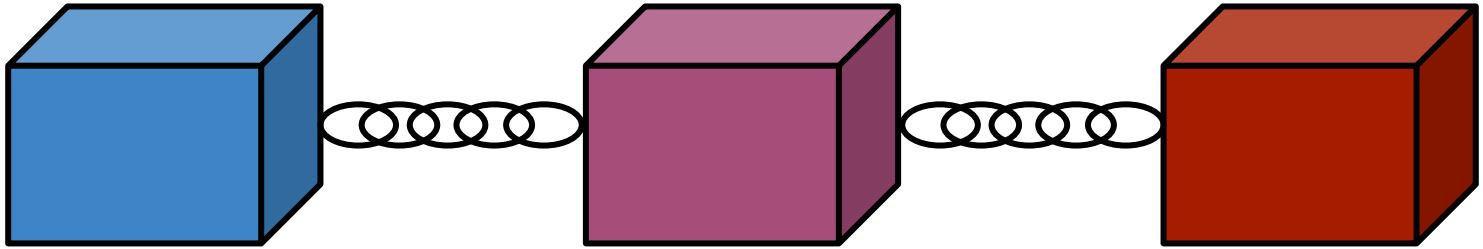
Introduction to Solidity and Vulnerabilities in Smart Contracts

Instructor : Chavhan Sujeet Yashavant

Part 1: Introduction to Blockchain and Smart Contracts

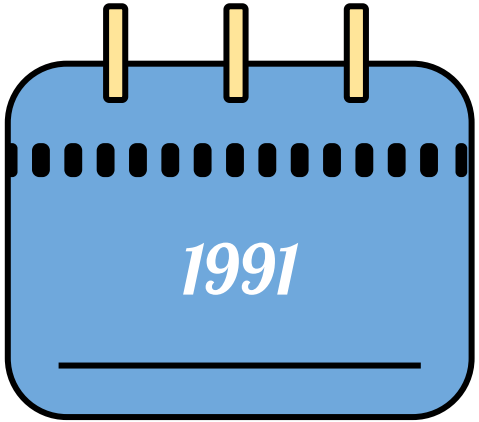
Blockchain: A Technology behind Bitcoin



Blockchain: Chain of blocks that contains information

Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

Digital Timestamps



Timestamp digital documents so that it is not possible to backdate them or tamper with them, like a notary

Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

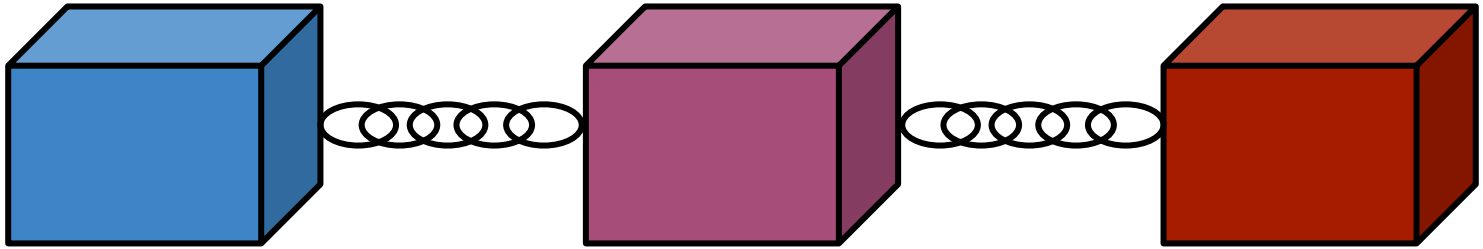
Bitcoin By “Satoshi Nakamoto”

Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

Invention of Bitcoin

- Person or a group of person pseudonym Satoshi Nakamoto published a whitepaper in 2008
- The paper describes an internet based currency which facilitates peer to peer transfer of money
- In 2009, bitcoin was launched

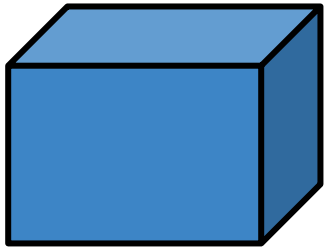
Distributed Ledger



- Open to anyone
- Nearly impossible to change recorded data

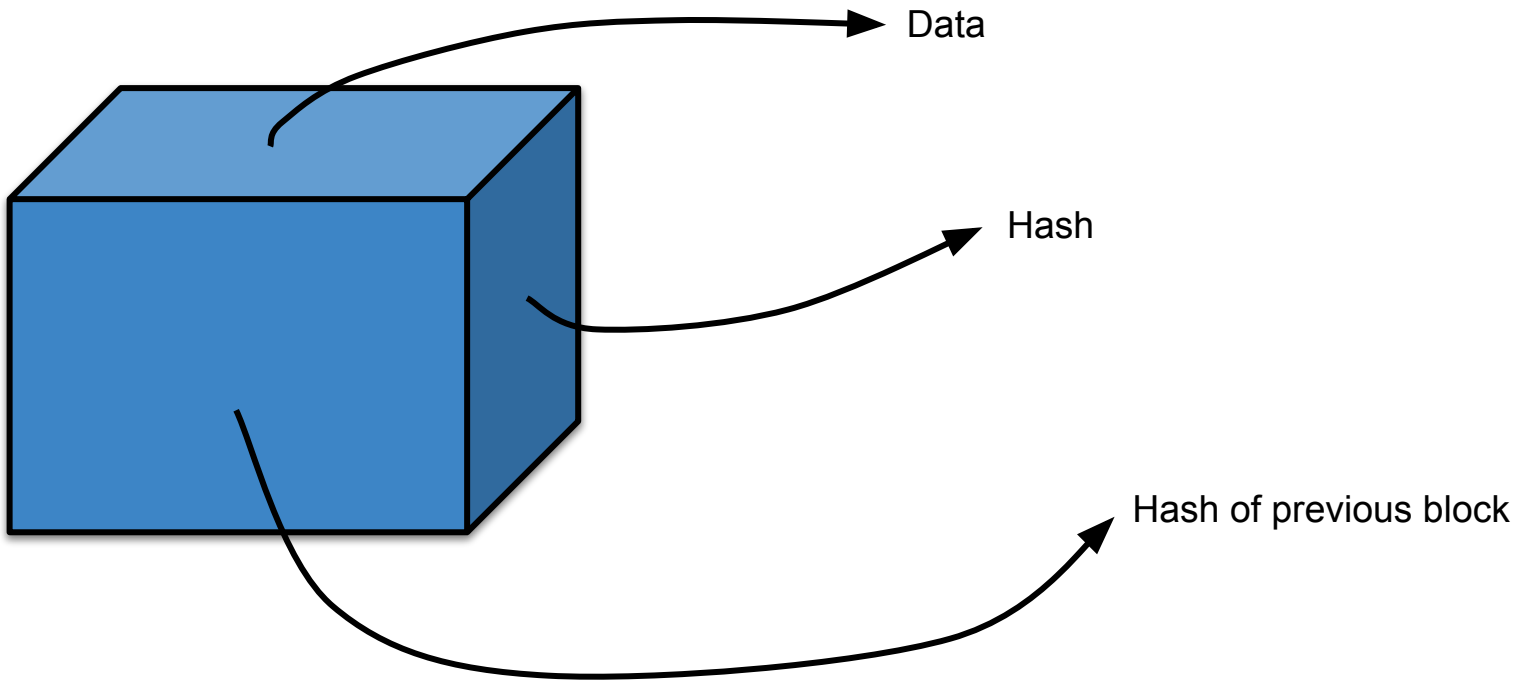
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

Block in a Blockchain



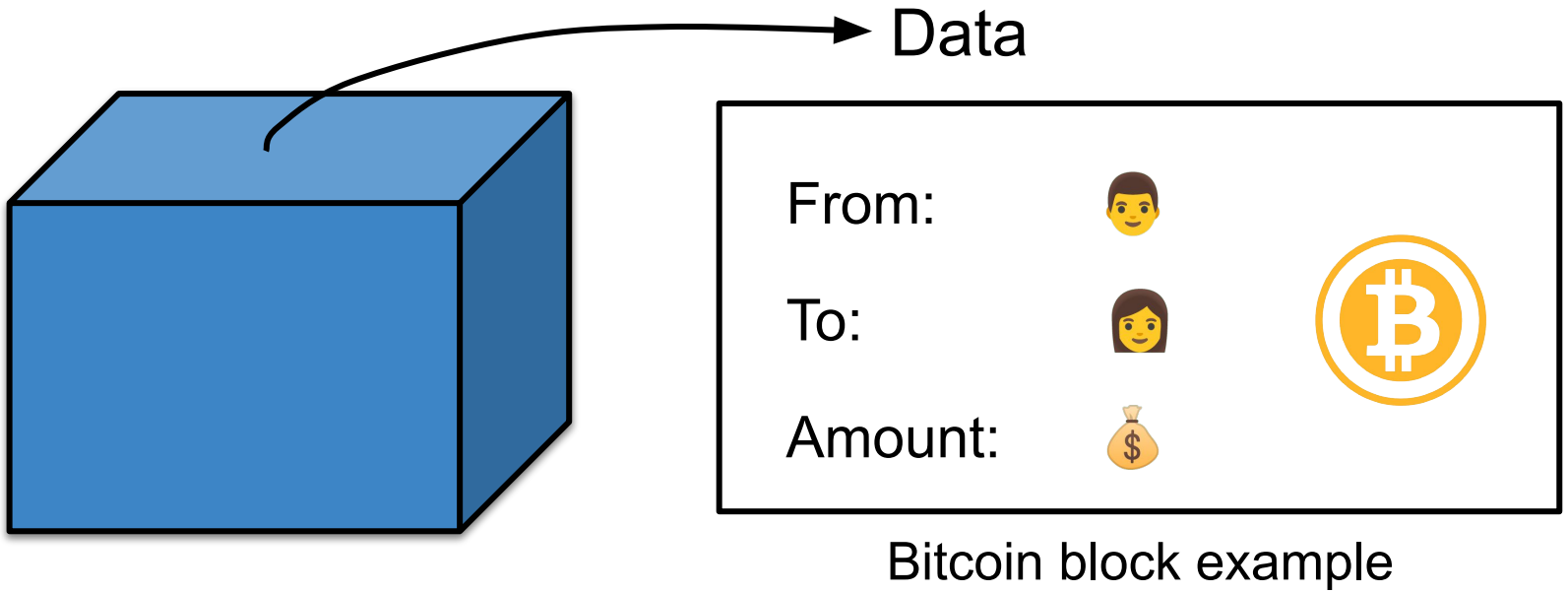
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

Block in a Blockchain



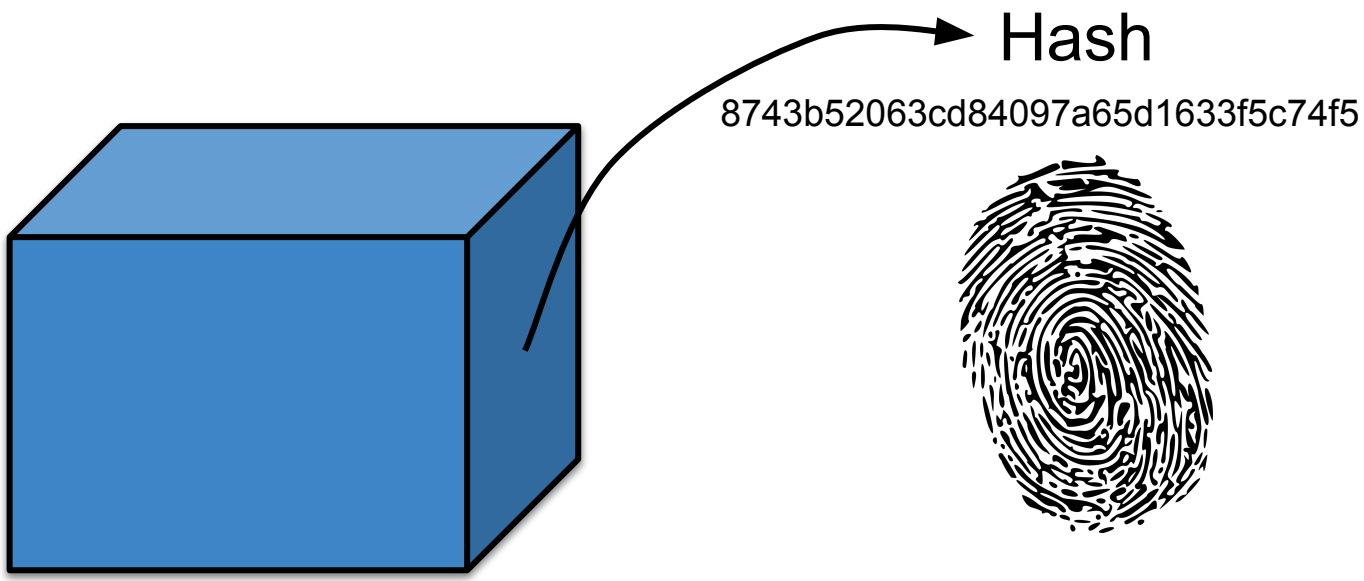
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

Block in a Blockchain



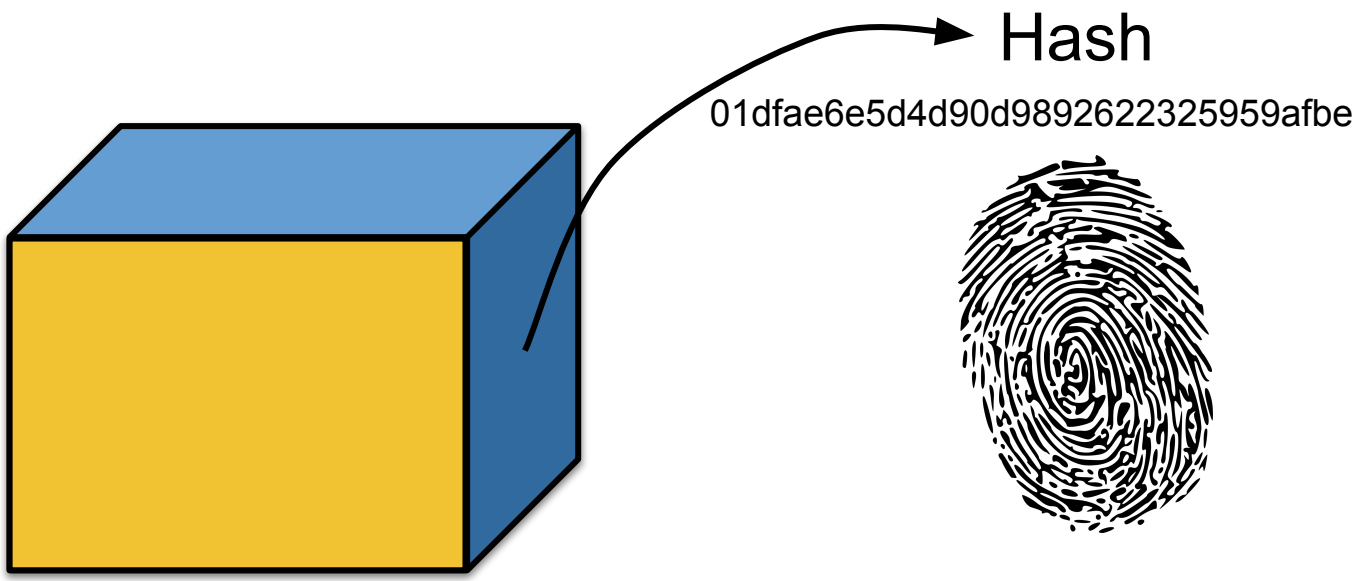
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work, https://freepngimg.com

Block in a Blockchain



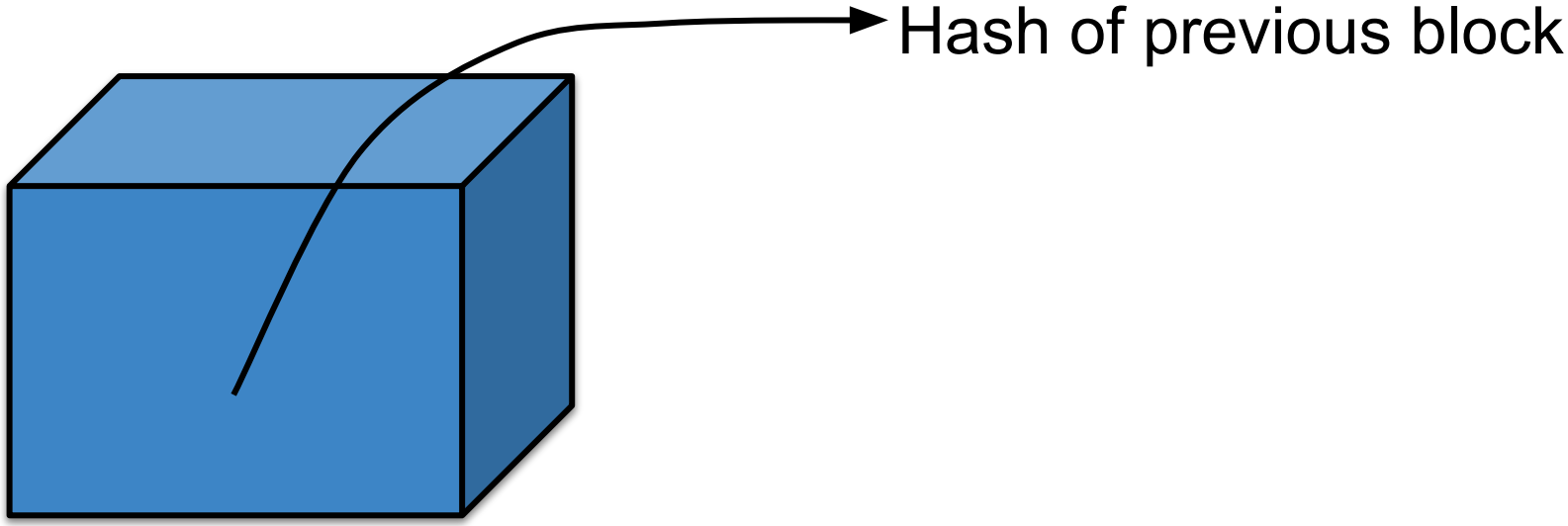
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work, https://www.pngall.com

Block in a Blockchain



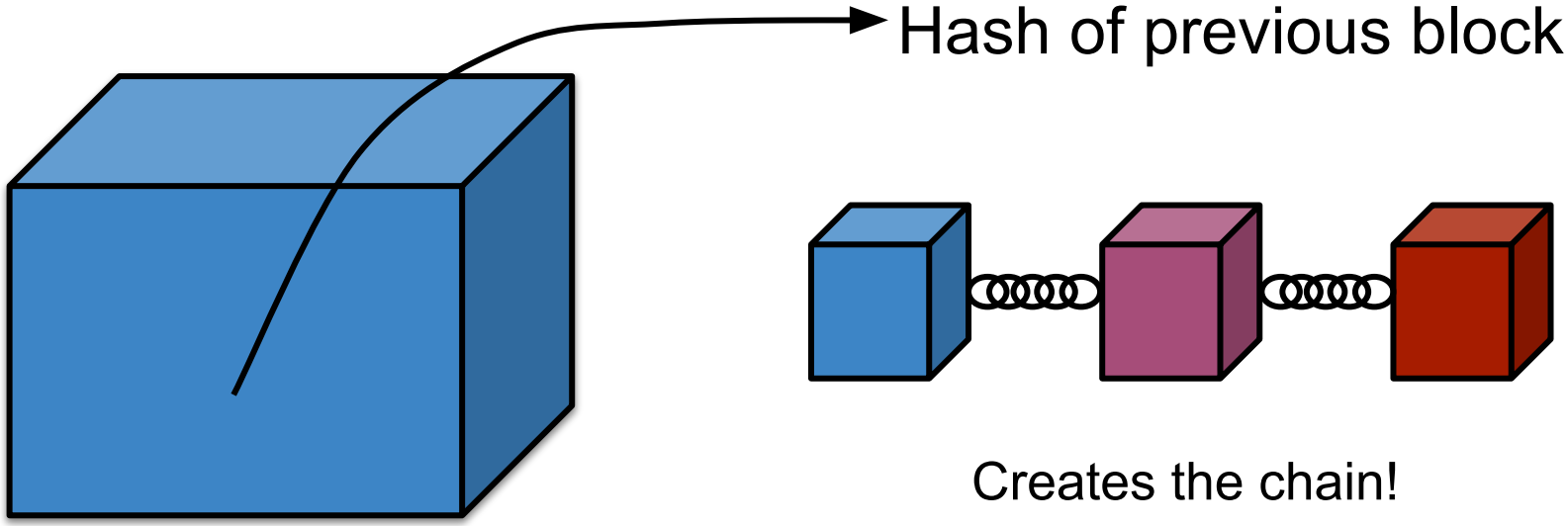
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work, https://www.pngall.com

Block in a Blockchain

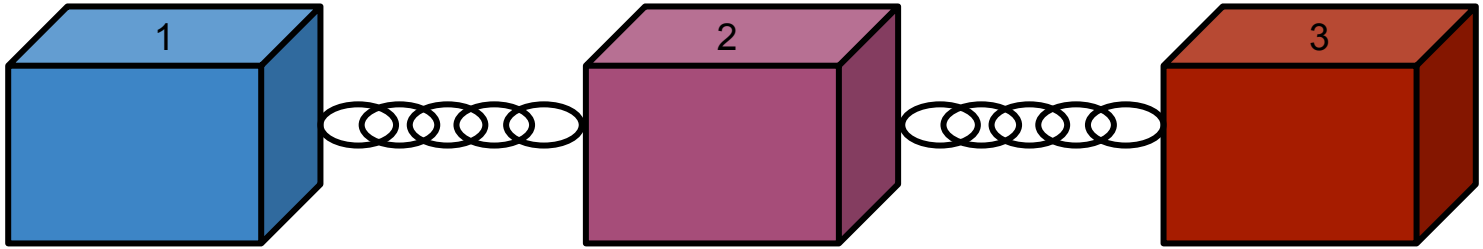


Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

Block in a Blockchain

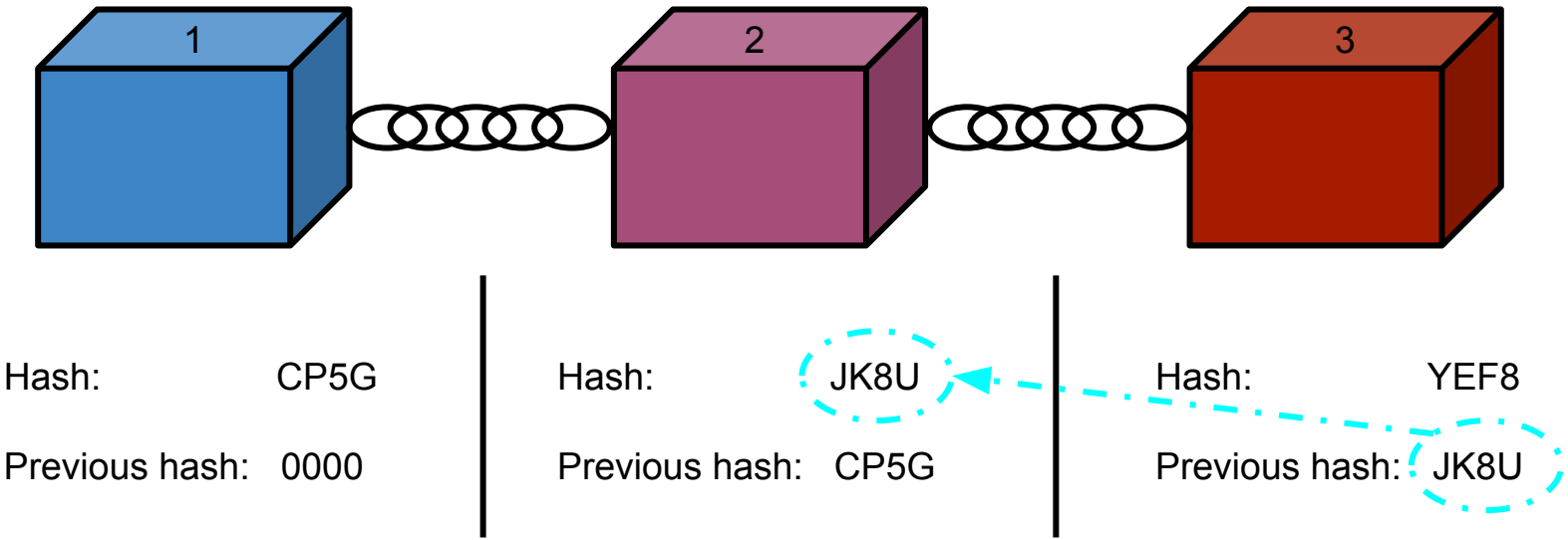


Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

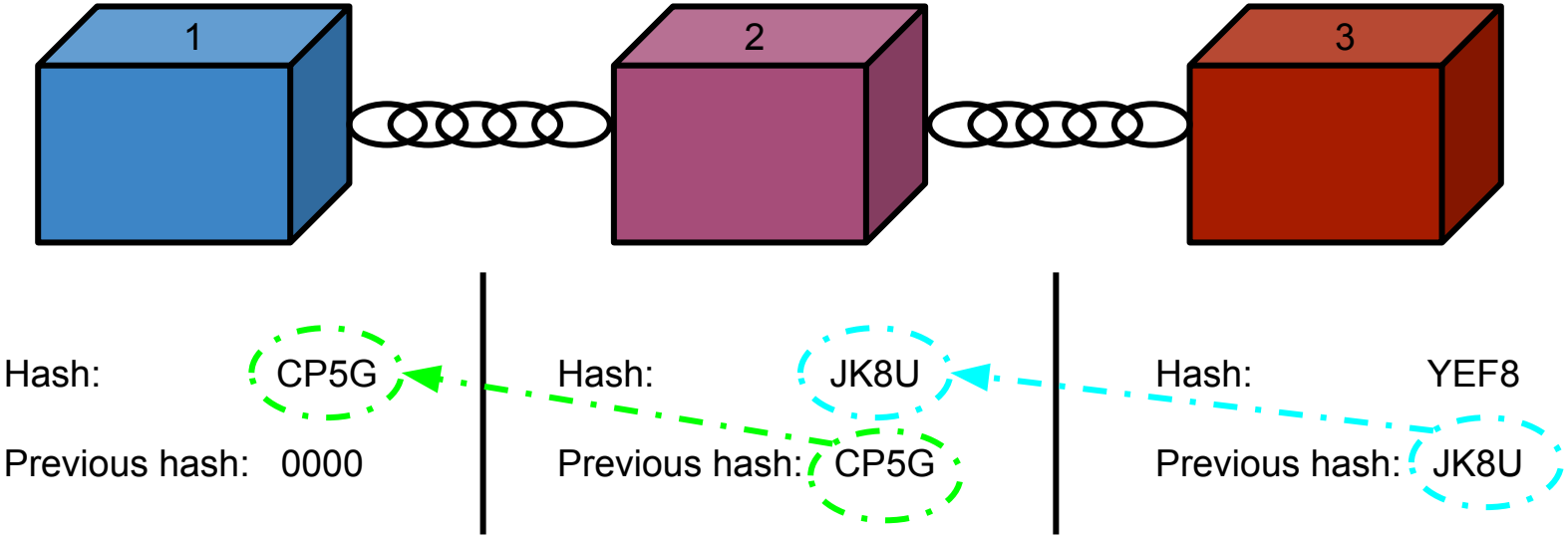


Hash:	CP5G	Hash:	JK8U	Hash:	YEF8
Previous hash:	0000	Previous hash:	CP5G	Previous hash:	JK8U

