Overview of Blockchain, Cryptocurrency, and Smart Contract

Instructor: Paruj Ratanaworabhan

Sources

- bitcoinbook.cs.princeton.edu
- bitcoin.org
- npr.org
- “The Economics of Digital Currencies”: Bank of England Quarterly Bulletin 2014 Q3
- blockchain.berkeley.edu
- D. Finlay (ConsenSys)

Agenda

- Evolution of database technology
- Bitcoin and blockchain
- Ethereum and smart contracts
- Conclusion

Once upon a time

Data on Papers

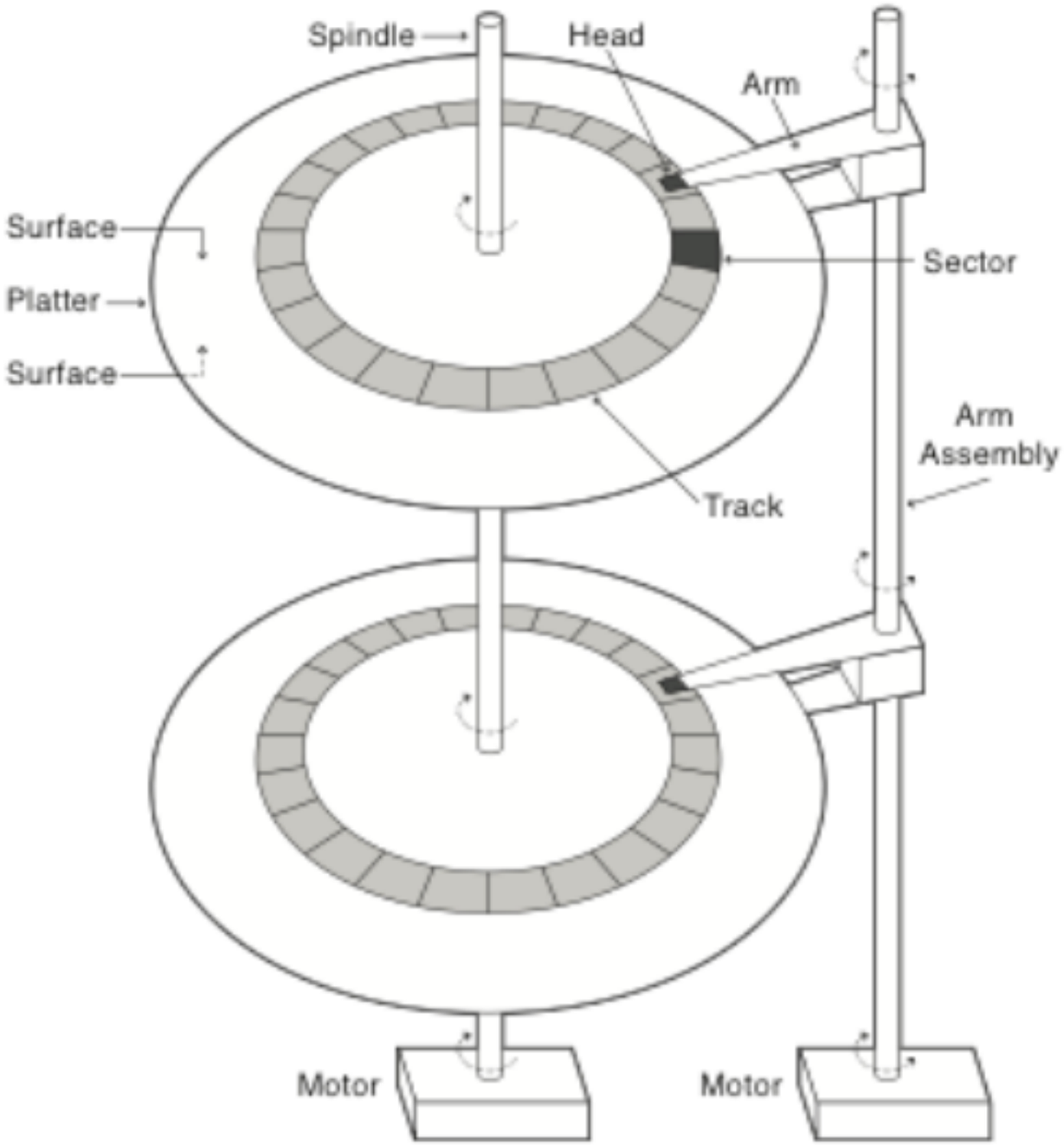
Advantages of Papers

- Handy and readable anywhere anytime
- (Somewhat) durable and have fixed formats
  - No “rotten bit” problems

Paper Storage and Processing

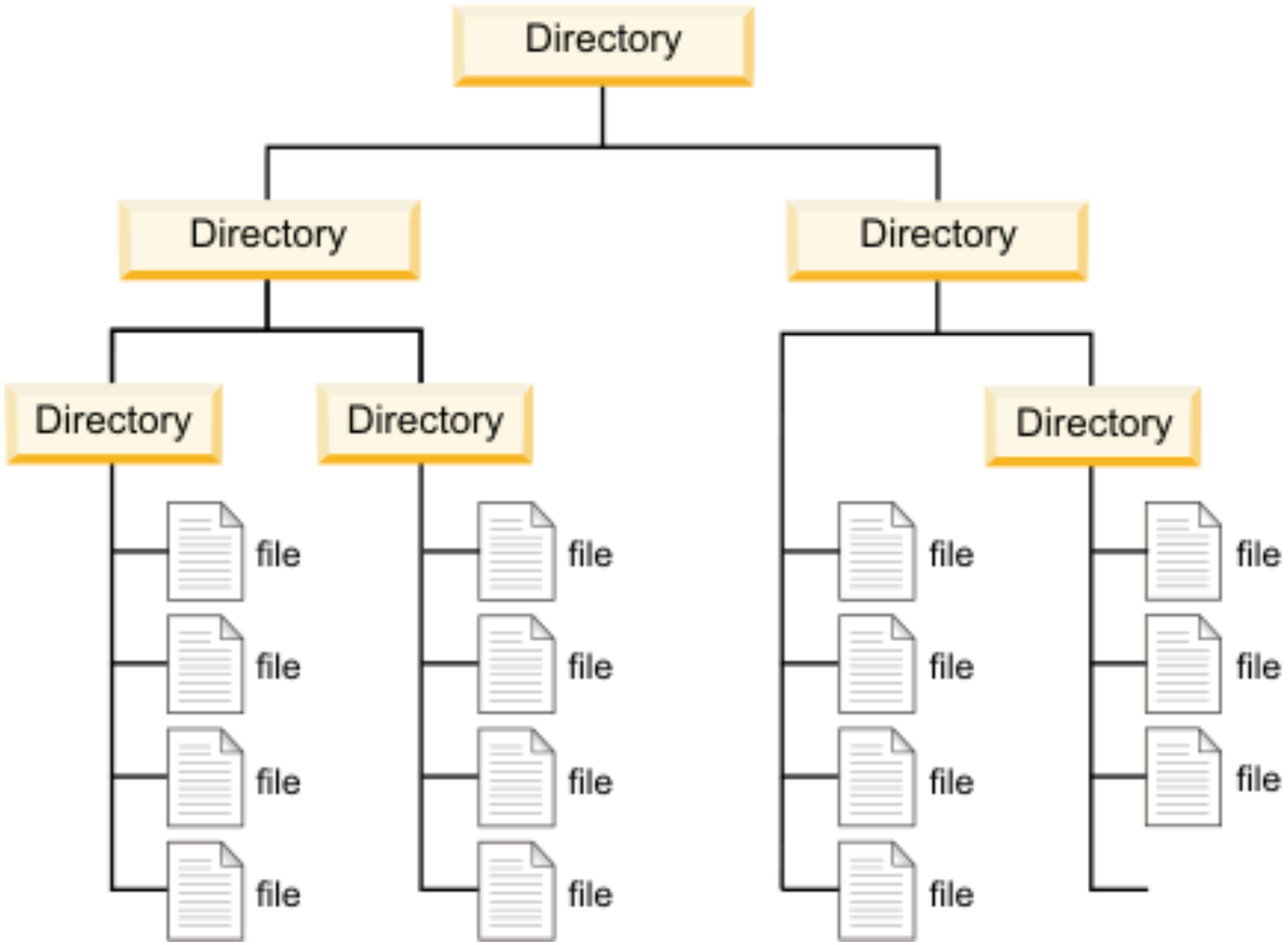
In the modern day, electronics media have largely supplanted papers primarily for efficiency of data storage and processing

Hard Drives



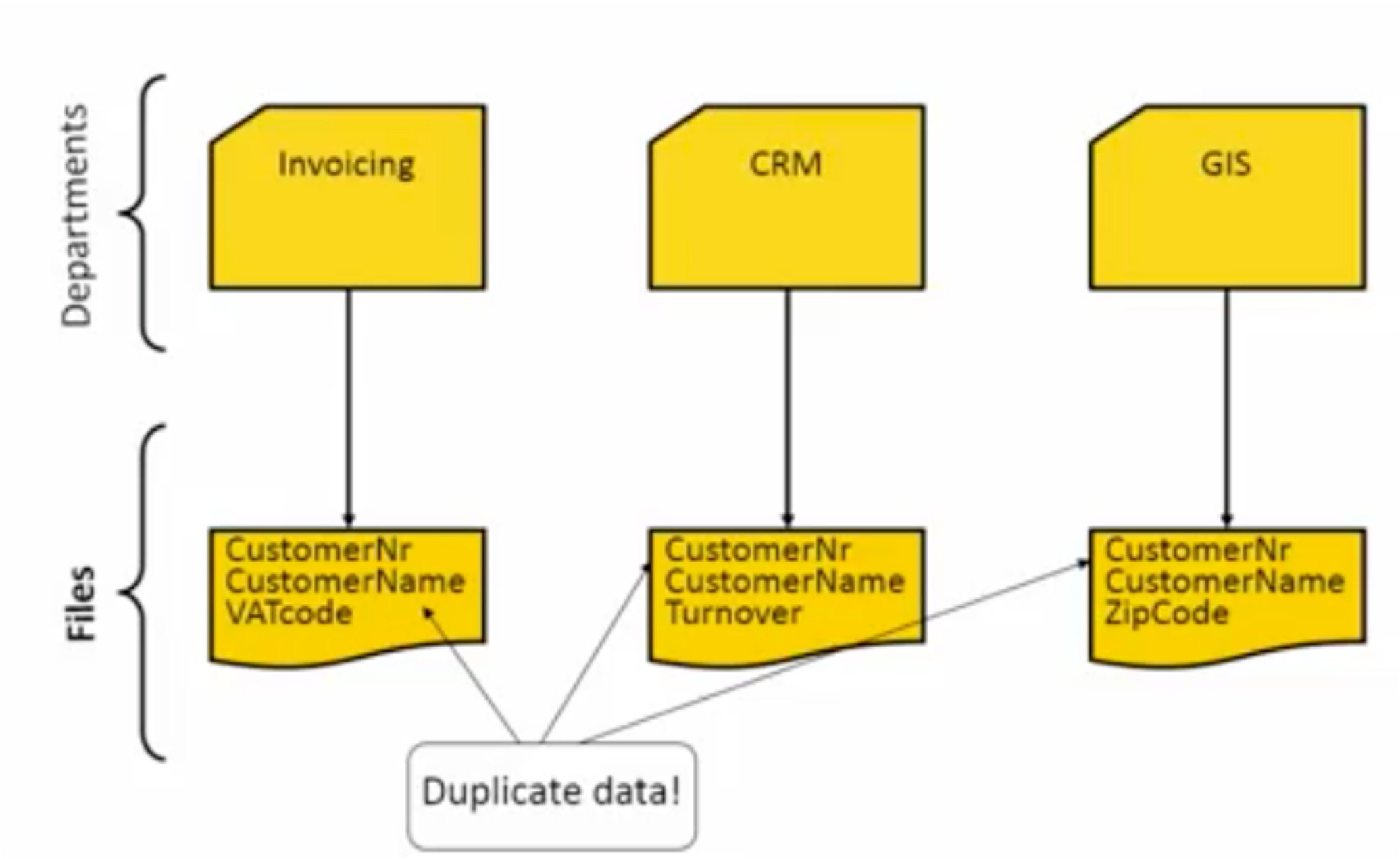
Popular permanent storage media, but difficult to work with for average users

Files and Directories



Easier to work with but still have problems

Data Duplication in File Systems



Customized File Processing Program

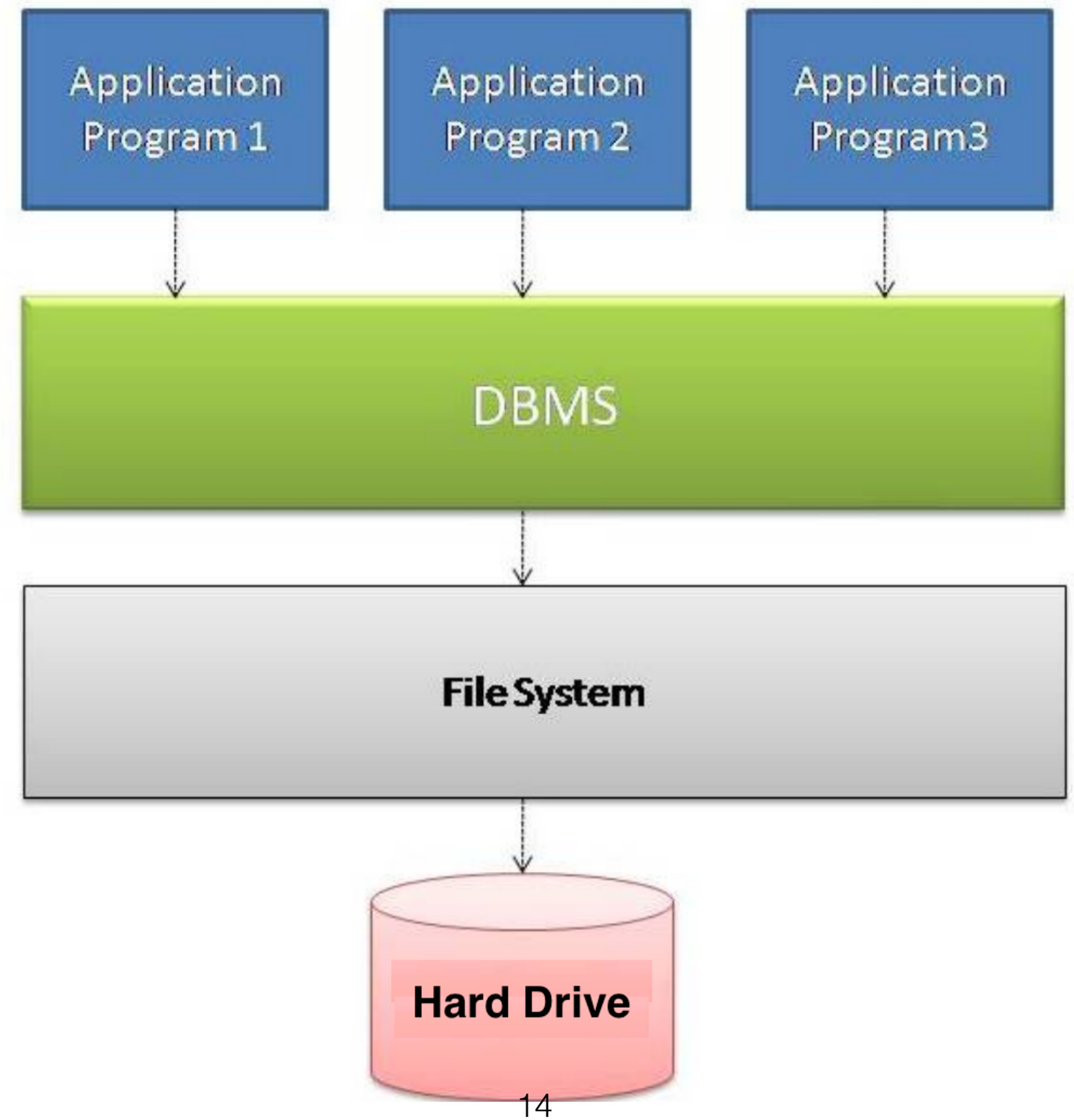
File-based (pseudo-code)

```
find person (name:input, record:output)
begin
open people
repeat while people has next
    people → go to next record
    record := people → current record
    if record → person is name
        done
    else
        continue
    end
end
record := invalid
end
```

What We Want

```
SELECT *
FROM people
WHERE name = $NAME
```

Data Processing from Application to Hard Drive

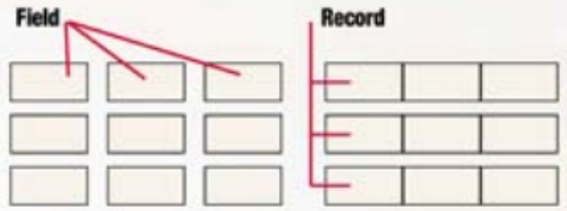


Relational Data Model for DBMS

"Activities of users at terminals and most application programs should remain unaffected when the internal representation of data is changed and even when some aspects of the external representation are changed."

Key Ideas: Programs that manipulate tabular data exhibit an algebraic structure allowing reasoning and manipulation independently of physical data representation

How Relational Databases Work



Computerized databases help people store and track huge amounts of information. The smallest unit of information in a database is called a **field**. Fields are grouped together to form **records**. Records are then grouped together to form **tables**.

Flat-file databases take all the information from all the records and store everything in one table. This works fine when you have a small number of records related to a single topic, such as a person's name and phone number, but if you have hundreds or thousands of records, each with a number of fields, the database quickly becomes difficult to use.

SID	SFName	SLName	SteleNumber	CID	Cname	TID	Trainer	TrnTeleNumber
1	Mary	Hinkle	555.123.4567	101	Data Basics	T01	Charles Hill	555.987.6543
2	Paul	Litz	555.258.8963	101	Data Basics	T01	Charles Hill	555.987.6542
1	Mary	Hinkle	555.123.4567	102	Web Design	T02	Glen Barber	555.879.4652
3	Dee	Coleman	555.357.9514	203	Relational Design	T03	Rick Dobson	555.324.2986
4	Don	Charney	555.369.8741	204	VBA Programming	T03	Rick Dobson	555.324.2986

Relational databases separate this mass of information into numerous **tables**. All the columns in each table should be about one topic, such as "student information," "class information," or "trainer information."

SID	SFName	SLName	SteleNumber
1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963
1	Mary	Hinkle	555.123.4567
3	Dee	Coleman	555.357.9514
4	Don	Charney	555.369.8741

CID	Cname
101	Data Basics
101	Data Basics
102	Web Design
203	Relational Design
204	VBA Programming

TID	Trainer	TrnTeleNumber
T01	Charles Hill	555.987.6543
T01	Charles Hill	555.987.6542
T02	Glen Barber	555.879.4652
T03	Rick Dobson	555.324.2986
T03	Rick Dobson	555.324.2986

The tables for a relational database are linked to each other through the use of **keys**. Each table may have one **primary key** and any number of **foreign keys**. A foreign key is simply a primary key from one table that has been placed in another table.

Primary Key

SID	SFName	SLName	SteleNumber
1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963
1	Mary	Hinkle	555.123.4567
3	Dee	Coleman	555.357.9514
4	Don	Charney	555.369.8741

Primary Key

SID	CID	Cname	TID
1	101	Data Basics	T01
2	101	Data Basics	T01
1	102	Web Design	T02
3	203	Relational Design	T03
4	204	VBA Programming	T03

Primary Key

TID	Trainer	TrnTeleNumber
T01	Charles Hill	555.987.6543
T01	Charles Hill	555.987.6542
T02	Glen Barber	555.879.4652
T03	Rick Dobson	555.324.2986
T03	Rick Dobson	555.324.2986

Foreign Key — Foreign Key

The most important rules for designing relational databases are called **Normal Forms**. When databases are designed properly, huge amounts of information can be kept under control. This lets you **query** the database (search for information) and quickly get the answer you need.

Query: "What students are taking classes from trainer CHARLES HILL?"

Answer:

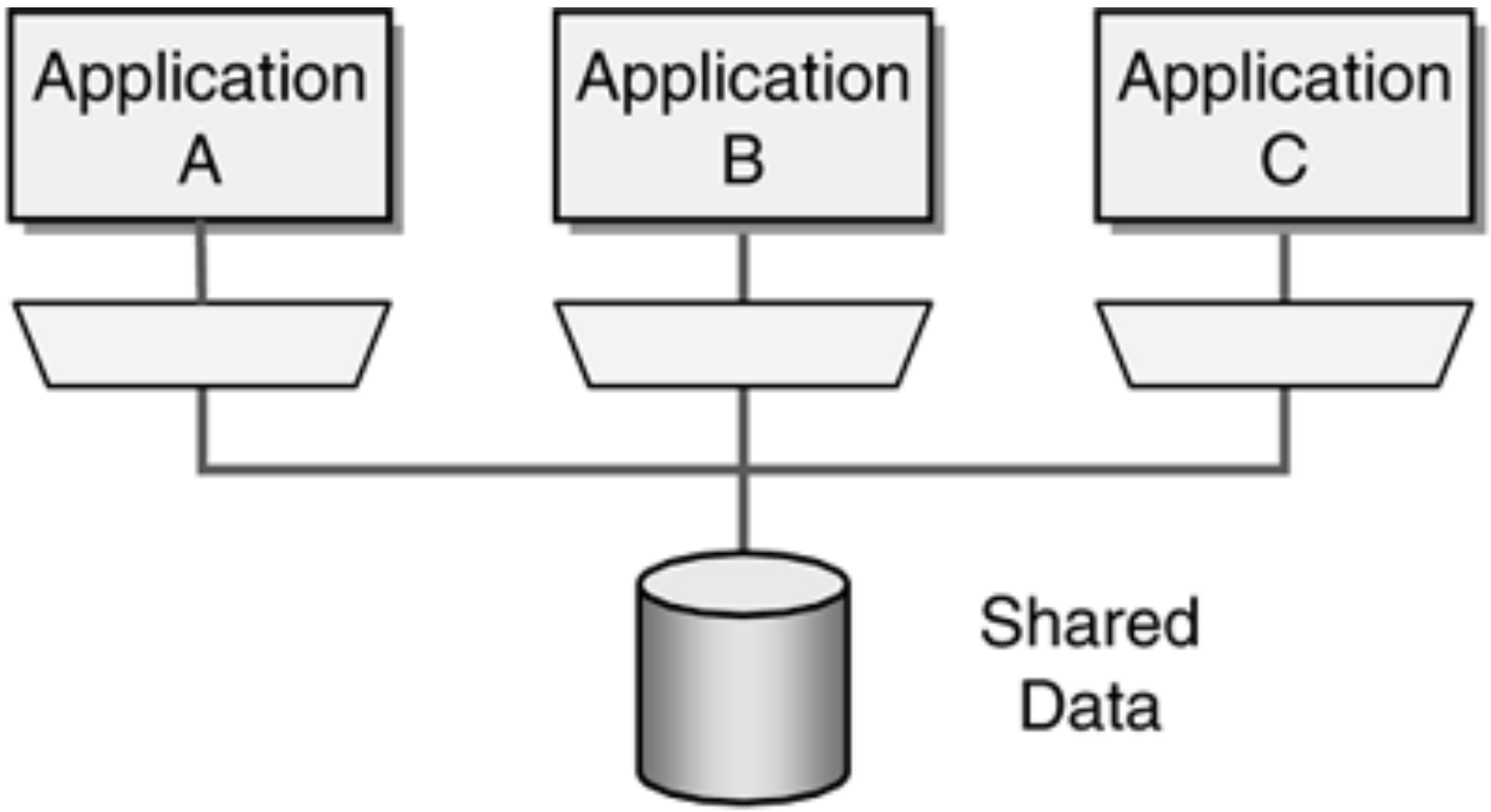
1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963

Compiled by Rick Dobson
Graphics & Design by Fred Schneider

Relational Database Advantages

- ACID transactions
- SQL
- Indexing ability
- Flexible modeling
- Integration database

Integration Database



Relational DBMS had conquered the world for almost 30 years since its inception and suddenly …

The Arrival of New Types of Applications

1970-2000: Mainly RDBMS solutions

SQL Server, MySQL, ORACLE, IBM DB2

2000-2005: DotCom bubble, new scale, NoSQL beginnings, whitepapers

amazon Try Prime, facebook, Google, IBM

2005-2010: Open Source & Mainstream

Cassandra, HBase, mongoDB, CouchDB, riak, redis

2010+: Adoption of cloud → DBaaS

IBM Cloudant, amazon DynamoDB

From SQL* to NoSQL

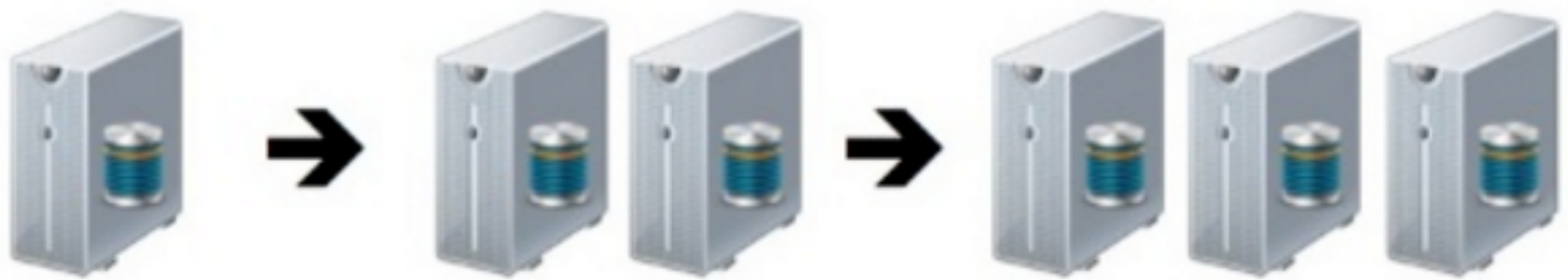
- The need to handle big data and big number of users
- Scale out by distributing the data across multiple Commercial Off-The-Shelf (COTS) servers
- Moving from centralized to distributed databases
- Moving from structured to unstructured (schema-less) data
- Requiring the system to be fault-tolerant

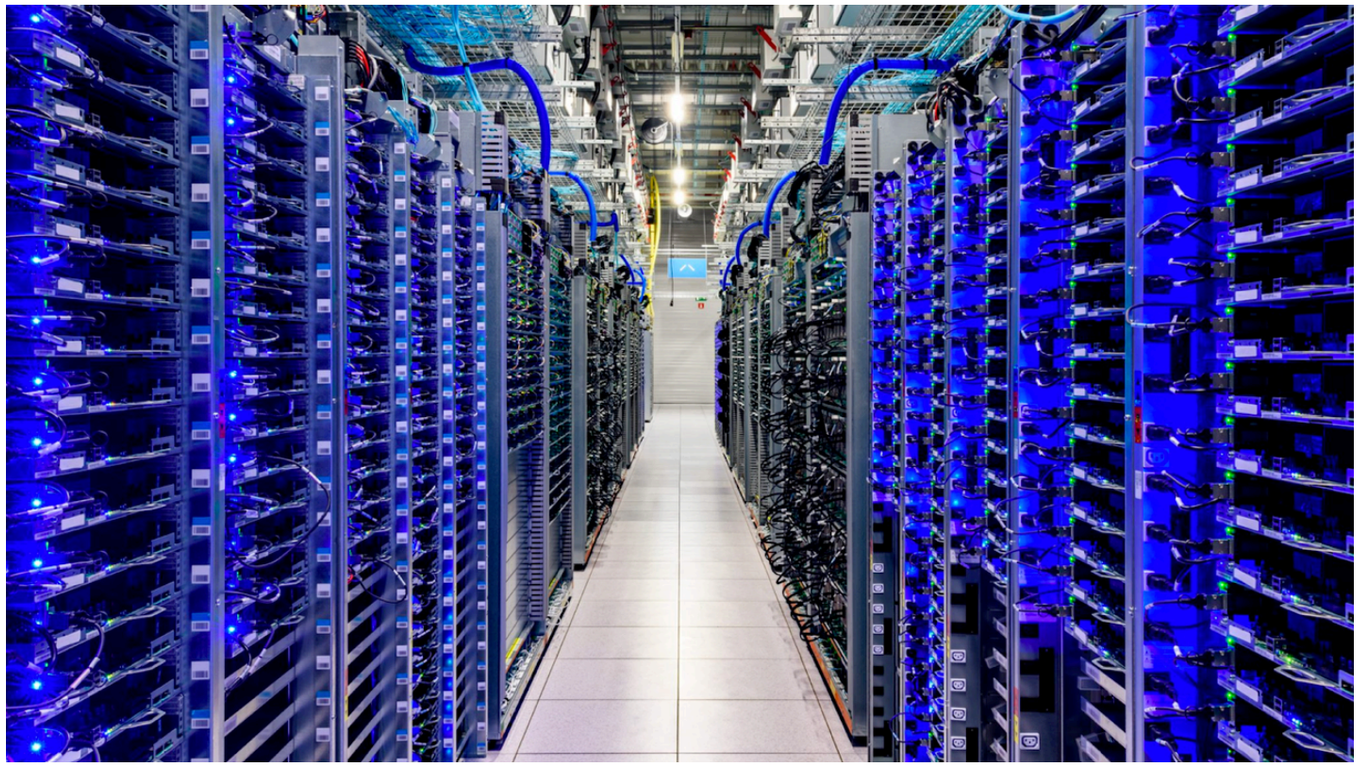
** Here SQL is synonymous with RDBMS*

Scale-Up VS Scale-Out

Scale-Up

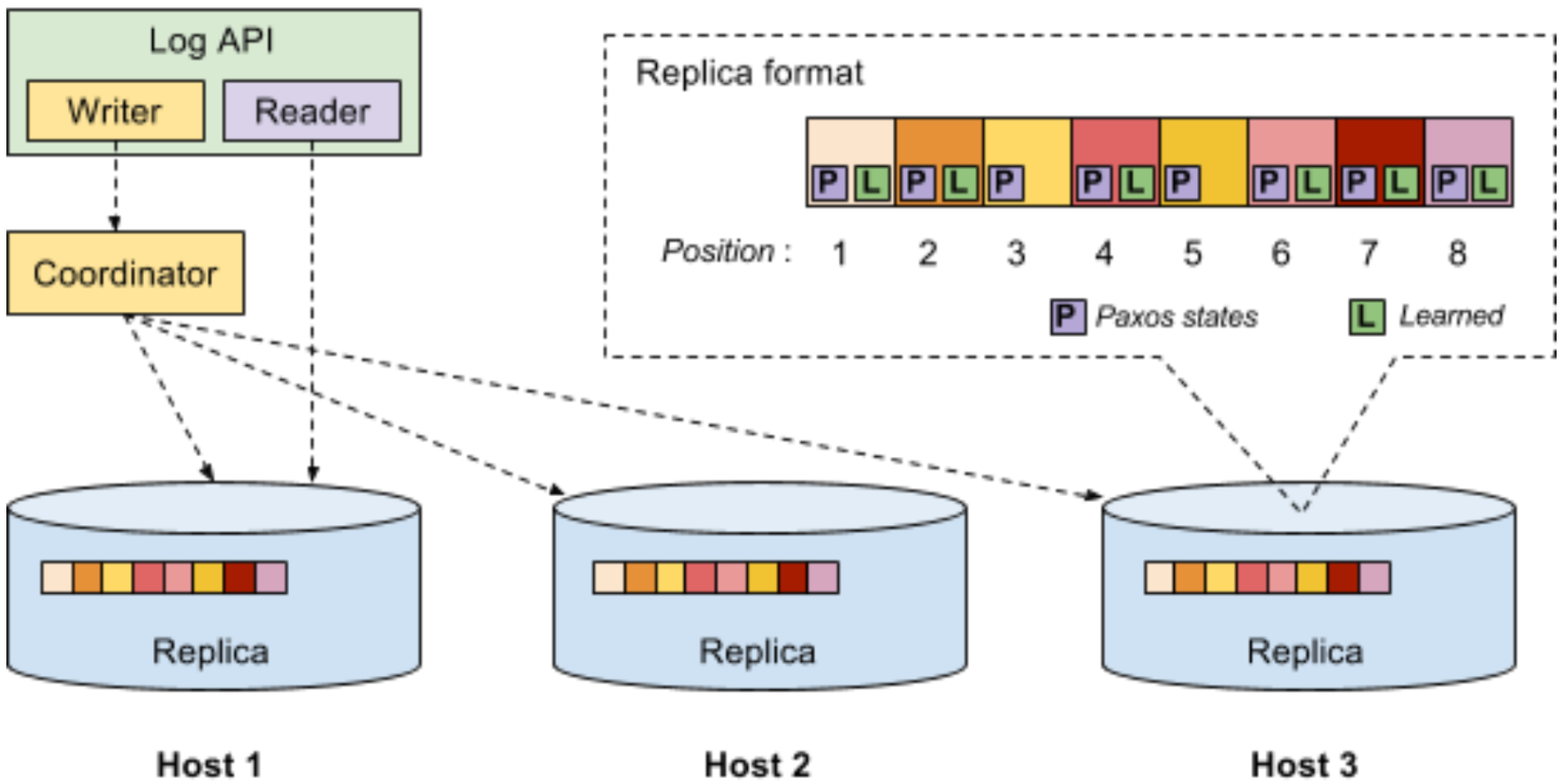
Scale-Out





Google's Scaling Out

Challenges to Scaling Out



- Must ensure data **consistency** upon updates
- Must execute a **consensus** protocol to obtain such consistency
- Need to have a **co-ordinator** to lead the consensus protocol
- **Consensus is a hard problem** to solve correctly and efficiently
  - Primarily because of the need to accommodate fault-tolerance
- If the co-ordinator can be trusted, there are classical algorithms to handle this problem

During the year 2000 - 2010, we had solved the scaling out problems somewhat effectively and companies like Google and Facebook are now running distributed database processing big data serving millions of users

Classifying Database Technology

Centralized (SQL)

Classifying Database Technology

Distributed (NoSQL)

Classifying Database Technology

Centralized Control

Centralized (SQL)

Distributed (NoSQL)

Classifying Database Technology

Centralized Control

Centralized (SQL)

Distributed (NoSQL)

Decentralized Control

?

Agenda

- Evolution of database technology
- Bitcoin and blockchain
- Ethereum and smart contracts
- Conclusion


cypherpunk

In the late 1980s, a group called Cypherpunk is formed by people who believe in freedom of expression and distaste government surveillance.

Members of the Cypherpunk envisage a society where individuals never have to reveal their identities, always communicate on private channels, and never rely on trusted authorities.

Some members of the group had gone on to become creators of important privacy and security technologies.

Prominent Members of the Cypherpunk

- Jacob Appelbaum: lead developer of the Tor browser
- Julian Assange: creator of WikiLeaks
- Nick Szabo: proposer of the idea of smart contracts
- Philip Zimmermann: inventor of PGP
- Moxie Marlinspike: co-founder of the Signal foundation

How Can a Cypherpunk Society Be Sustained

- Need some type of monetary system that adheres to the group's values
  - Must be on-line
  - Must be decentralized, no trusted authorities
  - Must preserve privacy

In the year 2009, a member of the Cypherpunk who went by the pseudo-name Satoshi Nakamoto proposed a solution to solve the wanted monetary system

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.


BITCOIN
DIGITAL DECENTRALIZED PEER TO PEER

Despite its name, Bitcoin is not a coin per se but a giant (and slow) accounting system

Ledger

	account number	balance
Carol	1G8bneji6etY...	12.5
	1K7A6wsyxj6...	323
	16pJcrGi51nr...	1
Bob	1MVbjHicuJr...	15.2
	1G4HyHp1oa...	100
	17UP3moev2...	.00000001
	1Eeq4FM2Ts...	45
	...	...

Bob

Carol

Ledger

	account number	balance	
Carol	1G8bneji6etY...	12.5	
	1K7A6wsyxj6...	323	
Carol	16pJcrGi51nr...	6.0	+5.0
Bob	1MVbjHicuJr...	10.2	-5.0
	1G4HyHp1oa...	100	
	17UP3moev2...	.00000001	
	1Eeq4FM2Ts...	45	
	...	...	

Bob

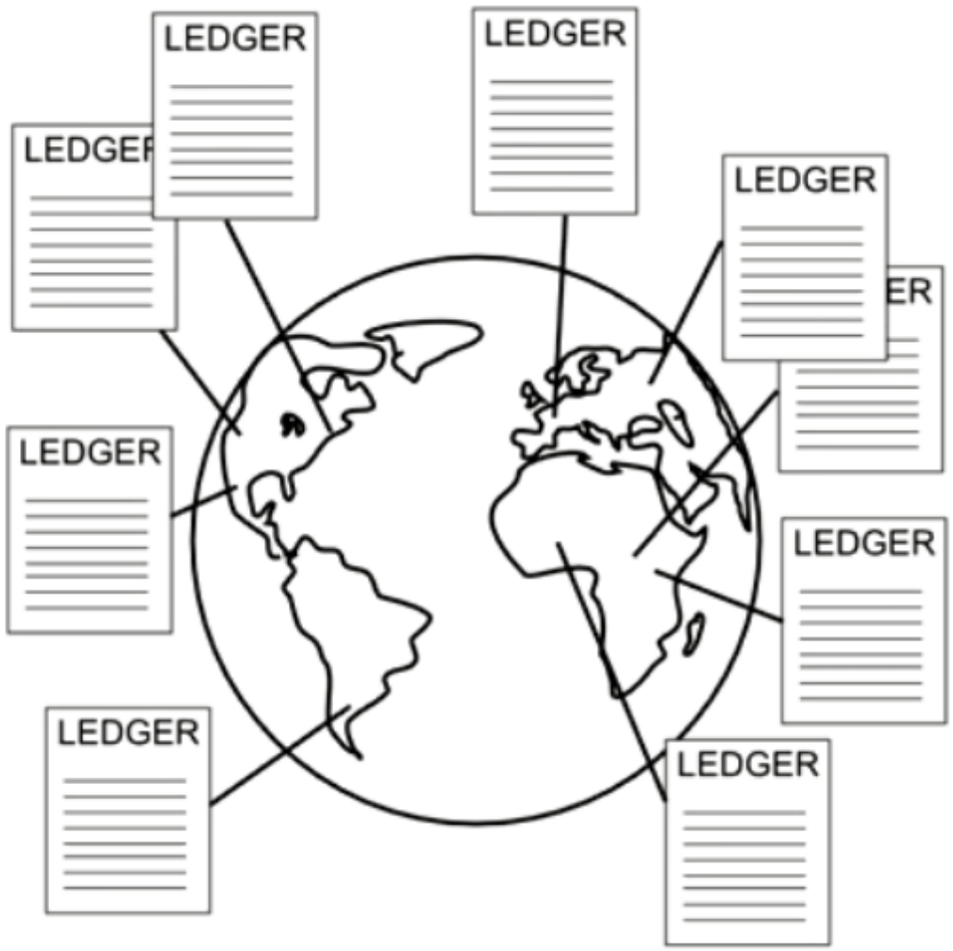
Carol

Unlike conventional banking systems, Bitcoin ledger is not centrally controlled.

Bitcoin ledger lives in a distributed database that no single authority controls it.

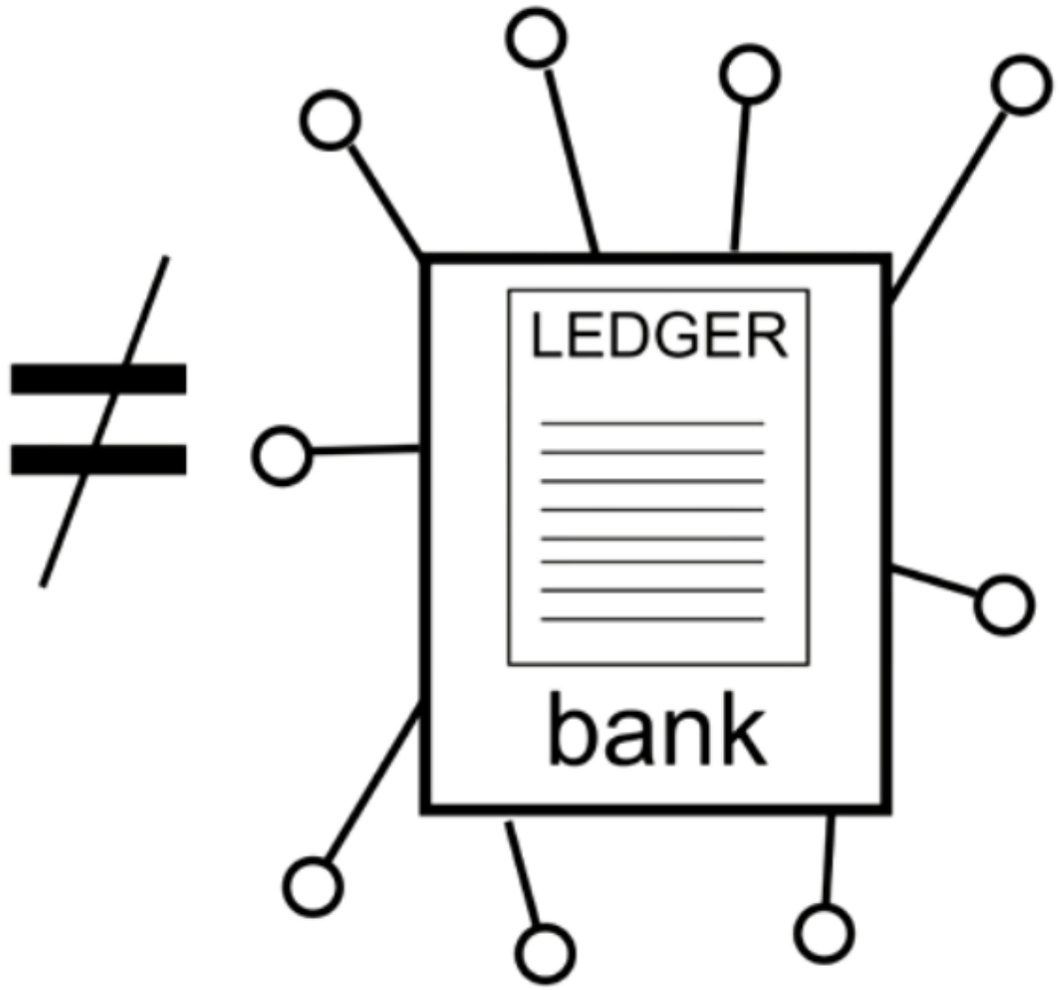
Such a distributed database used in Bitcoin is called blockchain.

Bitcoin



Decentralized Ledger

Centralized Bank (ex: PayPal)



Centralized Ledger

Transactions in Bitcoin

Transaction Message

From: **Bob** (1MVbjH...)

To: **Carol** (16pJcrG...)

Amount: **2.500**

7/27/2014

pay: Dave $ 100.00

One hundred and 00/100 dollars

Conventional banking systems rely on hand-written signature

Transaction Message

From: **Bob** (1MVbjH...)

To: **Carol** (16pJcrG...)

Amount: **2.500**

3045022100dc5
0feec13bc11eb..

Bitcoin relies on digital signature

CRYPTOGRAPHY

The U-Boats are coming!

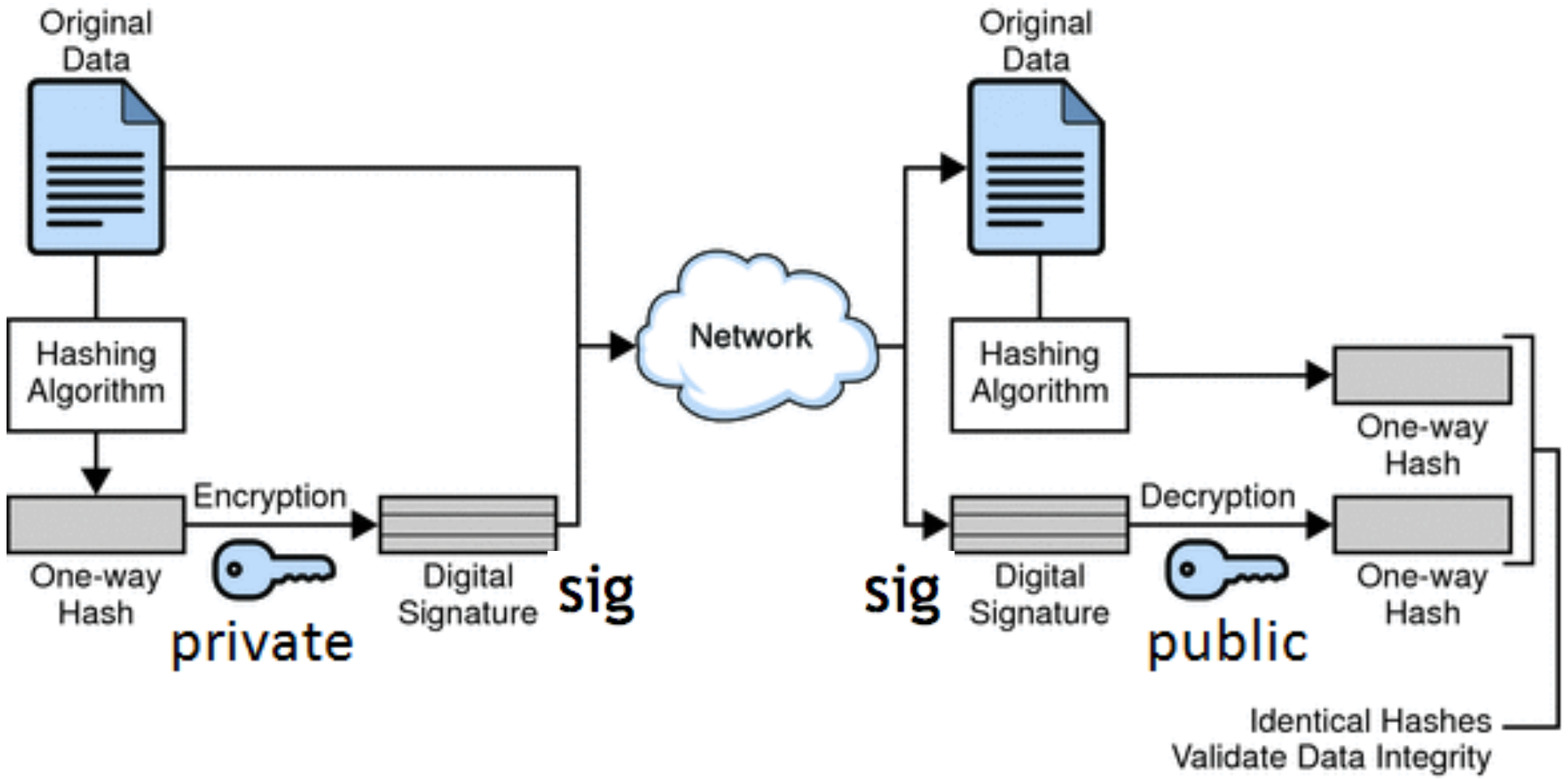
encrypt

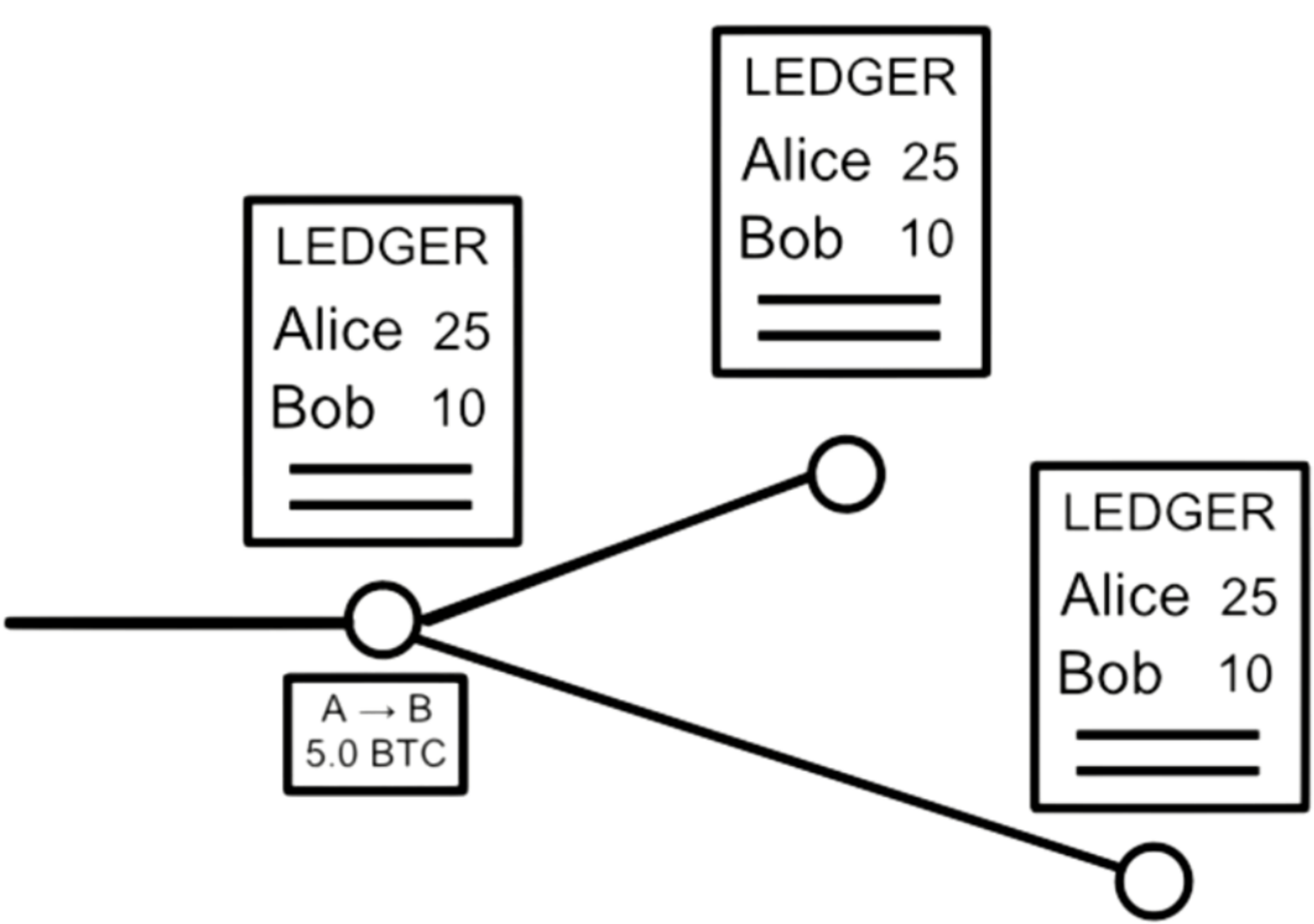
37si38d72kd039284hks

decrypt

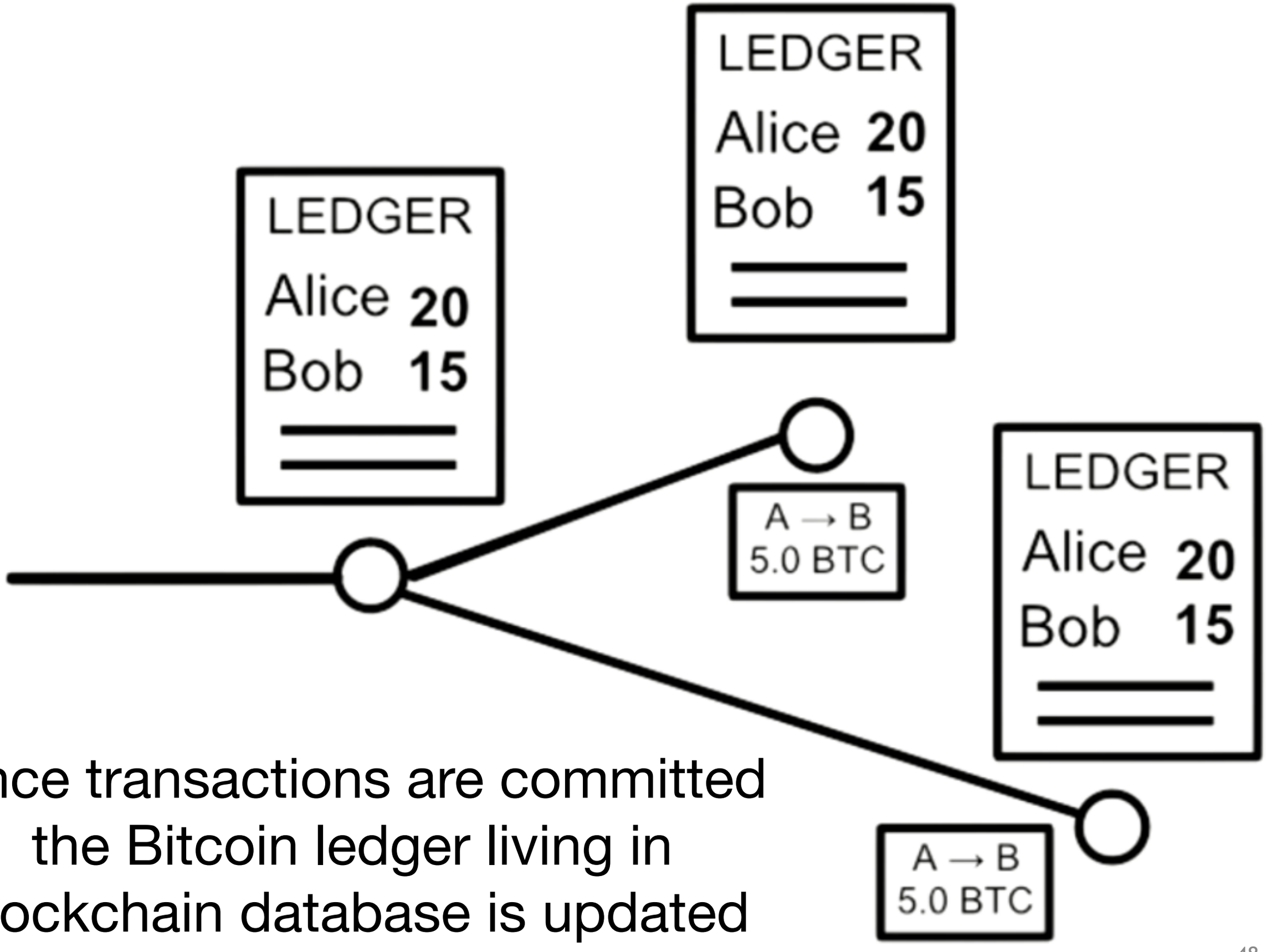
The U-Boats are coming!

Digital Signature Scheme



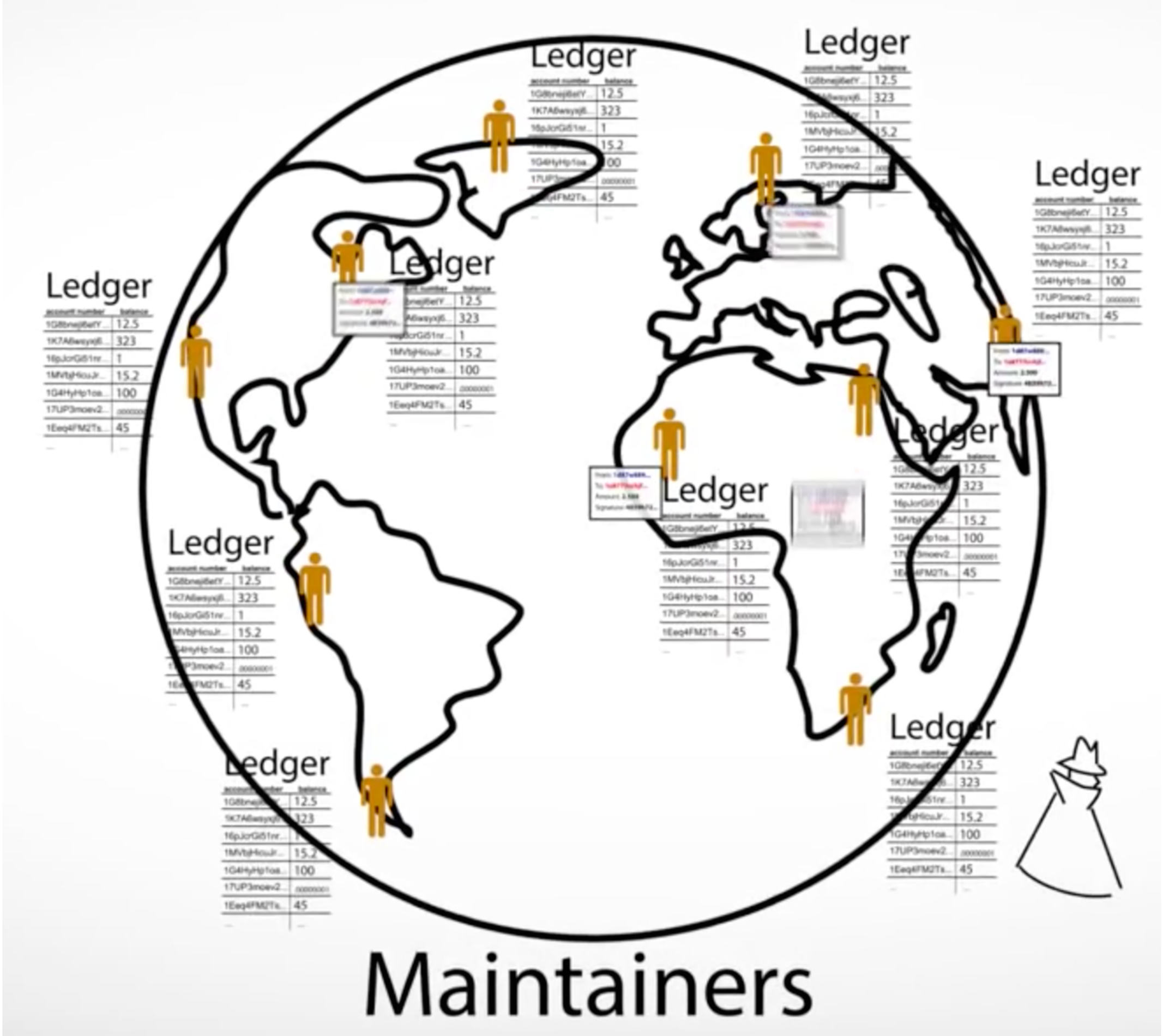


Once constructed, transactions are broadcasted through the Bitcoin peer-to-peer network

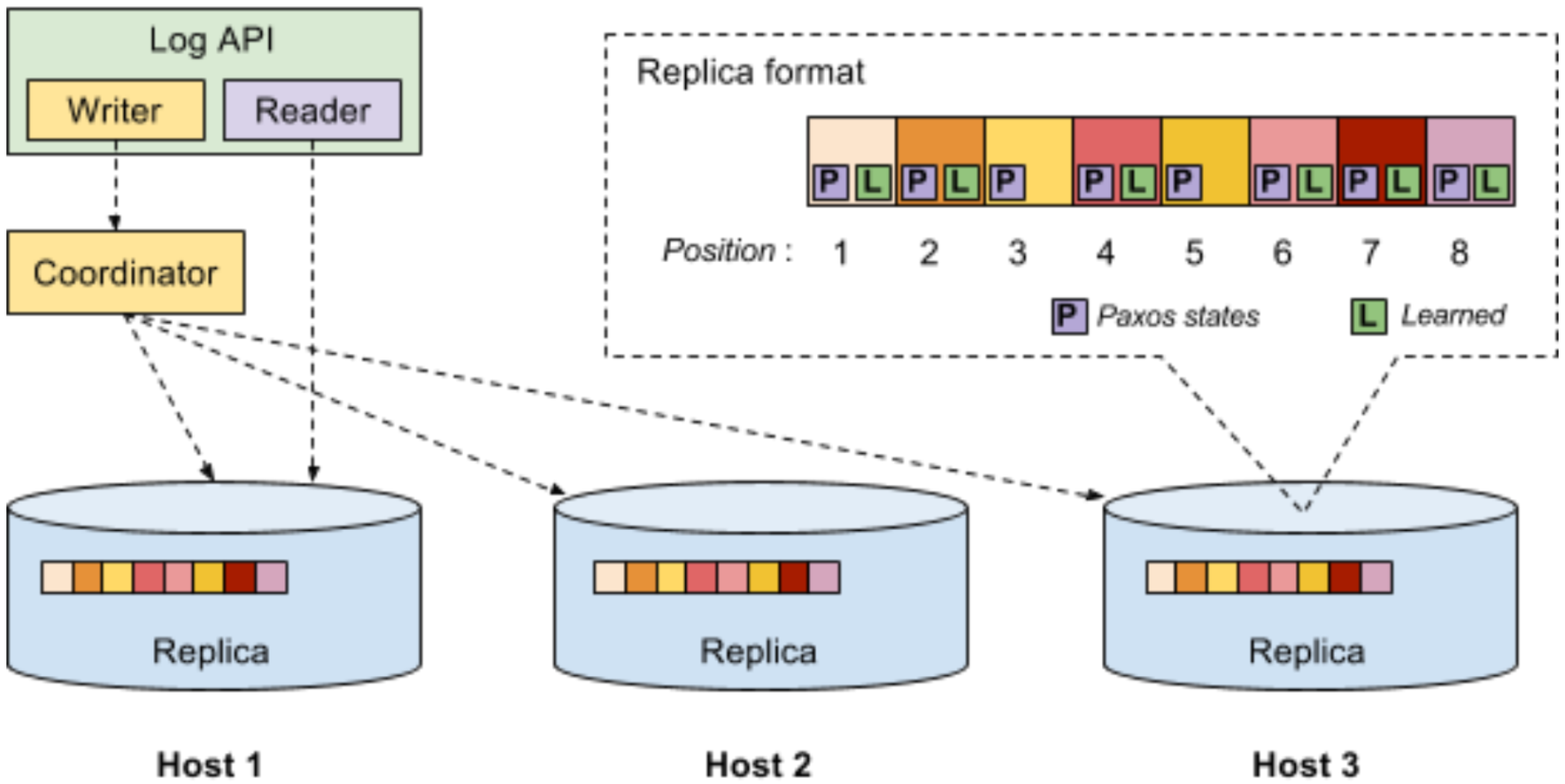


Once transactions are committed the Bitcoin ledger living in blockchain database is updated

Challenges in Updating Distributed Database with No Central Control


Ledger
account number
balance
1G8bnejj6etY...
12.5
1K7ABwsyxj6...
323
16pJcrGi51nr...
1
1MVbjHcuJr...
15.2
1G4HyHp1oa...
100
17UP3moev2...
.0000001
1Eeq4FM2Ts...
45
Maintainers

How Do We Update Centrally Controlled Distributed Database?



- Must ensure data consistency upon updates
- Must execute a consensus protocol to obtain such consistency
- Need to have a co-ordinator to lead the consensus protocol
- Consensus is a hard problem to solve correctly and efficiently
  - Primarily because of the need to accommodate fault-tolerance
- **If the co-ordinator can be trusted, there are classical algorithms to handle this problem**

Distributed Database with No Central Control

- Who is going to be the co-ordinator to lead the consensus so as to make sure that the ledger is consistent
  - There is simply no single trusted authority
- Some nodes in the Bitcoin peer-to-peer network are malicious and want to destroy it
  - Again, there is no single authority to block the membership of a decentralized peer-to-peer network

Bitcoin Consensus

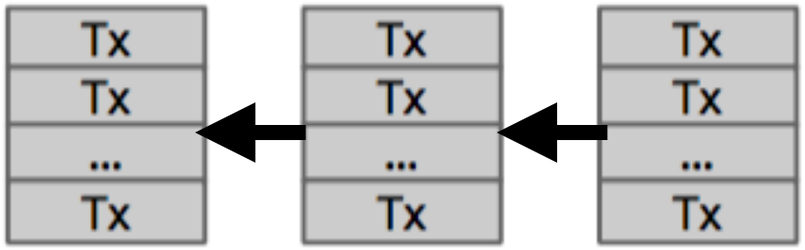
Nakamoto Consensus

- Each node competes to find a solution to an extremely difficult math problem (Proof-of-Work)
- The first node to obtain such a solution wins and is recognized to be a co-ordinator to lead the update of the ledger
- The update is broadcast to other peer nodes who gladly accept it and update their database accordingly

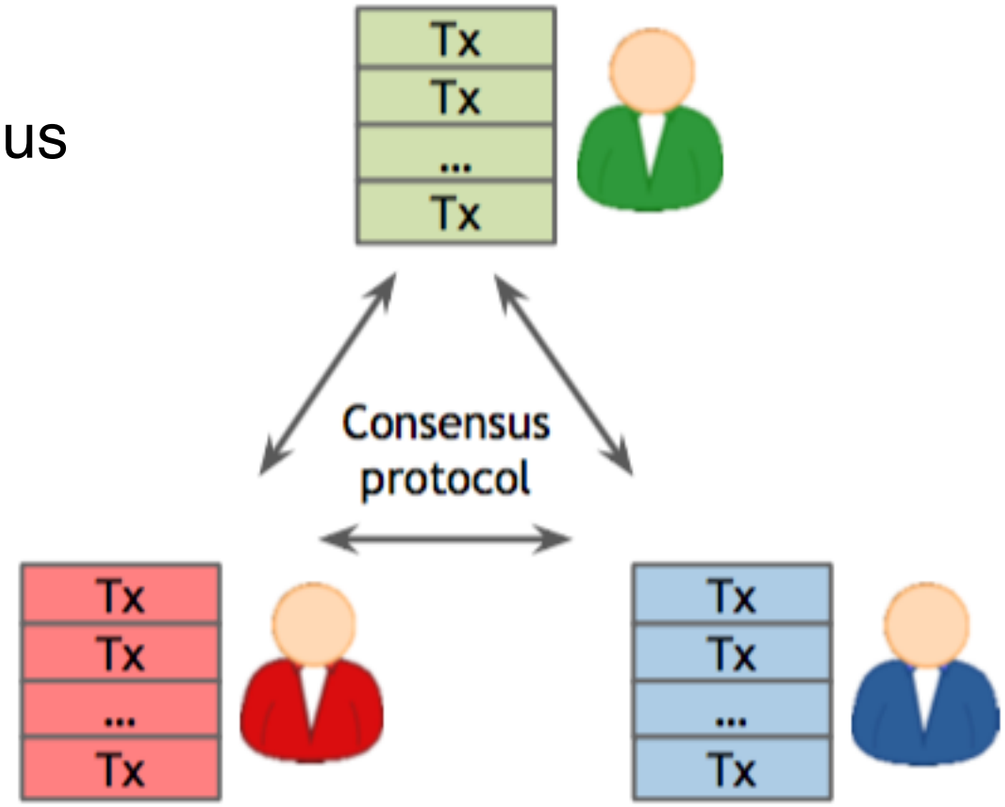
A node participating in the consensus is called a **Bitcoin miner**

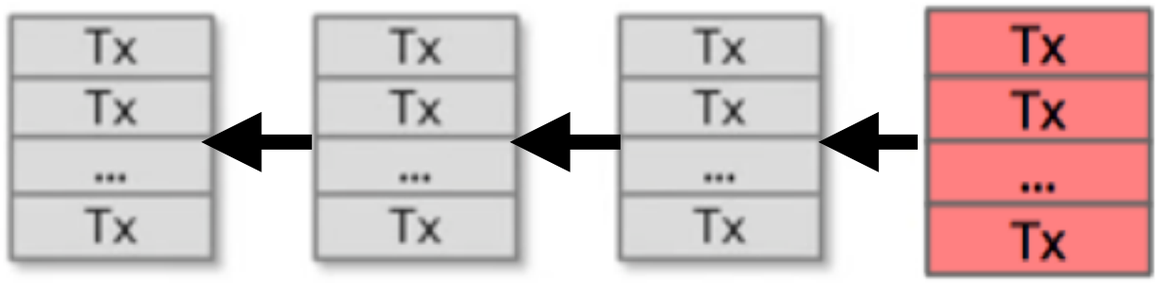
Updating of the Bitcoin Blockchain

Previous blocks accepted via consensus

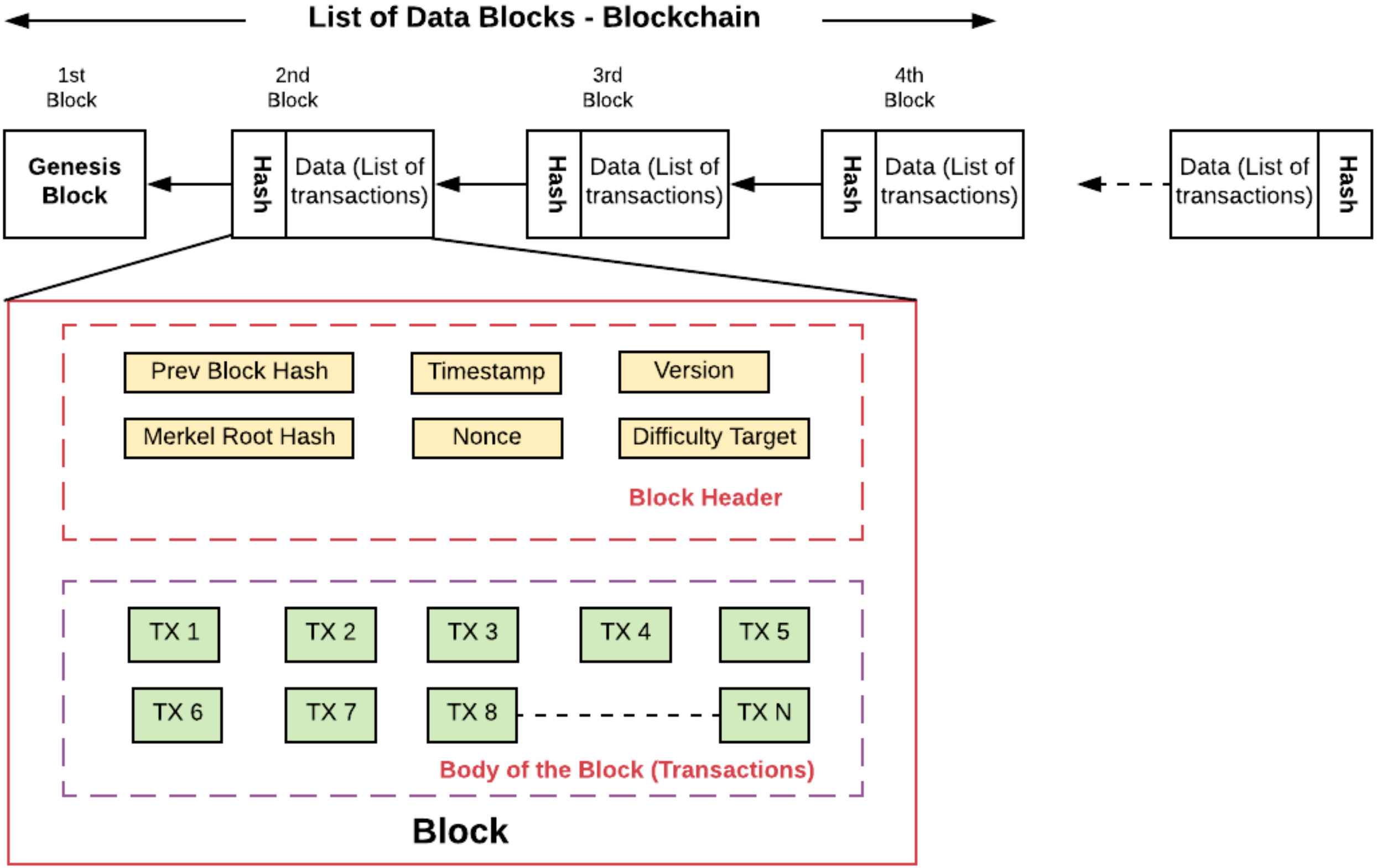


Protected by cryptography to ensure their integrity

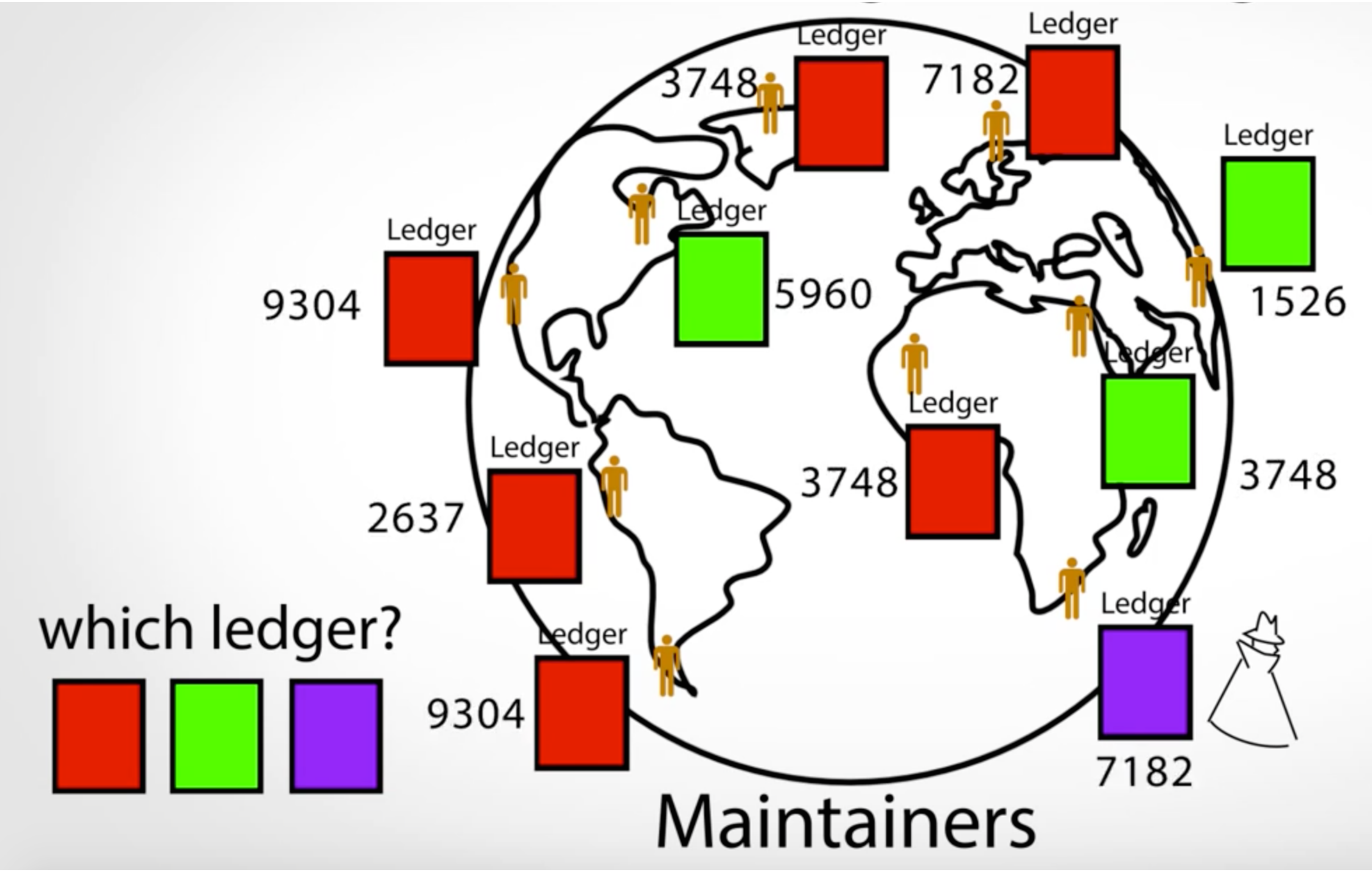


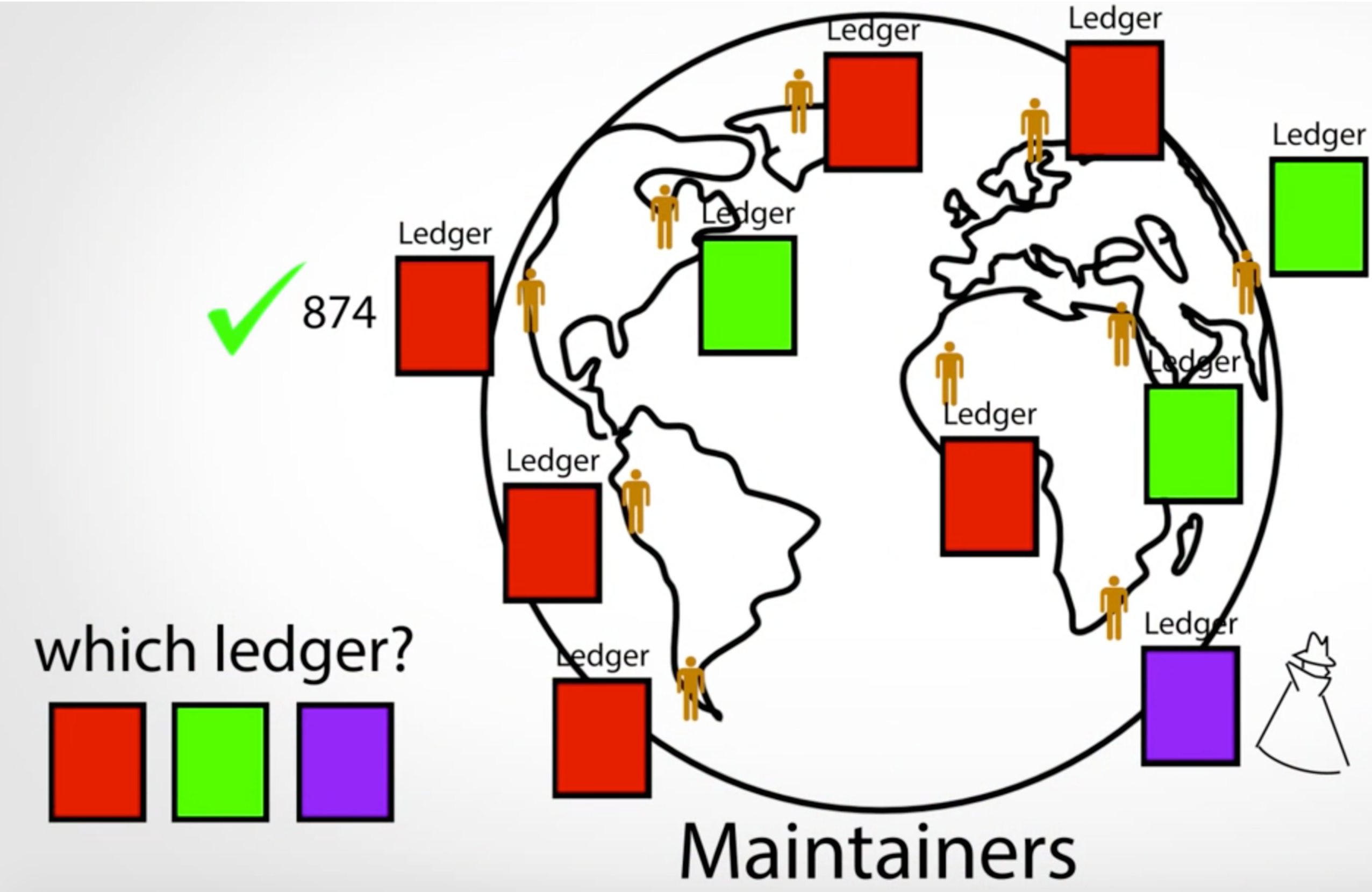


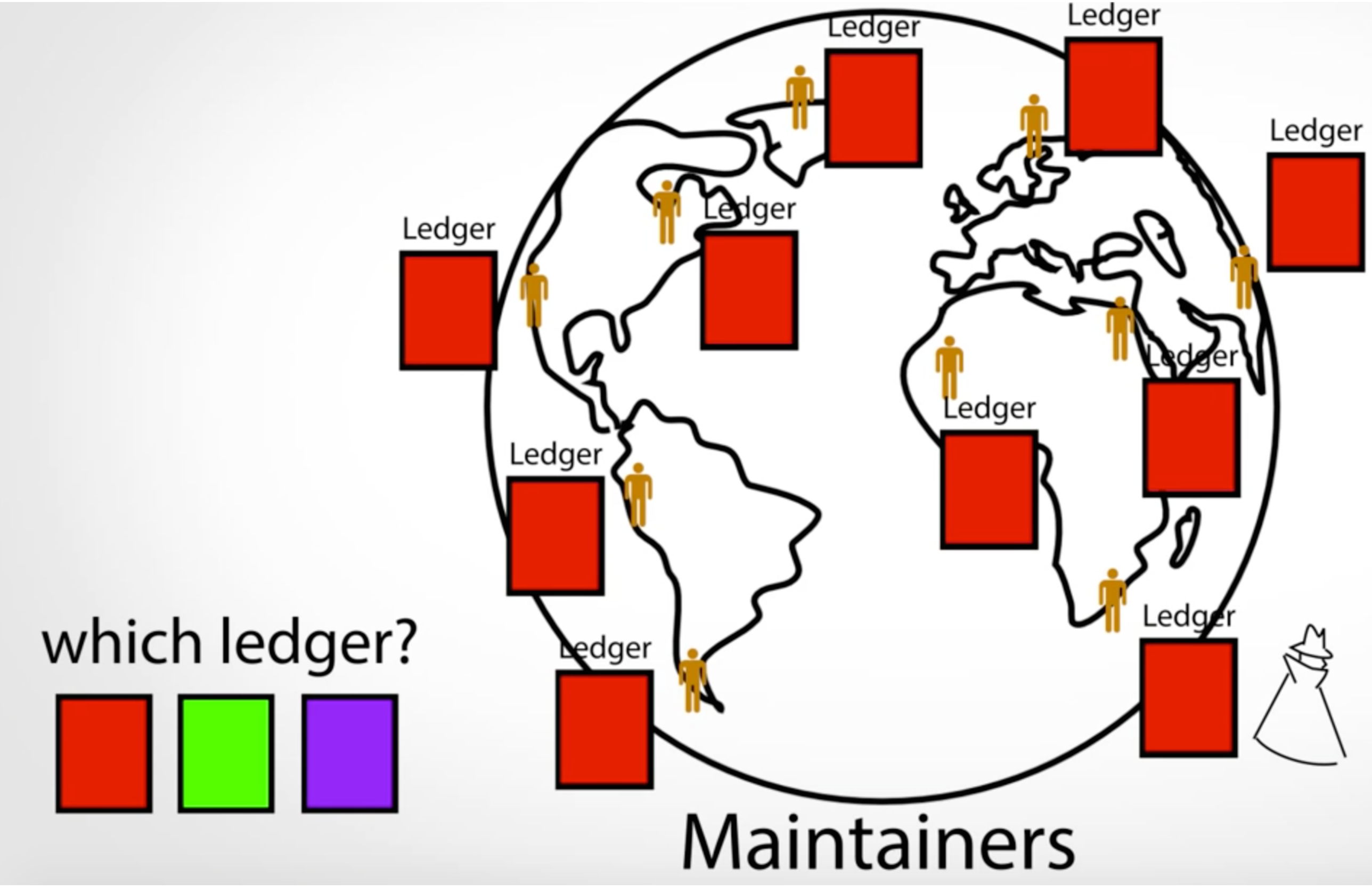
Latest block proposed by a Bitcoin miner who wins the race to solve the proof-of-work puzzle



From: https://vitalflux.com

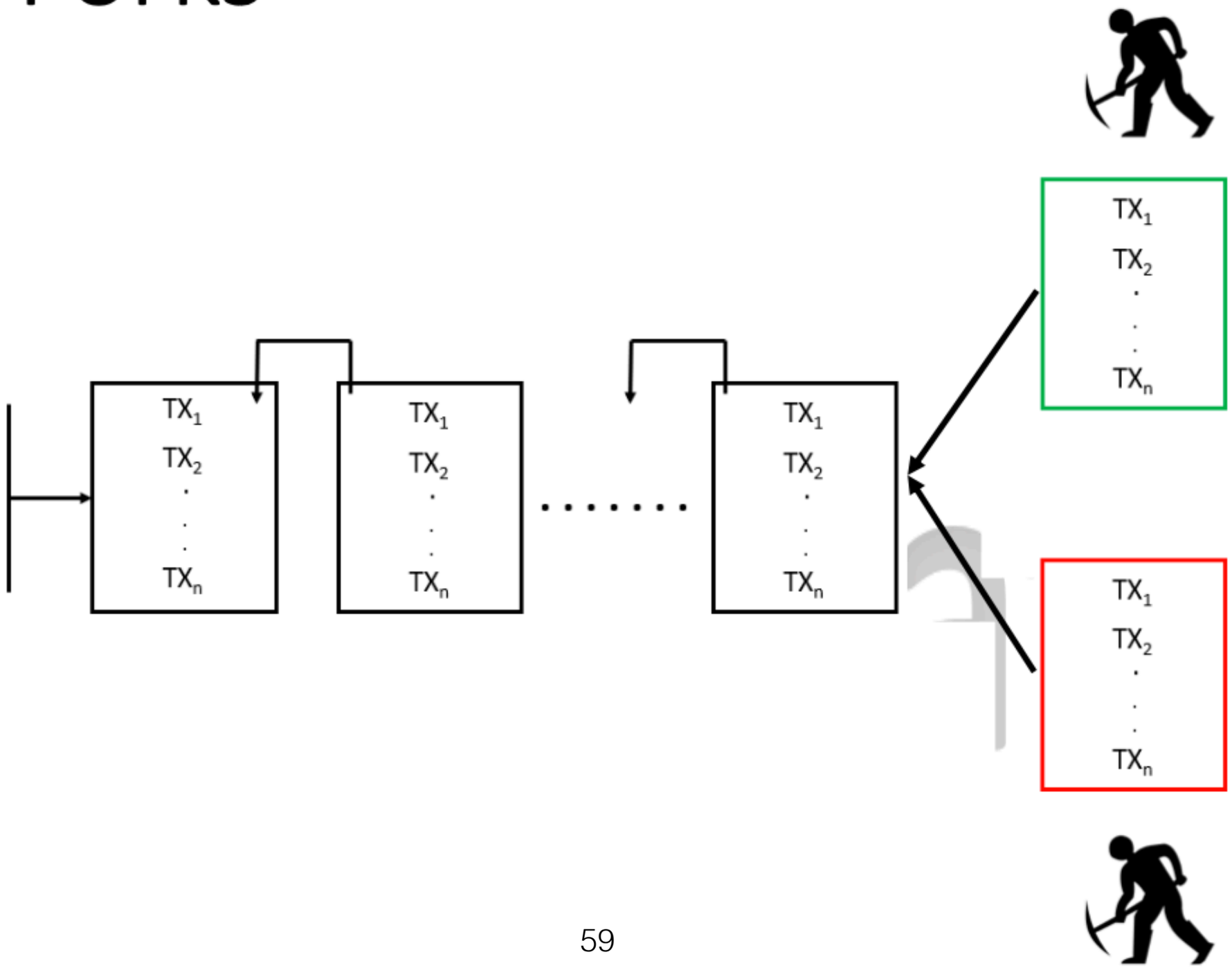

Ledger
3748
Ledger
7182
Ledger
Ledger
9304
5960
1526
Ledger
Ledger
3748
Ledger
2637
Ledger
Ledger
9304
7182
which ledger?
Maintainers


Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
874
which ledger?
Maintainers


Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Maintainers
which ledger?

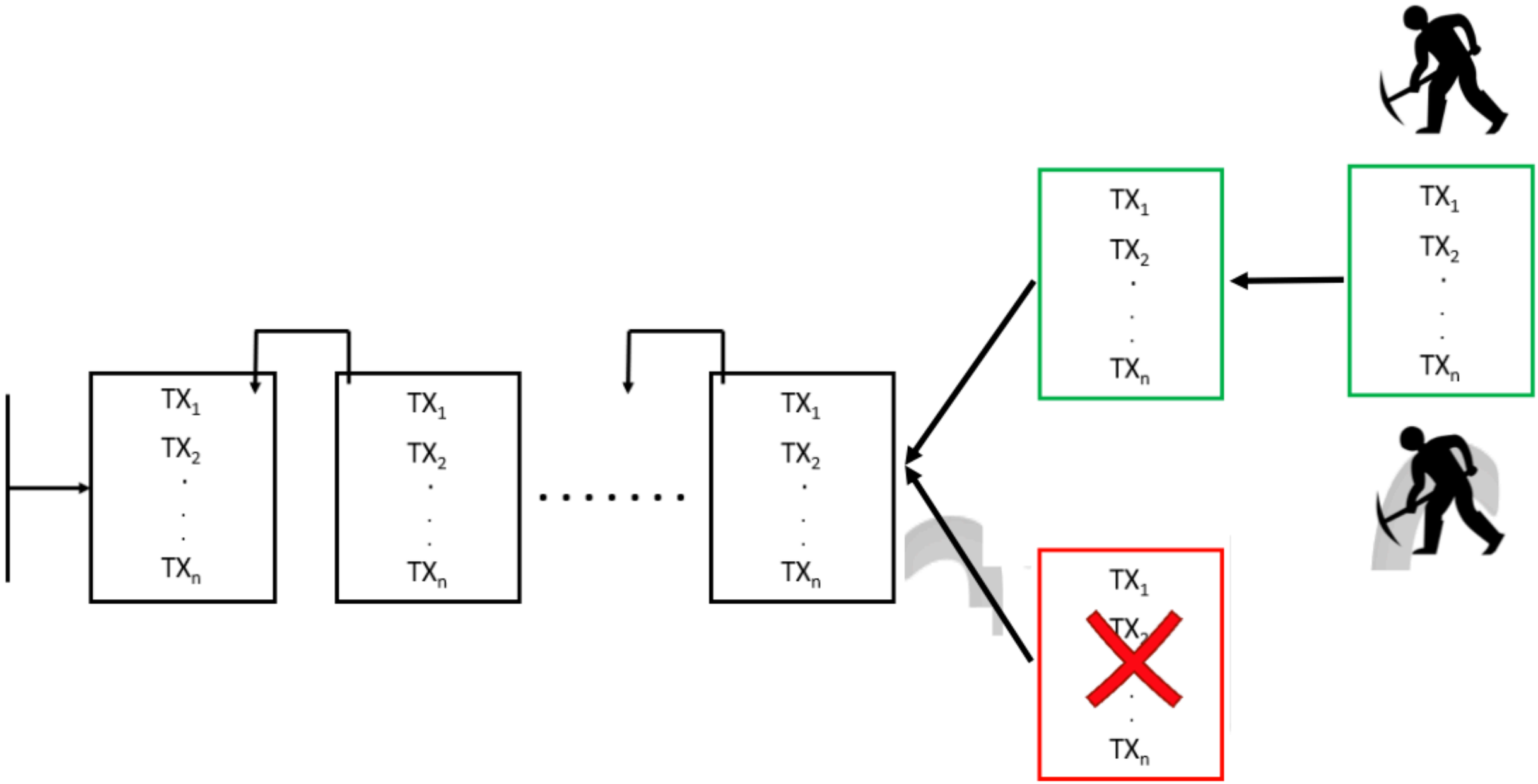
More Than One PoW Winners

Forks



Longest chain wins

Forks



Bitcoin Consensus

Nakamoto Consensus V2

- Each node competes to find a solution to an extremely difficult math problem (Proof-of-Work)
- The first node to obtain such a solution wins and is recognized to be a co-ordinator to lead the update of the ledger
- The update is broadcast to other peer nodes who gladly accept it and update their database accordingly
- **“Longest chain rule” decides which fork will be accepted**

Nakamoto Consensus and Malicious Nodes

- To update the ledger, every node must perform the proof-of-work in the competition
- Hence, if there are more than 50% of the honest nodes in the network, it is unlikely that the malicious nodes win the competition
- So, the malicious nodes is unlikely to update the ledger and destroy it
  - In case it does win the race and update garbage to the ledger, honest nodes will revert this state later

Why Would Anyone Want to Become a Miner

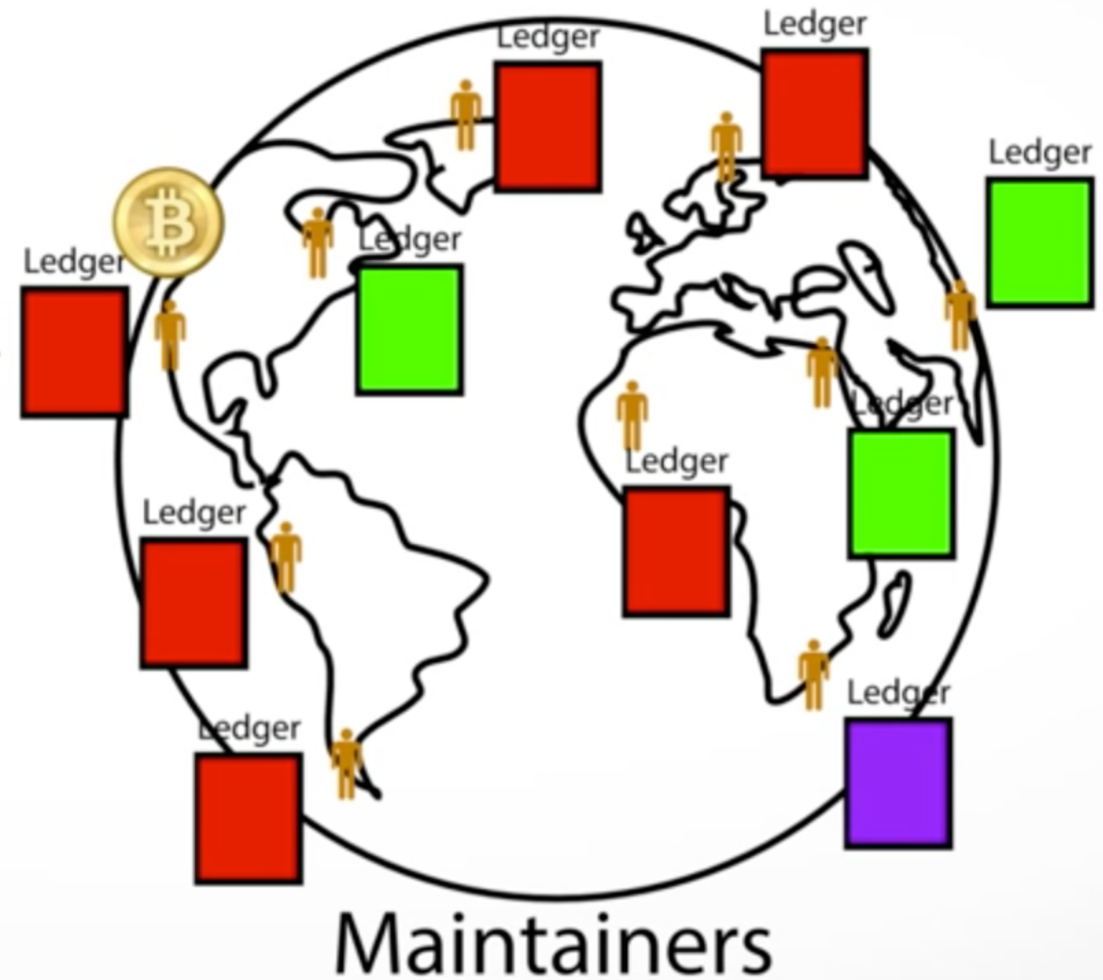
Money Creation

Ledger

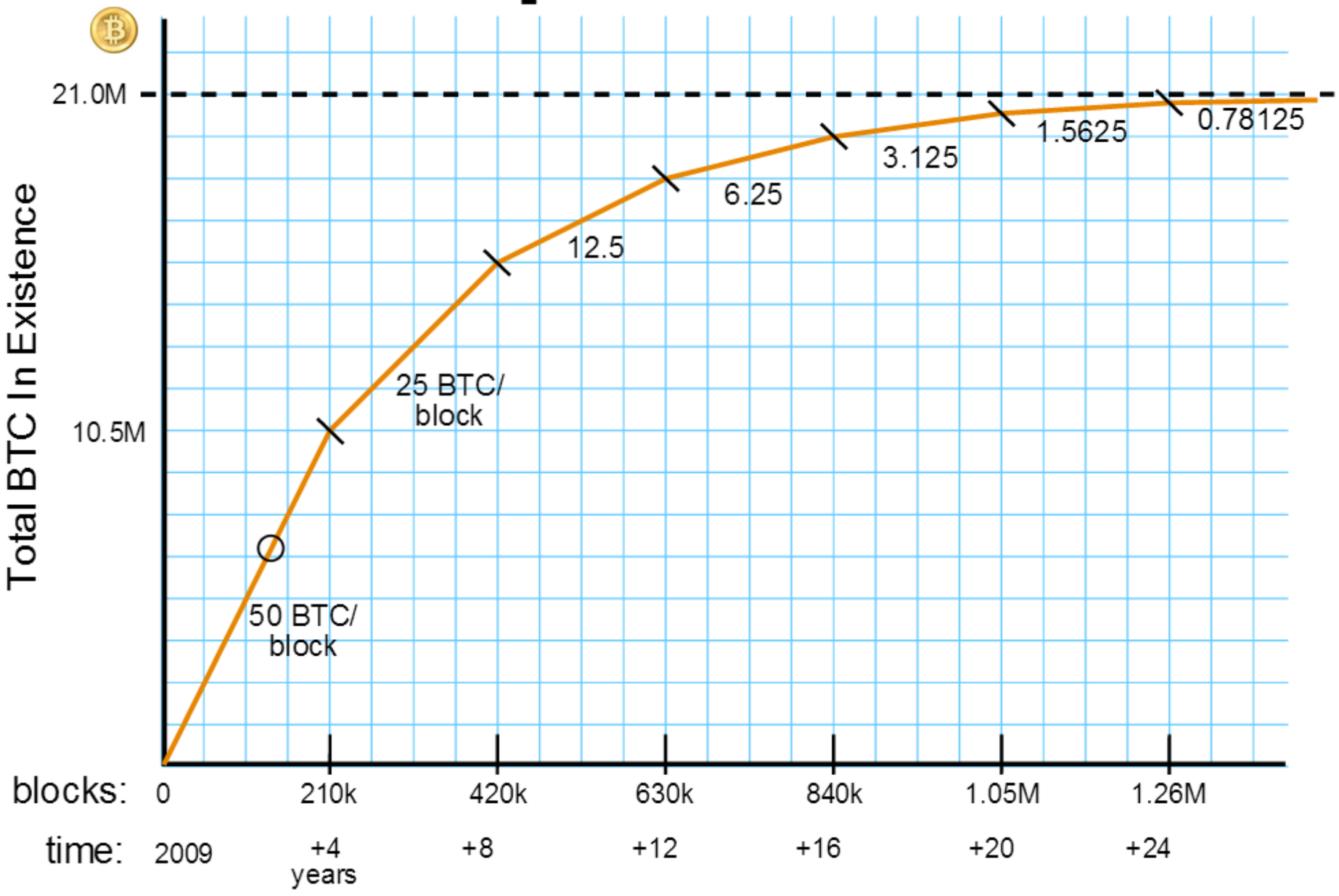
account number	balance
1G8bneji6etY...	12.5
1K7A6wsyxj6...	323
16pJcrGi51nr...	26 +25
1MVbjHicuJr...	15.2
1G4HyHp1oa...	100
17UP3moev2...	.00000001
1Eeq4FM2Ts...	45
...	...

winning maintainer

✓ 874



BTC Expansion Curve



What is the “fair” value of Bitcoin?

Current Market Price:

https://www.coindesk.com/price/bitcoin/

Can you estimate the value of each of these watches?

How much is this painting worth?

Rothko Fetches $75 Million at Record-Setting Sotheby's Sale

If you're looking for evidence that today's art market is alive and well, look no further

By Lily Rothman @lilyrothman | Nov. 14, 2012 | 59 Comments

In a Nov. 13 sale that scored a record total for Sotheby's auction house—$375,149,000 in one night, beating the previous record by more than $13 million—a canvas by the abstract expressionist Mark Rothko led the night with a whopping $75.1 million sale (including fees). The painting, *No. 1 (Royal Red and Blue)*, went to an anonymous bidder for the second-highest amount of any Rothko in history, far more than the pre-sale estimate of between $35 and $50 million. The price was surpassed only by the nearly $87 million, according to the New York *Times*, that was fetched by the Rothko painting *Orange, Red, Yellow* earlier this year.

The Rothko, which Sotheby's said in a statement is a seminal "masterpiece" and which is nearly ten feet tall, was one of only eight works that the artist personally selected for his 1954 solo show at the Art Institute of Chicago. It then remained in the collection of the same person for three decades. It was consigned by Anne Marion of Fort Worth, Tex., according to *Bloomberg*.

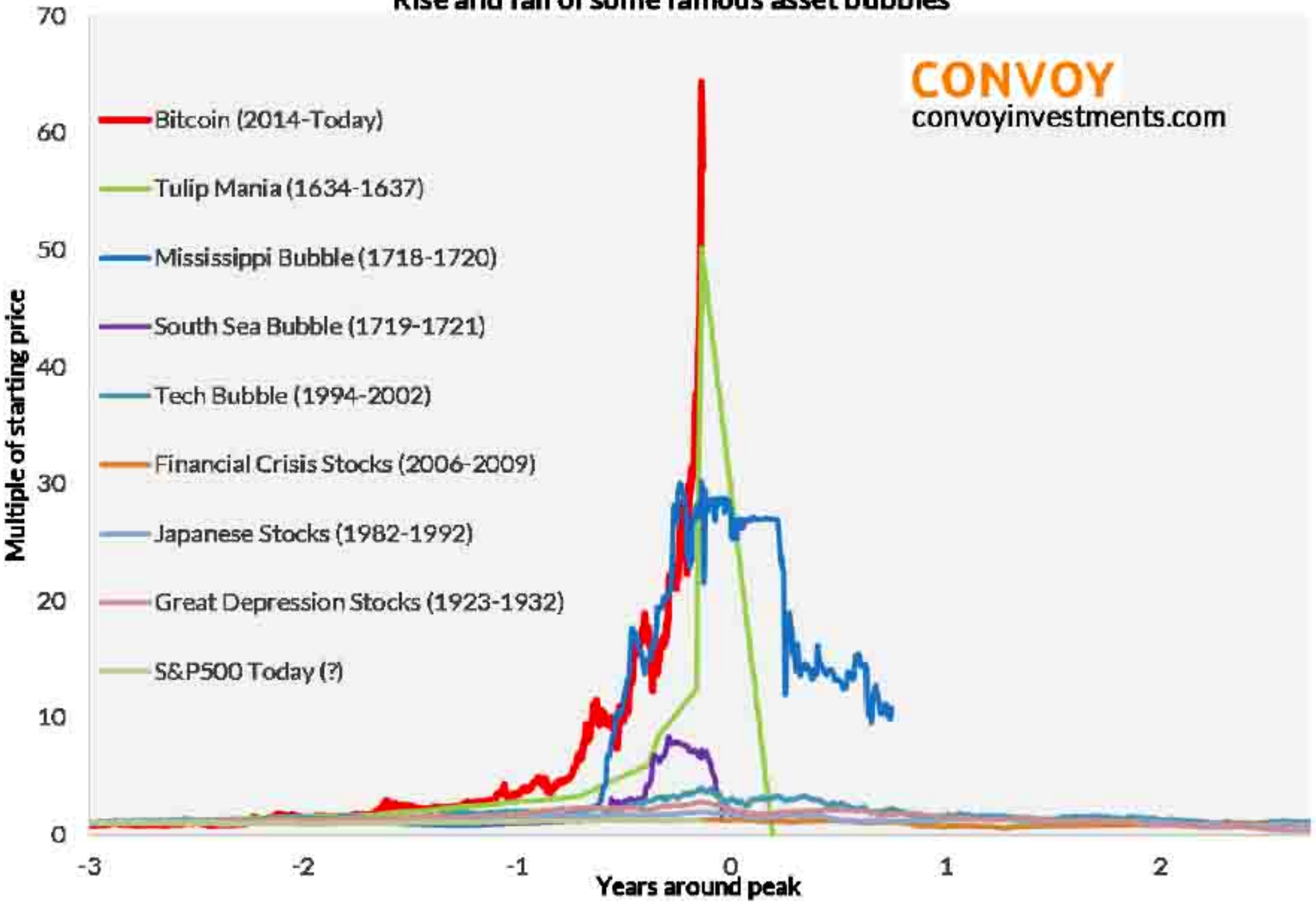
(**MORE**: A Recommendation Engine Takes on Fine Art)

Other highlights from the 69-lot contemporary art auction include Jackson Pollock's *Number 4, 1951*, which sold for $40.4 million; Francis Bacon's *Untitled (Pope)*, which sold for $29.8 million; Willem de Kooning's *Abstraction*, which sold for $19.7 million; and Gerhard Richter's *Abstraktes Bild*, which sold for $17.4 million. In addition, an Andy Warhol silkscreen, the 1964 print *Suicide*, sold for $16.3 million and set a record price for a Warhol work on paper.

SOTHEBY'S / EPA

Mark Rothko's painting No 1 was sold by Sotheby's New York during a contemporary art evening sale for 75,122,500 US dollar. The price far exceeded from the pre-sale estimated price of 35,000,000 - 50,000,000 US dollars.

Rise and fall of some famous asset bubbles



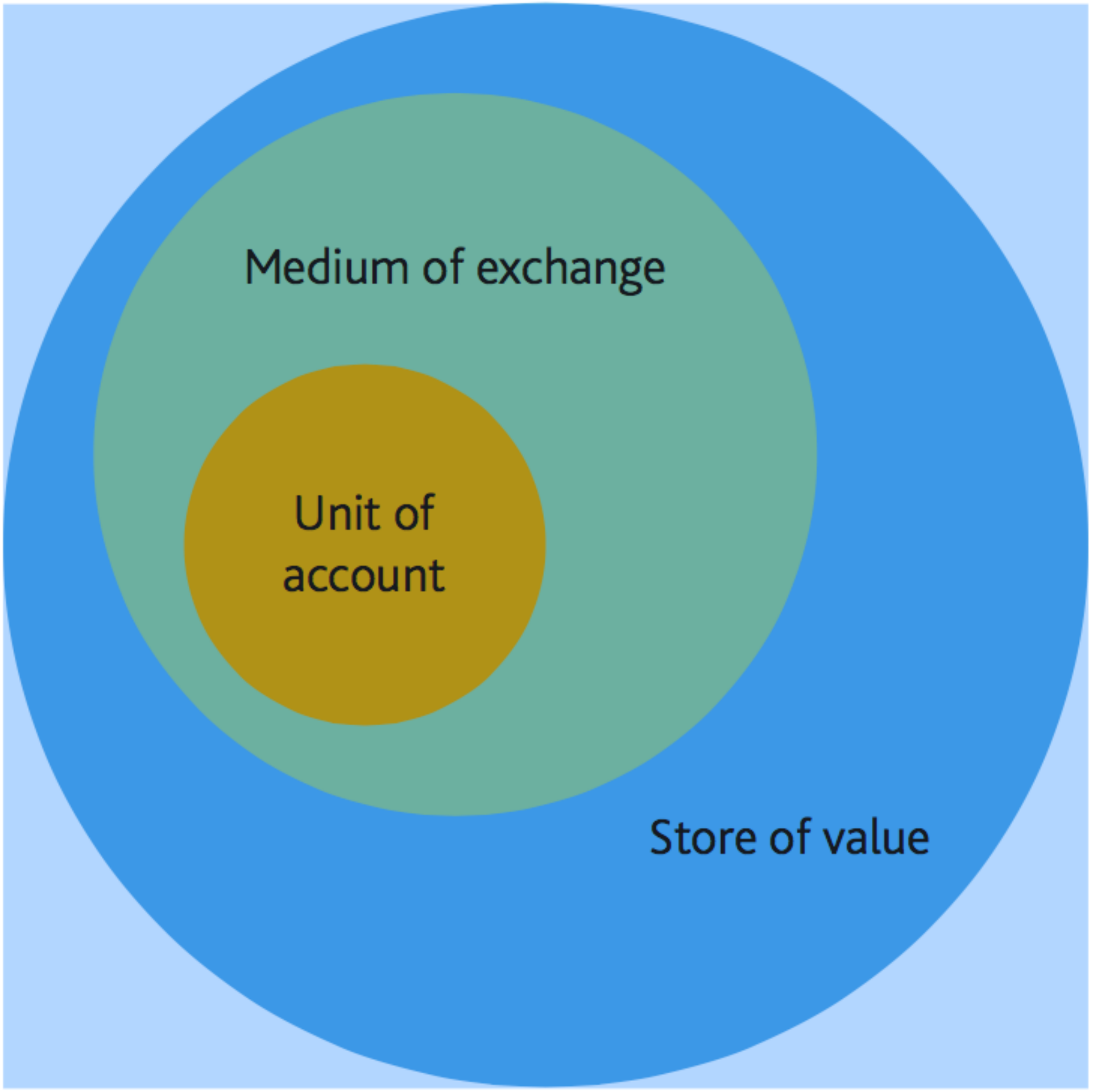
Source: Elliot Wave International, Yale SOM, St. Louis FRED, GlobalFin, and Convoy analysis

Bitcoin versus the Thai Baht

- Bitcoin is a cryptocurrency just like Litecoin, Bitcoin Cash, Chia, etc.
- The Thai Baht is a fiat currency just like the US dollar, the Japanese Yen, etc.

Desirable properties of money:

- Store of value
- Medium of exchange
- Unit of account


Medium of exchange
Unit of account
Store of value

The Thai Baht possesses all the three properties whereas Bitcoin currently (February 2022) has only two out of three (Bitcoin has not yet become a prevalent unit of account.)

Baht : Bitcoin
3 : 2

Usage of Bitcoin: Past to Present

- Transactions on businesses operated on the Darknet and paying ransom demanded by Ransomware
- On-line gambling
- Transactions on everyday life
- As a store-of-value asset
  - Buy/sell via crypto exchanges for long term investment or short term profit taking

Firefox | Welcome! | Silk Road | Welcome! | Silk Road

silkroadvb5piz3r.onion

Silk Road

anonymous marketplace

Welcome **Cult Leader**!

messages(0) | orders(0) | account($0.00) | settings | log out

search | (0)

8 days 2 hrs 51 mins 31 secs until Four Twenty!!!

Shop by category:

- Drugs(2679)
  - Cannabis(741)
  - Dissociatives(59)
  - Ecstasy(274)
  - Opioids(214)
  - Other(76)
  - Prescription(515)
  - Psychedelics(348)
  - Stimulants(256)
- Apparel(22)
- Books(283)
- Computer equipment(13)
- Digital goods(220)
- Drug paraphernalia(52)
- Electronics(19)
- Fireworks(1)
- Forgeries(41)
- Hardware(3)
- Home & Garden(5)
- Jewelry(1)

CRANBERRY KUSH & STRAWBERRY...
$36.82

10pc of Genuine Fake Blu Ray Discs
$49.50

30mg Oxycodone (Roxie, Roxy) IR...
$250.00

BITCOINS - NOW THE LOWEST PRICE...
$0.00

Diazepam (valium) 10mg - 1000...
$425.50

Anarcho47's Magikally Epic...
$2.48

News:

- Who's your **favorite**?
- Acknowledging **Heroes**
- A new annonymous market **The Armory**!
- **State of the Road Address**

TorBrowser

Domain seized | Silk Road

silkroadvb5piz3r.onion

Startpage

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York


bitcoin
ACCEPTED HERE
STARBUCKS
COFFEE

El Salvador becomes first country to adopt Bitcoin as an official currency

The cryptocurrency will be legal tender alongside the US dollar

By Jon Porter | @JonPorty | Sep 7, 2021, 4:58am EDT

SHARE

A recently-installed Bitcoin ATM.

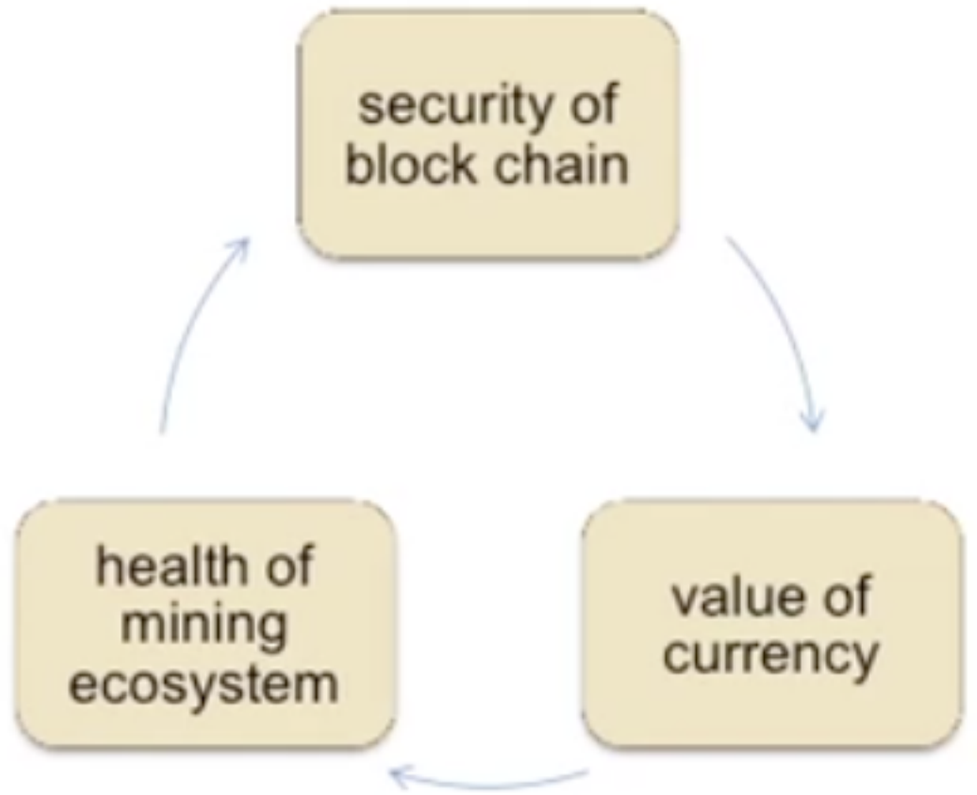
Business

MicroStrategy Buys Additional $25M Worth of Bitcoin During Market Dip

The acquisition rate in January was markedly lower than in December.

By Michael Bellusci, Jamie Crawley · Feb 1, 2022 at 8:17 p.m. · Updated Feb 3, 2022 at 4:02 a.m. ·

Sustainability of Bitcoin Blockchain



Bitcoin is bootstrapped

Back to Database Classification

Classifying Database Technology

Centralized Control

Centralized (SQL)

Distributed (NoSQL)

Decentralized Control

?

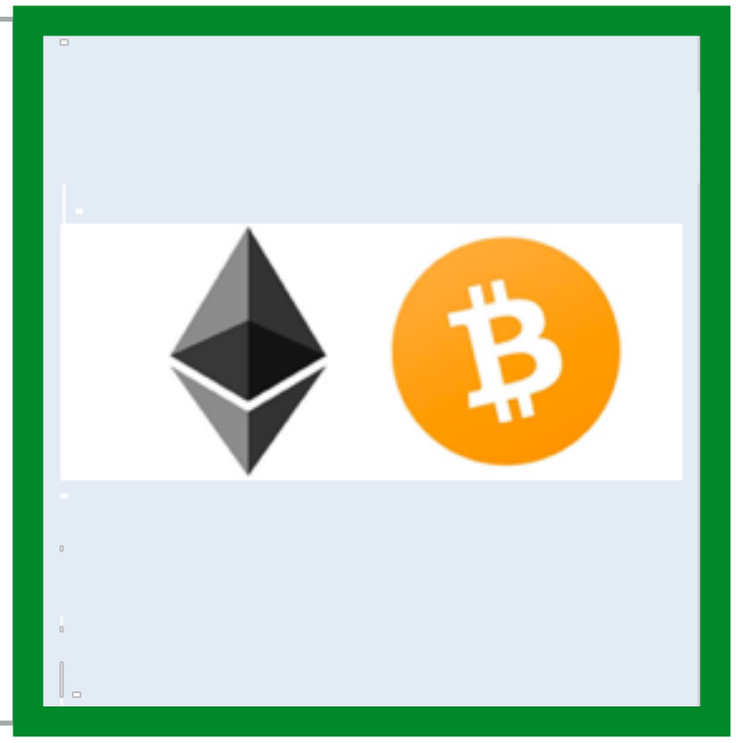
Classifying Database Technology

Centralized Control

Centralized (SQL)

Distributed (NoSQL)

Decentralized Control



Distributed (Blockchain)

Classifying Database Technology

Centralized Control

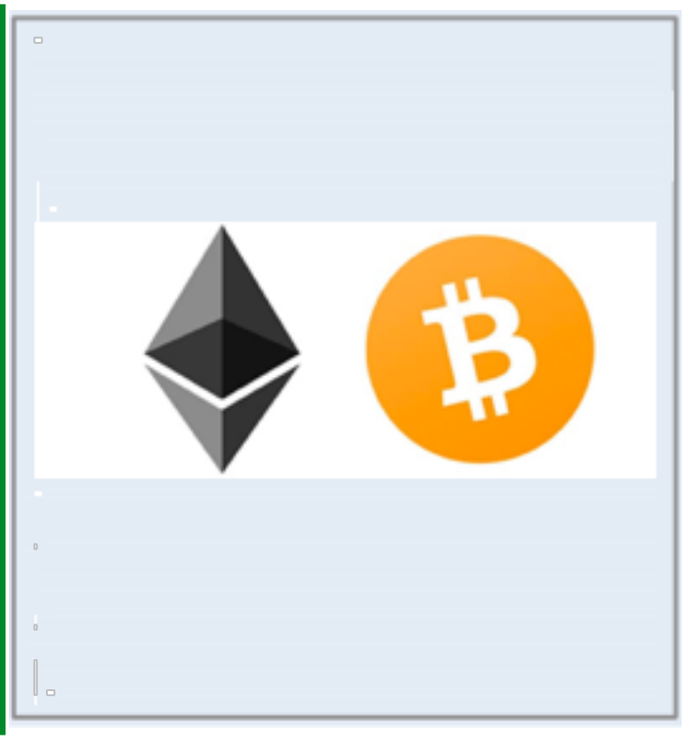
Centralized (SQL)

Distributed (NoSQL)

Decentralized Control

Centralized database with decentralized control

?



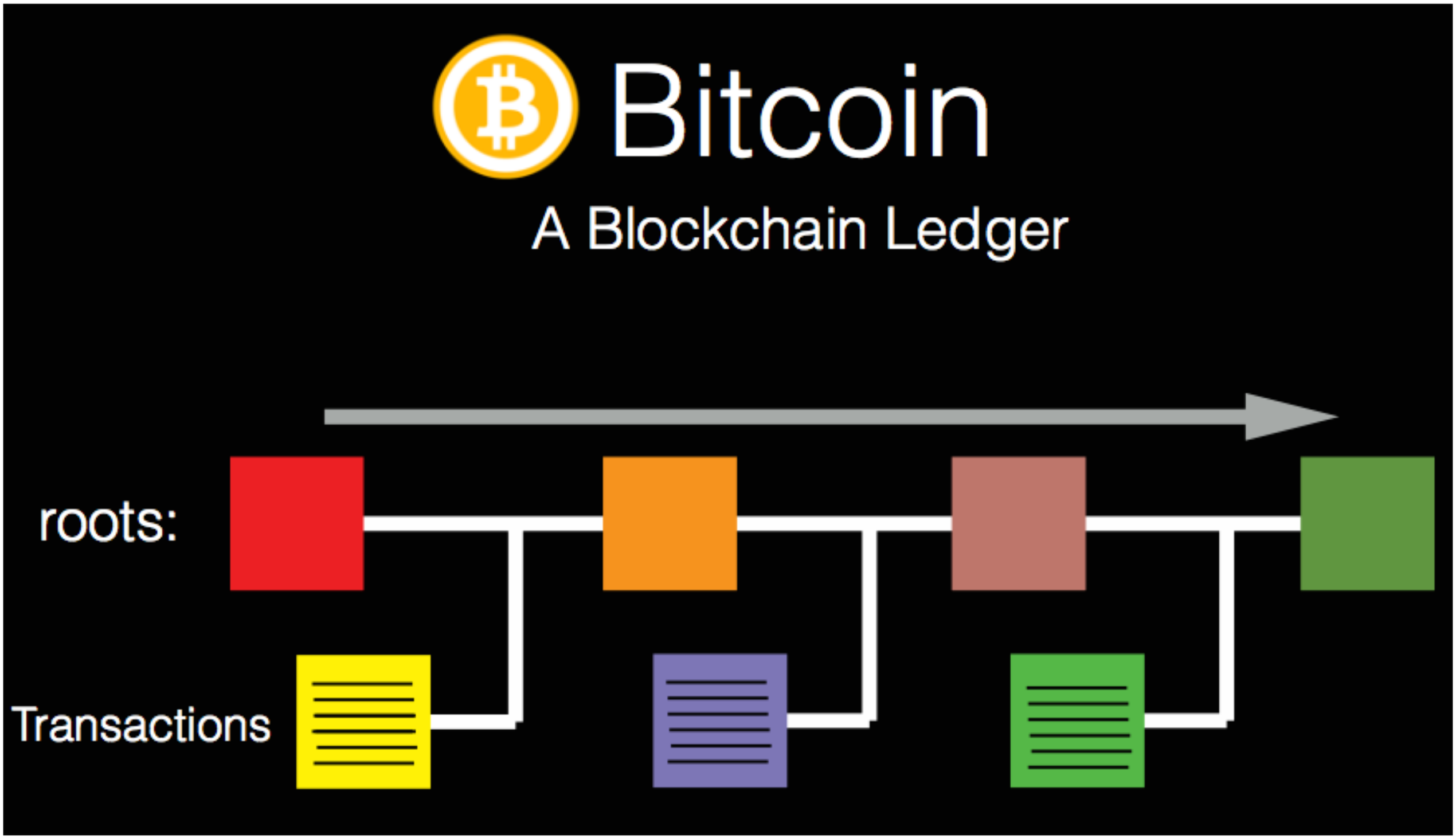
Distributed (Blockchain)

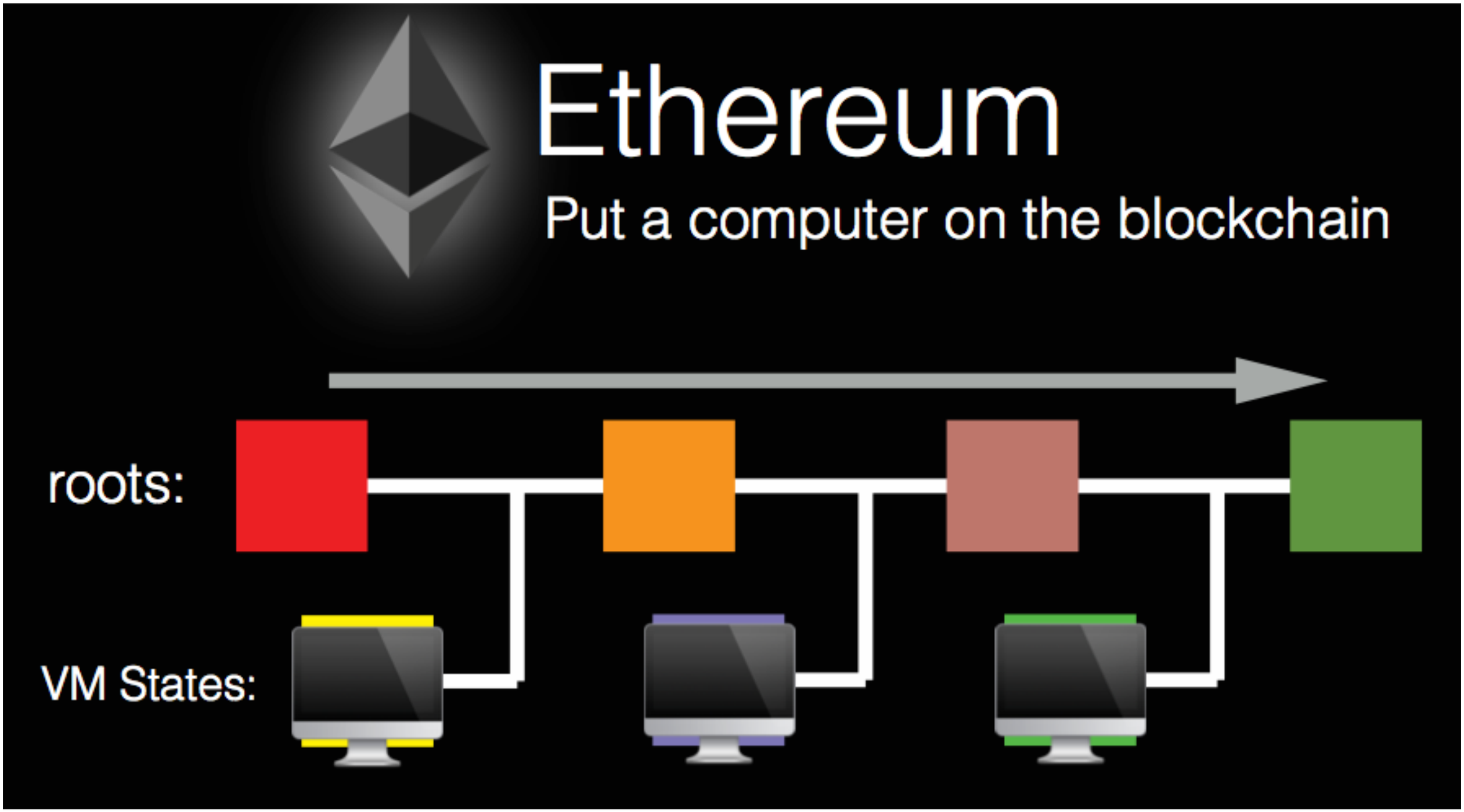
Bitcoin in Summary

- Bitcoin brought us a new type of system that does not rely on the control of some central authorities
- Bitcoin introduced us to blockchain, a new type of distributed database with decentralized control
- Bitcoin blockchain is a database that primarily stores Bitcoin transactions
- **What if we could have blockchain that not only stores transactions but also computer programs**
  - **Coming to you in the next section: the Etheruem blockchain**

Agenda

- Evolution of database technology
- Bitcoin and blockchain
- Ethereum and smart contracts
- Conclusion


Bitcoin
A Blockchain Ledger
roots:
Transactions


Ethereum
Put a computer on the blockchain
roots:
VM States:

Smart Contract

- Is a type of software stored on the Ethereum blockchain
- Is a representation of real world contracts, specifications, and rules
- In the real world, there are centralized trusted authorities that handle such things
  - Insurance companies, constitutional courts, etc.
- **Ethereum smart contracts** are written in a **high-level programming language** called **Solidity**

Why Smart Contracts

- The code is the law; let it decide without feeling or prejudice
- The code execution on the Ethereum blockchain is transparent and devoid of any dependence on trusted authorities
- Promote a trustless, democratic, and efficient society

From the words of Ethereum co-founder, Vitalik Buterin

Problem: most existing blockchain protocols were designed like this:


Or, at best, like this:

So… why not make a protocol that works like this?*

What Is Ethereum?

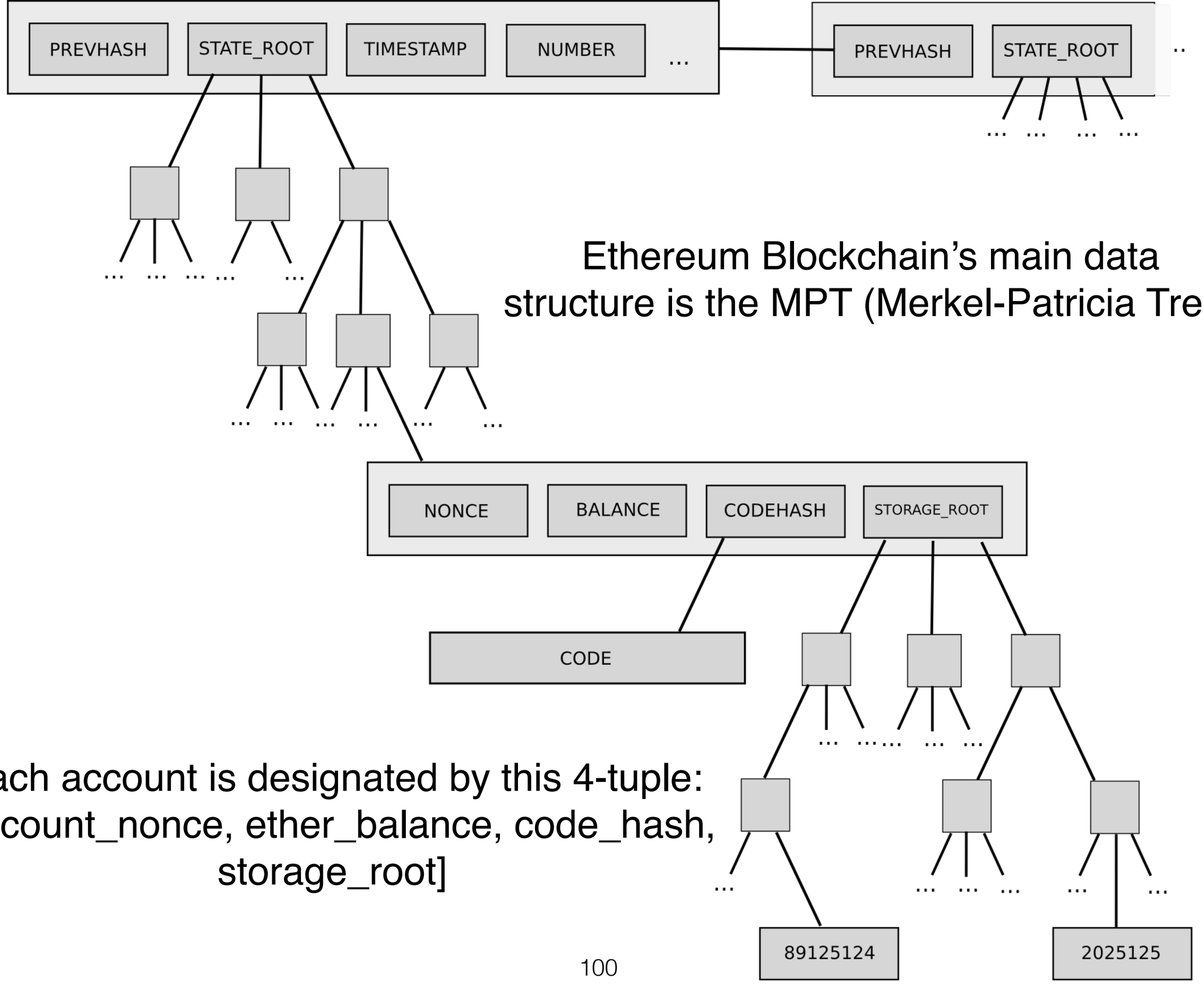
- Decentralized platform for smart contracts
  - Afford extremely high degree of fault-tolerance
  - Censorship resistant
- Act like decentralized computers
  - However, it is not the same as cloud computing
- The is a currency called Ether being rewarded to miners who are selected to update the Ethereum blockchain

Types of Accounts on Ethereum

- Externally Owned Account (EOA)
  - There is an owner of the EOA
  - Has an address
  - Has an Ether balance
  - Can transact with the contract code
- Contract Account (Contract)
  - Has an address
  - Has an Ether balance
  - Store smart contracts
  - Execute the stored smart contracts upon calls originated from transactions from EOA or other contract accounts

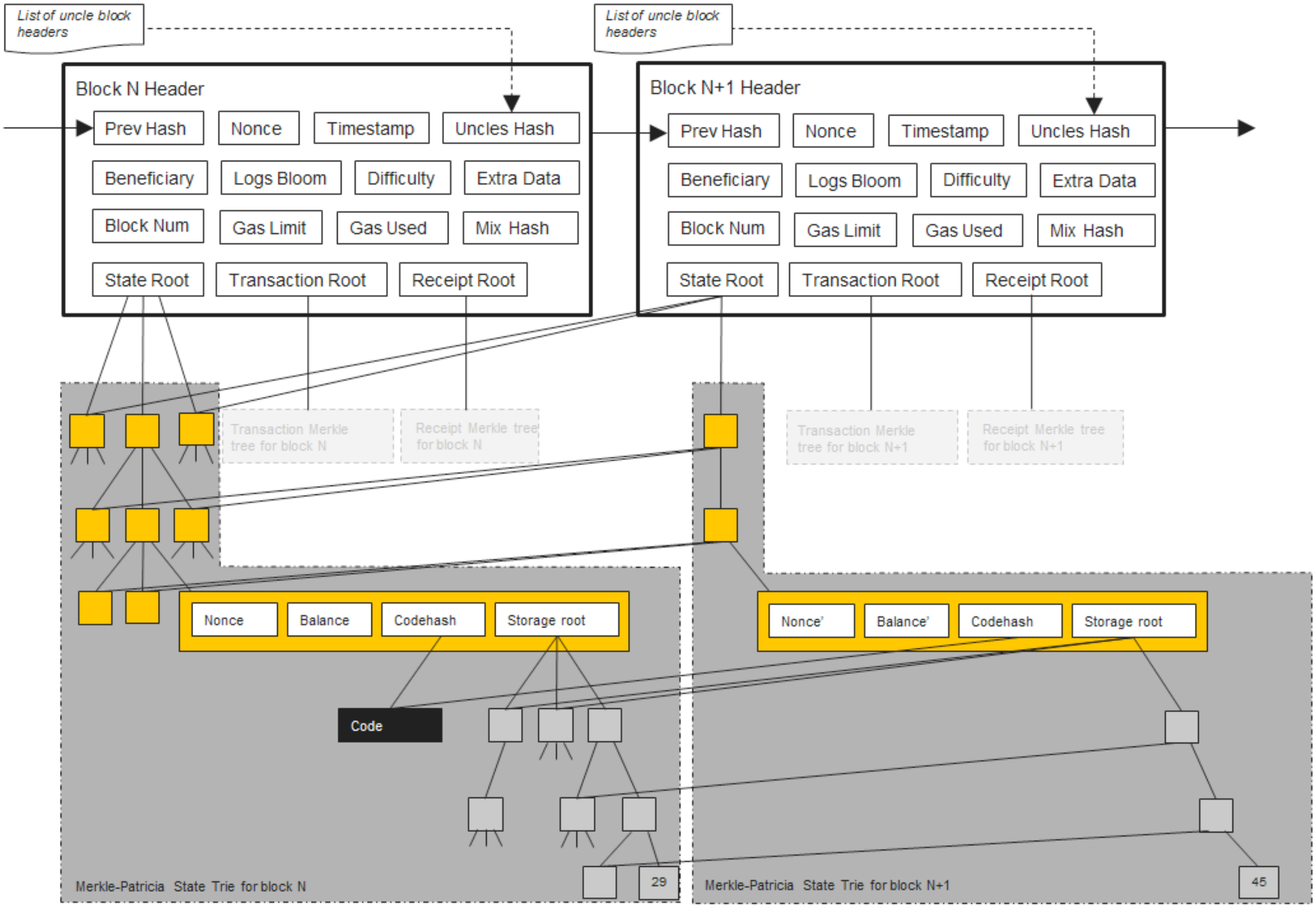
Network State

- State of all Ethereum accounts is the Ethereum network state
- State update occurs at every block
  - Going from one block to the next requires a miner who will lead the consensus mechanism
- Ethereum accounts interact via transactions



Ethereum Blockchain's main data structure is the MPT (Merkel-Patricia Tree)

Each account is designated by this 4-tuple: [account_nonce, ether_balance, code_hash, storage_root]



Updating the Ethereum blockchain

Ethereum Virtual Machine (EVM)

EVM

- EVM runs contract code
- EVM code = low-level stack-based bytecode language
- Every node in the Ethereum network runs EVM to verify blocks to be updated

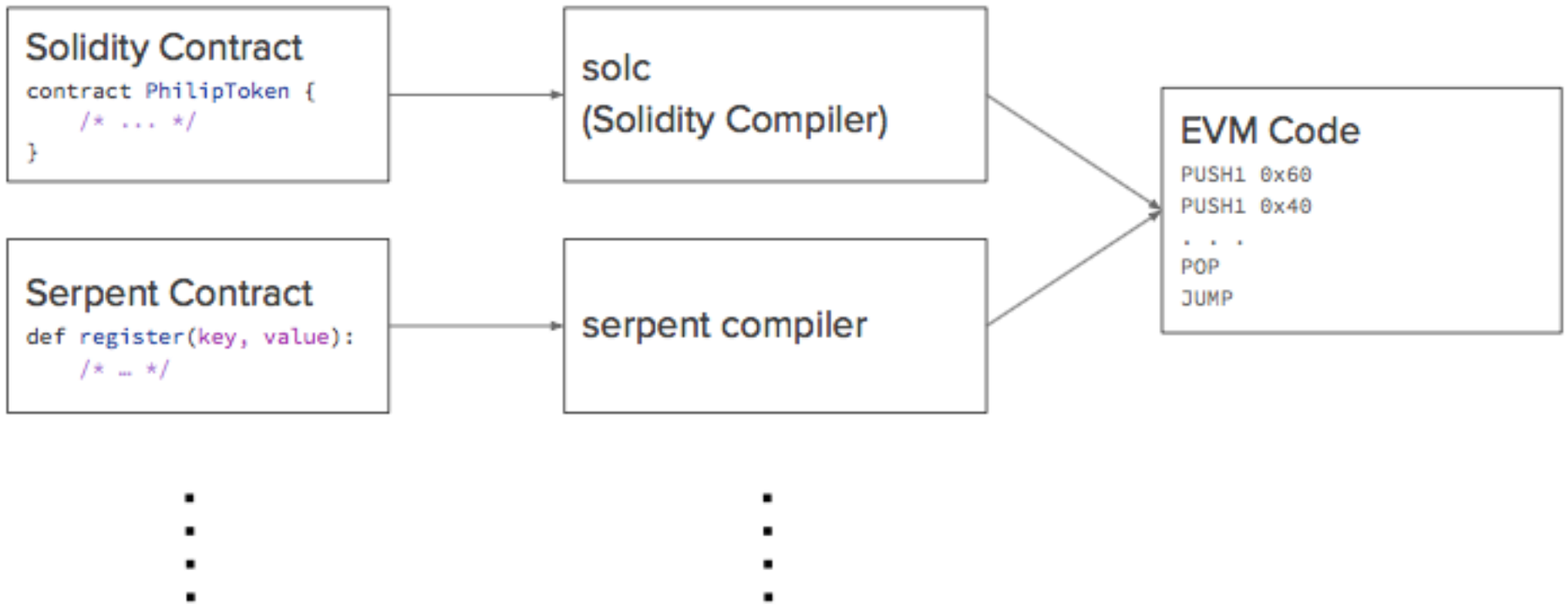
EVM Design Philosophy

- Simplicity - small number of low-level opcodes for ease of correctness and security proofs

