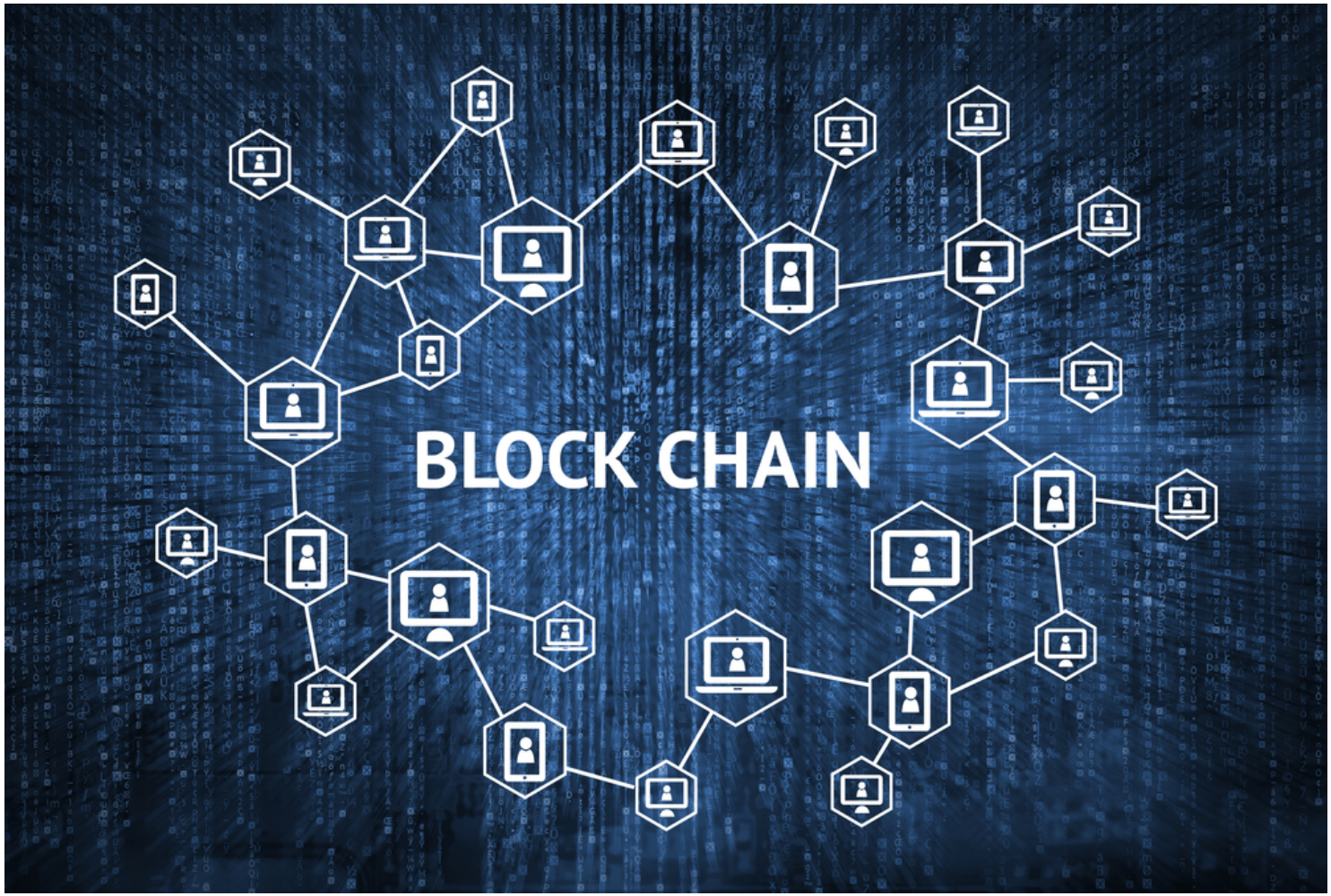


STEFANO BISTARELLI

Italian Distributed Ledger Technology Working Group

Born in January 2018 with the writing of the chapter on blockchain of the libro bianco della Cybersecurity

The group then met in Perugia for the organization of the first workshop on these issues, a workshop that included a round table with participation of institutional Lab CyberSec.

