BLOCKCHAIN

TRAINING ALLIANCE

BLOCKCHAIN
TRAINING ALLIANCE

# BLOCKCHAIN

## What is Blockchain

www.blockchaintrainingalliance.com

© Copyright 2017 | All Right Reserved


LETS START
AT THE BEGINNING
No prior knowledge of blockchains required
We'll be looking at Bitcoin, but mostly talking Blockchain
Start with a simplified overview of how it all works, then dive deeper into each section

# OVERVIEW

- Class time: (2 pm – 6 pm)
- 6 modules organized into
  - 45 minute sessions
  - 5 min Q&A (flexible)
  - 10 minute break
  - Start at top of the hour
  - Instructor available for additional Q&A at

Do you want to add text?

The premium Edit a PDF tool lets you m
images in PDF files.



© Copyright 2017 | All Right Reserved

# INTRODUCTION & PRIMER

## What you need to know

# What is Blockchain?

- **Blockchain technology is a software; a protocol for the secure transfer of unique instances of value (e.g. money, property, contracts, and identity credentials) via the internet without requiring a third-party intermediary such as a bank or government**
  - **Email over IP, Voice over IP, Money over IP**



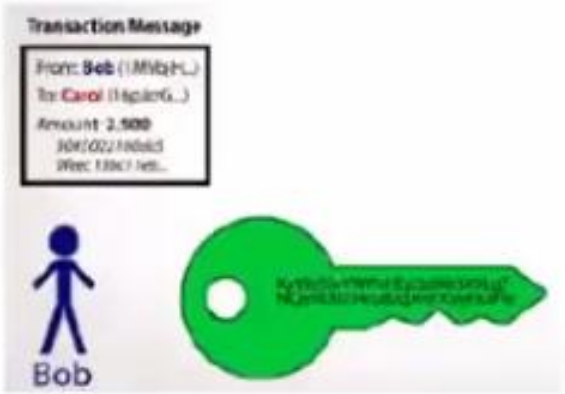
© Copyright 2017 | All Right Reserved

*How does Bitcoin work?*

# Use eWallet app to submit transaction


Scan recipient's address
and submit transaction


$ appears in recipient's eWallet




Wallet has keys not money
Creates PKI Signature address pairs

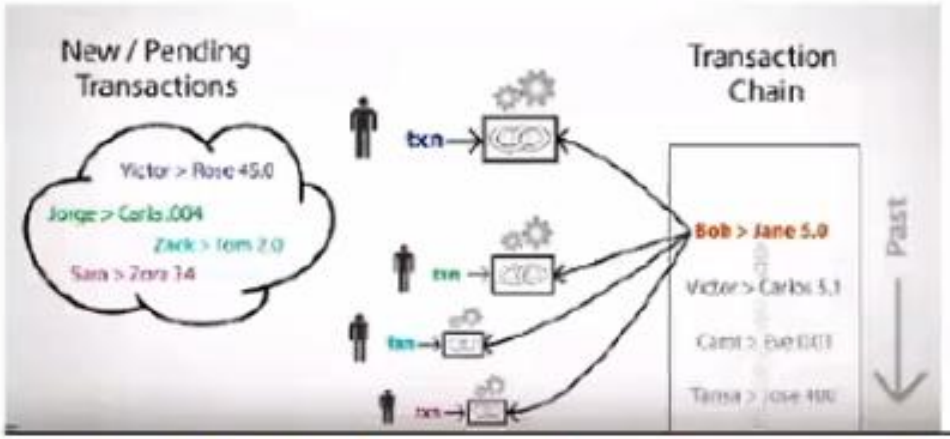

A new PKI hashed signature for each transaction

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



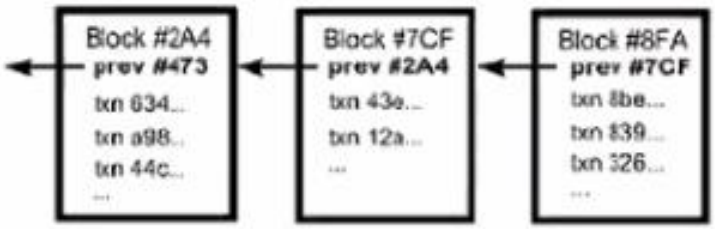
© Copyright 2017 | All Right Reserved

# 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*


© Copyright 2017 | All Right Reserved

# How robust is the Bitcoin p2p network?

- 11,678 global nodes run full Bitcoind (2/18); 160 gb

BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

**GLOBAL BITCOIN NODES DISTRIBUTION**

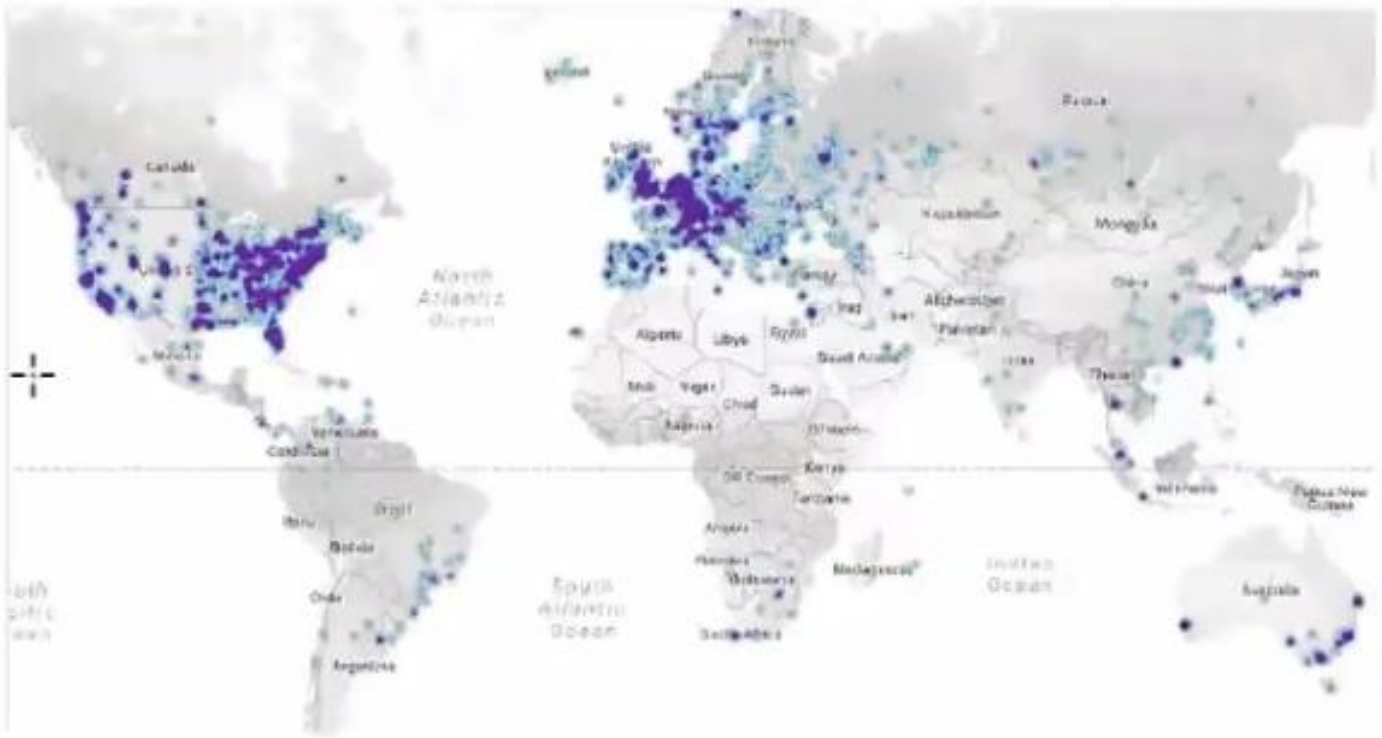
Reachable nodes as of Sun Jan 07 2018 21:10:11 GMT-0500 (Eastern Standard Time).

## 11678 NODES

24 hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

| RANK | COUNTRY | NODES |
|---|---|---|
| 1 | United States | 3269 (27.99%) |
| 2 | Germany | 1997 (17.10%) |
| 3 | China | 808 (6.92%) |
| 4 | France | 804 (6.88%) |
| 5 | Netherlands | 535 (4.58%) |
| 6 | Canada | 456 (3.90%) |
| 7 | United Kingdom | 439 (3.76%) |
| 8 | Russian Federation | 371 (3.18%) |
| 9 | n/a | 299 (2.56%) |
| 10 | Singapore | 219 (1.88%) |



*p2p: peer to peer; Source: https://bitnodes.21.co, https://github.com/bitcoin/bitcoin*



© 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

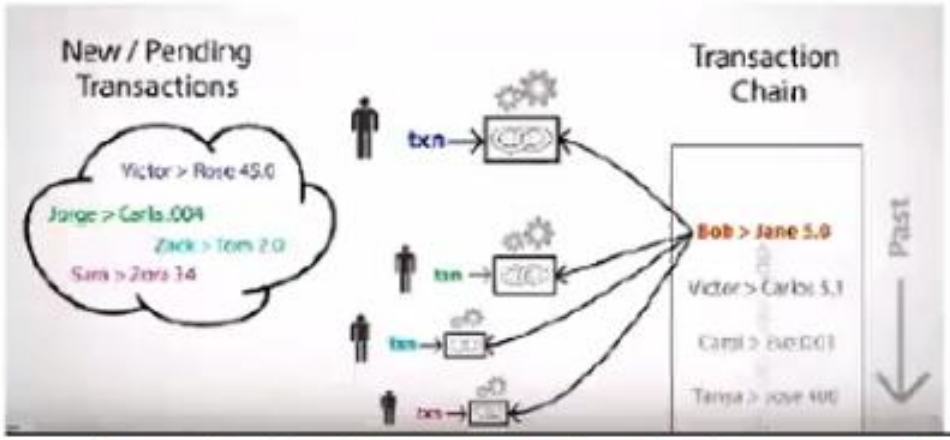
"Wasteful" effort deters malicious players

Fast because ASICs represent the hashing algorithm as hardware



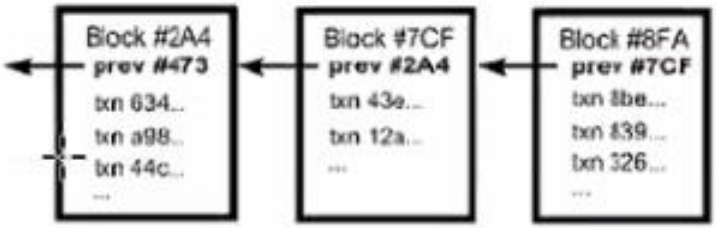
© Copyright 2017 | All Right Reserved

# 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*


© 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



© 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

# What is a Ledger?

- A ledger is like a database, a Google or Excel spreadsheet
- Add new records by appending rows
- Each row contains information
  - Account balances, who owns certain assets
  - Memory and execution state of a computer program

| Ledger | |
|---|---|
| Alice | $500 |
| Bob | $10 |
| Charlie | $1000 |


© Copyright 2017 | All Right Reserved

# Why Distributed?

- Distributed network
- Many nodes or peers that are connected in a network with no single point of failure or centralized control
- Security and resiliency: design the network so that if some peers crash or attack the network maliciously, the network can still operate (Byzantine Fault Tolerance)