- EVM assembly must be small and does not require a large amount of storage

- Deterministic execution; state transition can be predicted

EVM Code Compilation



Gas and Fee

What if contract code contains infinite loop? Could it generate DoS of the system?

```
function foo()
{
    while (true) {
        /* Loop forever! */
    }
}
```

Gas and Fee

- If we can tell whether some contract code will not terminate, this would be ideal
- But, we cannot as we cannot solve the Halting problem
- Ethereum's solution
  - For a contract to run, it needs some gas
  - Each transaction must specify startgas (max gas to utilize) and gasprice (fee in Ether the originator of the transaction is willing to pay)

Gas and Fee

- To execute a transaction, the amount of Ether = startgas * gasprice will be deducted from the account of the transaction sender
- If the transaction executes successfully, the remaining Ether will be returned to the sender
- If the transaction runs out of gas before it can execute successfully, the sender will loose all the Ether and gets nothing in return as if the transaction never gets executed

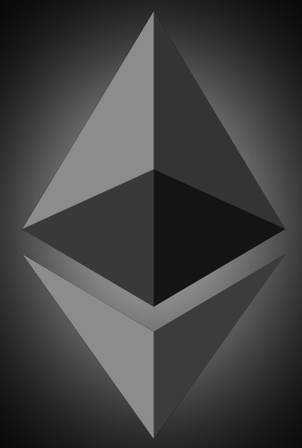
Gas and Fee Examples

- Addition or comparison = 1 gas
- Calculating SHA3 hash = 20 gas
- Write 256-bit word to some persistent storage =100 gas
- Before a transaction can start = 21,000 gas
- Gas per operation is constant
- However, gas price is not constant
  - Current Ether gas price:
    - https://etherscan.io/chart/gasprice

Running Smart Contracts

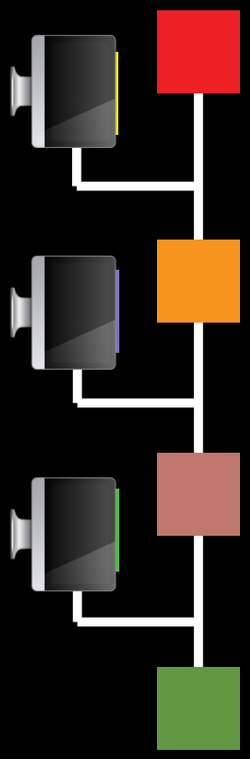
- Does not emphasize utmost efficiency like what cloud computing does
- Contracts run **redundantly in parallel** to achieve consensus of the network state without having a central authority to control

Different Ways to Run Smart Contracts



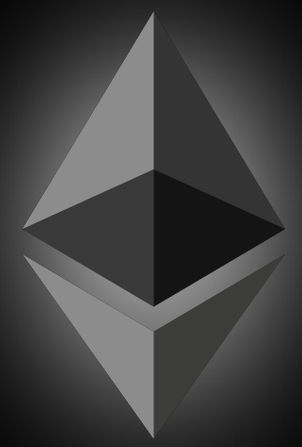
Ethereum

Transaction Structure



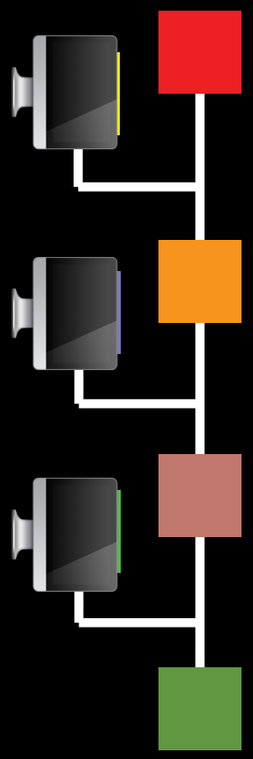
transactions

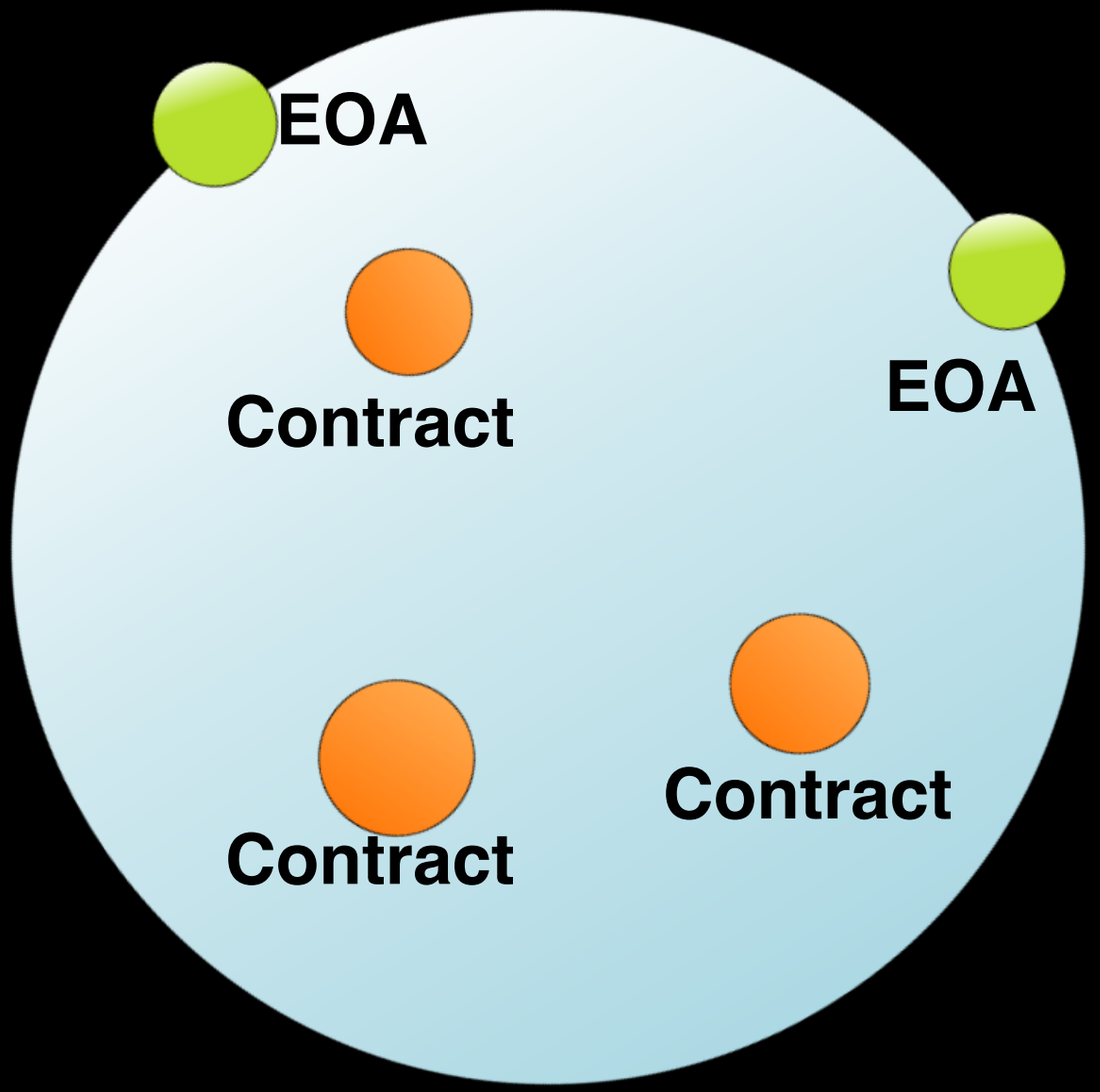
- from (address)
- to (address)
- gas price (per op)
- gas limit (for tx)
- value (sent ether)
- data (anything)
- signature