Sito web: **http://dltgroup.dmi.unipg.it**

62 MEMBRI

Coordinatore

Stefano Bistarelli

Core Members

Massimo Bartoletti

University of Cagliari

Paolo Mori

Istituto di Informatica e Telematica del CNR di Pisa

Maurizio Pizzonia

Università degli Studi di Roma Tre

Laura Ricci

Università degli Studi di Pisa

Andrea Vitaletti

Università degli Studi di Roma "La Sapienza"

Roberto Zunino

Università degli Studi di Trento

Members


Edimburgo
Glasgow
Regno Unito
Isola di Man
Dublino
Irlanda
Manchester
Liverpool
Londra
Amsterdam
Paesi Bassi
Bruxelles
Belgio
Lussemburgo
Colonia
Germania
Francoforte sul Meno
Parigi
Francia
Amburgo
Copenaghen
Danimarca
Berlino
Monaco di Baviera
Svizzera
Austria
Praga
Repubblica Ceca
Vienna
Slovacchia
Budapest
Ungheria
Slovenia
Zagabria
Croazia
Bosnia ed Erzegovina
Sarajevo
Serbia
Belgrado
Montenegro
Podgorica
Kosovo
Italia
Monaco
Andorra
Barcellona
Madrid
Spagna
Portogallo
Lisbona
Porto
Valencia
Siviglia
Granada
Málaga
Algeri
Tunisi
Roma
Tirana
Albania
Macedonia del Nord
Bulgaria
Sofia
Romania
Bucarest
Moldavia
Chișinău
Odessa
Ucraina
Polonia
Varsavia
Lettonia
Riga
Lituania
Vilnius
Minsk
Bielorussia
Kiev
Charkiv
Mosca
Istanbul
Bursa
Ankara
Grecia
Atene
Smirne
Turchia
Adalia
Adana

Formal Models for Blockchains

- Mathematical models of blockchain behavior
- Formal models for smart contracts
  - Languages for smart contracts (imperative / process algebras / ...)
  - Secure compilation
    - No vulnerabilities introduced by the compiler
  - Verification of contract-relevant properties
    - BitML Toolchain
- Verified protocols
  - Lotteries
  - Fair games

Cyber Security Research Group

University of Southampton, UK

- **Current Blockchain Research Topics**
  - Benchmark for the analysis of security and performance of permissioned blockchain
  - Scalability of permissioned blockchain
  - Life cycle management of smart contracts in permissionless blockchain
  - Application of blockchain technology to
    - Large-scale, complex supply chains
    - Transactive energy (i.e. p2p trading of electricity)

Point of contact: Dr Leonardo Aniello (l.aniello@soton.ac.uk)

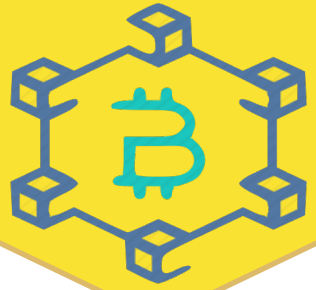
Mixing Services

Visualizations

Agrichain

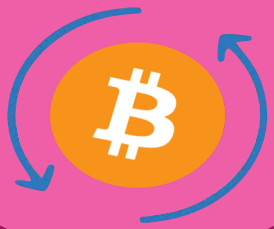
Scraper

Blockchain DB



Clustering

Tx Info



Evote

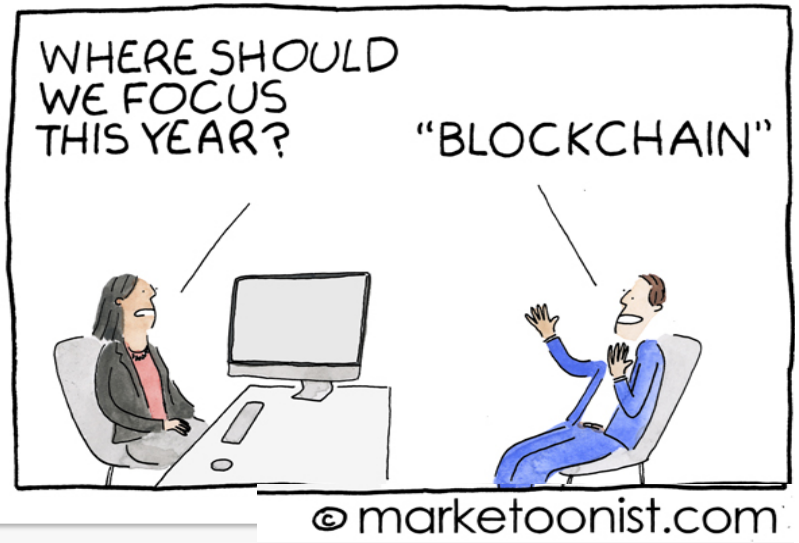
TradeBitcoin

Bitcoin Introduction

Google Trends | Esplora

Blockchain
Argomento

Italia | 01/01/16 - 26/11/19 | Tutte le categorie



Interesse nel tempo

More gold than coin

€6.502,50 EUR (-0,81%)

