Teaching the Fundamentals of Blockchains and Smart Contracts

- Debasis Bhattacharya, JD, DBA
- maui.hawaii.edu/cybersecurity
- University of Hawaii Maui College

- ATE 2019 – Demonstration Session

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

NSF

AMERICAN ASSOCIATION OF COMMUNITY COLLEGES
100 since 1920
A CENTURY OF SUCCESS

Google

bitcoin

All | News | Images | Videos | Shopping | More | Settings | Tools

About 472,000,000 results (0.64 seconds)

Official Site - Bitcoin IRA™ | Safe & Secure. Self-Trade 24/7

Ad www.bitcoinira.com/IRA-Lift-Off/🚀

The only platform that allows you to buy and sell crypto directly inside your IRA or 401K. 24/7 Self-Trading. Secured w/ BitGo™ Wallet. High Return Potential.

Video: How It Works · Create A Free Account · 24/7 Self-Trade Platform

Buy Bitcoin In 3 Minutes | Earn $10 For Your First Trade

Ad www.gemini.com/

Gemini Makes Buying **Bitcoin** Simple, Safe & Secure. Start Experiencing The Future of Money For Free! #1 In Security & Safety. Trade In Minutes. Crypto Insurance Provided. Services: Buy & Sell **Bitcoin**, Price Charts, Price Alerts, Secure Custody.

Buy Bitcoin Instantly · "Best Crypto Exchange" · Industry-Best Security

1 Bitcoin equals

7,913.16 United States Dollar

Oct 20, 6:04 AM UTC · Disclaimer

1D 5D 1M 1Y 5Y Max

1 | Bitcoin

7913.16 | United States Dolla

Bitcoin

Currency

Bitcoin is a cryptocurrency. It is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries. Wikipedia

Symbol: ₿

Ledger start: 3 January 2009 (10 years ago)

Supply limit: ₿21,000,000

Latest release: 0.18.1 / 9 August 2019 (51 days ago)

Founder: Satoshi Nakamoto

Total number: The theoretical total number of Bitcoin, 21 million, should not be confused with the total spendable supply.

seekingalpha.com

Google

blockchain

All | News | Videos | Images | Books | More | Settings | Tools

About 247,000,000 results (0.54 seconds)

IBM Blockchain Platform | Built for a Multi-Cloud World | IBM.com

Ad www.ibm.com/IBM-Blockchain/Platform

Build Innovative Applications for Your **Blockchain** Network Using Integrated Capabilities.

Get Started w/ Blockchain

Learn How to Architect Enterprise Blockchain Networks with IBM Today.

IBM Blockchain Overview

Develop & Operate Your Business Network with IBM Blockchain.

Deloitte's Blockchain Survey | New Report: Read the Results

Ad www.deloitte.com/

2019 Global **Blockchain** Survey: **Blockchain** Gets Down to Business. Learn More. Fortune 500 Clients. Local Knowledge. 20+ Industry Sectors. Innovative Solutions. Global Network of Firms.

Blockchain Applications · Blockchain Solutions · Blockchain in Health Care

Blockchain - The Most Trusted Crypto Company

https://www.blockchain.com

Blockchain is the world's most trusted all-in-one crypto company. We're connecting the world to the future of finance through our suite of products including the ...

Bitcoin Explorer

The most popular and trusted block explorer and crypto ...

Blockchain Wallet

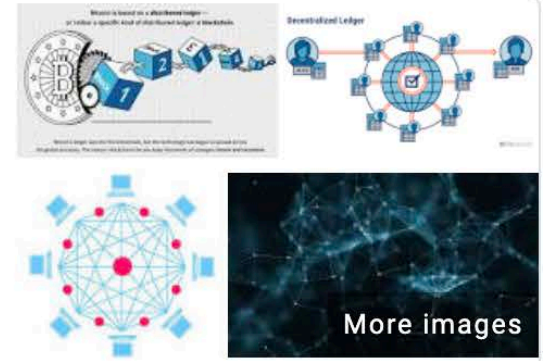
Discover the world's most popular bitcoin wallet. Visit today to ...

Wallet

Best in Class Security. Rest easy

What is Bitcoin

The digital asset, bitcoin, is used



Blockchain

A blockchain, originally block chain, is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data. Wikipedia

Blockchain companies

View 35+ more

Riot Blockchain | HIVE Blockchain | Long Blockchain Corp. | Interbit | Glb Gaming Technolo...

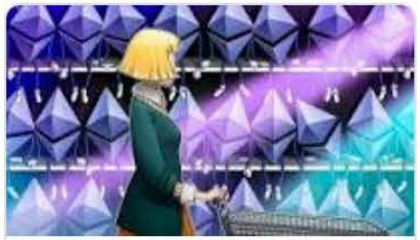
Google

ethereum

All | News | Videos | Images | Books | More | Settings | Tools

About 85,600,000 results (0.47 seconds)

Top stories



Ethereum Futures: The Next Big Derivative to Hit the Market?

Cointelegraph

6 hours ago

Dark Horses of dApps: 6 Blockchains With Ethereum In Their Sights

Crypto Briefing

2 days ago

As Bitcoin price nears 50% drop, analyst foresees deeper correction for Ethereum

CryptoSlate

1 hour ago

→ More for ethereum

Ethereum: Home

https://www.ethereum.org

Ethereum is a global, decentralized platform for money and new kinds of applications. On **Ethereum**, you can write code that controls money, and build ...

