BLOCKCHAIN
TRAINING ALLIANCE

GLOSSARY OF BLOCKCHAIN TERMS

ABI (Application Binary Interface)

An interface between two binary program modules, often one program is a library and the other is being run by a user

51% Attack

A situation in which a majority of miners in the blockchain launch an attack on the rest of the nodes (or users). This kind of attack allows for double spending.

Alt-coin

Any cryptocurrency that exists as an alternative to bitcoin

API

Application programming interface (part of a remote server that sends requests and receives responses)

Bitcoin

The first, and most popular, cryptocurrency based off the decentralized ledger of a blockchain

Blockchain (Public)

A mathematical structure for storing digital transactions (or data) in an immutable, peer-to-peer ledger that is incredibly difficult to fake and yet remains accessible to anyone.

Business logic layer

A part of code that determines the rules to be followed when doing business

Business network card

Provides necessary information for a user, entity or node to connect a blockchain business network

Casper

Consensus algorithm that combines proof of work and proof of stake. Ethereum is going to use casper as a transition to proof of stake.

CDN (Content Delivery Network)

Allows for a quick transition of assets needed to load internet content (html, js, css, etc.)

Centralized

Maintained by a central, authoritative location or group

Chaincode

A program that initializes and manages a ledgers state through submitted applications. It is the HyperLedger Fabric equal to Smart Contracts

Coin

Representation of a digital asset built on a new blockchain

Composer CLI

Hyperledger Fabric command line allowing for administrative tasks

Composer Rest Server

Generates a rest server and associated api from a deployed blockchain

Consensus

When a majority of participants of a network agree on the validity of a transaction

CRUD

Create,retrieve, update,delete

Cryptographic Hash Function

A function that returns a unique fixed-length string. The returned string is unique for every unique input. Used to create a "digital ID" or "digital thumbprint" of an input string.

Dapps

Decentralized Applications

DDos Attacks

A denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Decentralized

The concept of a shared network of dispersed computers (or nodes) that can process transactions without a centrally located, third-party intermediary.

Digital Asset

Any text or media that is formatted into binary source

Digital signature

A mathematical scheme used for presenting the authenticity of digital assets

Enum

Short for 'enumeration' - a fixed list of possible values. The list of US states could be considered an enum.

EOA

Externally Owned Account

ERC

Ethereum request for comments standard

Ethereum

Blockchain application that uses a built-in programming language that allows users to build decentralized ledgers modified to their own needs. Smart contracts are used to validate transactions in the ledger.

Fork

Alters the blockchain data in a public blockchain.

Gas (Ethereum)

Measures how much work an action takes to perform in ethereum

Genesis Block

The initial block within a blockchain.

Governance

The administration in a blockchain company that decides the direction of the company

Github

A web based hosting service for version control using git

Golang (Google language)

Created by google in 2009 golang is a programming language based on c

Gossip Protocol

A gossip protocol is a procedure or process of omputer-computer communication that is based on the way social networks disseminate information or how epidemics spread. It is a communication protocol.

Hard Fork

Alters the blockchain data in a public blockchain. Requires all nodes in a network to upgrade and agree on the new version.

BLOCKCHAIN TRAINING ALLIANCE

GLOSSARY OF BLOCKCHAIN TERMS

Hash function
A function that maps data of an arbitrary size

HYPERLEDGER
Started by the Linux foundation, hyperledger is an umbrella project of open source blockchains

Hyperledger Composer
Hyperledger Composer is Blockchain Application Development framework which simplify the blockchain application development on Hyperledger fabric

HYPERLEDGER FABRIC
Hyperledger project hosted by linux which hosts smart contracts called chaincode

IDE (Integrated development Environment)
Application for sofware developers that primarily consists of a source code editor, build automation tool, and debugger

Immutable
"unable to be changed" Data stored in a blockchain is unable to be changed.(not even by administrators)

Initial Coin Offering (ICO)
The form in which capital is raised to fund new cryptocurrency ventures. Modeled after an Initial public offereing (IPO). Funders of an ICO recieve tokens.

Instantiate(d)
To provide an instance of or concrete evidence in support of (a theory, concept, claim, or the like).

