



BLOCKCHAIN
TRAINING ALLIANCE



Blockchain Introduction

www.blockchaintrainingalliance.com



© Copyright 2021 | All Rights Reserved



What is Blockchain?

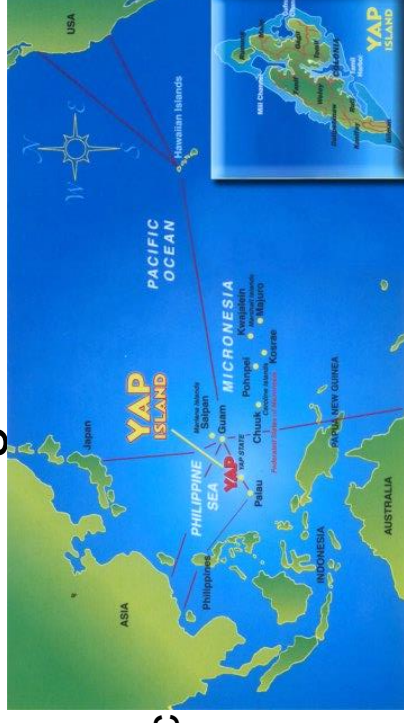
Chapter One

What is Blockchain?



❖ To understand D.L.T., we need to go back in time

- 1000 BC
- Small island in South Pacific
- Yap Island



➤ The Yapese people had a very unique form of currency

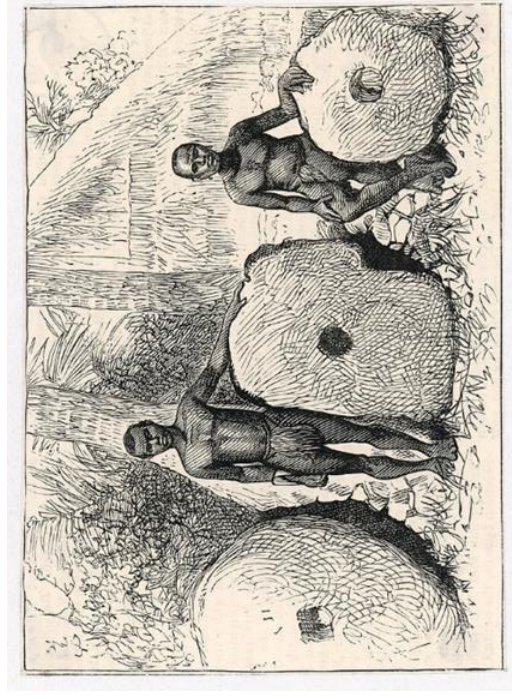
➤ Rai Stones – 12’/3-4m tall, 8,000lbs/3500+kg!!

What is Blockchain?



❖ What happens when money can't be *physically* traded?

- A ledger is kept
 - A ledger is a recording of all transactions
 - The ledger records:
 - What was exchanged?
 - Who exchanged it?
- Stones or coins do not have to be physically traded
- Their ownership can be tracked on a ledger



What is Blockchain?



- ❖ How did the Yapese manage the ledger?
- ❖ **Decentralized Ledger**
 - All tribe members keep a copy of the ledger in their head
 - Everyone knew who owned which Rai stone at any time
- ❖ When two parties wished to transact, the would **announce** their transaction to the tribe
- ❖ When a transaction was announced, all tribe members updated their mental ledger

Let's Review an Example

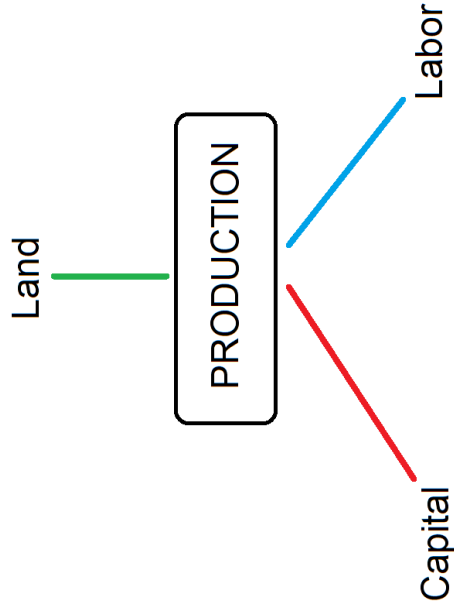


- ❖ Alice agrees to trade Bob her stone by the pond in exchange for all of his cattle.
- ❖ Alice and Bob announce their transaction to the tribe.
- ❖ Everyone updates their mental ledger. From this point on, they agree that the coin by the pond is owned by Bob until he trades it.

What is Blockchain?



- ❖ **Centralization** feels natural because we've lived our entire lives in an **industrial or post-industrial age**



What is Blockchain?



- ❖ If we had to solve this problem today, we would likely appoint a single person to manage the ledger
 - ❖ A banker
- ❖ This approach has a huge advantage – efficiency!
- ❖ However, several problems must be mitigated:
 1. The banker must be trustworthy
 2. The banker must protect the ledger
 3. The banker must be highly available
 4. The banker must not make mistakes

What is Blockchain?



- ❖ A note on efficiency...
- ❖ The long-standing value proposition of technology (for the enterprise) has been a gain in efficiency (*do more with less*).
- ❖ Technologists are the agents tasked with locating and purging inefficiency from the organizational landscape.
- ❖ Accepting (and embracing) a ***highly inefficient*** approach feels ***very strange***...
- ❖ For now, just accept that blockchain is ***extraordinarily inefficient***, and ***that's okay***. 😊

What is Blockchain?



- ❖ In the world of permissionless blockchain, truth is determined by *Group Consensus*
- ❖ The truth is always assumed to be what the majority of participants believe it to be.
- ❖ Group Consensus == Police Detective
- ❖ Side Note – Permissioned blockchain platforms such as Hyperledger rely on *Participant Consensus* to determine the truth

What is Blockchain?



- ❖ A decentralized ledger provides many of the same services as a bank.
- ❖ Example - Separation of possession and ownership



- One day a ship carrying a new coin back to the island sank in the harbor
- The tribe decided to add it to the ledger and trade it just like any other coin
- Possession does not equal ownership

Centralized vs Decentralized Ledger



- ❖ Decentralized Ledger == Bank
 - Decouples possession and ownership
 - Take deposits, issue credits
 - Provides a trust-able ledger to all parties
 - Acts a trust broker when two parties who don't trust each other want to trade

What is Blockchain?



Internet

Email
Streaming Media
Social Media



Blockchain

Bitcoin
Identity Management
???

Questions?

...

Why not use the Yapese system today?

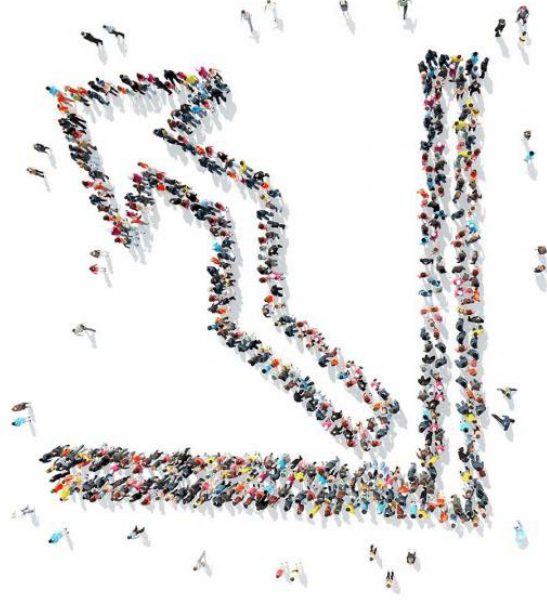


❖ Scalability

- Humans can only remember a small number of transactions mentally
- Even with pencil and paper, limited in how far could scale up system

❖ Privacy

- On Yap Island everybody knew the personal net worth of everyone else
- This is not plausible for modern society



Why not use the Yapese system today?



❖ Scalability

- Despite the advantages presented by taking a decentralized approach, technology just hasn't been good enough (until very recently) to allow us to pursue decentralized solutions at scale.

1982		2017		WHAT'S DIFFERENT?	
					
APPLE II <i>plus</i>		APPLE iMAC 21.5"			
48 KILOBYTES	MEMORY	8 GIGABYTES		166,666x MORE	
1 MHZ	CPU SPEED	1.6 GHZ		1600x FASTER	
140 KILOBYTES	STORAGE	1 TERABYTE		7,508,684x MORE	
\$1695 (WITH DRIVE)	PRICE	\$1099		3.9x LESS	

Why not use the Yapese system today?



