Introduction to Bitcoins, Blockchains, and Smart Contracts

Debasis Bhattacharya (debasisb@hawaii.edu, www.mau.hawaii.edu/cybersecurity)
University of Hawaii Maui College, July 2020
Presentation Overview

This presentation introduces bitcoins, blockchains, and smart contracts programmed with Ethereum Blockchains and the Solidity programming language. Cryptocurrencies such as bitcoins use blockchains and smart contracts to enforce transactions. Solidity is the programming language that is used to create smart contracts that are stored on the blockchain.
A **smart contract** is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.

[Smart contract - Wikipedia](https://en.wikipedia.org/wiki/Smart_contract)

---

**People also ask**

Who is using smart contracts?
Currencies - Online Transactions

• Physical cash
  • Non-traceable (well, mostly!)
  • Secure (mostly)
  • Low inflation

• Fiat Currency – legal tender whose value is backed by a government
  • Note that since 1971, the US$ has no backing with gold!
  • Cryptocurrencies are not fiat currencies!

• Physical currencies can’t be used online directly
  ➢ Electronic credit or debit transactions
    ◆ Bank sees all transactions
    ◆ Merchants can track/profile customers
    ◆ Cryptocurrencies are not associated with any bank or regulatory agency!
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 ~18.43 million (July 9, 2020)
• Total number of BitCoins generated cannot exceed 21 million.
  • Around 2.6 million left to be mined! Mining will end in the year 2140...

• Average price of a Bitcoin:
  • $9,220.41 on July 9, 2020
  • $10,635.28 on July 18, 2019
  • $10,360.45 on July 1, 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!)
Bitcoin Transactions

Public key 0xc7b2f68...

Public key 0xa8fc93875a972ea

Signature 0xa87g14632d452cd
Case Study – Track Alice Tx to Bob

Buying a Cup of Coffee
Alice, introduced in the previous chapter, is a new user who has just acquired her first bitcoin. In [getting_first_bitcoin], Alice met with her friend Joe to exchange some cash for bitcoin. The transaction created by Joe funded Alice’s wallet with 0.10 BTC. Now Alice will make her first retail transaction, buying a cup of coffee at Bob’s coffee shop in Palo Alto, California.

Bob’s Cafe recently started accepting bitcoin payments by adding a bitcoin option to its point-of-sale system. The prices at Bob’s Cafe are listed in the local currency (US dollars), but at the register, customers have the option of paying in either dollars or bitcoin. Alice places her order for a cup of coffee and Bob enters it into the register, as he does for all transactions. The point-of-sale system automatically converts the total price from US dollars to bitcoin at the prevailing market rate and displays the price in both currencies:

Total: $1.50 USD 0.015 BTC

Bob says, "That’s one-dollar-fifty, or fifteen millibits."
What Do Bitcoins “Look” Like?

Public Key (“Address”)
34 characters starting with 1 or 3
Represents a possible destination for payment

Private Key
51 characters starting with 5
Required to transfer value from the address
Figure 9. Alice’s transaction included in block #277316
<table>
<thead>
<tr>
<th>Block Number</th>
<th>277316</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>Confirmations</td>
<td>361,239</td>
</tr>
<tr>
<td>Timestamp</td>
<td>2013-12-27 12:11</td>
</tr>
<tr>
<td>Height</td>
<td>277316</td>
</tr>
<tr>
<td>Miner</td>
<td>Unknown</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>419</td>
</tr>
<tr>
<td>Difficulty</td>
<td>1,180,923,195.26</td>
</tr>
<tr>
<td>Merkle root</td>
<td>0x56508c2e57073e3f54f66eb2952c3237351f31577ffe0550b253ebcc3f2e</td>
</tr>
<tr>
<td>Version</td>
<td>0x2</td>
</tr>
<tr>
<td>Bits</td>
<td>419,668,748</td>
</tr>
<tr>
<td>Weight</td>
<td>874,716 WU</td>
</tr>
<tr>
<td>Size</td>
<td>218,629 bytes</td>
</tr>
<tr>
<td>Nonce</td>
<td>924,591,752</td>
</tr>
<tr>
<td>Transaction Volume</td>
<td>10296.98627636 BTC</td>
</tr>
<tr>
<td>Block Reward</td>
<td>25.00000000 BTC</td>
</tr>
<tr>
<td>Fee Reward</td>
<td>0.00000008 BTC</td>
</tr>
</tbody>
</table>
Bitcoin - Activities

• Blockchain Explorer of Bitcoins etc. - https://www.blockchain.com/explorer
• Coin Market of Various Cryptos- https://coinmarketcap.com/all/views/all/
• Coinbase Web Site Demo - https://www.coinbase.com/
• Stable Coin - USD Coin from Coinbase - https://www.coinbase.com/usdc
Bitcoin - Labs