Invariant
a function, quantity, or property that remains unchanged when a specified transformation is applied.

IPFS
Inter Planetary File System

Merkle Tree
a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes.

Mining
The act of validating Blockchain transactions. Requires computing power and electricity to solve "puzzles". Mining rewards coins based on your computing power

Mining pool
A collection of miners who come together to share their processing power over a network and agree to split the rewards of a new block found within the pool.

Mist
Browser for installing and using Dapps

MSP (Membership Service Provider)
A Hyperledger Fabric blockchain network can be governed by one or more MSPs

Node
A copy of the ledger operated by a user on the blockchain

Nonce
A number only used once in a cryptographic communication (often includes a timestamp)

Nothing at Stake problem
This is caused by validator nodes approving all transactions on old and new software after a hard fork occurs

NPM (Node Package Manager)
Default package manager runtime environment node.js. NPM manages dependencies for an application

Oauth protocol
Open Authorization is a standard that is used by third party services to keep and distribute users information without exposing their password

Ommer (aka Uncle)
A block which has been completely mined but has not yet been added to the Blockchain.

On-chain governance
A system for managing and implementing changes to a cryptocurrency blockchain

Orderer Network
A computer network that allows nodes to share resources.

P2P (Peer to Peer)
denoting or relating to computer networks in which each computer can act as a server for the others, allowing shared access to files and peripherals without the need for a central server

PKI (Public Key Infrastructure)
A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Pragma(s) or Pragma-line
Defines which compiler version the smart contract uses

Private Blockchain
Blockchain that can control who has access to it. Contrary to a public blockchain a Private Blockchain does not use consensus algorithms like POW or POS, instead they use a system known as byzantine fault tolerant(BFT). BFT is not a trustless system which makes a BFT system less secure.

Proof of Activity
Active Stakeholders who maintain a full node are rewarded

Proof of Burn
Miners send coins to an inactive address essentially burning them. The burns are then recorded on the blockchain and the user is rewarded.

Proof of Capacity
Plotting your hard drive (storing solutions on a hard drive before the mining begins). A hard drive with the fastest solution wins the block

Proof of elapsed time
Consensus algorithm in which nodes must wait for a randomly chosen time period and the first node to complete the time period is rewarded

Proof of Stake (POS)
A consensus algorithm that chooses the owner of a new block based on the wealth they have or (Stake). There is not a block reward so the forgers take the transaction fee.

BLOCKCHAIN
TRAINING ALLIANCE

GLOSSARY OF BLOCKCHAIN TERMS

Proof of Work (POW)

A consensus algorithm which requires a user to "mine" or solve a complex mathematical puzzle in order to verify a transaction. "Miners" are rewarded with Cryptocurrencies based on computational power.

Pub/Sub

Publish/Subscribe

Public key cryptography

Encryption that uses two mathematically related keys. A public and private key. It is impossible to derive the private key based on the public key.

REST API (representational state transfer API)

Defines restraints based on http

RPC (Remote Procedure Calls)

A protocol that is used from one program to request a service on another program located on a network

SDK

A software development kit provides the necessary tools for a developer to create software on a specific platform

Sharding

Dividing a blockchain into several smaller component networks called shards capable of processing transactions in parallel.

Smart Contract

Self executing contract with the terms of agreement written into the code

Token

Representation of a digital asset built on an existing blockchain

Turing Complete language

A language that is able to perform calculations that a computer is capable of

Ubuntu

Free open source operating system and linux distribution

UTXO (Unspent Transaction Outputs)

Unspent transaction outputs are used to determine whether a transaction is valid

VIPER

A programming language created to be a formal introduction to smart contracts

Virtual Machine

Emulation of a computing system

Wallet

Stores the digital assets you own.

Zeppelin (or Open Zeppelin)

Community of like minded Smart Contract developers

Distributed Ledger

A database held and updated independently by each participant (or node) in a large network. The distribution is unique: records are not communicated to various nodes by a central authority

DAOs

A decentralized autonomous organization is an organization that is run through rules encoded as computer programs called smart contracts.

Oracles

An agent that finds and verifies real-world occurrences and submits this information to a blockchain to be used by smart contracts.

Solidity

A contract-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms.