Blocklime
<ACADEMY/>

#Dappathon Tour - Kuala Lumpur

Day 1 : Dapp Development Training

The Fundamentals

I good in developing & imagining things but terrible on writing about myself. So, let's talk !

- Harpreet Maan

Harpreet Singh Maan

CEO & Sr.Blockchain developer | Blockchain Speaker & Trainer | T...

Co-Founder & CEO
Blocklime Technologies Sdn. Bhd.
DLT, Blockchain, Fintech, Insurtech & Regtech Enthusiast
Harpreet@blocklime.com
Linkedin.com/in/harpreet-maan

What is Blocklime?

- Blocklime Technologies Sdn. Bhd. (1260889-P) is a Blockchain Enabler based in Cyberjaya, Malaysia.
- Young and all rounded team of passionate blockchain developers and designers.

What services do we provide?

- Blockchain Development
- Blocklime Academy
- Tech and Business Consultancy
- Events

Dapp.com APAC #Dappathon Tour

Kuala Lumpur

Questions for Trainer

Sli.do

Bootcamp

#Q487

Hosted by dapp.com

For registration, please go to Eventbrite.com and search for "Dappathon".

Blocklime
<ACADEMY/>

Syllabus

1260889-P
Blocklime Technologies Sdn. Bhd.

Agenda

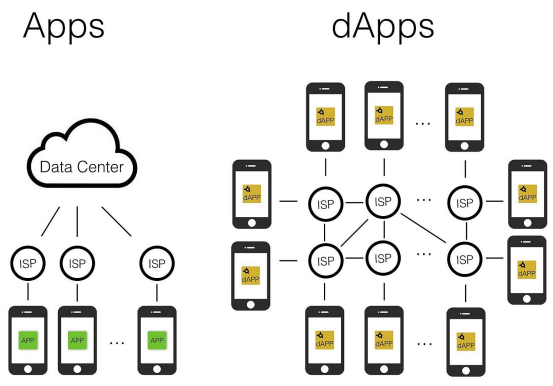
17th - Ethereum Dapp Development Bootcamp Powered by Blocklime

9:30 AM - 5:30 PM: Topics & Agenda

Registration	8:00AM - 9:00AM
Introduction to Blockchain and Dapps	9:00AM - 10:30AM
Break	10:30AM - 10:45AM
Smart Contracts & Solidity Language	10:50AM - 12:30PM
Lunch	12:30PM - 1:30PM
Web3.js & Truffle Introduction & Ganache & Let's Build a Dapp	1:35PM - 4:00PM
End & Networking Session	4:00PM - 5:00PM

What is DAPP ?

What is DAPP?



- DApp is an abbreviated form for decentralized application.
- A DApp has its backend code running on a decentralized peer-to-peer network. Contrast this with an app where the backend code is running on centralized servers.
- A DApp can have frontend code and user interfaces written in any language (just like an app) that can make calls to its backend.
- Furthermore, its frontend can be hosted on decentralized storage such as Swarm or IPFS.

Blockchains


Ethereum


Lisk


Neblio


Neo


Nem


Qtum


Stratis


Cardano


EOS


District 0x


Ethereum Classic

Aeternity

& Many More

0

DAPP?

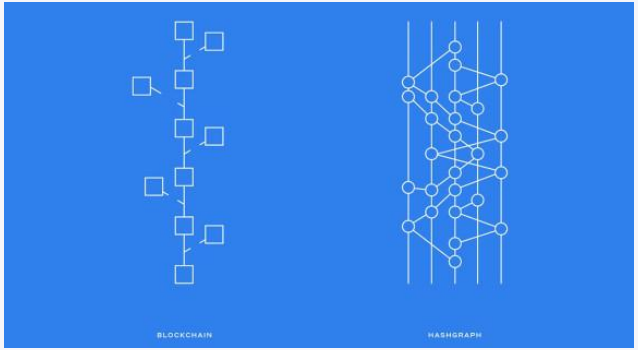
IPFS

swarm

Hedera Hashgraph

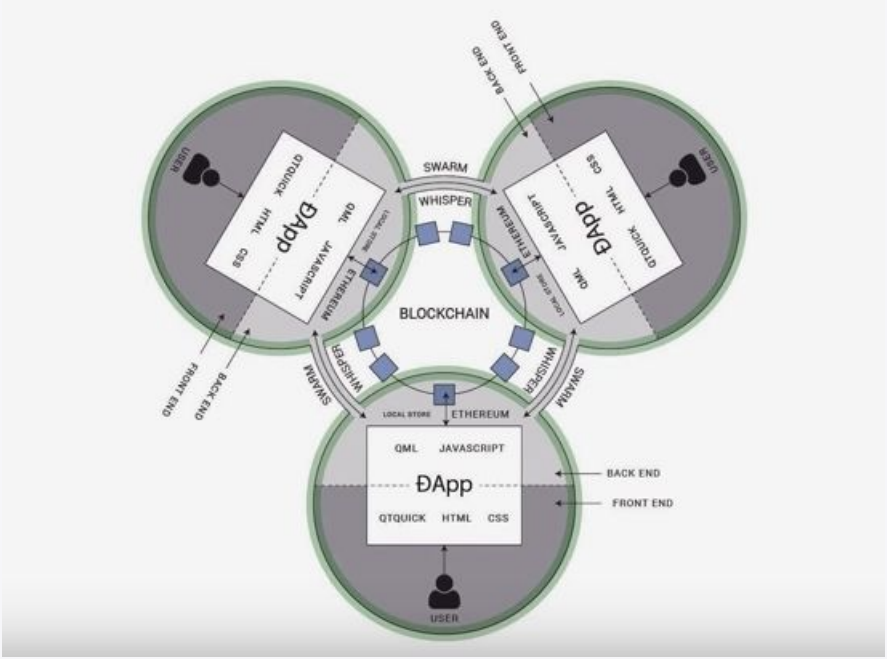
STORJ

sia

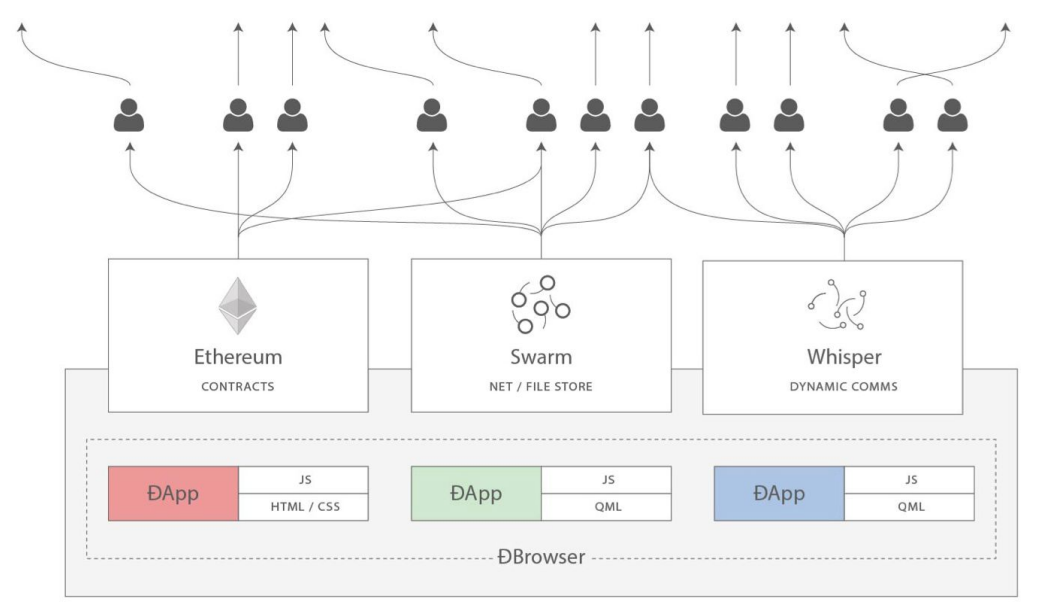


& Many More

Dapp in Ethereum



Dapp in Ethereum



1

Deep dive into Blockchain

Blockchain

From Wikipedia, the free encyclopedia

For other uses, see Block chain (disambiguation).

A **blockchain**,[1][2][3] originally **block chain**,[4][5] is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography.[1][6] Each block typically contains a cryptographic hash of the previous block,[6] a timestamp, and transaction data.[7] By design, a blockchain is resistant to modification of the data. It is "an

It's another data structure ☺

- *Me*

What is Blockchain Network?

- Form of distributed ledger technology (DLT)
- Key features of Blockchain Network
  - Distributed Network
  - Blockchain data structure
    - Asymmetric cryptography
    - Cryptographic hashing
  - Consensus Mechanism

Distributed Networking?