© Copyright 2017 | All Right Reserved

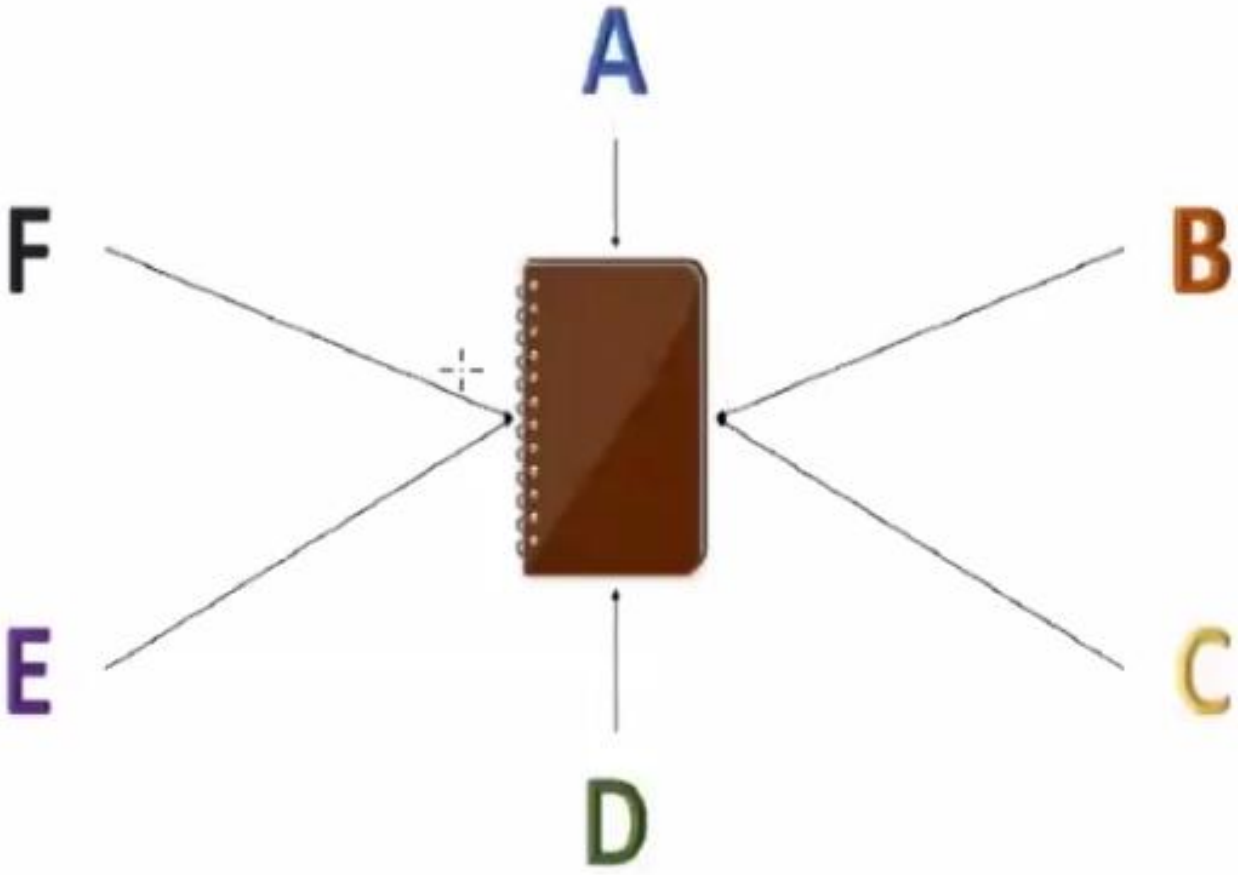
# What is Immutable?

- Cannot change the data once its committed to the ledger
- Data is auditable
- Change by issuing offsetting transaction
- Smart contract code


© Copyright 2017 | All Right Reserved

# What is Blockchain

- **Common Ledger**

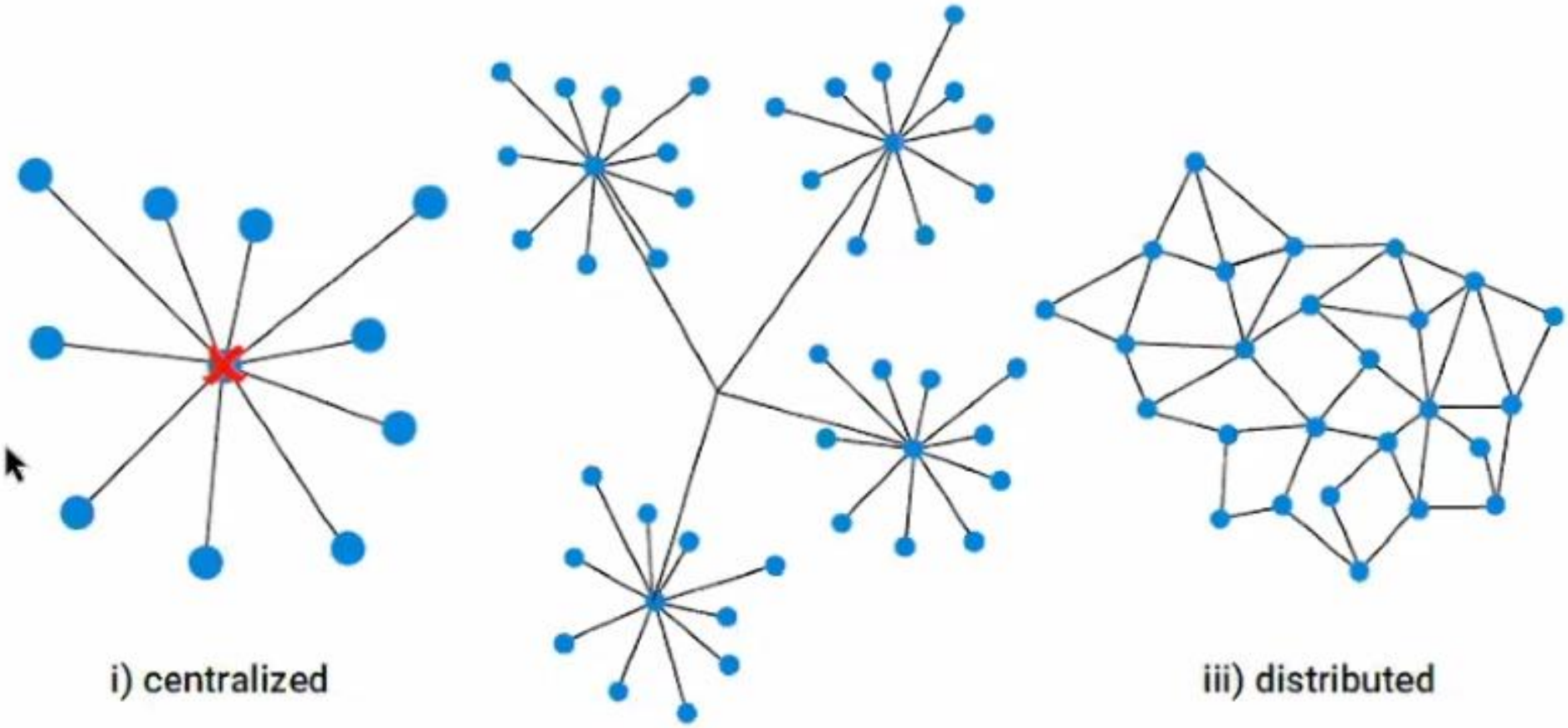




© Copyright 2017 | All Right Reserved


BLOCKCHAIN ADOPTION
One of the fastest-moving technology adoptions

# NETWORK EVOLUTION



i) centralized

ii) decentralized

iii) distributed



© Copyright 2017 | All Right Reserved

# What is Immutable?

- Cannot change the data once its committed to the ledger
- Data is auditable
- Change by issuing offsetting transaction
- Smart contract code


© 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


© Copyright 2017 | All Rights 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

# 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
  - The size of this group remains constant as the network grows


© Copyright 2017 | All Right Reserved

# Key Blockchain Concepts

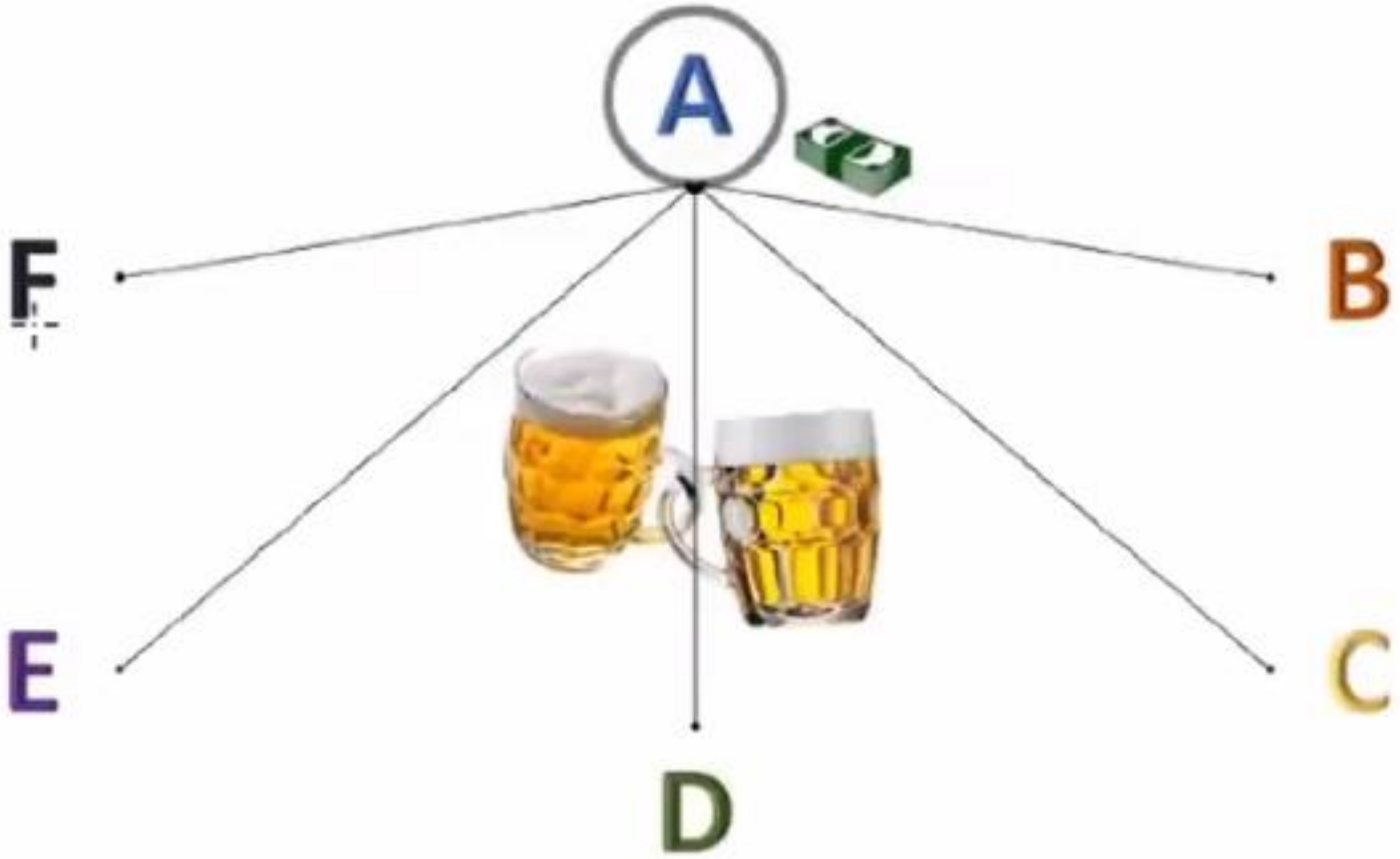
- Public-private networks
  - Trustless vs trusted
- Distributed network
- Consensus algorithms
- Immutability

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


© Copyright 2017 | All Right Reserved

# What problem does Blockchain solve?

- **Trip to the Bar**

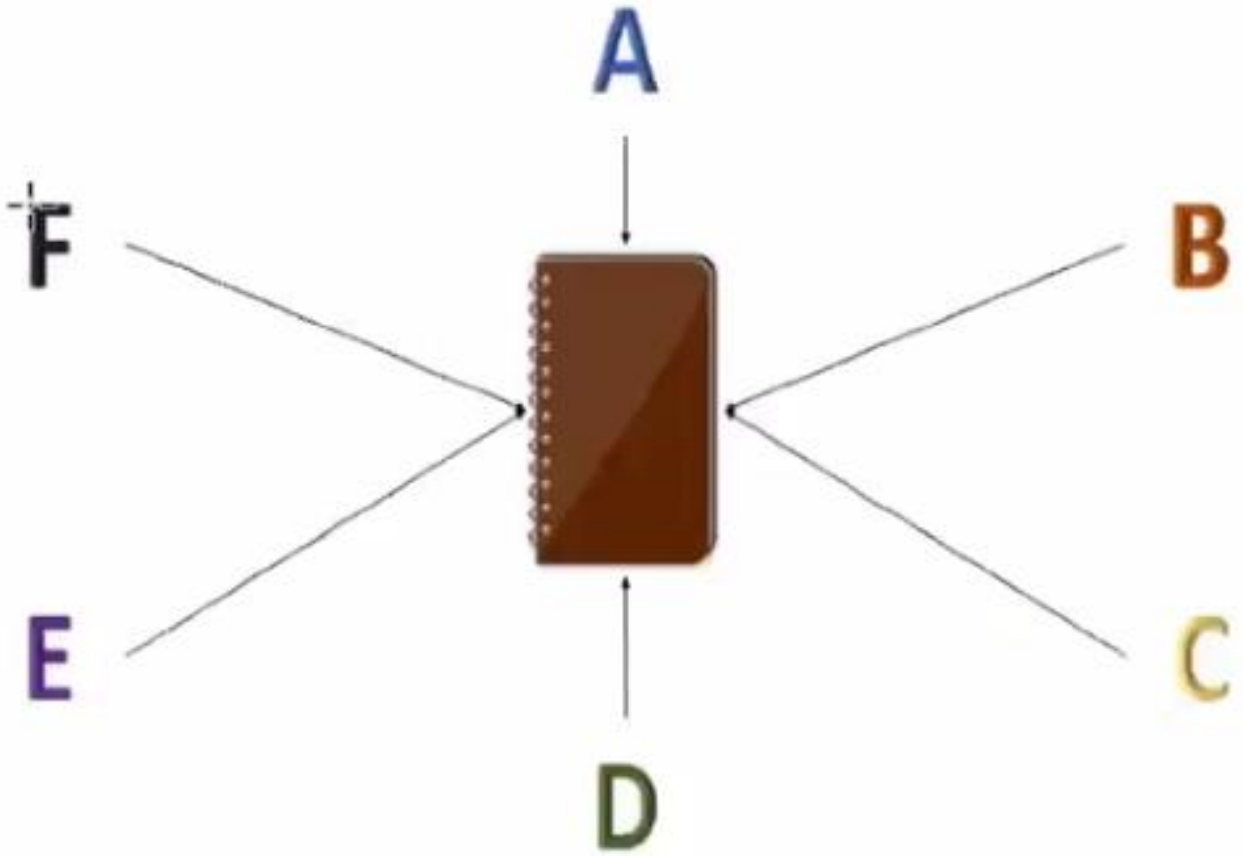




© Copyright 2017 | All Right Reserved

# What is Blockchain

- **Common Ledger**