SPONSORED

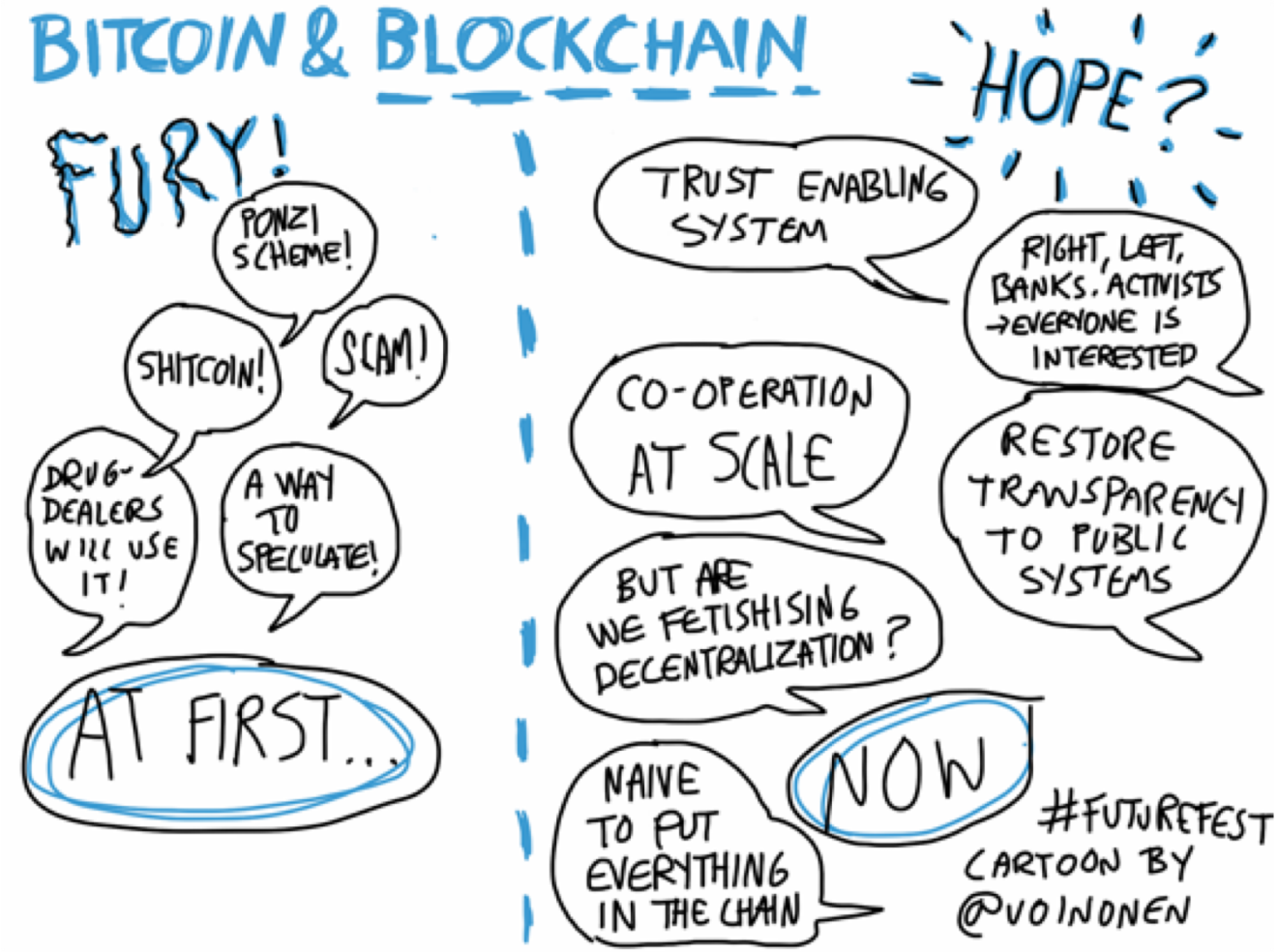
1,00000000 BTC (0,00%)

