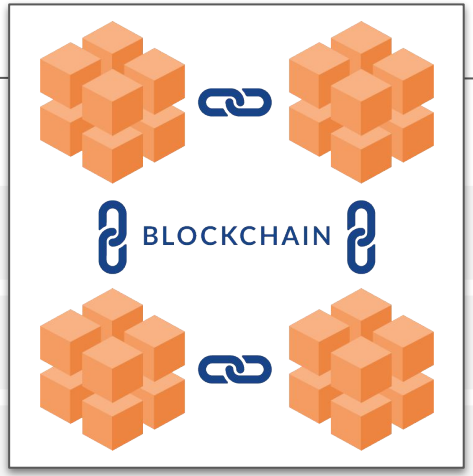
Blockchain Building Blocks

FinTech

Lesson 18.1

Class Objectives



By the end of this unit, you will be able to:

- Describe why blockchain exists.
- Explain blockchain technology and its use cases to someone that doesn't have any blockchain background.
- Describe the 5 Pillars of Open Blockchains.
- Use a blockchain wallet and explain how it works to somebody who doesn't know.
- Visualize transactions via block explorers.
- Brainstorm solutions for the those without robust financial institutions.
- Navigate the blockchain ecosystem.

Class Objectives

You will be learning about what blockchain technology is, what it's used for, and why it's important for you to learn as a FinTech entrepreneur.

By the end of this unit, we will build our own blockchain wallets, write smart contracts, and construct a blockchain from scratch!

Blockchain Skill Check

Blockchain Skill Check

How many of you have heard of blockchain before?

Blockchain Skill Check

How many of you have heard of cryptocurrency before?

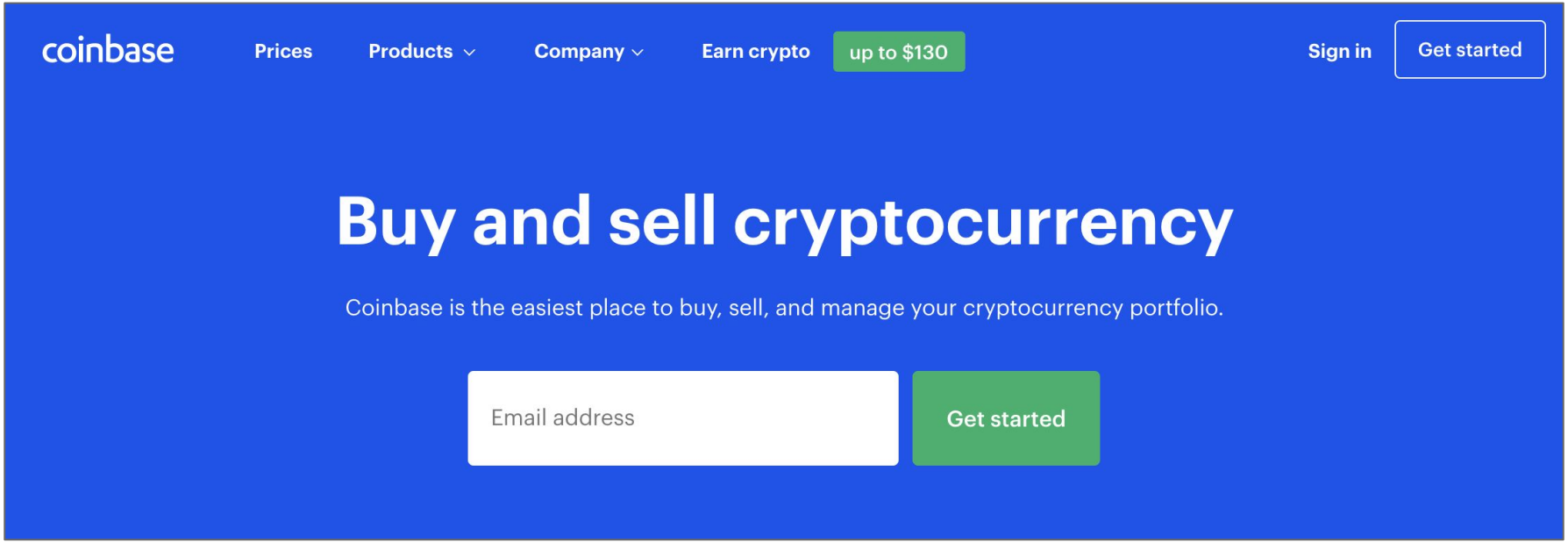
80% of Americans are Aware of Bitcoin, Study Reveals

Lester Coleman | September 6, 2018 22:00 UTC

Millennials are more optimistic about the chances of cryptocurrency being widely accepted, and nearly half of who think this would prefer using cryptocurrency over the U.S. dollar, according to a recently conducted consumer survey on awareness of and attitudes about cryptocurrency.

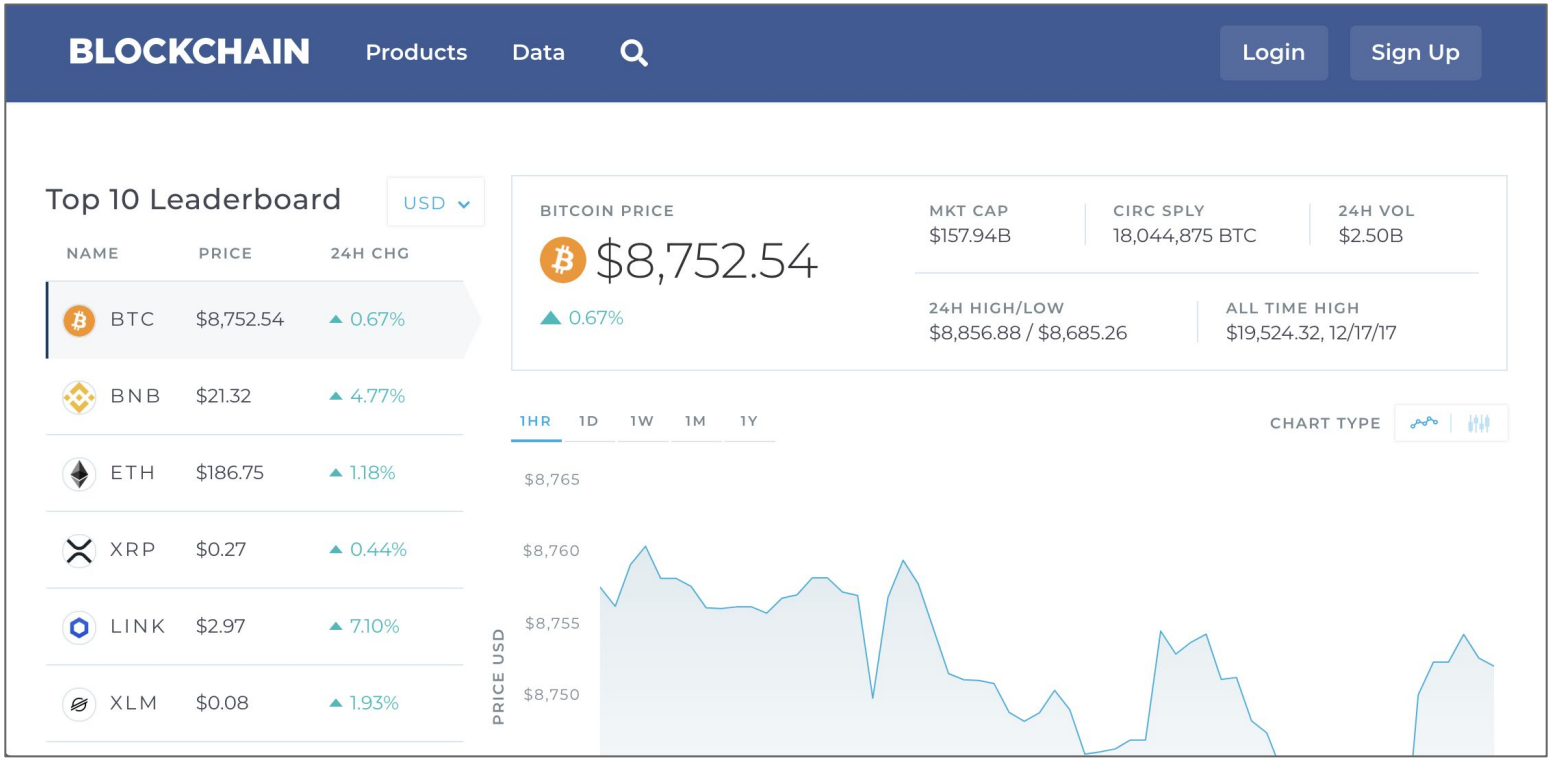
Blockchain Skill Check

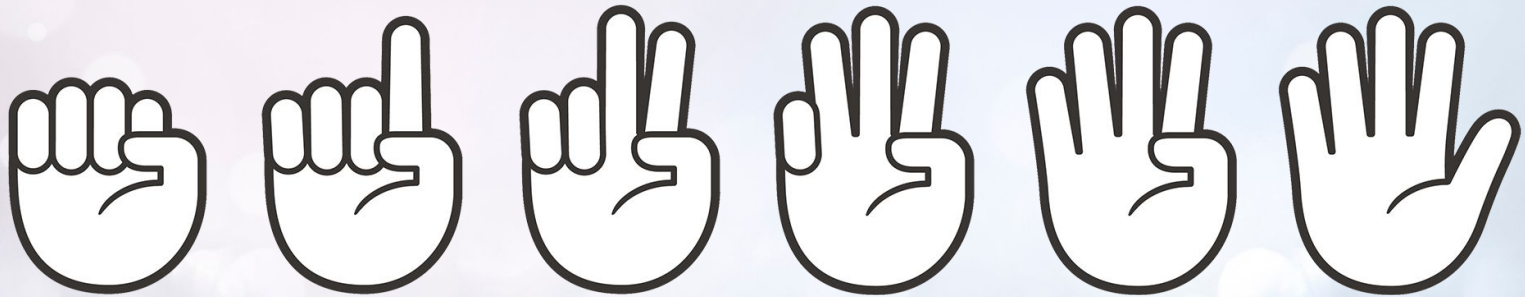
How many of you have ever used a blockchain, aka crypto wallet?



Blockchain Skill Check

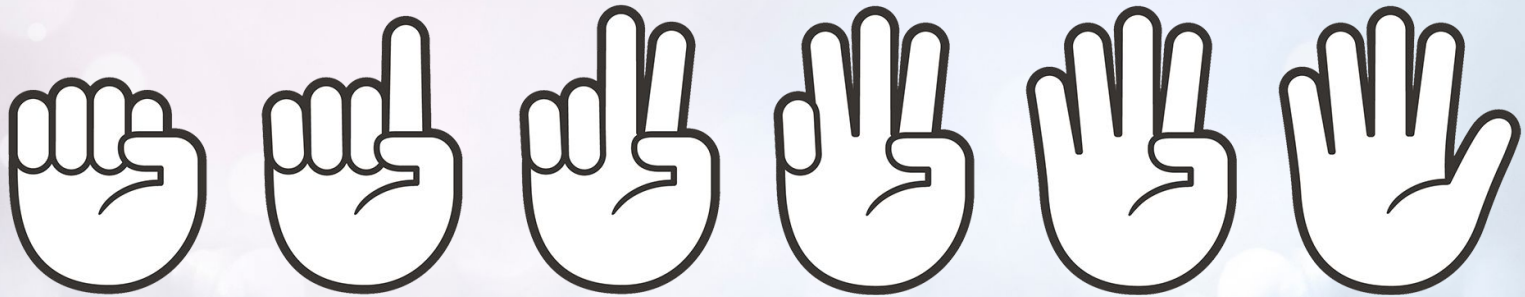
How many of you have ever traded cryptocurrency?





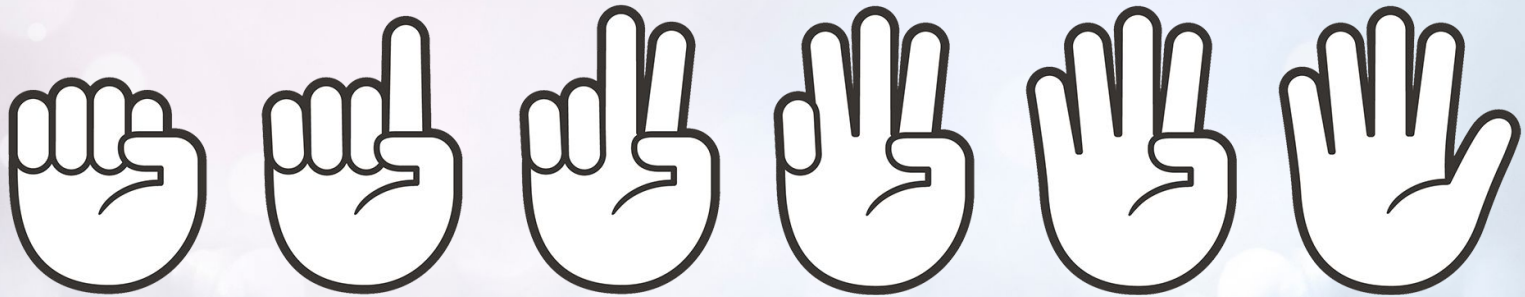
FIST TO FIVE:

How familiar are you with blockchain?



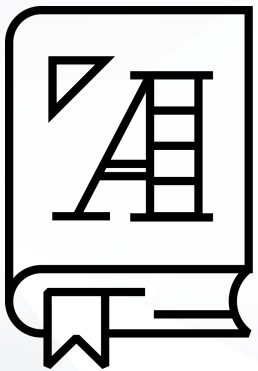
FIST TO FIVE:

How comfortable do you feel having a conversation about blockchain technology?



FIST TO FIVE:

How familiar are you with Ethereum?

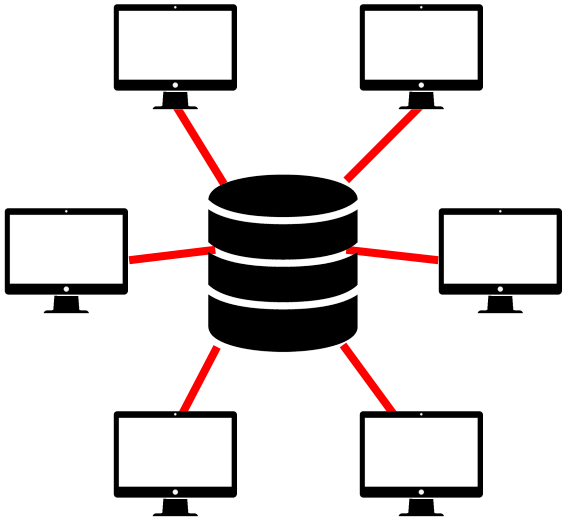


A **blockchain** is a distributed “immutable” database that is not controlled by a single, central authority.

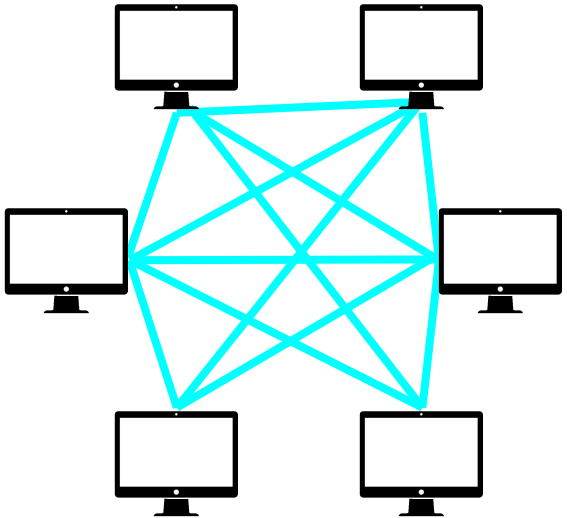
Blockchain

A blockchain is a distributed “immutable” database that is not controlled by a single, central authority.

Centralized Database

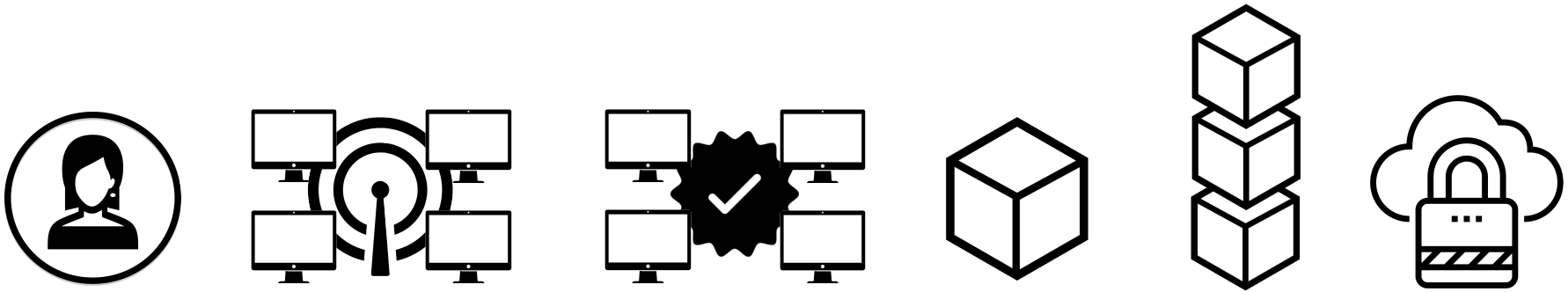


Decentralized Database



Blockchain

The database is synchronized across the network, with special rules in place to incentivize good actors and disincentivize bad actors.



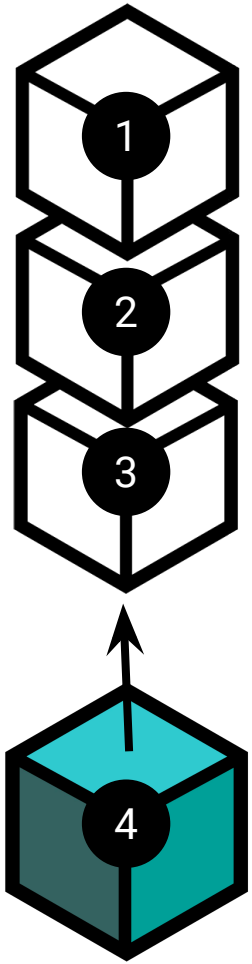
1. A transaction is initiated.
2. The transaction is broadcast to every node in the network.
3. The nodes form a consensus on whether the transaction is valid.
4. The nodes add valid transactions to a “block.”
5. The block is added to the blockchain.
6. Transaction complete.

Blockchain

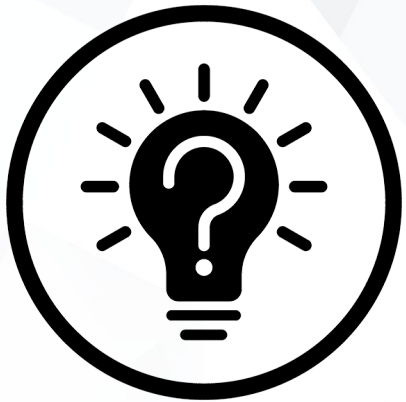
It is immutable, which means you can only add to the database: you cannot change the history.

This provides a powerful means of creating a trusted “source of truth” in a trustless environment.

Transactions are linked together in a chronological manner to form a continuous chain of blocks



The Importance of Blockchain



Why would a banker want to use a blockchain?

The Importance of Blockchain

Using a blockchain for interbank communication is faster, more secure, and cheaper than the systems in place now, Swift and ACH.

EUROMONEY

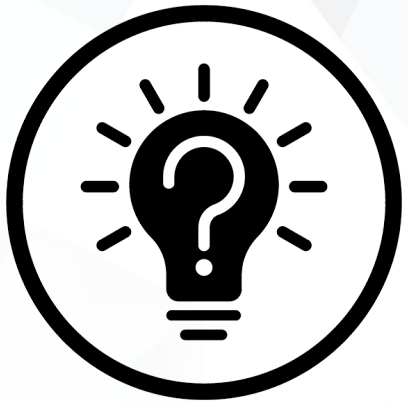
SUBSCRIBE FREE TRIAL

MARKETS | TRANSACTION SERVICES

Swift hacks expose bank security weaknesses

Kimberley Long | Thursday, September 15, 2016

Security breaches that have allowed hackers to infiltrate Swift's messaging network have raised questions about the safety of the messaging network, but the problems might rest with the individual banks.



Why would an individual in an underbanked, developing, or authoritarian country want to use a blockchain?

The Importance of Blockchain

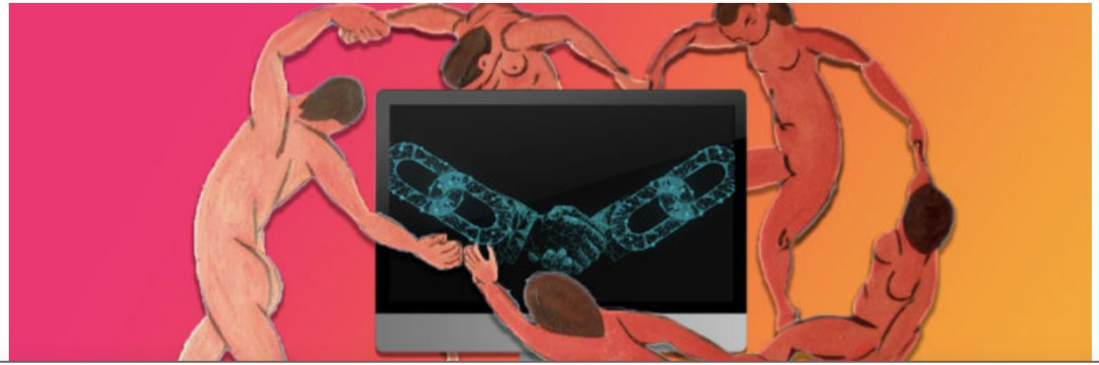
Transactions cannot be censored.

You only need a mobile device and internet connection, which is a common commodity, even in developing countries.

Blockchain Technology Could Prevent Internet Censorship

Christian Gundiuc — 6 months ago

Comments



Why would an individual in the US want to use a blockchain?

Importance of Blockchain

- Removes intermediaries like PayPal, Venmo, Cashapp, etc., and allows for peer-to-peer payments, thus lower fees.
- Custody over your funds, versus allowing a bank to have custody.
- Cheaper than domestic wire transfers.
- Brings financial services typically available to the upper class to everyone.

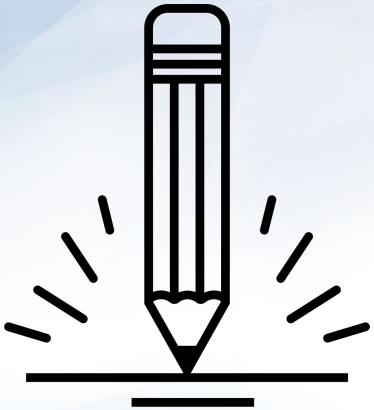
Why would anyone want to use blockchain?

Importance of Blockchain

Fast, global transactions that are not managed by a single authority.

Importance of Blockchain

Secure, modern infrastructure for the next generation of the internet. This is also known as Web 3.0.



Activity: Use Case Study

In this activity, you will complete a thought experiment in which you will get together in small groups and examine an example use case application for different cryptocurrency and blockchain projects.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Use Case Study

Some common features may be:

- Transparency
- Privacy (in the case of Monero)
- Smart contracts
- Neutrality
- Hedge against hyperinflated currencies
- Bridge of trust between parties that might not trust each other
- Cross-border nature
- Pseudonymous system (addresses are your alias, not necessarily attached to identity)

5 Pillars of Open Blockchains

As we talk through each pillar, keep in mind what you uncovered during the previous exercise. Which feature would you put in each category?

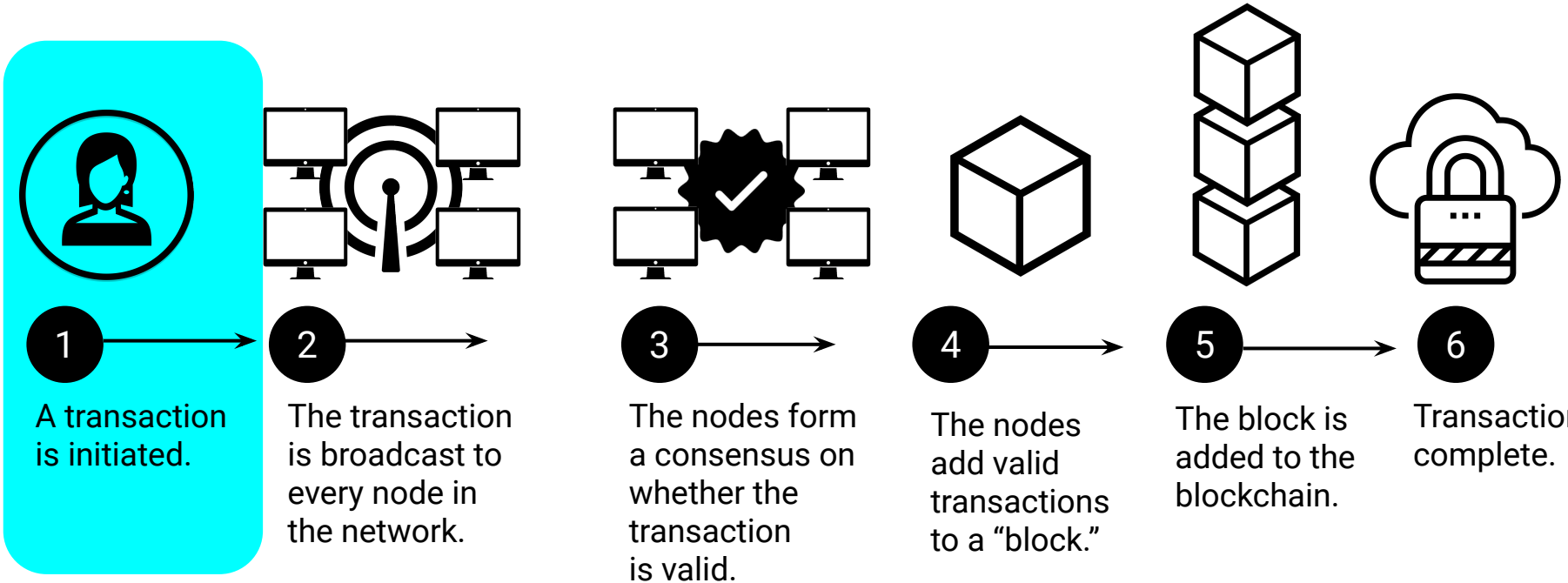
Pillar 1: Open

Anyone can access the source code and create a project from it, therefore developer access is high.

```
class Block {
    constructor(index, previousHash, timestamp, data, hash) {
        this.index = index;
        this.previousHash = previousHash.toString();
        this.timestamp = timestamp;
        this.data = data;
        this.hash = hash.toString();
    }
}
```

Pillar 1: Open

Anyone can access the chain and participate in the ecosystem.
Anyone can access the services the blockchain offers.



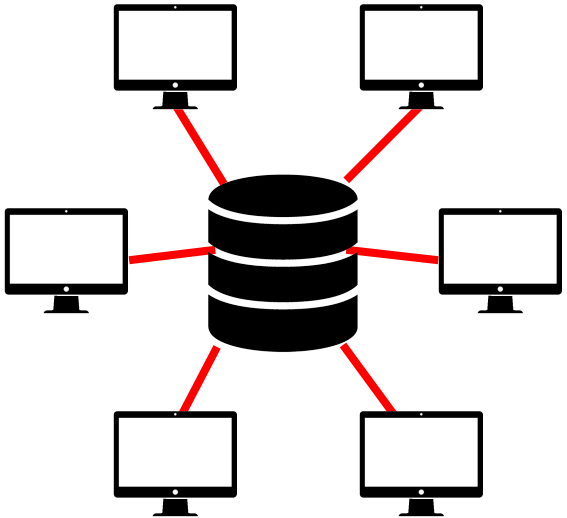
Pillar 1: Open

Openness means that the system is designed to incentivize users to keep it open. The internet is an example of this, and it is built on open protocols that anyone can learn and contribute to.

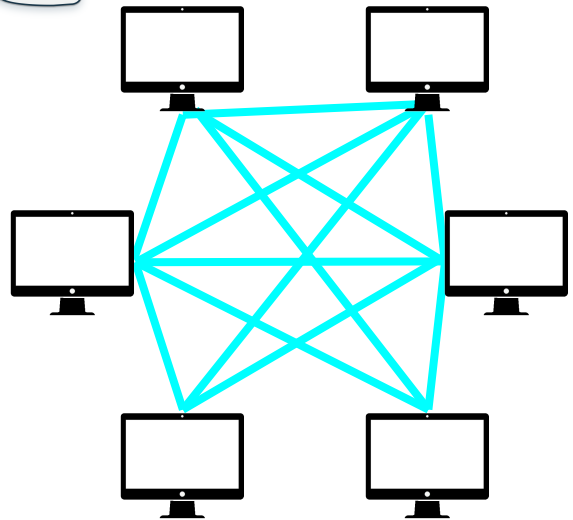
Pillar 2: Borderless

To be borderless, the network needs to be decentralized. This means that any central party does not hold control of the network.

Centralized Database

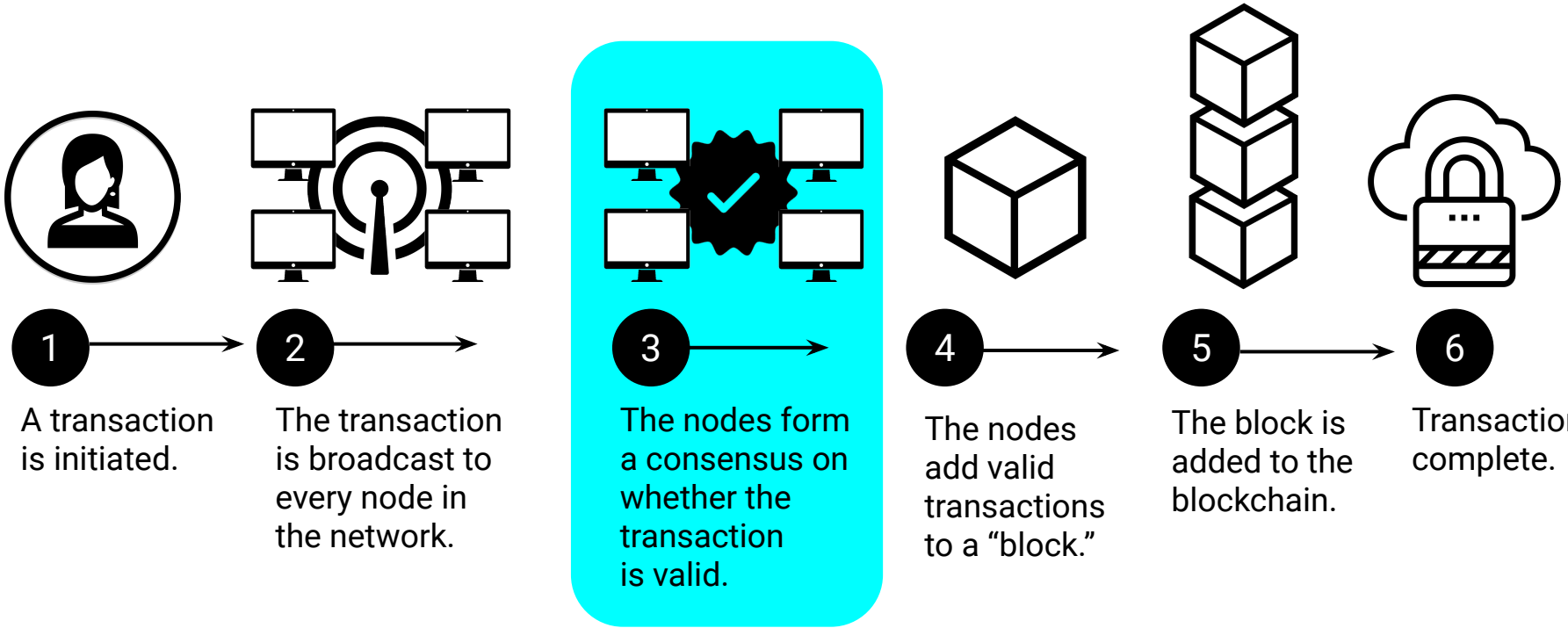


Decentralized Database



Pillar 2: Borderless

Since the blockchain is synchronized onto every device that helps maintain it (called nodes), it lives everywhere.



Are you moving money across a border when you bring a credit card across customs?

Much like the money is not on the card itself, a crypto wallet does not hold the crypto itself, just the access.

The blockchain is already synchronized to a device in the country you are traveling to, so accessing it is the same as if you were to swipe a Visa card internationally, only without Visa getting involved.

You can also use a satellite connection to connect to blockchain networks and broadcast transactions, therefore it is truly global.

Pillar 3: Neutral

Neutral means that the protocol does not discriminate against any user.

01

The blockchain is agnostic to the users, regardless of political or social status, or geographic location.

02

A wealthy banker or government leader uses the protocol in the exact same way anyone else would.

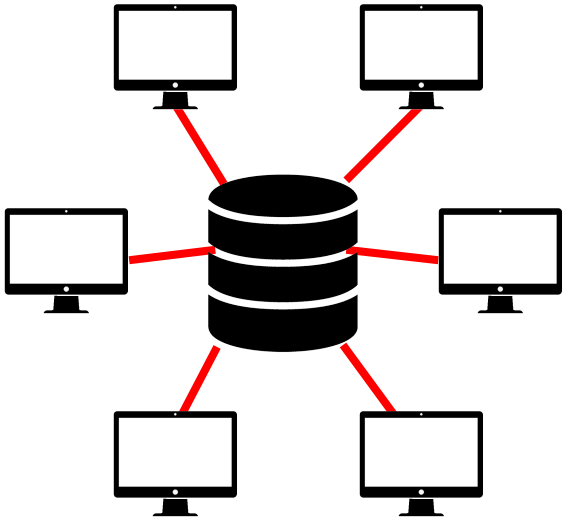
03

Open blockchain networks are also governed in a neutral fashion, with many using the blockchain itself for voting on the next network upgrades.

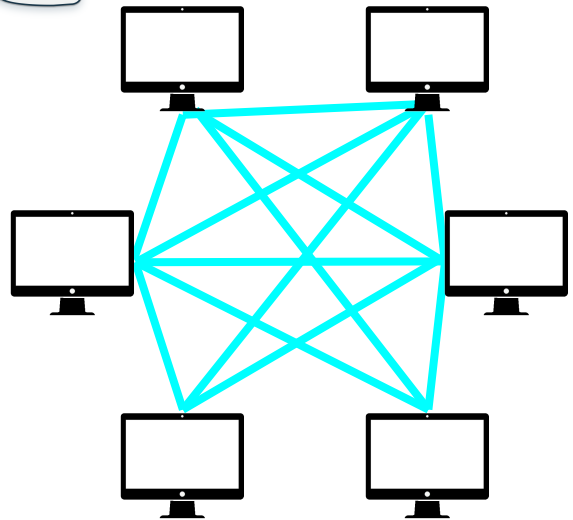
Pillar 4: Censor Resistant

Blockchains that are properly decentralized are highly resistant to censorship and authoritarian control.

Centralized Database



Decentralized Database



Pillar 4: Censor Resistant

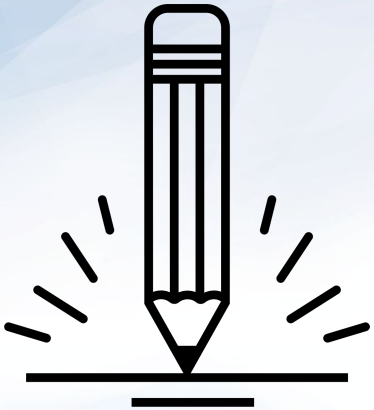
This means that people suffering in nations that have high censorship can still find a way to use these systems to reach out and to bypass the oppression.

Money is often compared to a form of speech. These are systems where this form of expression cannot be censored.

Pillar 5: Public

Open blockchains are separate from the state.
Public blockchain networks are suited for public affairs.

This separation of state and money is a first in history. It is similar to the separation of church and state to allow for religious freedom; only this allows for monetary freedom.

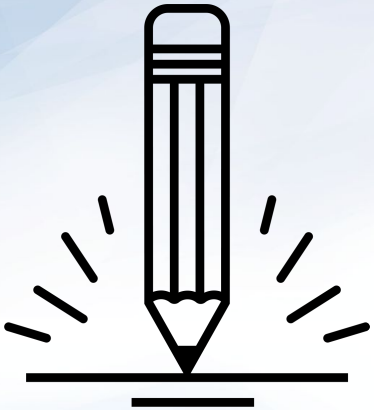


Activity: Peoplechain

In this activity, you will emulate the public, censor resistant and borderless nature of the blockchain by creating a distributed ledger like system breaking up into groups and using themselves as network participants.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.



Activity: Basic Terminology

In this activity, you'll google common terminology used in blockchain development.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Basic Terminology Review

Hash

A "hash" is a unique fingerprint of a piece of data.

Block 0

Index: 0
Timestamp: 17:15
1/1/2019
data: "block0data"
hash: 0xea34ad...55
previous Hash: 0

Block 1

Index: 0
Timestamp: 17:17
1/1/2019
data: "block0data"
hash: 0xf6e1da2.deb
previous Hash:
xea34ad...55

Block 2

Index: 0
Timestamp: 17:19
1/1/2019
data: "block0data"
hash: 0x9373b..36a21
previous Hash:
0xf6e1da2.deb

Hash

01

SHA256

There are several popular hashing algorithms, SHA256 being one of the most popular. It is easy to run the hash function over the same data again to verify the result is the same.

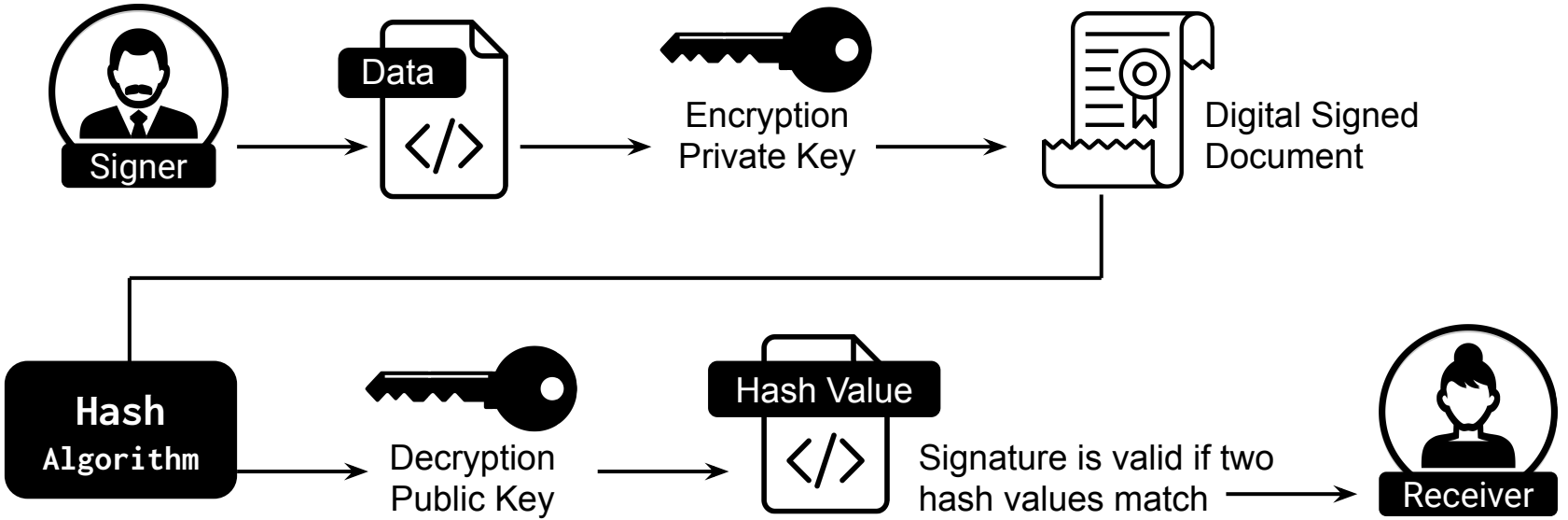
02

Data Integrity

If you were to change a single bit of the input, you would get a completely different hash. This allows for something called “data integrity” which is a very important part of internet and data security as well as blockchain technology.

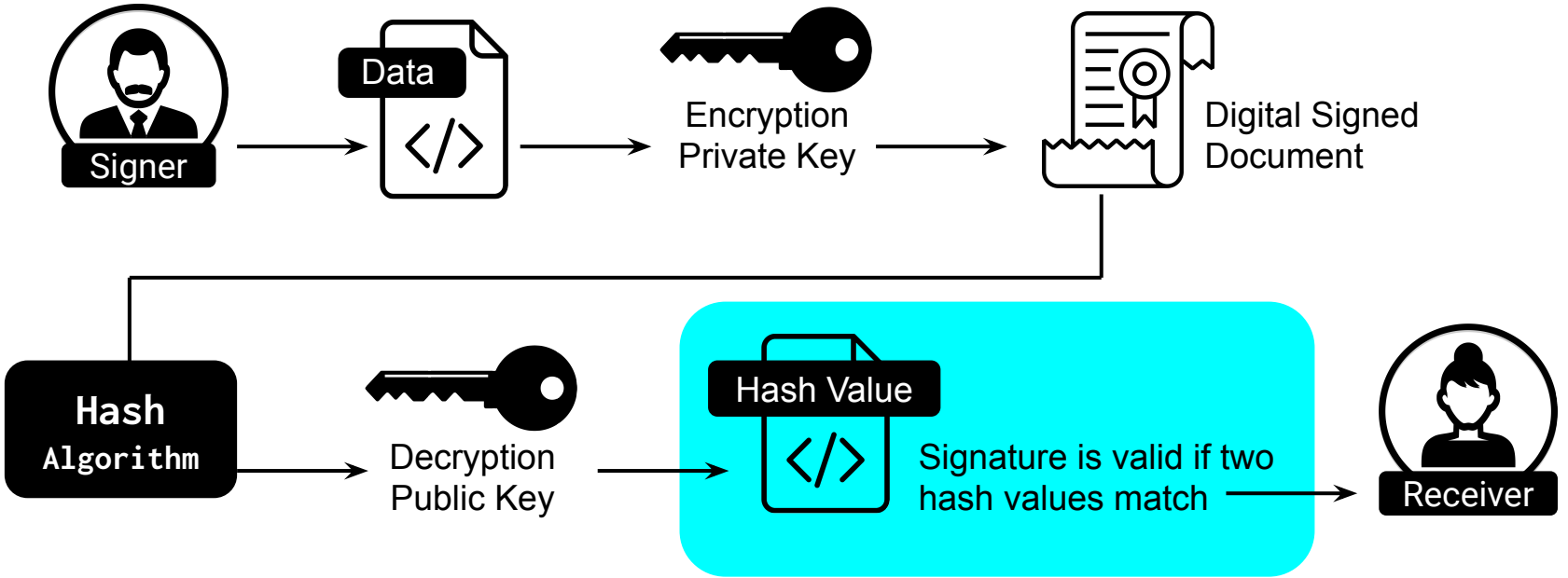
Digital Signature

Digital signatures are used to prove ownership or authenticity of data mathematically.



Digital Signature

If the signed message is modified, the signature will be invalidated.



Digital Wallet

A **Digital Wallet** is simply a set of “keys” to your funds that are on the blockchain.

With a wallet, you can create and send transactions, as well as view your balance.

You can also sign messages with your digital wallet to prove ownership or authenticity of something.

A digital wallet is much like the debit cards in your own wallet, you use them to access funds in your account. Only in this case, the card is now a key, and the bank is now the blockchain.

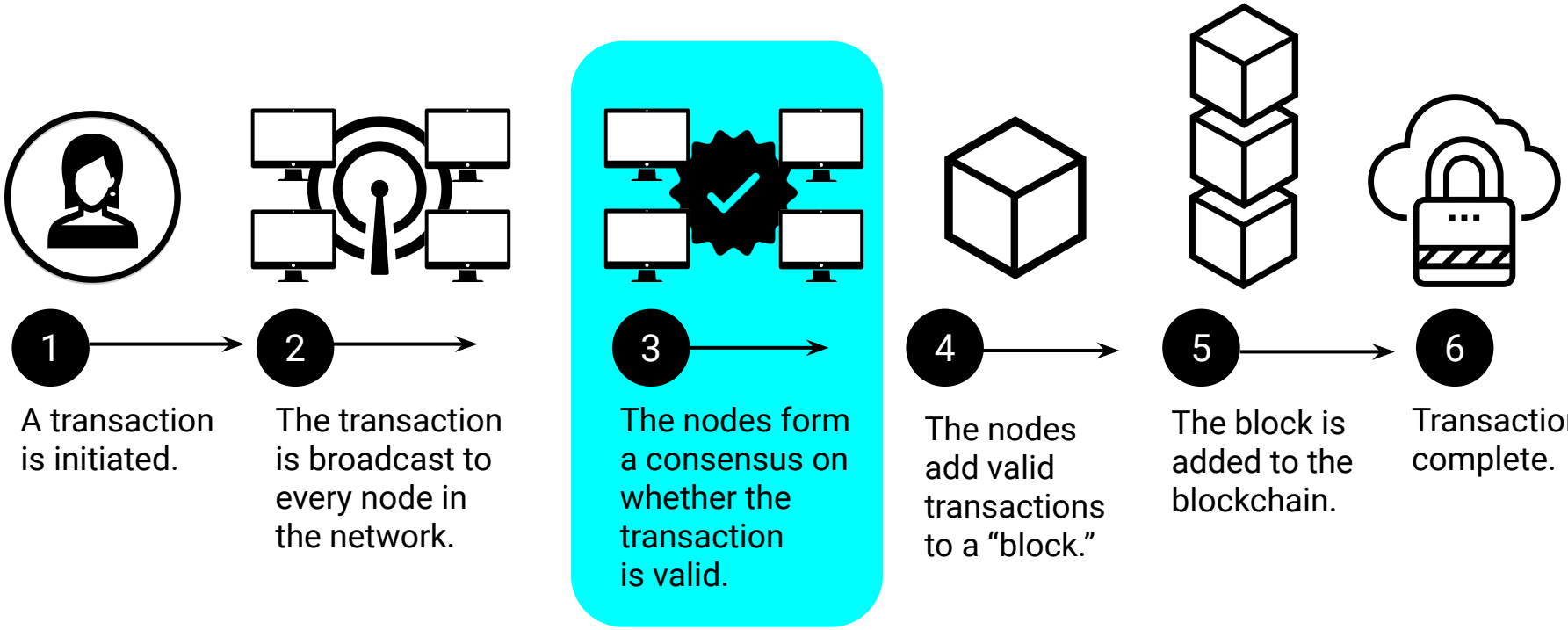
Transaction

A transaction is simply a signed message that authorizes a movement of funds between two parties.

It is essentially **"I sign off on the movement of X amount of value from account A to account B"** —now that it is signed off, nobody can modify it.

Blockchain Node

A full node keeps a copy of the blockchain. It verifies the signature of every transaction and throws out any that do not validate.



Blockchain Node

01 **Tracking**

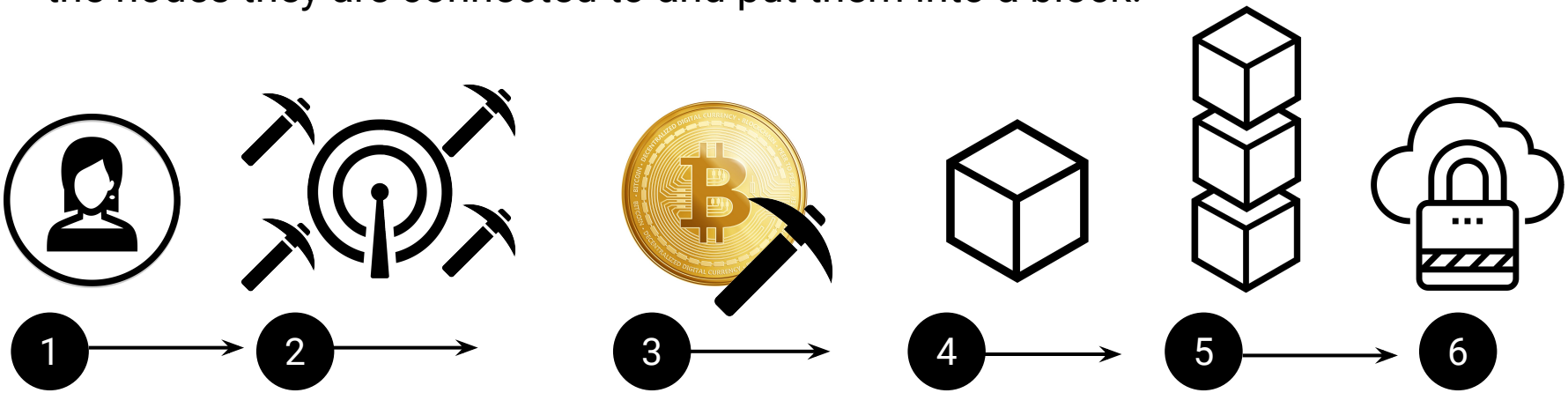
If you wanted to send a transaction, you would send it to a node to keep track of. Nodes broadcast the transaction to their neighbors until a miner comes along and finalizes the transactions.

02 **Security**

Nodes are enforcing all of the rules of the blockchain. Thus they are a very important part of the security of the network.

Miner or Block Producer

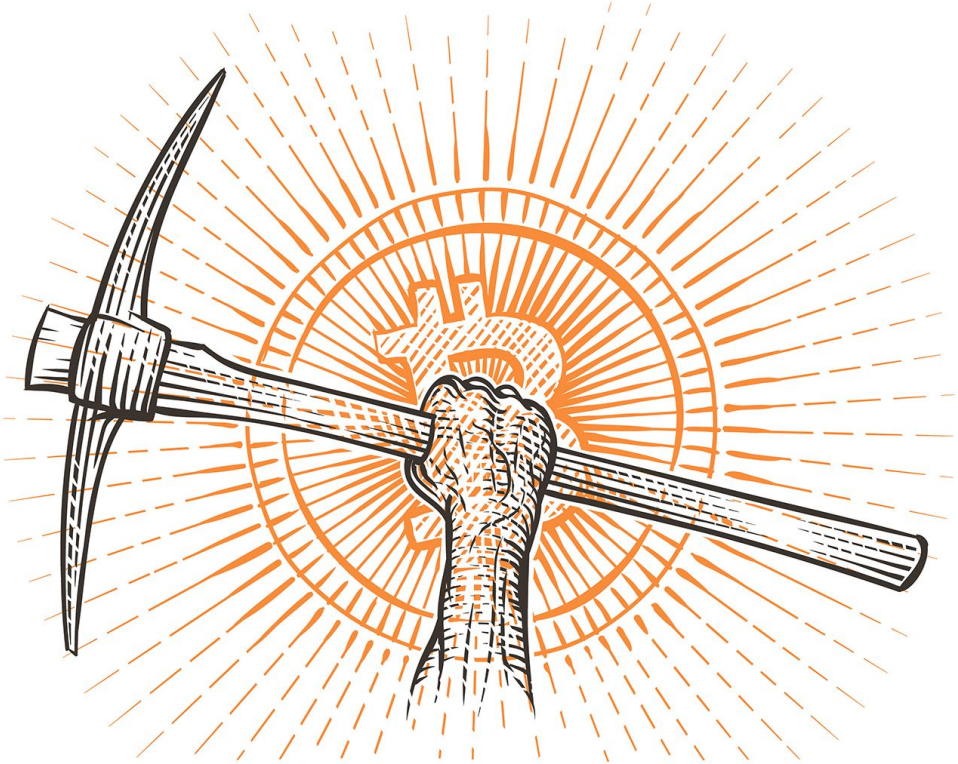
A miner/block producer is a special type of node that is working to solve computations to finalize transactions. Miners take the pending transactions from the nodes they are connected to and put them into a block.



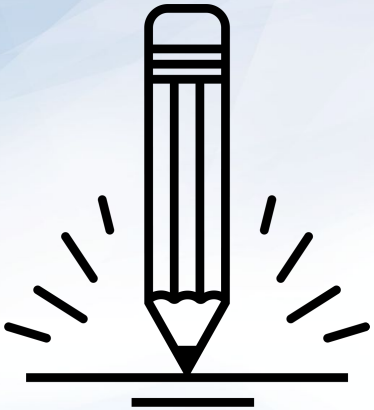
1. A transaction is initiated.
2. The transaction is broadcast to miners.
3. Mining is completed and miner gets a reward.
4. The transaction is validated.
5. The block is added to the blockchain.
6. Transaction complete.

Miner or Block Producer

Each miner races against each other to perform this process first, and the winner is rewarded by the network for its work. Then this race happens again and again for each new block in the chain.




Break

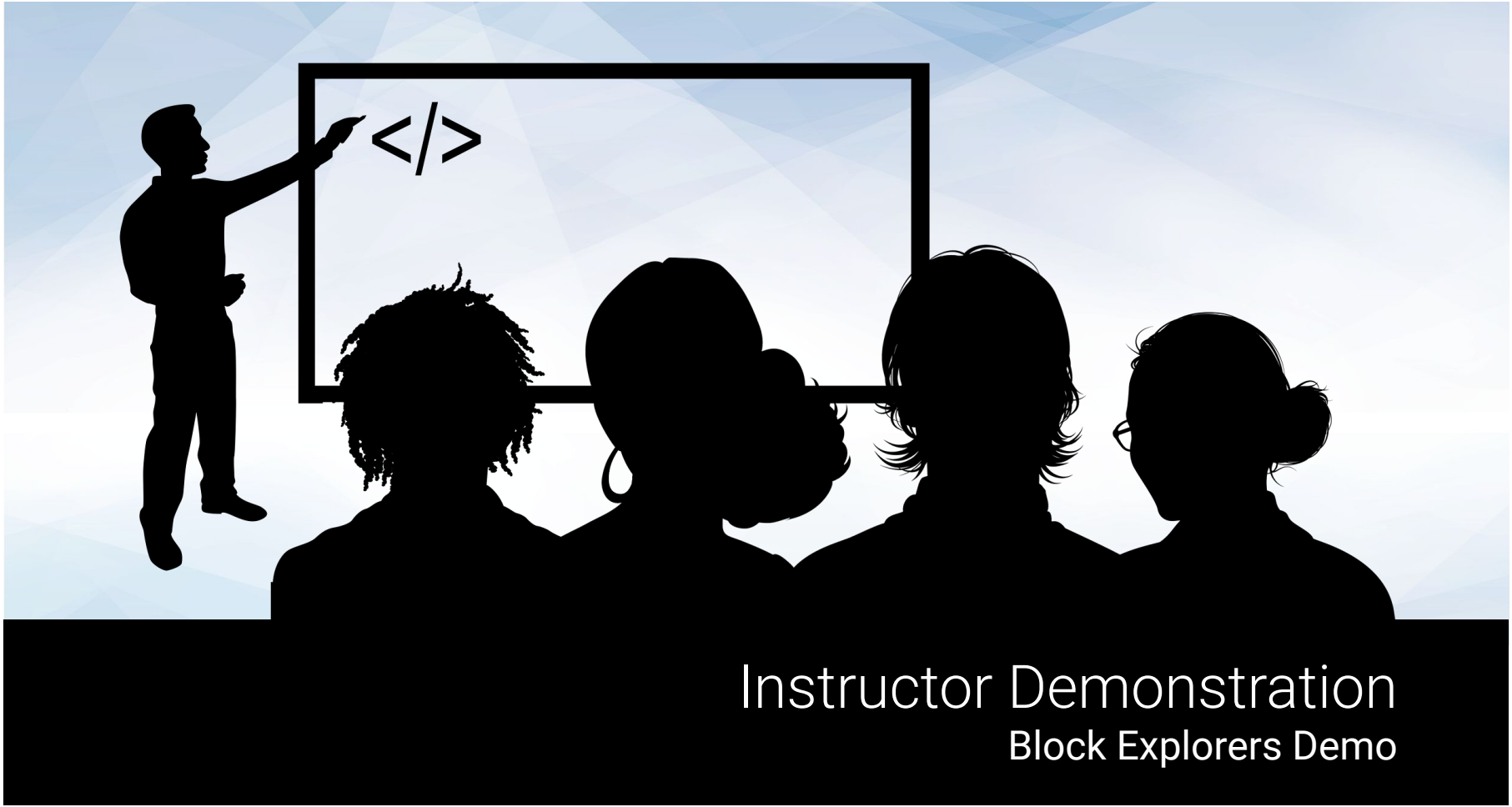


Activity: Using a Wallet

In this activity, you'll test a cryptocurrency wallet.

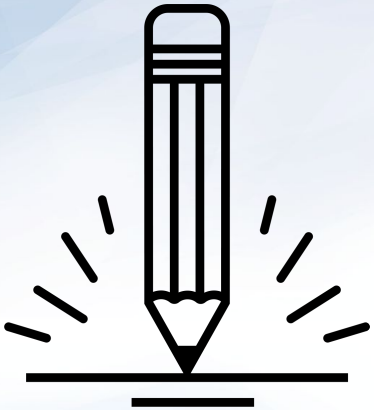
Suggested Time:
10 Minutes

Time’s Up! Let’s Review.



Instructor Demonstration

Block Explorers Demo



Activity: Visualizing Transactions

In this activity, you will visualize transactions using the same technique used in the demo.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Visualizing Transactions

BLOCKCHAIN WORKFLOW

01 BLOCKCHAIN

Someone sends a **transaction** from a wallet.

02 NETWORK

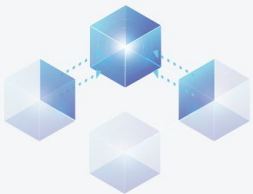
The requested transaction is broadcast to a peer-to-peer network consisting of computers known as **nodes**.

03 VALIDATE

The network of nodes **validates** the transaction's integrity.

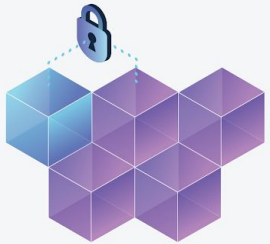
04 UNIFIED DATA

Once verified, the transaction is combined with other transactions to create a new **block of data** for the ledger.



05 ADDED BLOCKCHAIN

The new block is then added to the existing **blockchain**, in a way that is permanent and unalterable.



06 COMPLETE

The transaction is **complete**.

