BLOCKCHAIN

TRAINING ALLIANCE

WHAT IS BLOCKCHAIN?

What you need to know

Blockchain Defined

- In its simplest form, blockchain is a distributed database

- Blockchain is defined not only by what it is but why it's important:
  - Global, peer to peer, and distributed record of transactions
  - Highly secure and trustless

© Copyright 2017 | All Right Reserved

Blockchain as a distributed database

What you need to know

Database

- Data is information
  - Numbers, Images, Videos, etc.
- Databases are often used to securely store data
  - Usernames and passwords
  - Account information
- Banks use databases
  - Securely store account balances behind a login
- Databases are like a ledger in that it is a record of data

© Copyright 2017 | All Right Reserved

Island of Yap

- The stones themselves had no non-monetary value
- Eventually, spending your stones didn't require physically moving the stone – just acknowledgement of a change of ownership
- Impossible to do a trade in secret
- They developed a form of distributed ledger, but...
- It couldn't scale!

© Copyright 2017 | All Right Reserved

Distributed Ledger

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Distributed Database

- Why can't the Yapese system be used today?
  - Storing a mental ledger of every transaction between millions of people is impossible
- Databases are similar to ledgers but are kept digitally and often store huge amounts of data
- Distributed Database
  - Blockchain took the idea of a distributed ledger and applied it to a database

© Copyright 2017 | All Right Reserved

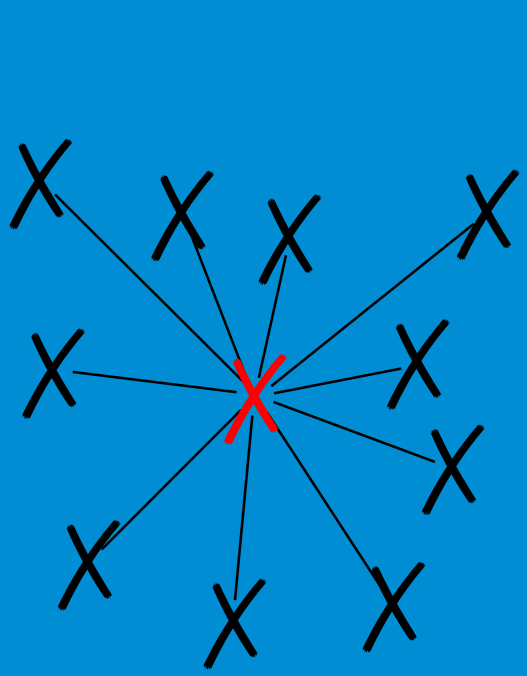
A BLOCKCHAIN IS AN IMPLEMENTATION OF A LEDGER

- Ledgers record transactions - the passing of value from owner to owner
- Transactions are time based
- Once a Txn is recorded you can't alter them (append only)
- You need to be able to detect if your ledger has been altered

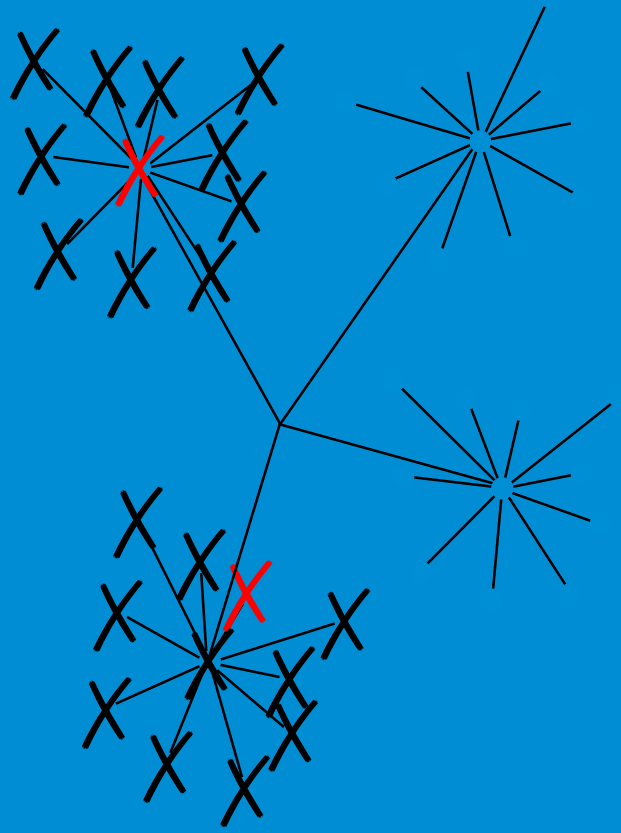
A blockchain is a protocol for building an immutable historical record of transactions

© Copyright 2017 | All Right Reserved

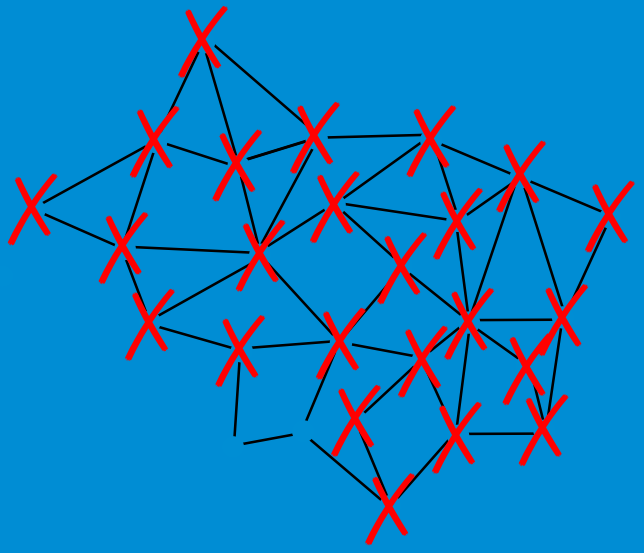
NETWORK EVOLUTION



i) centralized



iii) distributed



ii) decentralized

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Why Use Blockchain?

Advantages it may provide

Why use Blockchain?

- Blockchain is distributed
- A distributed database is:
  - Secure
  - Peer to Peer
  - Trustless
  - Transparent

© Copyright 2017 | All Right Reserved

Blockchain is Fault Tolerant

- Blockchain does not have a single point of failure
- Imagine a group text
  - Everyone in the group message has a record of every text sent in that group message
  - In order to delete the history of that group message everyone in the group must delete the record

© Copyright 2017 | All Right Reserved

Blockchain is Immutable

- Cannot be changed
- The history of a blockchain is constantly compared ensuring that data has not been tampered with
- Append only

© Copyright 2017 | All Right Reserved

Blockchain is
Immutable

- **EDX Video: Immutability**

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Blockchain is Trustless

- Blockchain eliminates the need for trust
- This trustless system is achieved through mechanisms by which all parties can achieve consensus on what the canonical truth is
- Allowing the public to view data could be advantageous for a business
  - Transparency shows honesty

© Copyright 2017 | All Right Reserved

Blockchain is Transparent

- Data in a blockchain can be read by the public
- Transparency of data is partially why blockchains are trustless
  - If data is completely transparent we can trust that actors are being honest

© Copyright 2017 | All Right Reserved

Blockchain is Transparent

- **EDX Video: Disintermediation - Trust Through Transparency**

© Copyright 2017 | All Right Reserved

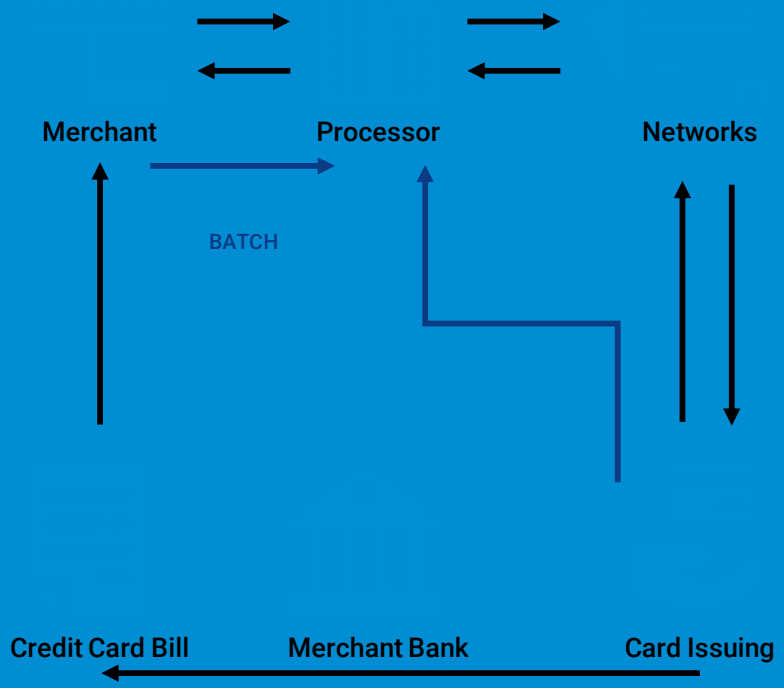
Blockchain is
Peer to Peer

- P2P - System of computers that can communicate directly without the need of a third party or intermediary
- Traditional databases are kept by trusted third parties like banks
- Distributed databases are kept on multiple computers and updated on multiple computers

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

ELECTRONIC MIDDLEMEN



Observations:

- Requires 3rd party trust
- The more complex the flow, the more middlemen required
- Specialized equipment needed (e.g. POS terminal, connection to Txn networks
- Fraud detection by 3rd parties
- Every step adds cost

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

MIDDLEMEN ADDING VALUE

- Provision of infrastructure
  (Terminals, network connections, etc.)
- Management of commercial relationships between parties
  (Lots of lawyers)
- Abstraction of complexity
- Fraud detection
- Customer service
- Regulatory compliance KYC, AML, Risk reporting
- Removal of bad-actors from the ecosystem

Until now, this is the best way we've been able to achieve the goal of person-to-person transactions at a distance.

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

How it Works

What you need to know

Block

- EDX Video let’s Cover the basics

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Block

- A Block contains:
  - Transaction data (in the form of a merkle tree)
  - Previous block header hash
  - Timestamp of when the block is added
- A block is summed up with a header hash which is a hash of the block data

© Copyright 2017 | All Right Reserved

How blocks are chained together

- Data from the previous block is included in every block
- This link creates the immutable, append only nature of a blockchain

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Cryptography

- **Video: Cryptography Basics**

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Hashing

- Hash Function
  - One way function
  - Takes any input of any size converts it to a unique 20 digit code
  - If any input data were to be changed the output would be completely different
- Hashing is used to compare entire database
  - Millions of nodes only need to compare 20 digits

© Copyright 2017 | All Right Reserved

HASH FUNCTIONS

'A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or hashes.'

There are many types, but Bitcoin uses SHA256; output is 256bits of data, or 64 hexadecimal characters

© Copyright 2017 | All Right Reserved

HASHING PROPERTIES

- Any size of data always results in the same length hash
- Slight changes of input data gives totally different hashes
  - ‘Hello World’ = a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
  - ‘Hello World!’ = 7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069
- The same input always produces the same output
- Hashes are ‘one way’

