Blockchain & Cryptocurrencies

Marios Karagiannopoulos

Western Greece Software Developers Group, POS, December 2017

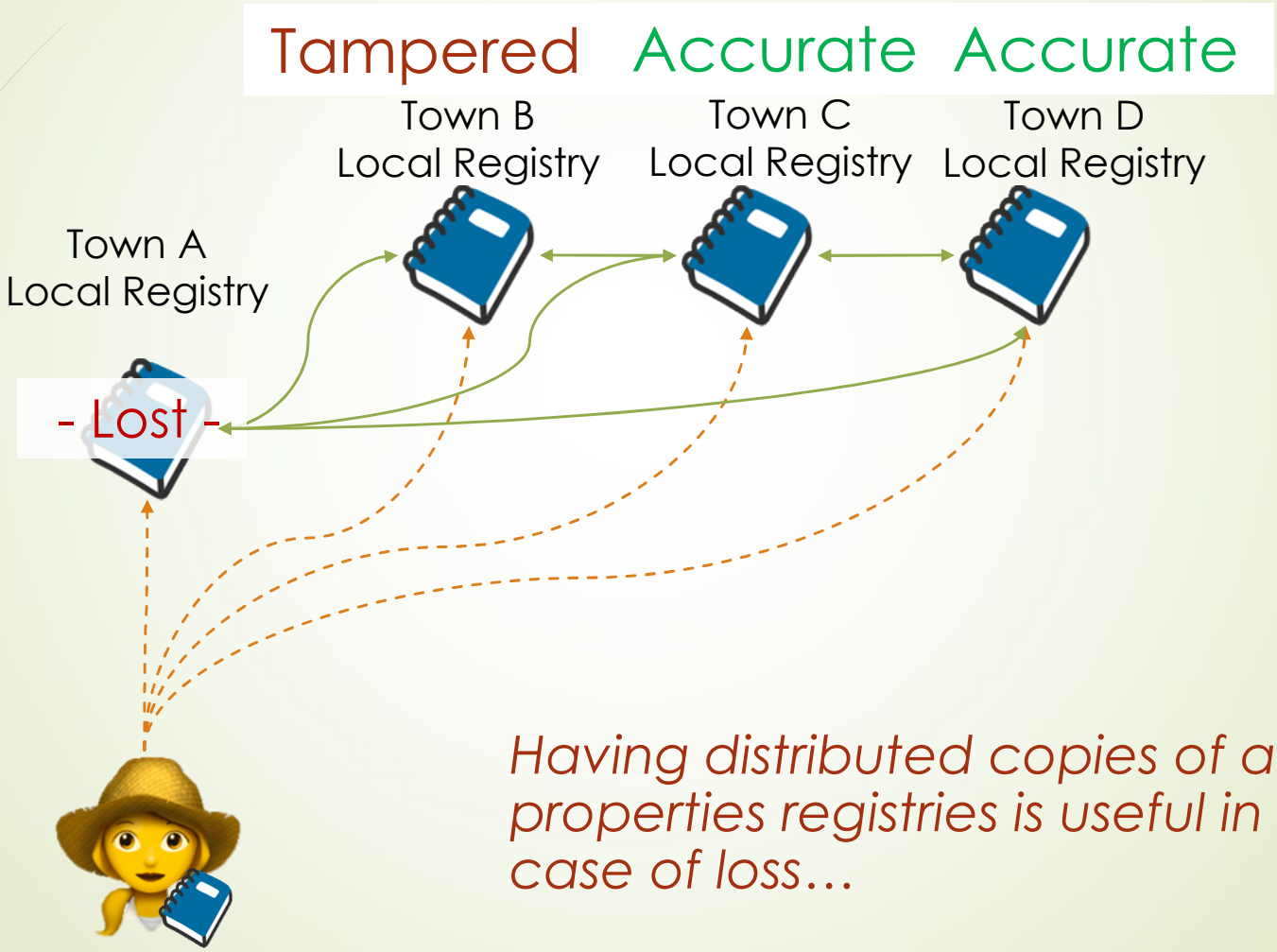
Agenda

- What is Blockchain?
- Traditional Transaction vs Blockchain Transaction
- Where it all started
- Patterns: Distributed Ledger
- 3 types of decentralization
- Explanation of blocks generation with examples
- Cryptocurrencies
- Mining
- Wallets
- Exchanges
- Smart Contracts
- ICOs

Real life scenario…(in Greece)

Imagine you've bought a house and your local property registry office is destroyed by a natural disaster…

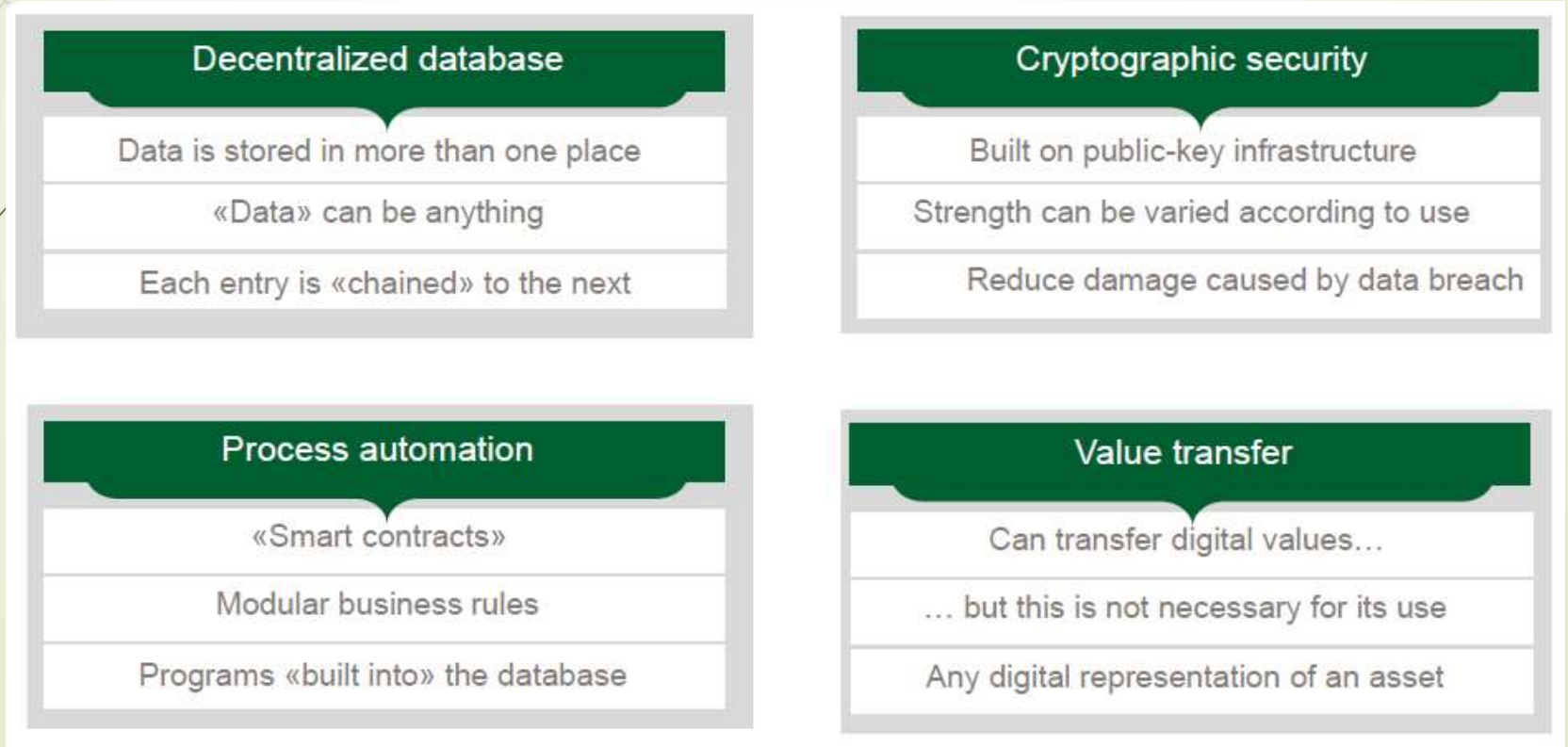
How could we prepare against this risk?



Having distributed copies of all properties registries is useful in case of loss…

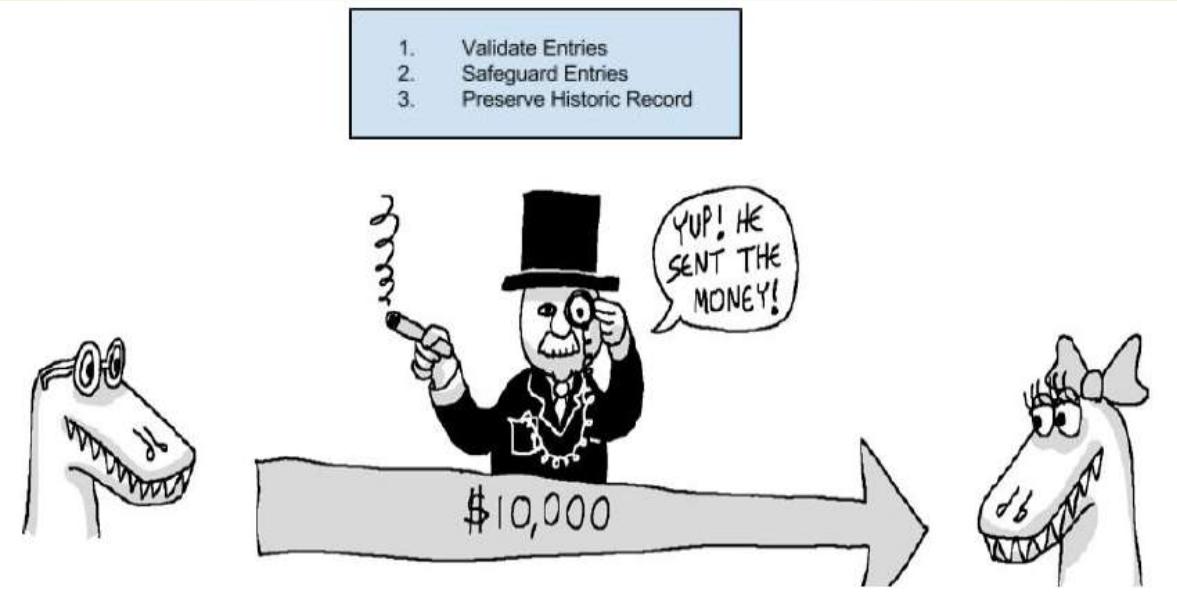
What is Blockchain?

