Smart contracts present and future

What is a smart contract? How are they related to blockchain? Why could they change the world

Who is Stefano?

- Enthusiast open source developer
- Red Hat Principal software engineer and associate manager

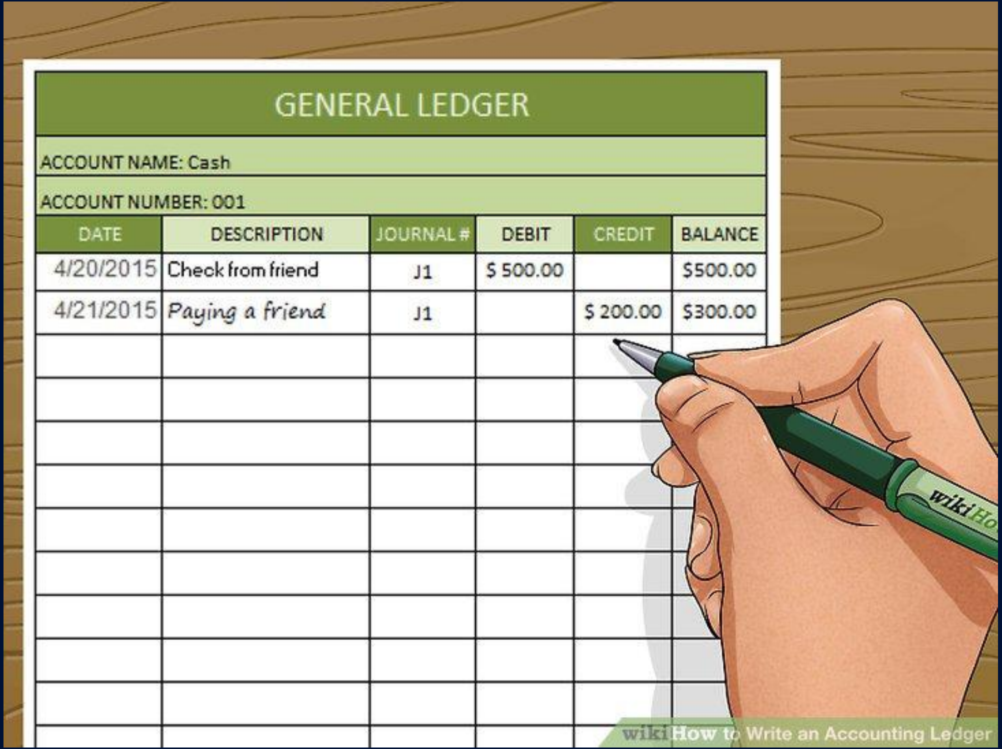
My matching pairs game: Java & JBoss, Open Source & Red Hat, Blockchain & Ethereum

- https://www.linkedin.com/in/maeste/
- https://twitter.com/maeste
- https://github.com/maeste/
- http://www.onchain.it/

Today’s Agenda

- Brief introduction to blockchain concepts
- Smart contracts and why you should care about
- Token and tokenization
- Concepts of fungibility and why NFT matters in the present and will play a big role in Blockchain future
- Use cases, present and future

What is the block chain?



GENERAL LEDGER

ACCOUNT NAME: Cash

ACCOUNT NUMBER: 001

DATE	DESCRIPTION	JOURNAL #	DEBIT	CREDIT	BALANCE
4/20/2015	Check from friend	J1	$ 500.00		$500.00
4/21/2015	Paying a friend	J1		$ 200.00	$300.00

What is the block chain?

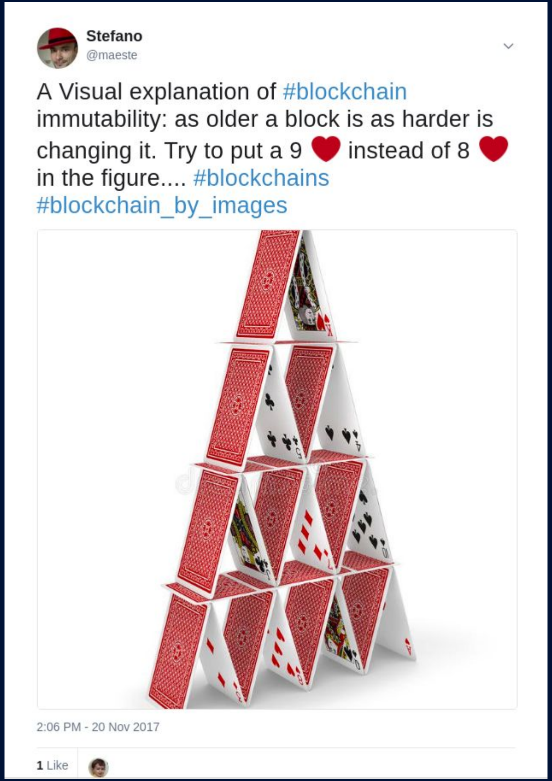
The Guardian: Blockchain is a **digital ledger** that provides a **secure** way of making and **recording transactions, agreements and contracts** – anything that needs to be recorded and verified as having taken place.

Wikipedia: A blockchain is a continuously growing list of records, called *blocks*, which are linked and **secured using cryptography**. Each block typically contains a **hash pointer** as a link to a previous block, a timestamp and transaction data. By design, blockchains are **inherently resistant to modification of the data**. A blockchain can serve as "an open, distributed ledger that can **record** transactions between two parties efficiently and **in a verifiable and permanent way.**"

What is a blockchain...a nice bullet list

- It’s a ledger of transactions and datas
- It’s persistent, secure and unmodifiable
- It’s based on computational trust
- It’s distributed and unstoppable
- Transaction parties are anonymous, but tx are public and verifiable
- It’s transactions could be about values (cryptocurrency)
- It’s trustless about nodes and users

Blockchain by images



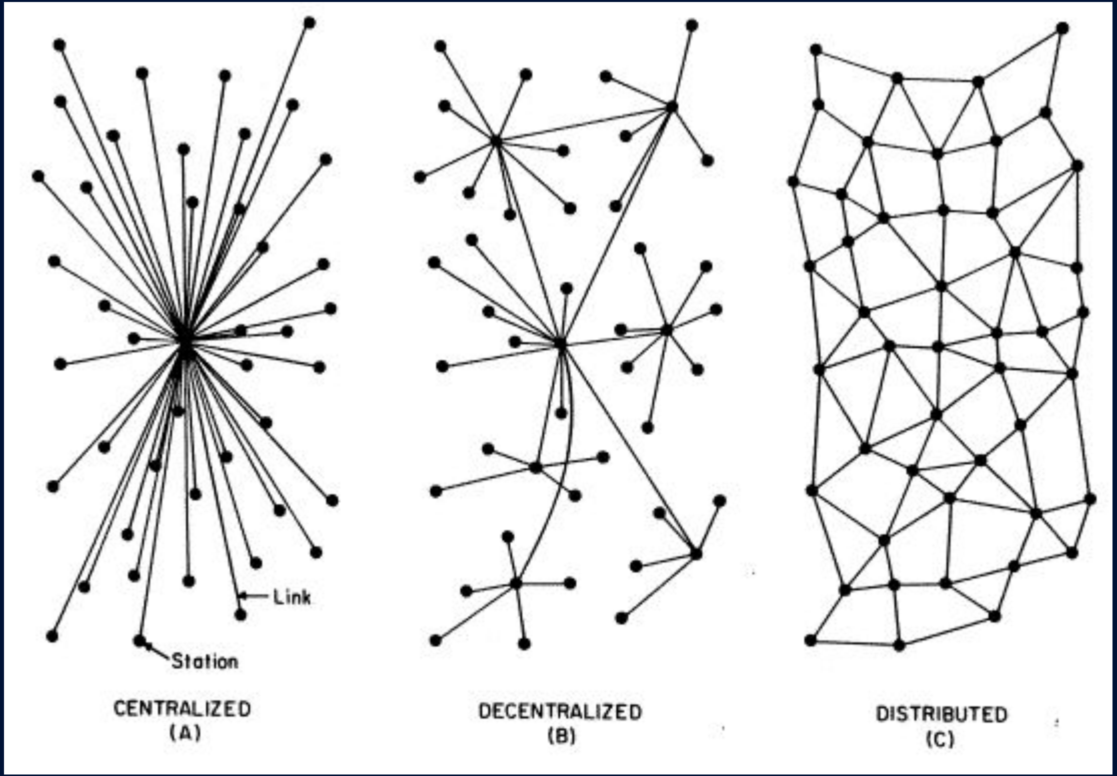
Stefano
@maeste

A Visual explanation of #blockchain immutability: as older a block is as harder is changing it. Try to put a 9 ❤ instead of 8 ❤ in the figure.... #blockchains #blockchain_by_images

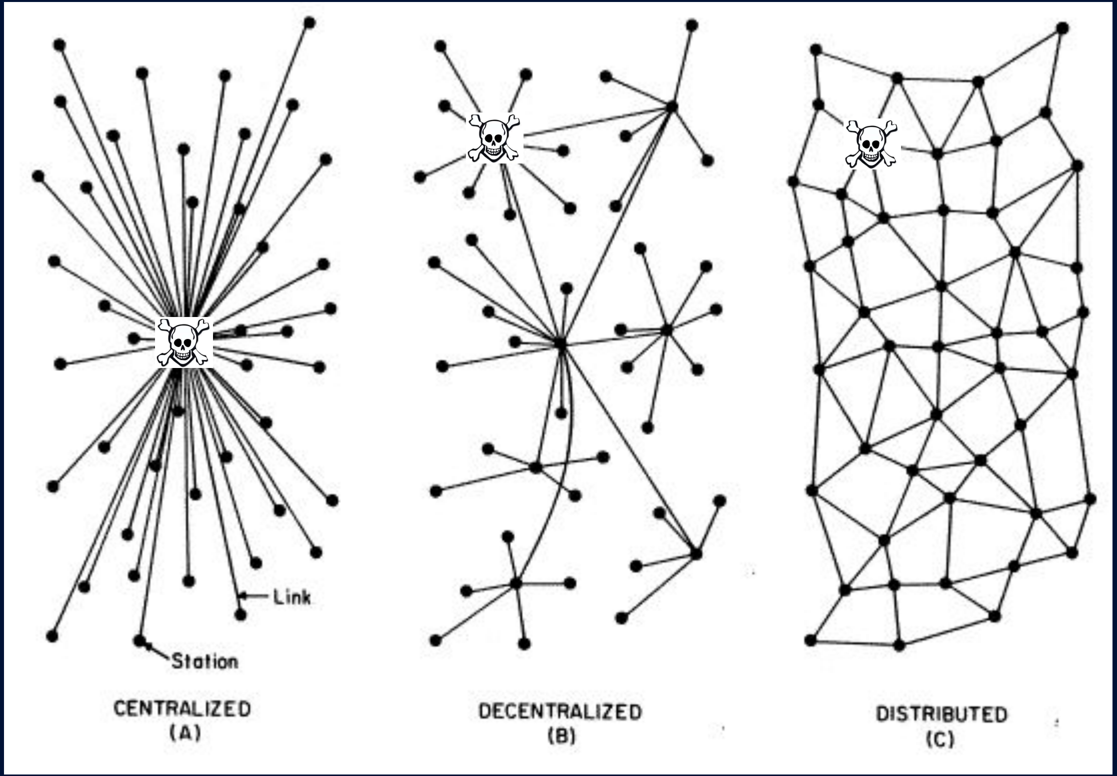
2:06 PM - 20 Nov 2017

1 Like

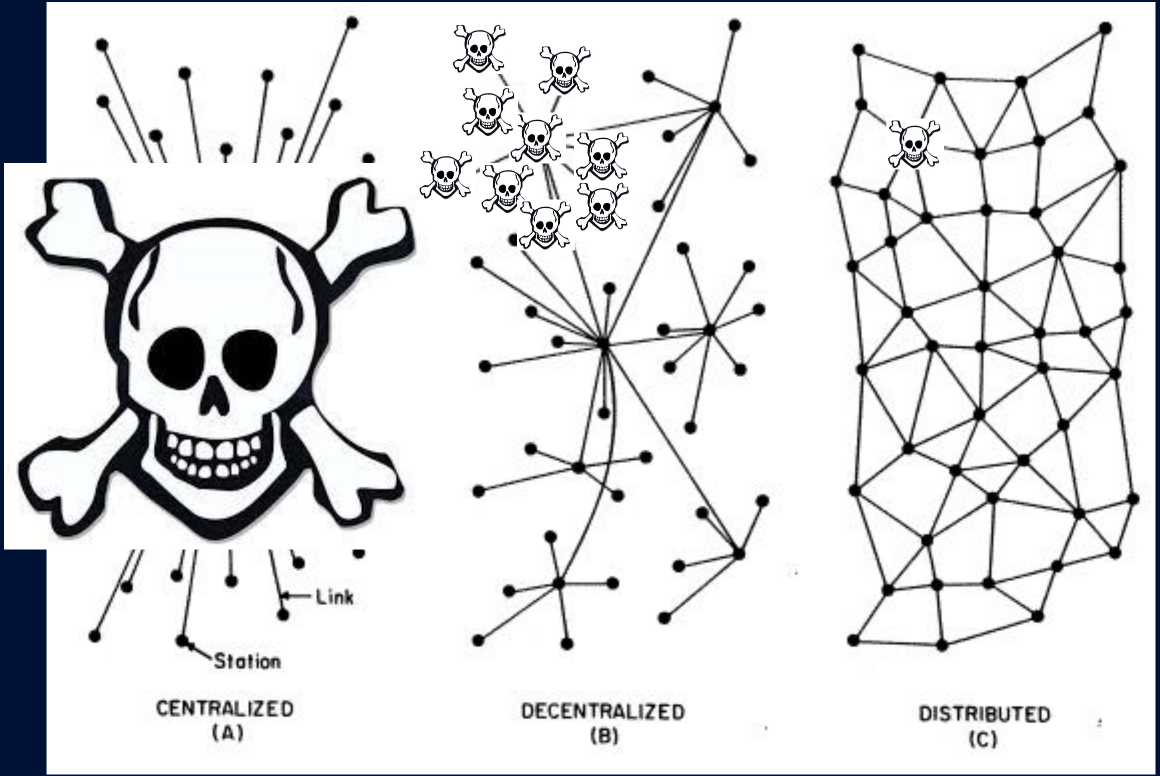
It’s distributed and unstoppable



It’s distributed and unstoppable



It’s distributed and unstoppable



Has those cryptocurrencies a real economic value? And why?

In economy “intrinsic value” concept doesn’t exist at all. We give value to money by convention, and more general anything gain value almost for 3 reasons (not strictly needed, but true in almost cases at least)

- It’s rare
- It’s hard to reproduce
- It could be exchanged
- Someone want to buy it (law of supply and demand)

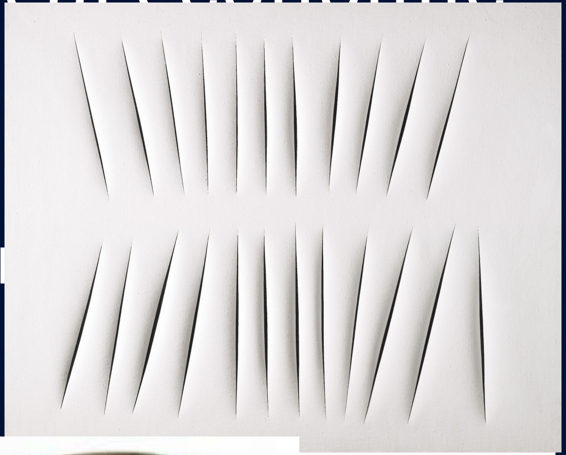
Has those cryptocurrencies a real economic value? And why?

In ec “intrinsic value” concept doesn’t exist at all
by co on, and more general anything gain value al
strict ded, but true in almost cases at least)

1 Euro

- It’s rare
- ard to reproduce
- ld be exchanged
- eone want to buy it (law of supply and dem

~ 7K Euro



M Euro

Manzoni’s artist's shit: ~275K Euro

What does trustless mean?

You are not trusting in peers of transaction or even in nodes of the network, you are trusting in the protocol itself. In other words you are trusting blockchain and cryptocurrency itself and not people owning them….moreover they are anonymous…

Does it recall anything you well known and use everyday?

What does trustless mean?

You are not trusting s of the network, you
are trusting in the pr sting blockchain and
cryptocurrency itsel ver they are
anonymous…

Does it recall anythi

What does trustless mean?

You are not trusting
s of the network, you
are trusting in the pr
sting blockchain and
cryptocurrency itsel
ver they are
anonymous…

Does it recall anythi

Smart Contracts

What is a smart contract?

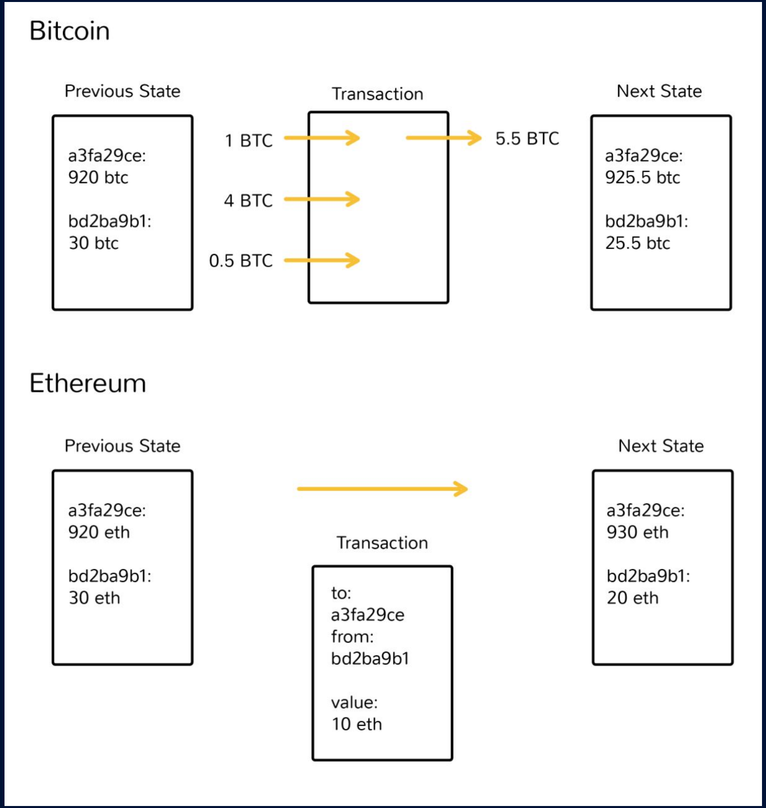
A **contract** is a voluntary arrangement between two or more parties that is enforceable by law as a binding legal agreement

A **smart contract** is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract.

Real world smart contracts

With the present implementations] "smart contract" is general purpose computation that takes place on a blockchain

BTC vs ETH state transition



Ethereum Virtual Machine

Internals

- **TURING COMPLETE VM**
- Stack based byte code (push, jump)
- Memory
- Storage
- Environment variables
- Logs
- Sub-calling

High level languages

- Solidity (c-like)
- Viper (python like)
- LLL (lisp inspired)
- Bamboo (experimental morphing language influenced by Erlang)

Everyone compiling to EVM code

EVM code execution

- Transaction sent to a **contract address**
- **<u>Every full node of ethereum run the code at this address and store the state</u>**
- Smart contract code can:
  - Could run any program (turing complete machine)
  - Read/write state
  - Call another contract
  - Send ETH to other address (both EOA and contract)

Why we need tokens?

Tokens can represent any asset:

- An hours worth of rooftop solar energy (utility token)
- A currency such as dollar or even a company share (security token)
- A promise for a product in a crowdfund...ICOs (utility/security token)
- A future download of a song from your favorite artist (utility token)

It’s something we are used in real world…..

Why we need tokens?

Tokens

- An
- A cu token)
- A pr n)
- A fu token)

It's som

How (fungible) tokens can be used?

Basically they could be used for some special purpose in their Dapp:

- Internal currency
- Right to vote
- Right to use some resources
- Anything it’s pure “counting”

Can be exchanged on the market

Fungibility definition

Wikipedia: In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable.

For example, one kilogram of pure gold is equivalent to any other kilogram of pure gold

ECR-20 standard Ethereum Tokens is fungible. IOW the only things that matter is how many token of a certain type you own.

Until November 2017 every ethereum token was fungible, every different use case was modeled with dedicated smart contracts

Tokens (fungible or not) are smart contracts

With the present implementations] "smart contract" is general purpose computation that takes place on a blockchain

Token contracts are special smart contracts (respecting a standard) storing in blockchain metadatas, balance and ownership for the token itself.

Token smart contracts could other functions doing “something” with or to the token itself. For example: “use” token to give right to vote, “use” token in a game to attack/defend etc. etc.

Fungible vs NonFungible Tokens

Fungible

- Every token is equal to each other
- Can be fractioned/aggregated (100 cents == 1 Dollar)
- Only the balance is registered in blockchain
- You could think it as pure counter of primitive (integer) type.

Non Fungible

- Every token is unique
- Cannot be fractioned
- Blockchain register ID, ownership, and metadatas
- You could think it as an indexed list of complex type (struct or object)

Why NFC matters?

Non Fungible token has unique IDs and may have **unique metadatas associated**.

Smart contracts could change metadatas in reaction of some function, or smart contract functions using NFC could have different behaviour based on NFC metadata.

IOW every NFC could be considered an instance of structured datas, with an owner and maybe a specific lifecycle.

Fungible and NonFungible in real life

Fungible!

Fungible and NonFungible examples

Fungible!

Fungible and NonFungible examples

Fungible!

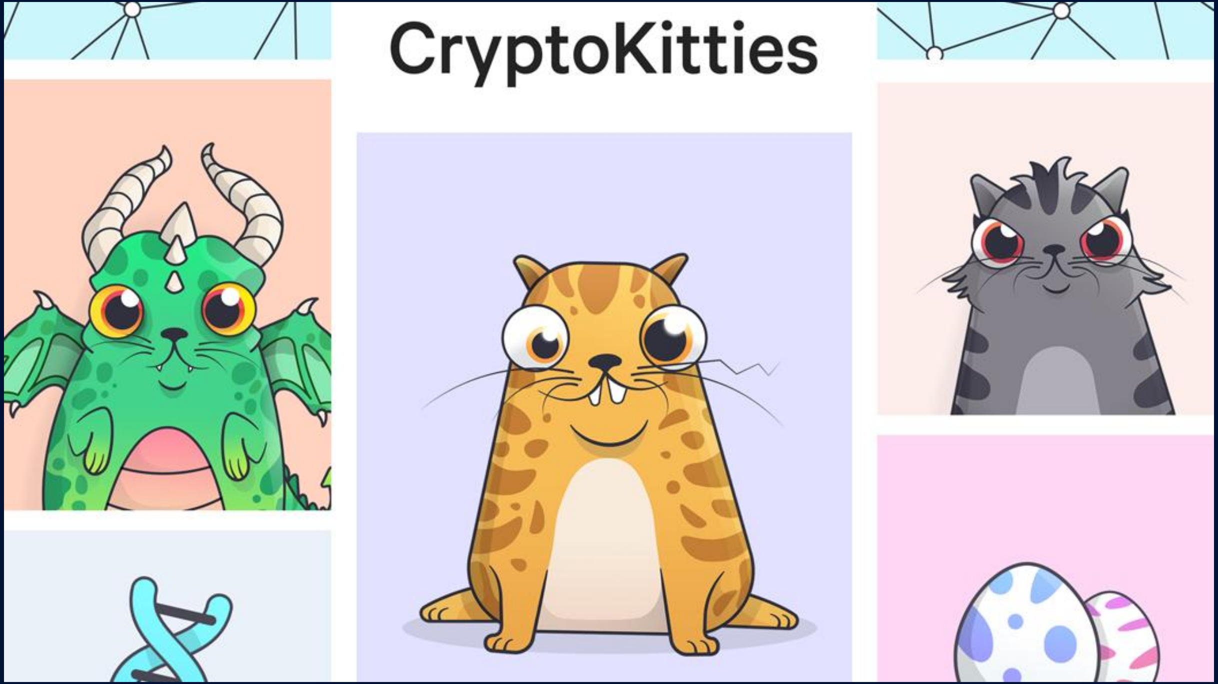
Fungible and NonFungible examples

NON Fungible!

NO: 584970727
JUNE
GARTH BROOKS
THE COUNTRY MEGASTAR WITH
FRIDAY OCT 30TH @ 10:30PM
ENERGY SOLUTIONS
NO: 584970727
OCTOBER 30TH 2015
GARTH BROOKS LIVE
THE COUNTRY MEGASTAR WITH TRISHA YEARWOOD
SECTION 103
ROW 01
SEAT 21
FRIDAY OCT 30TH @ 10:30PM
ENERGY SOLUTIONS ARENA
*these tickets are not actual tickets, tickets must be redeemed using Flash Seats

Fungible and NonFungible examples

NON Fungible!



Fungible and NonFungible in real life

Non Fungible!

Fungible and NonFungible examples

Fungible...or not?

Apple
An EMI Recording
23
The Beatles
Yellow Submarine
NOTHING IS REAL

Fungible and NonFungible in real life

Fungible!

Fungible and NonFungible in real life

Non Fungible!

Fungible and NonFungible in real life

Non Fungible!

Fungible and NonFungible in real life

Fungible!

Or better a non fungible
Made fungible by convention

Fungible and NonFungible in real life

Non Fungible!

Composed!

Fungible and NonFungible in real life

Non Fungible!

Fungible and NonFungible in real life

Fungible!

Mintable only by
Non fungible owner

Use cases

DAO: Distributed Autonomous Organization

https://aragon.one/

Use cases

Prediction Market

- https://gnosis.pm/
- https://www.augur.net/

Use cases

Gaming/collectible

https://www.cryptokitties.co/

Use cases

Gambling

https://dao.casino/

Use cases

Distributed Storage

https://ipfs.io/

https://storj.io/

Use cases

Distributed computing

- https://golem.network/
- https://sonm.com/
- https://www.elastic.pw/

Use cases

Startup and open source founding

- ICOs
- https://gitcoin.co/

Use cases

Supply chain

- NFT and CNFT for single item supply chain
- Provenance and certification

Use cases

Complex contracts and ownership tokenization (NFT)

- Credit management
- Real estate
- Art
- License management
- Patents
- Financial derivative
- Advanced tokenized notarization

Use cases

Identity management

- Personal identity (no google/FB anymore to identify yourself)
- ACL/permissions multi site multi platform
- Personal document notarization/ownership
- Assets/documents portfolio

Use cases

Energy

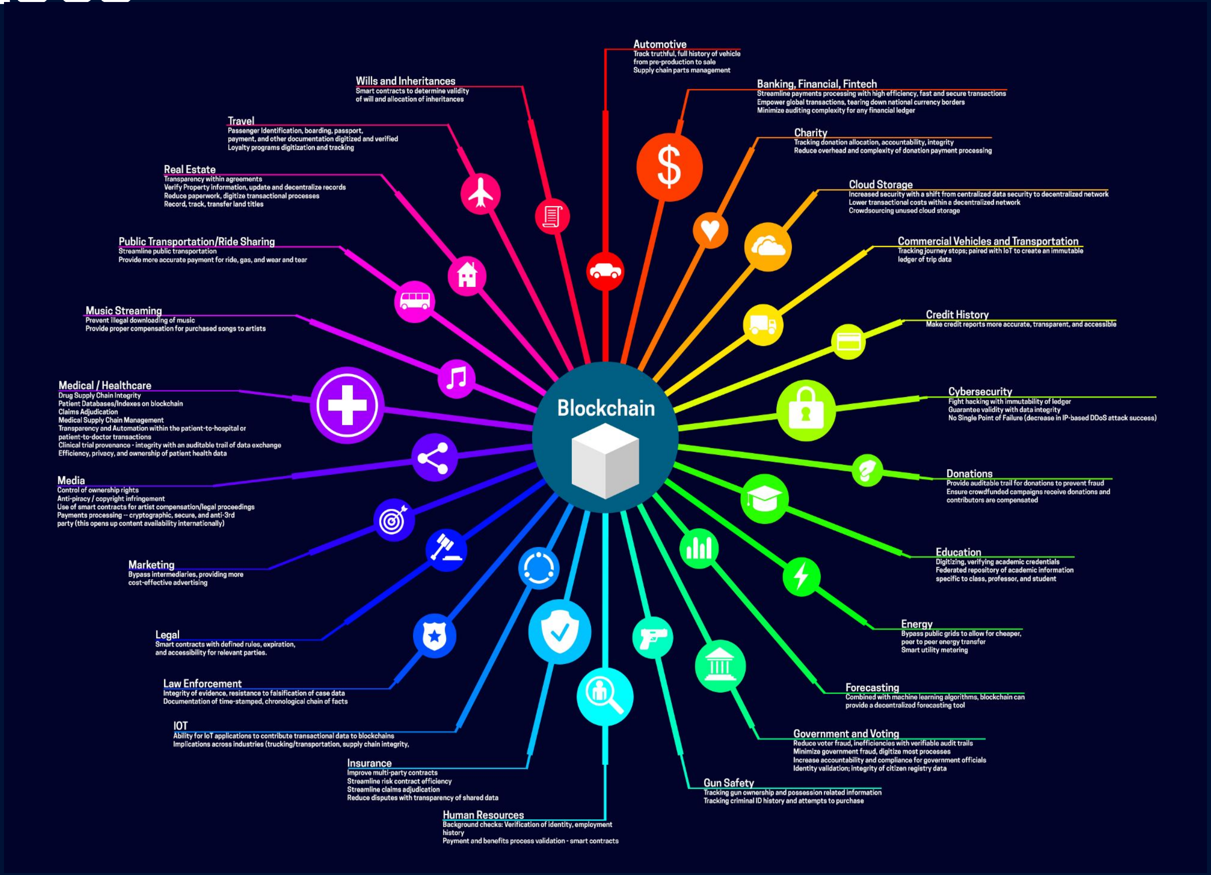
- Smart grid
- Smart charging
- Energy products market

Use cases

IOT

- Supply chain
- Micro payment
- Distributed computing/storage

Use cases



Blockchain

Automotive
Track truthful, full history of vehicle
from pre-production to sale
Supply chain parts management

Banking, Financial, Fintech
Streamline payments processing with high efficiency, fast and secure transactions
Empower global transactions, tearing down national currency borders
Minimize auditing complexity for any financial ledger

Charity
Tracking donation allocation, accountability, integrity
Reduce overhead and complexity of donation payment processing

Cloud Storage
Increased security with a shift from centralized data security to decentralized network
Lower transactional costs within a decentralized network
Crowdsourcing unused cloud storage

Commercial Vehicles and Transportation
Tracking journey stops; paired with IoT to create an immutable
ledger of trip data

Credit History
Make credit reports more accurate, transparent, and accessible

Cybersecurity
Fight hacking with immutability of ledger
Guarantee validity with data integrity
No Single Point of Failure (decrease in IP-based DDoS attack success)

Donations
Provide auditable trail for donations to prevent fraud
Ensure crowdfunded campaigns receive donations and
contributors are compensated

Education
Digitizing, verifying academic credentials
Federated repository of academic information
specific to class, professor, and student

Energy
Bypass public grids to allow for cheaper,
peer to peer energy transfer
Smart utility metering

Forecasting
Combined with machine learning algorithms, blockchain can
provide a decentralized forecasting tool

Government and Voting
Reduce voter fraud, inefficiencies with verifiable audit trails
Minimize government fraud, digitize most processes
Increase accountability and compliance for government officials
Identity validation; integrity of citizen registry data

Gun Safety
Tracking gun ownership and possession related information
Tracking criminal ID history and attempts to purchase

Human Resources
Background checks: Verification of identity, employment
history
Payment and benefits process validation - smart contracts

Insurance
Improve multi-party contracts
Streamline risk contract efficiency
Streamline claims adjudication
Reduce disputes with transparency of shared data

IOT
Ability for IoT applications to contribute transactional data to blockchains
Implications across industries (trucking/transportation, supply chain integrity,

Law Enforcement
Integrity of evidence, resistance to falsification of case data
Documentation of time-stamped, chronological chain of facts

Legal
Smart contracts with defined rules, expiration,
and accessibility for relevant parties.

Marketing
Bypass intermediaries, providing more
cost-effective advertising

Media
Control of ownership rights
Anti-piracy / copyright infringement
Use of smart contracts for artist compensation/legal proceedings
Payments processing -- cryptographic, secure, and anti-3rd
party (this opens up content availability internationally)

Medical / Healthcare
Drug Supply Chain Integrity
Patient Databases/Indexes on blockchain
Claims Adjudication
Medical Supply Chain Management
Transparency and Automation within the patient-to-hospital or
patient-to-doctor transactions
Clinical trial provenance - integrity with an auditable trail of data exchange
Efficiency, privacy, and ownership of patient health data

Music Streaming
Prevent illegal downloading of music
Provide proper compensation for purchased songs to artists

Public Transportation/Ride Sharing
Streamline public transportation
Provide more accurate payment for ride, gas, and wear and tear

Real Estate
Transparency within agreements
Verify Property information, update and decentralize records
Reduce paperwork, digitize transactional processes
Record, track, transfer land titles

Travel
Passenger Identification, boarding, passport,
payment, and other documentation digitized and verified
Loyalty programs digitization and tracking

Wills and Inheritances
Smart contracts to determine validity
of will and allocation of inheritances

Who is behind ethereum?

A Very young….extremely focused guy

Who is behind ethereum?

A Very young….extremely focused guy

Don’t you recall another very young extremely focused guy?

Who is behind ethereum?

Thanks for coming

0x41a6021A6Dc82cbB0cd7ee0E3855654D225F48C6

I’ll use ethers only for beers :)

- https://www.linkedin.com/in/maeste/
- https://twitter.com/maeste
- https://github.com/maeste/
- http://www.onchain.it/