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

HASHING USAGES

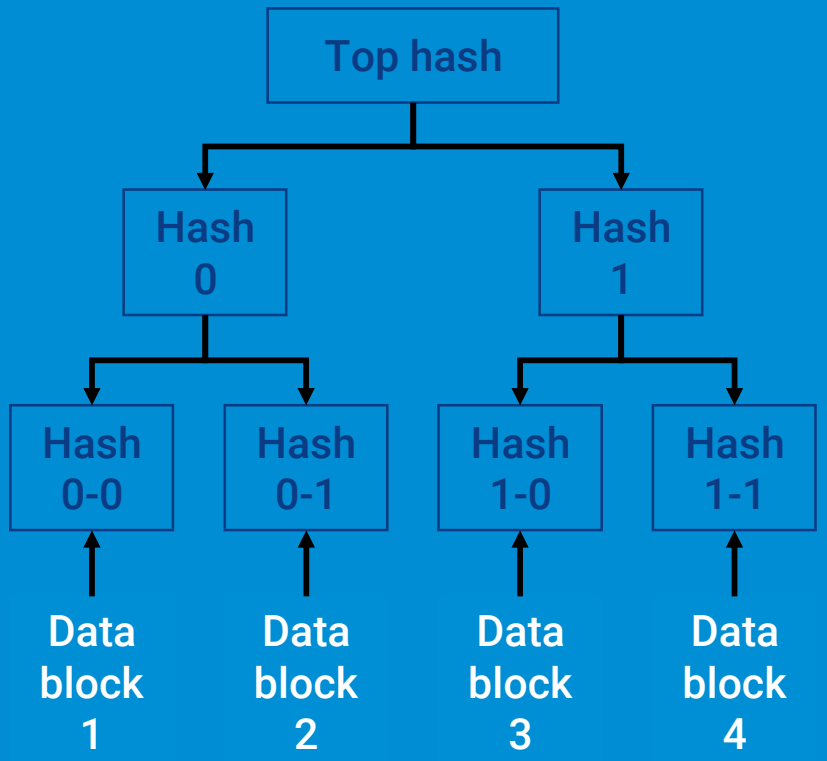
- To record a value while hiding the original value (e.g. a password)
- To verify the integrity of some data (store the hash, to check the data, hash it again and compare the values; should be the same hash value)
- To prove you've done calculations (generating hashes takes computing power)

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

MERKLE TREE - HASH OF HASHES

- Multiple blocks of data, in a certain order, into a single hash
- Allows you to work out which block has changed



BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

MERKLE TREE - HASH OF HASHES

- **EDX Video: Merkle Tree**

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Consensus in Distributed Networks

- In order to update the ledger, the network needs to come to consensus using an algorithm
- Consensus: what does it mean to come to consensus on a distributed network?
  - It means that everyone agrees on the current state (e.g. how much money does each account have) and making sure that no one is double-spending money (easy in Bitcoin, more complex in Ethereum, business networks)
- How do we come to consensus in this distributed manner?

© Copyright 2017 | All Right Reserved

Key Blockchain Concepts

- Public-private networks
  - Trustless vs trusted
- Distributed network
- Consensus algorithms
- Immutability

