

Similar to `dictionary[key]=value` , it is a key-value pair in dictionary, where **balances** has a set of **unit** data type values mapped by **address** data type.

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

A simplified example of DAO:

```
mapping (address => unit) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x());  
        balances[msg.sender] -= x;  
    }  
}
```

Assignment Project Exam Help
It returned the balance of a sender's address, as defined before.

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

A simplified example of DAO:

```
mapping (address => unit) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Assignment Projects Exam Help
Balance of the sender in this contract to the sender's account address
<https://powcoder.com>
Add WeChat powcoder

Reentrancy Attack on DAO

A simplified example of DAO:

```
mapping (address => unit) public balances;

function withdraw(uint x) {
    if (balances[msg.sender] >= x) {
        msg.sender.call.value(x)();
        balances[msg.sender] -= x;
    }
}
```

Assignment Project Exam Help is
recalculated only after sending the

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Honest User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    EventMoneyReceived(msg.value);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Honest User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    Event MyEvent.Received(msg.value);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The unnamed function, fallback function

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Honest User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    EventMoneyReceived(msg.value);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Honest User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    EventMoneyReceived(msg.value);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Honest User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    EventMoneyReceived(msg.value);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The user receives money if have enough balance in the DAO contact.

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

The user's balance in DAO is
recalculated.

Honest User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    EventMoneyReceived(msg.value);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The user receives money if have
enough balance in the DAO contact.

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

The user's balance in DAO is
recalculated.

Honest User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    EventMoneyReceived(msg.value);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The user receives money if have
enough balance in the DAO contact.

Group discussion:
what can go wrong?

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => unit) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Attacker User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    A.withdraw(5);  
}
```

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => unit) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Attacker User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    A.withdraw(5);  
}
```

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => unit) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Attacker User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    A.withdraw(5);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => unit) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

Attacker User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    A.withdraw(5);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The user receives money if have enough balance in the DAO contact, and asks to withdraw money again.

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

withdraw function is triggered again,
the user's balance in DAO is not recalculated!

Attacker User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    A.withdraw(5);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The user receives money if have
enough balance in the DAO contact,
and asks to withdraw money again.

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => uint) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

withdraw function is triggered again,
the user's balance in DAO is not recalculated!

Looping until:

- exception
- Out of gas
- Stack limit is reached

Attacker User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    A.withdraw(5);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The user receives money if have
enough balance in the DAO contact,
and asks to withdraw money again.

Reentrancy Attack on DAO

DAO Contract

```
mapping (address => unit) public balances;  
  
function withdraw(uint x) {  
    if (balances[msg.sender] >= x) {  
        msg.sender.call.value(x)();  
        balances[msg.sender] -= x;  
    }  
}
```

withdraw function is triggered again,
the user's balance in DAO is not recalculated!

Looping until:

- exception
- Out of gas
- Stack limit is reached

The user's balance in DAO is now recalculated.

Attacker User Contract

```
function MoneyWithdraw() {  
    A.withdraw(5);  
}  
function() {  
    A.withdraw(5);  
}
```

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

The user receives money if have enough balance in the DAO contact, and asks to withdraw money again.

The overflow and underflow attack

EthFiddle Security Audit Share Login

```
1 pragma solidity 0.4.20;
2
3 contract OverflowUnderFlow {
4     uint8 public a = 0;
5     uint8 public b = 255;
6     uint8 public c = 0;
7     uint8 public d = 1;
8
9     function overflow() public {
10         a+=b;
11     }
12
13    function underflow() public {
14        c-=d;
15    }
16 }
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The overflow and underflow attack

EthFiddle Security Audit Share Login

```
1 pragma solidity 0.4.20;
2
3 contract OverflowUnderFlow {
4     uint8 public a = 1;
5     uint8 public b = 255;
6     uint8 public c = 0;
7     uint8 public d = 1;
8
9     function overflow() public {
10         a+=b; //return 0
11     }
12
13    function underflow() public {
14        c-=d; //return 255
15    }
16 }
```

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

It happens ...

Etherscan

Eth: \$212.66 (+1.51%)

All Filters Search by Address / Txn Hash / Block / Token / Ens

Home Blockchain Tokens Resources More Sign In

Address 0xDF31A499A5A8358b74564f1e2214B31bB34Eb46F

Sponsored: AMFEIX - The World's First Smart Contract Trading Fund - Average 24% Returns including fees per month since January.

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

Overview

Balance: 0.000022365625 Ether

Ether Value: Less Than \$0.01 (@ \$212.66/ETH)

Token: \$343,398,726,944,783,...

Transactions Erc20 Tokens

Latest 14 txns

Txn Hash	Block Number	From	To	Value	Txn Fee
0xea37879343f720d...	583	SmartMesh (SMT)	0xd6a09bdb29e1ea...	0.02559 Ether	0.0000651
0xf6356e90e15ef10...	550	UG Token (UGT)	0xdf31a499a5a8358...	0 Ether	0.000021
0xa17df960900dfe4...	550	UG Token (UGT)	0xdf31a499a5a8358...	0 Ether	0.000105
		Subtotal:	\$343,398,726,944,783,000,000,000...		

Ethics

An ethical issue:

- Could an action (or product) be damaging to someone or some group?
- Identify the stakeholders; consult those who would be impacted
- Vulnerability disclosure
 - How to disclose vulnerabilities that impacts more than one blockchains is still an open challenge.
- Some key vulnerabilities still exist in the current systems
 - Not well regulated
 - DO NOT ATTACK!
(you can try attacks on testnets and in our labs)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Ethics

An ethical issue:

- Could an action (or product) be damaging to someone or some group?
- Identify the stakeholders; consult those who would be impacted
- Vulnerability disclosure
 - How to disclose vulnerabilities that impacts more than one blockchains is still an open challenge.
- Some key vulnerabilities still exist in the current systems
 - Not well regulated
 - DO NOT ATTACK!
(you can try attacks on testnets and in our labs)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

DO NOT ATTACK!

Reading

A nice place to expand your knowledge about smart contract:

<https://docs.soliditylang.org/en/v0.8.16/>

Assignment Project Exam Help

The book "Introducing Ethereum and Solidity" also has information
about Ethereum and Solidity (log in with Monash access):

<https://link.springer.com/book/10.1007/978-1-4842-2535-6>

Add WeChat powcoder

Next lecture: Proof-of-Work

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder