APPS AND DAPPS: BLOCKCHAIN DEVELOPMENT FOR IOS

Mark Joselli
PUCPR
mark.joselli@pucpr.br

AGENDA

- Value of money
- Bitcoin
- Mining
- Advantages and disadvantages of blockchain
- Smart Contracts
- Ethereum
- Creation of Apps using Blockchain

OBJECTIVES

- Understand the technology
- Understand how to develop

MOTIVATIONS

- It is a new technology
- Lack of good applications

WHAT'S MONEY?

- Account -> value
- Way to exchange stuff -> acceptability
- Reservation of value -> not perishable

AND A DIGITAL CURRENCY?

- Money that only are exchangeable digitally
  - Facebook Gold, Digital Gold, Bitcoin…
- And also: Electronic Payment Authorization (Credit cards)

MONEY

"something generally accepted as a medium of exchange, a measure of value, or a means of payment"

TYPE OF MONEY

- Commodity Money: The **commodity itself** becomes the **money**. Examples of commodity money include **gold** coins, beads, shells, spices, etc.

- Fiat Money: **Fiat** money gets its value from a **government** order.

- Fiduciary Money: **Fiduciary** money depends for its value on the confidence that it will be generally accepted as a **medium of exchange** (checks, bank notes…)

FIRST TOKENS

- Way to exchange products:
  - 1 cow for 10kg of carrots;
- Firs coins of metal

ACCOUNTS

- Certified credits for the production;
- Banks as a way to trade;
- Goldsmiths: deposits and promissory notes

BEGIN OF THE MODERN MONEY

- Notes from private bank
  - Loan based on the money in account;
  - Begin of faction reserve
- Money from the government
  - Support from gold and silver

END OF GOLD STANDARD

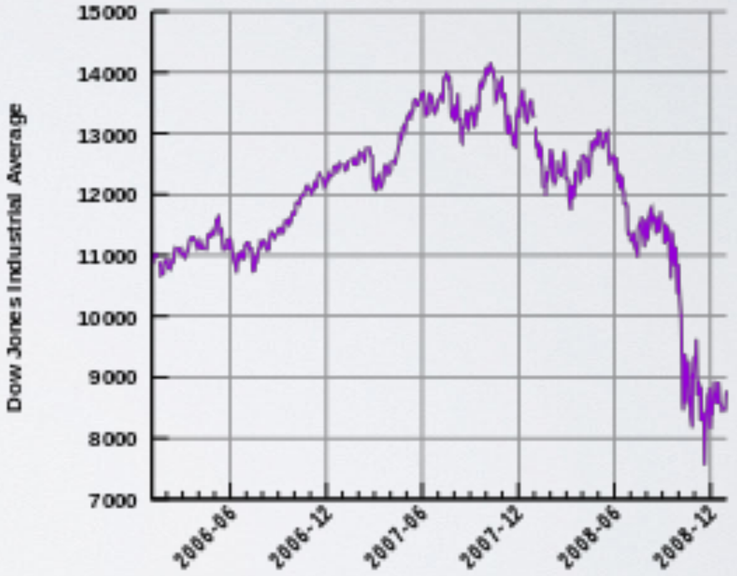
- Coins and notes are not reimbursed to gold;
- Exchange market
- Money by Government Decree
  - Supported by the ability to pay the debt
  - Can have inflation and disinflation.

Open Source Peer-to-Peer Money


INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
OCTOBER 31ST-NOVEMBER 6TH 2015
Economist.com
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

2008 CRASH

- It began in 2007 with a crisis in the **subprime** mortgage market;
- **Excessive risk-taking** by **banks** helped to magnify the financial impact globally;
- The **banks lost** the **money** from the **people** (deposits).
- Massive **bail-outs** of financial institutions by the **government** with **money** from the **people** (taxes).



BITCOIN CREATION

- 31/10/2008, a link to a paper authored by Satoshi Nakamoto titled Bitcoin: A Peer-to-Peer Electronic Cash System was posted to a cryptography mailing list.

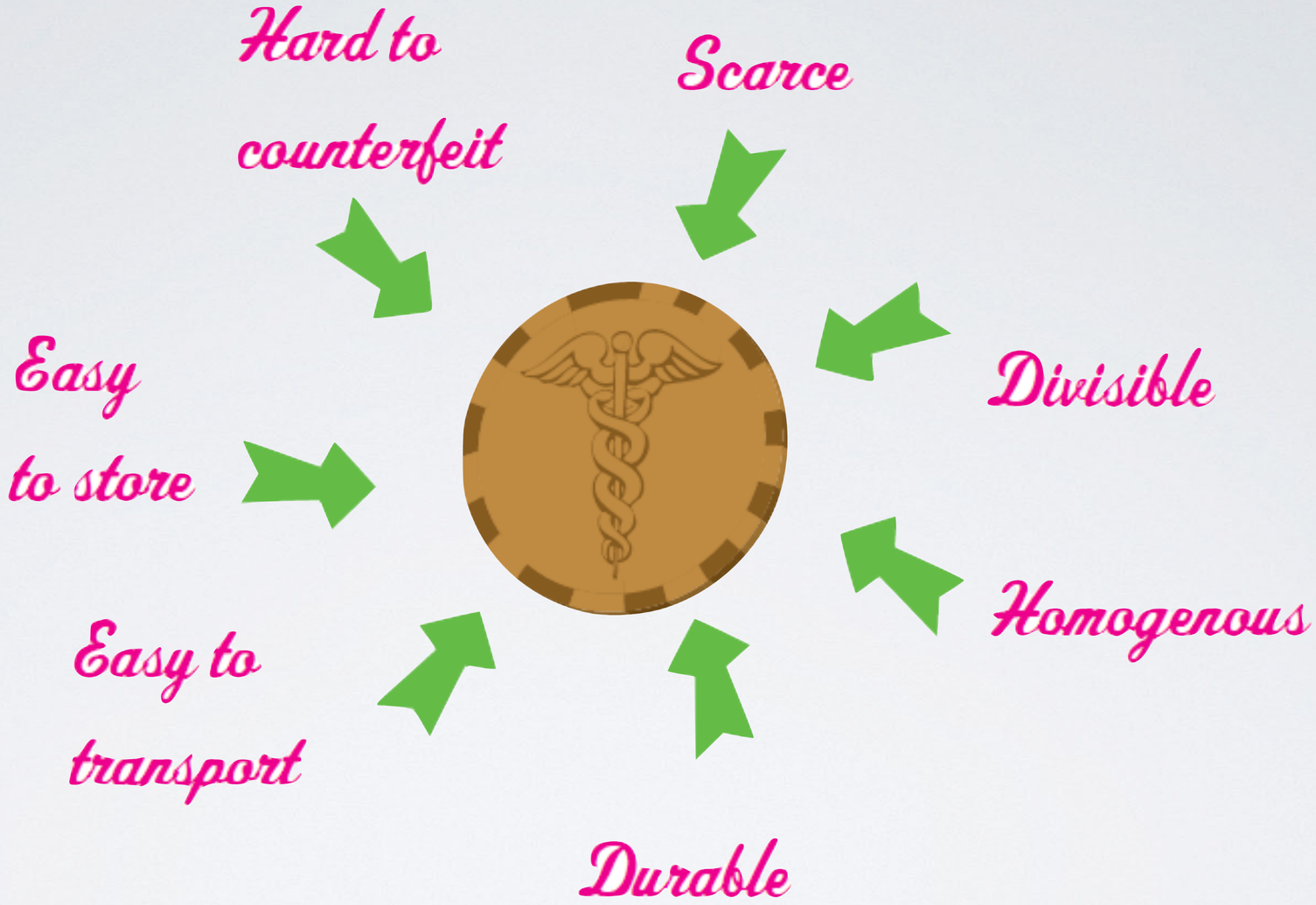
- 03/01/2009, the bitcoin network came into existence with Satoshi Nakamoto mining the genesis block of bitcoin (block number 0), with the text:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

BITCOIN

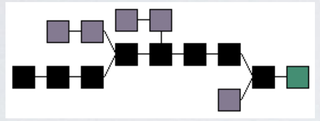
- Digital money
- A way to send and receive bitcoins to addresses
- An Open-source Decentralized Peer-to-peer (P2P) Payment Network
- The security is based on the decentralization and on cryptography

https://www.youtube.com/watch?v=Um63OQz3bjo


Hard to counterfeit
Scarce
Easy to store
Divisible
Homogenous
Easy to transport
Durable