• Beginner Lab – Where is Bitcoin?
  • https://github.com/UHMC/module-1-lab-beginner

• Intermediate Lab – Visualizing Bitcoin
  • https://github.com/UHMC/module-1-lab-intermediate
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
Distributed Consensus

At any given time:

- All nodes have a sequence of **blocks of transactions** they’ve reached consensus on
- Each node has a set of outstanding transactions it’s heard about

(Not all nodes have all the information at the same time (Latency))

Why consensus is hard

Nodes may crash
Nodes may be malicious

Network is imperfect
- Not all pairs of nodes connected
- Faults in network
- Latency

No notion of global time
How Blockchain Works
Here are five basic principles underlying the technology.

1. Distributed Database
   • Each party on a blockchain has access to the entire database and its complete history.
   • No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

2. Peer-to-Peer Transmission
   • Communication occurs directly between peers instead of through a central node.
   • Each node stores and forwards information to all other nodes.
3. Transparency with Pseudonymity
   • Every transaction and its associated value are visible to anyone with access to the system. (public key)
   • Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. (private key)
   • Users can choose to remain anonymous or provide proof of their identity to others. (signatures) Transactions occur between blockchain addresses.

4. Irreversibility of Records
   • Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they’re linked to every transaction record that came before them (hence the term “chain”).
   • Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.
5. Computational Logic

• The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed.
• users can set up algorithms and rules that automatically trigger transactions between nodes.

• Data Security
  • Keys
  • Signatures
  • Hashing
• Redundancy
• Improved workflow
The hash output, or fingerprint, is actually what’s used as the “previous block” reference.

- One result of this is that there’s no way to switch out a block in the middle of the chain, because the hash value for the new block would be different, and the next’s block reference would no longer point to it.

- Even more importantly, a block cannot be solved before the previous block is solved. The previous block reference is part of the text that goes through the hash function, so any changes to it would require resolving.
solving a block involves trying to get the cryptographic hash of the block to be below a certain value, and you do that by trying different random numbers. Once solved, the hash output is like a fingerprint that uniquely identifies that block. If even a single character in the block is changed, the block’s hash would be completely different.

Specified by “Blockchain” creator

OK to proceed
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.)
pragma solidity >= 0.4.22 <0.6.6;

contract Mortal{
    address owner;
    constructor() public {
        owner = msg.sender;
    }
    function die() public {
        if(msg.sender == owner)
            selfdestruct(msg.sender);
    }
}

contract HelloWorld is Mortal{
    string output = "Hello, World!";
    function printHello() public view returns (string memory) {
        return output;
    }
}
Demo Instructions

• Start Remix Compiler at https://remix.Ethereum.org
• Environments
  • Solidity
• From Top Left Panel, File Explorers -> Create a New File – Helloworld.sol
  • Cut and paste code into browser and save
• Solidity Compiler
  • Click on Blue Button to Compile Helloworld.sol
• Click on Deploy and Run Transactions
  • Make sure Environment is set to JavaScript VM
  • Click on pink button Orange Button Deploy under Helloworld
  • A smart contract Helloworld will be deployed in memory
• Run Code
  • Click on down arrow at Helloworld smart contract at bottom of screen (at memory location in blockchain)
  • Access its functions – die and printHello
  • Click on printHello function to see output “0: string: Hello, World”
  • Click on die function to remove smart contract from blockchain
References

- [www.bitcoin.org](http://www.bitcoin.org) – Original cryptocurrency, over 10 years old!
- [www.blockchain.com/explorer](http://www.blockchain.com/explorer) - Great explorer to find all Bitcoins, Ethereum, BTC in Blockchain
- [https://gavwood.com/paper.pdf](https://gavwood.com/paper.pdf) - Ethereum paper by Gavin Wood
- [Ethereum White Paper and Smart Contracts](https://www.ethereum.org) – by Vitalik Buterin in Nov 2013
- [XRP Ledger Consensus Protocol](https://www.xrp.com) – Chase and MacBrough, 2018
- [www.hyperledger.org](http://www.hyperledger.org) – The Linux Foundation Project – Hyperledger
- [https://anders.com/blockchain/](https://anders.com/blockchain/) - Blockchain Demo
- [https://www.ibm.com/blockchain](https://www.ibm.com/blockchain) - IBM Blockchain
- [https://aws.amazon.com/blockchain/](https://aws.amazon.com/blockchain/) - Amazon AWS Blockchain
Questions, Comments, Feedback?
Debasis Bhattacharya (debasisb@hawaii.edu www.mauí.hawaii.edu/cybersecurity) University of Hawaii Maui College, July 2020