- Distributed networking is a distributed computing network system, said to be distributed when the **computer programming**, the **software**, and the **data** to be worked on **are spread out across more than one computer**, but they communicate, or are d**ependant upon each other**. Usually, this is implemented over a computer network.

  - Wikipedia

Asymmetric cryptography

- Pair key encryption system
  - Public Key
  - Private Key
- Public keys which may be disseminated widely, and private keys which are known only to the owner.

What is public key, private key and address?

Private Key – generated from large random numbers

Public Key – generated from private key

Address – generated from public key

Cryptography

- Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages

Hash Function

- It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert. The only way to recreate the input data from an ideal cryptographic hash function output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes.

SHA-256

Secure Hash Algorithm 2 (SHA) is a set of hash functions designed by NSA

- SHA-256 :
  - 32-bit words
  - Operations : And, Xor, Rot, Add (mod 232), Or, Shr
  - Output Size : 256 bits

What is consensus?

1

DEEP DIVE INTO BLOCKCHAIN

1

A consensus algorithm is a process in computer science used to **achieve agreement on a single data** value among distributed processes or systems. Consensus algorithms are designed to achieve **reliability** in a network involving multiple unreliable nodes. Solving that issue known as the consensus problem is important in distributed computing, blockchain and multi-agent systems.

1

A proof-of-work (PoW) system (or protocol, or function) is an economic measure to deter **denial of service attacks** and other service abuses such as **spam** on a network by requiring some work from the service requester, usually meaning processing time by a computer.

Other Consensus

- Proof - of - Stake (POS)
- Proof of importance (POI)
- Proof of Certificate (POC)
- Proof of Existence (POE)
- Delegated Proof of stake (DPOS)
- Resulted Delegated proof of stake (RDPOS)
- Practical byzantine fault tolerance algorithm (PBFT)

Types of Blockchain Network

- Public Blockchain Network
  - Bitcoin, Ethereum, Cardano & etc
- Private Blockchain Network
  - Monax, Multichain, Hyperledger
- Consortium Blockchain Network
  - Corda, R3 (banks), B3i (insurance), EWF (energy)

Types of Blockchain Network

	Public	Private/ Consortium
Access	Open Read/Write	Permissioned read and/write
Speed	Slower	Faster
Security	Consensus mechanisms (POW, POS, and Others)	Pre-approved participants
Identity	Anonymous Pseudonymous	Know Identities
Assets	Native Assets	Any assets

Access Types in Blockchain Network

Permissioned	Permissionless
Faster	Slower
Managed upkeep	Public ownership
Private membership	Open and transparent
Trusted	Trust-free
Legal	Not regulated / regulated/illegal

What are smart contracts?

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 contracts were first proposed by Nick Szabo in 1994.

What is a Oracles?

For smart contracts, oracles are a middleware product in which data outside of the blockchain (such as real world data from weather to stocks) is connected to it. That data is then used for conditions of smart contracts. Ethereum is self-contained, so oracles would allow smart contracts to branch out into real world applications by bringing the data to it.

An example of this would be sports betting, where a smart contract would be resolved by receiving the scores of a sporting event.

2

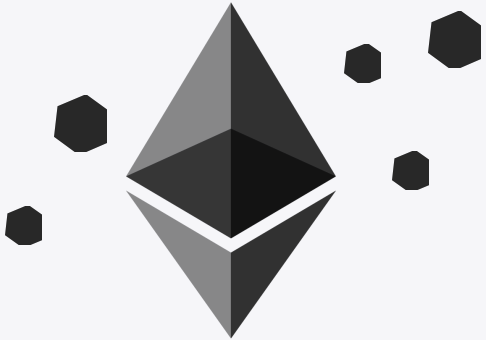
Ethereum Fundamentals

- What is Ethereum?
- What is Ether?
- What are the ether units?
- What is DAO?
- The ethereum development ecosystem
- What is Mist and How it works?
- What is Metamask?
- What is Remix?
- What is an account, a Faucet?

What is Ethereum?

- Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications (DAPPS).
- Ethereum is a blockchain network with Smart contracts :P

What is Ether?

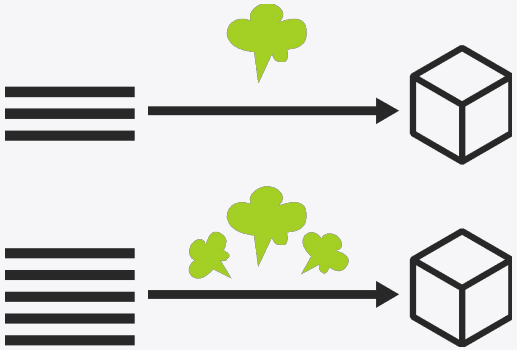


- Ether is a necessary element — a fuel — for operating the distributed application platform Ethereum.
- It is a form of payment made by the clients of the platform to the machines executing the requested operations.
- To put it another way, ether is the incentive ensuring that developers write quality applications (wasteful code costs more), and that the network remains healthy (people are compensated for their contributed resources).

What are Ether Units?

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

What is Gas?



Every operation that can be performed by a transaction or contract on the Ethereum platform costs a certain number of gas, with operations that require more computational resources costing more gas than operations that require few computational resources.

What is a DAO?

A decentralized autonomous organization (DAO), sometimes labeled a decentralized autonomous corporation (DAC), is an organization that is run through rules encoded as computer programs called smart contracts. A DAO's financial transaction record and program rules are maintained on a blockchain.

What are Wallets?

- Hot wallets
  - Luno, Binance, CoinHako and others...
- Cold wallets
  - Desktop wallet
  - Mobile Wallet,
  - Hardware wallets - Ledger, Trezor and others
  - Brain wallets
  - Paper wallets

Wallets (ext)

- Full-node wallet
  - Mist, Bitcoin wallet, Litecoin wallet and others
- Partial node wallet or Light node wallet
  - Parity, Mist and others
- API wallet
  - Metamask,Jaxx, Exodus and others

What is Ethereum Client?

What does the Ethereum client software do? You can use it to:

- Connect to the Ethereum network
- Explore Ethereum's blockchain
- Create new transactions and smart contracts
- Run smart contracts
- Mine for new blocks

Your computer becomes a 'node' on the network, running an Ethereum Virtual Machine, and behaves equivalently to all the other nodes. Remember in a peer-to-peer network there is no 'master' server and any computer has equivalent powers or status to any other. Example : GETH or Parity

What is Ethereum Virtual Machine?

The Ethereum Virtual Machine (EVM) is a simple but powerful, **Turing complete** 256 bit Virtual Machine that allows anyone to execute arbitrary EVM Bytecode. The EVM is part of the Ethereum Protocol and plays a crucial role in the consensus engine of the Ethereum system. It allows anyone to execute arbitrary code in a trust-less environment in which the outcome of an execution can be guaranteed and is fully deterministic.

Executing code within the Ethereum network takes time, and execution is generally pretty slow compared to other VMs. For every instruction, there's a cost associated, and an internal counter keeps track of the total cost, which is charged to the user. When a user initiates an execution through a transaction, they reserve some cash, which is the maximum amount they're willing to pay.

Development Ecosystem

- Clients
  - GETH & Parity
- Solidity IDE
  - Remix(Ethereum browser), ETHfiddle, Atom(solc compiler geth) and others.
- Explorers
  - Etherscan,Etherchain, Ethplorer and others
- Dev Wallets
  - Metamask, Mist, MyEtherwallet and others

Development Ecosystem

- **Ethereum Test Networks**
  - Rinkeby
  - Ropsten
  - Kovan
  - Morden - decommissioned
  - Local Testnet

Smart Contract Languages

- **Mutan,** a Golang-like language. It was deprecated in march 2015.
- **LLL,** a Lisp-like language. Still supported in core but hardly used.
- **Serpent,** a Python-like language Read the docs. However, it is no longer recommended to use.
- **Solidity** is very successful so far, other non-Ethereum projects also use it, Counterparty for instance.

- **Vyper - alpha stage**

What's coming up next on Ethereum

- Casper Protocol
- Plasma Protocol
- Sharding
- Raiden network
- Spank chain - side chain
- Loom network

Ethereum & Blockchain ecosystem Jargons

- **Mnemonic phrases**
- **Whisper -** p2p messaging protocol
- **Swarm -** p2p data storage protocol
- **RPC** - Remote Procedure Call
- **FORK -** (hard or Soft)
- **ERC -** Ethereum request for Comments Standards
- **EIP -** Ethereum Improvement Proposals

Blocklime
<ACADEMY/>

1260889-P
Blocklime Technologies Sdn. Bhd.

Q & A