Weekly Lesson Plan

Programming with Solidity

Blockchain Components

Peer-to-peer networking

NETWORK

A group of computers such as the BitTorrent network that can communicate among themselves without relying on a single central authority and therefore not presenting a single point of failure.

Asymmetric cryptography

SECURITY

Message encrypted for specific recipients such that anyone can verify the sender's authenticity, but only intended recipients can read the message contents.

In Bitcoin and Ethereum, asymmetric cryptography is used to create a set of credentials for your account, to ensure that only you can transfer your tokens.

Cryptographic hashing

MERKLE TREE

To generate a small, unique "fingerprint" for any data, allowing quick comparison of large datasets and a secure way to verify that data has not been altered; in both Bitcoin and Ethereum.

Record the canonical order of transactions, which is then hashed into a "fingerprint" that serves as a basis of comparison for computers on the network.

https://www.ikamy.ch/public/img/books/Introducing+Ethereum+and+Solidity.pdf (p4)

THE VALUE OF CRYPTOCURRENCY

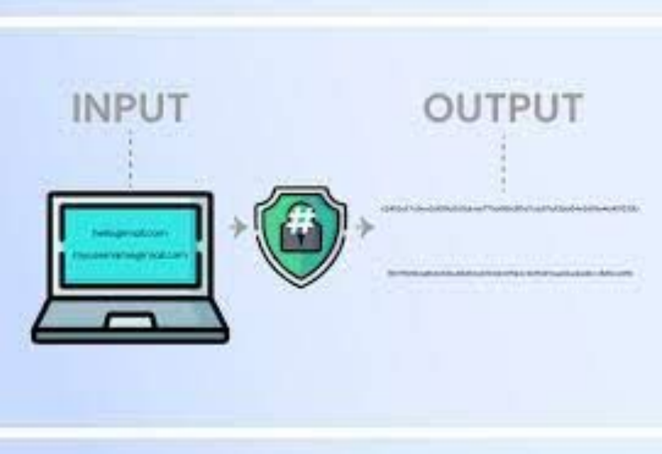
Is namely determined by the DEMAND for the currency.

You can redeem your bitcoins for US dollars, Euros, gold, or other fiat currency.

Just as the Bitcoin network moves bitcoin tokens, the Ethereum network moves ether tokens.

HASHCASH

2002



HASHCASH

The email anti-spam tool, like the proof-of-work algorithm, is also called hashcash and is used to create stamps to attach to mail to add a micro-cost to sending mail to deter spamming. The main use of the hashcash stamp is as a white-listing hint to help hashcash users avoid losing email due to content based and blacklist based anti-spam systems.

Verification can be done by a human eye (count leading 0s) even with availability of common preinstalled command line tools such as sha1sum.

The algorithm works with a cryptographic hash, such as SHA1, SHA256 or coming SHA3 that exhibits 2nd-preimage resistance. 2nd-preimage resistance is a stronger hash property than the collision resistance property.

At this point it is most widely used as the bitcoin mining function.

http://www.hashcash.org/

EVM

Ethereum Virtual Machine

Public vs. Private Chains

PRIVATE BLOCKCHAIN

“MAKE YOUR OWN ETHEREUM”

PUBLIC BLOCKCHAIN

Instead of reinventing the wheel, a duplication of effort by the existing Ethereum development community.

In both public or private Ethereum chains, you can do the following:

1. Send and receive ether
2. Write smart contracts
3. Create provably fair applications
4. Launch your own token based on ether

https://www.ikamy.ch/public/img/books/Introducing+Ethereum+and+Solidity.pdf (p18)

1. Send and Receive Ether

In order to trade dollars for ether, you need to join a cryptocurrency exchange, or buy from a commercial money transmitter such as Coinbase.

On a private chain you have private ether that’s a value-less scrip.

2. Write Smart Contracts

Control payments and transfers between accounts (and even between other contracts).

Available in Public and Private Chains.

3. Create “Provably” Fair Applications

Proof of Concept, like a fair game/ dealing.

4. Launch Your Own Token

A system of user accounts that agree to custody and exchange an Asset.

EX: A private transaction ledger, accessible to only you and your private group.

- Uses the underlying system of exchange and valuation of ETH.

WALLETS

Accounts in both Bitcoin and Ethereum are represented by long hexidecimal addresses.

Ethereum address= a long hexadecimal address.

0xB38AA74527aD855054DC17f4324FE9b4004C720C

Bitcoin address = encoded in base 58

1GDCKfdTo4yNDd9tEM4JsL8DnTVDw552Sy

ACCOUNT

The previous encoding represents a PUBLIC KEY which is required for a counterparty to a transaction in order to make an exchange.

An ACCOUNT is a data object: an entry in the blockchain ledger, indexed by its address, containing data about the state of that account, such as its balance.

An ADDRESS is the PUBLIC KEY belonging to a particular user; it’s how users access their accounts.

ACCOUNT: PRIVATE KEY

In the event that your hardware (cell phone, computer) is damaged all you need is your PRIVATE KEY, so that you can access your money from another NODE.

The EVM is a global machine, it has no way of knowing which node you'll create a transaction from.

https://www.ikamy.ch/public/img/books/Introducing+Ethereum+and+Solidity.pdf (23)

Blockchain Methodologies

Asymmetric cryptography

Asymmetric cryptography

Cryptographic hashing

NETWORK

Sending secure messages back and forth over a network, where the sender and the recipient do not trust the channel of communication.

ASYMMETRIC

Each party in a transaction has a pair of two different, but mathematically related, keys.

MERKLE TREE

Public-key cryptography was developed for wartime communications, and when used properly, can be extremely secure.

Unlike symmetric-key cryptographic, public key cryptographic communications don’t require a secure channel between parties.

https://www.ikamy.ch/public/img/books/Introducing+Ethereum+and+Solidity.pdf (p4)

SOLIDITY

DATA STORAGE

Stack

PUSH / POP

Add and remove values.

Dynamic Memory

HEAP

Infinitely expandable byte array.

Key/Value store

STORAGE

Account Balances

Contract Addresses

Value

Sender

https://www.ikamy.ch/public/img/books/Introducing+Ethereum+and+Solidity.pdf (p70)

CONTRACT ORIENTED LANGUAGE

```
contract PiggyBank {
        address creator;
        uint deposits;

        // Declaring this function as public makes it accessible to other users and smart contracts.

        function PiggyBank() public
         {
                creator = msg.sender;
                deposits = 0;
        }

        //      EX:     Check whether any ether has been deposited.
        //      When it is deposited, the number of deposits go up and the total count is returned.

        function deposit() payable returns (uint)
         {
                if(msg.value > 0)
                        deposits = deposits + 1;
                return getNumberOfDeposits();
         }
        ...
```

https://www.ikamy.ch/public/img/books/Introducing+Ethereum+and+Solidity.pdf (p80)

PiggyBank**.sol**

REMIX

https://www.dappuniversity.com/articles/solidity-tutorial

Introduction to REMIX

REMIX

Web Based IDE

We will be using this throughout the week to demonstrate how to Compile, test, and analyze smart contracts.

SOLIDITY: How to create an ECR20 Token

0XPROJECT ECR20

Create an ECR20 Token.

- Project Template
- REMIX

https://www.ikamy.ch/public/img/books/Introducing+Ethereum+and+Solidity.pdf