Blockchain platform technology includes a mix of decentralized database, process logic, cryptographic security and transparency… designed for value exchange



Traditional transaction…

Using a 3rd trusted party like Banks, Paypal, etc. → **CENTRALIZED LEDGER**

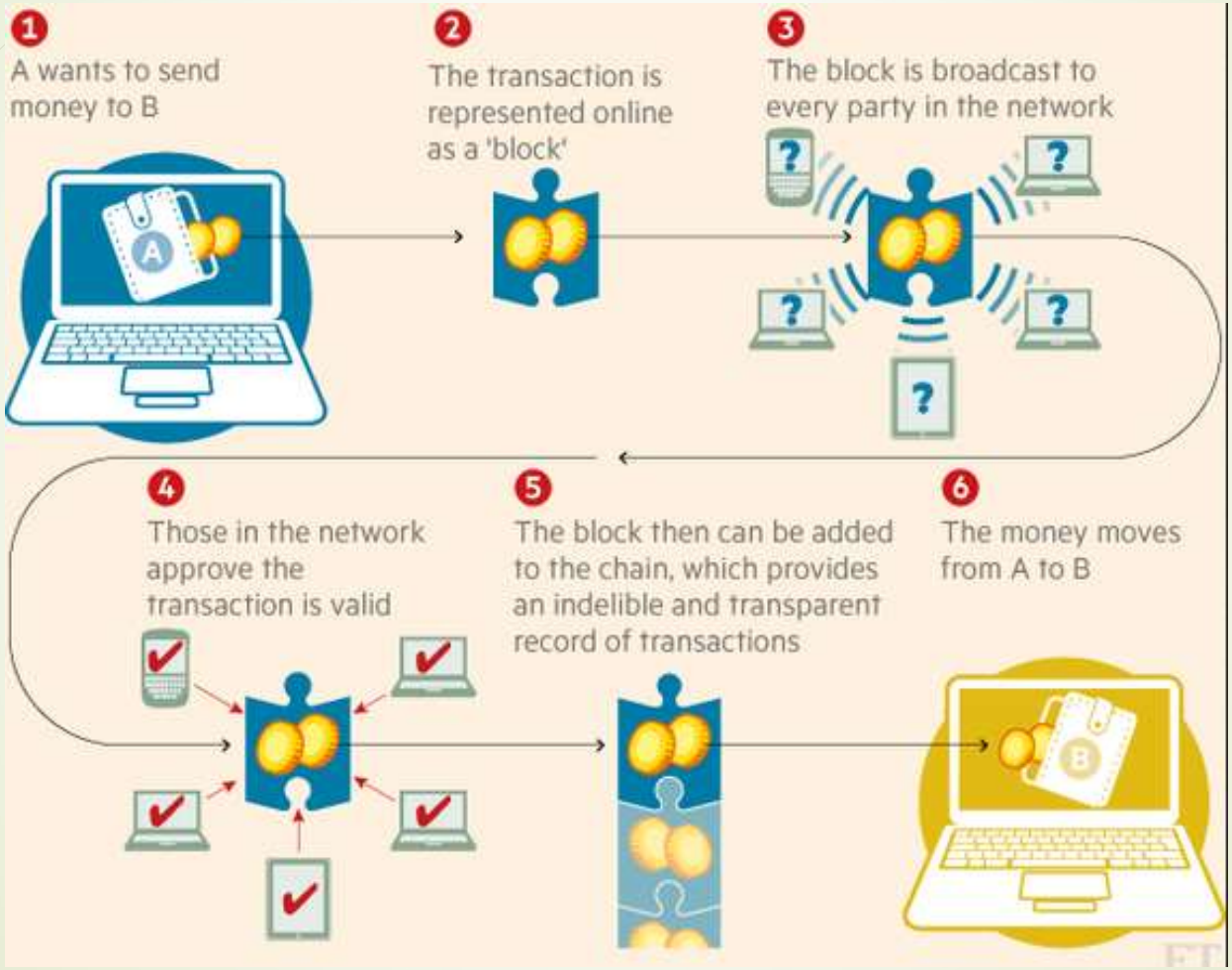


A typical ledger looks something like this:

LEDGER

ACCOUNT TYPE	CASH				
TRANSACTION DATE	TRANSACTION DETAIL	REFERENCE	DEBIT	CREDIT	BALANCE
1/1/16	Expenses for Jan	Ref#1	$100.00		$100.00
2/1/16	Tax withheld	Ref#2		$110.00	($10.00)

How Blockchain works



Where it all started…

Blockchain technology was first introduced in a whitepaper entitled: "Bitcoin: A Peer-to-Peer Electronic Cash System," by Satoshi Nakamoto in 2008.

- No reliance on trust
- Digital signatures
- Peer-to-peer network
- Proof-of-work
- Public history of transactions
- Honest, independent nodes control majority of CPU computing power
- Nodes vote with CPU computing power
- Rules and incentives enforced through consensus mechanism

Patterns: Blockchain is a DISTRIBUTED ledger technology

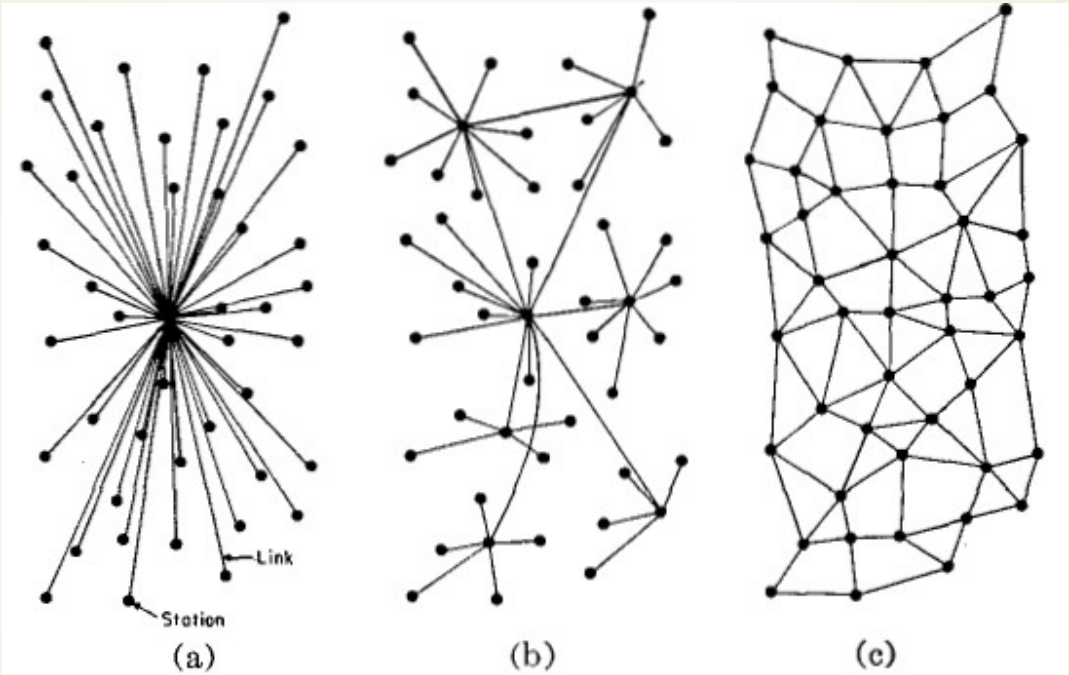


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

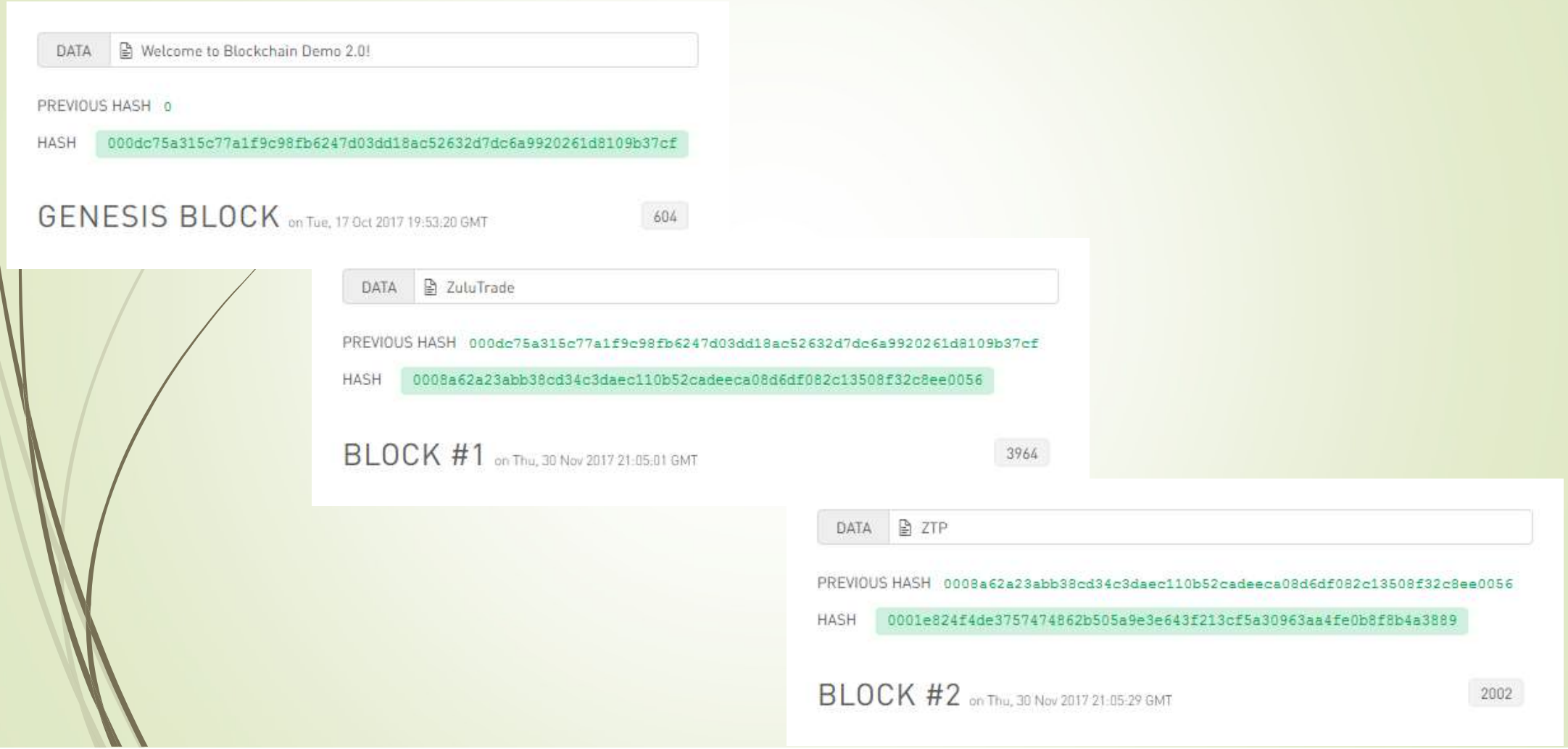
"distributed means not all the processing of the transactions is done in the same place", *whereas* ***"decentralized means that not one single entity has control over all the processing"***

3 types of decentralization

- **Political (de)centralization**—how many **individuals or organizations** ultimately control the computers that the system is made up of?
- **Architectural (de)centralization**—how many **physical computers** is a system made up of? How many of those computers can it tolerate breaking down at any single time?
- **Logical (de)centralization**— does the **interface and data structures** that the system presents and maintains look more like a single monolithic object, or an amorphous swarm? One simple heuristic is: if you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?

*Blockchains are **politically decentralized** (no one controls them) and **architecturally decentralized** (no infrastructural central point of failure) but they are **logically centralized** (there is one commonly agreed state and the system behaves like a single computer)*

https://blockchaindemo.io/



https://blockchaindemo.io/

Index (Block #): Which block is it? (Genesis block has index 0)

Hash: Is the block valid?
A valid hash is a hash that meets a certain requirement. For this blockchain, three leading zeros in front of the hash is the requirement for a valid hash.
The number of leading zeros required is the **difficulty**.