 FORD MUSTANG 4CYL		 FORD MUSTANG ECOBOOST 4CYL	
22 MPG	MPG	20 MPG	0.9x LESS
16.2 SEC	0-60 TIME	5.5 SEC	2.9x FASTER
88 HP	HORSEPOWER	310 HP	3.5x MORE
\$6789	PRICE	\$26,195	1.5x MORE

Why not use the Yapanese system today?



SO,

IF CARS DEVELOPED AT THE PACE OF COMPUTERS,
A 2017 FORD MUSTANG ECOBOOST WOULD HAVE:

 **660,764,192 HP**
GET FROM 0-60 IN **0.0034 SEC**
GET ABOUT **3,666,652 MPG** AND COST **\$4,471**

BUT,

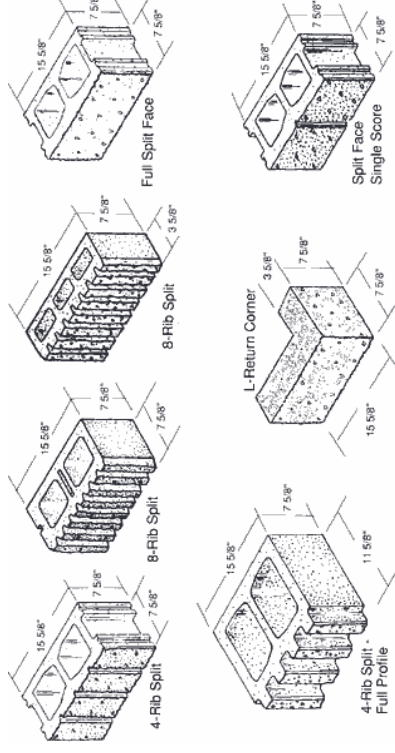
IF COMPUTERS DEVELOPED AT THE PACE OF CARS,
A 2017 APPLE IMAC 21.5" WOULD HAVE:

 **43.2K** OF RAM MEMORY,
WOULD RUN AT **2.9MHz**
WOULD BE ABLE TO STORE **490K** OF DATA
AND WOULD COST **\$6,529**

Mechanics of Blockchain



- ❖ What is a “block”?
 - Let’s say all transactions are recorded on paper
 - Each sheet of paper has 25 lines
 - When a sheet is filled, the tribe will “validate” the transactions on the current page
- Do we all agree with the data on the page?



Mechanics of Blockchain



- ❖ Once the page has been validated, it is added to a stack of previously validated sheets
 - Each sheet on the stack can be assumed to be trustworthy
 - Once a sheet is validated it can't be changed due to cryptographic linking. More to come...



Mechanics of Blockchain

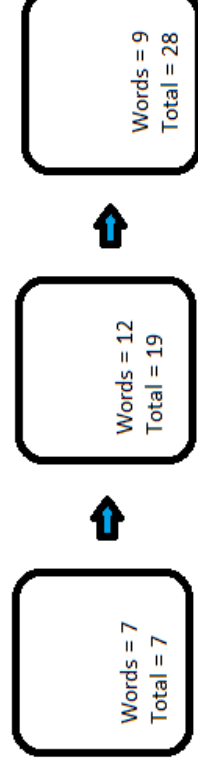


- ❖ How are blocks “chained” together?
 - Blocks are linked using cryptographic hashing
 - Each block is data is dependent on the data that comes before it to generate the proper hash.
 - Changing any data breaks this link going forward.

Mechanics of Blockchain



- ❖ How are blocks “chained” together?
 - Imagine a rule:
 - The number of words on each page is counted.
 - This number is added to the previous total.
 - The new total is written on the bottom of the page.
 - Changing data will break the word count going forward.

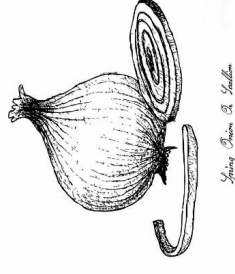


What is Blockchain?



❖ Three Types of "Transactions"

- Two or more parties, exchange of monetary value
 - Cryptocurrency
 - Most familiar
- Peel back the idea of monetary exchange
 - Two or more parties, but no exchange of monetary value
 - Update to medical records, notary services
- Peel back the idea of two or more parties
 - One party "announcing" an important "event"
 - Supply chain management, business process automation



Blockchain is...