Beginners · Learn · Ethereum Blog · Use

Ethereum

Ethereum is an open source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality. It supports a modified version of Nakamoto consensus via transaction-based state transitions. Wikipedia

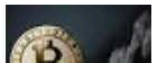
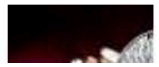
Initial release date: July 30, 2015

Original authors: Vitalik Buterin, Gavin Wood, Joseph Lubin

Written in: C++, Go, Rust, Solidity

People also search for

View 15+ more


Google

smart contract

All | News | Images | Books | Videos | More | Settings | Tools

About 313,000,000 results (0.56 seconds)

Hewlett Packard Enterprise | Blockchain for Enterprise

Ad www.hpe.com/info/nonstop

Read the Business Continuity Best Practices Guide for Surviving Data Center Disasters. NonStop Delivers an Integrated Software Stack Designed for Fault Tolerance & Scalability.

Read the White Paper
Drive Business Transformation.
Learn About DLT & Smart Contracts.

Learn More About HPE
Get Advice, Answers, & Solutions
When You Need Them.

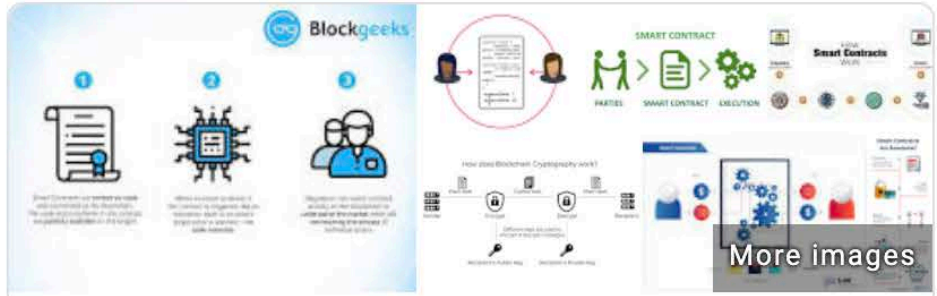
Smart Contracts Blockchain | Transform How You Do Business

Ad www.icertis.com/

Learn more about how **smart contracts** are changing the foundations of commerce! Use Icertis **Contract** Management Software. Trusted by global brands. 50% Compliance Increase. Choice Enterprise CLM. Adapt W/Click Of A Button. Cloud Based CLM Software.

Icertis ICM Platform · Our Customers · Why Icertis · Evaluation Resources

A **smart contract** is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a **contract**. **Smart contracts** allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.



Smart contract

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible. Wikipedia

Feedback

Separating the hype from the technology

- Crypto currencies are becoming popular with banks, consumers and various industries.
- Blockchains are in the news for supply chain, finance transactions, distributed ledger etc.
- There is a need for consumers and students to understand the basic underlying technology behind these crypto currencies.

Sample Course Topics Outline

1. Introduction to Bitcoin
2. Mining
3. Consensus
4. Cryptocurrency Security
5. Ethereum Basics
6. Cryptography
7. Wallets
8. Transactions
9. Smart Contracts Programming
10. Smart Contracts Security
11. Tokens
12. Oracles
13. Distributed Apps
14. Web3 – The Decentralized Web

Sample Course on Block Chain Technology

- Sample Course Description – ICS 2xx: Intro to Blockchain Technology
  - Provides an introduction to cryptocurrencies, blockchain technology, smart contracts and distributed applications (DApps). Topics include the origins of the Bitcoin cryptocurrency and its evolution over the past decade, the rise of the Ethereum Virtual Machine (EVM) and Blockchain, the proliferation of Smart Contracts using Solidity, and the emergence of DApps that use Blockchain for a variety of applications.
- Prerequisites – Basic understanding of JavaScript or Python
- Recommended Textbooks
  - Mastering Bitcoin 2 nd Ed., Andreas Antonopoulos, O'Rielly Media, ISBN-13: 978-1491954386, Available on Amazon
  - 2. Mastering Ethereum: Building Smart Contracts and DApps, O'Rielly Media, ISBN-13: 978-1491954386, Available on Amazon
- Course Objectives
  - Students will learn the underlying technology behind crypto currencies, blockchains, smart contracts and distributed applications using hands-on labs
  - Students will experience real-world case studies and applications of crypto currencies, blockchains, smart contracts and distributed applications

Embed Content and Labs within Traditional Programs/Courses

- Accounting
- Finance
- Business
- Computer Science
- Information Technology
- Cybersecurity
- Administration of Justice
- Law
- Etc…

Examples from CompSci and Business

- Computer Science
  - Proof of Work Protocol
  - Economic measure to deter DDOS or Spam
  - Extend understanding to create transaction block in a chain
  - Mining computers, hash rate
  - Electricity consumption
- Business: Accounting, Finance, Supply Chain, Security
  - Tax and government regulations
  - Distributed ledger for private/public supply chain
  - Cryptocurrencies for payments
  - Initial Coin Offering (ICO) for startups
  - Security of Wallets and Exchanges

Bitcoin

- A distributed, decentralized digital currency system
- Released by Satoshi Nakamoto 2008
- Effectively a bank run by an ad hoc network
  - Digital checks
  - A distributed transaction log

Size of the BitCoin Economy

- Number of BitCoins in circulation ~18 million (October 19, 2019)
- Total number of BitCoins generated cannot exceed 21 million.
  - Around 3 million left to be mined!
- Average price of a Bitcoin:
  - $7,913 on October 19, 2019
  - $4,110 on February 23, 2019
  - $3729 on Dec 29, 2018
  - $8,522 on May 15, 2018
  - $7,149 on April 8, 2018
  - $18,000 on December, 2017
  - $3,867 on September 25, 2017;
  - $2,350 on June 27, 2017
  - Price has been very unstable and speculative.
- Currently, 244,157 tx/day or ~170 tx/minute.
  (In contrast, Visa transaction 200,000 per minute!)

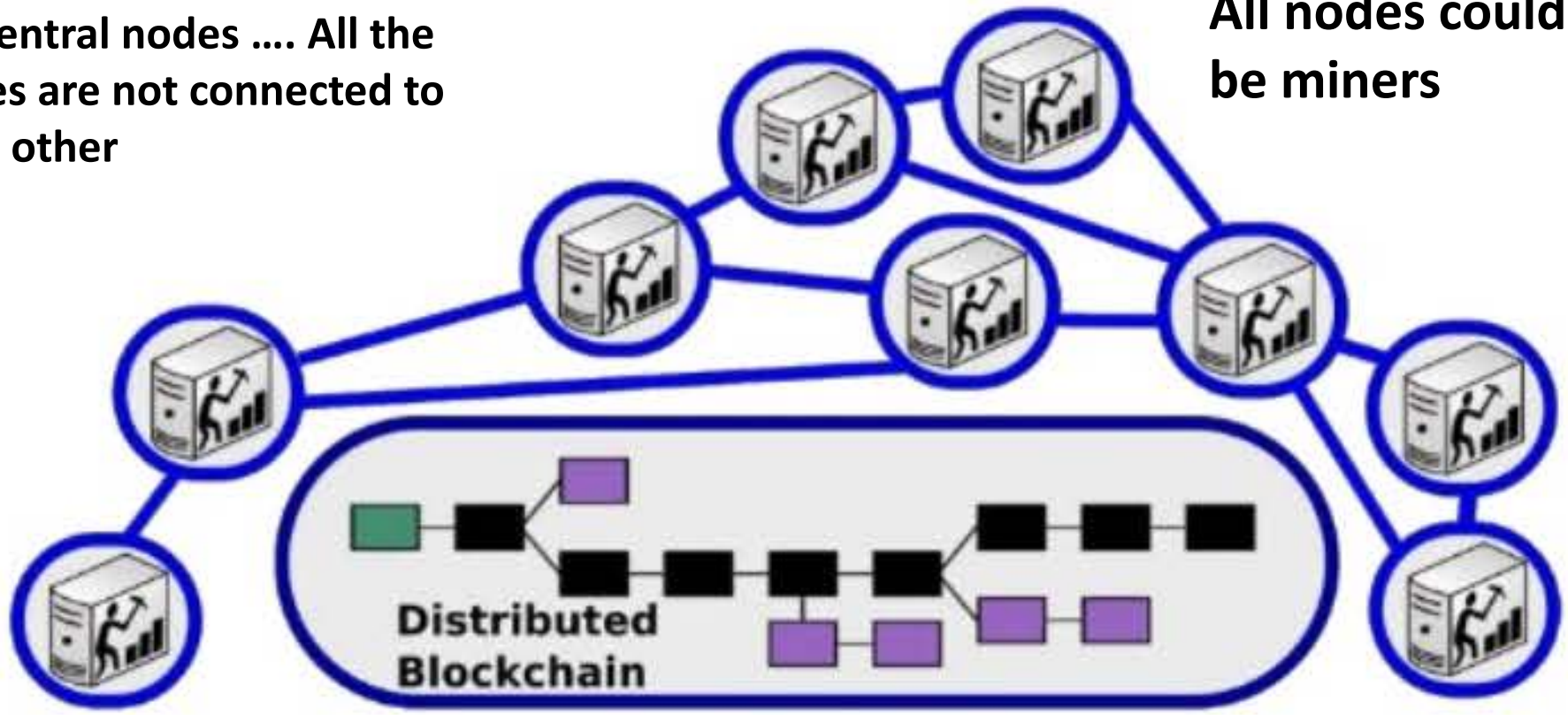

I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
S. Adams
E-mail: SCOTTADAMS@AOL.COM
© 1995 United Feature Syndicate, Inc.(NYC)