Previous Hash: Is the previous block valid?

Timestamp: When was the block added?

Data: What information is stored on the block?

Nonce: How many iterations did we go through before we found a valid block?

The data held on the block. In Bitcoin for example, the data would be money transactions. Since data is an input variable for the hash, changing the data will change the hash. Changing the hash will generate a new hash without four leading zeros, and the block becomes **invalid**.

How is the hash calculated?

The hash is generated by a cryptographic function called SHA256. The function has the following **input** variables: block index *(0)*, previous hash *(0)*, data *(Welcome to the blockchain!)*, timestamp *(1502208000)*, and nonce *(77177* = Number of iterations it took to find a valid hash).

***f(* index + previous hash + data + timestamp + nonce *)* = hash**

If any of the input variables change, a new and unique hash will be generated.

Replace the values for our genesis block, we get:
f (0 + "0" + 1508270000000 + "Welcome to Blockchain Demo 2.0!" + 604) =
000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

Did you notice the three leading 0's in the block hash?

The three leading 0's is a minimum requirement for a valid hash. The number of leading 0's required is called **difficulty**.

This is also known as the Proof-of-Work system.

```
function isValidHashDifficulty(hash, difficulty) {
  for (var i = 0, b = hash.length; i < b; i ++) {
      if (hash[i] !== '0') {
          break;
      }
  }
  return i >= difficulty;
}
```

isValidHashDifficulty(000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf, 3) ➔ true

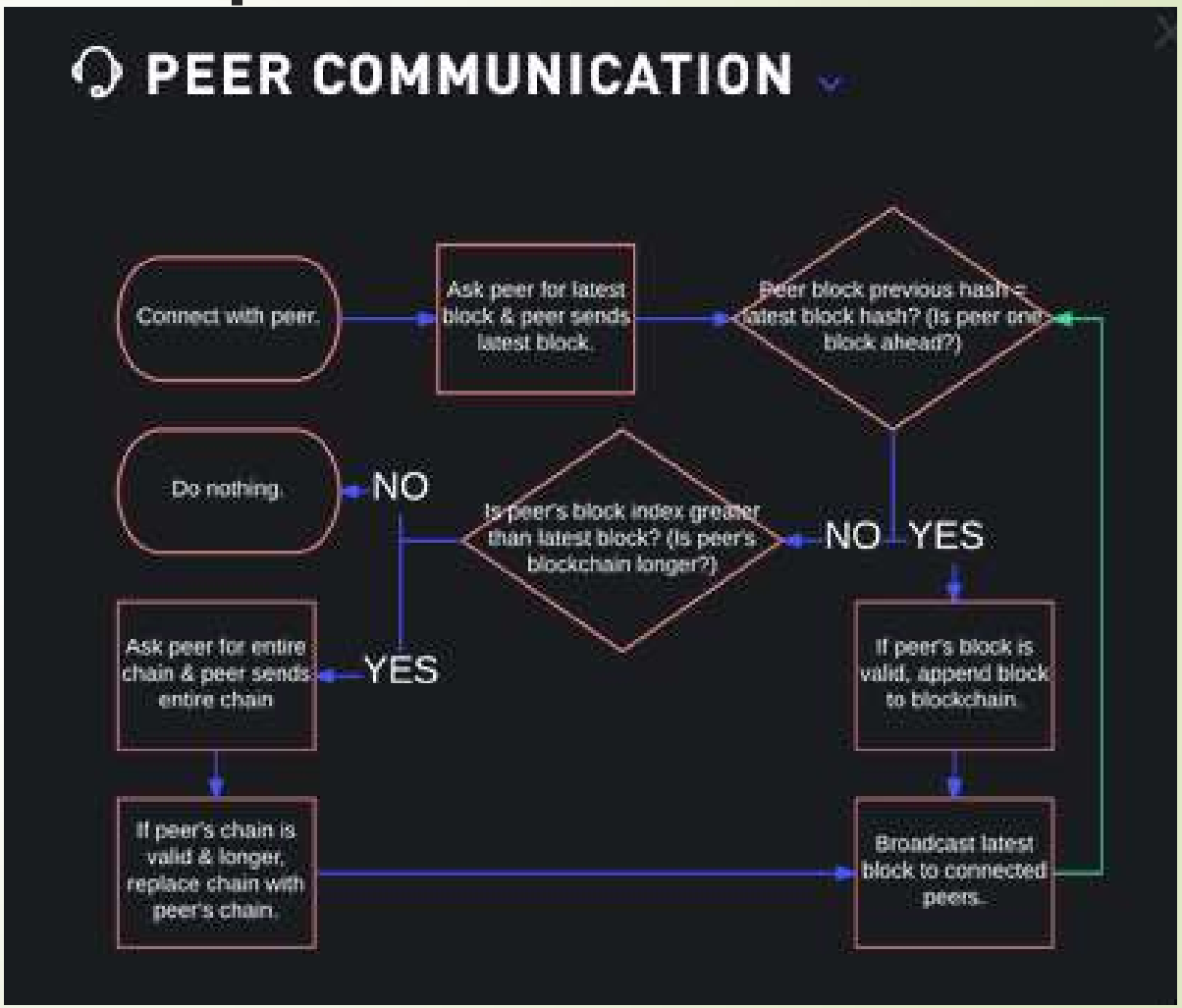
Connecting to other peers… demo

Steps

- ❑ Enter as **Satoshi**
- ❑ Mine a new block BLOCK #1
- ❑ Mine a new block BLOCK #2
- ❑ Create a new peer
- ❑ Make the **new peer** active
- ❑ Connect the new peer to Satoshi

Algorithm

- ❑ **Peer:** asks for latest the block
- ❑ **Peer:** if the previous hash of the latest Satoshi's block **!=** hash of the latest peer's block then…(Satoshi is one block ahead)
- ❑ **Peer:** latest peer's block index **<** latest Satoshi's block index
- ❑ **Peer:** Ask Satoshi for the entire chain
- ❑ **Peer:** If Satoshi's chain is valid & longer, replace peer's chain with Satoshi's one
- ❑ **Peer:** Broadcast latest block to connected peers (they run the algorithm again)



51% Attack

If a participant has more than 51% of the network, he could outmine the network and hack the blockchain.

