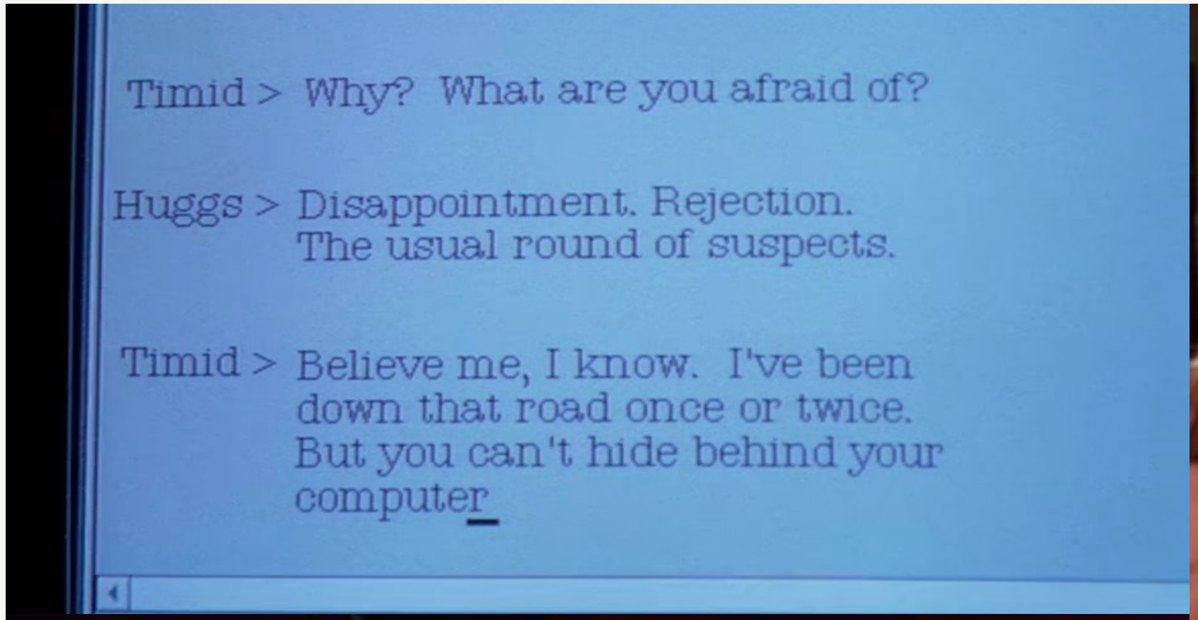
Lab 49 - Galina Fendikevich, Martin Masser and Ryan Leacock



Phoebe: How's your date with your cyber-chick going? [Gestures at laptop] Ooh, hey. What *is* all that?

Chandler: Oh, it's a website. It's the, uh, Guggenheim Museum. See, she likes art, and I like funny words.

Phoebe: What does she mean by "HH"?

Chandler: [Sheepishly] It means we're holding hands.

- First online sale was Pizza Hut in 1994 - PizzaNet
- One big problem though
- You couldn’t Pay online, nobody figured how to send money online
- Paid when you got the Pizza at your door

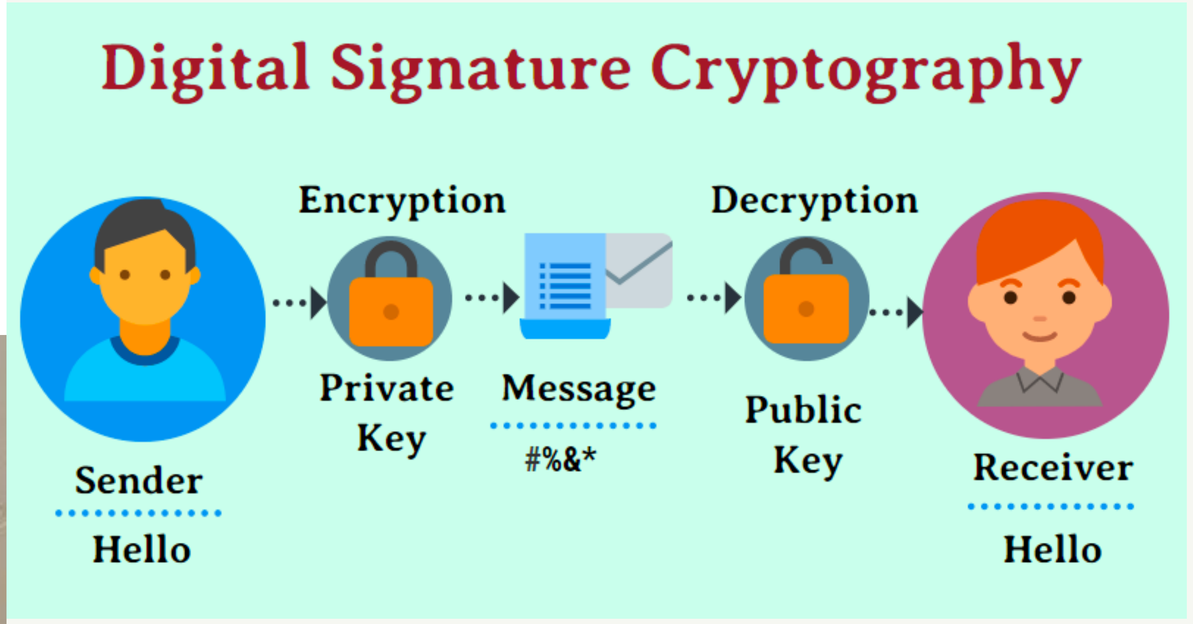
What’s cryptography?

Ancient Times - Syctale

Enigma machine - World War 2

Asymmetric Cryptography

1976 to present



Digital Innovation

Moving money

- Paypal - 1997 Making payments easy online
- Alipay - 2003
- MPESA 2007 - mobile cash people trading mobile minutes as a form of currency

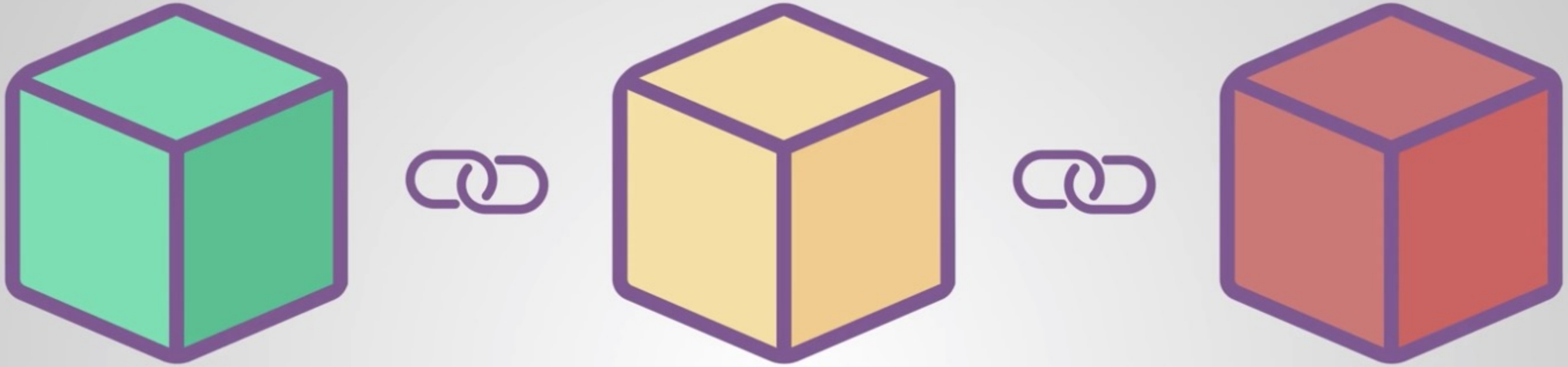
“I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”

Satoshi Nakamoto, 31st October 2008

The word’s first blockchain

Tamper-proofing data

- Stuart Haber and Scott Stornetta - envisioned the technology as a way to timestamp digital documents to verify their authenticity
- the ability to certify when a document was created or last modified is crucial for resolving things like intellectual property rights.
- time stamped “so that it is impossible to change even one bit of the document without the change being apparent.”
- impossible to change the timestamp itself.