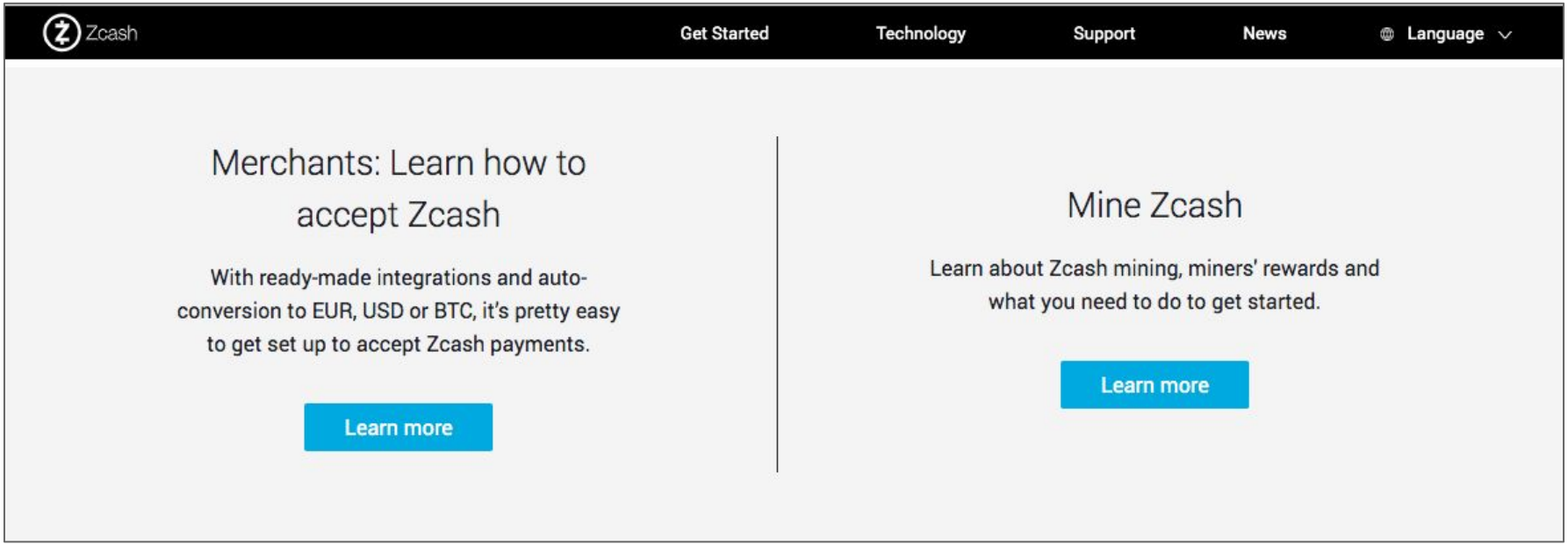
Intro to Ethereum

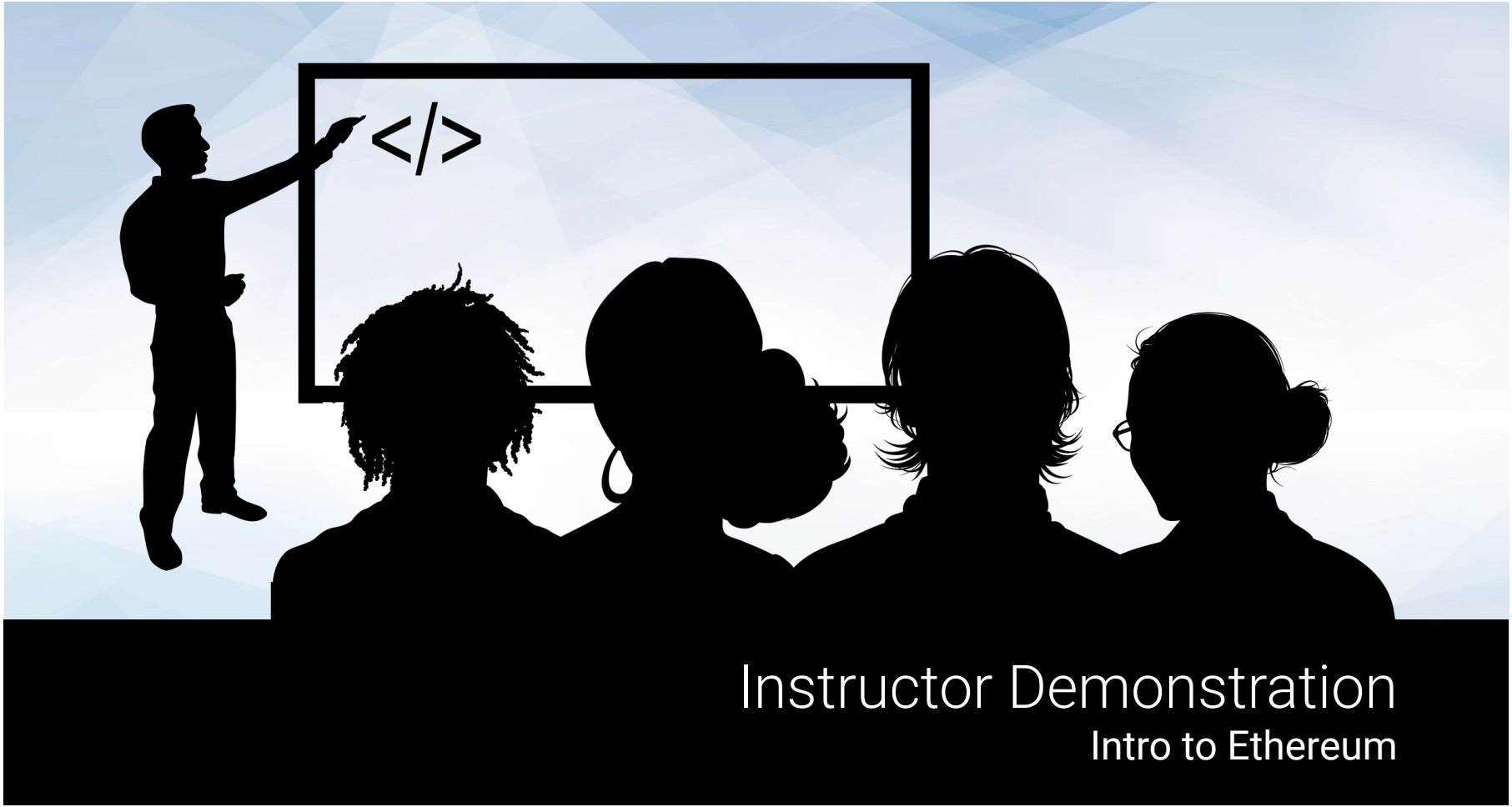
Intro to Ethereum

While the current version of Ethereum is pseudonymous, future updates will bring a technology called **“Zero Knowledge Proofs”** that will enable completely private transactions on a public network.

Intro to Ethereum

There are currently public blockchains, like Zcash, that implement this now by default, so be on the lookout for zero-knowledge protocols in future blockchain upgrades.





Instructor Demonstration

Intro to Ethereum

Intro to Ethereum

What would it be like to have money built into your programming language, as a first data type like string or number?

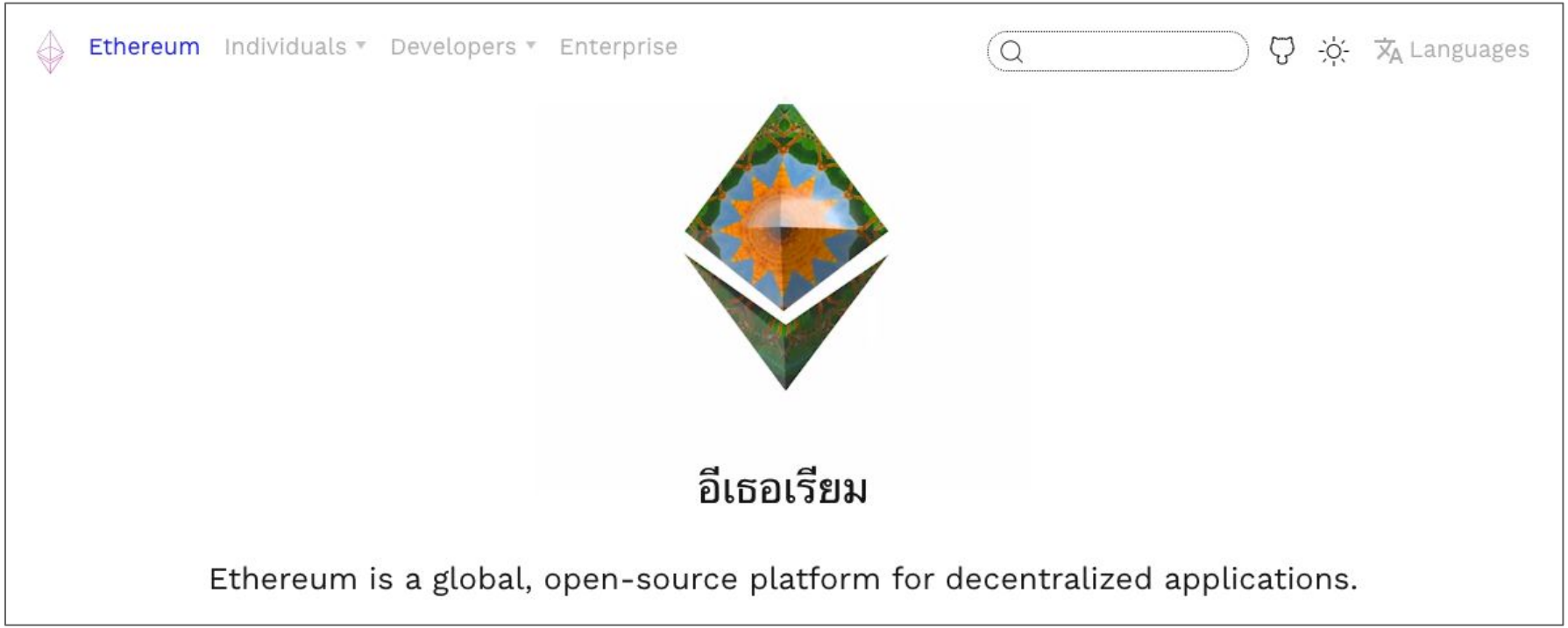
```
amount = $10 dollars
recipient = "JaneDoe123"
wallet.send_transaction(amount, recipient)
```