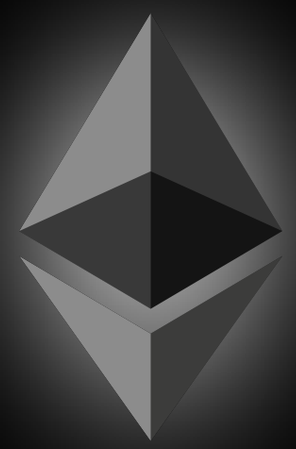


Ethereum

VM State: user accounts & contracts

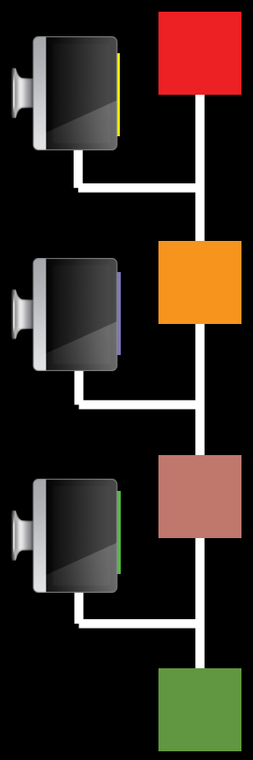


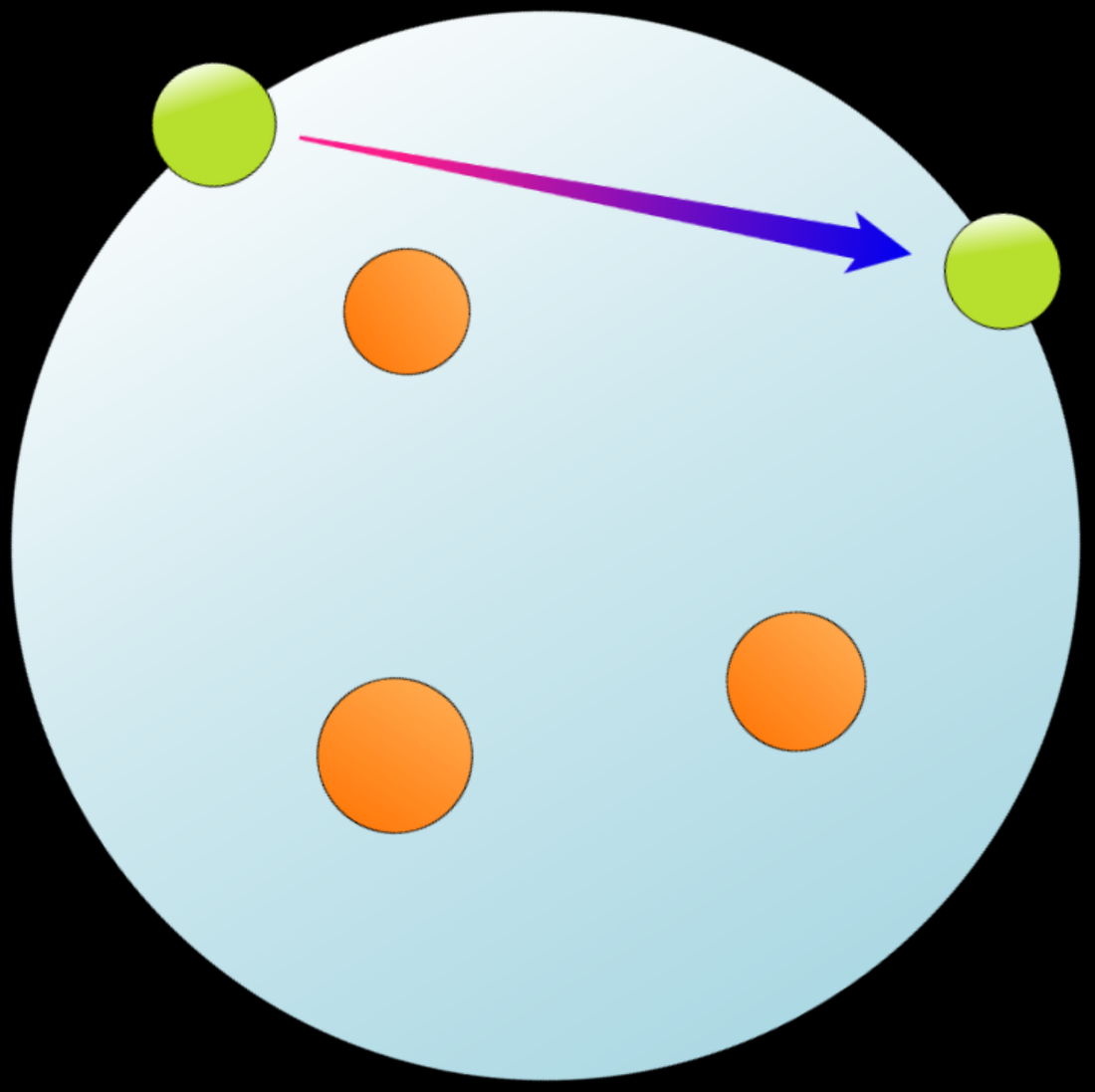


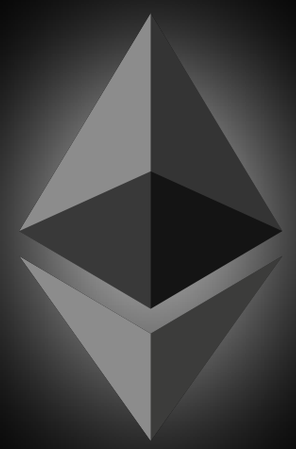


Ethereum

send ether between two accounts

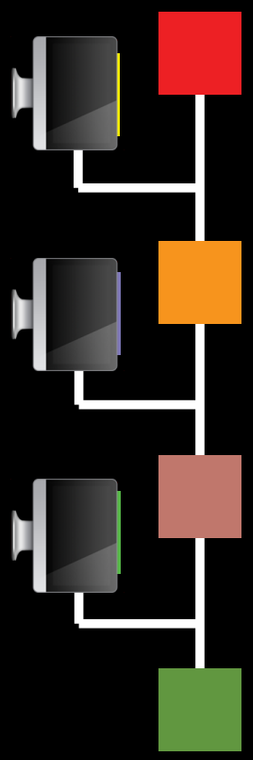


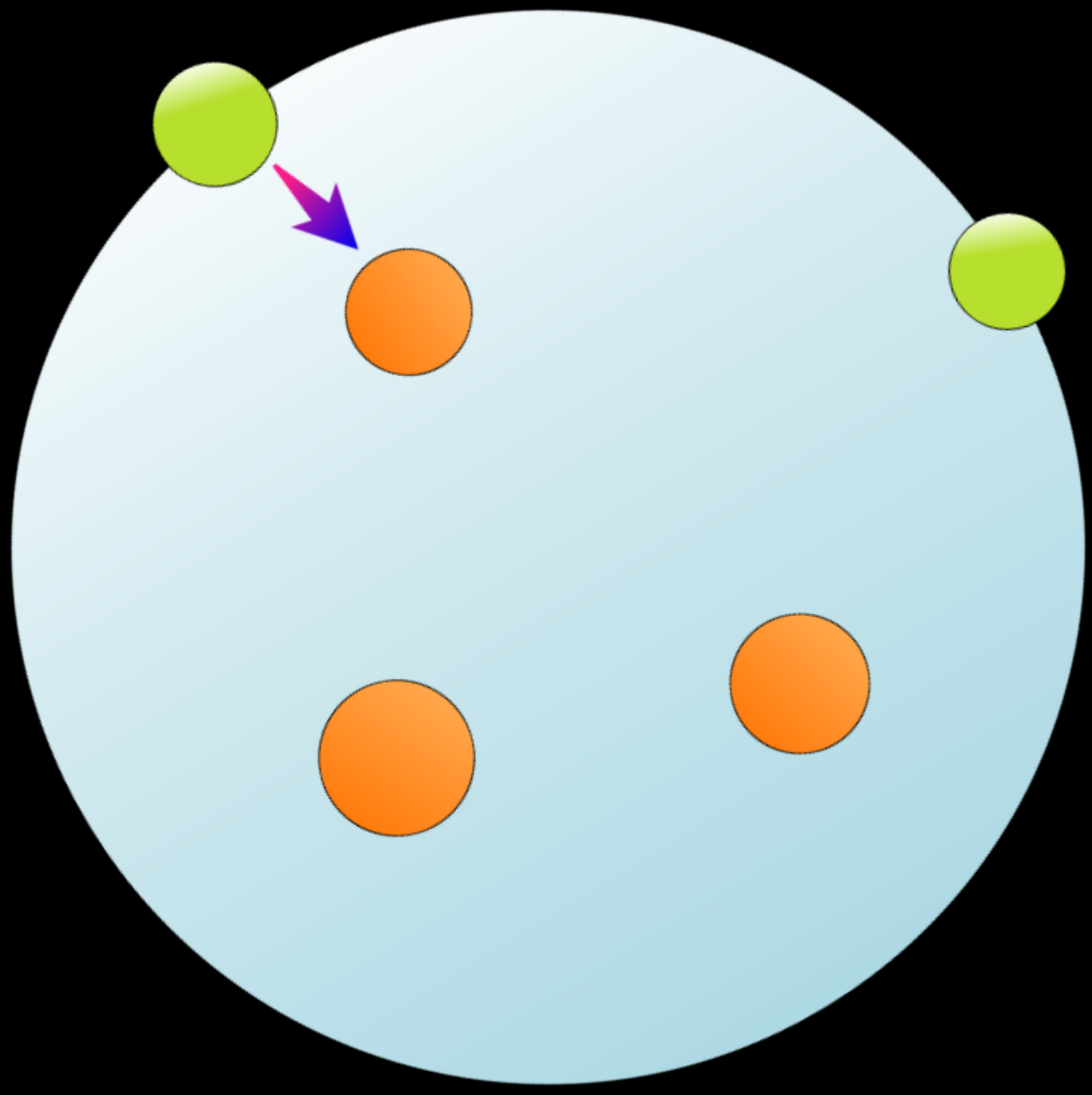


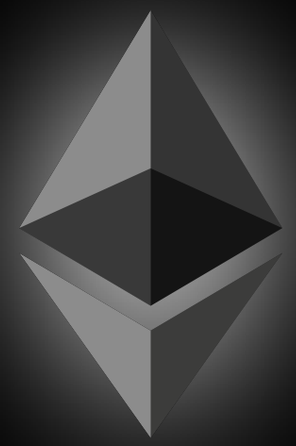


Ethereum

call method on a contract

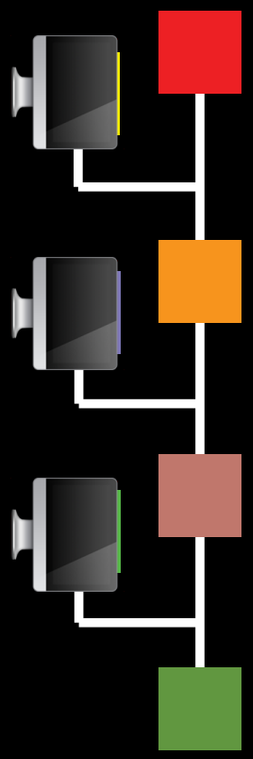


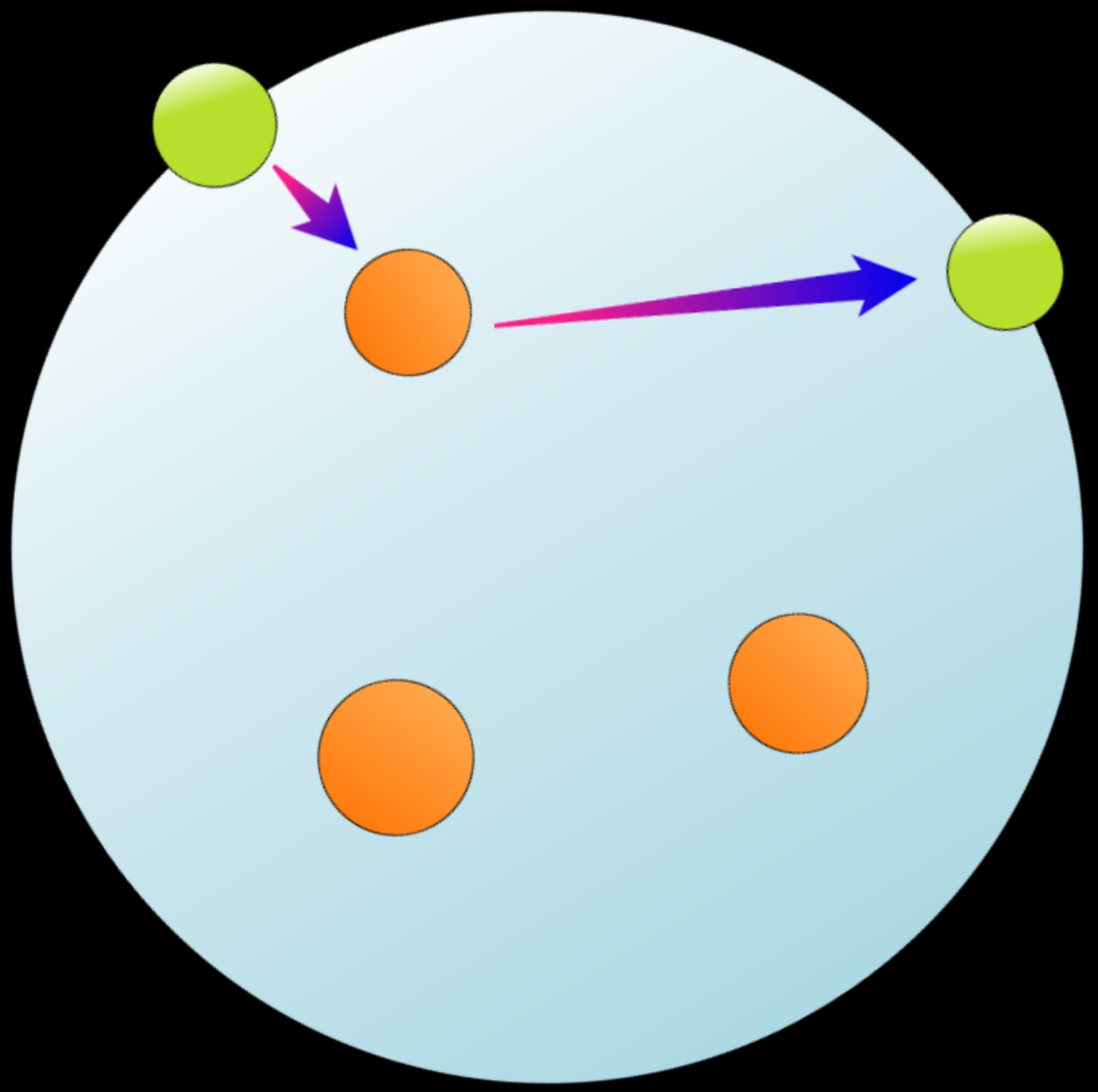


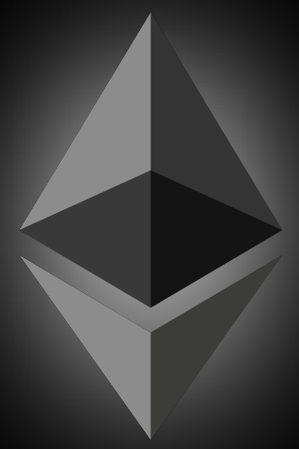


Ethereum

contract reacts to being called

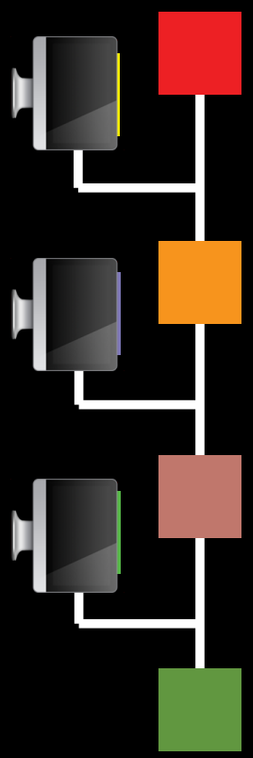


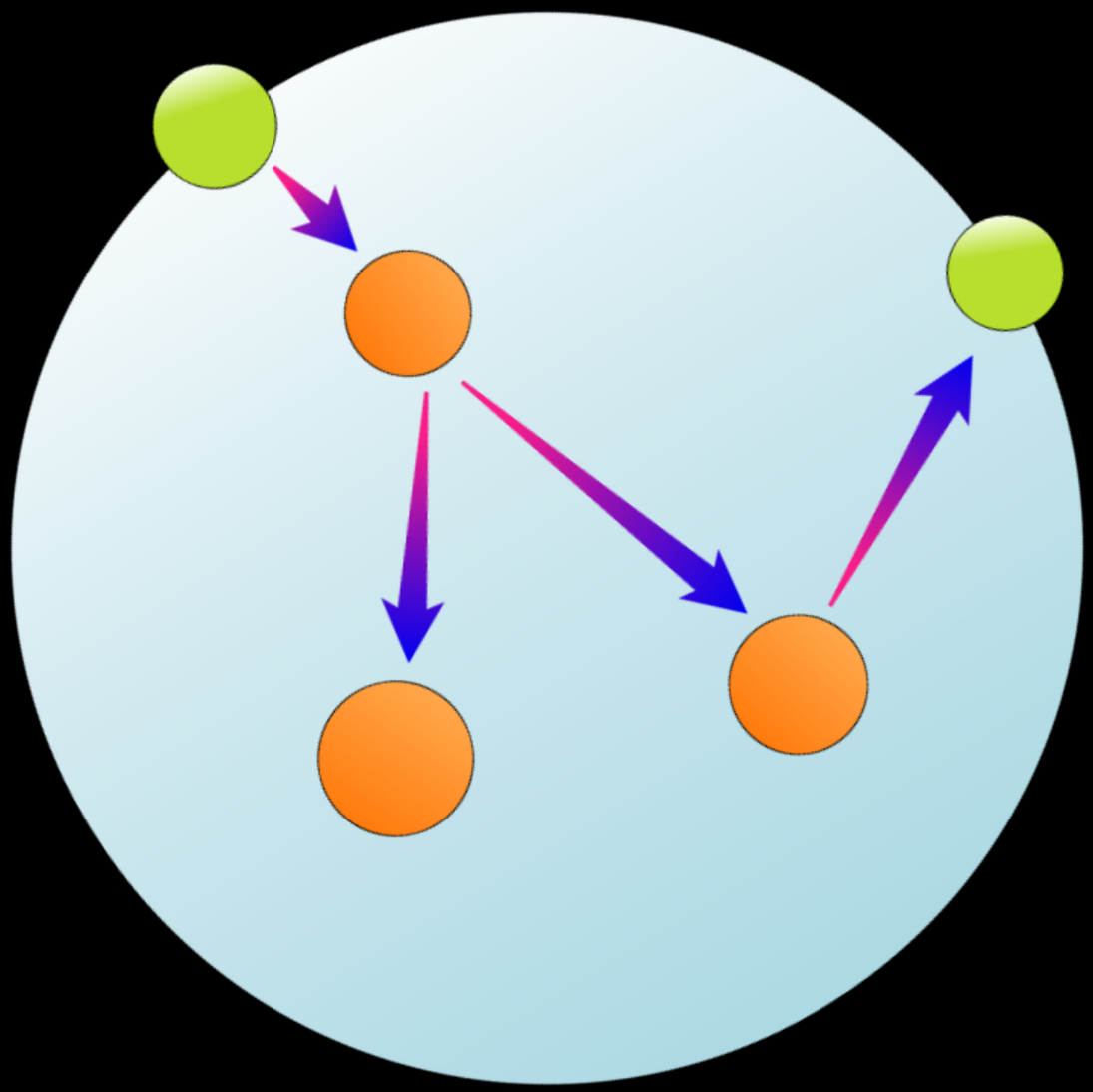


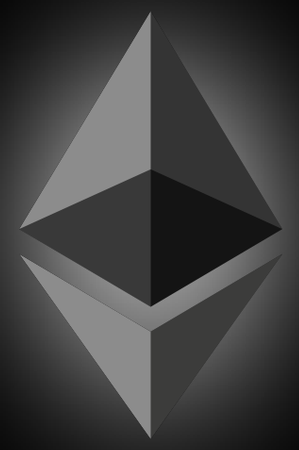


Ethereum

chain reactions

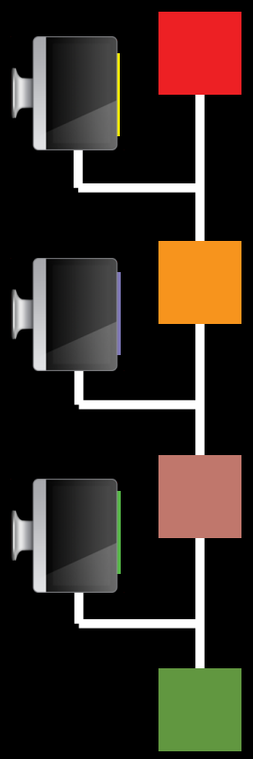


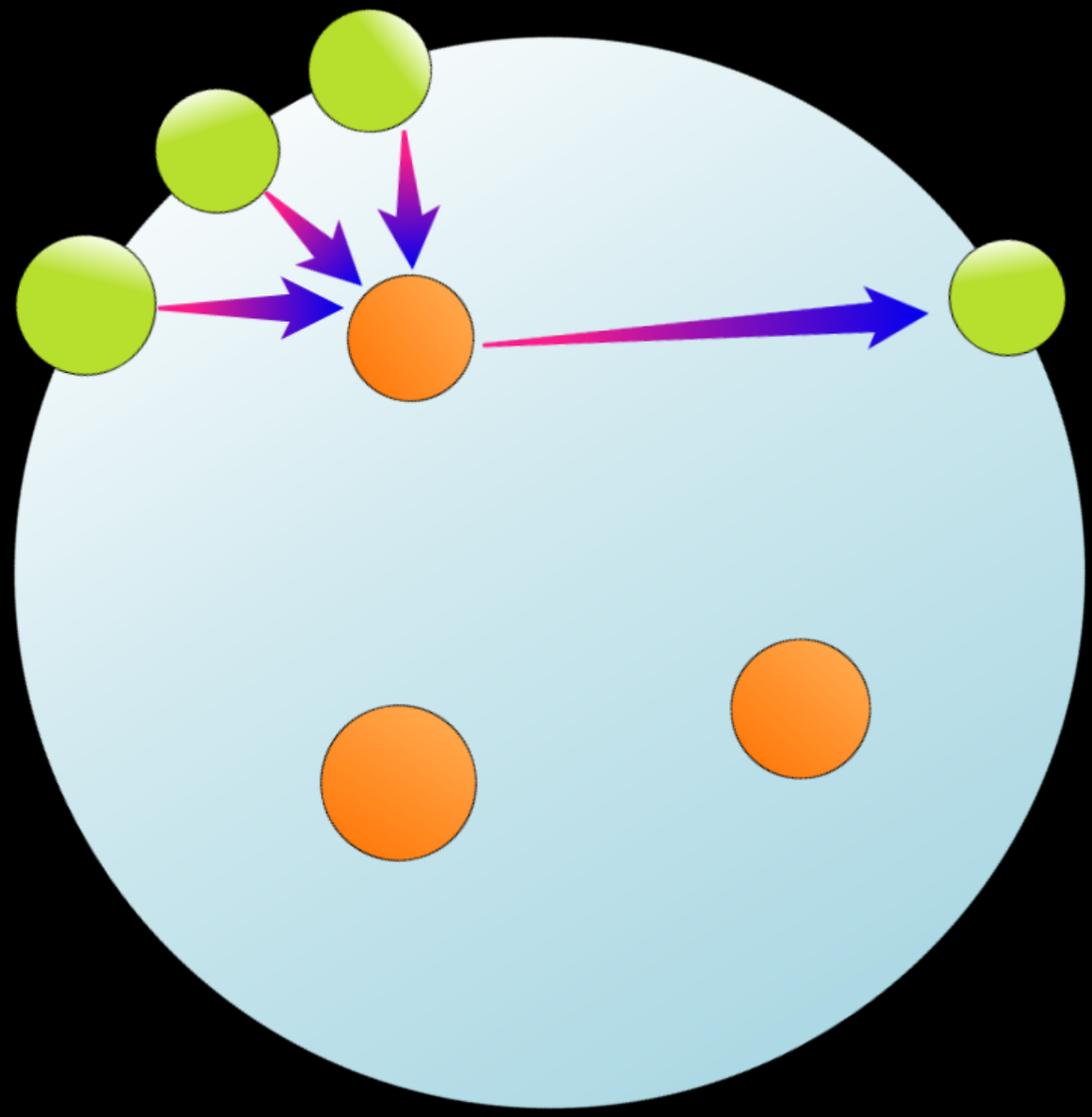


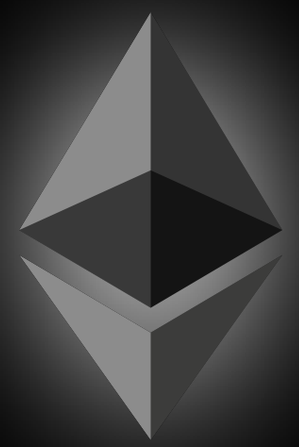


Ethereum

multi-sig via proxy contracts

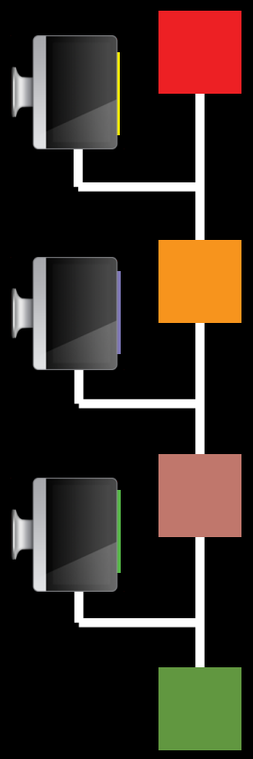


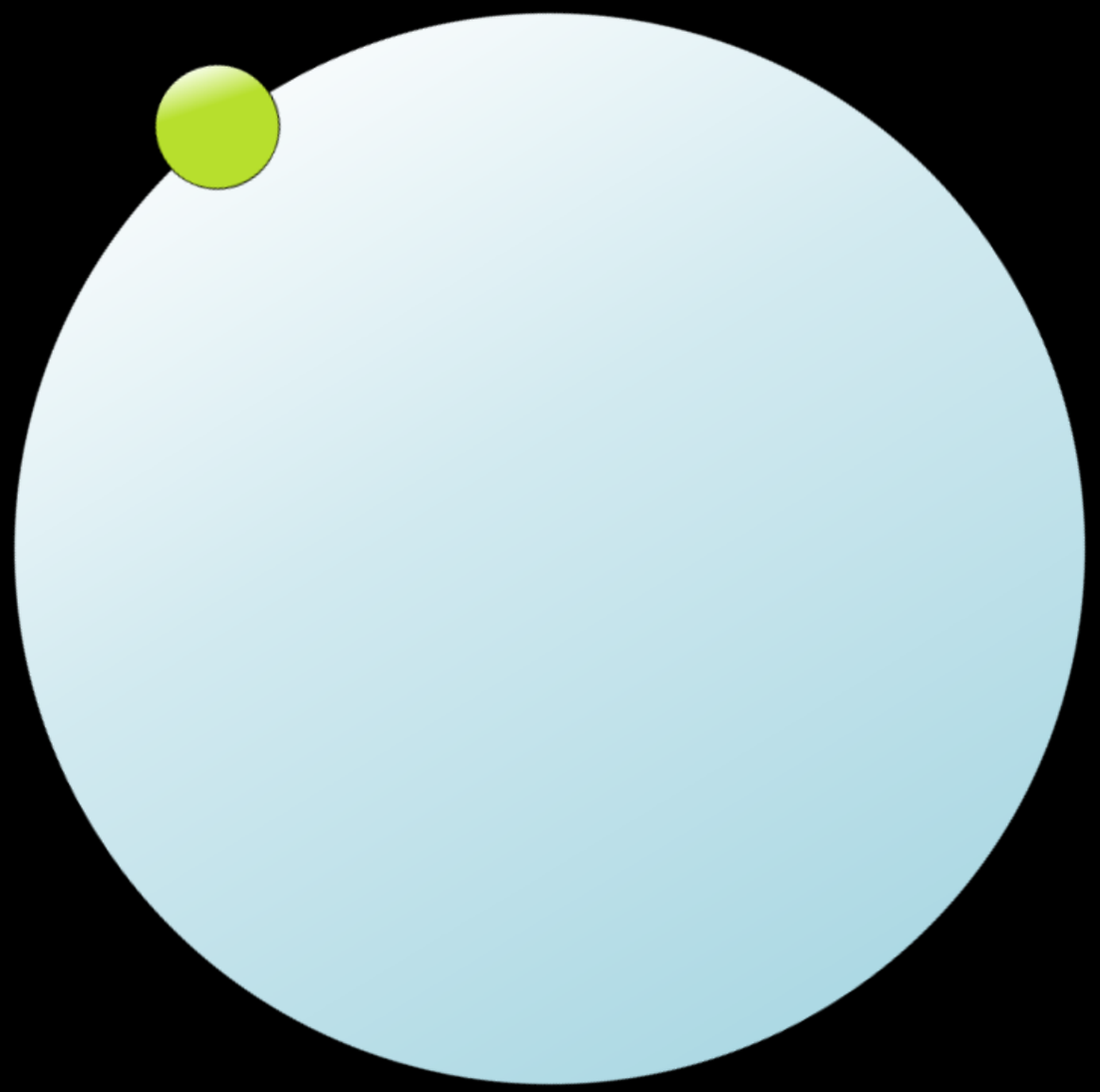


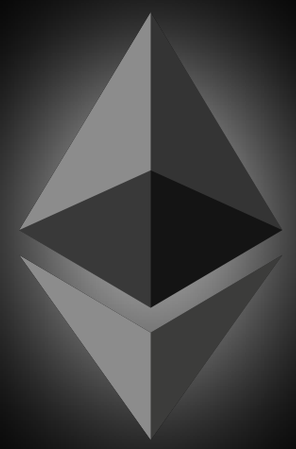


Ethereum

where do contracts come from?

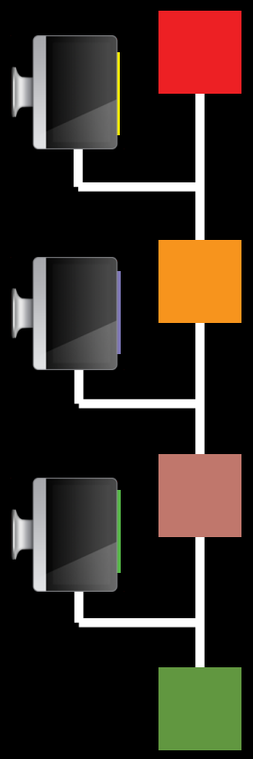


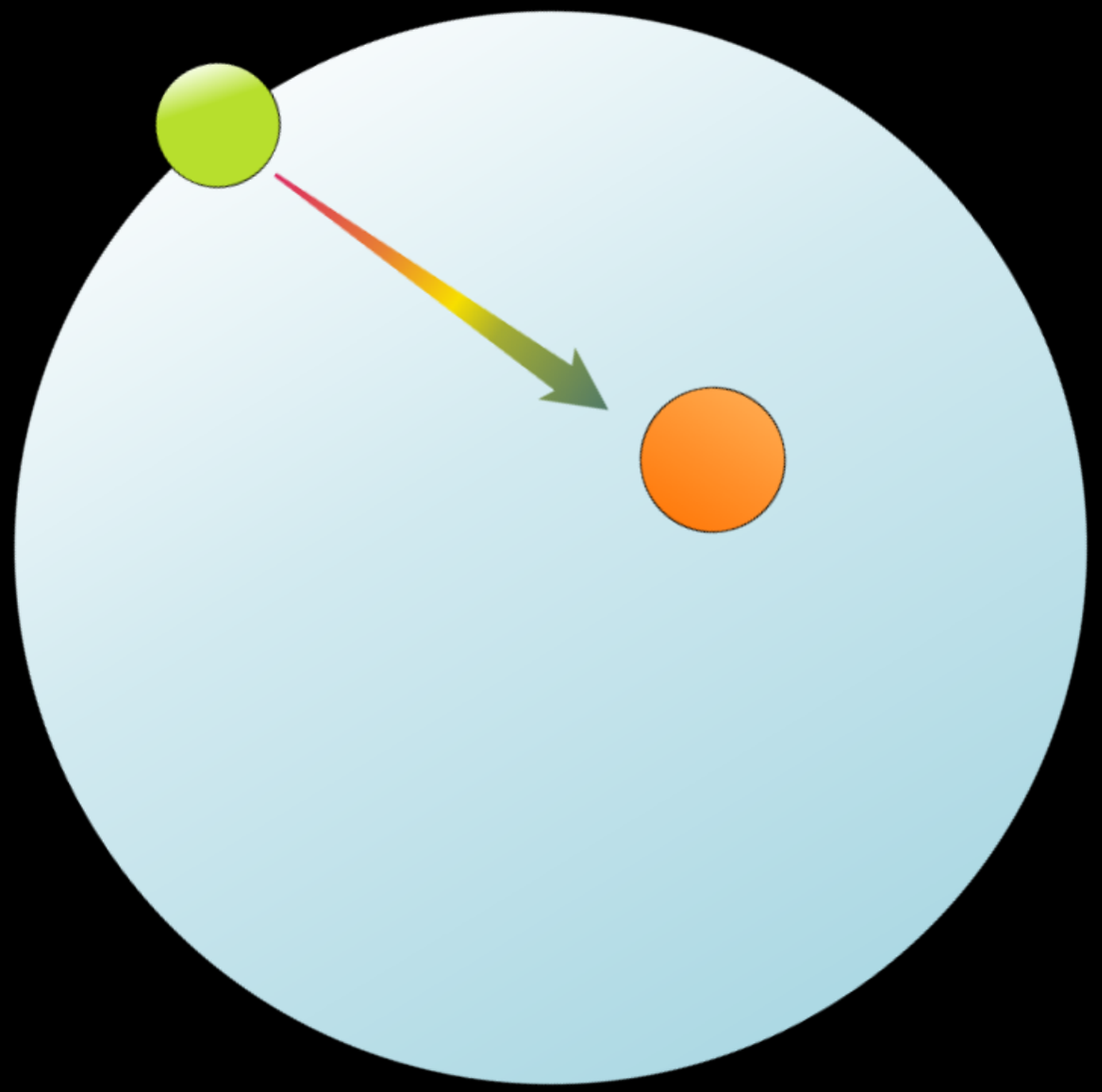




Ethereum

special tx (with empty ‘to’ field)
publishes data as executable





An Example Contract: Build Your Own Token (Currency)

```
contract PhilipToken {

    /* Maps account addresses to token balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply
       tokens to the creator of the contract */
    function PhilipToken(uint256 initialSupply)
    {
        // Give the creator all initial tokens
        balanceOf[msg.sender] = initialSupply;
    }

    /* Send tokens to a recipient address */
    function transfer(address to, uint256 value)
    {
        if (balanceOf[msg.sender] < value) throw;    // Check if the sender has enough
        balanceOf[msg.sender] -= value;              // Subtract from the sender
        balanceOf[to] += value;                      // Add the same to the recipient
    }
}
```

Top Ethereum Dapps

All | ETH | EOS | TRON | Ontology | ThunderCore | WAX | Steem | Hive | BORA

BSC | Polygon | Flow | NEAR NEW | Avalanche NEW | Telos NEW | Tezos NEW | Other

All Categories | Games | DeFi | Gambling | Exchanges | Collectibles | Marketplaces | Social | Other | High Risk

Only New Dapps

24H | 7D | 30D

		CATEGORY	PROTOCOL	BALANCE	USERS	VOLUME	ACTIVITY
1	Uniswap	Exchanges	ETH	$5.09B	462.16k -38.59%	$152.84B	
2	Uniswap V3	DeFi	ETH	$8.19	216.80k -24.26%	$10.70B	
3	Axie Infinity	Games	ETH	$47.37M	85.05k +238.24%	$143.84M	
4	SushiSwap	Exchanges	ETH	$3.51B	48.94k -10.64%	$9.90B	
5	1inch Network on Ethereum	DeFi	ETH	$3.83k	38.79k -33.82%	$1.87B	
6	OpenSea	Marketplaces	ETH	$27.70k	38.43k +72.06%	$142.61M	
7	OpenAlexa	High risk	ETH	$3.73k	30.68k +547.12%	$25.32M	

Dapps = smart contracts + front ends

Ethereum in Summary

- Decentralized platform for smart contracts
- Use blockchain to store smart contracts
- Nodes execute transactions to activate smart contract code that generate state changes
- A selected node leads the consensus to update the Ethereum blockchain

What We Have Learned

- Evolution of database technology
- Bitcoin blockchain
- Ethereum blockchain
- Smart contracts
- Blockchain as a distributed database with no central authorities to control it
- Bitcoin as an application that stores transactions on blockchain
- Ethereum as a platform that enables code execution where the code is stored on blockchain