GOOD MONEY

Blockchain



Protocol

Client

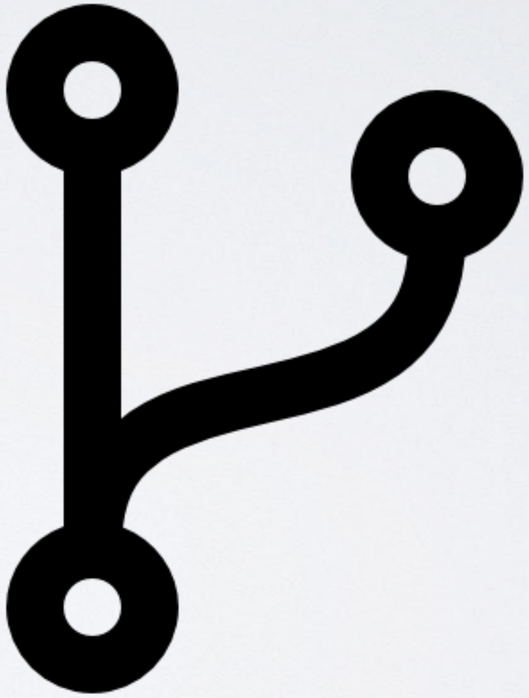
- Network open and decentralized
- Open-source
- Protocol transparent
- Public record of all transactions

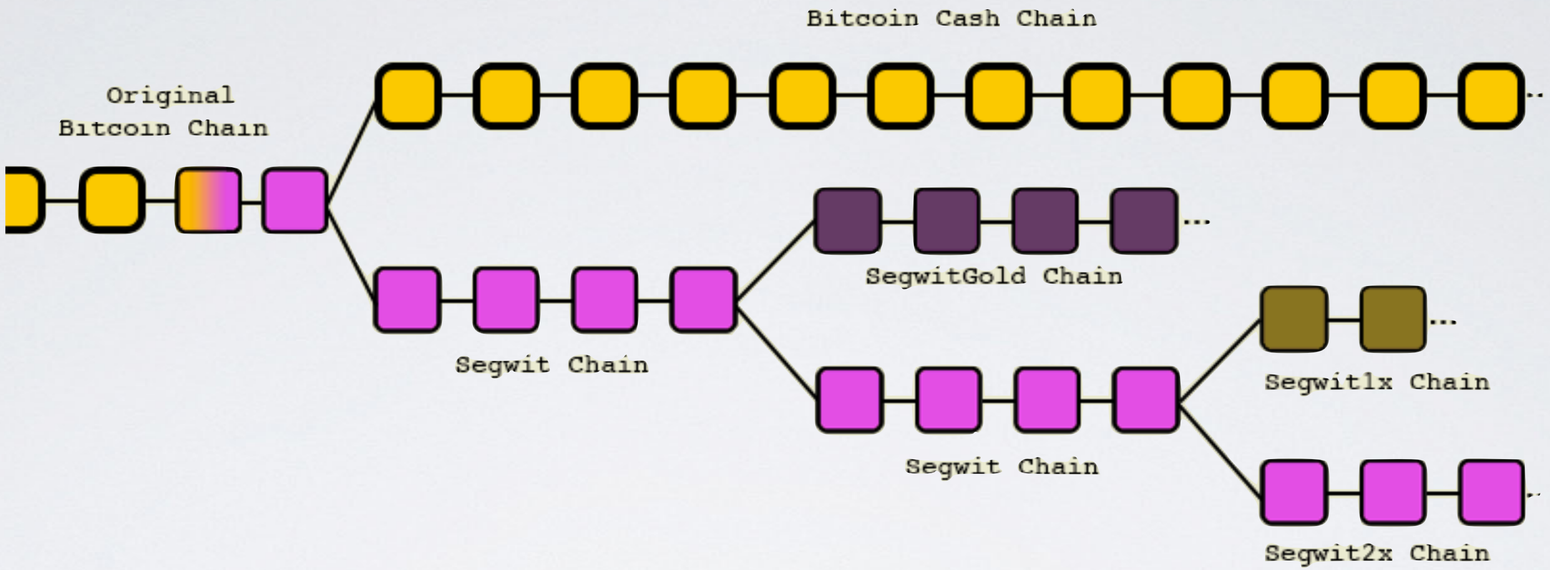
BITCOIN - GOVERNANCE

- An open source community of developers backed by the Bitcoin Foundation.

BITCOIN - DEMOCRATIC

- If someone don't like one of the changes,
- they can fork the chain and implement their own rules

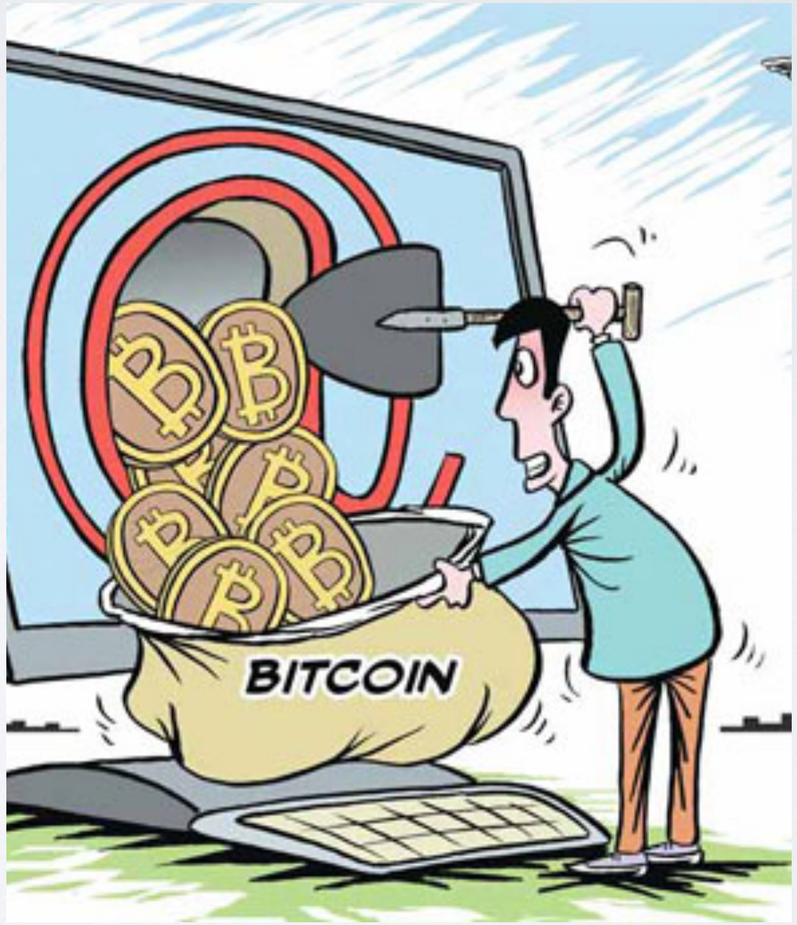




BITCOIN FORKS

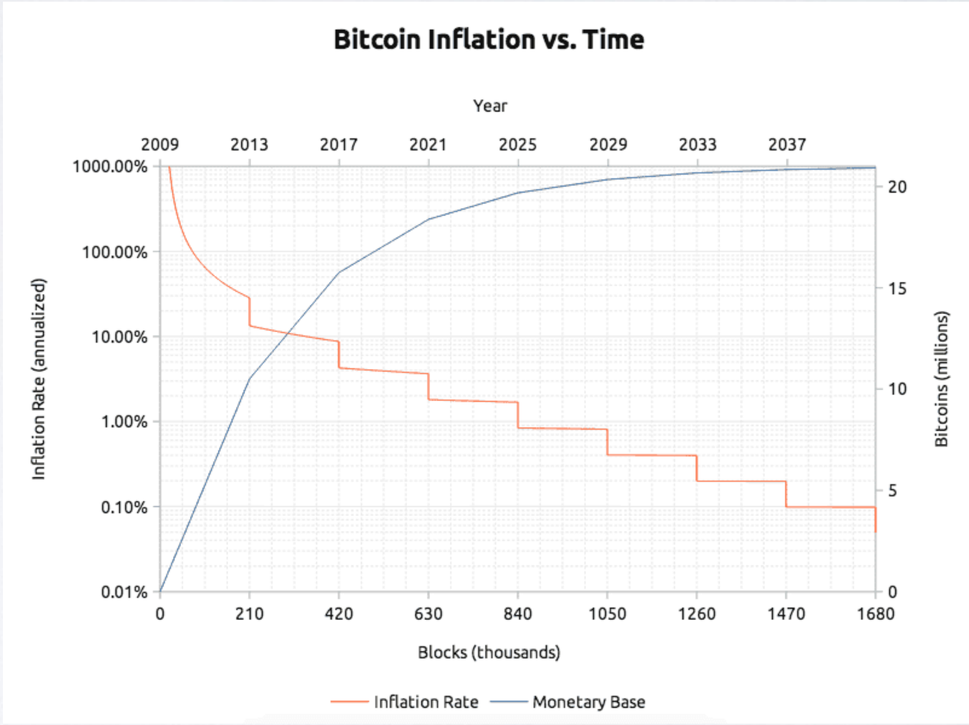
BITCOIN - CREATION

- The bitcoin was meant to be given to the people and not the banks;
- But nowadays are concentrated on few miners.