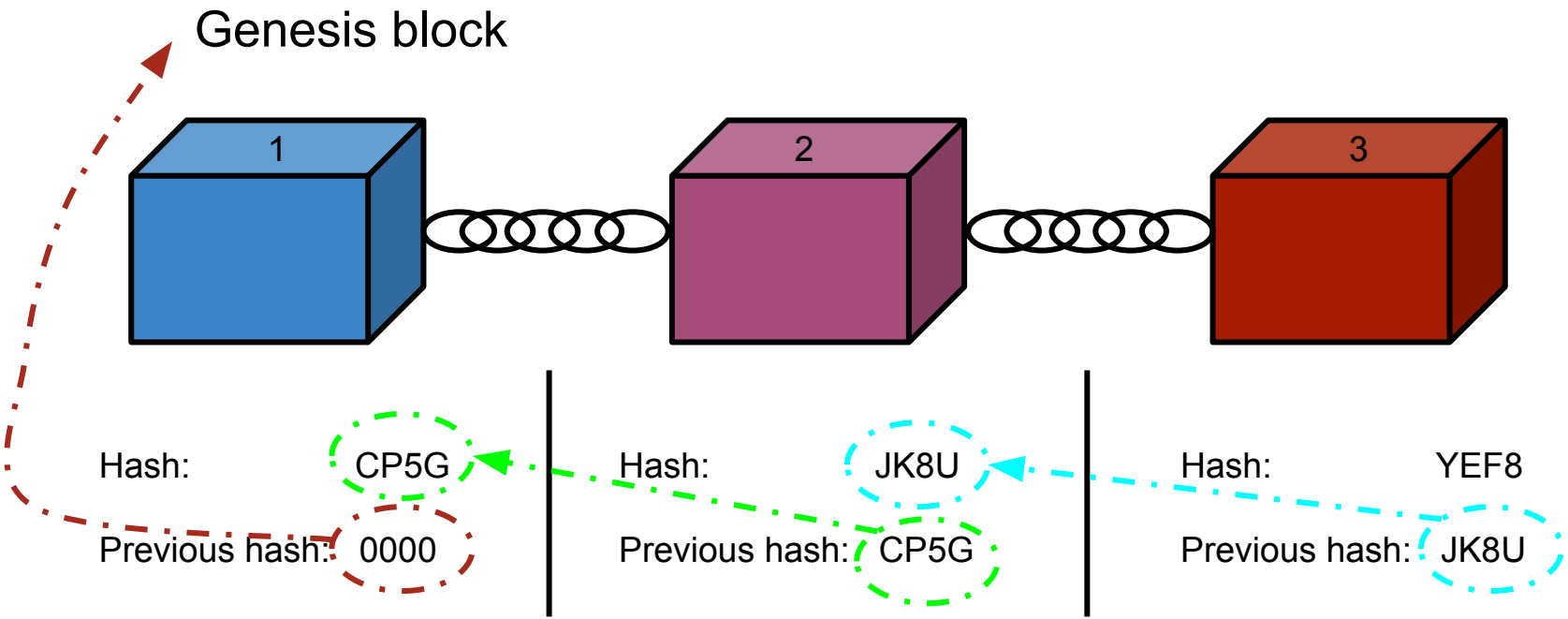
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work



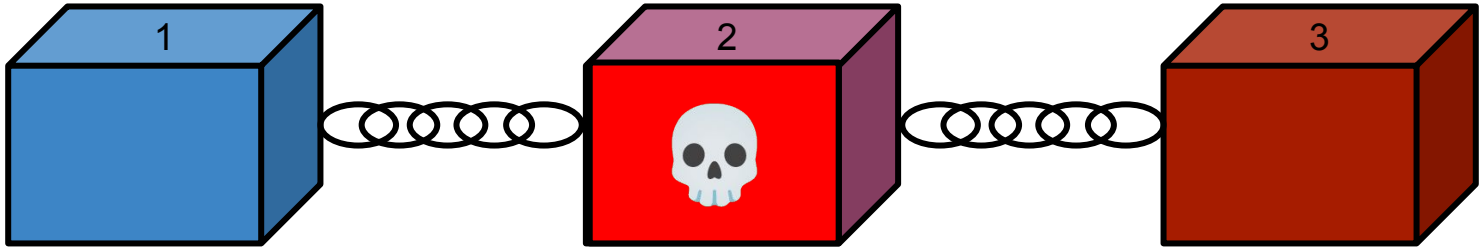
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work



Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

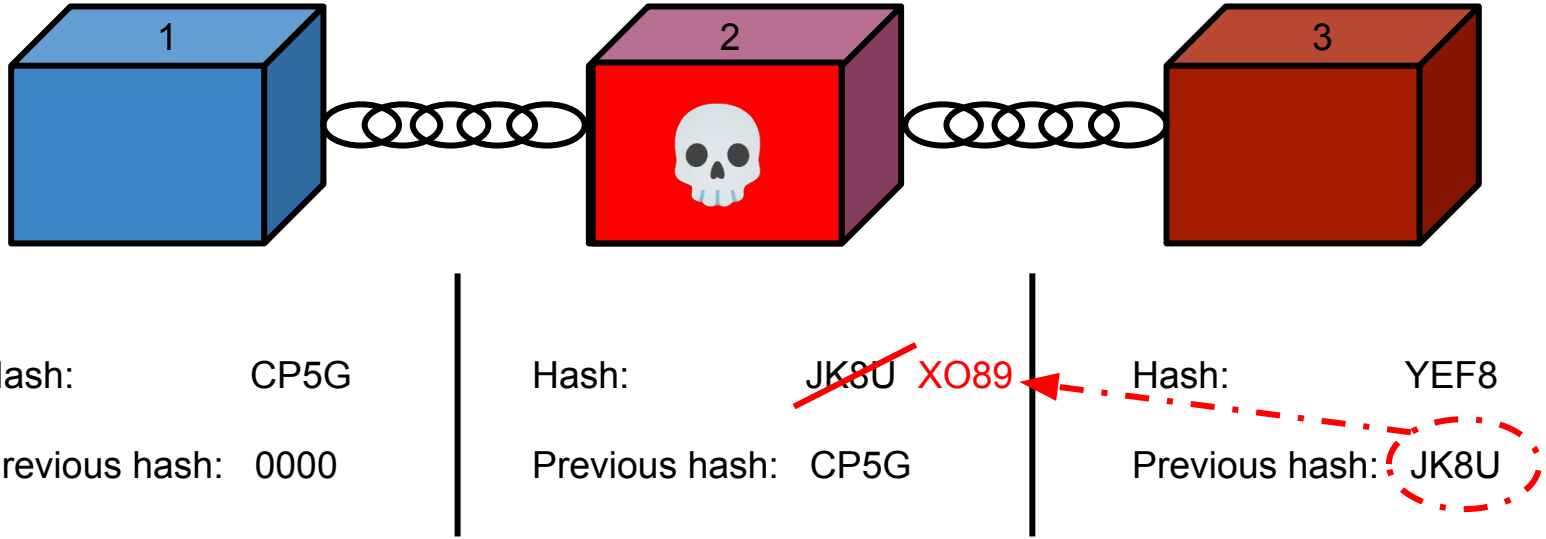


Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

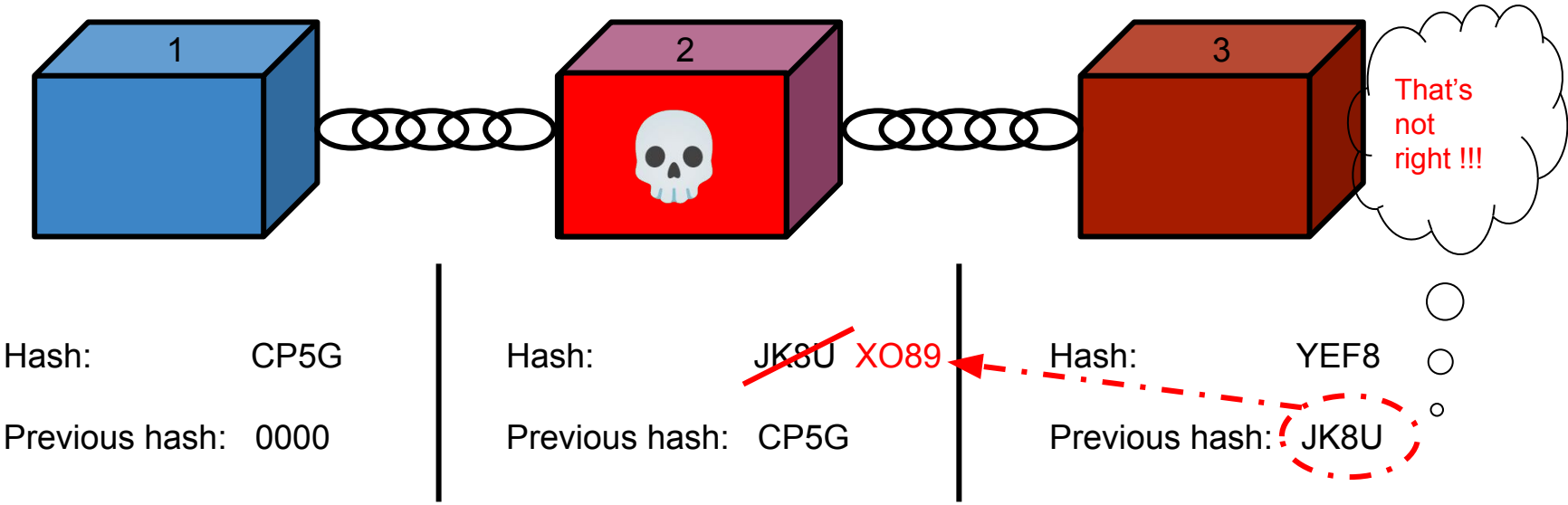


Hash:	CP5G	Hash:	JK8U	Hash:	YEF8
Previous hash:	0000	Previous hash:	CP5G	Previous hash:	JK8U

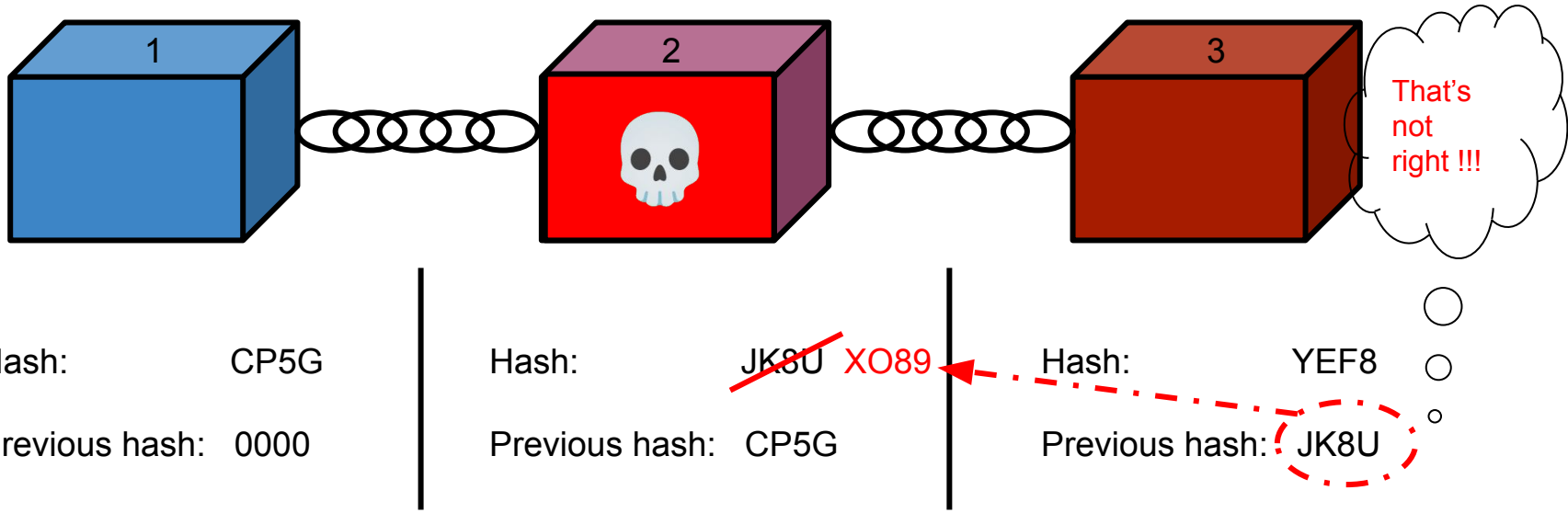
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work



Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

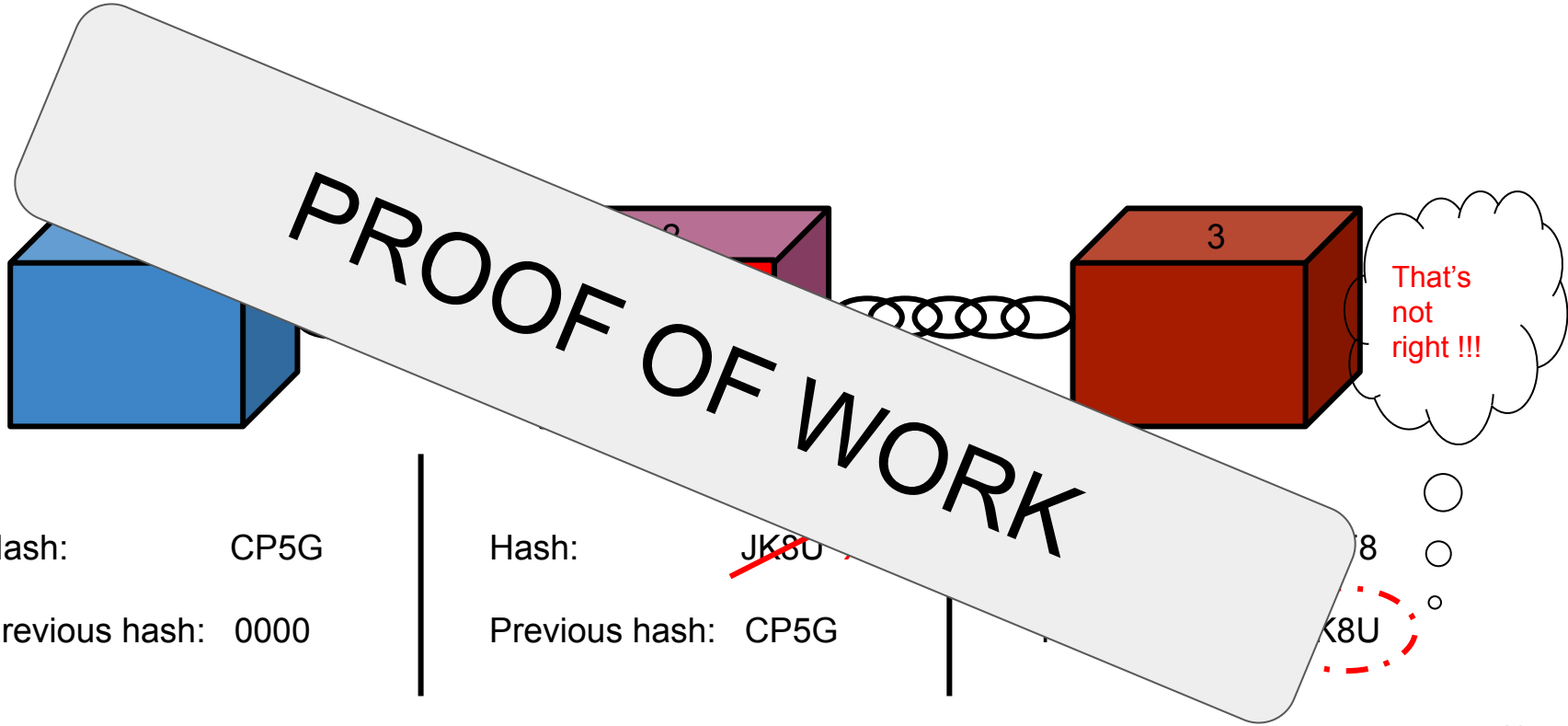


Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work



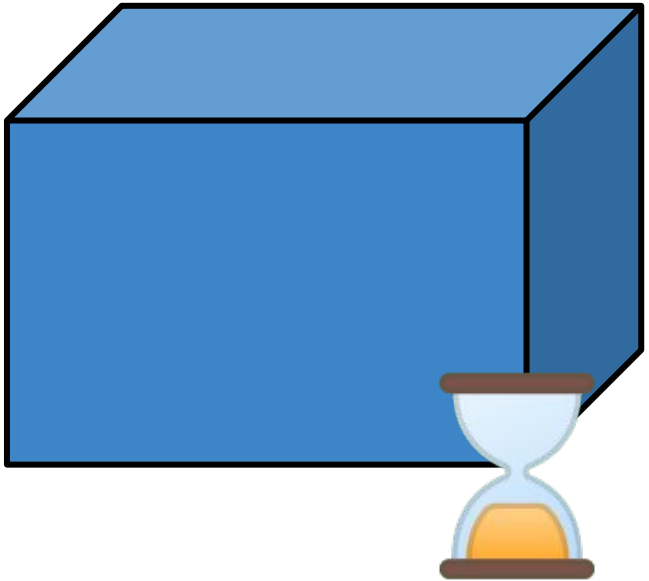
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

PROOF OF WORK



Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

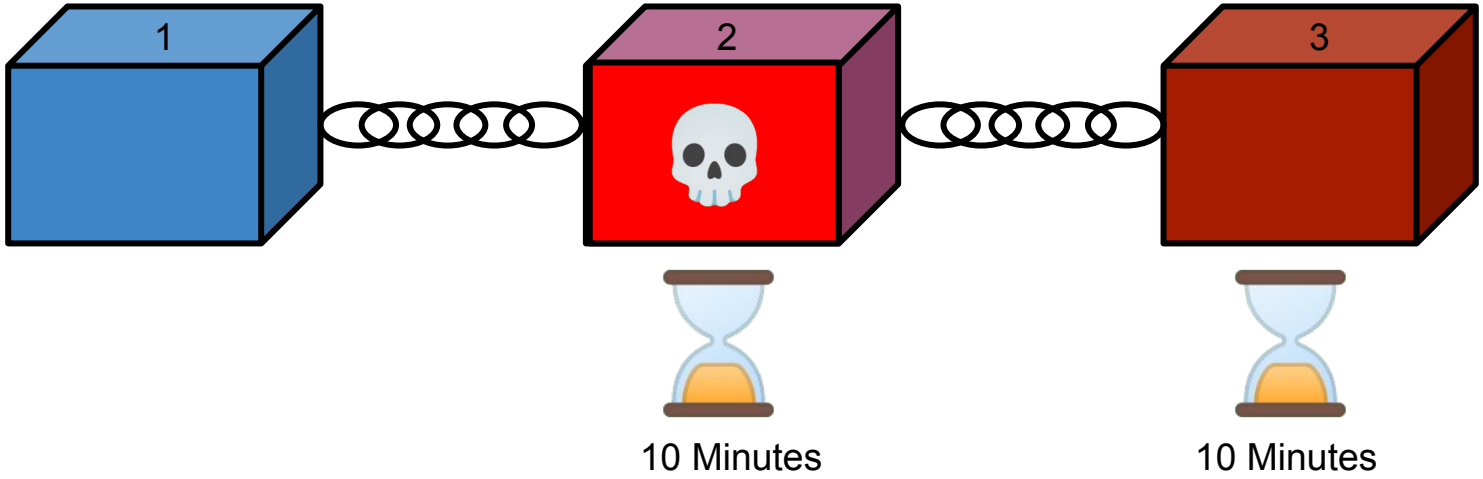
(proof of Work) PoW



Slow and Steady….

Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

PoW Time in Bitcoin



Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

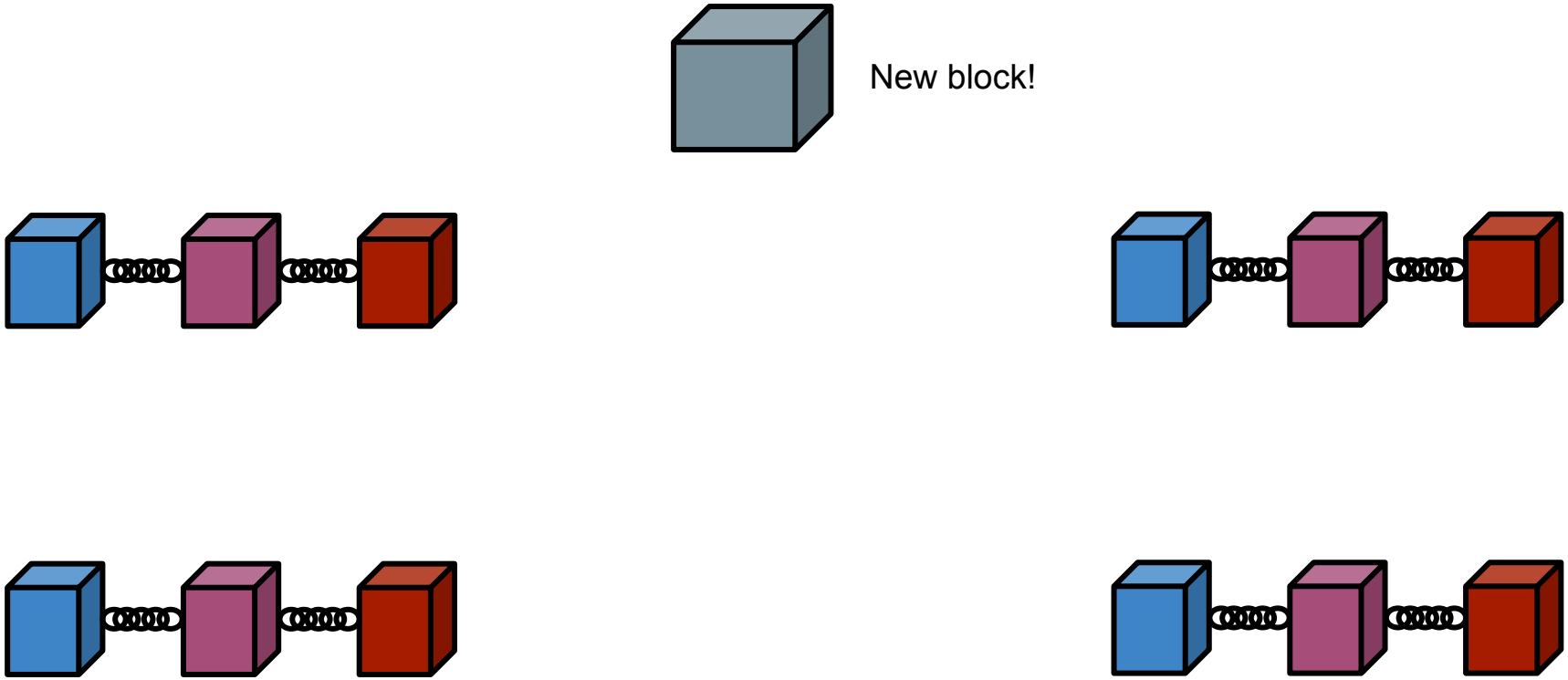
P2P Network

Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

P2P Network

Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

P2P Network

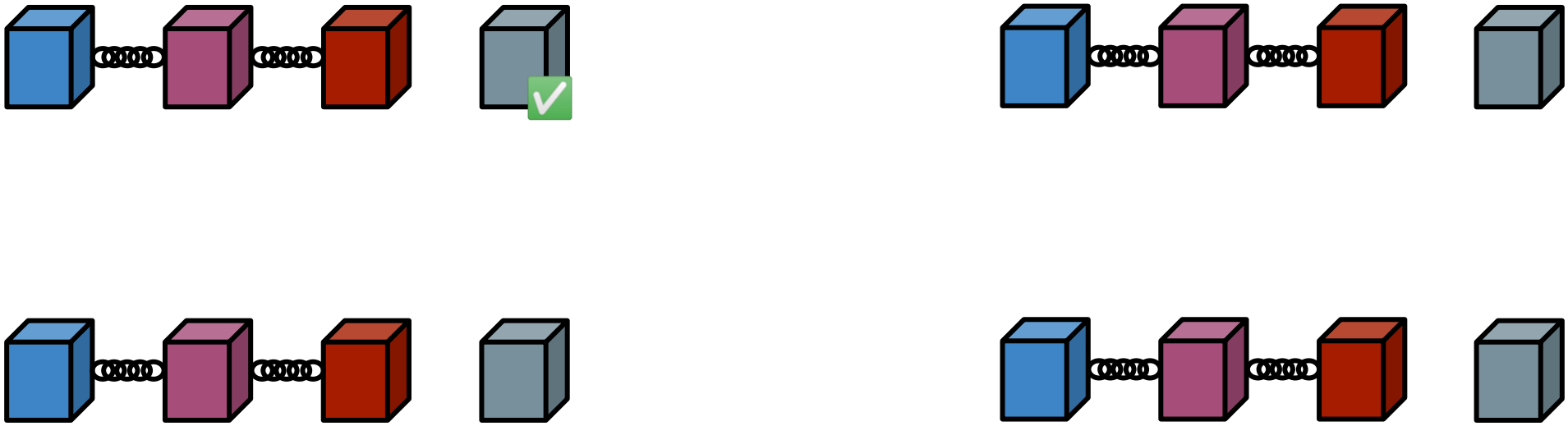


Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

P2P Network

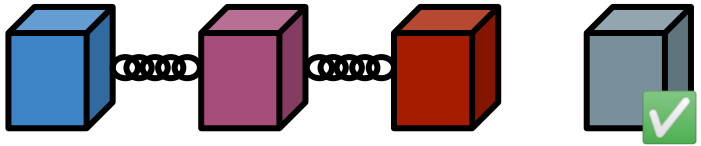
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

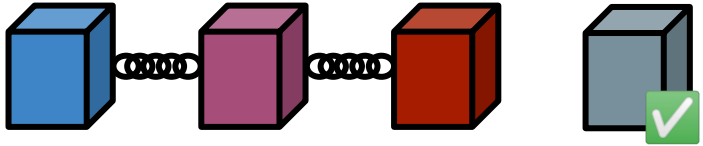
P2P Network

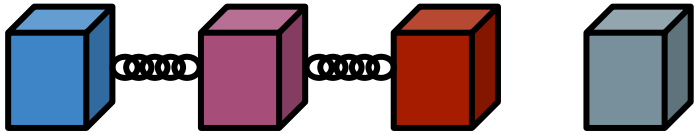


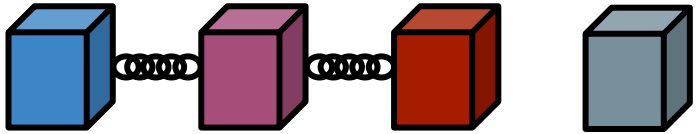
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

P2P Network



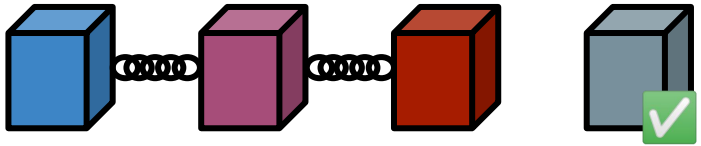


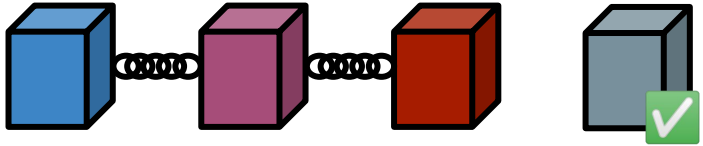


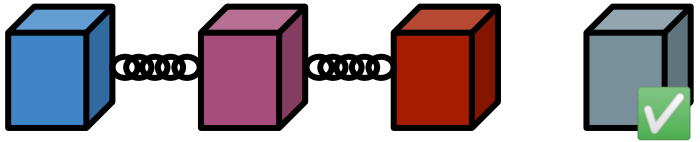


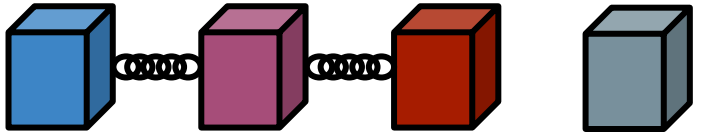
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

P2P Network



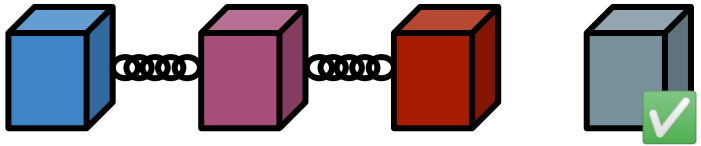


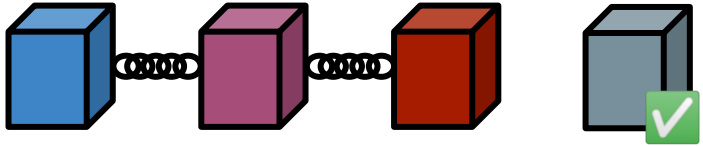


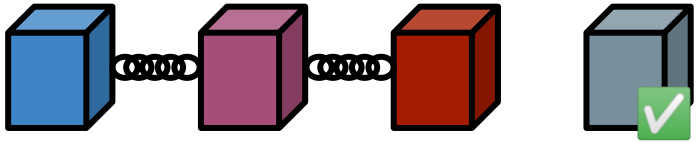


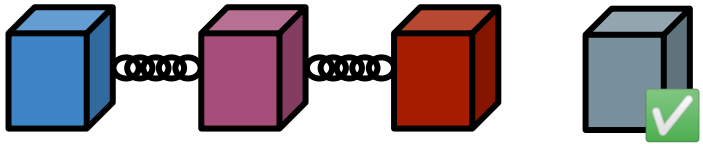
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

P2P Network



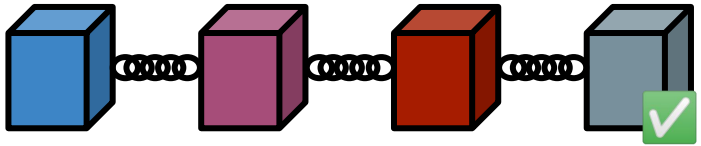


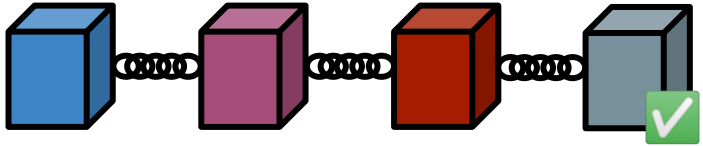


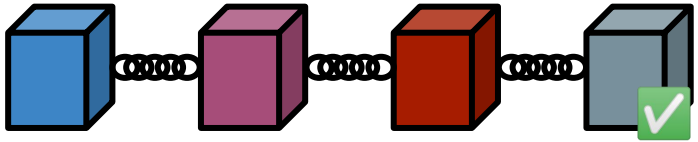


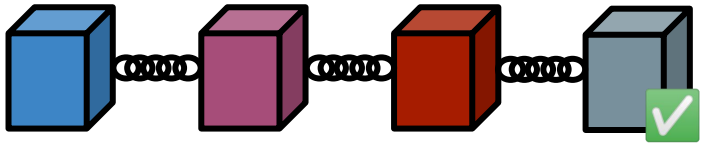
Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

P2P Network

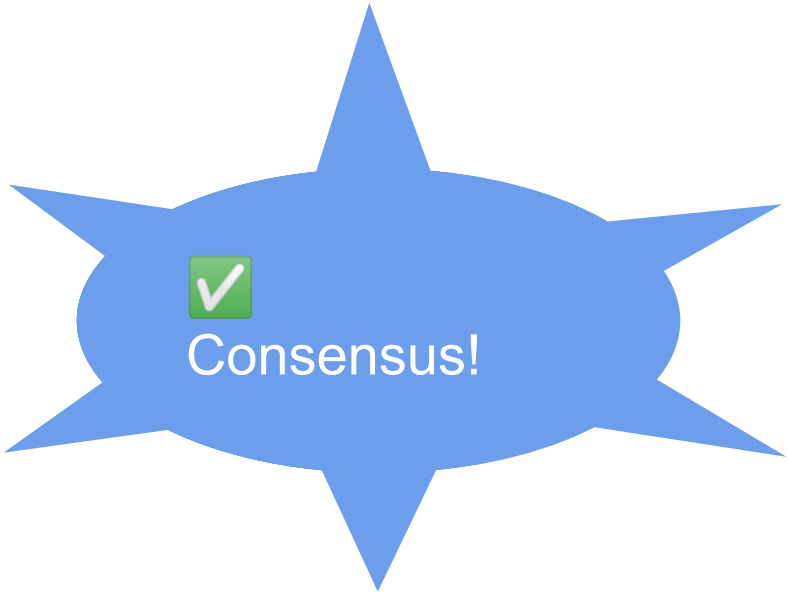








Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work



Ref: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work

Blockchain beyond Finance

- Many people argued in 2013 that blockchains can be used for Healthcare, Supply Chain Management, Voting, Identity System, Prediction Markets, Crowd Funding and many more
- But How?

Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

Why Ethereum?

Bitcoin Blockchain

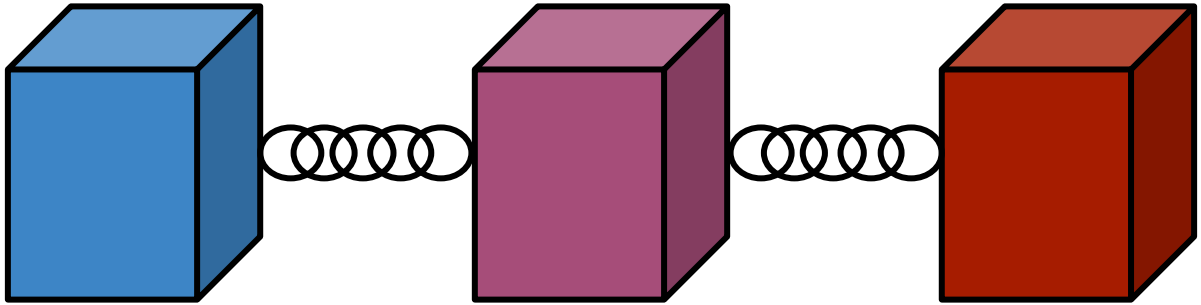
Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

Why Ethereum?

Need something like this

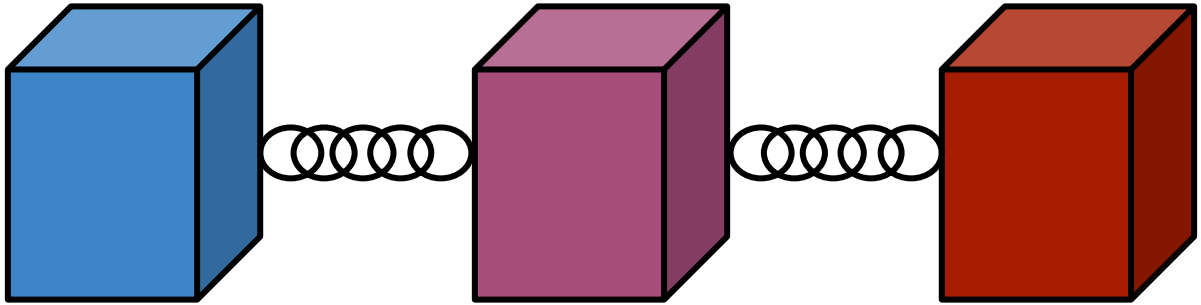
Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

What is Ethereum?



Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

What is Ethereum?



It’s a Blockchain ……. Boring Answer

Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

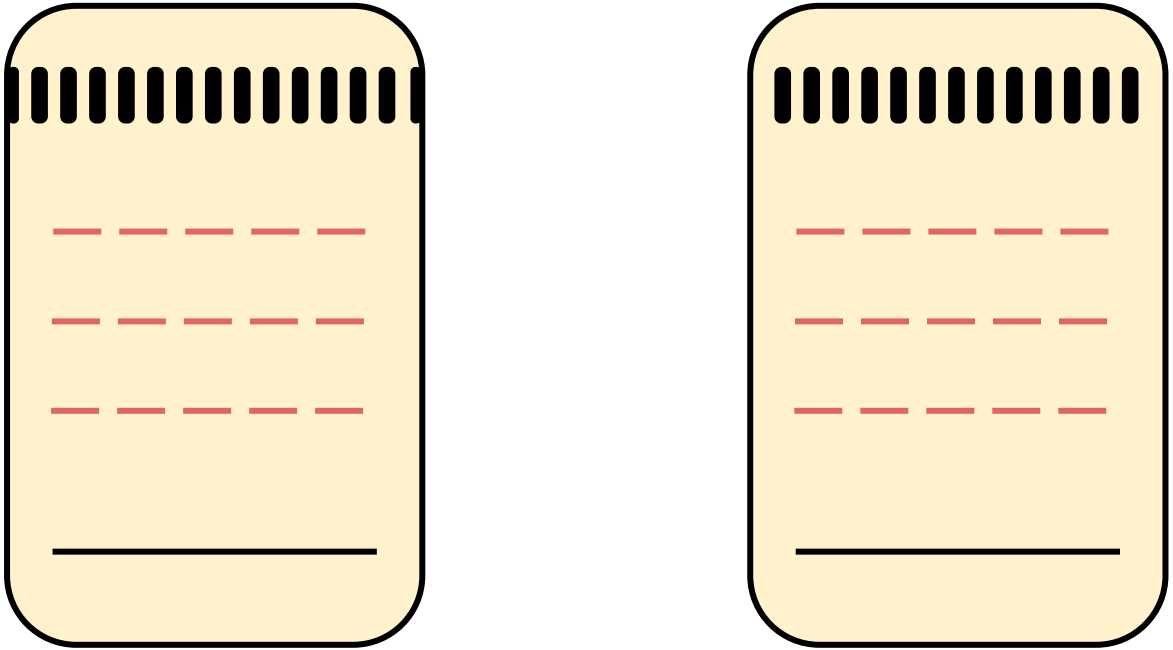
What is Ethereum?

It’s a Blockchain, with following additions

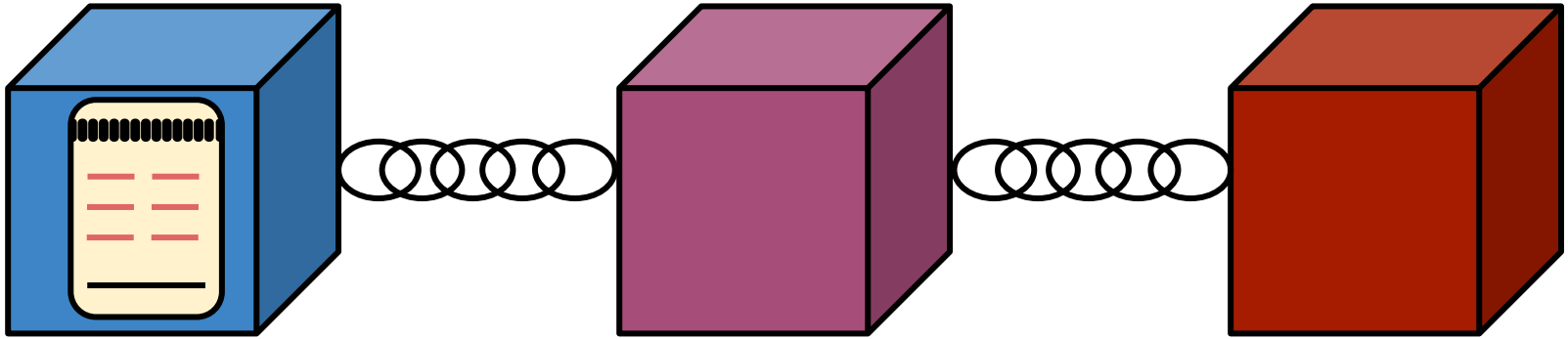
- A built-in programming Language
- Two types of accounts
  - User Accounts (Controlled by Private Keys)
  - Contract Accounts (Controlled by Code)
- Anyone can create an app by defining it as a Contract

Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

Smart Contracts



Smart contracts



- Tiny computer programs
- Stored inside a blockchain

Ref: https://savjee.be/videos/simply-explained/smart-contracts/

Smart Contract

- A code that resides on blockchain
- Executes when certain predetermined conditions are satisfied

Smart Contract

- agreement between mutually distrusting participants
- automatically enforced by the consensus mechanism of the blockchain
- without relying on a trusted authority.

Ref: Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A survey of attacks on ethereum smart contracts (sok)." *International conference on principles of security and trust*. Springer, Berlin, Heidelberg, 2017.