- ❖ An event tracking system – announcements mark events
- ❖ Events can be actionable (Smart Contracts)
- ❖ Smart Contracts make a workflow platform
 - Write rules around events

History of Blockchain



- ❖ Bitcoin – 2009
 - ❖ Ledger used to track the history of one asset – Bitcoin
 - ❖ Single, shared ledger
 - ❖ Blockchain 1.0 – Just a ledger, nothing more...
 - ❖ Anonymous and fully-transparent
 - ❖ Primary Focus: A ledger to enable and facilitate digital payments



History of Blockchain



Transaction View information about a bitcoin transaction

967c3d317c2cbee6e7f902bfc25eaa0f433ec12985dd073552cf4aad0384a0e

17QrQKaWKxwauF1RsPGsMWydGex1yJnRX

1C4jGmwpCoLL8ub57W6j3hTqSzQJUKZrP

4 Confirmations

0.04848376 BTC

0.04848376 BTC

Summary	
Size	191 (bytes)
Weight	764
Received Time	2019-05-22 15:33:26
Included In Blocks	577257 (2019-05-22 15:43:51 + 10 minutes)
Confirmations	4
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.0489428 BTC
Total Output	0.04848376 BTC
Fees	0.00141052 BTC
Fee per byte	738.492 sat/B
Fee per weight unit	184.623 sat/WU
Estimated BTC Transacted	0.04848376 BTC

Scripts

Show scripts & coinbase

History of Blockchain






- ❖ Ethereum – July 2015
 - ❖ Ledger used to track the history of Ether
 - ❖ Ledger can also be used to track ANY other asset, not just Ether!
 - ❖ Single, shared ledger
 - ❖ Blockchain 2.0 - Smart Contracts and the EVM
 - ❖ Program your own logic for how events should be handled
 - ❖ Blockchain as a workflow / BPM solution
 - ❖ ERC20 token standard
 - ❖ Standard architecture for tokenizing any type of asset
 - ❖ Anonymous and fully-transparent
 - ❖ Primary Focus: A platform to build consumer applications on



ethereum

History of Blockchain



Overview	State Changes	New	Comments
Transaction Hash: 0x831fd26634e7dad3852797a1d3358e70619f9a0e451ce77fa3899261614d1d1d 			
Status:	<div>Success</div>		
Block:	7810580 <div>3 Block Confirmations</div>		
Timestamp:	⌚ 1 min ago (May-22-2019 03:59:45 PM +UTC)		
From:	0xc24cb5d8890d2e0dbce4d91f73e2d243c4a890c 		
To:	0x219466a5a45ada2be276e0fa3e7e2c706ca832bc 		
Value:	4.90047421 Ether (\$1,257.02)		
Transaction Fee:	0.000378 Ether (\$0.10)		

History of Blockchain



Overview

Event Logs (1)

State Changes

[This is a Ropsten Testnet Transaction Only]

Transaction Hash:

0xbdb369501ef3ba2a61309b2593783558c597857ee4360f8e17934630b9c04c59

Status:

Success

Block:

3978391

1770659 Block Confirmations

Timestamp:

274 days 14 hrs ago (Aug-21-2018 01:51:41 AM +UTC)

From:

0x1f787c16c636143446076b76b6374e993e2467

To:

Contract 0xc22e0dbb3c9a54942396a01ecb61949b1bd609ca8

Value:

0 Ether (\$0.00)

Transaction Fee:

0.000139774 Ether (\$0.000000)

Gas Limit:

550,000

Gas Used by Transaction:

139,774 (25.41%)

Gas Price:

0.000000001 Ether (1 Gwei)

Nonce

Position

863

16

Input Data:

e04[Cooltest Person in Mike's ClassOksana Davis

History of Blockchain



- ❖ Hyperledger – December 2015
 - ❖ No native currency
 - ❖ Ledger can be used to track any kind of asset
 - ❖ Multiple ledgers
 - ❖ Blockchain 2.0 – Chaincode (aka Smart Contracts)
 - ❖ Identity and Permissioning
 - ❖ Primary Focus: A platform for building cross-organizational enterprise applications on



HYPERLEDGER

History of Blockchain



```
1 [{"class": "org.hyperledger.composer.system.AddParticipant",
2  "resources": [
3    {
4      "class": "org.acme.vehicle.auction.Member",
5      "balance": 0,
6      "email": "alice@abc.com",
7      "firstName": "Alice",
8      "lastName": "Johnson"
9    }
10  ],
11  "targetRegistry": "resource:org.hyperledger.composer.system.ParticipantR",
12  "transactionId": "f01890fd-8b01-49b3-adf9-1b3533119ecf",
13  "timestamp": "2019-05-22T17:39:52.673Z"
14 }]
```


Questions?
THANK YOU
...