BITCOIN - DEFLATIONARY

- Deflationary by design - money supply cannot be manipulated
- It is fixed at 21 million coins, each divisible up to 8 decimal



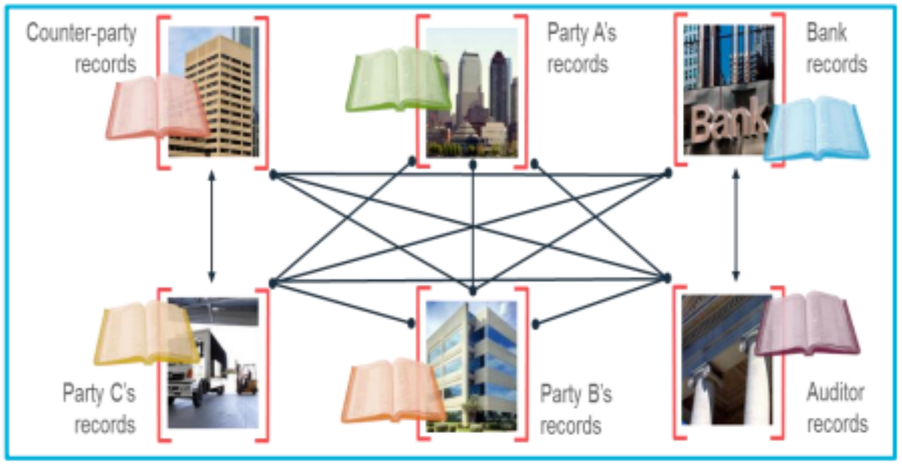
MONEY X BITCOIN

- Money in the past would like to be gold;
- Money nowadays has more value than gold, since it is more accepted.
- Any kind of money has its value based on thrust that they can trade it latter.

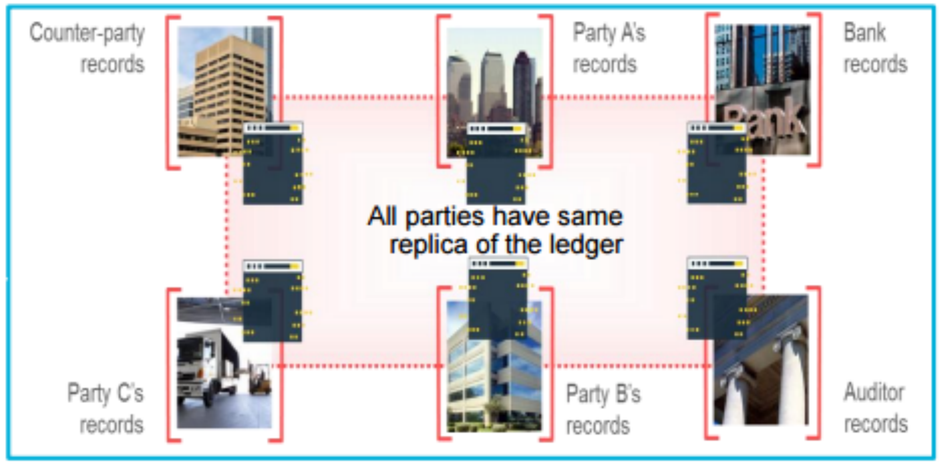
What's the difference with Blockchain?

What?

Without Blockchain



With Blockchain



Inefficient, expensive, vulnerable

Consensus, provenance, immutability, finality

6

outthink your limits

HOW DOES IT WORKS?

- The block chain is the fundamental data structure of the Bitcoin protocol.
- It is a single data structure (like a table or hash map) where participants validade and synchronize.
- This allows them to know who owns what.
- Anyone can change it by send bitcoins to someone else.
- Other users (miners) mathematically check the transaction to ensure its validity.

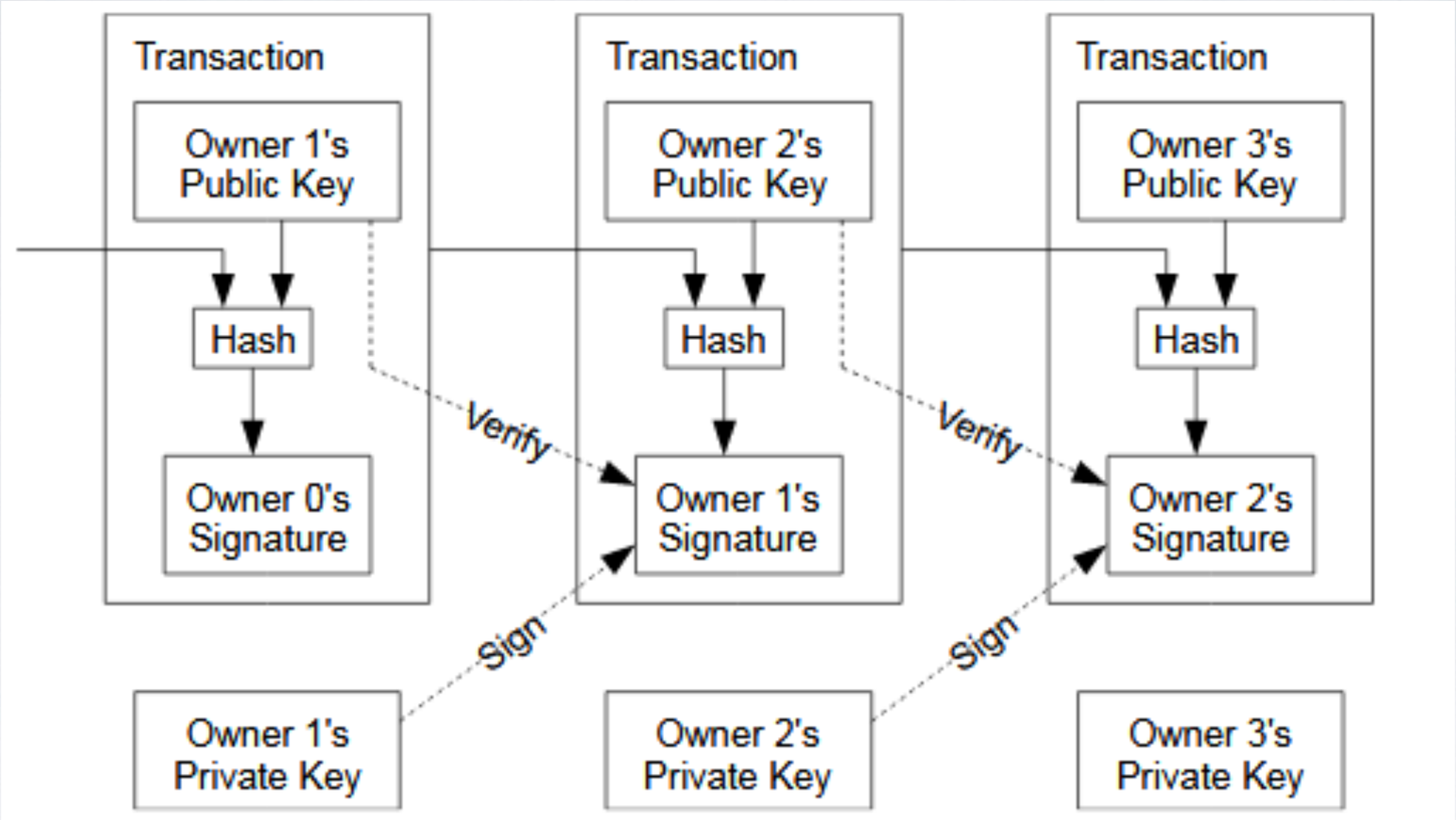
- It's essentially an accounting ledger:

  1. 5/10/18 Mark found : $15.00 (Mining)
  2. 5/10/18 Mark -> Fabio : $10.00
  3. 5/10/18 Maicris -> Mark : $4.00

- How much money does Mark have in his wallet?
  - Mark had $15, then gave $10 to Fabio, then received $4 from Maicris. Mark has $9 (15-10+4) now.

DOUBLE SPEND

- Bitcoin solves the so-called "double spending problem" with digital products.
- For example, if I have an mp3 file or an e-book on my computer, I can copy this file thousands of times freely and upload it to thousands of different people.
- For a digital currency, the possibility of unlimited copying would mean a rapid hyper-inflationary death.
- Bitcoin solves this by maintaining a P2P network and recording each transaction in a single blockchain call.
- If I send 1 bitcoin from my bitcoin address to my friend John. The bitcoins network registers this transaction in the block chain and I no longer have possession of that bitcoin.
- The coin "changed" from my bitcoins portfolio to John's wallet



TRANSACTIONS IN ACTION

MINING

MINING

- Miners collect the transactions in the network in large sets called blocks
  - Ex: "Alice pays Karim 10 bitcoins" and "Liam pays Sofia 8.3 bitcoins".
- These blocks are tied together in a continuous, authoritative record called blockchain,
  - which does not allow any conflicting transactions.
- And it lets you know with absolute certainty which transactions are reliable (No Double Spending!).

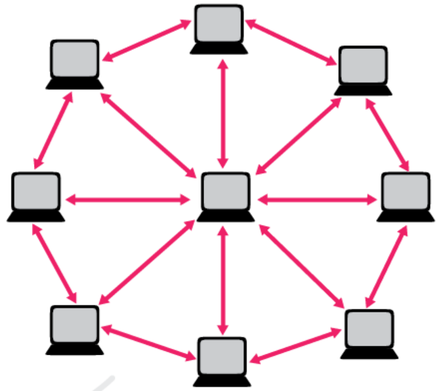
HASHING

- To understand mining, you need to understand what a hash function is.
- Simply put, a hash function gets an input and creates an apparently random output,
- but the output is consistent every time you run the function on a particular input,
- and it is very difficult to determine an input, considering only the output.

MINING STEPS

1. Collects network transactions
2. Validate them (not allowing conflicted transactions)
3. Put them in larger blocks
4. Computes cryptographic hashes until you find a hash "good enough to count"
5. Then sends the block to the network, adding it to the blockchain and gaining a reward in return

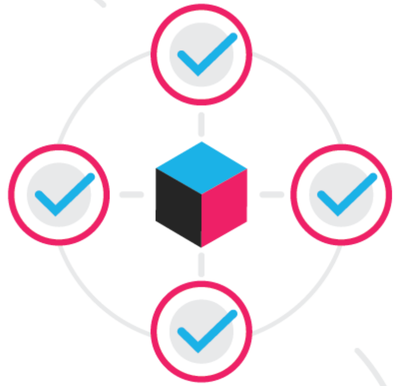
Someone requests a transaction.



The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**

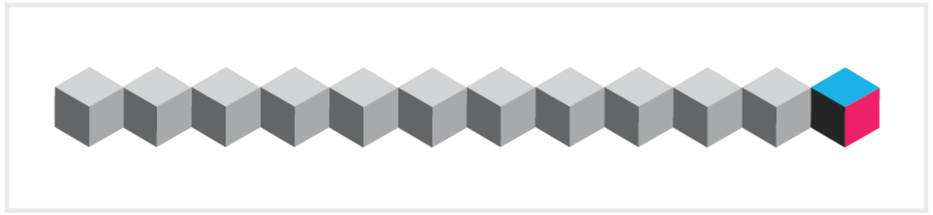
Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**



A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

cryptocurrency



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

The transaction is complete.

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

Has no intrinsic value in that is not redeemable for another commodity such as gold.

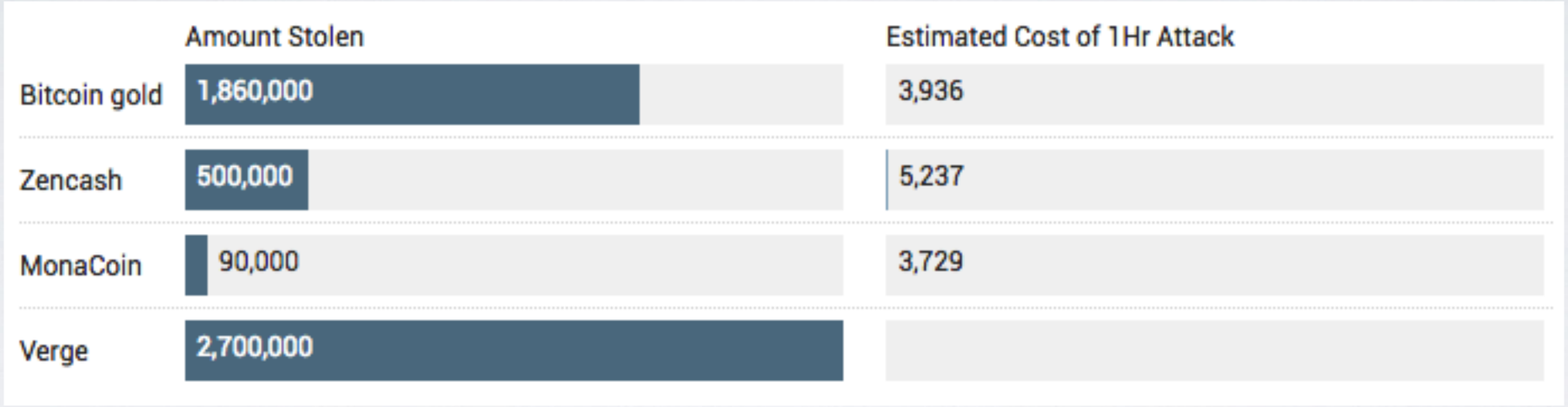
Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

51% ATTACK

- An attacker with> 50% power can hash
  - spend double: reverse transactions that it sends while it's in control
  - Prevent some or all transactions from gaining any confirmations
  - Prevent some or all other generators from getting any generations
  - https://www.crypto51.app/

SUCCESSFUL 51% ATTACKS

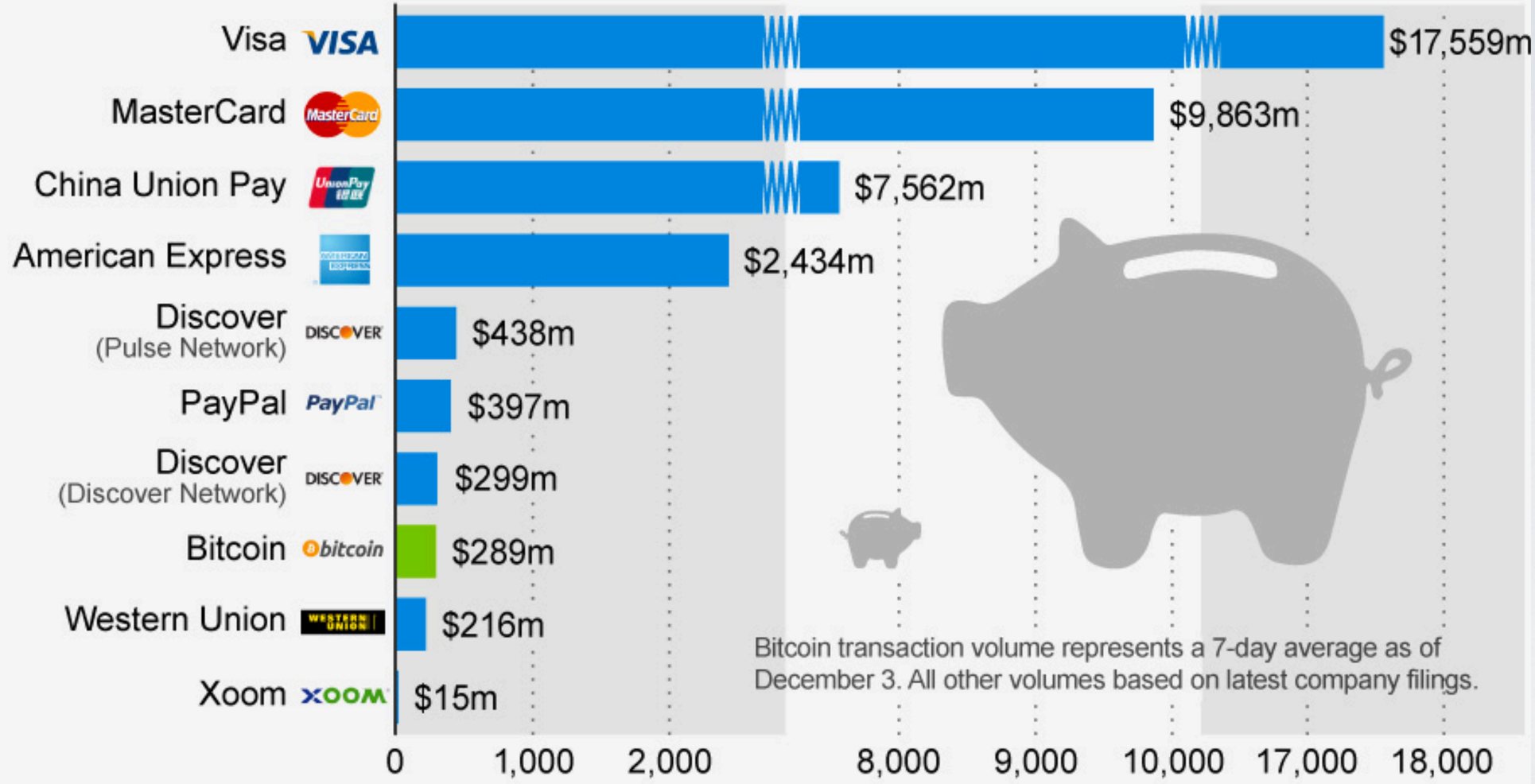


WHY BITCOIN

- Bitcoin can be used to buy goods anonymously (not anymore).
- Bitcoin is not bound by any country or subject to regulation.
- Advantages for small businesses because at Bitcoin there are no credit card fees or chargebacks (but have fees and long confirmation time).
- Some people buy bitcoins as an investment, hoping they will increase their value. This is one of the reasons for price instability
- Cases of value when in a hyper inflated economy.

How Bitcoin Activity Stacks Up Against Other Payment Networks

Average daily transaction volume of selected payment networks (in million U.S. dollars)

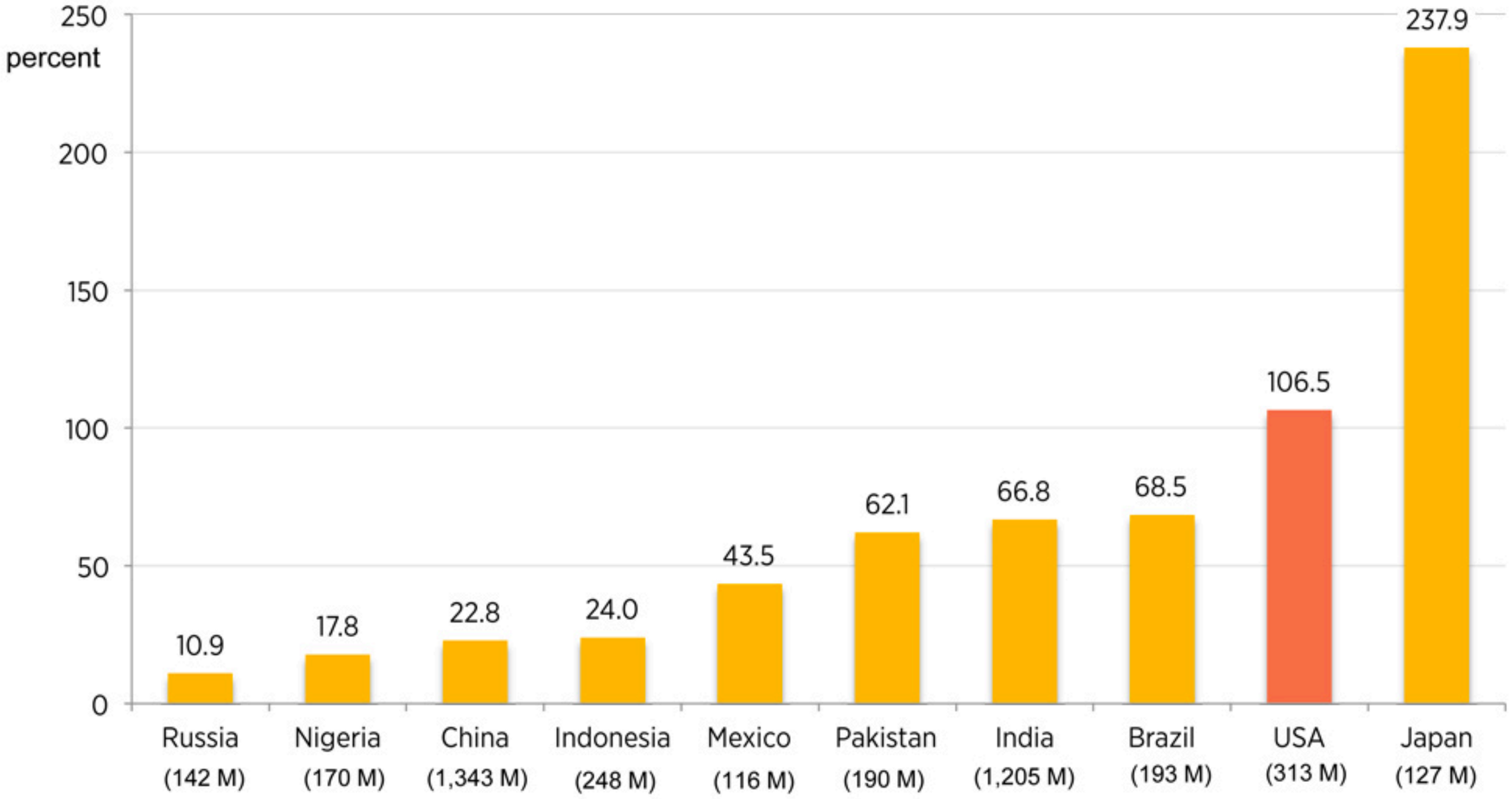


statista The Statistics Portal

@StatistaCharts

Source: Coinometrics

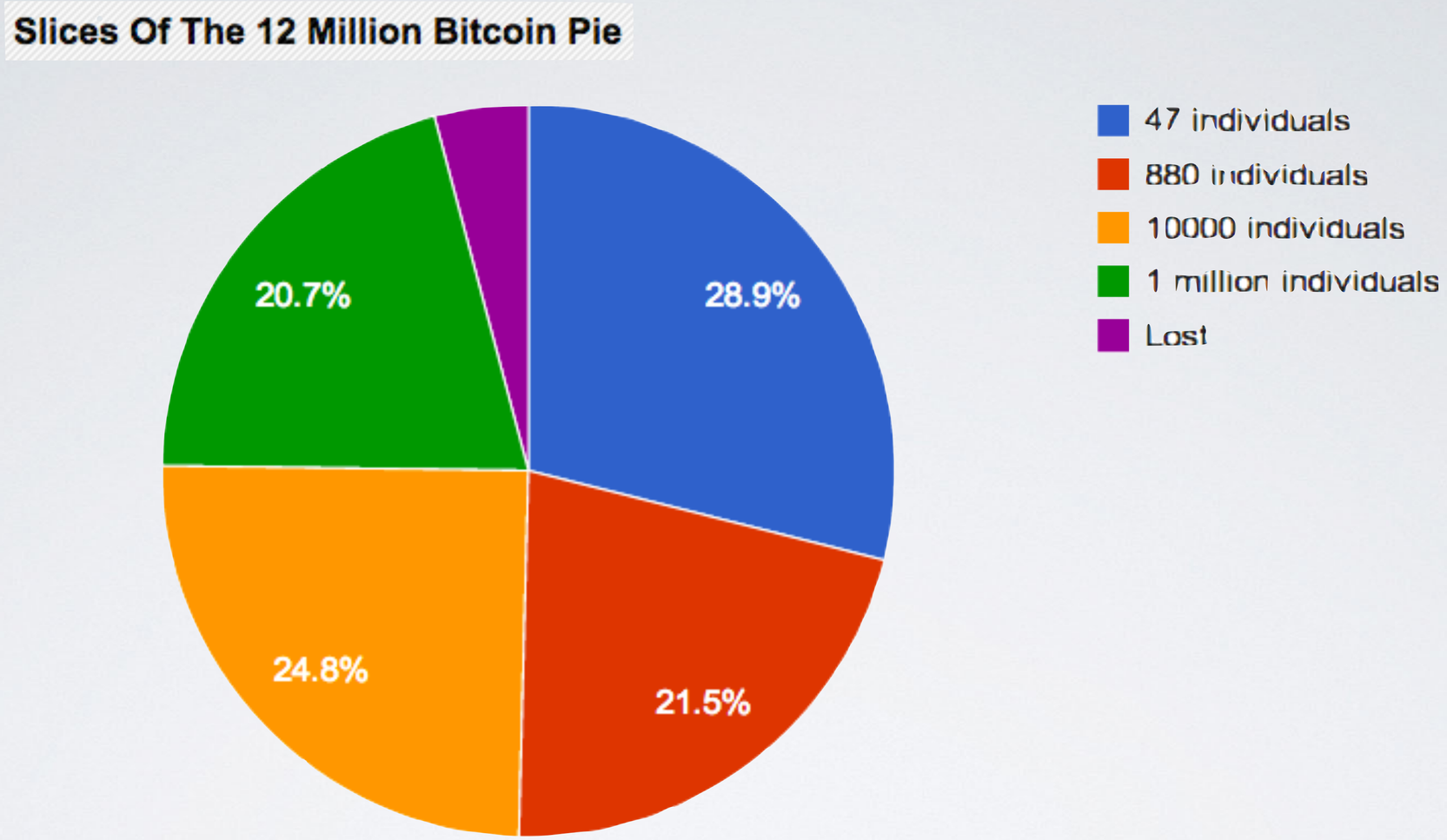
Debt-to-GDP of Most Populous Countries



Source: International Monetary Fund.
Data note: Data for Bangladesh (8th most populous country) unavailable.
Produced by Veronique de Rugy, Mercatus Center at George Mason University.