What a Contract can Do?

- Send ETH to other contracts

Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

What a Contract can Do?

- Send ETH to other contracts
- Read/write Storage

Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

What a Contract can Do?

- Send ETH to other contracts
- Read/write Storage
- Call (i.e. start execution in) other Contracts

Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

Smart Contract Execution

- Every node on Ethereum network processes every transaction

Ref: DEVCON1: Understanding the Ethereum Blockchain Protocol - Vitalik Buterin

Smart Contract Execution

```
pragma solidity ^0.4.17;
contract Inbox
{
        string public message;
        function Inbox(string initialMessage) public {
                message = initialMessage;
        }
        function SetMessage (string newMessage) public {
                message = newMessage;
        }
}
```

Solidity Compiler

```
bytecode:
'6060604052341561000f57600080fd5b60405161038e38038061038e8339810160405280805190910190506000818051610003d9291602001906100445650506100df565b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f1061008557805160ff191683800117855561000b2565b828001600101855582156100b2579182015b828111156100b2578251825591602001919060010190610097565b506100be9291506100c2565b5090565b6100dc91905b808211156100be576000815560010161006100c8565b90565b6102a0806100ee6000396000f300606060405263ffffffff7c0100000000000000000000000000000000000000000000000000000000000000600035041663882fabb3a811461004757578063e21f37ce1461009a57600080fd5b341561005257600080fd5b6100986004602481358181019083013580602060601f82018190048102016040519081016040528181529291906020840183838082843750949650610124955050505050505650565b005b34156100a557600080fd5b6100ad61013b565b604051602080825281908101838181518152602001915080519060200190808383600005b838110156100e9578082015183820152602001610100d1565b50505050905090810190601f168015610116578082038051600183602003610100a03191681526020019150b50925050506040518091039060f35b600081805161013792916020019061010d9565b5050565b600080546001816001161561010002031660029004801560601f016020809104026020016040519081016040528092919081815260200182805460018160011615610100020316600290048015610100d15780601f106101a657610100808354040283529160200191610100d1565b820191906000526020600020905b815481529060010190602001808311610100b457829003601f168201915b505050505081565b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f1061021a57805160ff191683800117855561024756582518255916020019190600101906102 2c565b506102539291506102575650565b6102719190 5b808211156102535760008155600101610250565b905600a165627a7a723058208f0f3e57d60457b58d09389d0da7d2d5375adecd20cfdb52a65ef21ee981d1440029',
```

Smart Contract Execution

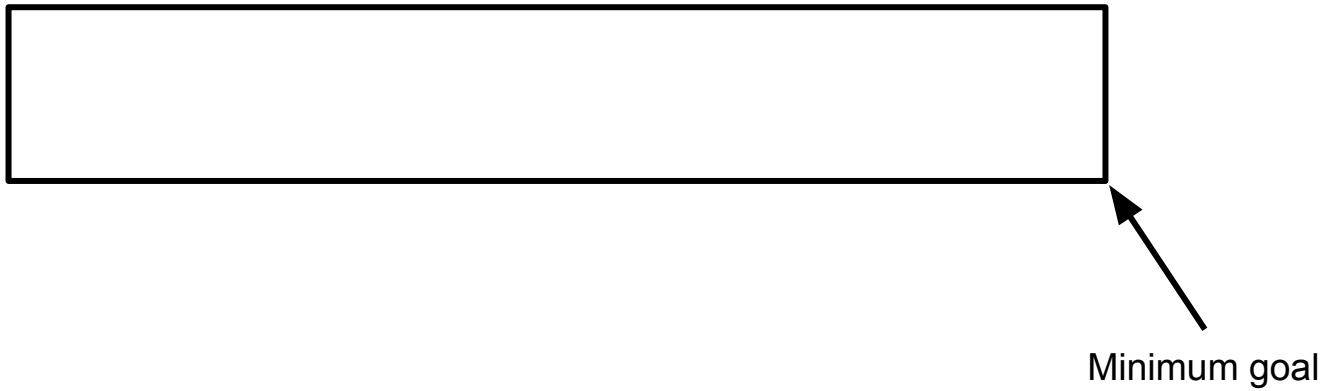
```
bytecode:
 '6060604052341561000f57600080fd5b60405161038e38038061038e8339810160405280805190910190506000818051610003d92916020019061004456 5b50506100df565b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f1061008557805160ff1916838001178555610b2565b828001600101855582156100b2579182015b828111156100b2578251825591602001919060010190610097565b506100be9291506100c2565b5090565b6100dc91905b808211156100be576000815560010161 00c8565b90565b6102a0806100ee6000396000f300606060405263ffffffff7c01000000000000000000000000000000000000000000000000000000006000350416638 8fabb3a811461004757806 3e21f37ce1461009a57600080fd5b341561005257600080fd5b6100986004602481358181019083013580602060 1f82018190048102016040519081016040528181529291906020840183838082843750949650610124955050505050505 65b005b34156100a557600080fd5b6100ad61013b565b6040516020808252819081018381815181526020019150805190602001908083836000 5b838110156100e957808201518382015260200161 00d1565b50505050905090810190601f168015610116578082038051600183602003610100 0a031916815260200191505b509250505060405180910390f35b60008180516101379291602001906101d9565b5050565b60008054600181600116156101000203166002900480601f016020809104026020016040519081016040528092919081815260200182805460018160011615610100020316600290048015610101d1565b820191906000526020600020905b815481529060010190602001808311610 1b457829003601f168201915b505050505081565b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f1061021a57805160ff1916838001178555610247565b828001600101855582156102475792182015b828111156102475782518255916020019190600101906102 2c565b50610253929150610257565b5090565b61027191905b808211156102535760008155600101610 25d565b905600a165627a7a723058208f0f3e57d60457b58d09389d0da7d2d5375adecd20cfdb52a65ef21ee981d1440029',
```

EVM
(Ethereum
Virtual
Machine)

Ethereum Virtual Machine (EVM)

- Global Singleton Computing Machine with a shared ledger of data

Crowdfunding platform



Ref: https://savjee.be/videos/simply-explained/smart-contracts/

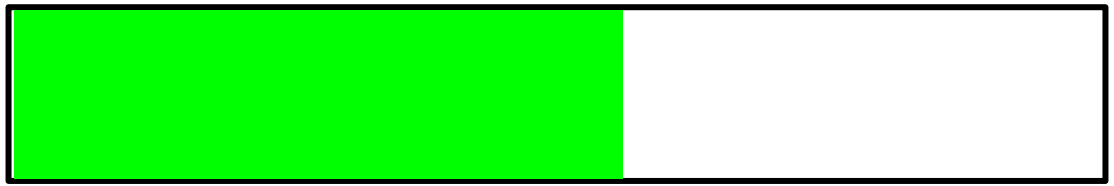
Crowdfunding platform

Ref: https://savjee.be/videos/simply-explained/smart-contracts/

Crowdfunding platform

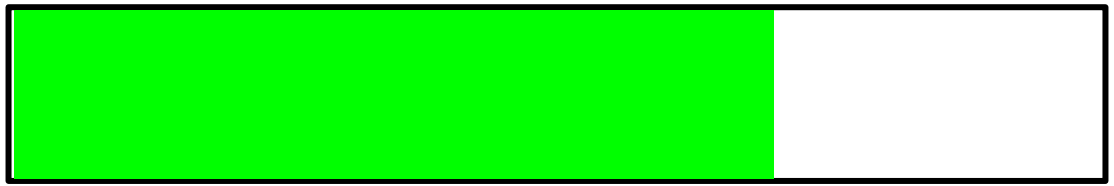
Ref: https://savjee.be/videos/simply-explained/smart-contracts/

Crowdfunding platform



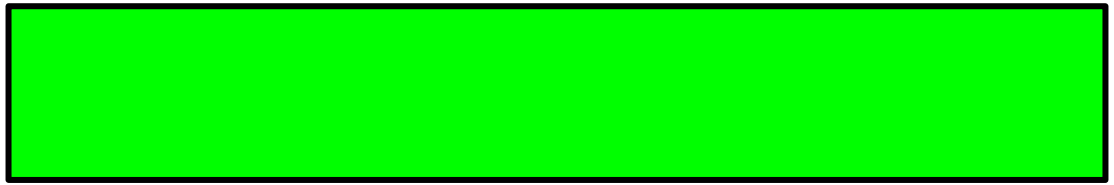
Ref: https://savjee.be/videos/simply-explained/smart-contracts/

Crowdfunding platform



Ref: https://savjee.be/videos/simply-explained/smart-contracts/

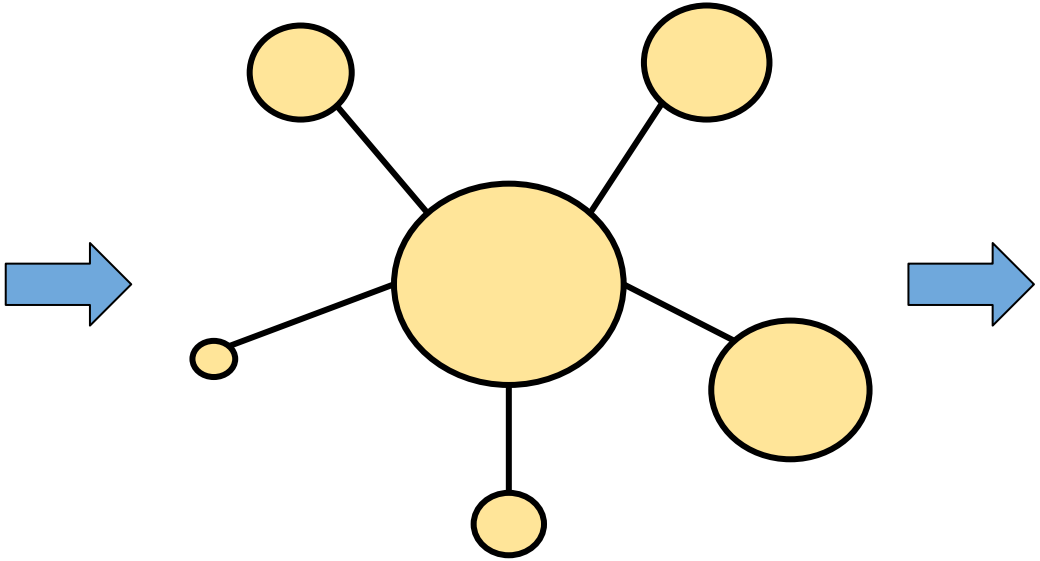
Crowdfunding platform



Funded!

Ref: https://savjee.be/videos/simply-explained/smart-contracts/

Kickstarter for Crowdfunding platform



Supporters

Product team

Ref: https://savjee.be/videos/simply-explained/smart-contracts/

Kickstarter for Crowdfunding platform

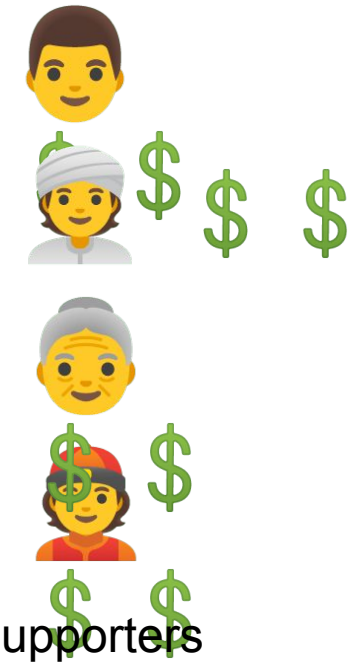
Trusting a third-party is required

Ref: https://savjee.be/videos/simply-explained/smart-contracts, https://pngimg.com

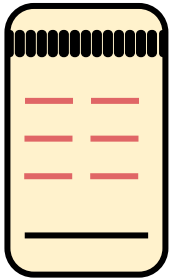
Smart contracts

We can build a similar system with a Smart Contracts without the requirement of any third party

Kickstarter with Smart Contract



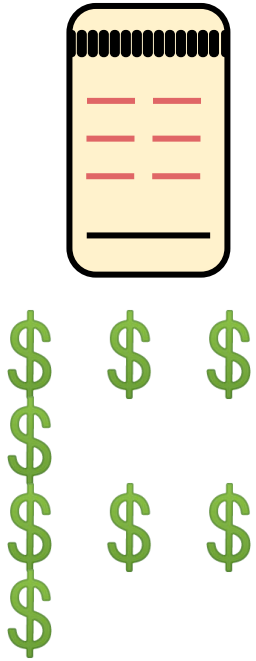
Supporters



Product team

Kickstarter with Smart Contract

Supporters

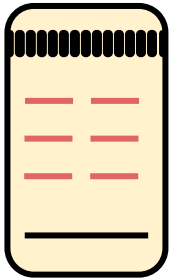


Product team

Kickstarter with Smart Contract

Supporters

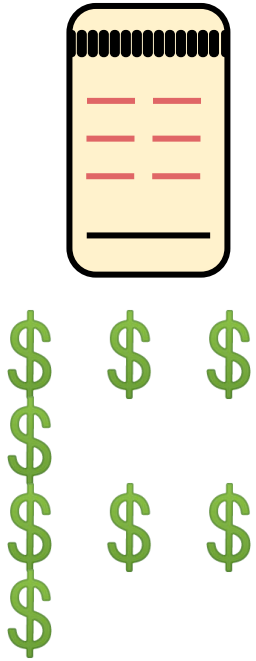
Funded!