Blockchain Process… Decentralization

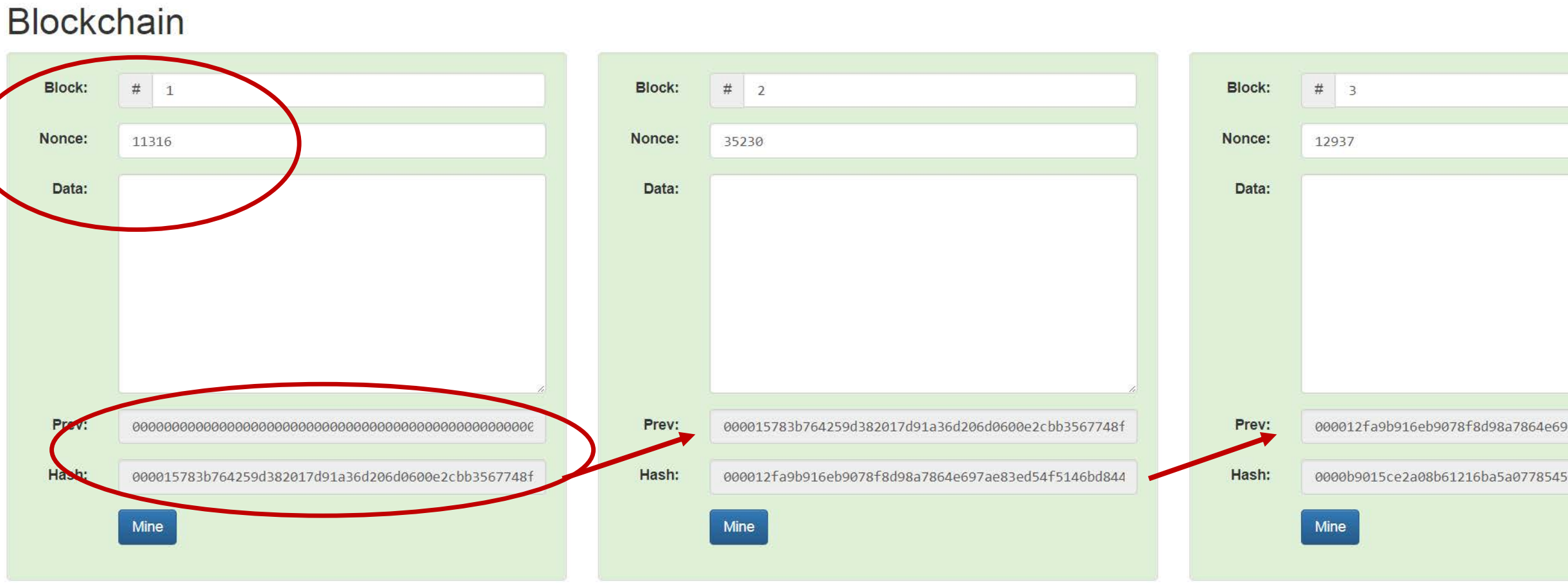
> The blockchain network is a **peer-to-peer network** of independent nodes communicating together by message broadcasting.