WHY NOT BITCOIN

- Portfolio Vulnerable to Robbery and Hacks
- No regulation (yet)
- Bitcoins are concentrate in the hand of a few
- Market manipulations
- Energy consumption
- Tulip mania



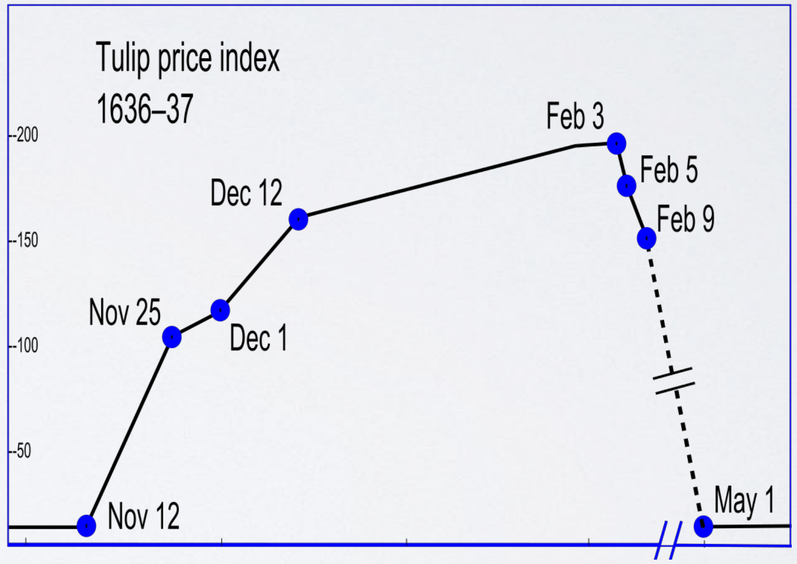
50% OF ALL BITCOINS ARE CONCENTRATED IN 1000 PERSONS

ENERGY CONSUMPTION

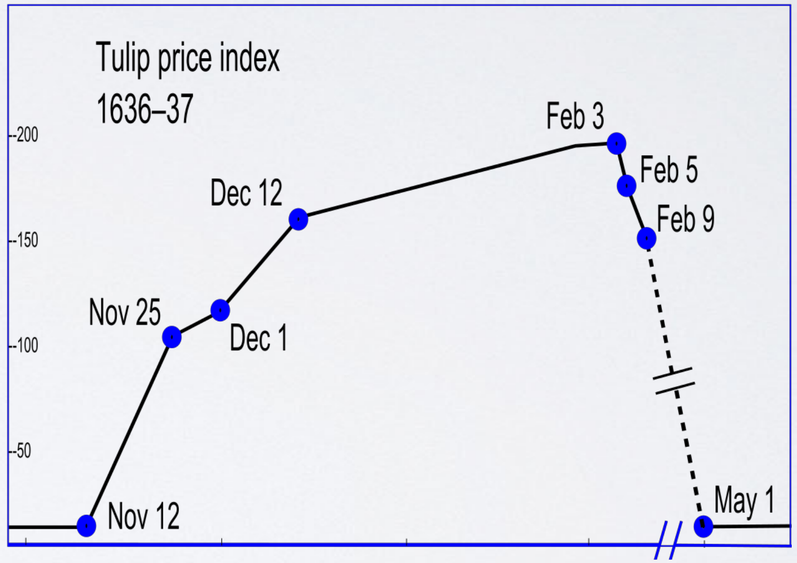
- An area of heavy criticism has to do with the vast amount of energy needed to process and store transactions, especially as the use of blockchain technology increases
- Miners in Bitcoin's blockchain network are seeking 450 billion trillion solutions per second in efforts to validate transactions by using substantial amounts of computer power
- Resources wasted: Mining with Bitcoin wastes enormous amounts of energy ($ 15 million / day - Same as Austria)

TULIP MANIA

- Tulip mania was a period in which contract prices for some bulbs of tulips reached extraordinarily high levels
- and then dramatically collapsed in February 1637.
- It is generally considered the first recorded speculative bubble.



- Bitcoin > 300% in less than 40 days (from $5,500 to $19,900)
- Then back to price in 50 days.



TOKENS

- A wider use is supported by the digital infrastructure introduced by Bitcoin, they are represented by "tokens".
- A "token" can be defined as a "scarce digital asset based on the underlying technology inspired by Bitcoin."
- Tokens can use similar code bases, but different blockchain databases.
- The Ethereum was inspired by Bitcoin, but has its own blockchain and was designed to be more programmable. Tokens can be issued at the top of the blockchain Ethereum.
- Token buyers are buying private keys, which are similar to the API keys, but can be transferred to other parties without the consent.

3 LEVELS OF BLOCKCHAIN

1. Storage for digital records
2. Exchanging digital assets (called tokens)
3. Running Smart Contracts

- Basic rules - Terms and conditions registered in the code
- Distributed network performs contract and monitors compliance
- Results are automatically validated without third parties

SMART CONTRACTS

- Consensus protocols are critical to determining the sequence of actions resulting from the contract code.
- This allows you to negotiate everything using peer-to-peer, from renewable energy to automated reservations of hotel rooms.

WHAT ARE SMART CONTRACTS?

- They are computer protocols that facilitate, verify or reinforce the negotiation or execution of a contract or make a contractual clause unnecessary
- It can help to exchange money, property, stocks or anything of value in a transparent and conflict-free manner, avoiding the services of an intermediary
- Set the rules and penalties around a contract in the same way as a traditional contract, but also automatically impose those obligations (code is law)

Average Settlement Time By Transaction Type

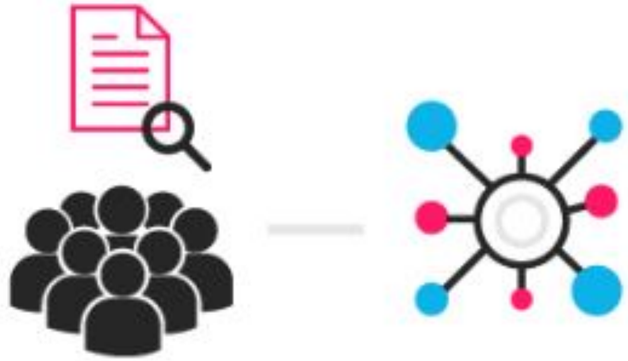
1

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

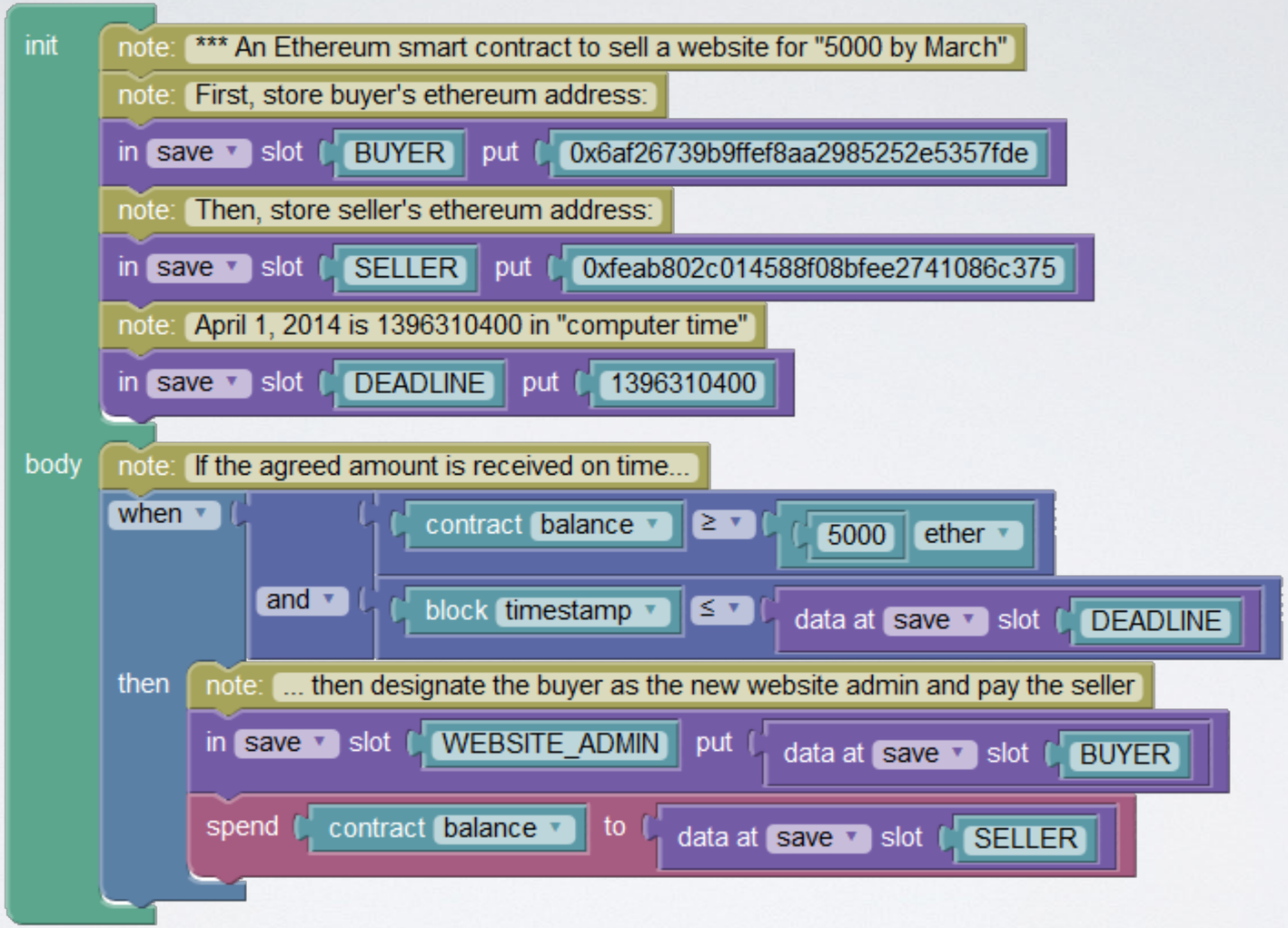
2

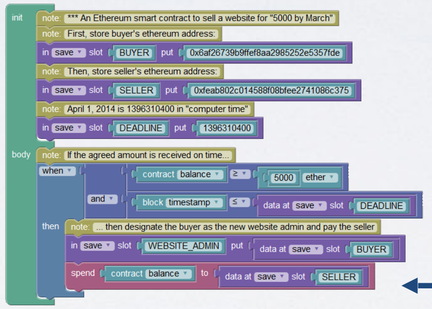
A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3



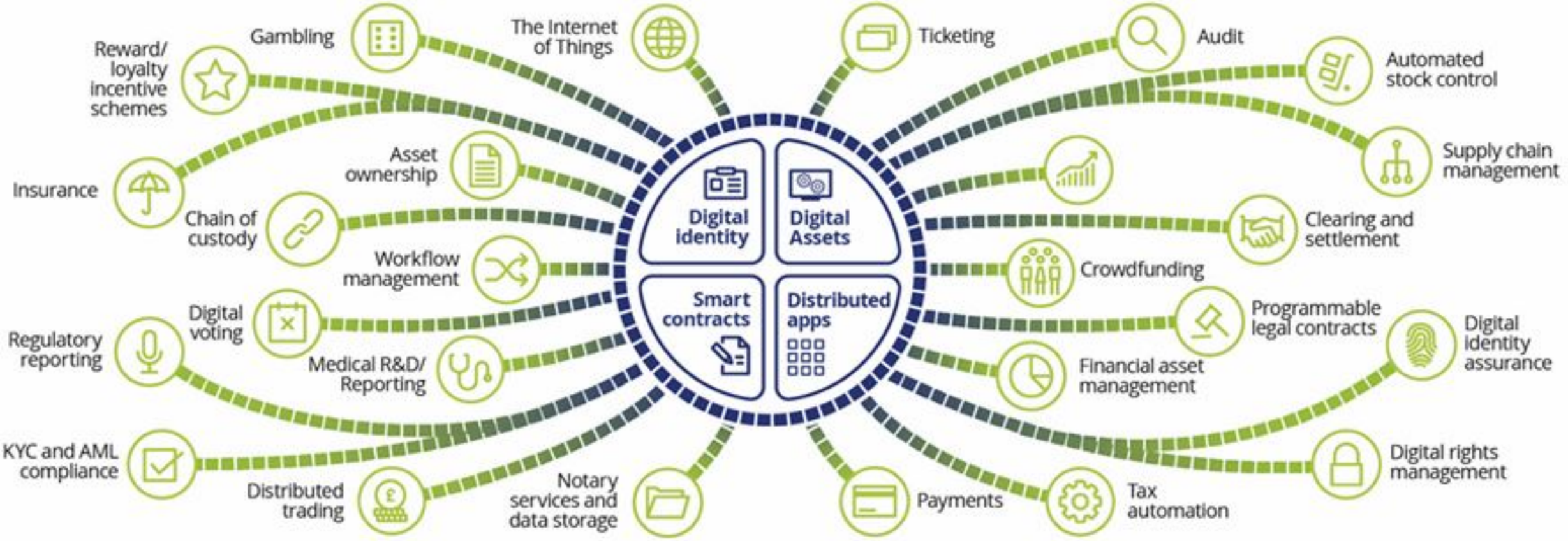
Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions


init
note: *** An Ethereum smart contract to sell a website for "5000 by March"
note: First, store buyer's ethereum address:
in save slot BUYER put 0x6af26739b9ffef8aa2985252e5357fde
note: Then, store seller's ethereum address:
in save slot SELLER put 0xfeab802c014588f08bfee2741086c375
note: April 1, 2014 is 1396310400 in "computer time"
in save slot DEADLINE put 1396310400
body
note: If the agreed amount is received on time...
when
contract balance ≥ 5000 ether
and
block timestamp ≤ data at save slot DEADLINE
then
note: ... then designate the buyer as the new website admin and pay the seller
in save slot WEBSITE_ADMIN put data at save slot BUYER
spend contract balance to data at save slot SELLER


init
note *** An Ethereum smart contract to sell a website for "5000 by March"
note First, store buyer's ethereum address:
in save slot BUYER put 0x6af26739b9ffef8aa2985262e5357fde
note Then, store seller's ethereum address:
in save slot SELLER put 0xfeab802c014588f08bfee2741086c375
note April 1, 2014 is 1396310400 in "computer time"
in save slot DEADLINE put 1396310400
body
note If the agreed amount is received on time...
when
contract balance ≥ 5000 ether
and
block timestamp ≤ data at save slot DEADLINE
then
note ... then designate the buyer as the new website admin and pay the seller
in save slot WEBSITE_ADMIN put data at save slot BUYER
spend contract balance to data at save slot SELLER

What can you do with a blockchain?

KYC – Know Your Customer
AML – Anti-Money Laundering



Deloitte.

www.deloitte.co.uk/blockchain

ethereum

The World Computer - Open Source Peer-to-Peer Applications

ETHEREUM

- Ethereum is a decentralized platform that executes smart contracts: applications that run exactly as scheduled without any chance of downtime, censorship, fraud, or third-party interference.

- These applications run on a custom blockchain, an extremely powerful shared global infrastructure that can move value and represent ownership of the property.

- This allows developers to create markets, store debt records or promises, move funds according to past instructions (such as a will or a future contract), and many things that have not yet been invented, all without an intermediary or counterparts risk .

ETHER

- Ether is the fuel for the Ethereum network.
- Ether is a necessary element - a fuel - to operate the Ethereum distributed application platform.
- It is a form of payment made by platform customers for the machines that perform the requested operations, serving as the incentive that ensures that developers write quality applications and that the network remains healthy.
- Developers wishing to create applications that will use the Ethereum blockchain need ether.
- Users who want to access and interact with smart contracts in the Ethereum blockchain also need ether.

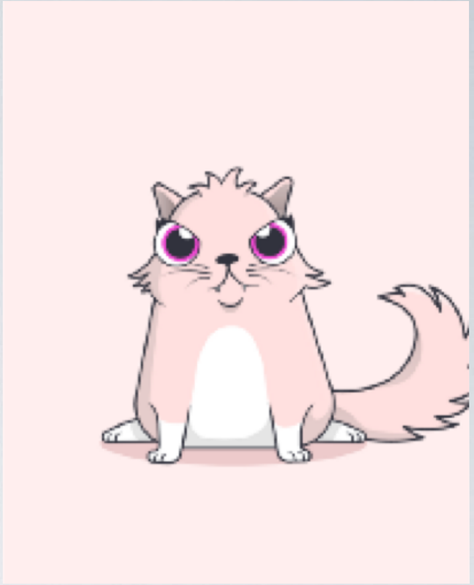
ERC-20

- ERC (Ethereum Request for Comments) is an official protocol for making suggestions to improve the Ethereum network;
  - 20 - is the unique identification number of the offer.
- Tokens that meet these specifications are known as ERC-20 tokens and are actually smart contracts for the system
- The ERC-20 standard defines a set of rules that must be met in order for a token to be accepted and capable of interacting with other tokens on the network.
- The tokens themselves are block assets, which can have value, and can be sent and received like any other cryptomade of Ethereum blocks.

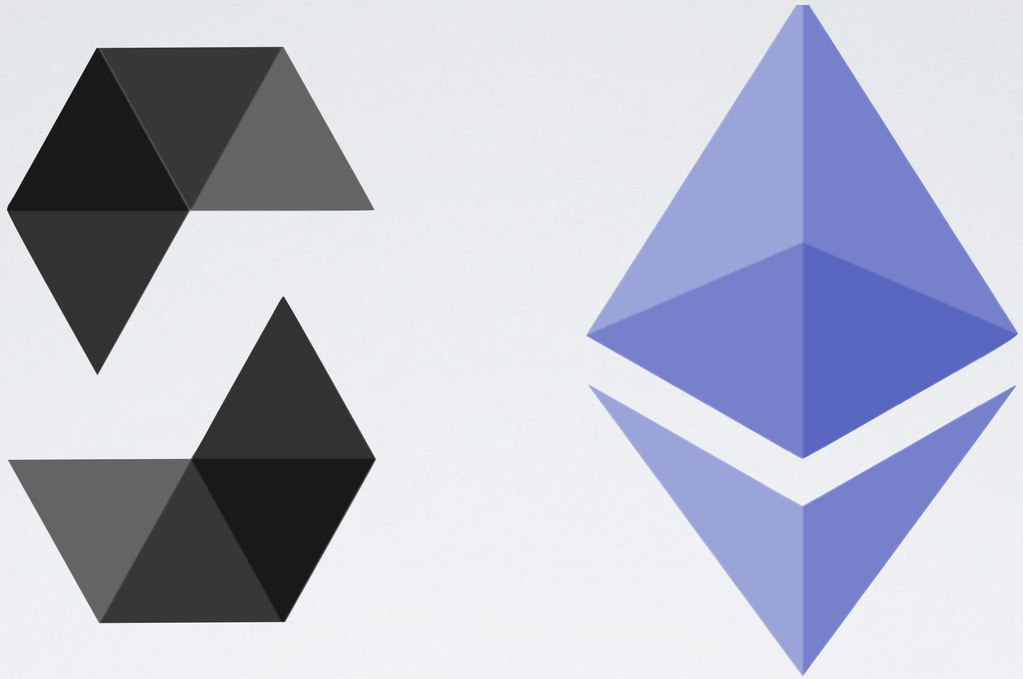
ERC-721

- ERC-721 is an open, free standard that describes how to create non-fungible or exclusive coins in the Ethereum blockchain.
- While most tokens are fungible (each token is the same as any other token), ERC-721 tokens are all unique.
- Think of them as rare and unique collectibles.

CRYTOKITTIES



- CryptoKitties is a virtual blockchain based game developed by Axiom Zen that allows players to buy, collect, play and sell various types of virtual cats.
- It represents one of the first attempts to deploy blockchain technology for recreational and leisure purposes.
- The popularity of the game in December 2017 congested the Ethereum network, causing it to reach a record of transactions and slow significantly.
- On March 20, 2018, it was announced that CryptoKitties would be dismantled in its own company and raised $ 12 million from various venture capital firms and angel investors.
- In December 2017, a CryptoKitty was sold for $ 100,000.

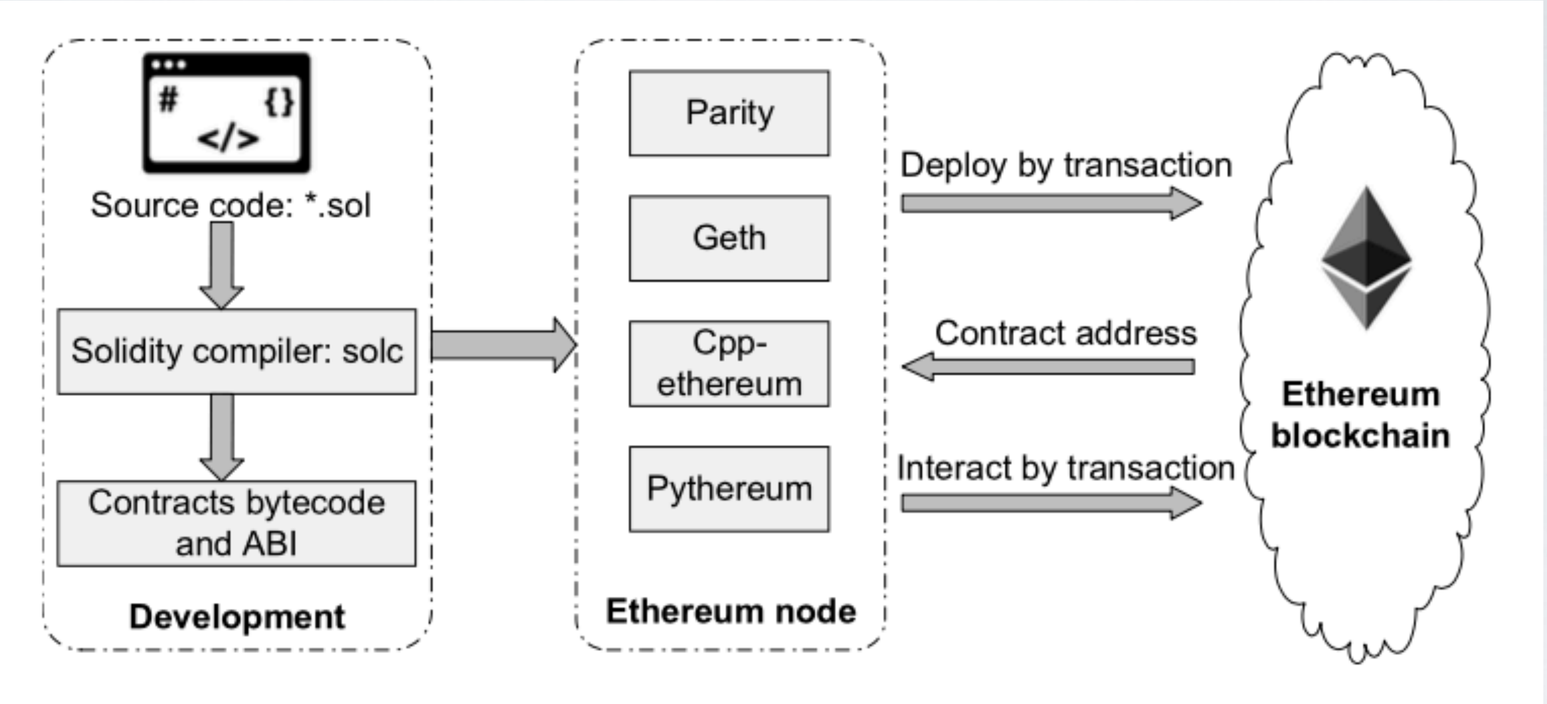


SOLIDITY

Language to create smart contracts

SOLIDITY

- High-Level Object-Oriented Language for Smart Contracts
- Solidity allows programming in Ethereum, a blockchain-based virtual machine
- Solidity is a programming language with static typing that has similarities to Javascript and C
- Solidity is compiled to bytecode which is executable in EVM



SMART CONTRACT DEPLOYMENT

IOS APPS

- Creation of a token and an economy (that can be shared between games/apps);
- Creation of unique itens (that can also be traded and shared between games/apps);
- Allowing payment in cryptocurrencies;
- Creation of smart contracts to automatize of services and also transparency;

INTERESTING TOOLS FOR DEVELOPMENT

- https://remix.ethereum.org - Platform for development and publishing a Contract
- Metamask - ETH Wallet
- https://github.com/matterinc/web3swift - Pod for interaction between App and the contract

PRACTICAL EXAMPLE

- Creating a Smart contract
- Creating an iOS App to interact with the contract
- Code:
  - https://github.com/mjoselli/ETH_iOS_workshop

MINICHALLENGE EXAMPLE

- Big Idea: Blockchain
- Essential Question: How can the blockchain change peoples live?
- Challenge: Develop an App that use the blockchain to help people?