Blockchain: from electronic cash to redefining trust

Gabriel Aleixo
researcher

ITS Rio

BLOCKCHAIN TECHNOLOGY

Provides a new way for transferring and storing data in multiple aspects, without relying on a single entity or centralized server to guarantee that all its functions work properly.

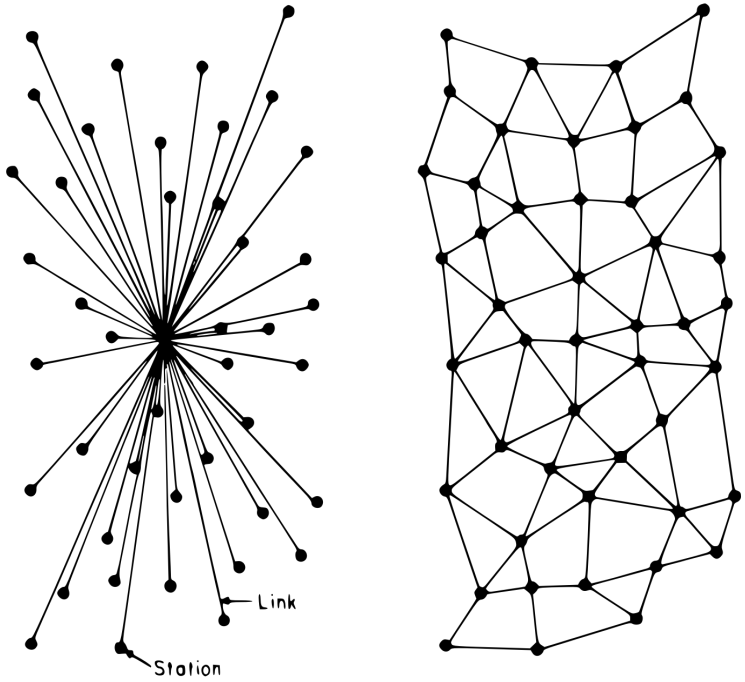
Blockchain is revolutionary because it creates a new paradigm: once it is among us, to be freely adopted with different use cases in mind, it makes possible for the first time **to have a service without a traditional service provider behind.**

Even better: everything is automated in these distributed databases.

BLOCK CHAIN

A **public ledger** containing all the transaction of a given system, secured by a **decentralized network** where anyone can start or stop being a peer at any moment without changing the principles by which everything works.

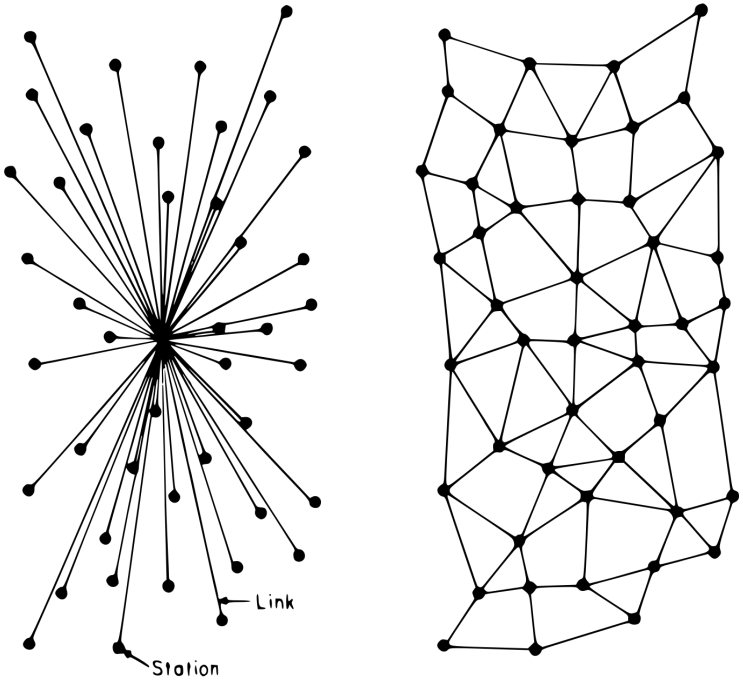
Computational proof of work is what creates and establishes trust among this network, granting that **consensus** is updated every few minutes among people who don’t know each other, without any sort of central coordination.



BLOCK CHAIN

Once the consensus is established, it's then broadcasted in the form of **blocks** of new information. This lets everyone update their own copy of the database and check for themselves the previous validation made by the network.

Code is the (only) law and it's responsible for the validation of what is true and the rejection of what is false (like double-spending attempts in Bitcoin). These blocks are generated in a **chronological** way whenever (only and only if) a new **proof-of-work** challenge is solved by someone in the network.



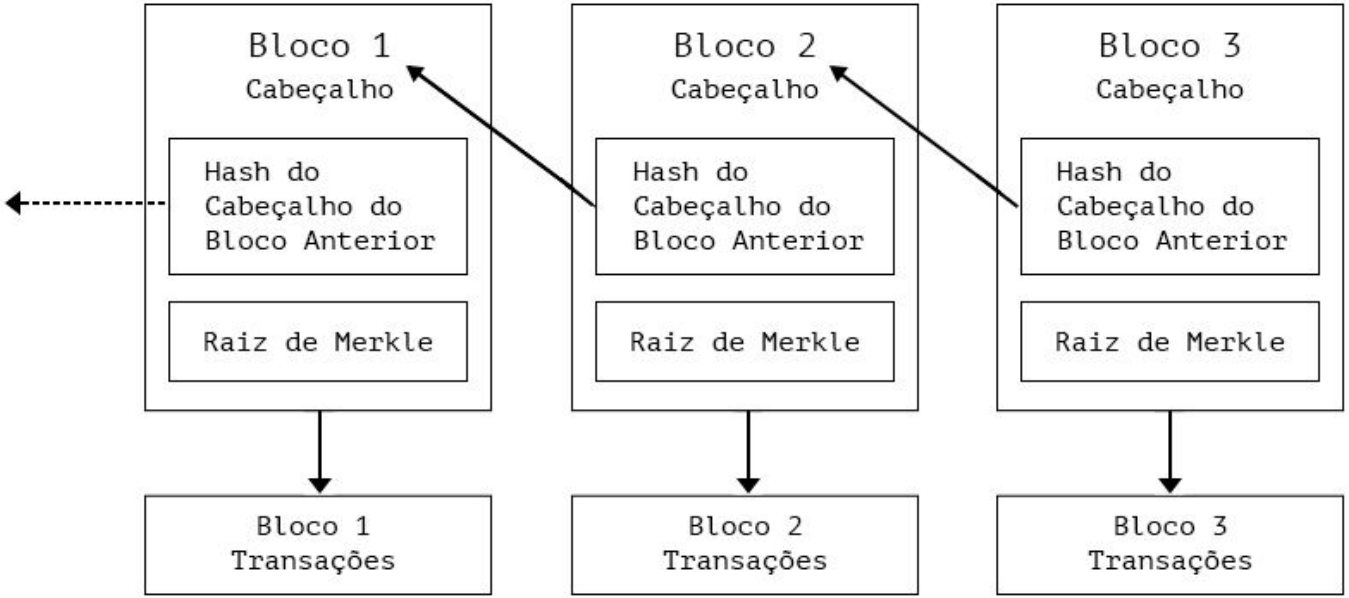
BLOCK CHAIN

As each new proof-of-work challenge trying to be solved by the networks is tied to the information contained in the previous block, all blocks form a **chronological** chain

Hence, ***block chain*** :)

Or ***blockchain***, as used to describe both the decentralized **database** and the **technology** that keep the consensus among its distributed copies

BLOCK CHAIN



Blockchain do Bitcoin Simplificada

BLOCKCHAIN TECHNOLOGY

These protocols provide unseen levels of **data security** and also a decentralized approach for **timestamping** any document, in some cases at much lower costs.

Moreover, having thousands of copies of the same database without losing the consensus among them makes every information **available**, **transparent** and **immutable** once recorded in a blockchain.

By doing so, we can secure the **authenticity** and **prove the existence** of any document/information without any third-party.

EDUCATION + BLOCKCHAIN

Universities, colleges, schools, MOOCs, etc, can digitize their certificates and register their unique digital IDs on a blockchain.

By doing so, you are creating a link between the document and the digital world, guaranteeing that no one can ever change its original content and authorship once the ID is registered on a blockchain.

No photoshopped documents can go through the system without being immediately noticed and pointed out as a fraud, with its authenticity being easily denied. These verifications can be done by anyone at any time, forever.

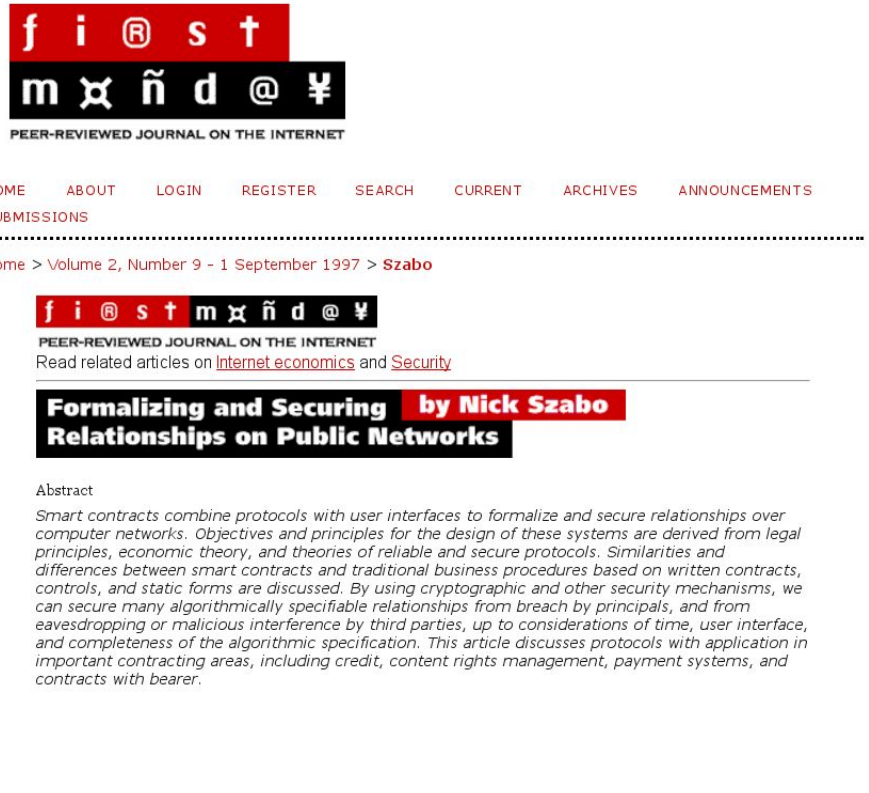
FINANCE + BLOCKCHAIN

A cryptographic token is the unit of account on a blockchain. The function of a blockchain dictates the characteristics of the corresponding tokens. If a blockchain primary function is a system for value transfer, the token will be something like a coin. If on the other hand, the blockchain is being used primarily as a voting mechanism, the token may have no monetary value at all, just being used as a “vote” itself. The characteristics of a cryptographic token are as numerous as the applications for blockchain technology, and the list is always growing: loyalty program points, gift cards, coupons, digital currencies, shares and so on are among the most promising and exciting ones.

GOVERNMENT + BLOCKCHAIN

Establishing an online digital identity for e-government, creating e-voting and participatory platforms, improving public registries and the notary system, improving land registries, enhancing transparency and accountability over financing political campaigns and political parties, creating new systems to license, manage, and collect royalties for intellectual property - which are less dependent on intermediaries, generating unique certificates of origin for physical goods, such as wood, preventing the commercialization of wood from illegal deforestation areas are the most promising capabilities of blockchain for public interest.

Smart Contracts
Nick Szabo (1993-97)



f i ® s t
m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

HOME ABOUT LOGIN REGISTER SEARCH CURRENT ARCHIVES ANNOUNCEMENTS SUBMISSIONS

Home > Volume 2, Number 9 - 1 September 1997 > **Szabo**

f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET
Read related articles on Internet economics and Security

Formalizing and Securing Relationships on Public Networks by Nick Szabo

Abstract

Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols. Similarities and differences between smart contracts and traditional business procedures based on written contracts, controls, and static forms are discussed. By using cryptographic and other security mechanisms, we can secure many algorithmically specifiable relationships from breach by principals, and from eavesdropping or malicious interference by third parties, up to considerations of time, user interface, and completeness of the algorithmic specification. This article discusses protocols with application in important contracting areas, including credit, content rights management, payment systems, and contracts with bearer.

Smart contracts are **pieces of code** capable of executing an action B once a **condition** A is satisfied.

Once a smart contract is deployed, everything else is **automated**.

Blockchain = nice addition :)

> *Ethereum intends to provide a blockchain that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in* ***a few lines of code****.*

ethereum, 2013

Blockchain Startups

Top Blockchain startups disrupting non-financial markets

Venture Radar

PAST

THE WALL STREET JOURNAL.

THE TIMES

HM Government

Hilton

PRESENT

facebook

twitter

Dropbox

UBER

airbnb

FUTURE

Cloud storage

Filecoin

TIERION

STORJ.IO

Smart Contracts

TRUST

ETHERPARTY

appliedblockchain

Social Networking

synereo

GEMS

Anti-Counterfeiting

everledger

BLOCKVERIFY

Governance

OTONOMOS

Swarm

followmyvote

BITNATION

GOVERNANCE 2.0

Digital Identity

ONENAME

ShoCard

Supply Chain

Tradle

thingchain

Art & Ownership

VERISART

Bitproof.io

MONEGRAPH

colu.

Prediction Markets

augur

Internet of Things

FILAMENT

More: https://www.ventureradar.com/


Blockchain
(Use Cases)
Source: GrowthPraxis
Proof of ownership and a marketplace for sales and purchase of digital assets
Company: MyPowers
Enables authenticity of a review through trustworthy endorsements for employee peer review
Company: TRST.im
Decentralized prediction platform for the share markets, politics etc
Company: Augur
Decentralized patient records management
Company – BitHealth (Healthcare IT)
Proof of ownership for digital content
Arts, pictures and images
Companies: Blockai, Bitproof, ascribe, Artplus
Other companies: Chainy.Link, Stampery
Digitizing assets: Improves anti-counterfeit measures
Consumer electronics, Automotive
Companies: The Real McCoy, ChainLink
Other companies: Everpass, BlockVerify
Degree Verification
Company: Degree Of Trust
Provides digital identity that protects consumer privacy
Internet, car locks: Onename
Elections Voting: Follow My Vote
Customer identification: Trustatom
Enables authenticity of a review
Helps users engage, share reputation and collect feedback
Company: The World Table
Through trustworthy endorsements
Company: Asimov
Decentralized internet and computing resources to every home and business
Company: ePlug
Digitizing company incorporations, transfer of equity/ownership and governance
Company: Otonomos
Escrow/Custodian service
Gaming industry
Companies: PlayCoin, Bitnplay
Gaming industry and loan servicing
Company: New System Technologies
E-commerce
Company: Fundrs.org
A smart contract IT portal executing order fulfilment in ecommerce/manufacturing
Company: UbiMS
Provides digital identity that protects consumer privacy
Companies: Sho Card, Uniquid
Decentralized IoT
Home automation: Chimera-inc.io
Industries: Filament
Decentralized storage using a network of computers on blockchain
Company: Storj
Digitization of documents/contracts and proof of ownership for transfers
Company: Colu (Colored Coins)
Digital security trading: ownership and transfer
Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA
Points based value transfer for ride sharing
Company – La'Zooz
Proof of ownership of modules in app development
Company: Assembly
Proof of ownership for digital content storage and delivery
Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN

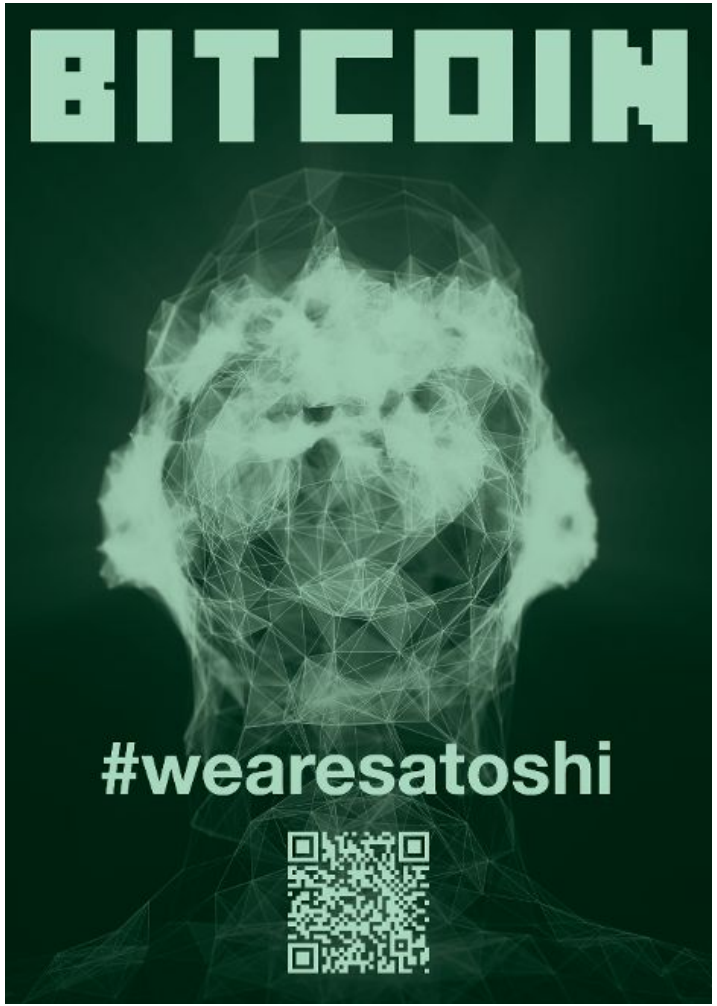
Blockchain & Climate/Environment

CarbonX

Everledger

Redd Chain

Plastic Bank



THANK YOU!

Gabriel Aleixo
researcher

aleixo@itsrio.org