No central nodes …. All the nodes are not connected to each other

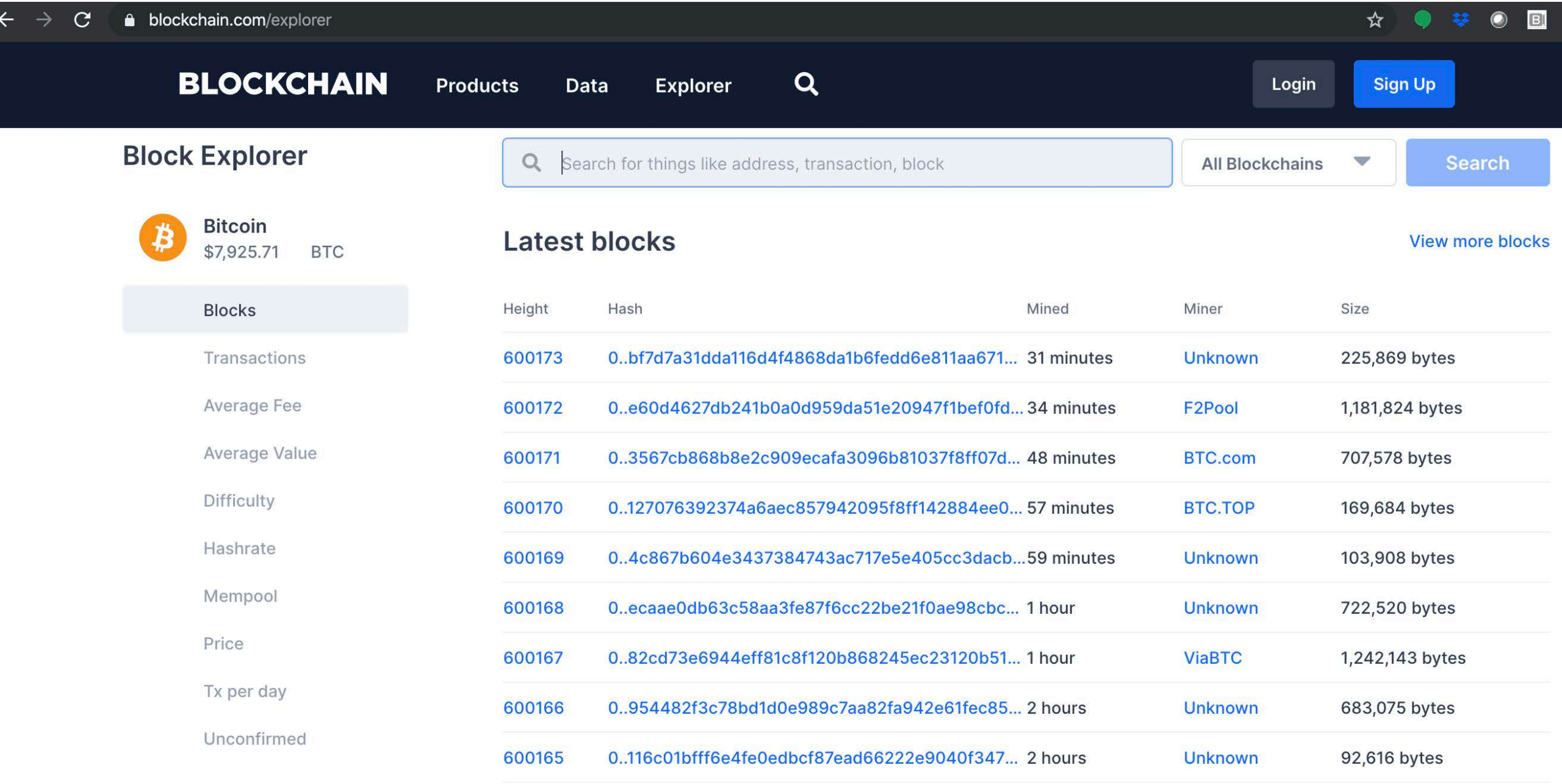
All nodes could be miners



Blockchain Demo: Interactive: https://anders.com/blockchain/blockchain.html



Block 1: Genesis Block
req: start with "0000"


blockchain.com/explorer
BLOCKCHAIN
Products
Data
Explorer
Login
Sign Up
Block Explorer
Search for things like address, transaction, block
All Blockchains
Search
Bitcoin
$7,925.71 BTC
Blocks
Transactions
Average Fee
Average Value
Difficulty
Hashrate
Mempool
Price
Tx per day
Unconfirmed
Latest blocks
View more blocks
Height Hash Mined Miner Size
600173 0..bf7d7a31dda116d4f4868da1b6fedd6e811aa671... 31 minutes Unknown 225,869 bytes
600172 0..e60d4627db241b0a0d959da51e20947f1bef0fd... 34 minutes F2Pool 1,181,824 bytes
600171 0..3567cb868b8e2c909ecafa3096b81037f8ff07d... 48 minutes BTC.com 707,578 bytes
600170 0..127076392374a6aec857942095f8ff142884ee0... 57 minutes BTC.TOP 169,684 bytes
600169 0..4c867b604e3437384743ac717e5e405cc3dacb... 59 minutes Unknown 103,908 bytes
600168 0..ecaae0db63c58aa3fe87f6cc22be21f0ae98cbc... 1 hour Unknown 722,520 bytes
600167 0..82cd73e6944eff81c8f120b868245ec23120b51... 1 hour ViaBTC 1,242,143 bytes
600166 0..954482f3c78bd1d0e989c7aa82fa942e61fec85... 2 hours Unknown 683,075 bytes
600165 0..116c01bfff6e4fe0edbcf87ead66222e9040f347... 2 hours Unknown 92,616 bytes

Block #600173

Summary	
Number Of Transactions	559
Output Total	1,653.24479113 BTC
Estimated Transaction Volume	97.49559812 BTC
Transaction Fees	0.04989164 BTC
Height	600173 (Main Chain)
Timestamp	2019-10-20 06:10:58
Received Time	2019-10-20 06:10:58
Relayed By	Unknown
Difficulty	13,008,091,666,971.9
Bits	387294044
Size	225.869 kB
Weight	733.58 kWU
Version	0x20C00000
Nonce	3013413449
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000000bf7d7a31dda116d4f4868da1b6fedd6e811aa67190dae
Previous Block	00000000000000000000e60d4627db241b0a0d959da51e20947f1bef0fdf9b09c
Next Block(s)	00000000000000000000227c73e69d556cfe5ff9ce2e12e7508de61ae4b6fd6d1
Merkle Root	3e86f6f02d8acd849d124621a65115f19a6c2c53968018975740af7f0ec95067

Transactions

387497b293135c37731c3f161fb03d004f1a0eadd5eced51dfa393cfe12b2703			2019-10-20 06:10:58
No Inputs (Newly Generated Coins)	→	1MvYASoHjqynMaMnP7SBmenyEWiLsTqoU6 Unable to decode output address Unable to decode output address	12.54989164 BTC 0 BTC 0 BTC 12.54989164 BTC
9d4fbd8562fe9a6f0536670c6bacadb3e611c8e613a1cfad63f5b58efef7f239			2019-10-20 06:08:31
16hcPw3TGU8Mj9at5KLLnuTzB9aDYjvrrq	→	1AMVx8nbAPgebTTVfgJo9hDbccQjtsXVMN 1HVAVGkGB5iT5zVTgmtuazkpCPfrceXj73	19.9985 BTC 0.9995 BTC 20.998 BTC
3addaa5cf63dc4adf7cccad0739fe663ca061e4f2d2ae59e4471ac108269faa0			2019-10-20 06:08:31
197zMZHUDjUitFgvuJ7afUvks2En4ZDSwD	→	1AMVx8nbAPgebTTVfgJo9hDbccQjtsXVMN 16hcPw3TGU8Mj9at5KLLnuTzB9aDYjvrrq	19.9985 BTC 80 BTC 99.9985 BTC
5c98e5349945cf49f1fecd4524ec863e103e88eefe0ba0127c21c296633a27d4			2019-10-20 06:08:31
1AcjX7tW78dbMBiqpjbFLGEXA1y9SngrLe	→	1AMVx8nbAPgebTTVfgJo9hDbccQjtsXVMN 1DmyPKtANnsjNYVkVSK7PGFCPxWdvqMoF1	19.9985 BTC 39.88357118 BTC 59.88207118 BTC
ec835256017a91b63e3e8d13bbf4db0613b7ab1a48328e37d2a0f8b0cb01a970			2019-10-20 06:09:07
3M92sq9ssFaNbEwF47uteVKJsbw125juS7	→	3M92sq9ssFaNbEwF47uteVKJsbw125juS7 3EGfTnVgzJqFvFY47xTAhiiVyRR36DjDz1	2.37604987 BTC 1.002 BTC

What is Ethereum?

Ethereum is a blockchain that allows you to run programs in its trusted environment. This contrasts with the Bitcoin blockchain, which only allows you to manage cryptocurrency.

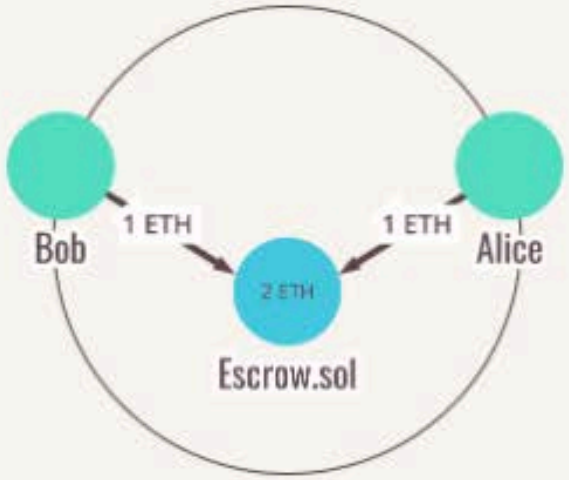
To this end, Ethereum has a virtual machine, called the Ethereum Virtual Machine (EVM). The EVM allows code to be verified and executed on the blockchain, providing guarantees it will be run the same way on everyone's machine. This code is contained in "smart contracts" (more on these below).

Beyond just tracking account balances, Ethereum maintains the state of the EVM on the blockchain. All nodes process smart contracts to verify the integrity of the contracts and their outputs.

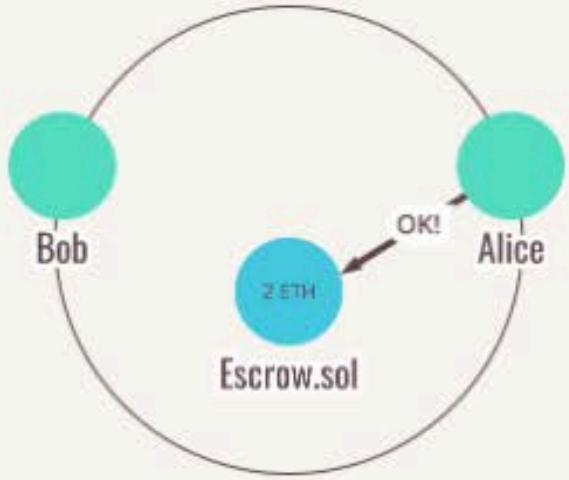
What is a smart contract?

A smart contract is code that runs on the EVM. Smart contracts can accept and store ether, data, or a combination of both. Then, using the logic programmed into the contract, it can distribute that ether to other accounts or even other smart contracts.

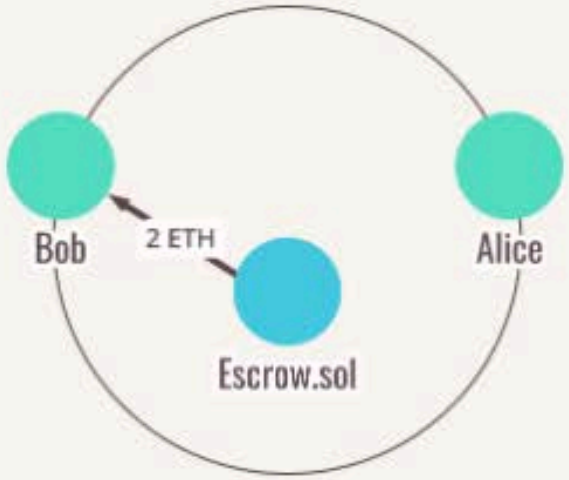
Here's a smart contract example with Bob and Alice again. Alice wants to hire Bob to build her a patio, and they are using an escrow contract (a place to store money until a condition is fulfilled) to store their ether before the final transaction.



1. Alice agrees to store her payment for the patio within the escrow contract, and Bob agrees to deposit an equal amount

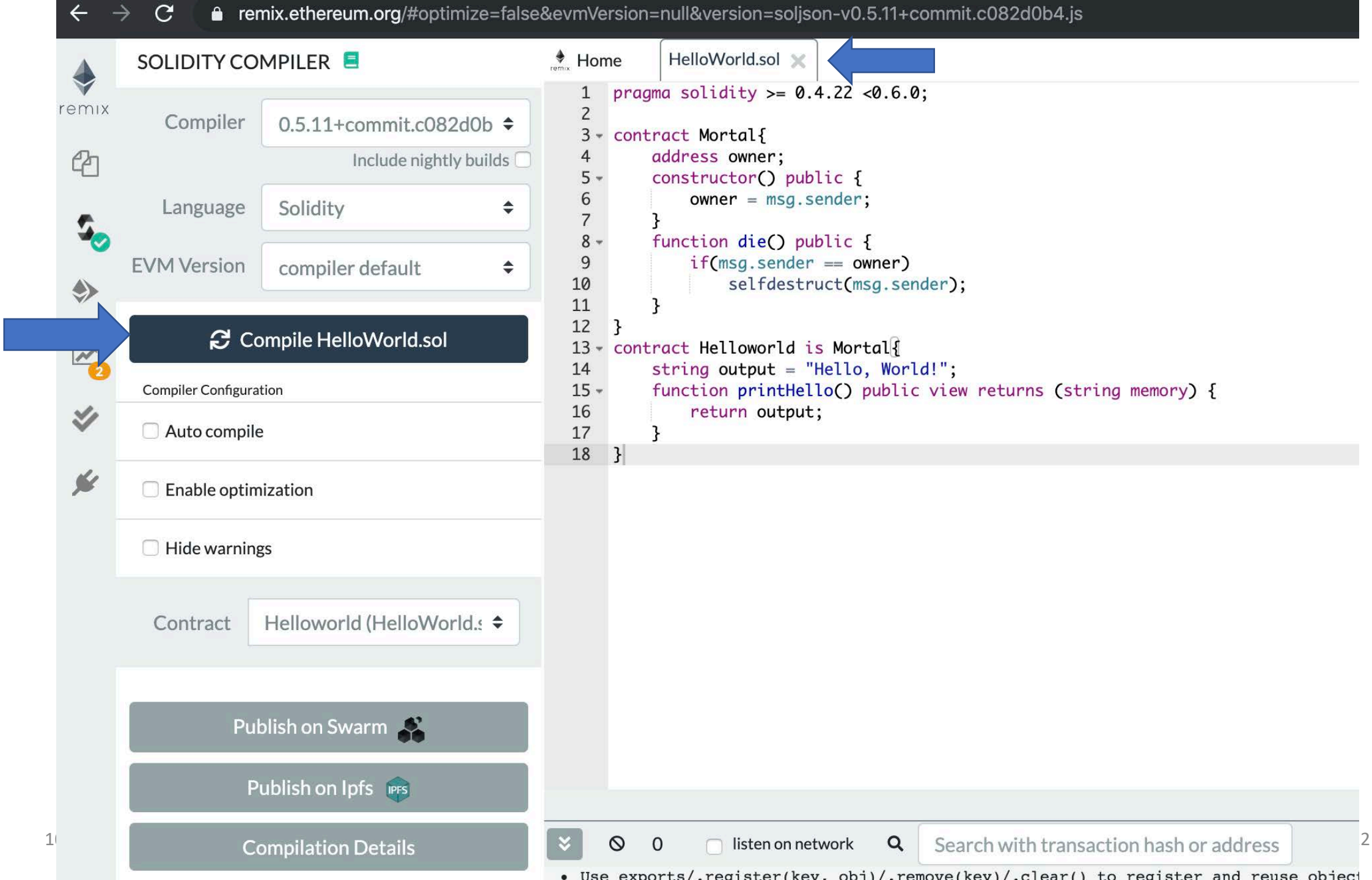


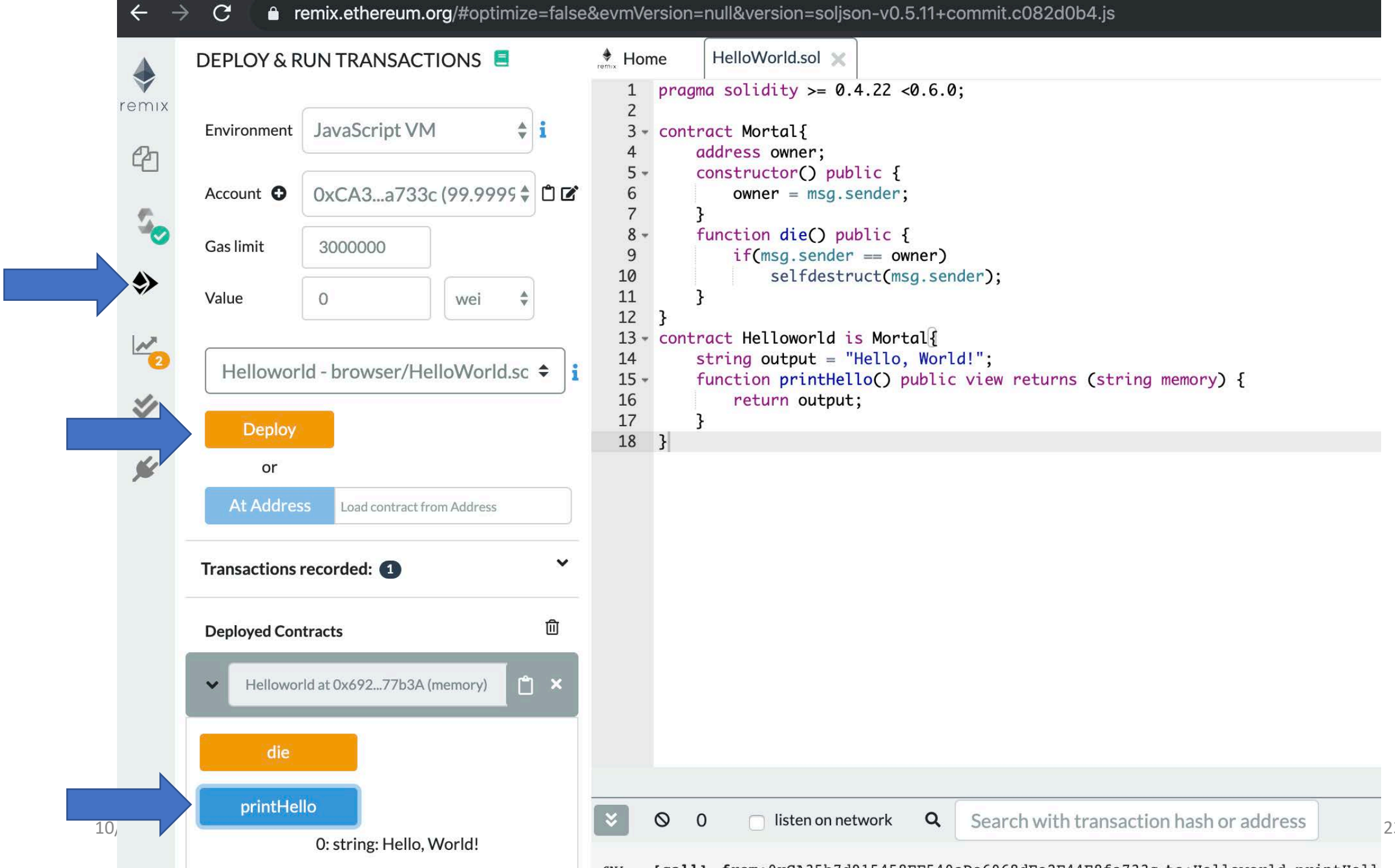
2. Bob completes the patio project and Alice gives the smart contract permission to release the funds