When there are more miners in the network, the processing power becomes more distributed and no one has majority power. This leads to a more secure blockchain.

Cryptocurrency

- Bitcoin was the first digital, i.e., cryptocurrency
- A maximum of 21 million Bitcoins can be generated
- Just as with real world mining, energy must be invested to solve complex mathematical problems by which systems earn Bitcoins
- https://www.cryptocoincharts.info/coins/info claims to be indexing 4,220 cryptocurrencies
- Most circulated: Bitcoin, Ethereum, Litecoin

The Technology Behind Bitcoin

- Think of Bitcoin as an **electronic asset** (as well as a digital currency)
- **A network of computers** keeps track of Bitcoin payments, and adds them to an ever-growing list of all the Bitcoin payments that have been made, called **"The Bitcoin Blockchain".**
- **The file** that contains data about all the Bitcoin transactions is often called a **"ledger".**
- Bitcoin value is created through transaction processing, referred to as "mining" which is performed by distributed processors called "nodes" of the peer-to-peer network.

Mining Evolution

- Mining is the process whereby value is created through transaction processing that occurs on the nodes of the network.
- In 2009, one could mine 200 Bitcoins with a personal, home computer. In 2015, it would take about 98 years to mine just 1 Bitcoin.
- Today there is almost no money to be made through traditional home mining.
- ASIC (Application Specific Integrated Circuit) has been designed strictly for mining Bitcoins.
- Groups of miners have formed mining pools, with each being paid their relative share for their contribution to the work performed.

Mining Pools

Mining pools:
validate transactions + mine coins

Wallets

Cryptocurrency wallets:

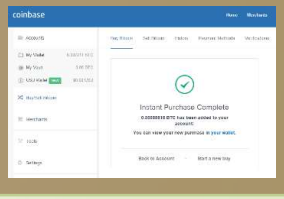
Store securely public and private keys of your blockchain assets

Hold multiple addresses + private keys
May hold BTC, ETH, ERC20 tokens, etc.