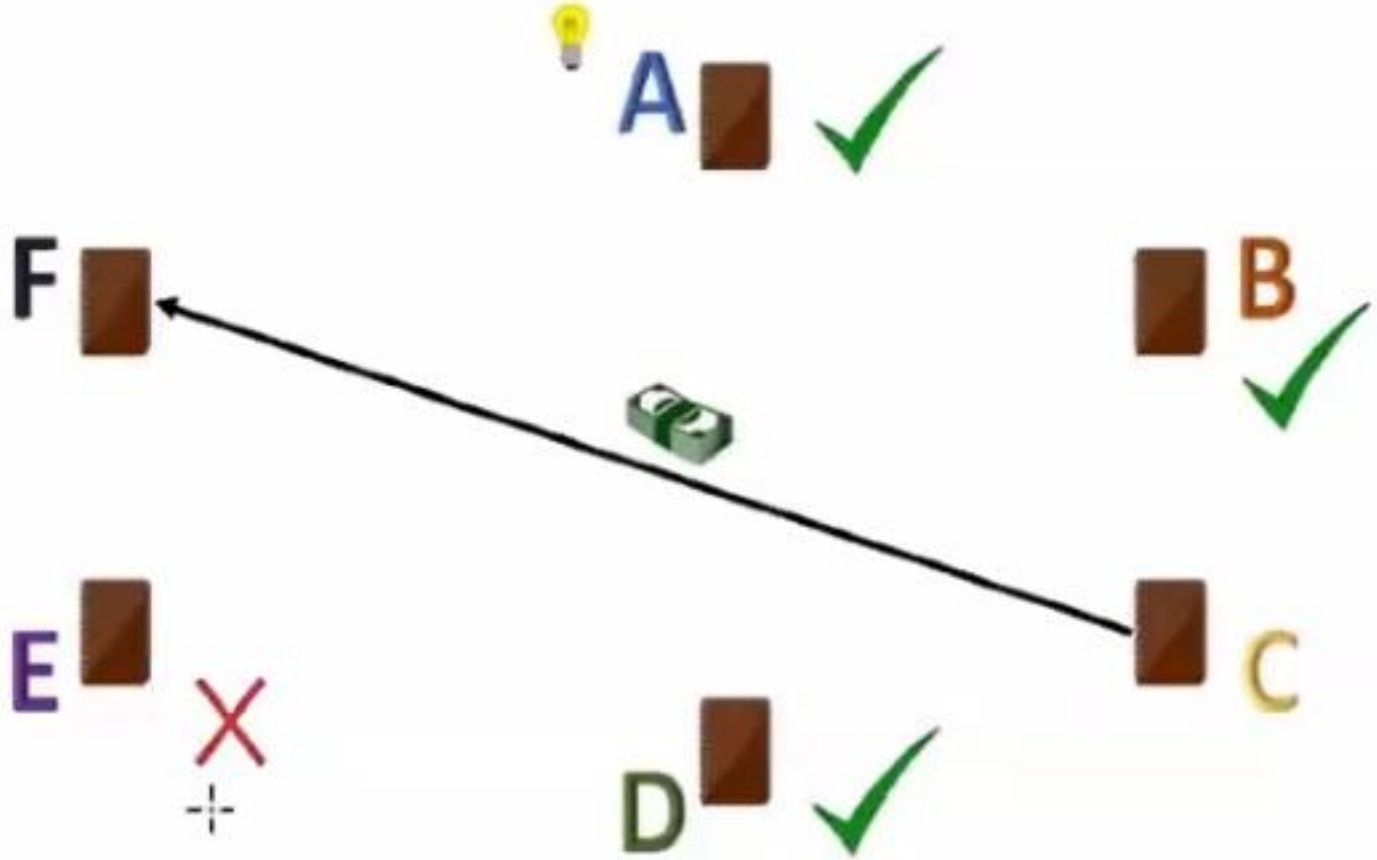




© Copyright 2017 | All Right Reserved

# What is Blockchain

- **A More Common Ledger**





© Copyright 2017 | All Rights Reserved

# BLOCKCHAIN ADOPTION

One of the fastest-moving technology adoptions