- Blockchain: trustless, distributed (peer-based), consensus-driven, immutable

© Copyright 2017 | All Right Reserved

Blockchain for Business

One of the fastest-moving technology adoptions

Permissioned Blockchains

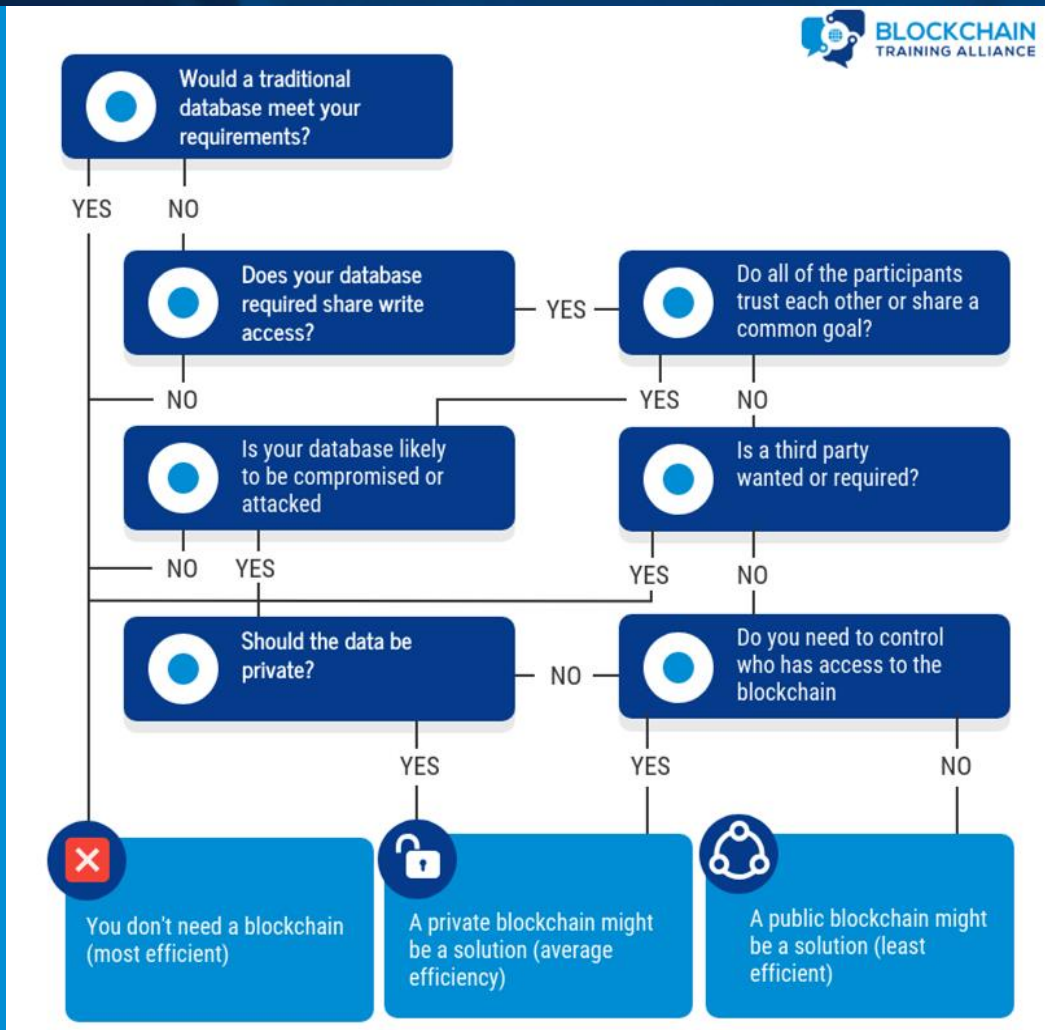
- **Video: Public (Permissionless) Blockchains**

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Blockchain Decision Chart

- Blockchain is not always a good alternative
- There are many things to consider



BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Blockchain is like hot Sauce

- edX Blockchain is like hot sauce

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Smart Contracts

- Video Smart Contracts

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

What do Smart Contracts Provide

- Autonomy
- Efficiency
- Backup
- Accuracy
- Cost Savings

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

BLOCKCHAIN VS DATABASE

DISTRIBUTED

HIGHLY SECURE
1

Blockchain is immutable and fault tolerant. Meaning it cannot be changed or altered

APPEND ONLY:
2

Transactions in a blockchain can only be added and read

PEER TO PEER:
3

Blockchain allows for peers to transact without the need of a third part or intermediary but at the cost of efficiency

CENTRALIZED

VULNERABLE
1

A single point of failure leaves a database vulnerable to attacks

CRUD:
2

Transactions in a database can be created, read, updated, and deleted

INTERMEDIARIES
3

Trust in a third party is required which could lead to dishonest or falsified transactions as well as transaction costs.

BLOCKCHAIN TRAINING ALLIANCE

Blockchain in Bitcoin

Blockchain’s breakout use Case

PARALLELS TO THE INTERNET

Blockchains today have been likened to the Internet in 90s.

- Similar investment levels
- Similar excitement levels
- Similar visions of potential uses

History doesn't repeat, but it rhymes: We expect similar...

- Similar path to maturity – people, tools, process
- Similar adoption curve (perhaps faster)
- Evolution of protocol/services built on blockchains (perhaps faster)

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Banking, the Centralized Industry

- Intermediaries (Banks)
  - Vulnerable to attacks
  - Possible dishonesty
- Banking industry became centralized
  - Caused by lack of alternatives in banking
  - Led to possibility of high transaction fees

© Copyright 2017 | All Right Reserved

Double-Spending

Cleverly combined software components

- Distributed Systems
- Peer-to-peer networks
- Hashing functions
- Public - Private key cryptography
- Cryptographic signatures
- Elliptic curve cryptography

© Copyright 2017 | All Right Reserved

Bitcoin
Anonymity

- Decentralized application would solve:
  - Transaction fees
  - Dishonest intermediaries
  - Cyber Attacks
- Decentralized apps require:
  - Data that is open to the public
  - Financial data should never be public
- Anonymity public key cryptography
  - A way to keep data public without user identity being revealed

BLOCKCHAIN TRAINING ALLIANCE
© Copyright 2017 | All Right Reserved

PUBLIC/PRIVATE KEY CRYPTO

- 2 uniquely related cryptographic keys (Public Private)
- Public key is derived from private key
- Public key is the public address associated with transactions
- Private key is private for your eyes only
- Impossible to find private key based on public key

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

PUBLIC/PRIVATE KEY CRYPTO

- **Private/Public Key Cryptography**

© Copyright 2017 | All Right Reserved

Cryptographic Identity

- To use the network, need a Cryptographic Identity
  - (sort of like an email address)
  - If want to access your email, you need the password, which functions similarly to a private key and your public key is like your address (more complicated)
- Authentication: peers sign transactions with their cryptographic identity, this enables account "ownership" and can attribute blame

BLOCKCHAIN TRAINING ALLIANCE
© Copyright 2017 | All Right Reserved

DIGITAL SIGNATURES

- Verify the messages came from the correct person
- Verify the messages hasn’t been changed or tampered with
- Can be used to prove that you have the private key
- Main aim is confidence in identity (in messaging)

© Copyright 2017 | All Right Reserved

Bitcoin Consensus
Proof of Work

© Copyright 2017 | All Right Reserved

Proof of Work Demo

- **EDX Video Proof of work hashing demo**

© Copyright 2017 | All Right Reserved

Three Primary Consensus Algorithms

- POW: Proof of Work (Bitcoin)
  - Expensive, not ecological, wasteful computation
- POS: Proof of Stake (Ethereum)
- Next-gen: PBFT: Practical Byzantine Fault Tolerance (DFINITY, Algorand)
  - Law of large numbers: **diversity of participants**
  - For each block of transactions, randomly select a small, one-time group of users in a safe and fair way
  - To protect from attackers, the identities of these users are hidden until the block is confirmed

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

What is Bitcoin mining?

Run the software yourself:

bitcoin / bitcoin

Mining is the accounting function to record transactions, fee-based ($130,000/block each 10 min)

Mining ASICs “discover new blocks”

- Mining software makes nonce guesses to win the right to record a new block (“discover a block”)
  - At the rate of 2^32 (4 billion) hashes (guesses)/second
- One machine at random guesses the 32-bit nonce

Winning machine confirms and records the transactions, and collects the rewards

- All nodes confirm the transactions and append the new block to their copy of the distributed ledger

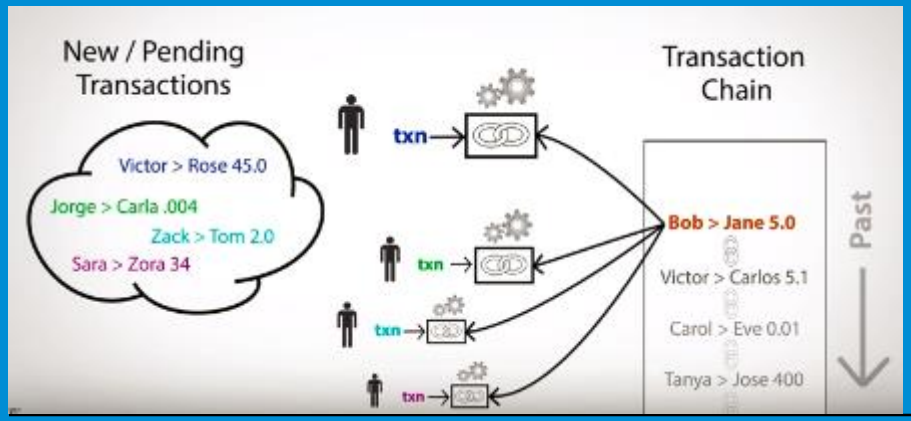
“Wasteful” effort deters malicious players

Fast because ASICs represent the hashing algorithm as hardware

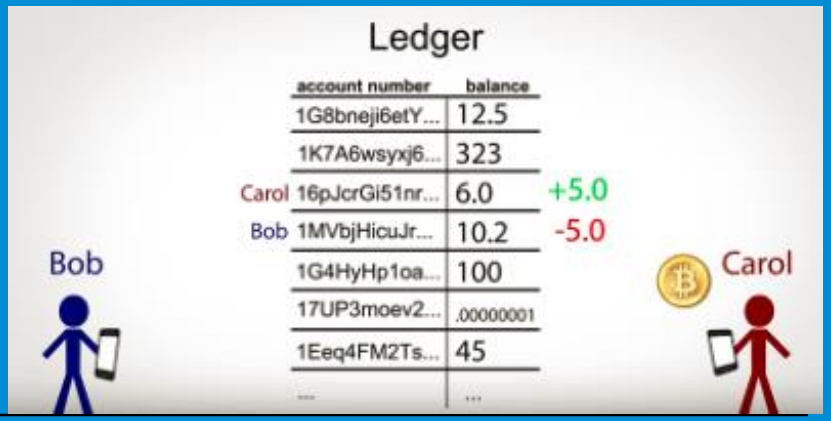
BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

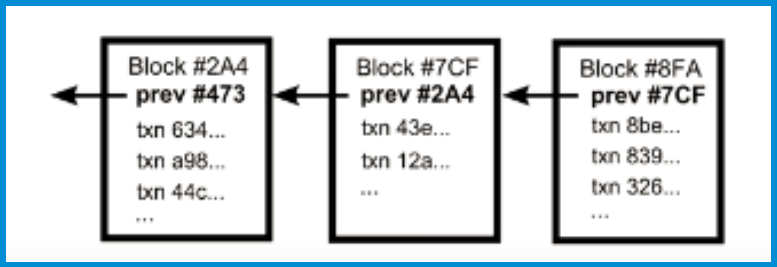
P2P network confirms & records transactions



Transactions submitted to mempool, and miners assemble new batch (block) of transactions each 10 min



Transaction computationally confirmed
Ledger account balances updated



Each block includes a cryptographic hash of the last block, chaining the blocks, hence “Blockchain”

Peer nodes maintain distributed ledger

Source: https://www.youtube.com/watch?v=t5JGQXCTe3c

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Blockchain Recap

- **Blockchain is a _____ Database.**
  - **Distributed**
  - **Fault Tolerant**
  - **Immutable**
  - **Highly Secure**
  - **Trustless**
  - **Scalable**

© Copyright 2017 | All Right Reserved

BLOCKCHAIN CONCEPTUAL OVERVIEW

The blockchain is:

- Decentralized
- Immutable
- Transparent
- Disintermediated
- Consensus-based

Use Cases

Blockchain Applications

Who is using Blockchain? EDX Video

- **EDX Video: Who Is Using Blockchain?**

© Copyright 2017 | All Right Reserved

Potential Use Cases

- Voting
- Music
- Law
- Healthcare
- Identity Management
- Land Records
- Supply Chain
- IoT
- Energy

© Copyright 2017 | All Right Reserved

Voting

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Music

© Copyright 2017 | All Right Reserved

Law Enforcement

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Healthcare

© Copyright 2017 | All Right Reserved

Identity Management

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Land Records and Government

© Copyright 2017 | All Right Reserved

Supply Chain

© Copyright 2017 | All Right Reserved

Internet of Things

BLOCKCHAIN TRAINING ALLIANCE

© Copyright 2017 | All Right Reserved

Energy

© Copyright 2017 | All Right Reserved

Questions?

THANK YOU

...

© Copyright 2017 | All Right Reserved

BLOCKCHAIN
TRAINING ALLIANCE