This is what Ethereum brings to the table, just replace a couple fields:

```
amount = 0.05 Ether
recipient = "0xc3879B456DAA348a16B6524CBC558d2CC984722c"
wallet.send_transaction(amount, recipient)
```

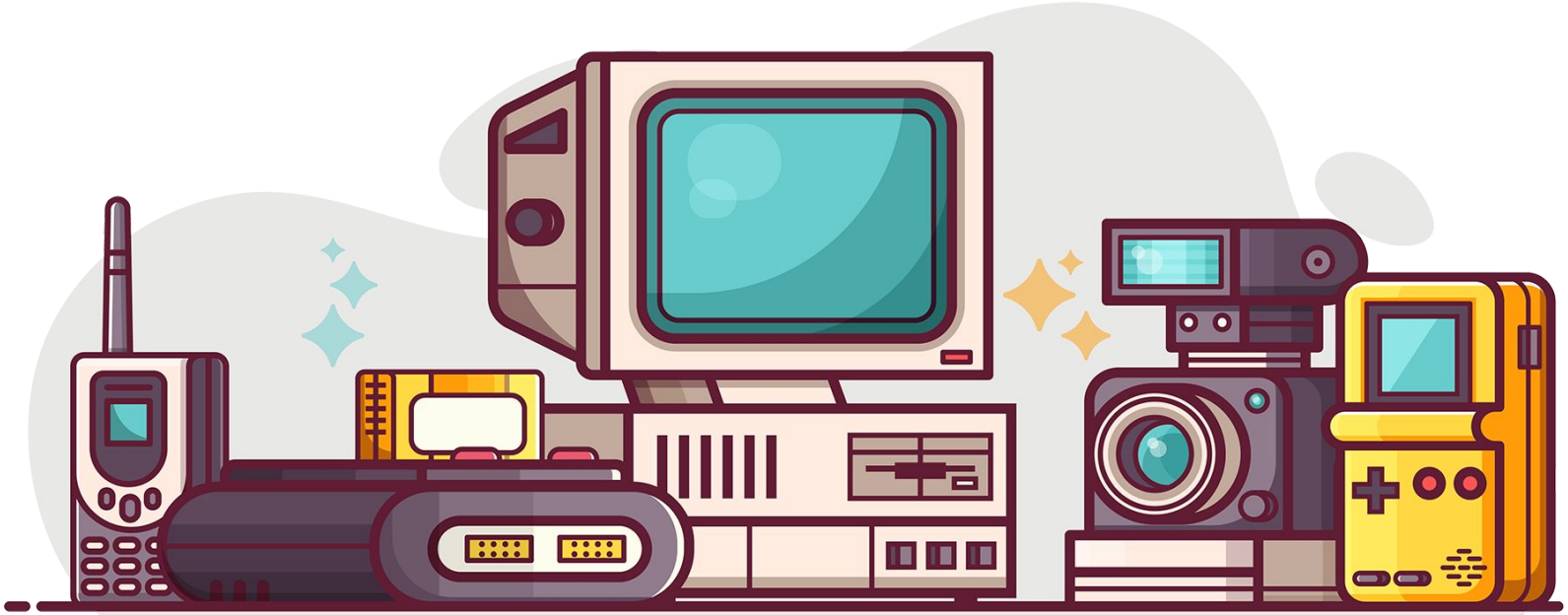
Intro to Ethereum

Ethereum secures over $20 billion in assets without a central authority. It powers a huge ecosystem of decentralized applications and financial ecosystems.



Intro to Ethereum

First generation blockchains were much like the days of carrying a cell phone, iPod, and calculator with you. Each solved a specific problem.



Intro to Ethereum

Ethereum brought to blockchains what the iPhone brought to personal computing, a general purpose platform where apps take the place of separate devices.

Intro to Ethereum

Now, you can build fully fledged applications on top of the blockchain with Ethereum.

Beyond Bitcoin: Why Ethereum Could Change The World

Smart Contracts, DApps, and ICOs will become the new internet. Ethereum brings them all together

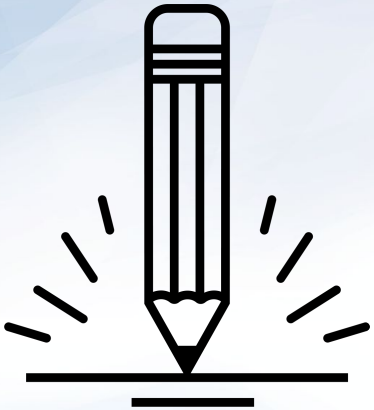
Noam Levenson Follow

Nov 30, 2017 · 12 min read

Intro to Ethereum

These are the types of financial services that you can build with Ethereum:

Payments	Remittances	Loans	Deposit taking	Notary services
Peer-to-Peer, Business-to-Business, Business-to-Customer, Machine-to-Machine.	Movement of funds across borders into a bank account.	Using crypto-currency as collateral for loans to reduce costs of transactions.	Storing crypto in wallets to use as interest-earning assets.	Blockchain based notary services that authenticates documents.
Brokerage services	**Foreign exchange**	**Decentralized crypto exchange**	**Tokenizing assets**	
Trading tokens and other digital assets on the blockchain.	Using crypto as a bridge between fiat/government currencies to reduce the cost of foreign currency fees.	Using the blockchain as a backend to support a crypto-trading exchange.	Representing things from the US Dollar, Gold, Securities, to unique video game assets an on the blockchain.	



Activity: Use Case Brainstorm

In this activity, you'll break into groups and come up with different decentralized application ideas, as well as discuss dapps you're familiar with.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Activity Review: Use Case

What are the main benefits of decentralizing your application?

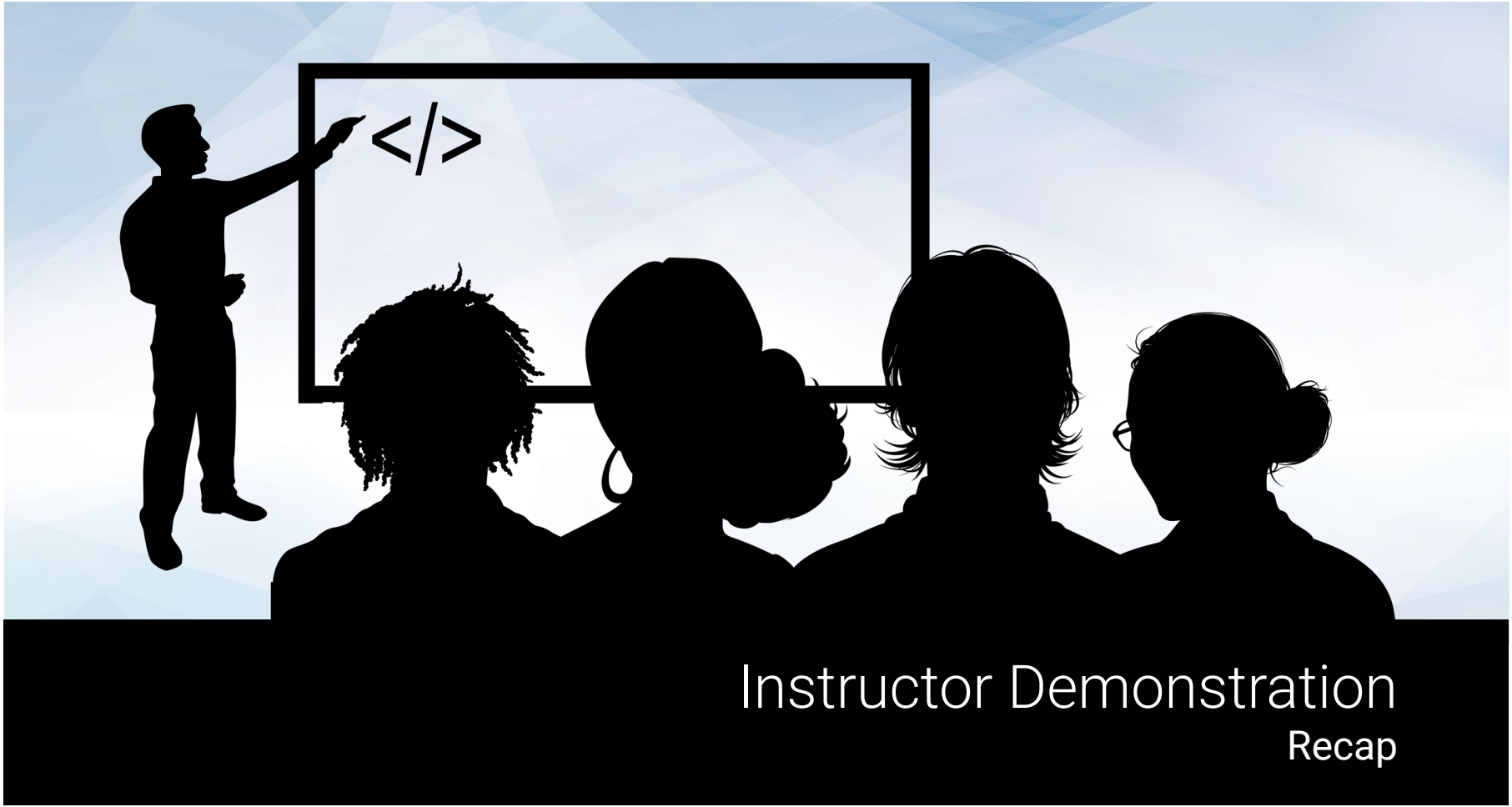
The application can only go down if the entire Ethereum network goes down.

The application can run without a central server.

The application could potentially live forever (as long as Ethereum exists).

The application is pay-per-use, much like a decentralized AWS Lambda.

If you chose a game-based use case, what type of assets have you represented?



Instructor Demonstration

Recap

Questions?


The End