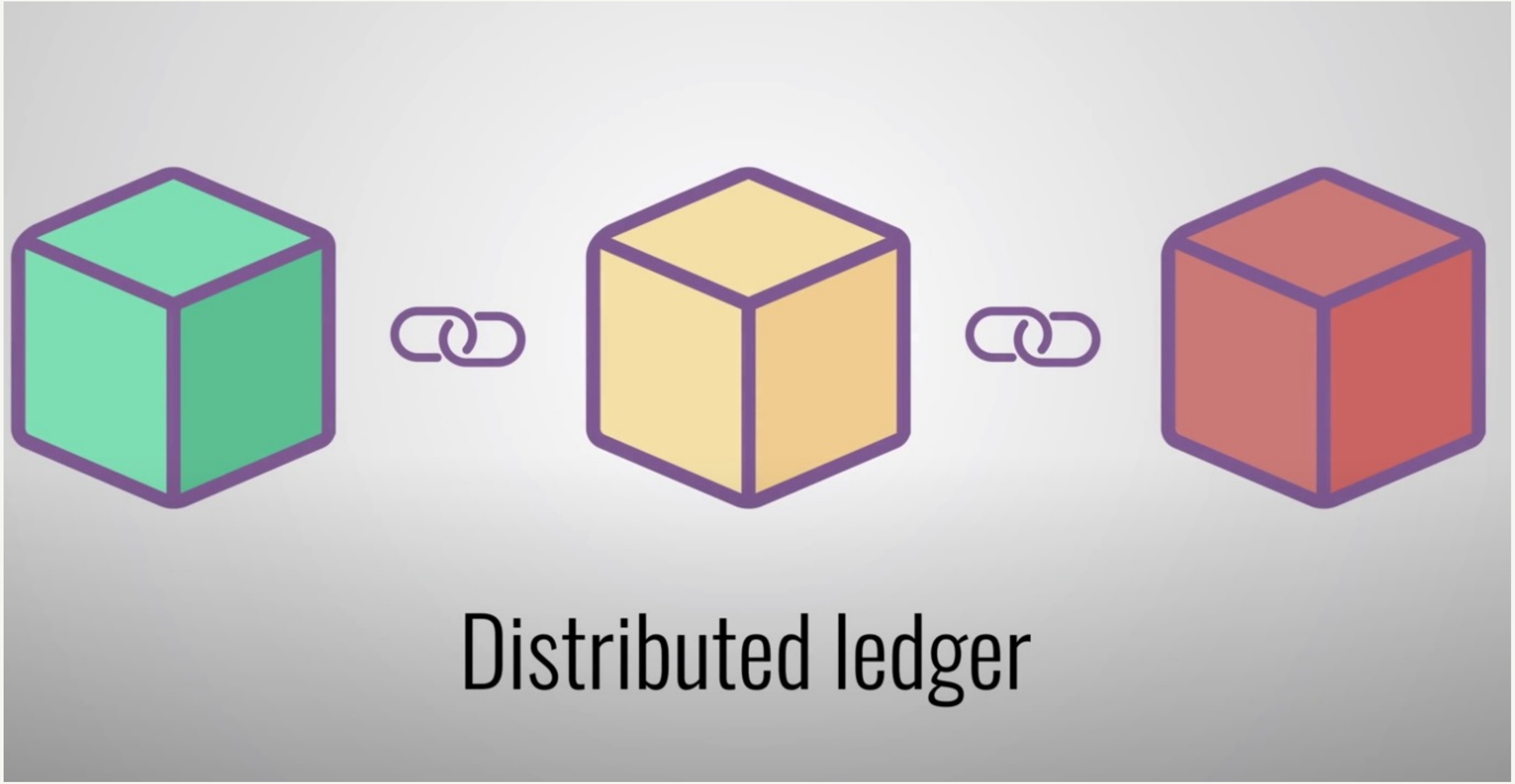
Blockchain

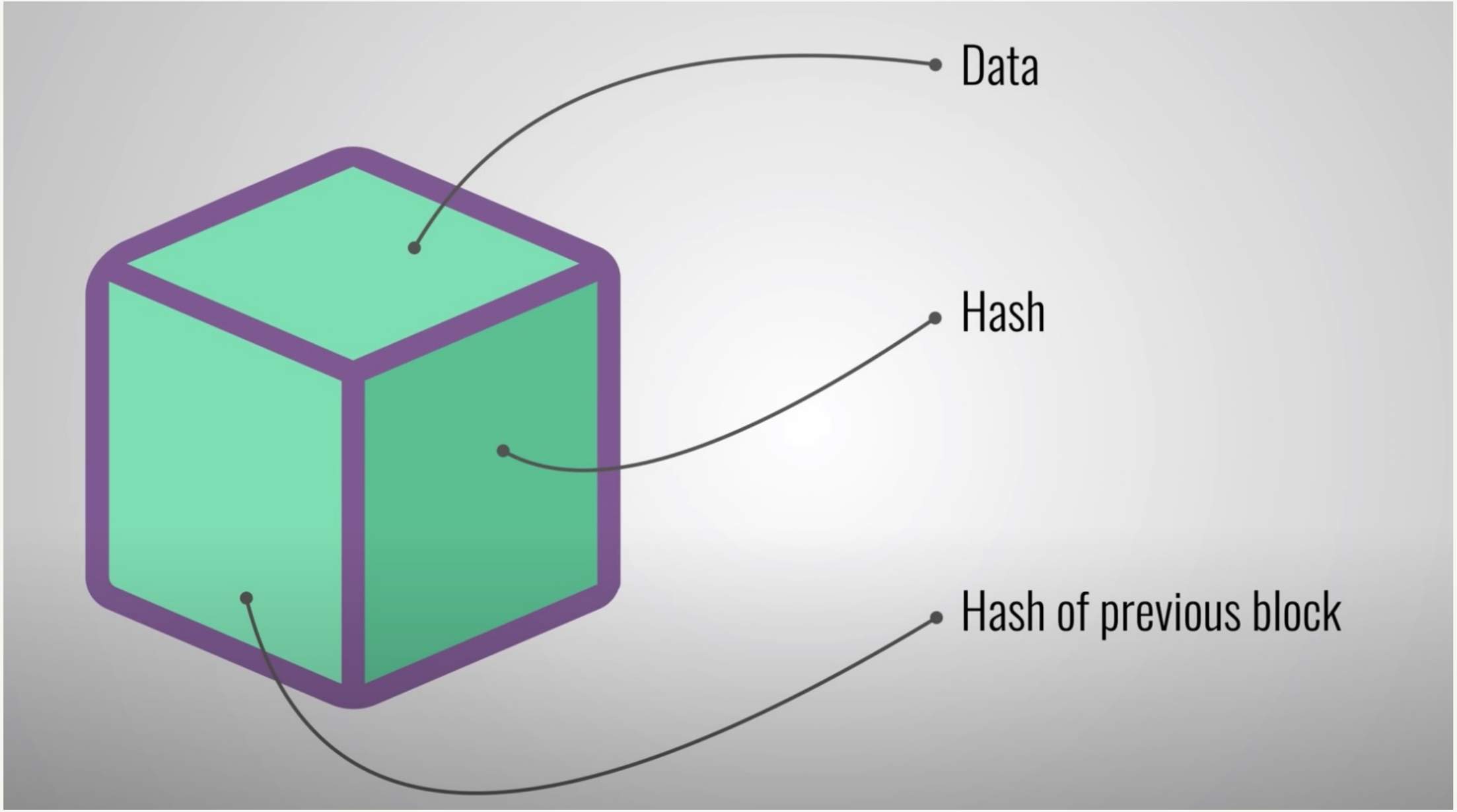
— Simply explained —

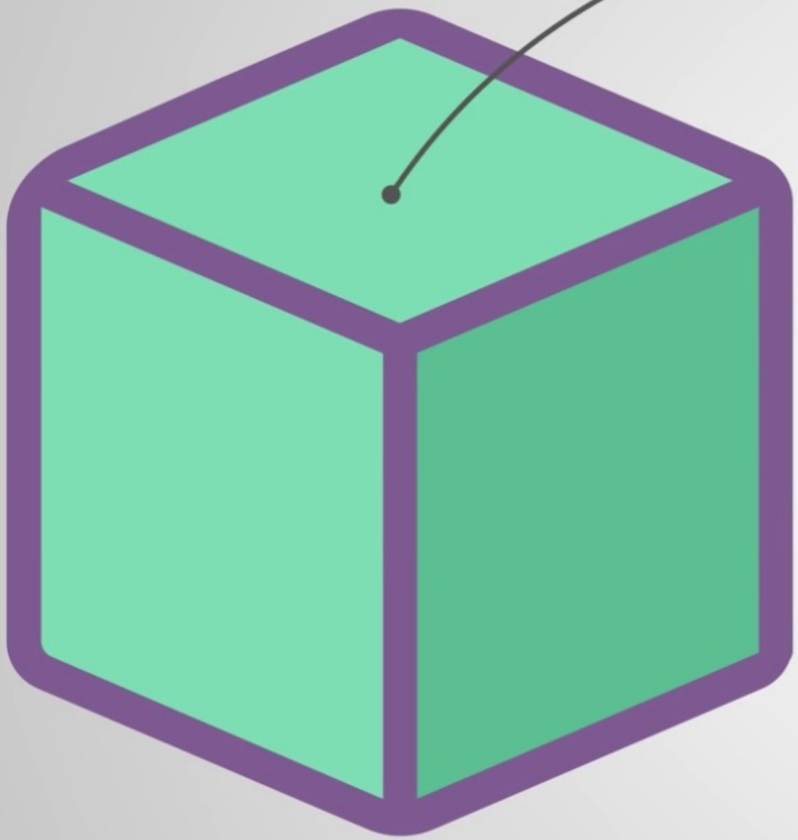
I love you, blockchain

Blockchain explained

- Central system as you can deny it, nobody can endorse it
- Central system with a backup, can convince the waiter to lie for you
- With random and multiple witnesses = Blockchain.


Distributed ledger


Data
Hash
Hash of previous block



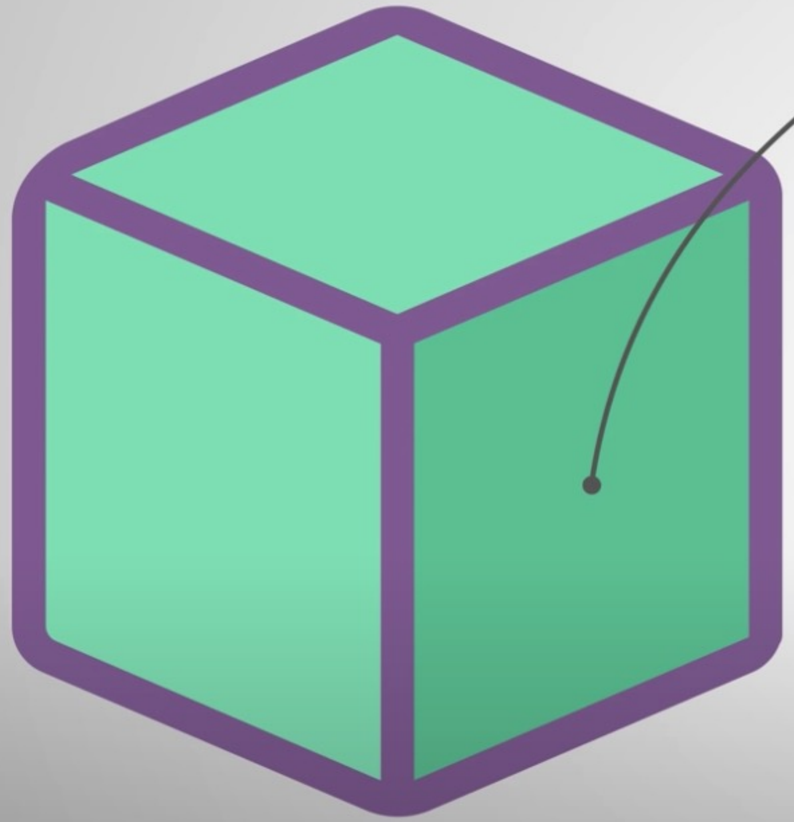
Data

From: 👩

To: 👨

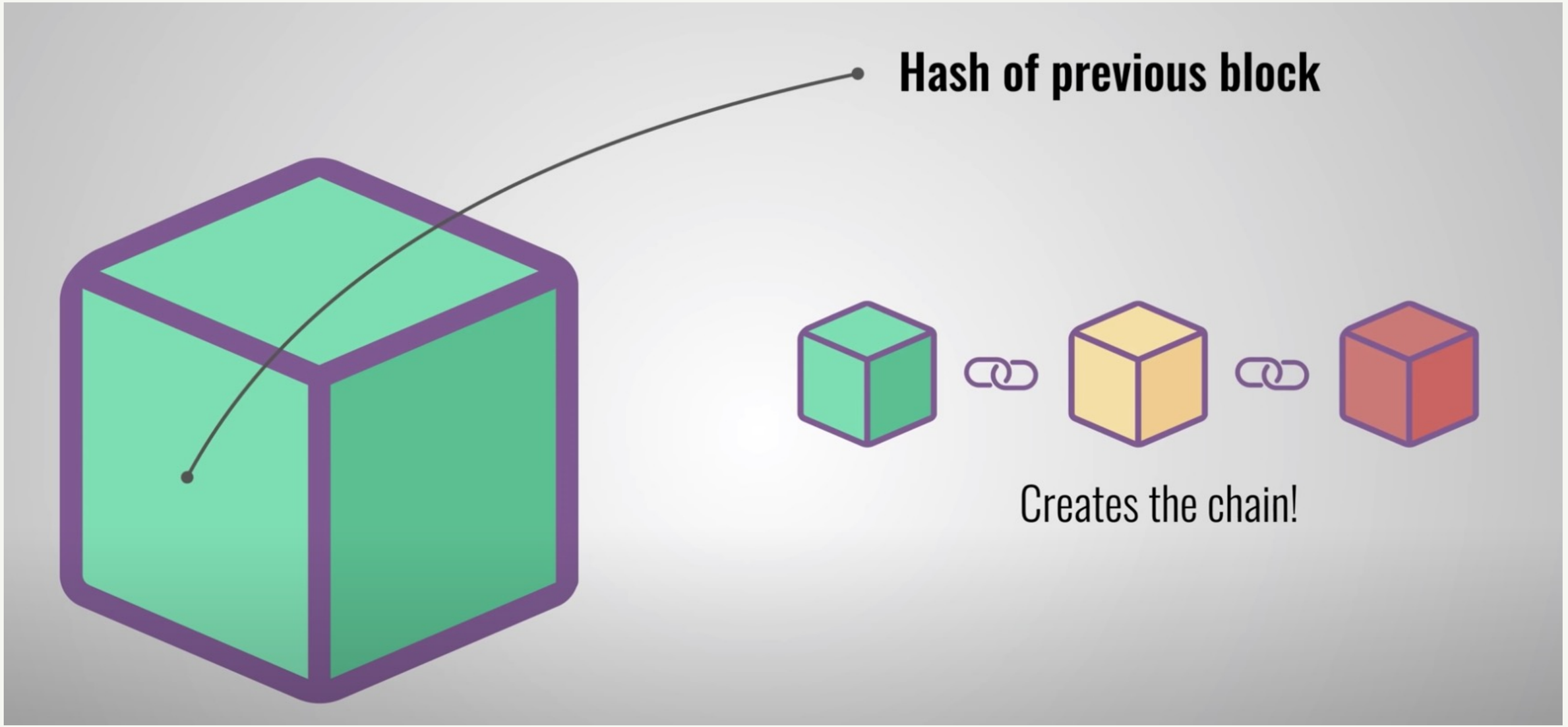
Amount: 💵

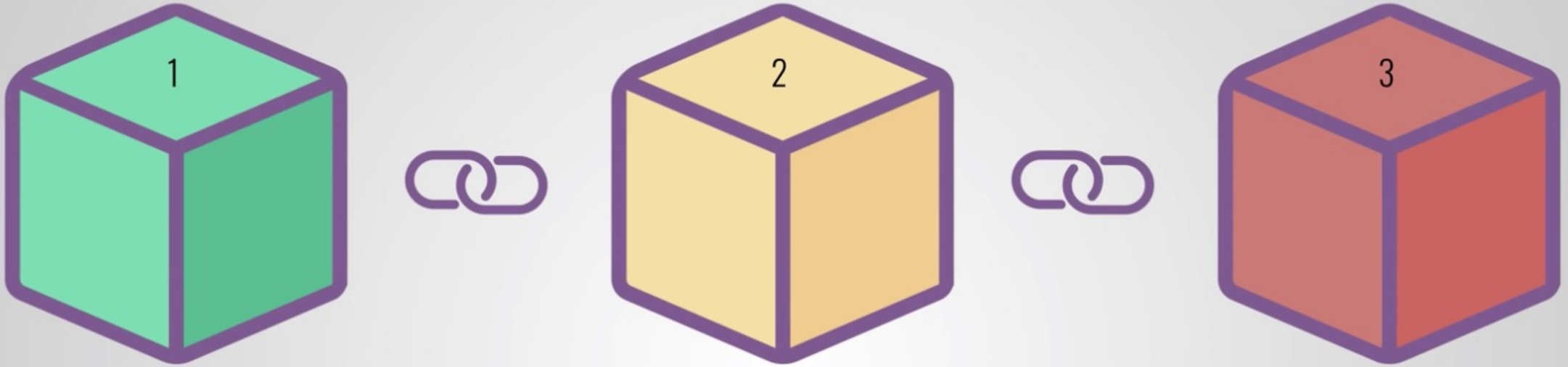
Bitcoin block example



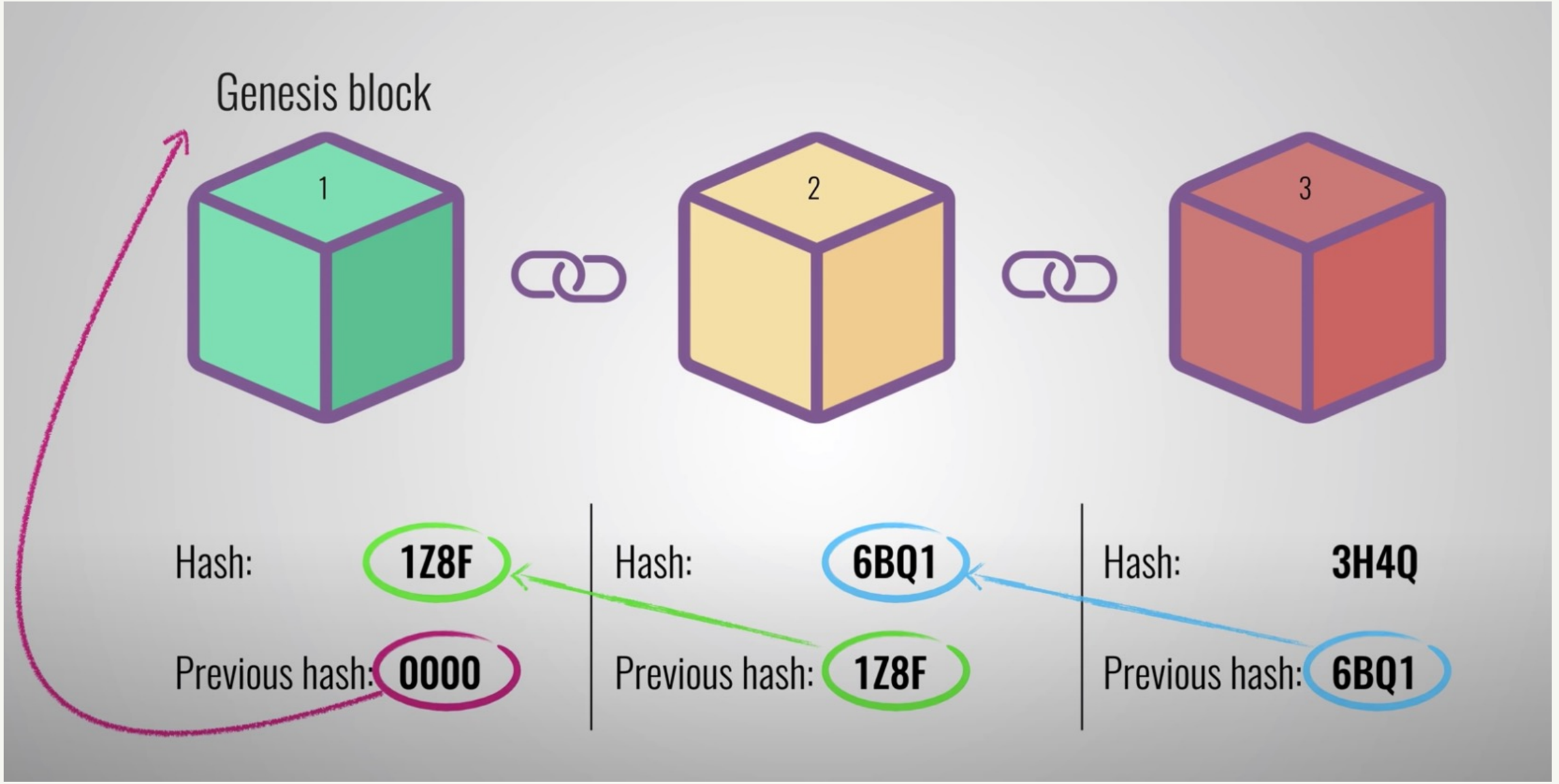
Hash

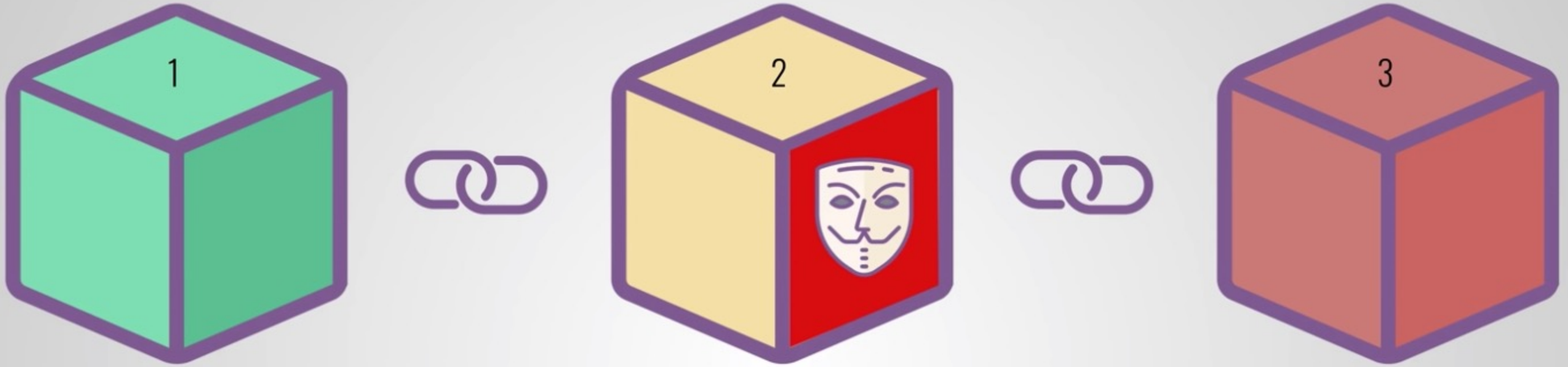
e2c521bc53bb5db4fc0aa497da2ba5d4c8444db3


Hash of previous block
Creates the chain!



Hash:	**1Z8F**	Hash:	**6BQ1**	Hash:	**3H4Q**
Previous hash:	**0000**	Previous hash:	**1Z8F**	Previous hash:	**6BQ1**


Genesis block
1
2
3
Hash:
1Z8F
Previous hash:
0000
Hash:
6BQ1
Previous hash:
1Z8F
Hash:
3H4Q
Previous hash:
6BQ1



Hash:	**1Z8F**	Hash:	~~6BQ1~~ **H62Y**	Hash:	**3H4Q**
Previous hash:	**0000**	Previous hash:	**1Z8F**	Previous hash:	**6BQ1**

Uh thats not right??

Slow and steady...

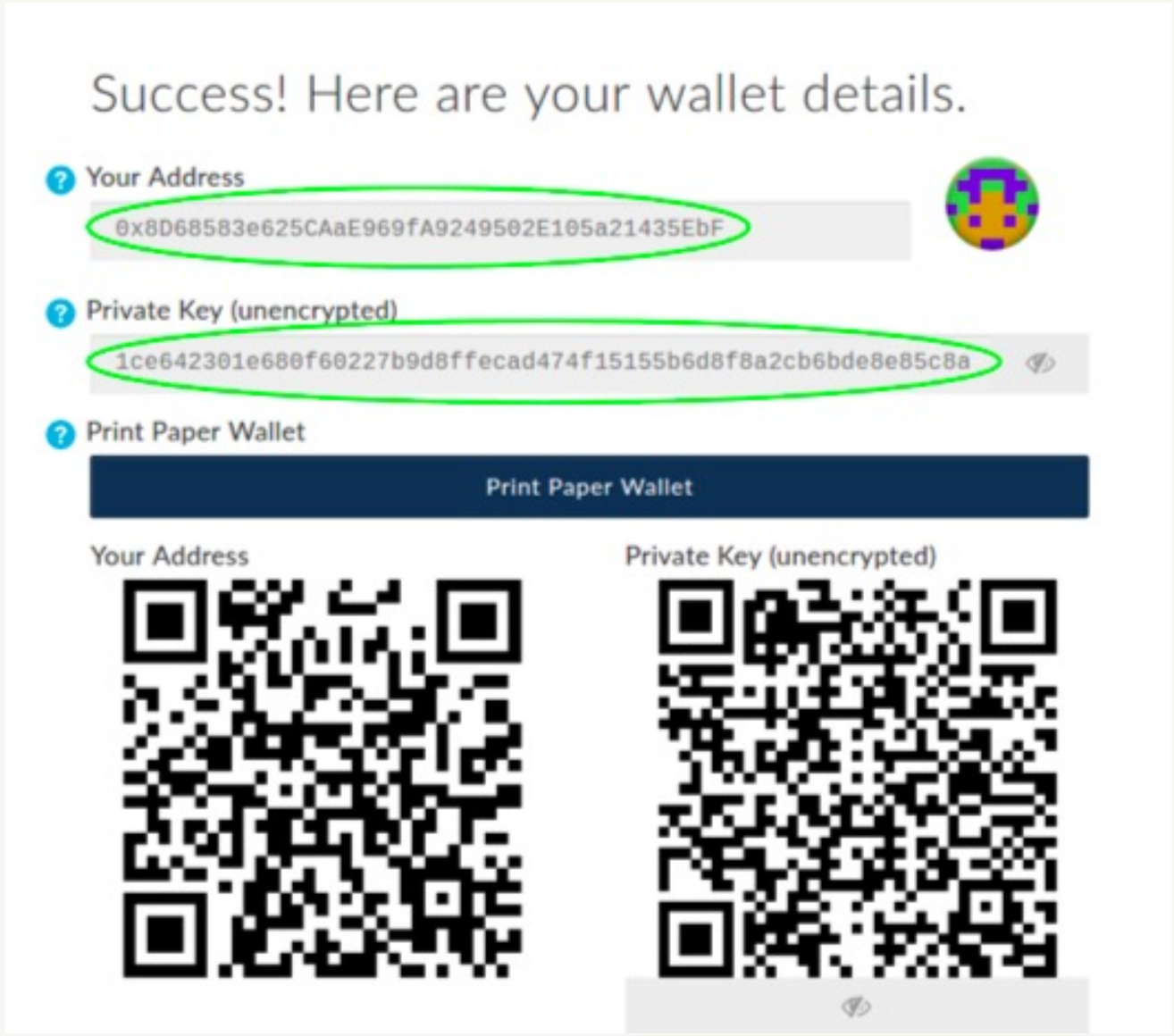
Proof of work

Proof of Work (POW)

Consensus mechanism

- It is the consensus mechanism (e.g. Proof-of-work) that allows us to distinguish a valid from an invalid blockchain
- Winner that everyone can verify
- The winner of the lottery must prove that they won it fair and square by producing a solution to a puzzle that doesn’t have any shortcuts outside of work/stake

Being your own bank



Your Seed Phrase

Your Seed Phrase is used to generate and recover your account.