Condividi | Guarda

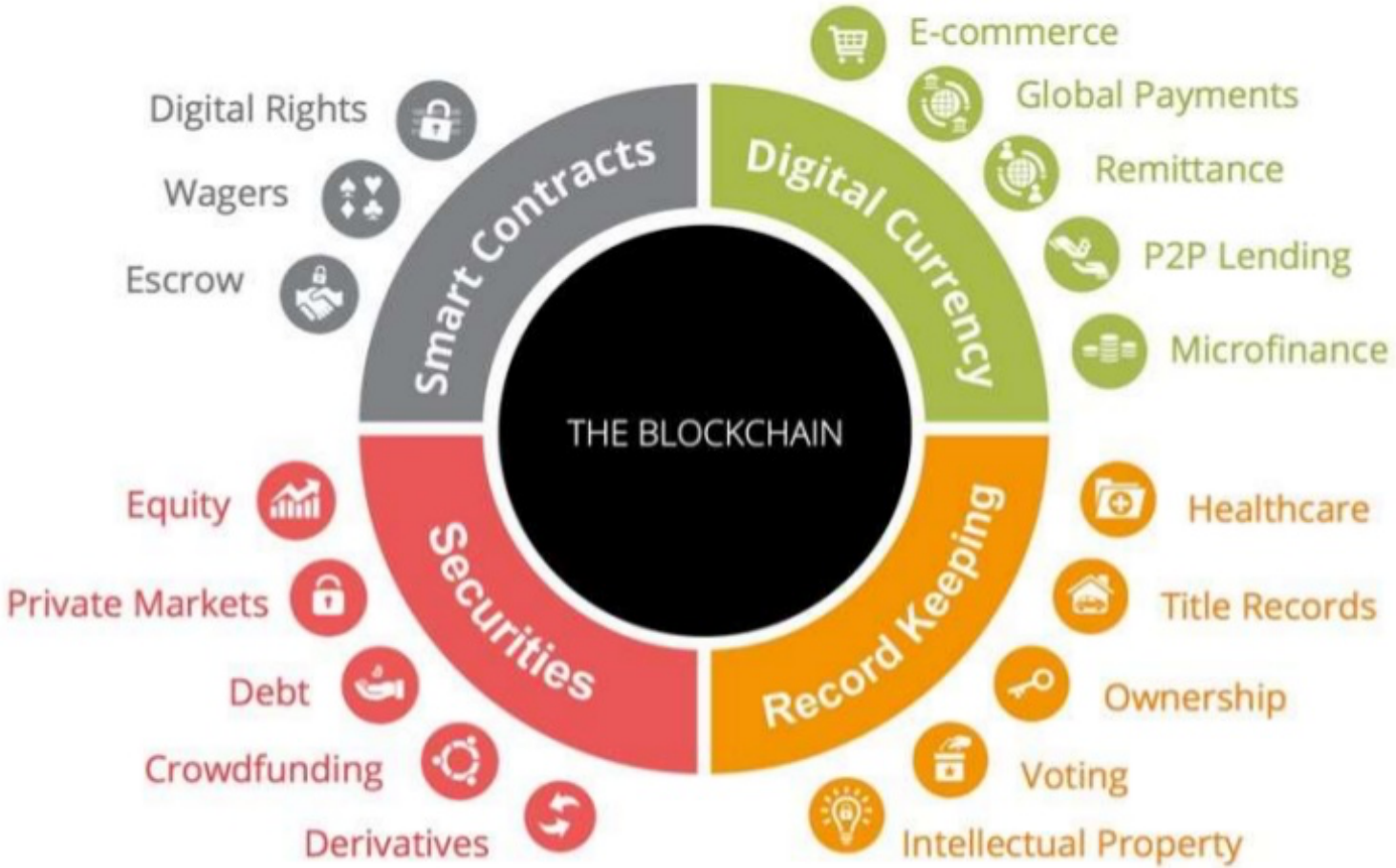
Cap. del mercato	Volume (24h)	Rifornimento circolante
€117.490.057.416 EUR 18.068.450 BTC	€21.675.172.668 EUR 3.333.361 BTC	18.068.450 BTC

Rifornimento massimo
21.000.000 BTC

Friend... Or Foe...



Friend… (to protect)



… or Foe?


Your files are encrypted
To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 21/01/15 - 09:30 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR
Prior to increasing the amount left:
167h 59m 30s
Refresh
Payment
FAQ
Decrypt 1 file for FREE
Support
We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?
bitcoin
Locker v1.7
Locker v1.7
Information
Payment
Files
Status
Time remaining:
69:55:47

What the Hell is this Bitcoin

Trying to explain BitCoin in short form is
no easy task so you must make a choice:

RED PILL

I'll tell you the REAL definition

Don't blame me after.

BLUE PILL

I'll tell you the MATRIX definition

Red Pill Version

BitCoin is an information technology breakthrough that define and implement a secure, decentralized payment system and a tool for the storage, verification and auditing of information, including digital representations of values.

The bitcoin protocol defines an overlay network over Internet that mine bitcoins, each node manage a group of addresses that holds coins, each address is a hashed image of an underlying private-public pair of cryptographic keys and act as a pseudonym of the coin's holder.