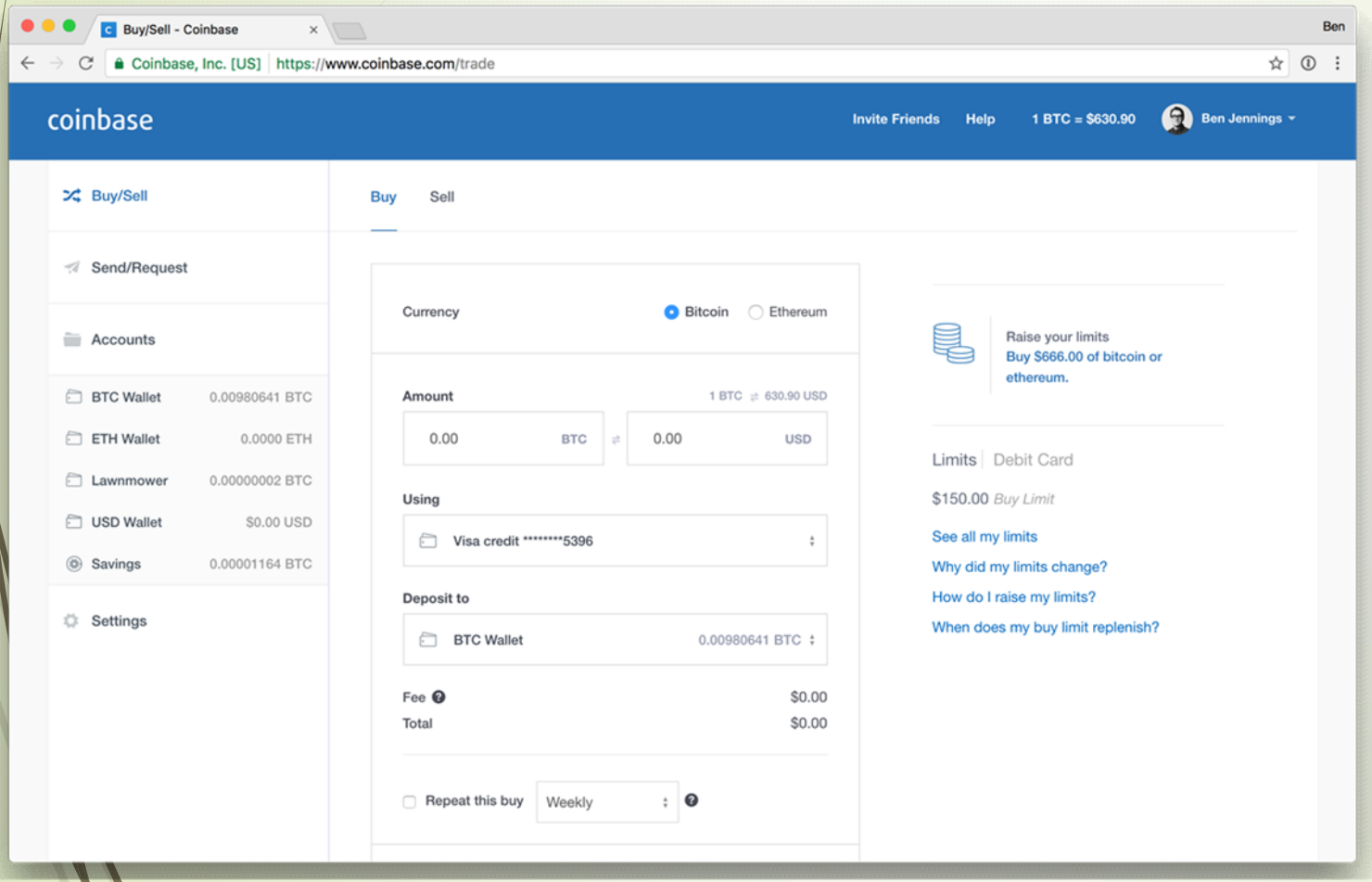
Software wallets

Hardware wallets

Online wallets



Cryptocurrency Exchanges



BITFINEX

bithumb

coinone

POLONIEX
CRYPTOCURRENCY EXCHANGE

BITTREX
NEXT GENERATION CRYPTO EXCHANGE

kraken

GDA

SHAPE SHIFT

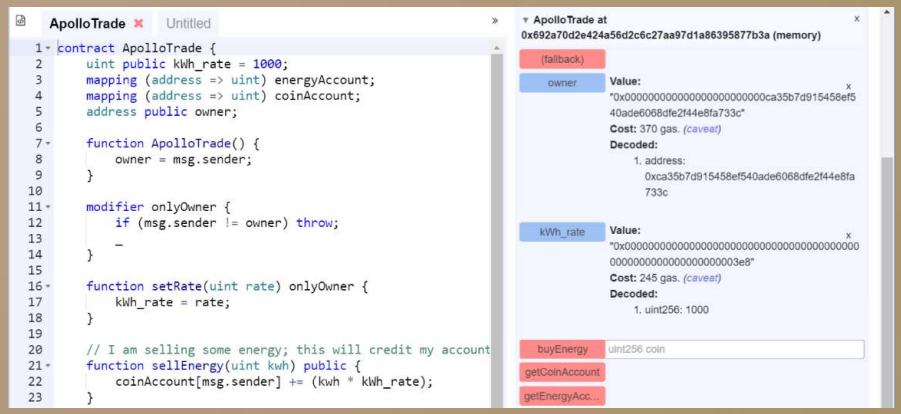
Smart Contracts

Smart Contracts

Code (custom logic) running in the blockchain network

Solidity

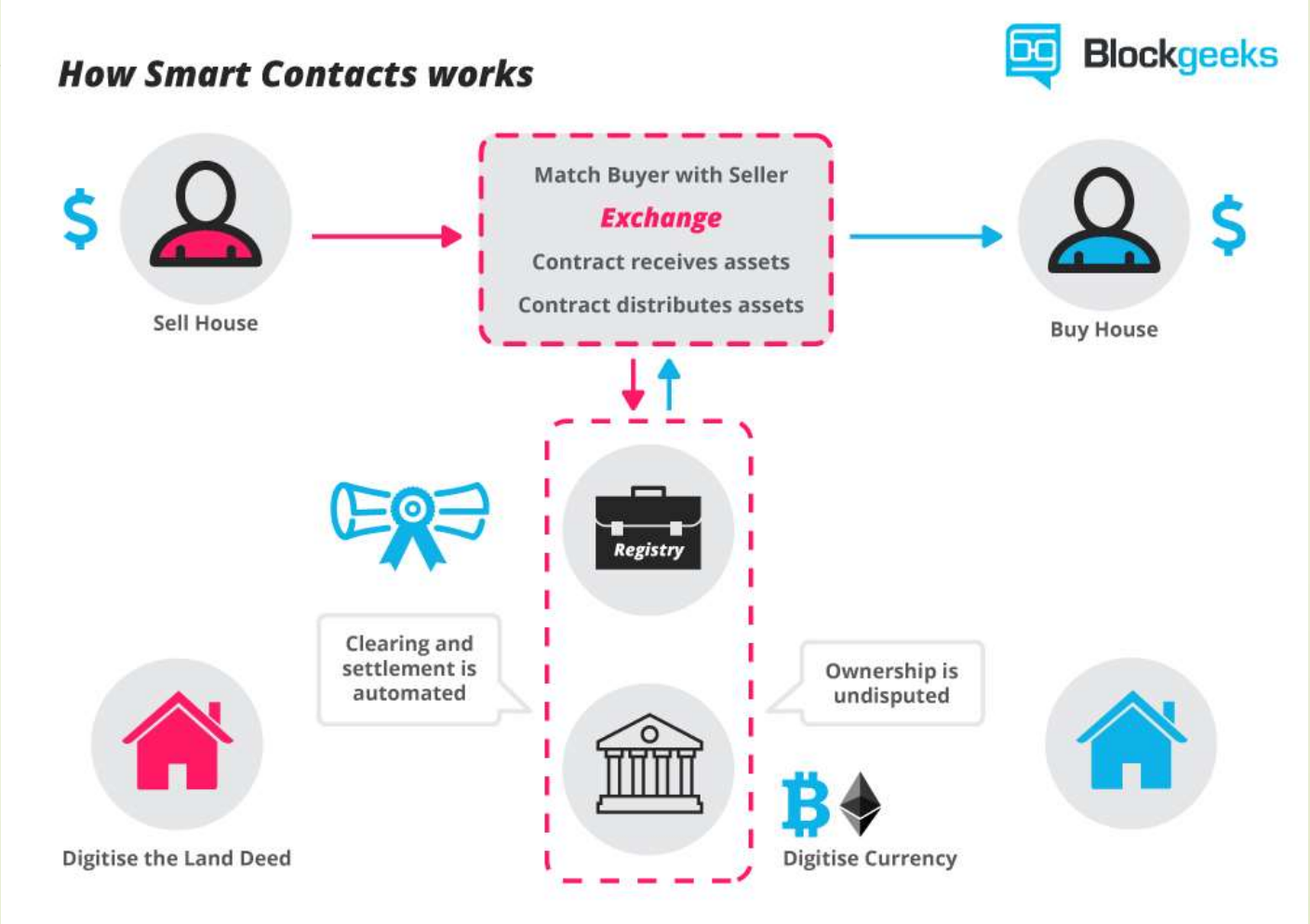
Blockchain programming language for the Ethereum network, running on EVM



```
ApolloTrade  Untitled
1  contract ApolloTrade {
2      uint public kWh_rate = 1000;
3      mapping (address => uint) energyAccount;
4      mapping (address => uint) coinAccount;
5      address public owner;
6
7      function ApolloTrade() {
8          owner = msg.sender;
9      }
10
11     modifier onlyOwner {
12         if (msg.sender != owner) throw;
13         _
14     }
15
16     function setRate(uint rate) onlyOwner {
17         kWh_rate = rate;
18     }
19
20     // I am selling some energy; this will credit my account
21     function sellEnergy(uint kwh) public {
22         coinAccount[msg.sender] += (kwh * kWh_rate);
23     }
```

```
ApolloTrade at
0x692a70d2e424a56d2c6c27aa97d1a86395877b3a (memory)
(fallback)
owner
Value:
"0x0000000000000000000000ca35b7d915458ef5
40ade6068dfe2f44e8fa733c"
Cost: 370 gas. (caveat)
Decoded:
1. address:
0xca35b7d915458ef540ade6068dfe2f44e8fa
733c
kWh_rate
Value:
"0x0000000000000000000000000000000000000
0000000000000000000003e8"
Cost: 245 gas. (caveat)
Decoded:
1. uint256: 1000
buyEnergy
uint256 coin
getCoinAccount
getEnergyAcc...
```