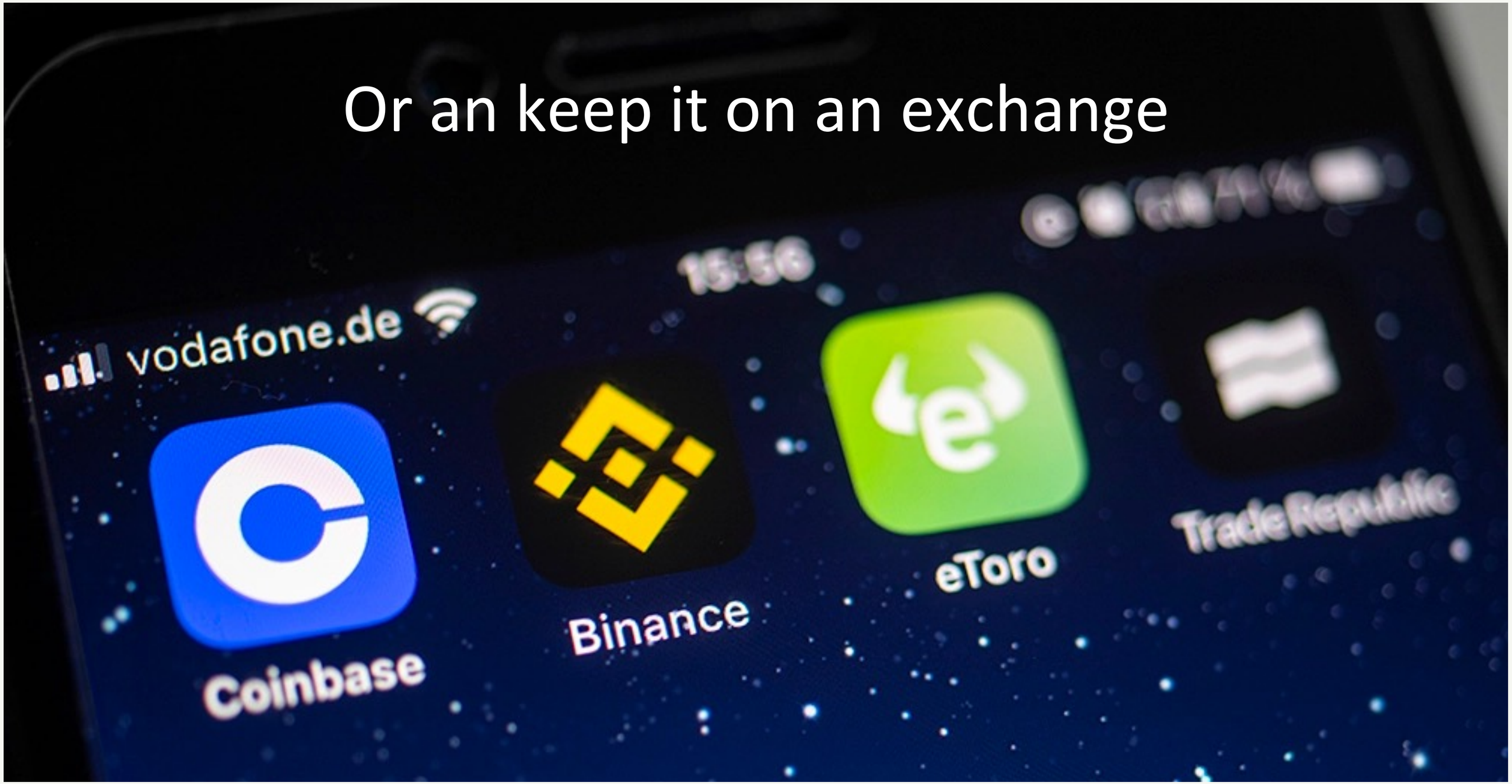
1. issue	2. flame	3. sample
4. lyrics	5. find	6. vault
7. announce	8. banner	9. cute
10. damage	11. civil	12. goat

Please save these 12 words on a piece of paper. The order is important. This seed will allow you to recover your account.

I understand that if I lose my seed phrase that I will not be able to recover my account.

Accept

Or an keep it on an exchange



Not your keys, not your crypto


Who doesn’t like pizza?

Author | Topic: Pizza for bitcoins? (Read 327851 times)

laszlo
Full Member

Activity: 199

Trust: **0**: -0 / +0(0)
Ignore

Pizza for bitcoins?

May 18, 2010, 12:35:20 AM

quote #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

Report to moderator

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

laszlo
Full Member

Activity: 199
Merit: 590

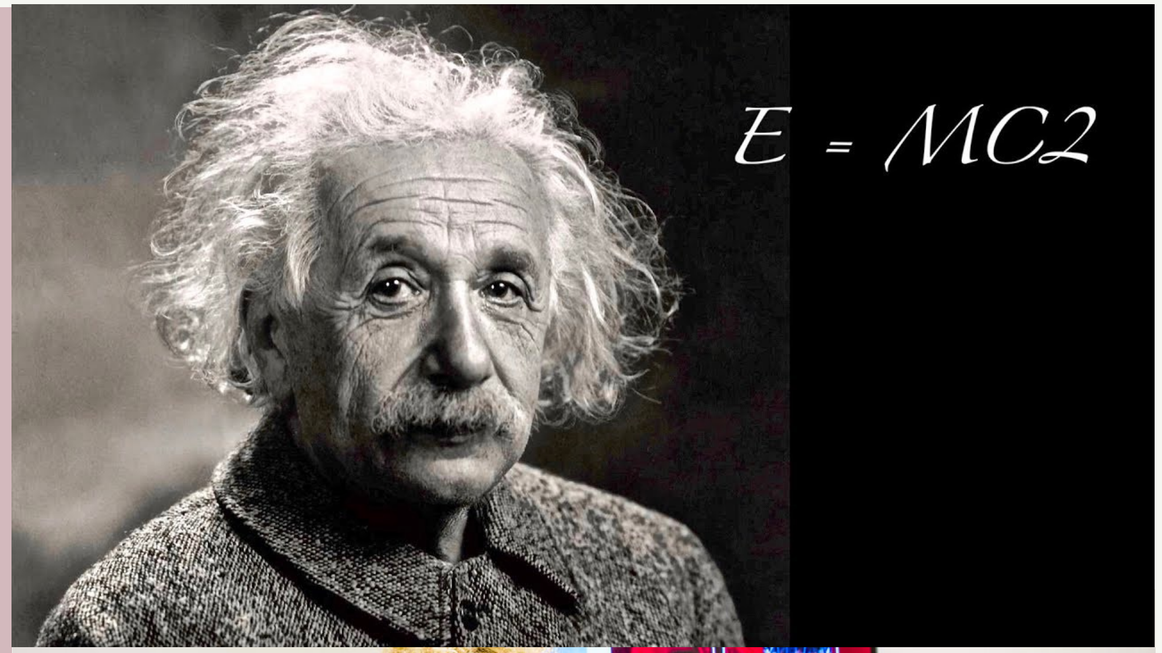
Re: Pizza for bitcoins?
May 22, 2010, 07:17:26 PM

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

Smart Contracts



Kickstarter

My cooler idea

- I have an idea of an amazing cooler and a goal to raise $100,000 in donations
- Want to give my cooler to everyone who donates $100
- After a week, I pass my goal of $100,000
- Kickstarter will now give me my $100,000 money after holding it
- If I didn’t get my goal, Kickstarter will return the money to everyone

Just a piece of code

</>

- Most common is : If this, Then that
- Ethereum used (solidity)

```
{-# STDLIB_VERSION 3 #-}
{-# SCRIPT_TYPE ACCOUNT #-}
{-# CONTENT_TYPE DAPP #-}

@Callable(i)
func request (name: String) = {
    # verify the certificate is not in data state yet
    let wasRequested = match getInteger(this, name) {
        case a: Int => true
        case _ => false
    }
    if (wasRequested)
        # throw a friendly exception
        then throw("The certificate was already requested")
        # store the certificate request
        else WriteSet([DataEntry(name, 0)])
    }

@Callable(i)
func approve (name: String, id: Int) = {
    # verify the call is made by dApp owner
    if (this != i.caller)
        # throw a friendly exception
        then throw("dApp owner allowed only")
        # add certificate ID to the state
        else WriteSet([DataEntry(name, id)])
```