The nodes view of this common state is formed by a BlockChain, a shared, append-only, trustable, ledger of all coins transactions. The limits of distributed consensus defined in the Byzantine Problem and CAP Theorem are solved using the technique of proof-of-work…

Blue Pill Version

A story to start…

in **2009**

A norwergian student
purchased **5600 BTC** with **19 €**

Kristoffer Koch

A story to start…

in **2009**

A norwergian student
purchased **5600 BTC** with **19 €**

… then forgot…

Kristoffer Koch

A story to start…

in **2009**

A norwergian student
purchased **5600 BTC** with **19 €**

… then forgot…

in **2013**

1 BTC = 205 €

Koch was Millionaire

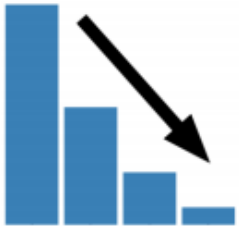
Kristoffer Koch

bitcoin

Peer-to-peer transactions

No need for third parties

Worldwide payments

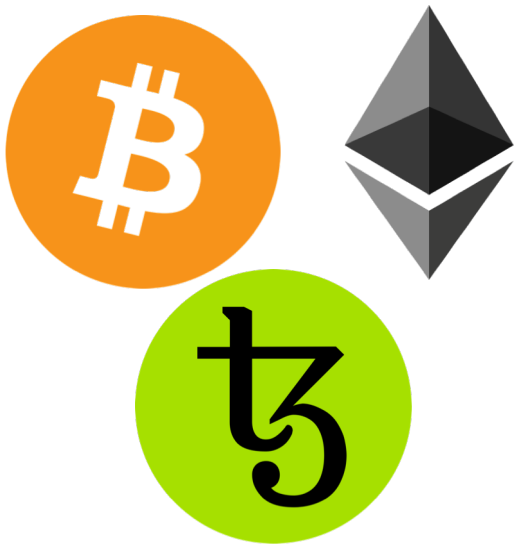


Low processing fees

- 2008 S. Nakamoto. **Bitcoin: A peer-to-peer electronic cash system**. Whitepaper sent on cryptography mailing list.
- 2009 first version of bitcoin node implementation **Bitcoin-Qt**: start of the network and generation of the first bitcoins.

Existing Blockchains

Permissionless



Permissioned

HYPERLEDGER FABRIC

MultiChain

corda

Modello Pubblico

Modello «purista» distribuito

Informazioni registrate pubblicamente in Blockchain, disponibili e verificabili da tutti i player della rete abilitati

Modello Privato

Logica «club ristretto e chiuso»

Partecipazione «su invito» di attori selezionati, con i quali esiste già un consolidato rapporto di fiducia

Public vs Permissioned

Advantages of permissioned blockchains

- Resource control

- Faster Transactions

- Better Scalability

- Consensus More Efficient (less nodes)

HYPERLEDGER
FABRIC

Hyperledger is a great project, first created by IBM, now under the control of The Linux Foundation, which aims to develop blockchain solutions.

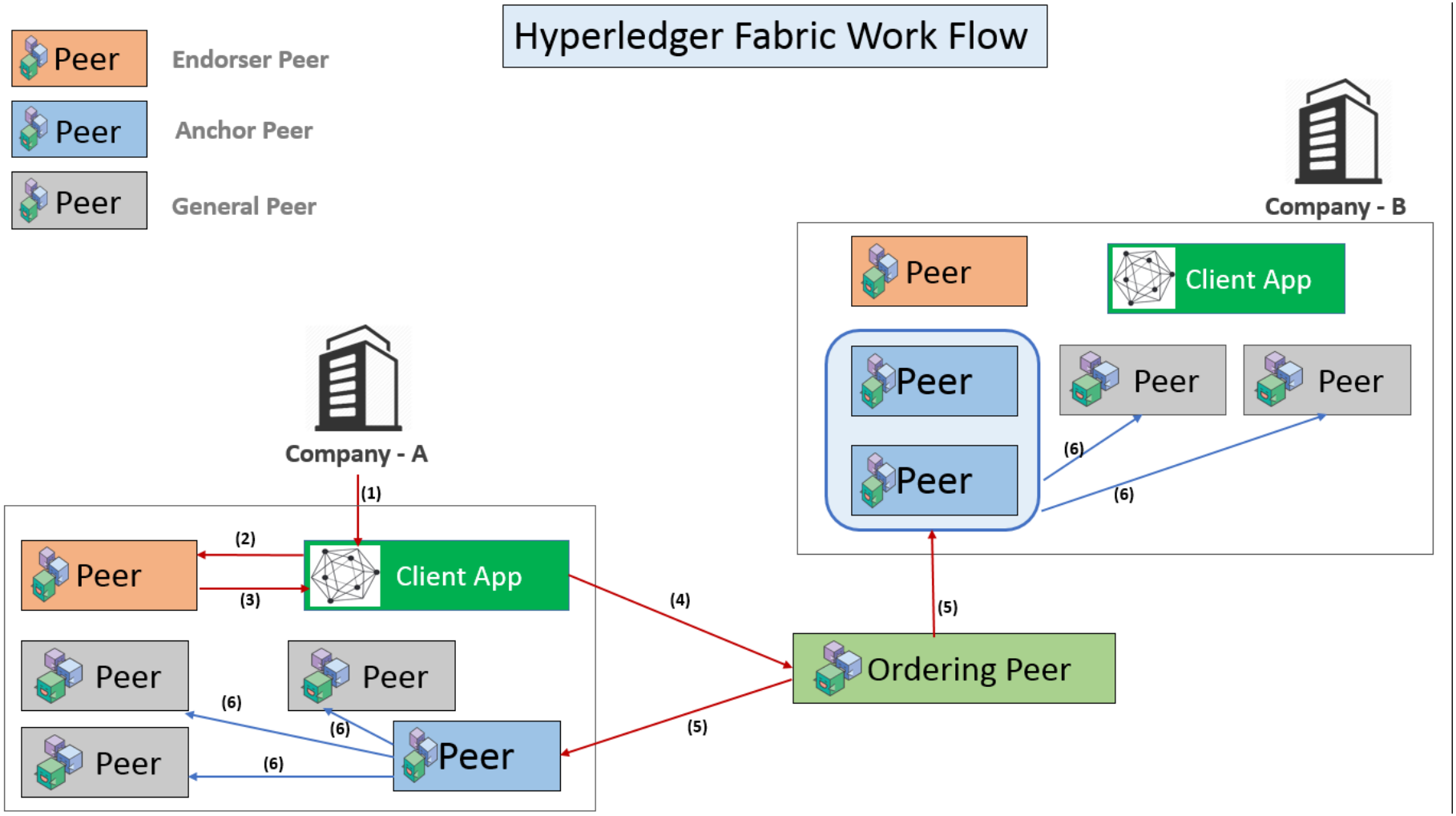
- Modular architecture
- Division of roles between network nodes
- Smart Contract (*chaincode*) powered by different programming languages

