



# Cryptocurrencies

Carlos Faria

[carlosfaria.com](http://carlosfaria.com)

[bitcoinportugal.org](http://bitcoinportugal.org)

Satoshi Nakamoto  
satoshi@lists.gmx.com  
www.bitcoin.org

# Who am I ?

- 24y. From Madeira. Living in Lisbon.
- Computer Science master student at IST
- Co-Founder at Blockbird Studio ([www.blockbird.studio](http://www.blockbird.studio))
- Founder at Bitcoin Portugal ([www.bitcoinportugal.org](http://www.bitcoinportugal.org))
- Former Volunteer at SINFO ([www.sinfo.org](http://www.sinfo.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

# What is Bitcoin Portugal ? [www.bitcoinportugal.org](http://www.bitcoinportugal.org)

- Free source of information about Bitcoin in Portuguese
- Help people in Portugal understanding Bitcoin
- Anyone can collaborate (<https://github.com/Bitcoin-Portugal>)



# What we do at Blockbird Studio ? [www.blockbird.studio](http://www.blockbird.studio)

- We are developing the first-of-its-kind Blockchain Simulator: **BlockSim**
- We focuses on developing disruptive blockchain & distributed ledger solutions



What is >SINFÜ?





Scott Chacon  
Github, CIO



Richard Stallman  
GNU Project,  
Founder



Joel Spolsky  
Stack Overflow,  
Trello, Founder



Peter Sunde  
The Pirate Bay,  
Co-founder



Steve Huffman  
Reddit,  
Co-Founder



Drew Hintz  
Google,  
Security Engineer



Mike Ambinder  
Valve,  
Senior Psychologist

# >SINFO

[www.sinfo.or](http://www.sinfo.or)

Let's talk about  
cryptocurrencies





# Evolution of Money

Money is anything used as a medium of exchange



# Evolution of Money: Commodity Money

## → Barter system (1000 a.C.)

- ◆ Pastoral society used livestock
- ◆ Agriculture society used grain and foods
- ◆ The Roman used cattle and salt



→ **Problems:** Storing, durability, transportation and divisibility

# Evolution of Money: Metallic Money

## → Uncoined metals

- ◆ Metal were not used as coin but as a bullion
- ◆ Problem: measuring the weight and value



## → Coined metals

- ◆ Standard coins were created
- ◆ They had a standard weight and value
- ◆ **Fully bodied**: whose face value is equal to the value of the metal contained in it
- ◆ **Token money**: its face value is higher than value of metal



## → **Problem:** Storing and transportation

# Evolution of Money: Paper Money

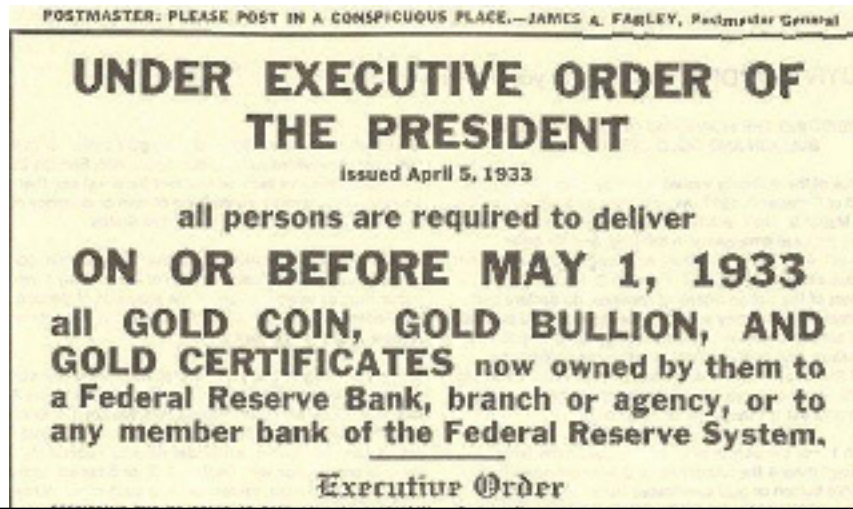
- Originated as a receipt issued by Goldsmiths
- These receipts were then later on used for payments
- In 1900 it was created in U.S. the gold standard money



# Evolution of Money: Fiat Paper Money



- A currency without intrinsic value that has been established as money, often by government regulation
- **Fiat money does not have use value**, and has value only because a government maintains its value, or because parties engaging in exchange agree on its value



# Evolution of Money: Electronic Money





# Evolution of Money: Cryptocurrencies

Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible (Interchangeable)	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure (Cannot be counterfeited)	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce (Predictable Supply)	Moderate	Low	High
Sovereign (Government issued)	Low	High	Low
Decentralized	Low	Low	High
Smart (Programmable)	Low	Low	High

Table 3.0 The degree to which gold, fiat, and cryptographic currencies fulfill the traditionally recognized traits of currency as well as the new traits made possible by the invention of the blockchain.



Why did cryptocurrencies  
come into existence?





POLITICS

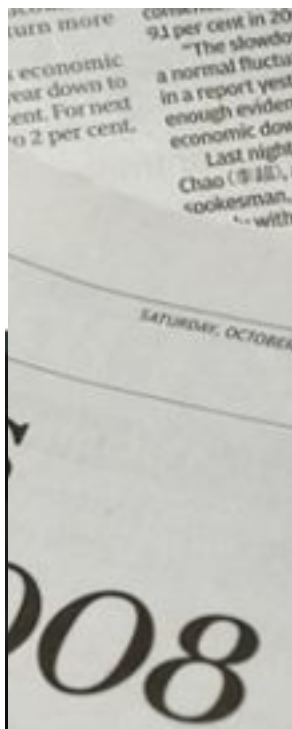
## House Extends Surveillance Law, Rejecting New Privacy Safeguards

By CHARLIE SAVAGE, EILEEN SULLIVAN and NICHOLAS FANOOS JAN. 11, 2018



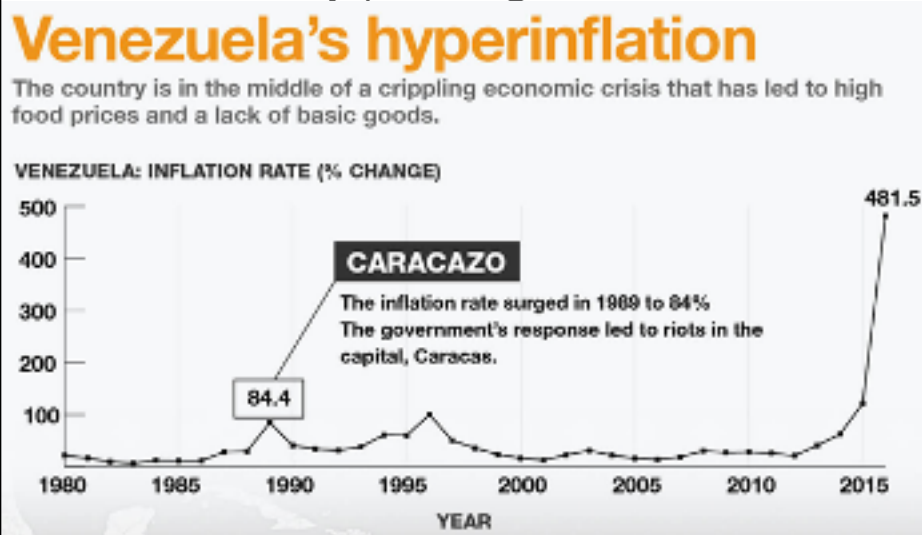
President Trump tweeted in support of an amendment to the Foreign Intelligence Surveillance Act, or FISA, on Thursday. It was the latest example of him contradicting his administration, his party and even himself. *By CHRIS CREELD on January 11, 2018. Photo by Patrick Semanay/Associated Press.*  
[Watch in Times Video »](#)

WASHINGTON — The House of Representatives voted on Thursday to extend the National Security Agency's warrantless surveillance program for six years with minimal changes, rejecting a push by a bipartisan group of lawmakers to impose significant privacy limits when it sweeps up Americans' emails and other personal communications.



# Actual monetary system

- We give the power to governments and central banks to decide the value of a currency
- Money printing when bad used can cause serious damage to society



news / opinion / sport / arts / life



world / europe / US / americas / asia / australia / middle east / africa / more

## Venezuela

## Growing number of Venezuelans trade bolivars for bitcoins to buy necessities

Bitcoin users still represent a tiny minority, but some believe that the currency will become more popular in Venezuela as economic uncertainty escalates



WORLD

## Venezuela Crisis: Bitcoin Seen As More Stable Alternative Amid Surge In Inflation, Banknote Chaos

BY JASON LE MIERE



ON 12/18/16 AT 8:10 AM

## VICE NEWS

Unable to Get Dollars, Venezuelans Turn to Bitcoins

AMERICAS

## Unable to Get Dollars, Venezuelans Turn to Bitcoins

By Payton Gulon

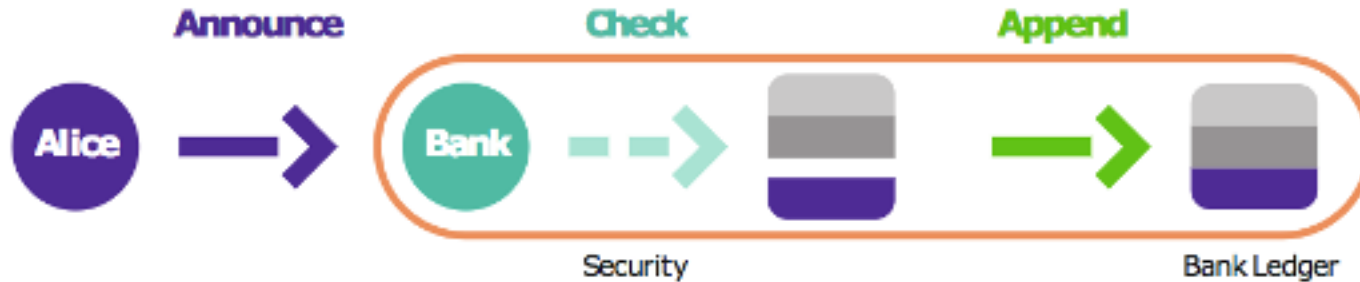
October 14, 2014 | 11:20 pm

Most of the world's economies run in accordance to the old Wu-Tang Clan mantra of C.R.E.A.M.: "cash rules everything around me." The idea is pretty straightforward: if you have cash, you can buy things. If you don't, you can't.

But in Venezuela, citizens can have buckets of bolivars (the national currency) and still find themselves unable to buy the sorts of goods that many in the developed world take for granted.

How can we transfer value to  
someone without trusting any  
organization?

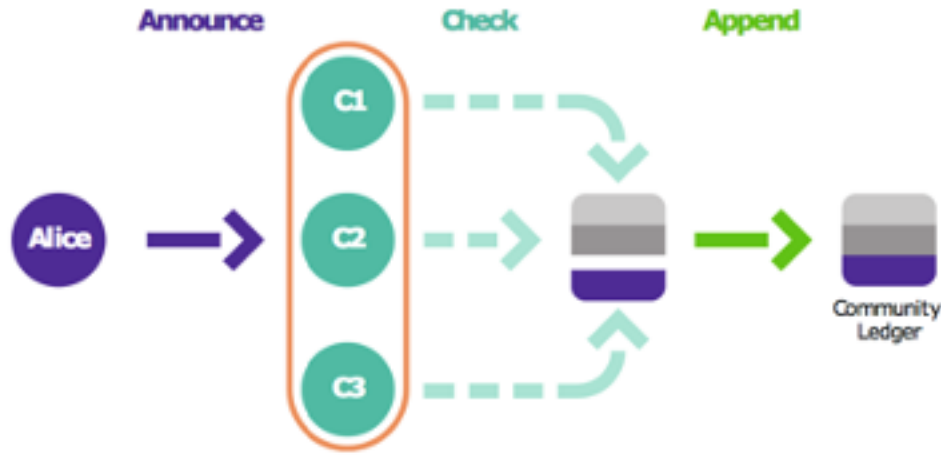
# A Centralized Money System



- Alice tells Bank she wants to send money to Bob
- Bank verifies if Alice is authorized and checks her funds
- Bank adds the transaction to its ledger
- **Trust in Bank is essential**
- The Bank ledger can be tampered
- The Bank can freeze accounts
- High transactions fees

From	To	Amount	Time	ID
Joe	Jane	5	3/21/17 10:30 AM	341
Chuck	Daisy	3	3/21/17 10:35 AM	342
Alice	Bob	2	3/22/17 10:30 AM	343

# A Decentralized Money System



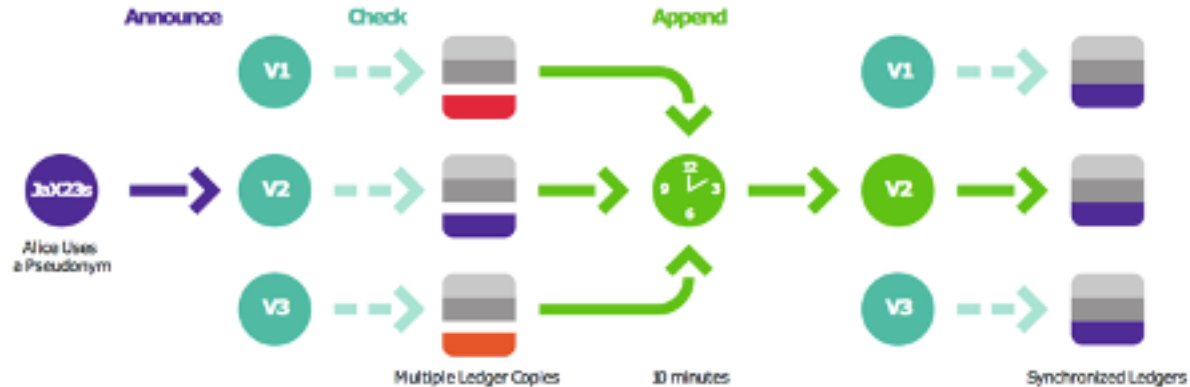
- No bank, replaced by a town hall with a public community ledger
- Transactions are announced to the entire community
- Transactions validated by majority of members
- A designated person adds transactions to community ledger
- Process managed by community and not a single authority

But ...

- How to keep the ledger secure?
- Verification is better performed by dedicated workers than entire community
- No privacy

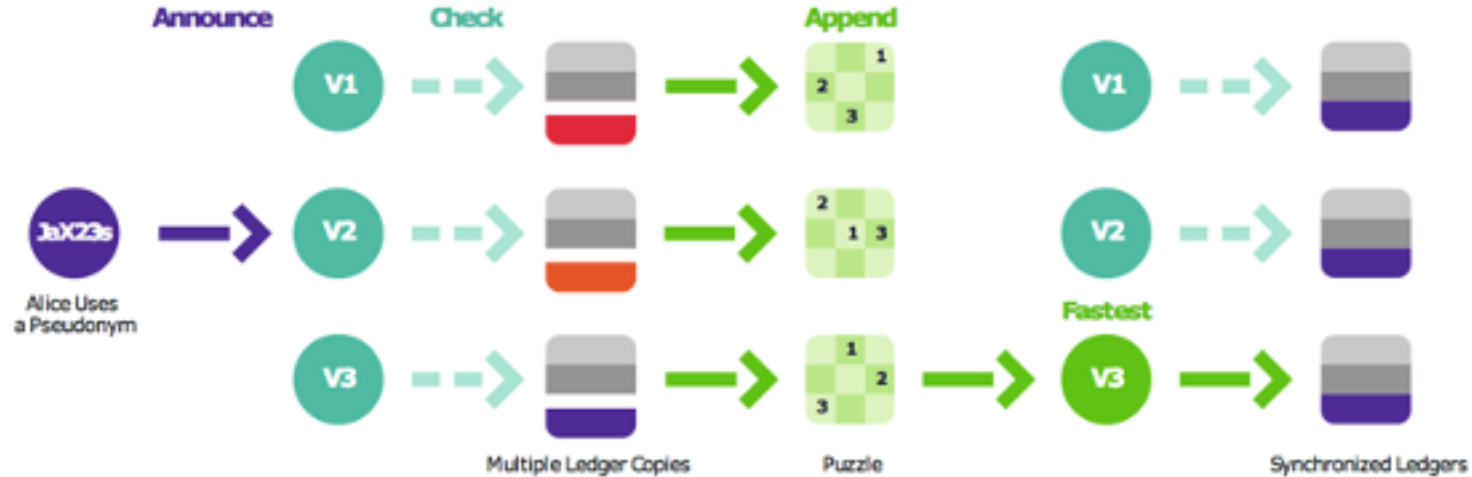
Source: Rasheed Sabar, "What Are Cryptocurrencies?"

# A Decentralized & Distributed Money System



- Everyone owns a personal copy of ledger and it must be synchronized with others based on certain rules (no single point of failure as several ledgers would have to be tampered)
- Community members do not verify transactions - they employ validators who get paid for the job in the community's currency (validators can be audited by community and ledger is still open)
- System is now digital, transactions now between randomized emails that each member can access with their own secret password

# A Secure Decentralized & Distributed Money System



- Instead of randomly choosing a validator, choose one that solves a cryptographic puzzle fastest
  - Solving puzzles costs real-world resources, this procedure makes it costly to propose ledger updates
  - Tampering with a ledger requires more resources than other validators combined
- ◆ This is called “Nakamoto consensus”



# Bitcoin



*Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.* – **Satoshi Nakamoto, 09 January 2009**, announcing Bitcoin on SourceForge.

- Bitcoin solved the **double spending problem**: preventing that one entity spends the same amount twice
- In Bitcoin the “validators” are called **Miners**
- These miners are rewarded via issuance of new bitcoins
- Bitcoin supply is limited to 21M coins by 2040
- The “community ledger” is called **Blockchain**

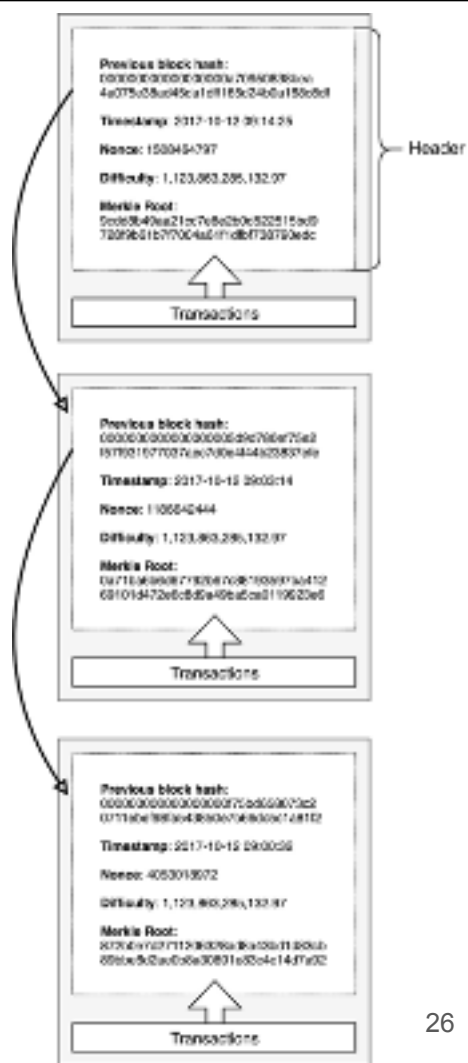
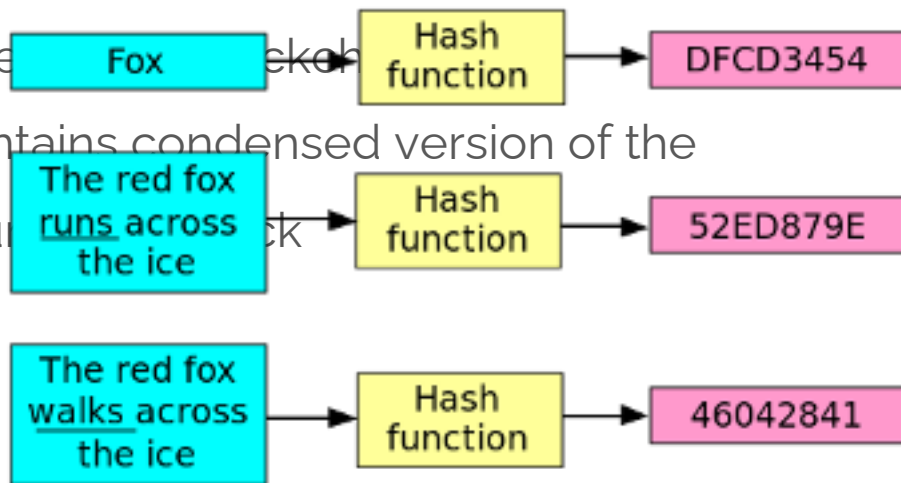
# Blockchain?

- Input** **Hash sum**

→ Blocks of transactions are chained together via hash functions to create a digital signature

→ Each block contains condensed version of the previous one up to the previous block

```
graph LR; subgraph "Block 1"; B1[Fox]; end; subgraph "Block 2"; B2["The red fox runs across the ice"]; end; B1 --> H1[Hash function]; H1 --> S1[DFCD3454]; B2 --> H2[Hash function]; H2 --> S2[52ED879E];
```



# Decentralised

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Apr 05 2018

21:32:11 GMT+0100 (WEST).

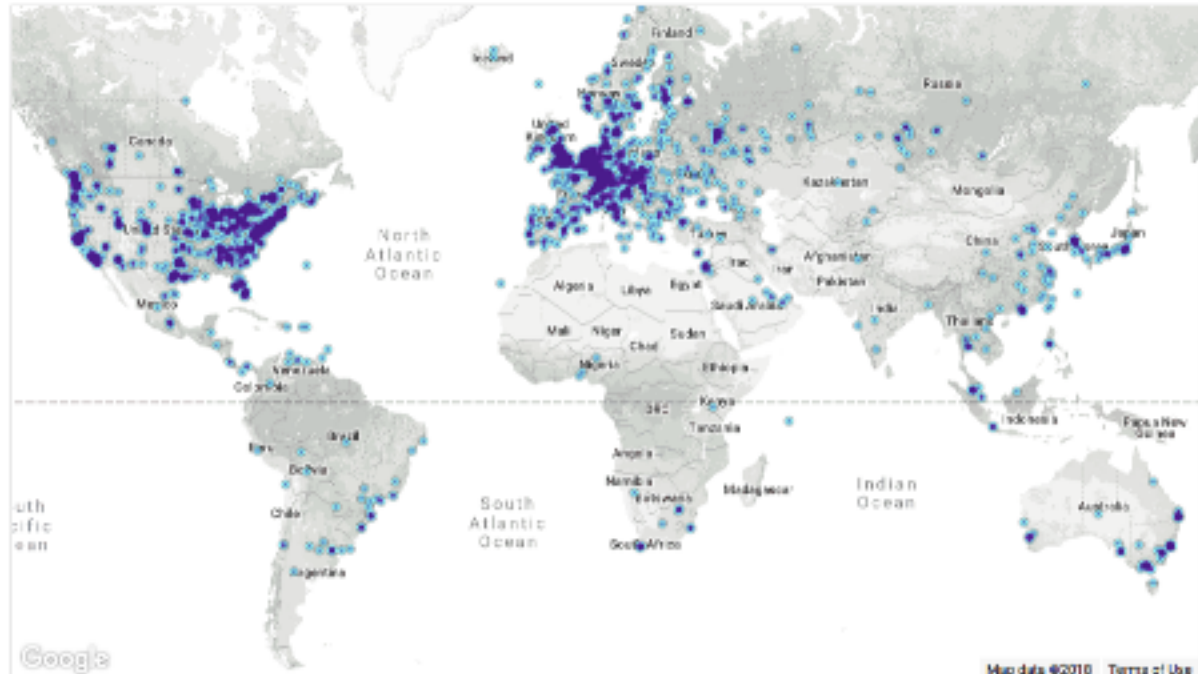
### 11183 NODES

24-hour charts >

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2712 (24.25%)
2	Germany	2013 (18.00%)
3	China	1083 (9.68%)
4	France	681 (6.09%)
5	Netherlands	509 (4.55%)
6	United Kingdom	418 (3.74%)
7	Canada	402 (3.59%)
8	Russian Federation	359 (3.21%)
9	n/a	299 (2.67%)
10	Singapore	234 (2.09%)

More (104) >



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

# Cryptocurrencies?

- Serve different purposes and can differ by features:
  - ◆ Transaction speed, privacy, monetary policy, tamper resistance mechanics, governance
- It uses cryptography to secure the system
- Private key owner owns the cryptocurrency unit
- Permissionless: open to anyone
- Transparent
- Limited supply

# Cryptocurrencies serve different purposes

Currency



Bitcoin



Litecoin

Privacy



Monero



Zcash

Storage



Distributed Computing



Ethereum



Cardano



IOTA



Bitcoin Cash



Dash



Verge



NEO

More than 1500 cryptocurrencies on the markets

# Smart contracts



1



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

2



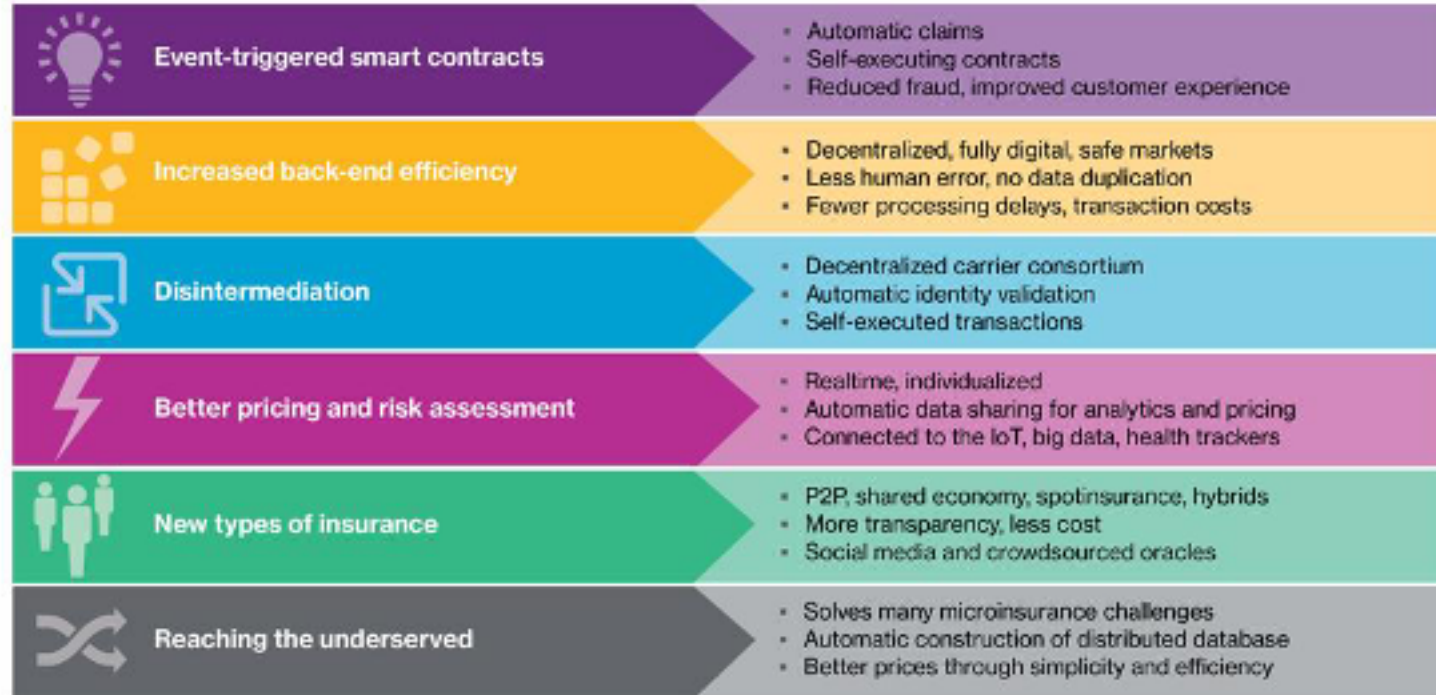
A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3

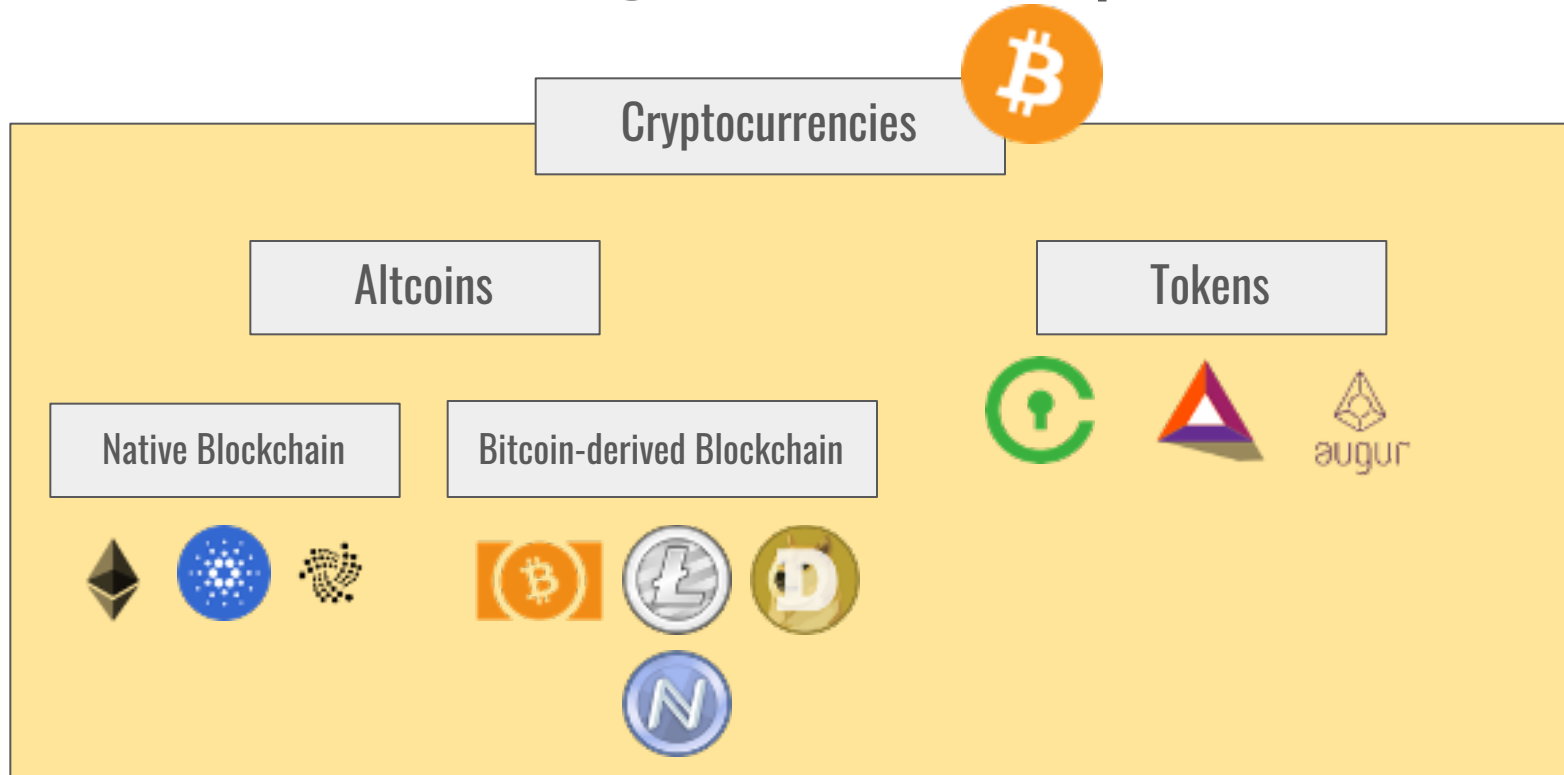


Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

# Why Smart contracts?



# Coins vs Tokens: Categorization of Cryptocurrencies





# Tokens Made in Portugal



Appcoins

Raised: \$15,300,000

1 AAPC = 0.30 USD



UTRUST

Raised: \$20,000,000

1 UTK = 0.11 USD



eSolidar


ICO coming this year



# Initial Coin Offerings (ICOs)

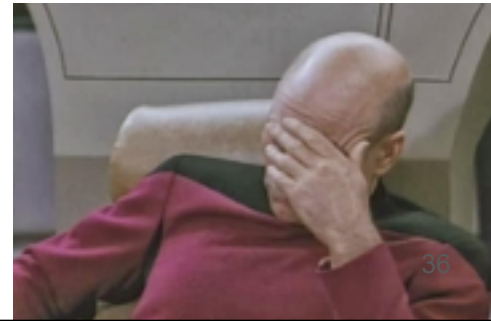
- Developers who build dApps create “tokens” to provision services in their applications
- Developers can sell tokens to investors in order to raise funds at various stages of dApp development
- An unregulated mean of **crowdfunding** via use of cryptocurrency
  - ◆ Can be a source of capital for startup companies
- In an ICO a percentage of the newly issued tokens are sold to investors in exchange for legal tender or other cryptocurrencies such as Ethereum or Bitcoin

# Top ICOs

- Telegram  **\$1.7B** : Storage, Proxy, DNS, Services, Payments
- Filecoin **\$250M** : Decentralized storage network
- Tezos **\$232M** : Self-amending cryptographic ledger
- EOS **\$185M** : Open source platform for scalable decentralized apps
- BAT **\$35M** in 30 seconds (\$1.2M per second) : Blockchain-based digital advertising
- UET **\$40,000** in 3 days

UET = Useless Ethereum Token, it is a "joke coin"

"UET is a standard [ERC20 token](#), so you can hold it and transfer it. Other than that... nothing. Absolutely nothing."



# Why Most ICO's Will Fail: A Cold Hard Truth

- Investors are investing millions into concepts that don't even have an alpha version of their product
- Investors are desperate to put their money in because they think that ICOs are a way to get rich quick
- In order to cash in on this, developers are creating products more aimed towards ICOs than to give actual value
- Because of the "Greater Fool Theory," the value of the tokens gets inflated

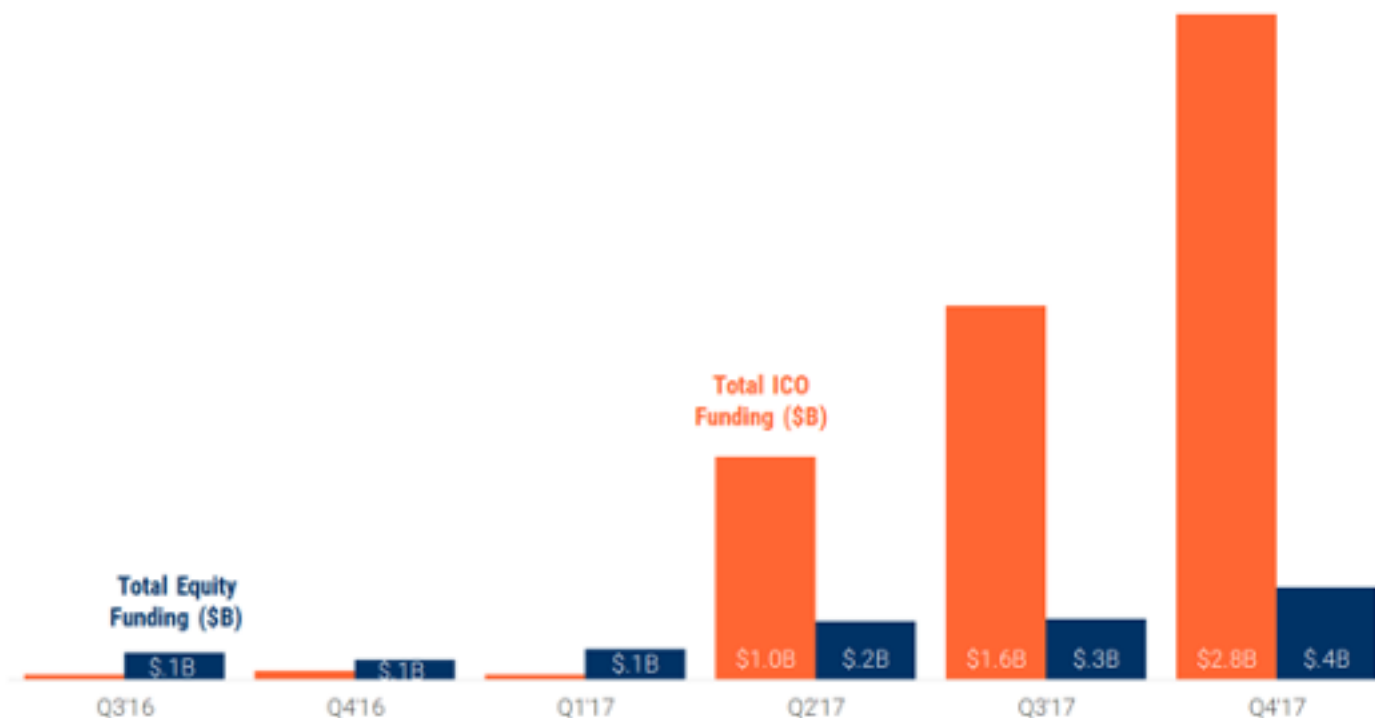
# ICOs compared to traditional fundraising mechanisms

	ICO	Equity Crowdfunding	Reward Crowdfunding	VC	IPO
Startup stage	Prototype	Prototype	Prototype	Prototype→Late stage	Late stage
Equity	No	Yes	No	Yes	Yes
Requirement	White paper (optional) <ul style="list-style-type: none"> <li>- Desired amount</li> <li>- Project milestones</li> <li>- Team</li> <li>- Types of tokens</li> <li>- Exchange ratio</li> </ul>	Educational materials <ul style="list-style-type: none"> <li>- Investment description</li> <li>- Types of securities</li> <li>- Investment limits</li> </ul>	Educational materials <ul style="list-style-type: none"> <li>- Project description</li> <li>- Marketing deck</li> <li>- Types of rewards</li> </ul>	Pitch deck <ul style="list-style-type: none"> <li>- Management</li> <li>- Use of funds</li> <li>- Business model</li> </ul>	Prospectus <ul style="list-style-type: none"> <li>- Company description</li> <li>- Types of securities</li> <li>- Management</li> <li>- Financial info</li> </ul>
Investors	Blockchain enthusiasts	Angel investors	Early adopters	Limited partners	Public
Period	3-6 months	1-3 months	1-2 months	3-12 months	> 1 year
Fundraising cost	Low	Medium	Low	High	High
Channel	Online	Online	Online	Offline	Offline
Liquidity	Medium	Low	Low	Low	High
Downside risks	Project fails, fraud	Bankrupt	Project fails	Devalue, bankrupt	Price drops



## Blockchain equity funding pales in comparison to ICOs

Quarterly blockchain equity and ICO financing. Q3'16 - Q4'17



Source: CB Insights, TokenData

# Do you have a great idea?



[www.blockbird.studio](http://www.blockbird.studio)

We'll help you build it



**BlockChange** Capital

[www.blockchange.capital](http://www.blockchange.capital)

We'll help you in the fundraising

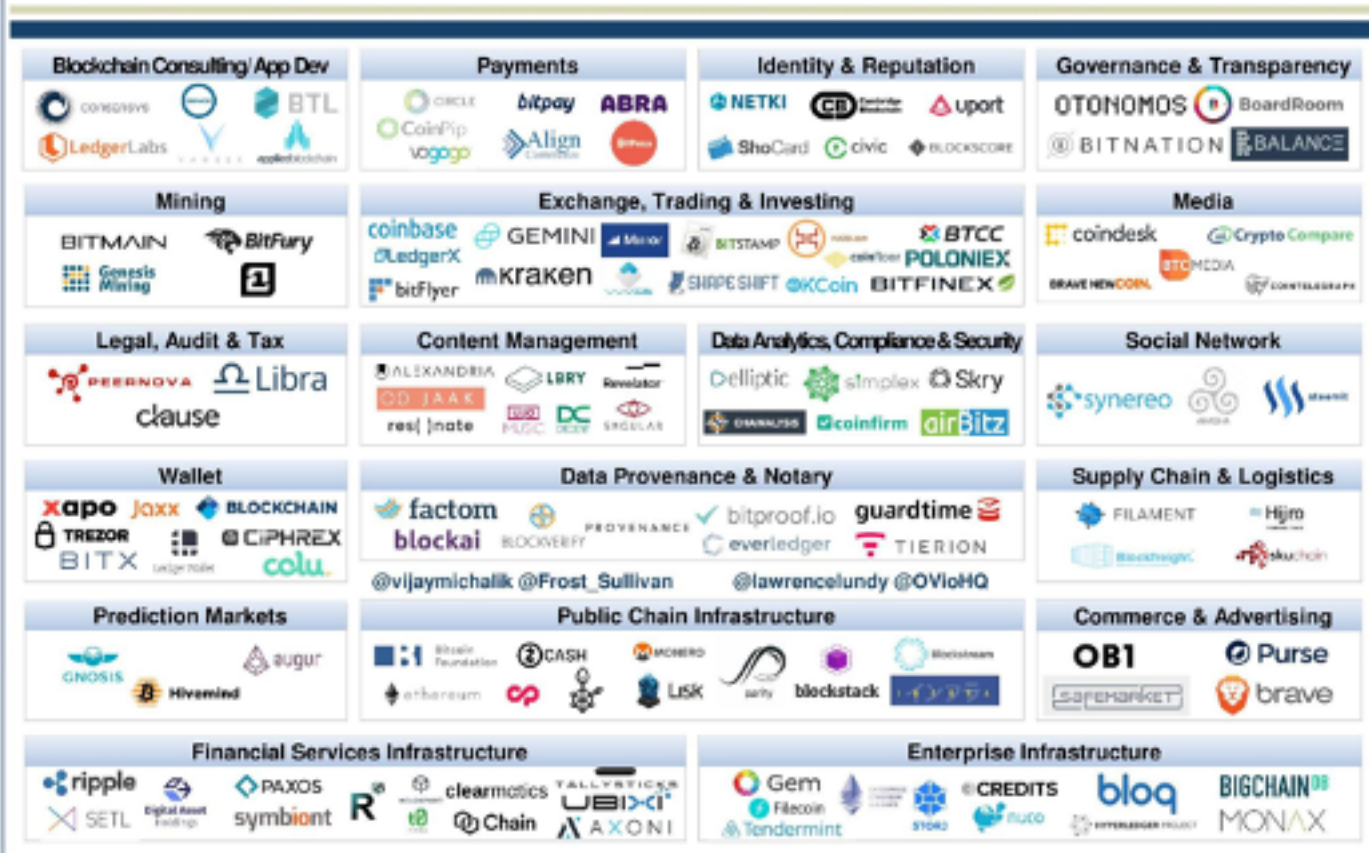
Contact us!



# Cryptocurrency market into perspective



# Blockchain Startup Landscape



7.7 bi \$

The market for blockchain-related products and services forecast for 2022, up from \$242 million last year.

57%

Percentage of large corporations that are actively considering or in the process of deploying blockchain solutions.

10%

Percentage of global GDP that could be stored, via digital assets, on blockchain by 2025, according to the World Economic Forum.

1.2 bi \$

Venture capital investment, to date, into more than a thousand blockchain startups, about one third in Europe.



*"I see blockchain as a game changer and I want Europe to be at the forefront of its development. We need to establish the right enabling environment - a Digital Single Market for blockchain so that all citizens can benefit, instead of a patchwork of initiatives."*

**European Commissioner for the Digital Economy and Society, Mariya Gabriel (Feb 2018)**



*"Technologies like blockchain can help reduce costs while increasing trust, traceability and security. They have huge potential for making social and economic transactions more secure online by guarding against an attack and removing the need for any middleman. We want to build on Europe's substantial talent base and excellent startups to become a leading world region that will develop and invest in the rollout of blockchain."*

**Vice-President for the European Digital Single Market, Andrus Ansip (Feb 2018)**

# Questions?

[carlosfaria.com](http://carlosfaria.com)

[bitcoinportugal.org](http://bitcoinportugal.org)

[blockbird.studio](http://blockbird.studio)

email@carlosfaria.com

# Start with Bitcoin

→ How to start using Bitcoin?

- ◆ PT: [bitcoinportugal.org/comecar](https://bitcoinportugal.org/comecar)
- ◆ EN: [bitcoin.org/en/getting-started](https://bitcoin.org/en/getting-started)

→ I'm developer. Can I play with Bitcoin? Yes!

- ◆ “*Mastering Bitcoin*”: [bitcoinbook.info](https://bitcoinbook.info)
- ◆ Bitcoin in JavaScript World:
  - [bcoin.io](https://bcoin.io)
  - [github.com/bitcoinjs/bitcoinjs-lib](https://github.com/bitcoinjs/bitcoinjs-lib)

*email@carlosfaria.com*