3. Bob receives Alice's payment along with his collateral

(Provisions could be written into the contract code releasing Bob's collateral to Alice if Bob were to fail to build the patio or if he were to perform a poor job.)


remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.5.11+commit.c082d0b4.js
SOLIDITY COMPILER
remix
Compiler
0.5.11+commit.c082d0b
Include nightly builds
Language
Solidity
EVM Version
compiler default
Compile HelloWorld.sol
Compiler Configuration
Auto compile
Enable optimization
Hide warnings
Contract
Helloworld (HelloWorld.s
Publish on Swarm
Publish on Ipfs
IPFS
Compilation Details
Home
HelloWorld.sol
1 pragma solidity >= 0.4.22 <0.6.0;
2
3 contract Mortal{
4 address owner;
5 constructor() public {
6 owner = msg.sender;
7 }
8 function die() public {
9 if(msg.sender == owner)
10 selfdestruct(msg.sender);
11 }
12 }
13 contract Helloworld is Mortal{
14 string output = "Hello, World!";
15 function printHello() public view returns (string memory) {
16 return output;
17 }
18 }
0
listen on network
Search with transaction hash or address


remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.5.11+commit.c082d0b4.js
DEPLOY & RUN TRANSACTIONS
Environment
JavaScript VM
Account
0xCA3...a733c (99.9999
Gas limit
3000000
Value
0
wei
Helloworld - browser/HelloWorld.sc
Deploy
or
At Address
Load contract from Address
Transactions recorded: 1
Deployed Contracts
Helloworld at 0x692...77b3A (memory)
die
printHello
0: string: Hello, World!
Home
HelloWorld.sol
1 pragma solidity >= 0.4.22 <0.6.0;
2
3 contract Mortal{
4 address owner;
5 constructor() public {
6 owner = msg.sender;
7 }
8 function die() public {
9 if(msg.sender == owner)
10 selfdestruct(msg.sender);
11 }
12 }
13 contract Helloworld is Mortal{
14 string output = "Hello, World!";
15 function printHello() public view returns (string memory) {
16 return output;
17 }
18 }
0
listen on network
Search with transaction hash or address

References

- https://bitcoin.org/bitcoin.pdf – Original Paper by Satoshi Nakamoto, 10/28
- www.Ethereum.org – Created a Virtual Machine for any Token
- www.blockexplorer.com – Bitcoin Block Explorer
- Byzantine Generals Problem – Lamport, Shostak, Pease, 1982
- https://gavwood.com/paper.pdf - Ethereum paper by Gavin Wood
- Ethereum White Paper and Smart Contracts – by Vitalik Buterin in Nov 2013
- https://solidity.readthedocs.io/en/v0.5.3/introduction-to-smart-contracts.html – Solidity Smart Contracts
- https://remix.ethereum.org Remix IDE for Smart Contracts in Ethereum
- www.hyperledger.org – The Linux Foundation Project – Hyperledger
- https://anders.com/blockchain/ - Blockchain Demo
- https://www.ibm.com/blockchain - IBM Blockchain
- https://aws.amazon.com/blockchain/ - Amazon AWS Blockchain
- https://azure.microsoft.com/en-us/solutions/blockchain/ - MS Azure Blockchain

Questions? Comments? Feedback?

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

- Debasis Bhattacharya, JD, DBA
- maui.hawaii.edu/cybersecurity
- University of Hawaii Maui College

- ATE 2019 – Demonstration Session

AMERICAN ASSOCIATION OF COMMUNITY COLLEGES
100 since 1920
A CENTURY OF SUCCESS