Product team

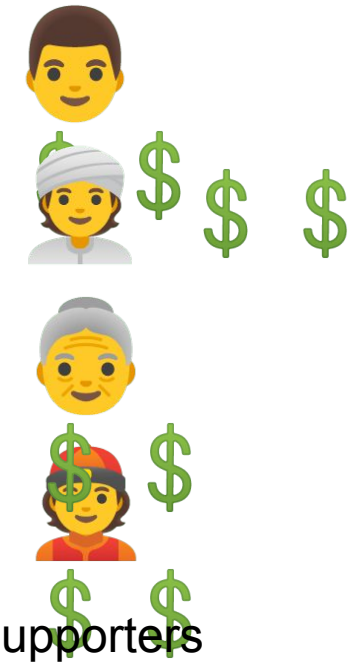
Kickstarter with Smart Contract

Supporters



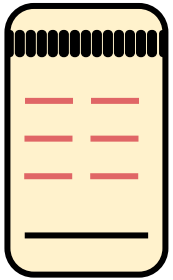
Product team

Kickstarter with Smart Contract



Supporters

Failed!



Product team

Introduction to Solidity

```
pragma solidity ^0.4.17;
contract Inbox {
    string public message;
    function Inbox(string initialMessage) public {
        message = initialMessage;
    }
    function setMessage(string newMessage) public {
        message = newMessage;
    }
    function getMessage(
    ) public view returns (string) {
        return message;
    }
}
```

Version Pragma

```
pragma solidity ^0.4.17;
```

- Instructions to the compiler on how to treat the code.
- All solidity source code should start with a “version pragma” which is a declaration of the version of the solidity compiler this code should use.
- This helps the code from being incompatible with the future versions of the compiler which may bring changes.

Ref: https://www.geeksforgeeks.org

Contract keyword

```
1 pragma solidity ^0.4.17;
2 contract Inbox {
```

- It declares a contract under which the code is encapsulated.
- Contract is similar to classes in OOP
- Contains
  - state variables
  - Functions

Ref: https://www.geeksforgeeks.org

Address in Ethereum

- Externally Owned Address (EOA)
  - public account that holds the funds
  - accessible by private key pairs
- Contract Address
  - address hosting a collection of code

Types in Solidity

Boolean	bool	**True, False**
Integer	int/uint/uint8 to uint256 in steps of 8	`uint32` → `0` up to 2^{32}-1 `int, uint` → `int256, uint256`
Address	address	Holds a 20 byte value (size of an Ethereum address)
String	Array of characters	string **public** str = "GeeksforGeeks";
Arrays	group of variables of the same data type	**uint[5] public array = [1, 2, 3, 4, 5] ;**

Ref: docs.soliditylang.org/en/latest/types.html

Types in Solidity

Struct	grouping together related data	`struct Todo {`
		`  string text;`
		`  bool completed;`
		`}`
		`// An array of 'Todo' structs`
		`Todo[] public todos;`

Mapping	• Dictionary • Key-value pair	// Mapping from address to uint **mapping**(**address** => **uint**) **public** myMap;
….	…….	……..

Ref: www.geeksforgeeks.org, solidity-by-example.org

State Variables

```
1 pragma solidity ^0.4.17;
2 contract Inbox {
3     string public message;
4     function Inbox(string initialMessage) public {
5         message = initialMessage;
6     }
```

- Permanently stored in contract storage → written to Ethereum Blockchain
- Declared inside a contract and outside of function
- Adding a slot to a Database

Ref: https://www.geeksforgeeks.org

State Variable Visibility

Public	can be accessed by any contract
Private	can be only accessed by the contract in which the variable is defined
Internal	can be accessed by contract in which the variable is defined or by its inherited contracts

Ref: https://docs.soliditylang.org/en/latest/contracts.html#visibility-and-getters

Function declaration

```
1  pragma solidity ^0.4.17;
2  contract Inbox {
3      string public message;
4      function Inbox(string initialMessage) public {
5          message = initialMessage;
6      }
7      function setMessage(string newMessage) public {
8          message = newMessage;
9      }
10     function getMessage(
11     ) public view returns (string) {
12         return message;
13     }
14 }
```

Constructor

Ref: https://www.geeksforgeeks.org

Constructor

- It invokes only once when the contract is deployed
- used to initialize the contract state
- optional to create a constructor
- Version < 0.4.22, constructors → the same name as the contract
- Version > 0.4.22 contractors → constructor() keyword

Ref: https://www.geeksforgeeks.org

Constructor

```
pragma solidity ^0.4.17;
contract Inbox {
    string public message;
    function Inbox(string initialMessage) public {
        message = initialMessage;
    }
```

Constructor

- Initializes message variable with input passed while contract creation

Ref: https://www.geeksforgeeks.org

Other Functions

```
1  pragma solidity ^0.4.17;
2  contract Inbox {
3      string public message;
4      function Inbox(string initialMessage) public {
5          message = initialMessage;
6      }
7      function setMessage(string newMessage) public {
8          message = newMessage;
9      }
10     function getMessage(
11     ) public view returns (string) {
12         return message;
13     }
14 }
```

Ref: https://www.geeksforgeeks.org

Function Visibility

```
pragma solidity ^0.4.17;
contract Inbox {
    string public message;
    function Inbox(string initialMessage) public {
        message = initialMessage;
    }
    function setMessage(string newMessage) public {
        message = newMessage;
    }
    function getMessage(
    ) public view returns (string) {
        return message;
    }
}
```

Visibility

View keyword

Function Visibility

Public	can be called by any contract
Private	can be only called by the contract in which the function resides
Internal	can be called contract in which the function is present or by its inherited contracts
External	can be called by external contracts only

Ref: www.geeksforgeeks.org

View and Pure functions

View	Read-only function
Pure	Does not read or modify the state variables

Ref: www.geeksforgeeks.org

msg Global Variables in Ethereum

- Special global variables
- Always exists globally

msg.sender	address where the current function call came from
msg.value	the amount of wei (money) sent
.....	.....

Ref: https://medium.com/upstate-interactive/what-you-need-to-know-about-msg-global-variables-in-solidity-566f1e83cc69

Function Modifiers

- change the behavior of functions in a declarative way
- automatically check a condition prior to executing the function.
- The placeholder statement (_) → where the body of the function should be inserted.

Ref: docs.soliditylang.org

Function Modifiers

```
pragma solidity >=0.4.22 <0.9.0;

contract Purchase {
    address public seller;

    modifier onlySeller() { // Modifier
        require(
            msg.sender == seller,
            "Only seller can call this."
        );
        _;
    }

    function abort() public view onlySeller { // Modifier usage
        // ...
    }
}
```

Ref: docs.soliditylang.org

Events

- events are a way to log and notify external entities
- emitting and recording data onto the blockchain
- similar to logs or records
- When an event is emitted it generates an event log that is stored on the blockchain.

Ref: medium.com/coinmonks

Events

```
pragma solidity >=0.4.21 <0.9.0;

contract ClientReceipt {
    event Deposit(
        address indexed from,
        bytes32 indexed id,
        uint value
    );

    function deposit(bytes32 id) public payable {
        // Events are emitted using `emit`, followed by
        // the name of the event and the arguments
        // (if any) in parentheses. Any such invocation
        // (even deeply nested) can be detected from
        // the JavaScript API by filtering for `Deposit`.
        emit Deposit(msg.sender, id, msg.value);
    }
}
```

Ref: docs.soliditylang.org

Retrieving Events

```
const contract = new web3.eth.Contract(abi, contractAddress);
contract.getPastEvents('NewTransaction', {
  filter: { sender: '0x123abc' }, // Optional event filtering
  fromBlock: 0, // Start block number
  toBlock: 'latest' // End block number
})
.then(function(events) {
  // Process the retrieved events
  console.log(events);
})
.catch(function(error) {
  // Handle errors
  console.error(error);
});
```

Event Name

Ref: docs.soliditylang.org

Contract ABI

- The ABI (Application Binary Interface): JSON file that describes the
  - interface of the smart contract
    - functions that it exposes (with parameters)
    - Events from the Smart Contracts

Ref: https://blockchain.oodles.io/dev-blog/How-to-Use-a-Web3-JS-Call-Contract-Function.

Code Execution on Real Blockchain (Try this after success on Local Blockchain)

- Testnet:
  - Can use **Remix** and **Metamask**
  - Can use **hardhat** to deploy on **Goerli Testnet**
- Mainnet
  - Require real money
  - Do not try unless you become expert

Ref: https://www.geeksforgeeks.org

Code Execution on Local Blockchain

- Offline (Blockchain inside local machine): It takes time to setup.
  - Can use **Remix** and **Ganache**
- Online (Blockchain inside browser): Remix IDE
  - Simple one, first try this

Ref: https://www.geeksforgeeks.org

“Hello World” Smart Contract in Remix-IDE

```
pragma solidity ^0.4.17;

contract HelloWorld
{
    function get() public pure returns (string memory)
    {
        return 'Hello Contracts';
    }
}
```

Let’s see a Demo

Ref: https://www.geeksforgeeks.org

“Inbox” Smart Contract in Remix-IDE

```
pragma solidity ^0.4.17;
contract Inbox {
    string public message;
    function Inbox(string initialMessage) public {
        message = initialMessage;
    }
    function setMessage(string newMessage) public {
        message = newMessage;
    }
    function getMessage(
    ) public view returns (string) {
        return message;
    }
}
```

Let’s see a Demo

Ref: www.geeksforgeeks.org

Crowdfunding Smart Contract

```
pragma solidity ^0.4.19;
contract Crowdfunding {
    address owner;
    uint256 deadline;
    uint256 goal;
    mapping(address => uint256) public pledgeOf;
    function Crowdfunding(uint256 numberOfDays, uint256 _goal) public {
        owner = msg.sender;
        deadline = now + (numberOfDays * 1 days);
        goal = _goal;
    }
    function pledge(uint256 amount) public payable {
        require(now < deadline);                // in the fundraising period
        require(msg.value == amount);
        pledgeOf[msg.sender] += amount;
    }
    function claimFunds() public {
        require(address(this).balance >= goal); // funding goal met
        require(now >= deadline);               // in the withdrawal period
        require(msg.sender == owner);

        msg.sender.transfer(address(this).balance);
    }
    function getRefund() public {
        require(address(this).balance < goal);  // funding goal not met
        require(now >= deadline);               // in the withdrawal period
        uint256 amount = pledgeOf[msg.sender];
        pledgeOf[msg.sender] = 0;
        msg.sender.transfer(amount);
    }
}
```

Currency Example

```
pragma solidity ^0.8.4;
contract Coin {
    // The keyword "public" makes variables
    // accessible from other contracts
    address public minter;
    mapping(address => uint) public balances;
    // Events allow clients to react to specific
    // contract changes you declare
    event Sent(address from, address to, uint amount);
    // Constructor code is only run when the contract
    // is created
    constructor() {
        minter = msg.sender;
    }
    // Sends an amount of newly created coins to an address
    // Can only be called by the contract creator
    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        balances[receiver] += amount;
    }
    // Errors allow you to provide information about
    // why an operation failed. They are returned
    // to the caller of the function.
    error InsufficientBalance(uint requested, uint available);
    // Sends an amount of existing coins
    // from any caller to an address
    function send(address receiver, uint amount) public {
        if (amount > balances[msg.sender])
            revert InsufficientBalance({
                requested: amount,
                available: balances[msg.sender]
            });
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        emit Sent(msg.sender, receiver, amount);
    }
}
```

Let’s see a Demo

Part 2: Vulnerabilities in Smart Contracts

Smart Contract Security

- Correctness is ensured by the consensus mechanism
- Unfortunately, correctness is not sufficient to make Smart Contracts secure.

Ref: Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A survey of attacks on ethereum smart contracts (sok)." *International conference on principles of security and trust*. Springer, Berlin, Heidelberg, 2017.

Classification of Blockchain based Attacks

- Malicious Acts
- Weak Protocol
- Defraud
- Application Bugs

Ref: Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Classification of Blockchain based Attacks

- Malicious Acts
- Weak Protocol
- Defraud
- Application Bugs

Ref: Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Application Bugs

- Programs are correct but may have loopholes
- People can take advantage of it by exploiting loophole
- Example: buffer overflow

Ref: Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Application Bugs

- Blockchains are new
- Smart contract developers may write buggy code

Application Bugs

- Loophole in the smart Contract Code
- The DAO Attack ($60 M Loss)
- Attacker can steal money, influences an application to function differently

Ref: Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Application Bugs

- Reentrancy
- Overflow, Underflow
- Default Visibilities
- Timestamp Dependence
- Transaction Ordering Dependence

Ref: Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

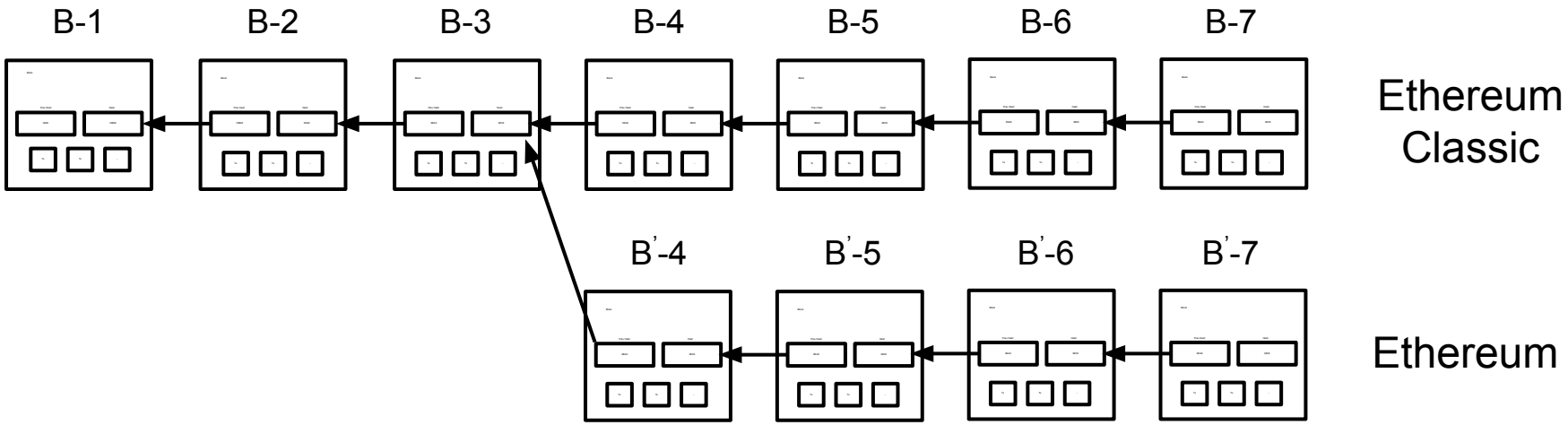
The DAO Hack on Ethereum

- DAO was crowdfunding platform
- It raised $150 Million
- Got hacked due to bug in Smart Contract (Reentrancy) and lost $60 Million
- Ethereum blockchain was hard forked to restore stolen funds