How Smart Contracts Work?



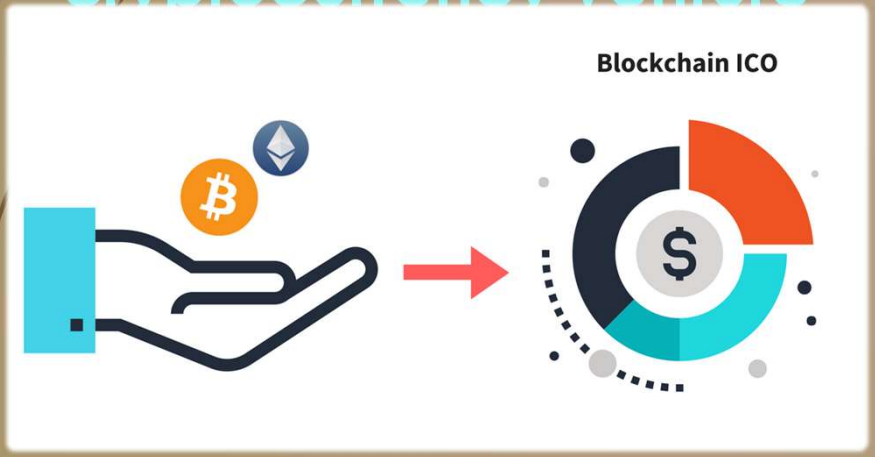
Smart Contracts vs Legal Contracts

Legal contracts	Smart contracts
Good at subjective (ie. requiring human judgement) claims	Good at objective (ie. mathematically evaluable) claims
High cost	Low cost
May require long legal process	Fast and automated
Relies on penalties	Relies on collateral/security deposits
Jurisdiction-bound	Potentially international (“a-legal”)

ICO / Token Sale Events

ICO (Initial Coin Offering)

Funds raised for a new cryptocurrency venture



Token Sale Events

Digital tokens raised through a smart contract

Corporate Blockchains

Hyperledger

https://www.hyperledger.org/members

Azure Blockchain

https://azure.microsoft.com/solutions/blockchain

Why Corporate Blockchain?

Public immutable ledger: trust between businesses + b2b smart contracts

Why are people so excited about blockchain?

Figure 3. The three characteristics to remember

Decentralized and distributed

Ledger storage and integrity

- Ledger replicated across parties, each keeping a full record of transactions
- Distributed system operation, no single point of failure
- Transactions verified cryptographically and updated immediately across all parties
- Provides unbroken and timely recordation of authoritative truth

Irreversible and immutable

Each transaction record is indelible

- The ledger is append-only, invalid transaction errors are surfaced and rejected—immediate reconciliation
- All transactions encrypted and include time, date, participants, and hash to previous block
- Trust is enabled via consensus protocols, cryptography, and collective bookkeeping
- Allows trusted value exchange

Near real time

Transactions verified and settled in minutes vs. days

- Parties interact directly—no third-party intermediary
- Moves parties from information exchange to value exchange
- A transaction may include code to run against the ledger
- Enables smart contract automation and enforcement

Source: Deloitte analysis.

References

- https://github.com/crytography/blockchain-demo
- http://blockchaindemo.io/
- https://bitcoin.org/bitcoin.pdf
- A Gentle Introduction to Bitcoin by Antony Lewis, https://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Bitcoin-WEB.pdf
- My Dirty Little Bitcoin Secrets by Ofir Beigel, www.99bitcoins.com
- https://www.amazon.com/Mastering-Bitcoin-Unlocking-Digital-Cryptocurrencies/dp/1449374042
- https://www.youtube.com/watch?v=T2zH-T_hmLs
- https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
- https://en.bitcoin.it/wiki/Difficulty
- http://icorating.com/
- https://www.youtube.com/watch?v=w9WLo33KfCY


THANK
YOU