BLOCKCHAIN PRIMER

02.24.18

Sage Franch
@theTrendyTechie

Sage Franch aka @theTrendyTechie

- Blockchain educator
- Former Microsoft Azure evangelist and MOOC instructor
- Creator of tech lifestyle blog trendytechie.ca

```
Level.set(0);
```


bitcoin

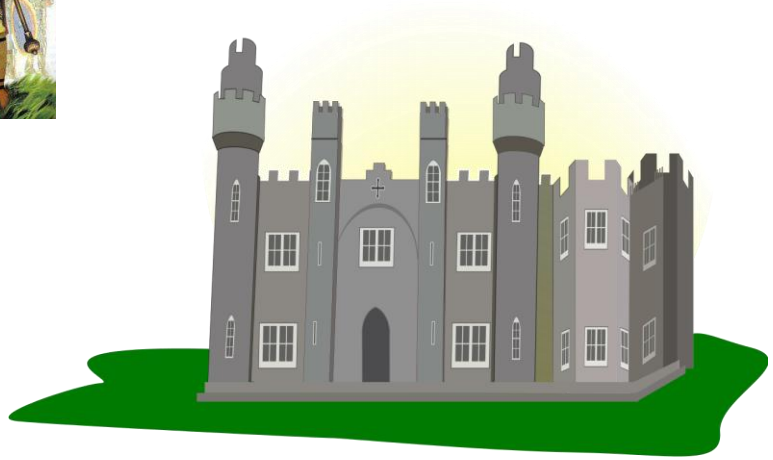
bitcoin Whitepaper

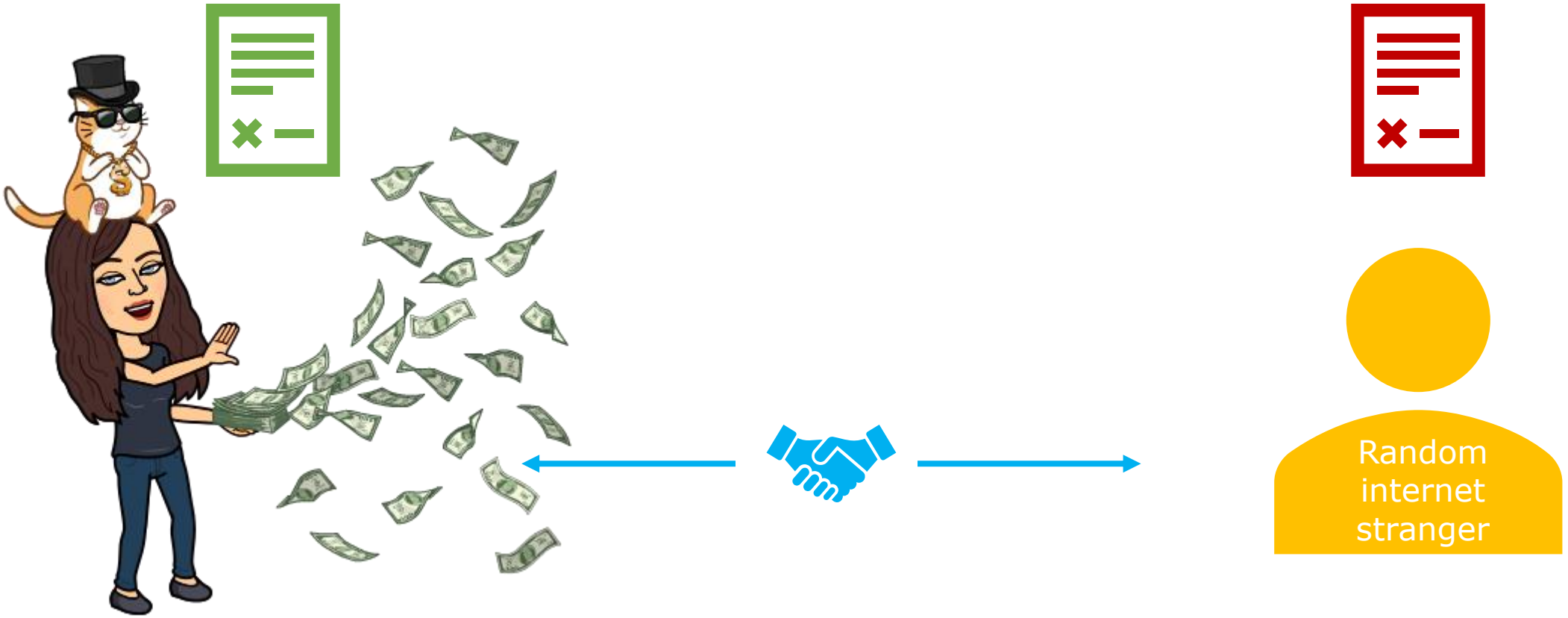
We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

https://bitcoin.org/bitcoin.pdf

Byzantine Generals Problem



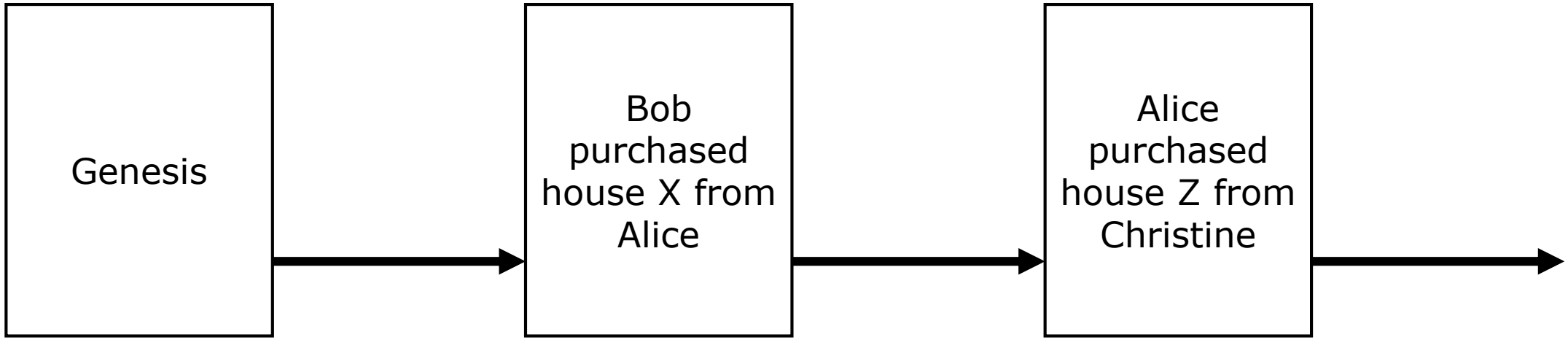

Random
internet
stranger


3rd party authority
TRUST
Random internet stranger

When the ledger is maintained by one entity

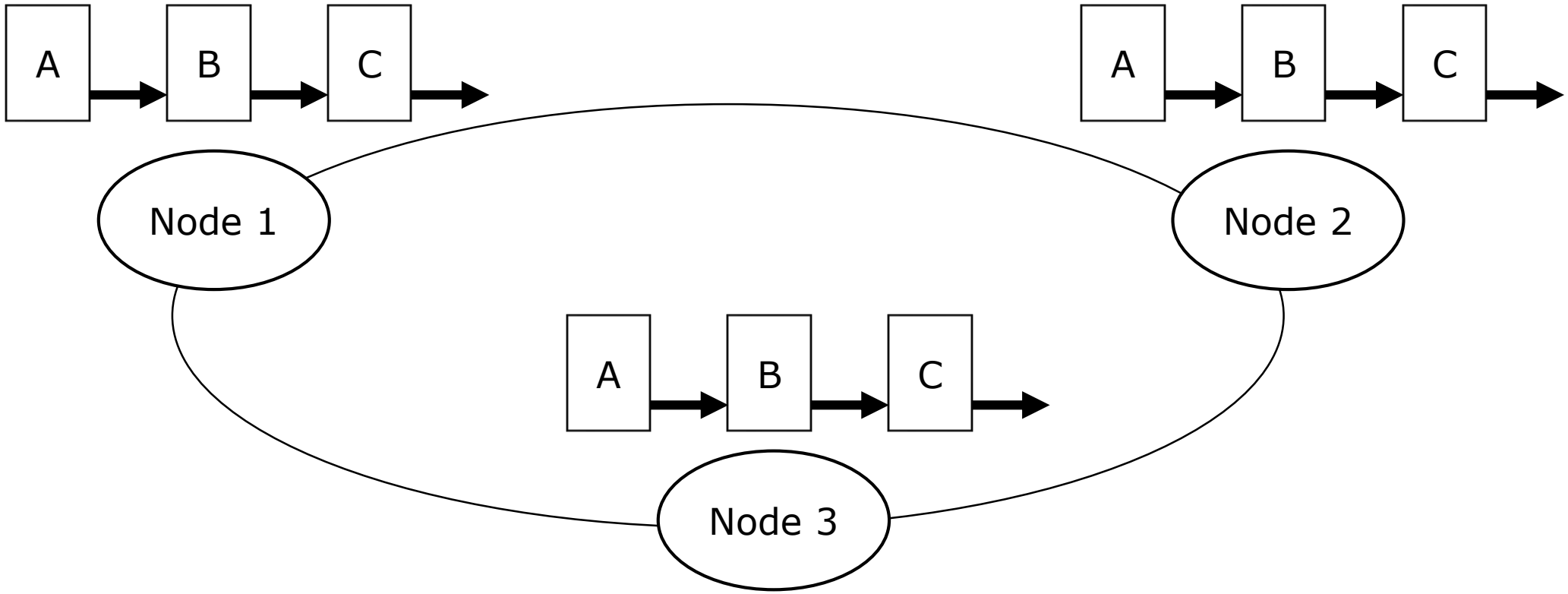
Property	Ownership
House X	Alice <-Bob buys X
House Y	Bob
House Z	Christine <-Alice buys Z
…	…

The same records on a blockchain



So who maintains them?

Everyone!



Decentralization
+
Immutability

TRUST in the digital age

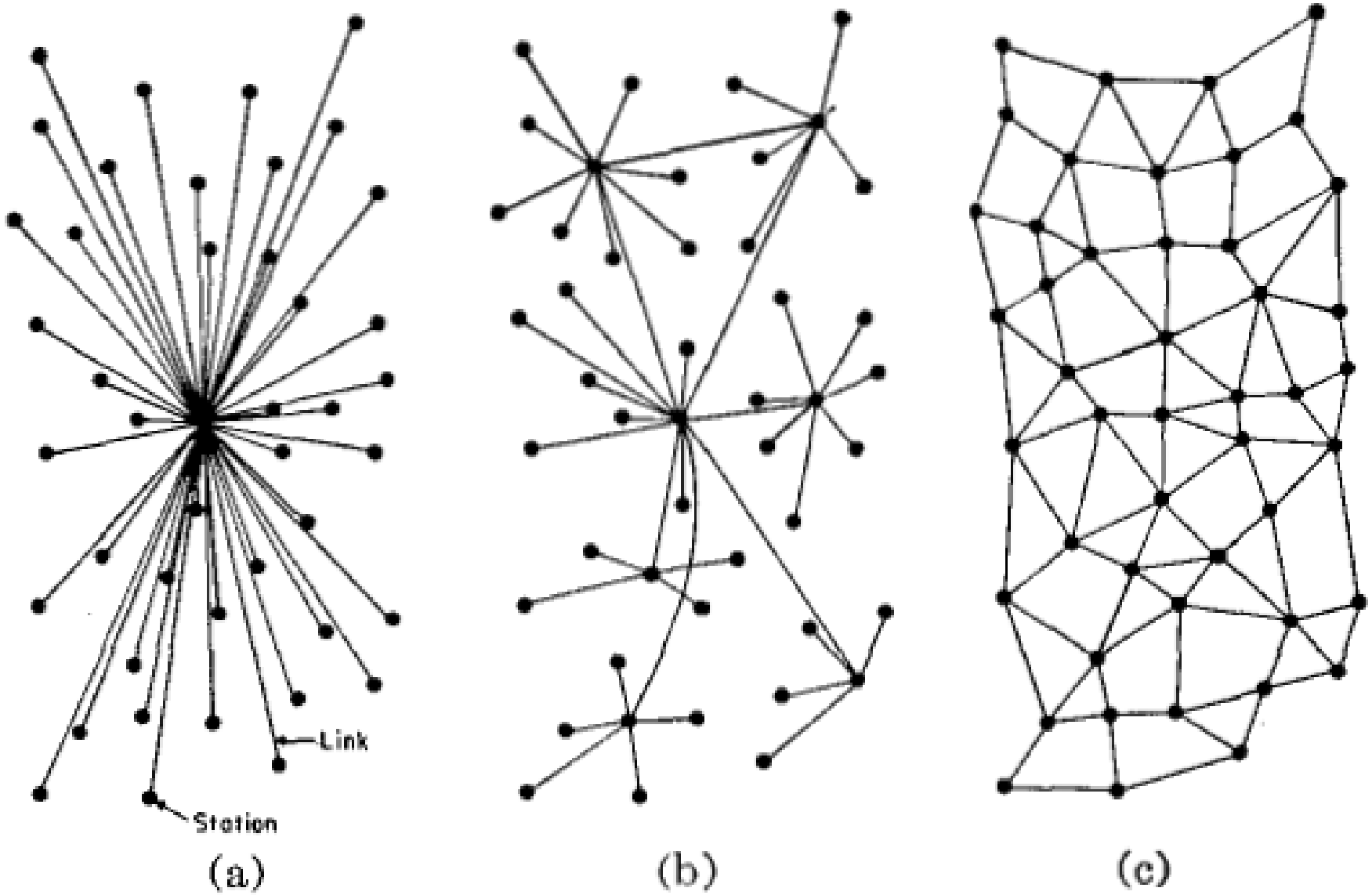


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

http://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf

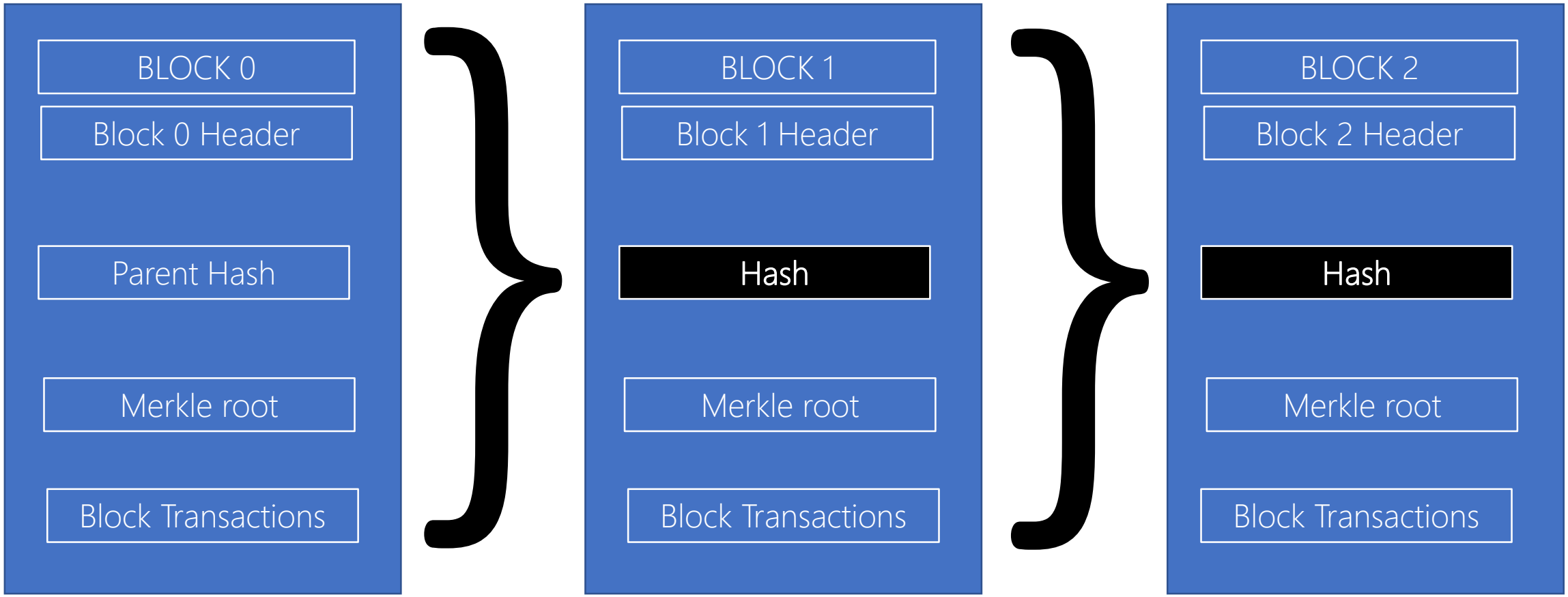
Consensus

Consensus

Consensus

Consensus

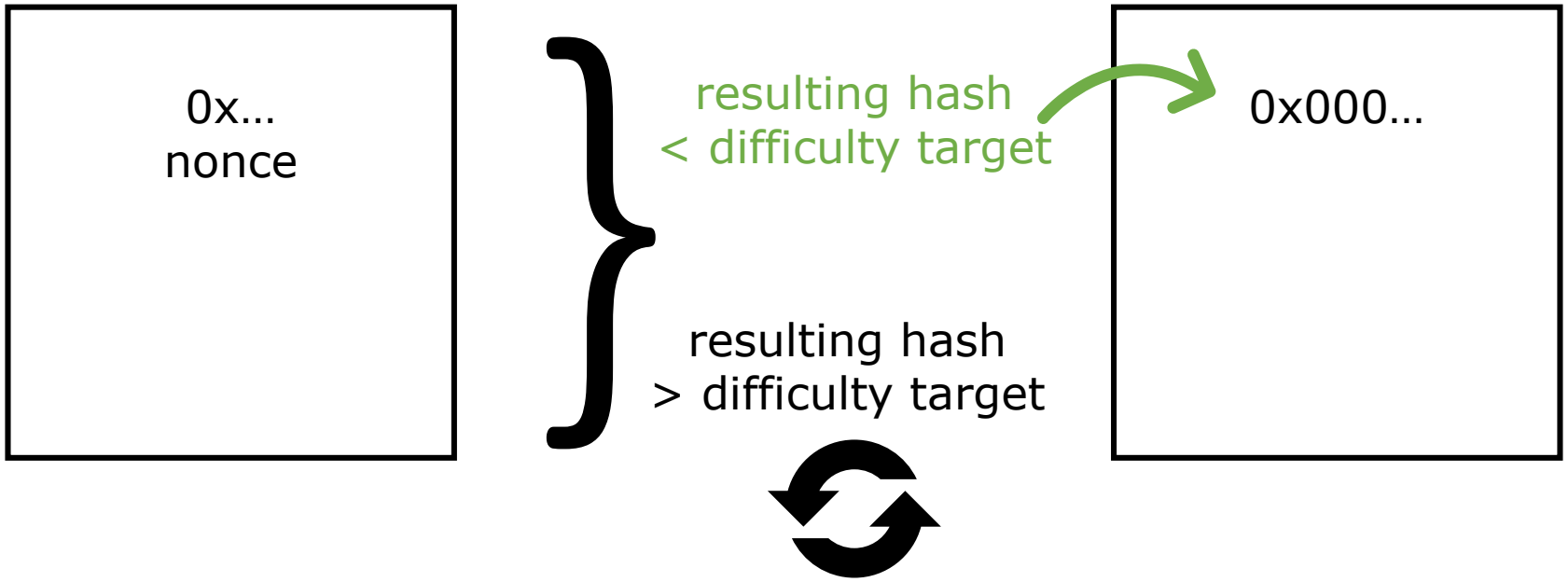
Consensus

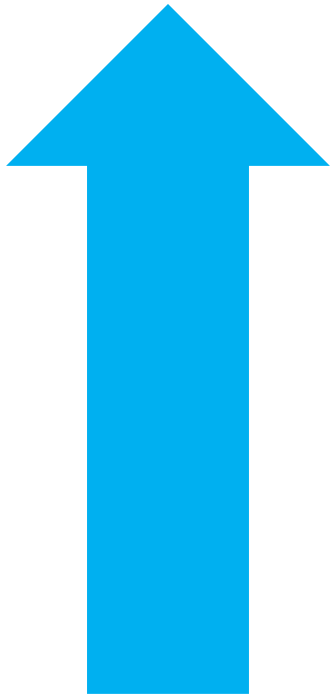


Immutability

Proof of Work

Hard to produce, easy to verify





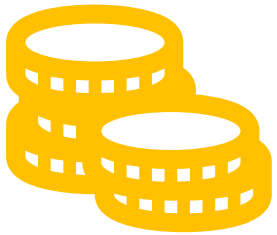
nodes

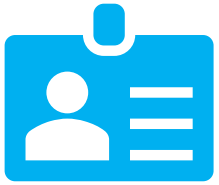
security

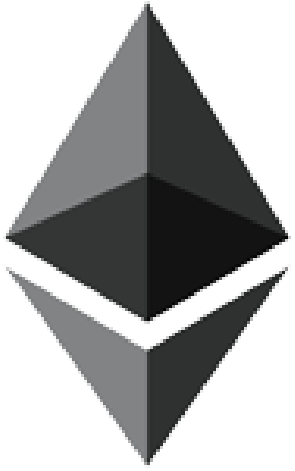
transaction speed

Decentralized Applications

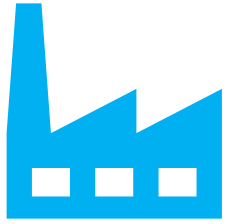
aka “Dapps”

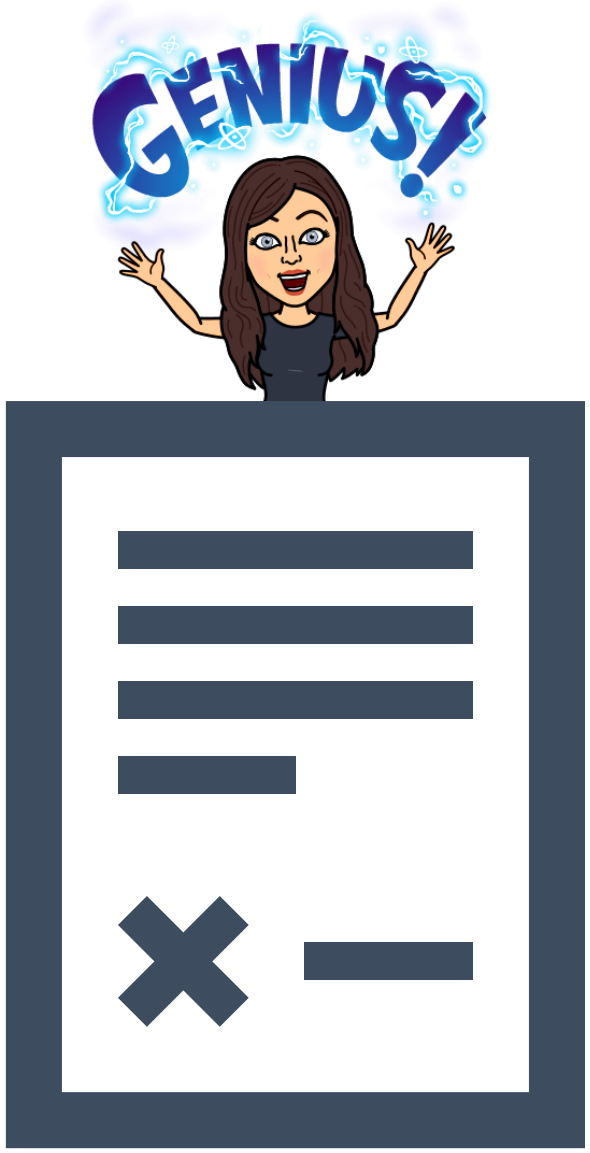






ethereum

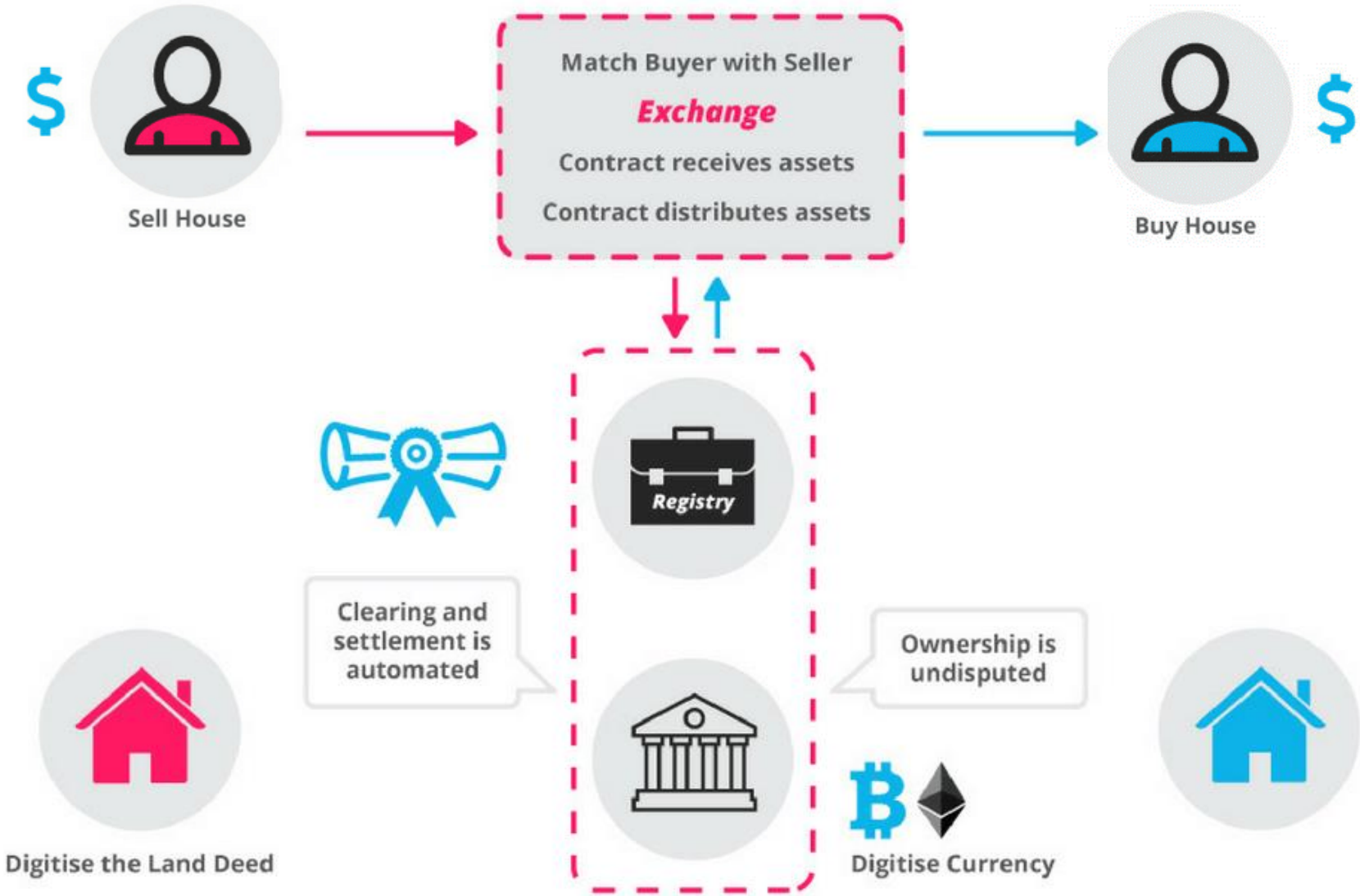




Smart Contracts

How Smart Contracts Works

Blockgeeks



Smart Contracts Are…

- Published on the blockchain
- Executable by any participant
- Not protected

Blockgeeks

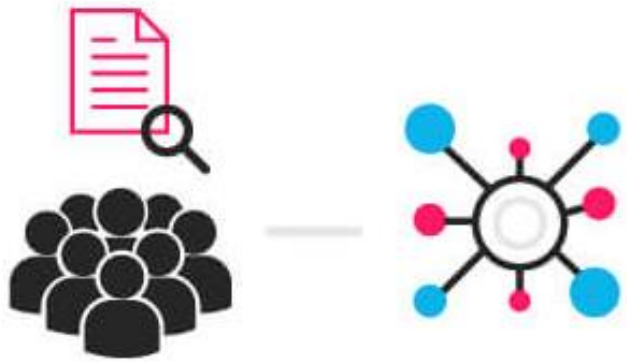
1

An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