Hard Fork Example

- Demonetization (Govt banned 500 and 1000 Rupees notes)
- Let's say that one group don’t agree and accept old notes
- Normal people agreed to Govt decision
- Two currencies in existence

Hard Fork



Smart Contract Vuln

```
contract Puzzle {
  uint256 amount = 0.5; //0.5 ethers
  function submit_answer (string answer) {
    //Logic to check submitted answer
    if (/*answer is correct*/)
      _sendEther();
  }
  function _sendEther(){
    msg.sender.tranfer(amount);
  }
}
```

Ref: Sayeed, Sarwar, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Smart Contract Vuln: Default Visibilities

Programmer forgot to add Visibility for the function _sendEther()

```
contract Puzzle {
  uint256 amount = 0.5; //0.5 ethers
  function submit_answer (string answer) {
    //Logic to check submitted answer
    if (/*answer is correct*/)
      _sendEther();
  }
  function _sendEther(){
    msg.sender.tranfer(amount);
  }
}
```

Ref: Sayeed, Sarwar, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Smart Contract Vuln: Default Visibilities

Let's see a Demo

```
contract Puzzle {
  uint256 amount = 0.5; //0.5 ethers
  function submit_answer (string answer) {
    //Logic to check submitted answer
    if (/*answer is correct*/)
      _sendEther();
  }
  function _sendEther(){
    msg.sender.tranfer(amount);
  }
}
```

Ref: Sayeed, Sarwar, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Smart Contract Vuln: Timestamp Dependence

- A smart contract that utilizes a current timestamp to produce random numbers in order to determine lottery results
- Miners can put a timestamp within 30 seconds of block validation
- Miners can alter outcome of random number generator

Ref: Sayeed, Sarwar, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Smart Contract Vuln: Timestamp Dependence

```
pragma solidity ^0.5.0;
contract TimedCrowdsale {
  event Finished();
  event notFinished();
  // Sale should finish exactly at January 1, 2019
  function isSaleFinished() private returns (bool) {
    return block.timestamp >= 1546300800;
  }
  function run() public {
    if (isSaleFinished()) {
        emit Finished();
    } else {
        emit notFinished();
    }
  }
}
```

Ref: https://swcregistry.io/docs/SWC-116

Recursion

Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Fallback Function in Solidity

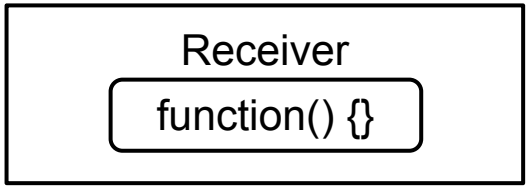
- Declare with fallback() and have no arguments.
- If it is not marked **payable**, the contract will throw an exception on receiving Ether without data
- No Return value, Once per contract
- Executed → if caller meant to call a non-available function or receive() does not exist
- Visibility: external.

Ref: https://www.geeksforgeeks.org/solidity-fall-back-function

Reentrancy Example (Expected Behavior)

```
function revoke() remote{
  uint256 value = balances[msg.sender];
  require(msg.sender.call.value(value) ());
  balances[msg.sender] = 0;
}
```

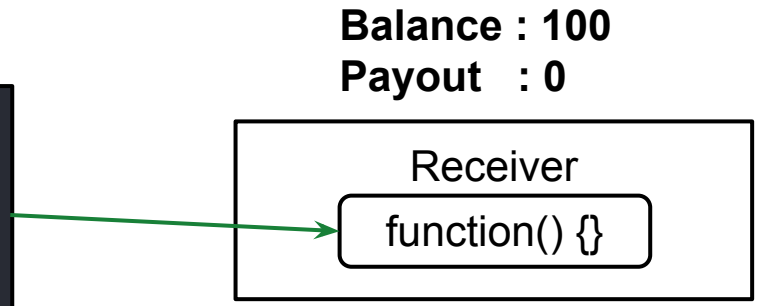
Balance : 100
Payout : 0



Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Expected Behavior)

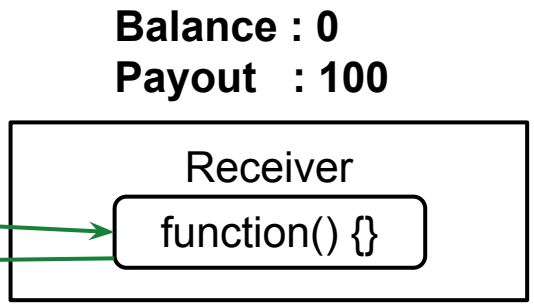
```
1  function revoke() remote{
2    uint256 value = balances[msg.sender];
3    require(msg.sender.call.value(value) ());
4    balances[msg.sender] = 0;
5  }
```



Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Expected Behavior)

```
function revoke() remote{
  uint256 value = balances[msg.sender];
  require(msg.sender.call.value(value) ());
  balances[msg.sender] = 0;
}
```

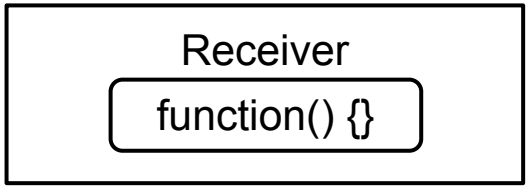


Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Exploit)

```
function revoke() remote{
  uint256 value = balances[msg.sender];
  require(msg.sender.call.value(value) ());
  balances[msg.sender] = 0;
}
```

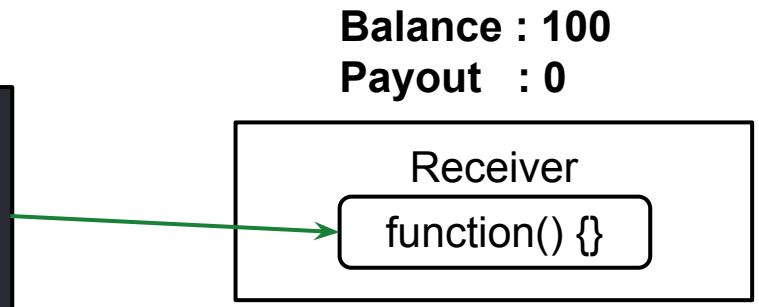
Balance : 100
Payout : 0



Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Exploit)

```
function revoke() remote{
  uint256 value = balances[msg.sender];
  require(msg.sender.call.value(value) ());
  balances[msg.sender] = 0;
}
```



Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Exploit)

```
function revoke() remote{
  uint256 value = balances[msg.sender];
  require(msg.sender.call.value(value) ());
  balances[msg.sender] = 0;
}
```

Balance : 100
Payout : 100

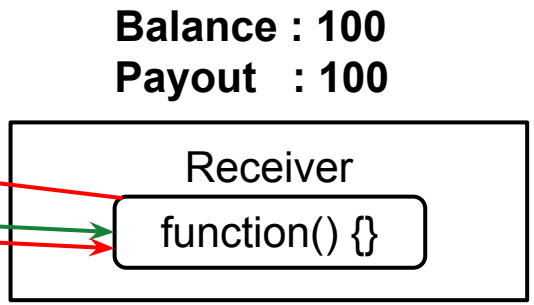
Receiver

function() {}

Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Exploit)

```
1  function revoke() remote{
2    uint256 value = balances[msg.sender];
3    require(msg.sender.call.value(value) ());
4    balances[msg.sender] = 0;
5  }
```



Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Exploit)

```
function revoke() remote{
  uint256 value = balances[msg.sender];
  require(msg.sender.call.value(value) ());
  balances[msg.sender] = 0;
}
```

Balance : 100
Payout : 200

Receiver

function() {}

Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Exploit)

```
1  function revoke() remote{
2    uint256 value = balances[msg.sender];
3    require(msg.sender.call.value(value) ());
4    balances[msg.sender] = 0;
5  }
```

Balance : 100
Payout : 200

Receiver

function() {}

Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Example (Exploit)

```
function revoke() remote{
  uint256 value = balances[msg.sender];
  require(msg.sender.call.value(value) ());
  balances[msg.sender] = 0;
}
```

Balance : 100
Payout : 300 …

Receiver

function() {}

Ref: CS 410b, Blockchain Development and Security, Instructor: Wu-chang Feng, Portland State University

Reentrancy Bug Fixed

```
function revoke() remote{ //Insecure
    uint256 value = balances[msg.sender];
    require(msg.sender.call.value(value) ());
    balances[msg.sender] = 0;
}

function revoke() remote{ //Secure
    uint256 value = balances[msg.sender];
    balances[msg.sender] = 0;
    require(msg.sender.call.value(value) ());
}
```

Ref: Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Reentrancy Example-2

```
function Collect(uint _am)
public
payable
{
    var acc = Acc[msg.sender];
    if( acc.balance>=MinSum && acc.balance>=_am && now>acc.unlockTime)
    {
        if(msg.sender.call.value(_am)())
        {
            acc.balance-=_am;
            LogFile.AddMessage(msg.sender,_am,"Collect");
        }
    }
}
```

```
uint public MinSum = 2 ether;
```

```
struct Holder
{
    uint unlockTime;
    uint balance;
}

mapping (address => Holder) public Acc;
```

Reentrancy Example-3

```
modifier onlyOwner{
    require(msg.sender == owner);
    _;
}
...
function execute( address _to, uint _value, bytes
    _data) external onlyOwner {
    ...
    _to.call.value(_value)(data);
}
```

Code example: Identify control based permission control

Ref: Zibin Zheng, Neng Zhang, Jianzhong Su, Zhijie Zhong, Mingxi Ye, and Jiachi Chen. 2023. Turn the Rudder: A Beacon of Reentrancy Detection for Smart Contracts on Ethereum. In Proceedings of the 45th International Conference on Software Engineering (ICSE '23). IEEE Press, 295–306. https://doi.org/10.1109/ICSE48619.2023.00036

Unchecked Call Return Value

- Return value of message call → not checked.
- If
  - call fails accidentally
  - attacker forces the call to fail
    - may cause unexpected behaviour in the subsequent program logic.

Ref: https://swcregistry.io/docs/SWC-104/

Unchecked Call Return Value

```
pragma solidity 0.4.25;

contract ReturnValue {



  function callnotchecked(address callee) public {
    callee.call();
  }
```

Ref: https://swcregistry.io/docs/SWC-104/

Unchecked Call Return Value

```
pragma solidity 0.4.25;

contract ReturnValue {

  function callchecked(address callee) public {
    require(callee.call());
  }

  function callnotchecked(address callee) public {
    callee.call();
  }
```

Ref: https://swcregistry.io/docs/SWC-104/

Unchecked Call Return Value

```
// Bad Code:
function Transfer(address _addr) public {
    (bool success, bytes memory data) = _addr.call{value: msg.value, gas: 5000}();
```

Ref: https://sm4rty.medium.com/unchecked-call-return-value-solidity-security-1-fe794a7cdb6f

Unchecked Call Return Value

```
// Bad Code:
function Transfer(address _addr) public {
    (bool success, bytes memory data) = _addr.call{value: msg.value, gas: 5000}();


// Good Code
function Transfer(address _addr) public {
    (bool success, bytes memory data) = _addr.call{value: msg.value, gas: 5000}();
    require(success, "Transfer Failed")
```

Ref: https://sm4rty.medium.com/unchecked-call-return-value-solidity-security-1-fe794a7cdb6f

THE END

Backup Slides

Smart Contract Vuln: Overflow and Underflow

```
mapping (address => uint256) public balanceOf;

// INSECURE
function transfer(address _to, uint256 _value) {
    /* Check if sender has balance */
    require(balanceOf[msg.sender] >= _value);
    /* Add and subtract new balances */
    balanceOf[msg.sender] -= _value;
    balanceOf[_to] += _value;
}

// SECURE
function transfer(address _to, uint256 _value) {
    /* Check if sender has balance and for overflows */
    require(balanceOf[msg.sender] >= _value &&
      balanceOf[_to] + _value >= balanceOf[_to]);
    /* Add and subtract new balances */
    balanceOf[msg.sender] -= _value;
    balanceOf[_to] += _value;
}
```

Ref: Sayeed, Sarwar, Hector Marco-Gisbert, and Tom Caira. "Smart contract: Attacks and protections." IEEE Access 8 (2020): 24416-24427.

Gas assigned per Opcode

Operation	Gas	Description
ADD/SUB	3	Arithmetic Operation
MUL/DIV	5	
ADDMOD/MULMOD	8	
AND/OR/XOR	3	Comparison Operation
LT/GT/SLT/SGT/EQ	2	Stack Operation
POP	3	

Ref: Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* (2014)

Gas assigned per Opcode

Operation	Gas	Description
BALANCE	400	Get balance of an account
CREATE	32000	Create a new account using CREATE
CALL	25000	Message-call into an account

Ref: Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* (2014)

Gas assigned per Opcode

Operation	Gas	Description
MLOAD/MSTORE	3	Memory Operation
JUMP	8	Unconditional Jump
JUMPI	10	Conditional Jump
SLOAD	200	Storage Operation
SSTORE	5000/20000	

Ref: Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* (2014)