Smart Contracts Swapping

1 Eth for 1,000 Doge

Smart Contracts Rewards

If you get over 1m subs on YouTube

Then YouTube will pay you $100,000

Smart Contracts Insurance

If it is 95+ degrees for 5 days in a row this year

Then Farmer Phil gets $100,000 as insurance

Insurance

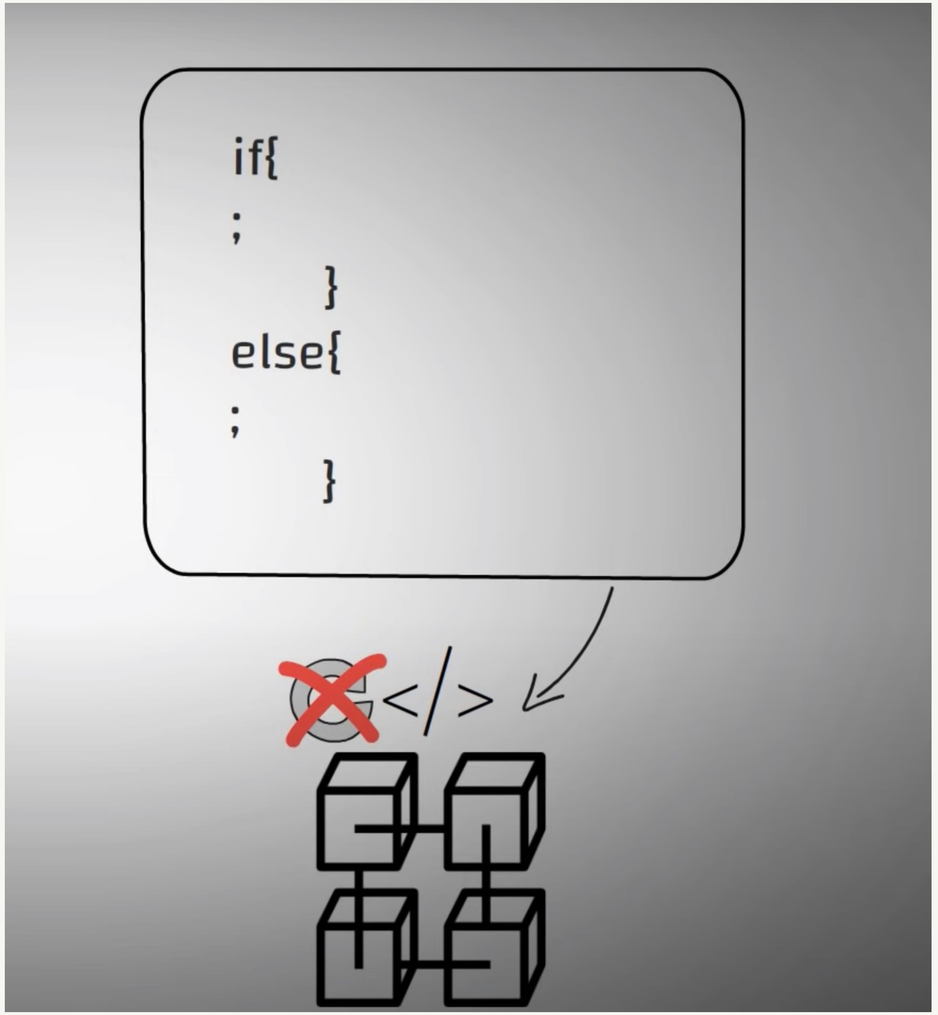
Oracles - helpful tools to any smart contract

Trust source for real world information to be sent to a smart contract

Two benefits of smart contracts

Can’t change it

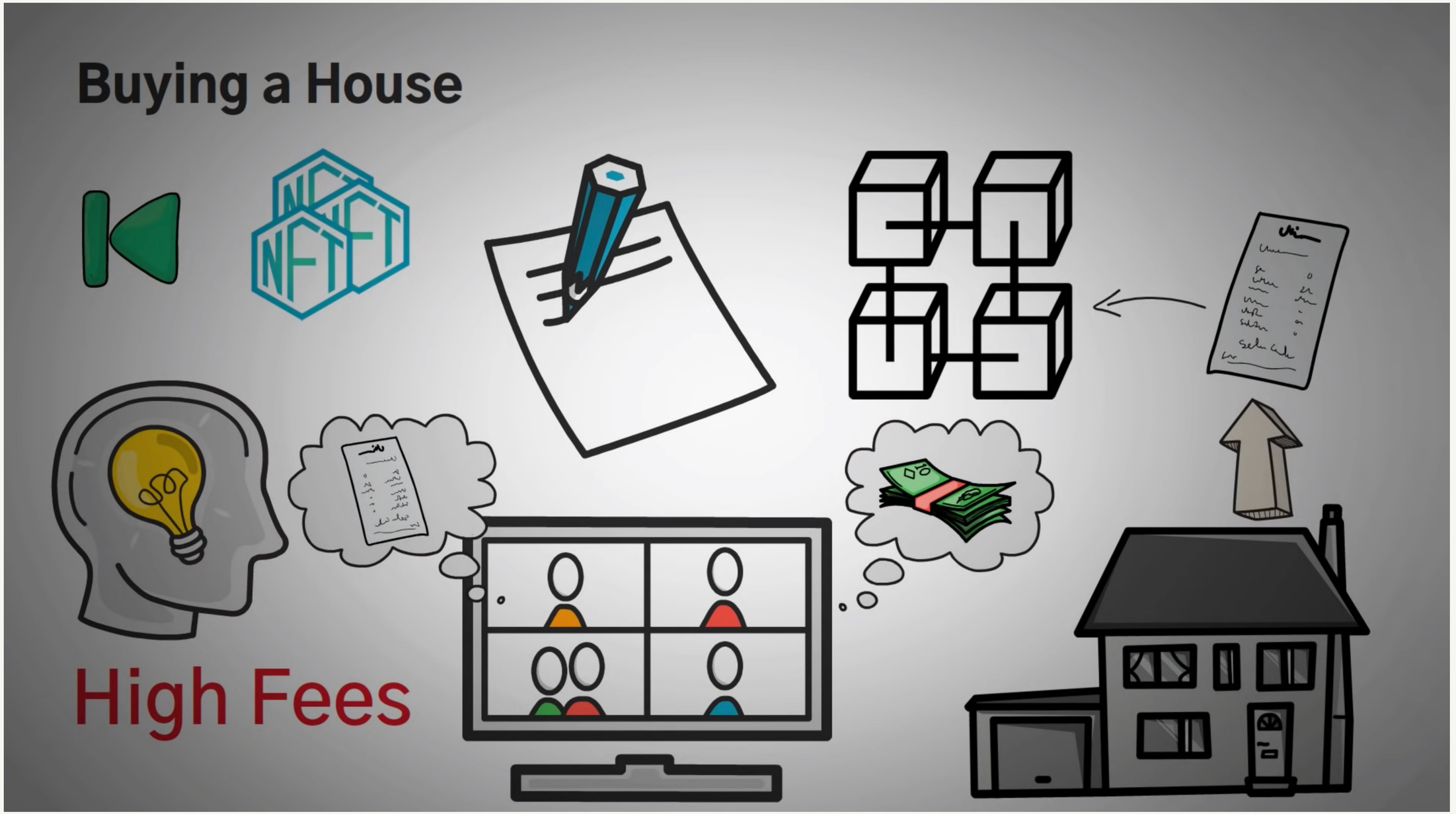
- Immutable - they do not change
- What happens if there is a bug?
- You would just change the smart contract and tell people to use the new one