2

A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

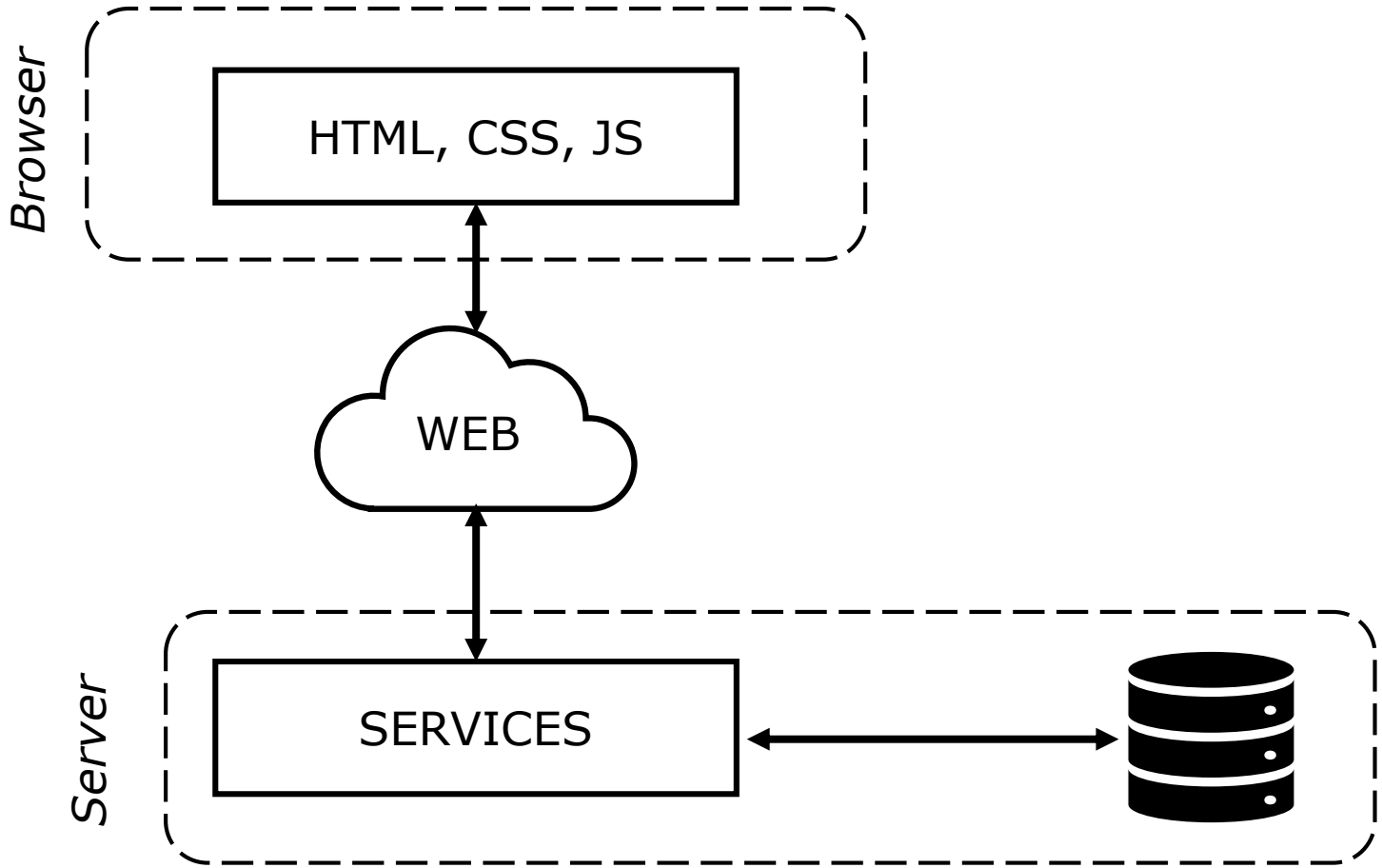
3



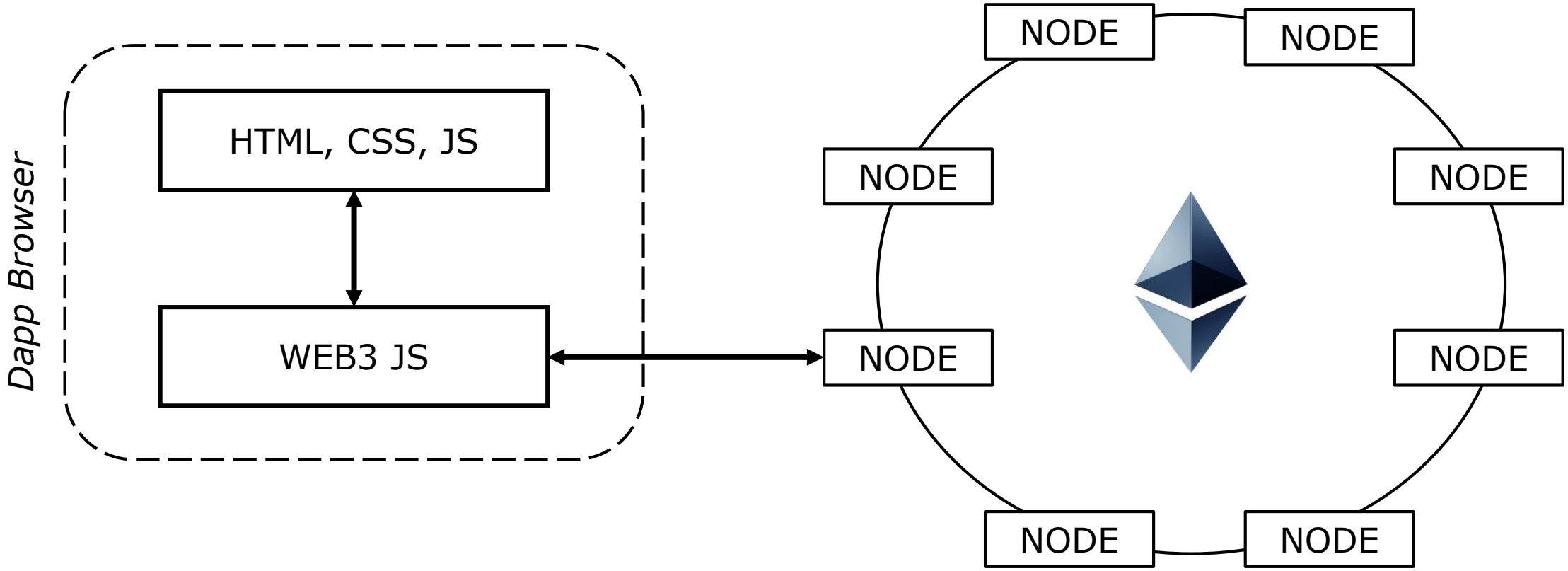
Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

Building a Dapp

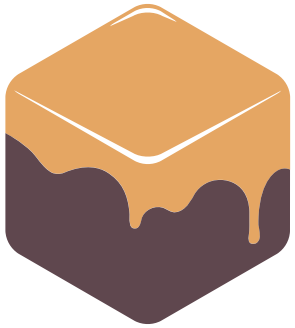
Traditional Web App Architecture

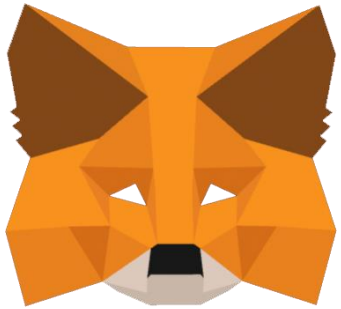


Dapp Architecture




TRUFFLE





Let’s code!

1. “Hello Blockchain” with ganache-cli
2. Using Truffle to interact with smart contract
3. Using Ganache GUI with Truffle
4. Building a booking Dapp

Starter Project At:
github.com/thetrendytechie/bed-and-blockchain-start

Complete Code At:
github.com/thetrendytechie/bed-and-blockchain

All Resources At:
github.com/thetrendytechie/blockchain101