Hyperledger architecture

We can have different types of peer nodes:

- Endorser
- Anchor
- Orderer

Hyperledger Fabric Workflow



How data is stored

- Ledger
- State database

The ledger is the actual "blockchain": stores serialized blocks. It is immutable.

The state database holds the last known committed value for any given key.

There are currently two options for the state database: an embedded *LevelDB* or an external *CouchDB*.

TEZOS

Decentralized Blockchain: Governance on chain
No Fork: Voting on improvement

Delagete Proof of Stake

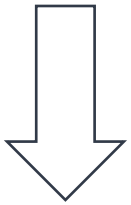
- Virtual "miner" (Backer)
- Communities delegate Backers
- Formal Verification
- Ocam and Michelson

Alphanet:
https://tezos.gitlab.io/tezos/introduction/alphanet.html#alphanet

Policy of Tezos

Possibility of producing new "amendments"

- new policy of the governance
- new voting specifications
- smart contract parameters
- add a block to chain



VOTE

voting on large majority (80%)
Only token holder can vote
It may be possible to delegate the vote

Policy of Tezos

- every cicle all proposals are gathered.
- each proposal is voted by supermajority (80%).
- all the pased proposals are implemented in a soft-fork net (test) for 48h.
- after the test period there is another supermajority vote on the test governance.
- if the test pass, the new governance will be implemented on live net.

Blocks on Tezos

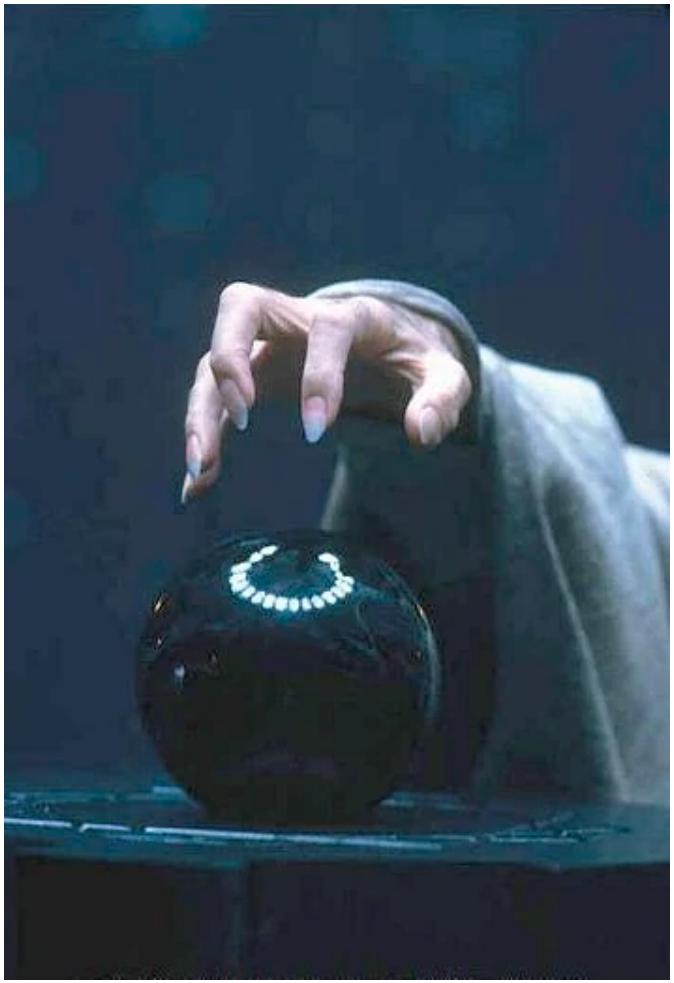
- bounding 8000 XTZ a node can have 1 roll.
- to be a Baker you need at least 1 roll.
- every clock (60'') a block is proposed.
- among all bakers one roll is selected for validation.
- if there are 32 vote, the block pass.
- only after 4096 blocks (1 cicle) the XTZ are unbounded.

Smart Contract

What they can do

- They work as a 'multi-signature' account, that is, the funds are spent only when there is a certain percentage of people involved
- They manage agreements between users, for example an insurance service or the sale of an asset
- They provide services to other contracts (similar to how a software library works)
- They store information about an application, such as user information and their activities in the application.

Oracles



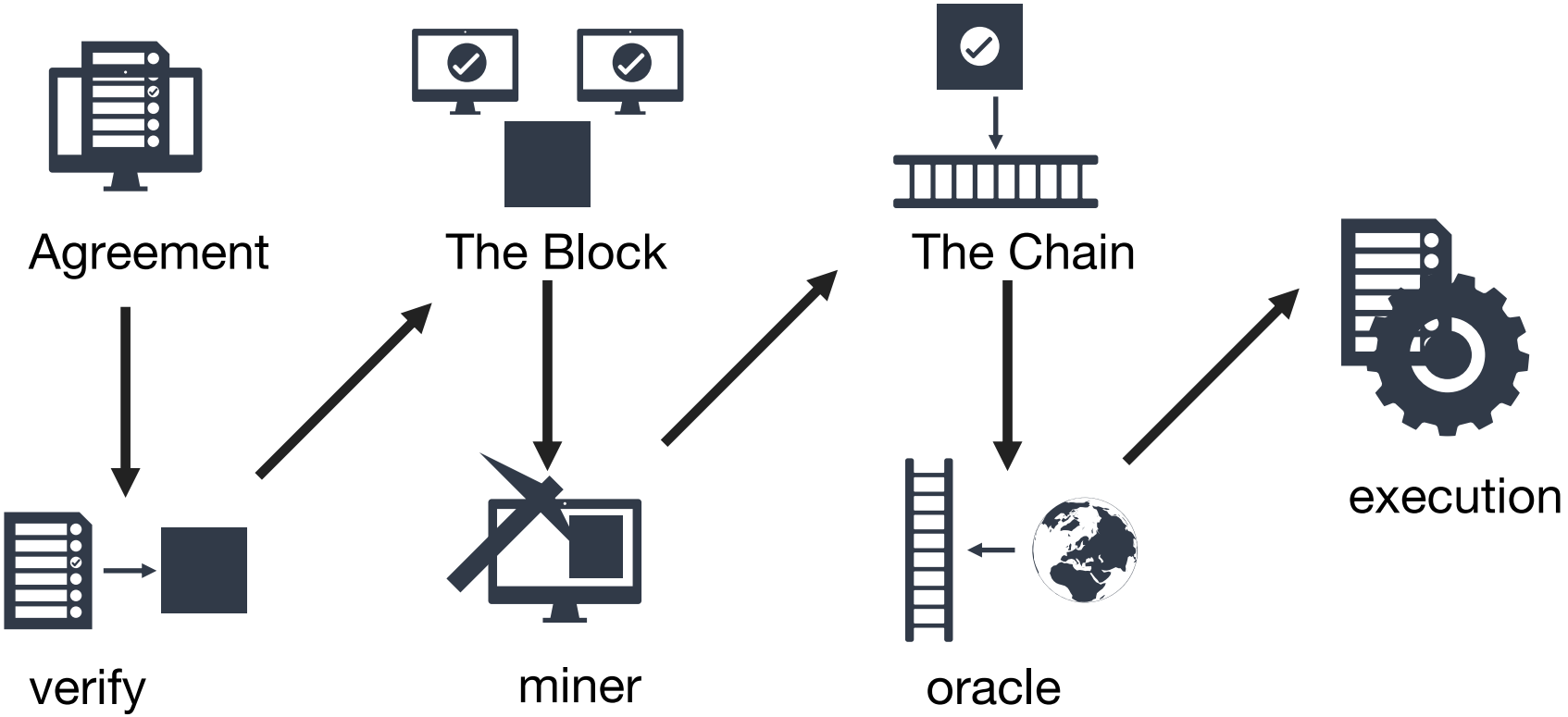
Provable

Provable

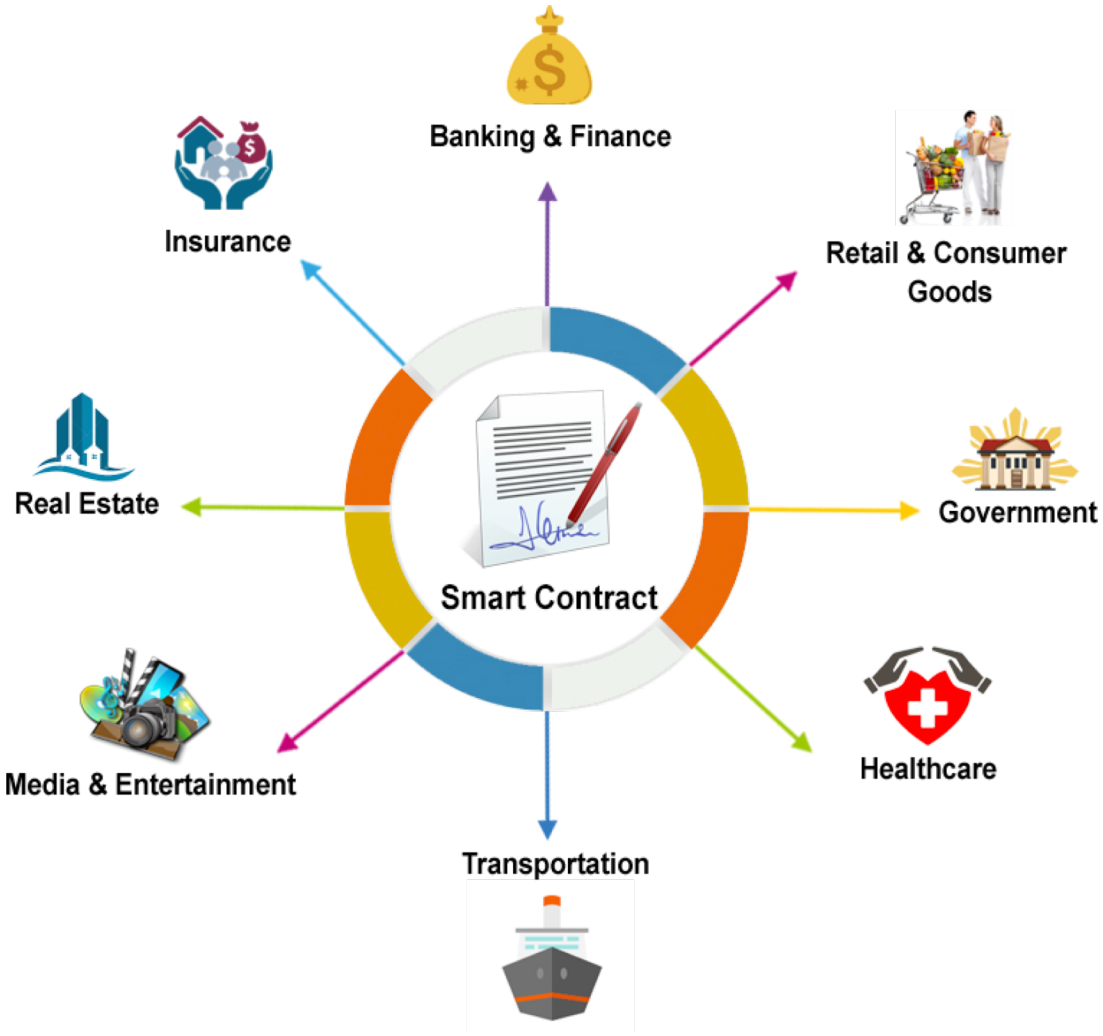
Maker dao

The contracts developed by MakerDAO use the **oracles to know the value of Ethereum** in dollars and to keep the value of the DAI token by means of cryptoeconomic incentives.

Life of a smart contract



Application fields



Examples

BANKING & FINANCE

Compound

GNOSIS

GOVERNAMENT

ARAGON

REAL ESTATE

golem

INSURANCE

Ethlance

HEALTHCARE

uport

MEDIA & ENTERAINEMENT

CryptoKitties

Italian law

"A computer program that operates on technologies based on distributed registers and whose execution automatically binds two or more parts on the basis of predefined effects".

BUGS!

Estimates in ethereum

- 34,200 potentially vulnerable
- 3.4% of total smart contracts
- Involving about 4.105 Ether
- For a value greater than € 803,000

The Dao

Thanks for your attention.