Two benefits of smart contracts

Distributed

- Distributed - means no discrepancies, anyone can view it
- No need for lawyers
- These are contracts that are between a few parties that are automatically executed, when certain conditions are met
- It’s code that removed human errors and issues

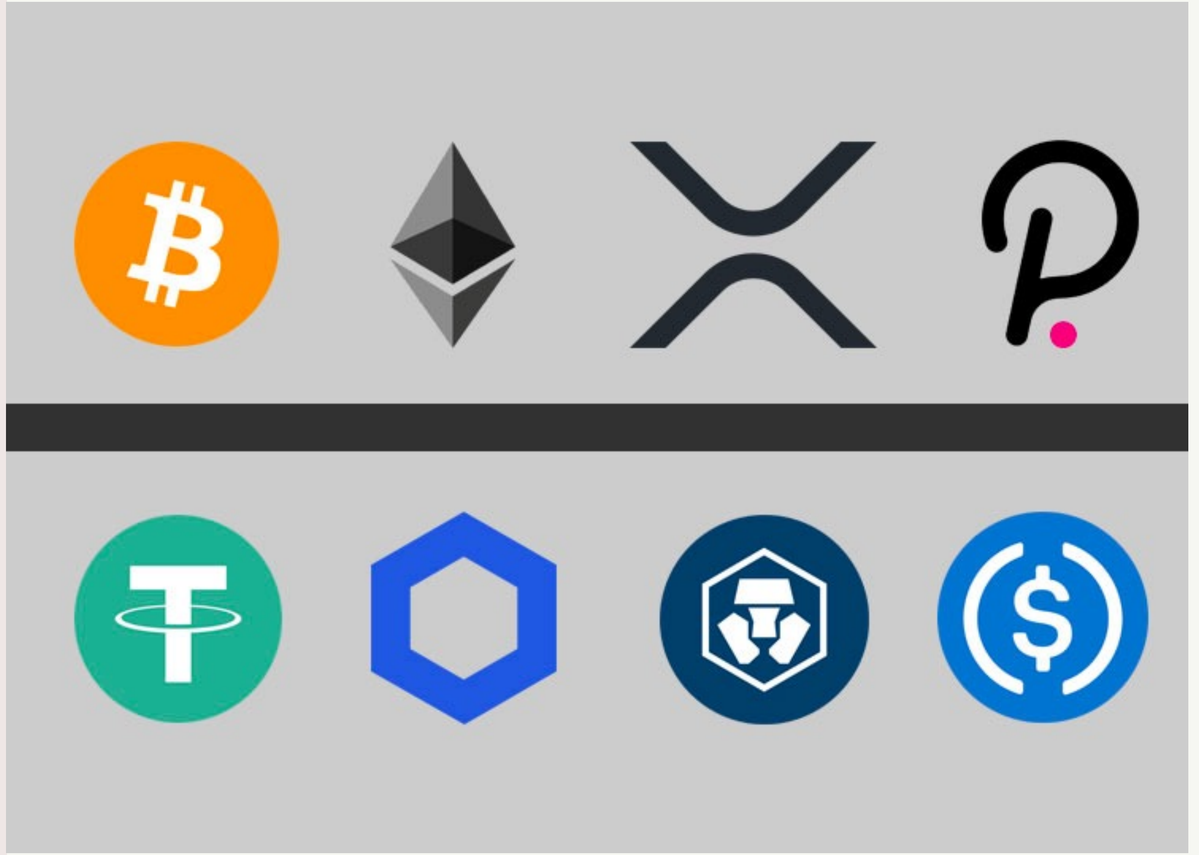

Buying a House
NFT
High Fees


GUESS WHAT? I'VE BEEN IN YOUR HOUSE WHEN YOU WEREN'T HOME!
AND YOURS. AND YOURS. NO,
I'M NOT A BURGLAR. I'M A REALTOR.

Coins v Tokens

Aren’t they the same?

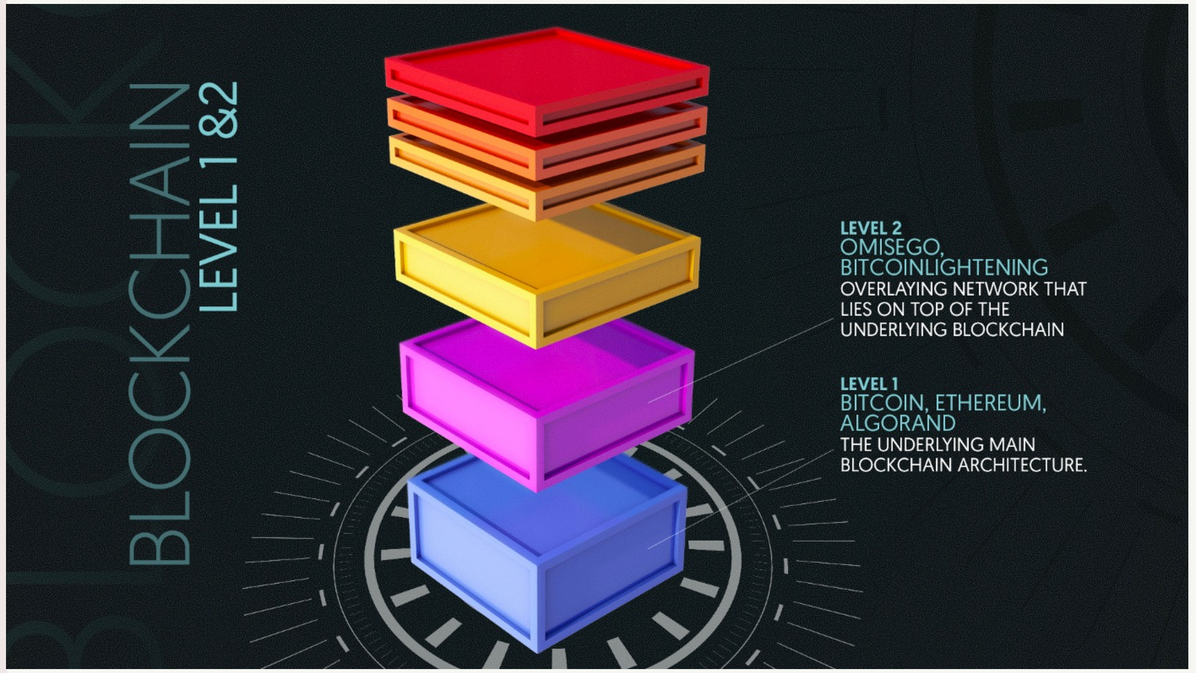
- Coins there own network / own independent blockchain (BTC/ETH/LTC)
- Token is the opposite. It is a cryptocurrency that does not have its own blockchain. Instead it operates on another blockchain (USDT/BAT/DOGE/NFTs/DApps)
- Token are - Utility Tokens, Security Tokens, Asset Tokens, Stablecoins, DEFI, Equity Tokens and Non-Fungible Tokens (NFTs)



How to scale

Layer 2

- Blockchain technology comes with many benefits:
- However, as its usage becomes more common, a number of problems are surfacing. One such problem is scalability.
- Layer 2 scaling solutions don’t tamper with the base layer protocol.
- Additionally, these solutions allow multiple microtransactions without requiring users to pay sky-high transaction fees, or waste time on miner verification.



Layer 1 vs Layer 2 Protocols

Base Layers

Scaling

Over to Ryan
For some Demos